Підсумовуючи викладене, зазначимо, що наведені завдання слідчого експерименту можуть виступати підставою для виділення окремих видів цієї слідчої (розшукової) дії, які дозволять визначати доцільність її проведення в певних слідчих ситуаціях.

Література:

1. Інтернет ресурс. URL : https://reyestr.court.gov.ua (дата звернення 10.04.2021).
2. Стратонов В. М. Автореф. дис. …. канд. юрид. наук. – Харків, 2002.
3. Котюк О. І. Слідчий експеримент – процесуальні аспекти / О. І. Котюк // Бюлетень Міністерства юстиції України. 2013. № 3 (137). С. 130–135.
4. Балицький Т. М. Слідчий експеримент в системі слідчих (розшукових) дій у кримінальному провадженні України : дис. …канд.. юрид. наук : спец. 12.00.09 / Т. М. Балицький. – Ірпінь, 2015. 216 с.
5. Кримінальний процесуальний кодекс України. Закон від 13.04.2012 № 4651-VI. Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/4651-17 (дата звернення: 12.04.2021).
6. Криміналістика: підручник / за ред. В. Ю. Шепітька. 4-е вид., переробл. і допов. Х.: Право, 2008. С. 326.
7. Дунаєвська Л. Г., Пилипчук О. П. Перевірка показань на місці як вид слідчого експерименту / Л. Г. Дунаєвська, О. П. Пилипчук // Вісник кримінального судочинства. 2018. № 4. С. 29.

DOI https://doi.org/10.30525/978-9934-26-074-2-64

ПРОБЛЕМНІ ПИТАННЯ ФОРМУВАННЯ КРИМІНАЛІСТИЧНОЇ ХАРАКТЕРИСТИКИ КІБЕРЗЛОЧИНІВ

Латиш К. В.
кандидат юридичних наук,
асистент кафедри криміналістики
Національного юридичного університету імені Ярослава Мудрого
м. Харків, Україна

Криміналістична характеристика кіберзлочину являє собою певну інформаційну модель (базис) з криміналістично значущими ознаками цього виду злочинів. Саме за допомогою цієї моделі можливе в подальшому вироблення криміналістичних рекомендацій щодо типових

слідчих ситуацій та побудови слідчих версій, вибору напрямку розслідування, особливостей проведення окремих слідчих (розшукових) дій та вироблення рекомендацій щодо взаємодії між учасниками слідчої діяльності. Досвід побудови та використання цієї моделі бере свій початок щонайменше ще з 1924р., коли І.М. Якимов видав «Практическое руководство к расследованию преступлений» [1]. Безпосередньо термін «криміналістична характеристика злочину» вперше був використаний у 1967 р. в авторефераті докторської дисертації О.Н. Колесніченко «Наукові та правові основи розслідування окремих видів злочинів» [2].

Важливість розробки та використання криміналістичної характеристики кіберзлочинів підкреслюється ще й тим, що цей злочин не має національних кордонів. Через всесвітню мережу інтернет кіберзлочинці можуть вільно об'єднуватися у групи та обмінюватися досвідом. У той час, як правоохоронні органи таких держав позбавлені можливості оперативно відслідковувати такі кооперації та вживати заходів до викриття.

У науці вирізняють також кримінально-правові, кримінологічні та кримінально-процесуальні характеристики злочинів, які істотно різняться від криміналістичної характеристики за змістом та метою формування.

До елементів криміналістичної характеристики кібервандалізму відносяться предмет злочинного посягання, спосіб злочину, у тому числі готування, вчинення та його приховування, обстановка, час та місце вчинення, особа злочинця та потерпілого, типові сліди злочину.

Способи та знаряддя вчинення кіберзлочинів, як і «слідова картина», що утворюється, є специфічними та нетрадиційними для криміналістики. Так, зокрема, це простежується у такій справі, коли «ботоферми» використовувались для спроби викрадення персональних даних шляхом розсилки спаму у месенджері на особисті номери працівників СБУ. У повідомленнях містилося посилання на веб-ресурс, після переходу на який скачувався архівний документ із вірусом. Він надавав доступ до інформації на уражених пристроях, зокрема до log-файлів з ключами доступу до банківської системи, поштових сервісів та облікових записів соціальних мереж тощо. В якості знарядь, які використовуються для вчинення кіберзлочинів, використовувалося спеціальне обладнання, понад тисяча SIM-карток українських мобільних операторів, GSM шлюзи на 78 онлайн-каналах, комп'ютерне обладнання зі шкідливим програмним забезпеченням, мобільні пристрої, флеш-накопичувачі та інші речові докази [3].

