танням протоколу огляду. У другому випадку процес документування оформлюється протоколом негласної слідчої (розшукової) дії щодо зняття інформації з електронних інформаційних систем, доступ до яких не обмежується її власником, володільцем або утримувачем або не пов'язаний з подоланням системи логічного захисту, а тому не потребує дозволу слідчого судді (ч. 2 ст. 264 Кримінального процесуального кодексу України). Різниця в підходах пояснюється суперечностями щодо належності інформації в електронній формі до місцевості, приміщення, речей або документів, щодо яких можна здійснювати огляд (ч. 1 ст. 237 Кримінального процесуального кодексу України). Водночас більшість правоохоронних органів в регіонах все ж тяжіють до використання першого підходу – оформлення електронних доказів протоколом огляду.

Список використаних джерел:

1. Виявлення, попередження та розслідування злочинів торгівлі людьми, вчинених із застосуванням інформаційних технологій (Проект): навчальний курс / [В. Гузій, Д. Девіс, В. Дубина, М. Каліжевський, О. Манжай, В. Марков]. К., 2015. 158 с.
2. Cybercrime and its victims / Edited by Elena Martellozzo, Emma A Jane. 2017. Routledge. 230 p.
3. British paedophile Paul Leighton jailed for 16 years for rape. URL: https://www.theguardian.com/uk-news/2017/sep/04/british-paedophile-paul-leighton-jailed-for-16-years-for-rape (дата звернення: 22.09.2017).

Одержано 30.10.2017

УДК 343.13

Євгеній Олександрович НАЛИВАЙКО,
кандидат юридичних наук, викладач відділу підготовки прокурорів з нагляду за додержанням законів органами, які проводять оперативно-розшукову діяльність, дізнання та досудове слідство Національної академії прокуратури України

КРИМІНАЛІСТИЧНІ ТА ПРОЦЕСУАЛЬНІ ОСОБЛИВОСТІ У ЗЛОЧИНАХ ПОВ'ЯЗАНИХ ІЗ КІБЕРЗЛОЧИННІСТЮ

На актуальність та необхідність теми вдосконалення боротьби з кіберзлочинністю вказує кількість злочинів у даній сфері яка постійно зростає.

Відповідно до принципів сучасного міжнародного кримінального права злочини з використанням комп'ютерних технологій (інакше «кіберзлочини») віднесені до злочинів міжнародного характеру. Перелік видів кіберзлочинів визначається

Конвенцією про кіберзлочинність (2001 р.), яка називає серед інших наступні склади: незаконний доступ до комп'ютерної системи, нелегальне перехоплення технічними засобами комп'ютерних даних, втручання у комп'ютерні данні, втручання у функціонування комп'ютерної системи, підробку та шахрайство пов'язане з комп'ютерами.

На сучасному етапі, в Україні, до найбільш актуальних схем кіберзлочинів можливо віднести – фішинг, вішинг, соцінженерія та злочини у банкоматній мережі. З цього приводу навіть є «Методичні рекомендації МВС України щодо виявлення та документування злочинів пов'язаних з несанкціонованим використанням пристроїв - ,,скіммерів", для отримання інформації про банківські платіжні картки Управління боротьби з кіберзлочинністю МВС України» 2013 року.

Одним з проблемних питань є те, що діючий Кримінальний процесуальний кодекс фактично не містить положення, які дають змогу використовувати докази в електронній формі. Таким чином, значно ускладнюється можливість доказування наявності того чи іншого протиправного діяння, пов'язаного з рухом інформації в електронному вигляді в реальному масштабі часу. Саме рух інформації в цифровому вигляді є об'єктом протиправних діянь, які кваліфікуються як кіберзлочини. Разом із тим особливості слідоутворення та збору доказової бази залежить від середовища їх скоєння.

Згідно зі ст. 84 КПК доказами в кримінальному провадженні є фактичні дані, отримані у передбаченому КПК порядку, 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. Особливою формою є електронні докази. Процесуальними джерелами доказів є: показання, речові докази, документи, висновки експертів. Зазначений перелік є вичерпним.

Поряд із цим можливо вказати на позитивну норму в контексті означеної проблеми, а саме: ч. 2 ст. 8 Закону України «Про електронні документи та електронний документообіг», відповідно до якої допустимість електронного документа як доказу не може бути спростована лише на підставі того, що він має електронну форму.

