

злочинця; інформаційні сліди у вигляді аудіо-відео записів, що мають відношення до справи.

Ефективність розслідування залежить від того, наскільки діяльність слідчого та взаємодіючих з ним органів дізнання відповідає особливостям злочину та обстановки, що складається під час розслідування. Така відповідність насамперед багато в чому визначається чітким уявленням про предмет доказування.

Вважаємо, що для підвищення ефективності розслідування торгівлі людьми є дослідження і подальша розробка типових слідчих ситуацій і розробка на цій основі рекомендацій з методики розслідування торгівлі людьми необхідні для правильної побудови слідчих версій, визначення напрямку розслідування, виявлення обставин, що мають значення для справи.

Одержано 30.10.2017

УДК 343.38

Андрій Анатолійович ВАСИЛЬЄВ,

кандидат юридичних наук, доцент, професор кафедри кримінального права і кримінології факультету № 1 Харківського національного університету внутрішніх справ

ДО ПИТАННЯ ПРО ПОСИЛЕННЯ ВІДПОВІДАЛЬНОСТІ ЗА ВЧИНЕННЯ ЗЛОЧИНУ З ВИКОРИСТАННЯМ ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМ

Інформаційно-телекомунікаційні, інформаційні та телекомунікаційні системи як засоби або способи для з'єднання окремих користувачів у мережі Інтернет, а також соціальні служби (мережі) чи відеохостинги, настільки глибоко проникли у наше повсякденне життя, що ігнорування тих загроз, які існують поряд із безумовно позитивними їх якостями вже не тільки помилково, а у окремих випадках навіть злочинно. Мова йде про використання указаних систем як для вчинення явно злочинних діянь (наприклад, шахрайства, збуту наркотичних засобів та психотропних речовин, а в окремих випадках зброї та небезпечних матеріалів), так і для поширення закликів до вчинення протиправних діянь, схилення до розпалювання ненависті чи розбрату, поширення неправдивої інформації, яка містить відомості, що ганьблять конкретну особу чи групу осіб тощо. Інформація, що поширюється мережею Інтернет, користувачем, нажаль, не завжди сприймається критично, що використовується автором або «власником» цієї інфо-

рмації у корисливих чи інших цілях, іноді злочинних. Указане свідчить про необхідність перегляду норм чинного законодавства, перш за все кримінального, в частині врегулювання указаних проблем.

Питання врегулювання сфери Інтернет-відносин, упорядкування того масиву інформації, яка поширюється в цій мережі, у тому числі кримінальної відповідальності за порушення у цій сфері не є новим для нашої країни, так, зокрема, воно було предметом дискусій на інформаційних форумах, розглядалося на сторінках друкованих видань. Так, спроби вирішити окремі питання відповідальності за кіберзлочини та злочини у сфері використання ЕОМ (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку розглядалися в роботах Д. С. Азарова, Ю. М. Батуріна, П. Д. Біленчука, М. В. Карчевського, М. О. Кравцової, В. В. Крилова, Ю. І. Ляпунова, О. В. Манжя, А. А. Музики, П. І. Орлова, С. О. Орлова, Д. В. Пашнева, Н. А. Розенфельда та інших науковців.

Однак, навіть ураховуючи внесок указаних науковців у вирішення питання протидії кіберзлочинності на сьогодні, на жаль, доводиться констатувати як підвищення кримінального комп'ютерного професіоналізму, високу мобільність злочинців при недостатній кількості фахівців-правоохоронців, так і відсутність законодавчо врегульованого механізму забезпечення протидії поширенню кіберзагроз.

Безумовно, окремі кроки у напрямі врегулювання обігу потенційно шкідливого контенту здійснені і на державному рівні, так, указом Президента від 15 травня 2017 року № 133/2017 було введено в дію рішення Ради національної безпеки і оборони України від 28 квітня 2017 року «Про застосування персональних спеціальних економічних та інших обмежувальних заходів (санкцій)» [1], яким, зокрема, було обмежено доступ до російських інформаційних ресурсів в Інтернеті: Yandex, соцмереж «ВКонтакте» та «Однокласники», а також заборонено використання бухгалтерського програмного продукту 1С. Не вдаючись до оціночних суджень щодо необхідності саме такого способу протидії потенційним небезпекам, які поширюються в інформаційному просторі, слід зазначити, що це лише незначний крок на шляху упорядкування обігу шкідливих даних, адже існує безліч способів оминати таке блокування. Потребує вироблення цілий комплекс заходів, спрямованих на убезпечення безпеки як держави в цілому,

так і окремих громадян. Одним із найбільш дієвих способів запобігання вчиненню правопорушень залишається криміналізація окремих форм вчинення діяння або посилення (введення додаткових умов) відповідальності за використання деяких способів вчинення діяння. Однак, як слушно зазначають І. В. Владенова та Е. А. Кальницький, «у формуванні політики і засобів боротьби з проблемою кіберзлочинності необхідно уникати надмірного регулювання при збереженні відкритості Інтернету і захисту прав людини, як-то: право на приватне життя і інформаційне самовизначення, свободу слова, інформації та комунікації» [2].