Криміналістично значущі ознаки кіберзлочинця можуть різнитися залежно від виду кіберзлочину. Деякі науковці пропонують виходити із розмежування наявних видів кіберзлочинів за формою прояву злочинного діяння на активні та пасивні. Так, до активних відносять кібертероризм, погроза фізичної розправи, кіберпереслідування, кібер-

сталкінг. До групи пасивних: кіберкрадіжки, кібервандалізм, кібершахрайство, кібершпигунство та поширення спаму і вірусних програм [4, с. 201]. Інші науковці поділяють кіберзлочинців на три категорії: до першої групи належать особи, в яких простежується поєднання комп'ютерного професіоналізму та програмування з елементами своєрідного фанатизму і винахідливості, які сприймають засоби комп'ютерної техніки як виклик своїм творчим і професійним знанням; до другої групи відносяться особи, які страждають на інформаційну (комп'ютерну) залежність; до третьої групи входять професійні «комп'ютерні» злочинці з яскраво вираженими корисливим мотивами [5].

Типові сліди кіберзлочинів представлені у вигляді традиційних матеріально-фіксованих слідів та віртуальних (електронних). Відносно матеріально-фіксованих слідів є багато досліджень, які об'єднані у таку галузь криміналістичної техніки, як трасологія. Що стосується віртуальних слідів, то тут точаться дискусії з приводу формування визначення, поняття та змісту цієї категорії. Так, у теорії криміналістики є різні думки про те, що варто розуміти під віртуальними слідами: 1) віртуальні сліди як зміна автоматизованої інформаційної системи; 2) віртуальні сліди з точки зору фізичної і квантової теорії; 3) віртуальні сліди як результат логічних і математичних операцій з двійковим кодом і багато інших [6, с. 305].

Отже, на цей час у науці відсутня превалююча думка з приводу поняття віртуальних слідів, що потребує подальших розробок. При цьому необхідно враховувати не лише сліди, залишені на комп'ютерних та інших стаціонарних джерелах такі, як сліди на жорсткому диску, магнітній стрічці, оптичному диску, на дискеті; сліди в оперативних запам'ятовуючих пристроях ЕОМ, периферійних пристроях, комп'ютерних пристроях зв'язку і мережевих пристроях; сліди в дротяних та інших електромагнітних системах і мережах зв'язку [7, с. 159–160], але й у більш широкому сенсі – щодо усіх цифрових носіїв та хмарних сховищ, які не мають матеріалізованої форми.

Під час вчинення кіберзлочинів активно використовуються технології блокчейн, що є новим для криміналістичної методики. Електронні гроші, криптовалюти та електронні платіжні системи (зокрема, таких, як «Яндекс. Деньги», «Qiwi-гаманець», Perfect Money та інші) все активніше використовуються для розрахунку між злочинцями, що значно ускладнює процес ідентифікації та процес розслідування.

Переважна більшість теоретичних та практичних аспектів розслідування кіберзлочинів залишаються нерозробленими та потребують постійного оновлення відповідно до сучасних тенденцій практики. Кіберзлочини не мають кордонів та комунікація між злочинцями є вільною та латентною. Саме сформована криміналістична характеристика кіберзлочинів стане інформатизованим провідником для слідчих під час розслідування злочинів цієї категорії.

Література:

1. Якимов И. Н. Практическое руководство к расследованию преступлений. – М., 1924.
2. Колесниченко А.Н. Научные и правовые основы расследования отдельных видов преступений. Автрореф. дис.... д-ра юрид. наук: 12.00.09. – Харьков: Юрид. институт, 1967. – 28 с.
3. У Львові викрито діяльність «ботоферм», які використовувалися для викрадення персональних даних працівників СБУ. URL: https://www.gp.gov.ua/ua/news?_m=publications&_c=view&_t=rec&id=293792
4. Ткачова О.В., Науменко К.В. Кримінологічна характеристика кіберзлочинця. Юридичний науковий журнал. 2018. №2. С. 200–204.
5. Романюк Б., Гавловський В., Гуцалюк М., Бутузов В. Виявлення та розслідування злочинів, що вчиняються у сфері інформаційних технологій: наук.-практ. посібник / за заг. ред. Я. Кондратьєва. К.: Вид. А.В. Паливода, 2004. – 144с.
6. Найдьон Я. Поняття та класифікація віртуальних слідів кіберзлочинів. Підприємництво, господарство і право. 2019. № 5. С. 304-307.
7. Волеводз А.Г. Противодействие компьютерным преступлениям: правовые основы международного сотрудничества. Москва: ООО «Издательство «Юрлитинформ», 2001. 496 с.

DOI https://doi.org/10.30525/978-9934-26-074-2-65

ЗАБЕЗПЕЧЕННЯ ПРАВ ПОТЕРПІЛОГО У КРИМІНАЛЬНОМУ ПРОВАДЖЕННІ: АКТУАЛЬНІ ПРОБЛЕМИ

Мазур М. Р.
кандидат юридичних наук,
доцент кафедри кримінального процесу та криміналістики
юридичного факультету
Львівського національного університету імені Івана Франка
м. Львів, Україна

У 2012 році в Україні було ухвалено новий Кримінальний процесуальний кодекс (КПК України) [1]. Незважаючи на схвальну оцінку даного законодавчого акту як вітчизняними науковцями і практиками, так і міжнародною спільнотою, досі низка його інститутів потребує