Наразі фактично єдиним способом використання електронної інформації як доказів у суді є висновок експерта. Таким чином, доказами у кримінальній справі можуть бути ви-

користанні висновки комп'ютерно-технічної експертизи, виконаної відповідно до Закону «Про судову експертизу». Позитивним в цьому аспекті є можливість здійснення експертизи не тільки в державних спеціалізованих установах, а й у незалежних експертів, які атестовані в порядку, визначеному законодавством України.

На даний час проаналізувавши експертну практику можливо пересвідчитися у постійному збільшенні кількості експертних завдань щодо пошуку на комп'ютерних носіях інформації, яка стосується роботи користувача персонального комп'ютера (ПК) у глобальній мережі Інтернет, тобто звернення його на конкретні сайти, хронології чи історії звернень тощо. Це зумовлено збільшенням кількості кримінальних проваджень, пов'язаних з противоправним поширенням у глобальній мережі певної інформації, у тому числі кримінального характеру (щодо торгівлі людьми, розповсюдження порнографічних зображень тощо).

Вважаємо за необхідне наголосити на невідповідність тяжкості покарання передбаченому у законодавстві України у вказаній категорії злочинів, що також не є стримуючим фактором у діях злочинців, тобто міра покарання практично усіх злочинах не перевищую середню тяжкість, а отже не завжди можливо застосування НСРД.

Як приклад у Іспанії лише за перетинання границі з фальшивими кредитними карточками, борговими картками чи акредитивами передбачене покарання від восьми до десяті років позбавлення волі та штрафу у десятикратному розмірі підроблених грошей.

Ще одним проблемним питанням у злочинах пов'язаних із кіберзлочинністю можна назвати відсутність можливості дослідження електронних доказів, котрі зберігаються на віддалених серверах. На даний час ними можуть бути сервіси зберігання інформації в мережі Інтернет (Adrive, Box.net, Clip2Net, DropBoks, SkyDrive, MediaMax та ін.), електронні скриньки, системи інтернет-банкінгу та ін. Натомість відбувається дослідження їх паперових аналогів. Однак завдяки порівняно нескладному обладнанню, дослідження таких доказів може вийти на якісно новий рівень. Це також могло б суттєво підвищити ефективність дослідження не лише електронних, а й інших доказів (фотоілюстрацій висновків експертів, протоколів слідчих дій, інших додатків).

З огляду на викладене, з метою покращення можливостей розслідування даної категорії злочинів необхідне вдосконалення як процесуального законодавства так і криміналістичного (постійної розробки новітньої методиці збирання та дослідження електронних доказів на досудовому провадженні, та методика дослідження цих доказів у судовому засіданні). З урахуванням сучасних можливостей криміналістики необхідно підвищити принаймні базовий рівень знань у галузі ІТ технологій усіх осіб, які здійснюватимуть пошук і фіксацію та досліджуватимуть електронні докази.

Одержано 01.11.2017

УДК 343.1 + 004

Віталій Вікторович НОСОВ,
кандидат технічних наук, доцент, професор кафедри кібербезпеки факультету № 4 Харківського національного університету внутрішніх справ

ДЕЯКІ ПРАКТИКИ ЗАБЕЗПЕЧЕННЯ НАЛЕЖНОСТІ ДОКАЗІВ, ОТРИМАНИХ З ОНЛАЙН РЕСУРСІВ

Злочини, що пов'язані із торгівлею людьми, широко застосовують інформаційні технології шляхом: організації в онлайн-режимі секс-чатів, відео трансляцій сексуальних дій; вербування жертв через веб-сайти з оголошеннями про працевлаштування; публікації на різноманітних ресурсах в Інтернеті пропозицій щодо надання сексуальних послуг; і таке інше.

При розслідування злочинів торгівлі людьми, вчинених із застосуванням інформаційних технологій, здійснюється пошук доказів, на підставі яких суд буде вирішувати питання про вину підозрюваних в учиненні кримінального злочину. Онлайн-ресурси в Інтернеті, пов'язані із торгівлею людьми, можна розглядати як цифрові джерела речових доказів, які мають певні унікальні характеристики порівняно із традиційними доказами.

Відповідно до ст. 94 Кримінального процесуального кодексу України кожен доказ у кримінальному провадженні має оцінюватися з точки зору належності, допустимості, достовірності. При оцінці належності доказів із цифрових джерел інформації можуть використовуватися критерії: справжності, повноти, надійності, переконливості.

Для забезпечення належності доказів, отриманих з онлайн ресурсів в Інтернеті, представляється доцільним використання