Використання мережі Інтернет чи інших систем або мереж, по-перше, полегшує вчинення окремих злочинів через свою доступність, по друге, через можливість анонімності є привабливим способом вчинення злочину та породжує «ілюзію уседозволеності», і, нарешті – спосіб спрямований на невизначене коло осіб, що створює небезпеку як для осіб, які розуміють протиправність посягання, так і для неповнолітніх чи малолітніх, які не здатні усвідомлювати небезпеки.

Слід вказати, що у чинному КК України вже передбачено у якості кваліфікуючої ознаки для окремих складів злочинів їх вчинення «з використанням засобів масової інформації». Однак, згідно закону, під засобами масової інформації розуміються газети, журнали, теле- і радіопрограми, кінодокументалістика, інші періодичні форми публічного розповсюдження масової інформації, які відповідним чином зареєстровані. До них не можна відносити, зокрема, блогерів, які мають акаунти на відеохостінгу «Youtube», осіб, які створюють і модерують групи у соціальних мережах чи месенджерах.

Використання ж можливостей указаних мереж або систем дає змогу звертатися до невизначеної кількості осіб і розповсюдження інформації, поширення якої створює певні умови (обставини), наявність яких ставить у небезпеку певні суспільні відносини (наприклад, поширення у соціальних мережах реклами щодо придбання наркотичних засобів, реклама «ес-корт» послуг тощо).

Зазначене дозволяє зробити висновок про необхідність урахування розвитку інформаційних технологій і сфер використання інформаційно-телекомунікаційних систем, зокрема, при внесенні змін у кримінальне законодавство. Зміни, спрямовані на посилення відповідальності за вчинення злочину з використанням інформаційно-телекомунікаційних систем,

можливі у таких формах: введення кваліфікуючої ознаки та утворення кваліфікованого складу злочину (наприклад, у ч. 3 ст. 109, ст. 113, ч. 2 статей 161, 182, ч. 3 ст. 190, ч. 2 статей 258, 258-2 КК України тощо) або введення такого «використання» в якості обставини, що обтяжує покарання (наприклад, у ст. 67 КК України). Однак, такі істотні нововведення потребують подальших наукових досліджень та додаткового обґрунтування підстав криміналізації.

Список використаних джерел:

1. Про застосування персональних спеціальних економічних та інших обмежувальних заходів (санкцій): Указ Президента України від 15.05.2017 р. № 133/2017. URL: <http://zakon3.rada.gov.ua/laws/show/n0004525-17> (дата звернення: 26.10.2017).
2. Владленова І. В., Кальницький Е. А. Кіберзлочинність як виклик інформаційному суспільству. *Гілея: науковий вісник*. 2013. № 77. С. 142–146. URL: http://nbuv.gov.ua/UJRN/gileya_2013_77_45 (дата звернення: 26.10.2017).

Одержано 30.10.2017

УДК 343.1 + 004

Андрій Вікторович ВІНАКОВ,

кандидат юридичних наук, керуючий партнер компанії ІЛР

Ірина Андріївна МАНЖАЙ,

завідувач навчального відділу Харківського економіко-правового університету

ОКРЕМІ ПИТАННЯ ФІКСАЦІЇ ЕЛЕКТРОННИХ ДОКАЗІВ

На теперішній час в Україні нема єдиної сталої термінології, яка б визначала докази, одержані з носіїв цифрових даних, а також чітко не визначено порядок роботи з ними. Тому на практиці нерідко виникають питання щодо правильного оформлення таких доказів та їх представлення в суді.

20.06.2017 року Верховна Рада України в першому читанні прийняла проект закону № 6232 «Про внесення змін до Господарського процесуального кодексу України, Цивільного процесуального кодексу України, Кодексу адміністративного судочинства України та інших законодавчих актів». У даному документі пропонується розуміти під електронними доказами інформацію в електронній (цифровій) формі, що містить дані про обставини, що мають значення для справи, зокрема, елек-