ІНФОРМАЦІЙНІ СЛІДИ В КОНТЕКСТІ МЕХАНІЗМУ ВЧИНЕННЯ ЗЛОЧИНІВ ІЗ ВИКОРИСТАННЯМ ОБСТАНОВКИ КІБЕРПРОСТОРУ

Олена Самойленко
к. ю. н., доцент, доцент кафедри криміналістики
Національного університету «Одеська юридична академія»

Діана Паляничко
к. ю. н., доцент кафедри криміналістики
Національного університету «Одеська юридична академія»

Олексій Баланюк
старший викладач кафедри криміналістики
Національного університету «Одеська юридична академія»

Ірина Ващенко
асистент кафедри криміналістики
Національного університету «Одеська юридична академія»

Анотація

Стаття присвячена значення інформаційних слідів злочинів в контексті механізму їх вчинення із використанням обстановки кіберпростору. Розглядаються питання щодо локалізації таких слідів та їх зв'язків з іншими елементами механізму злочину вказаної категорії.

***Ключові слова**: злочин; інформаційні сліди; кіберпростір; комп'ютер; місце злочину; нетрадиційні сліди.*

Кібернетичні технології стали сьогодні визначальним чинником у формуванні стилю життя, цінностей, інститутів та інших елементів сучасного суспільства. Результати використання нових технологій залежать від мети суб'єкта їх застосування. Тому, виникнувши як суто технічний спосіб передавання інформації, кіберпростір перетворився на важливе соціальне явище, яке вдало використовують й зі злочинною метою. Останнє зумовлює залишення пов'язаних із цим змін як в органічному, так і в неорганічному середовищі, якими в гносеологічному аспекті є сліди злочину.

Окремі аспекти механізму слідоутворення при вчиненні злочину в обстановці кіберпростору стають об'єктом дослідження з позицій методики розслідування суто комп'ютерних злочинів [1 – 3], або судової експертизи [4; 5]. Втім, поза уваги науковців залишається значення інформаційних слідів злочинів в контексті механізму їх

вчинення із використанням обстановки кіберпростору, що буде становити мету цієї статті.

Будь-яка злочинна діяльність відбувається за відповідними закономірностями, які обумовлюються об'єктивними і суб'єктивними чинниками, та відбиваються в слідах [6, с. 51]. Тому з одного боку природа слідів злочину зумовлена ознаками та якостями особи злочинця, які прямо впливають на регуляцію злочинної діяльності, з іншого – сам злочинець знаходиться під впливом об'єктивних умов оточуючого середовища, яке може впливати на злочинця вже підчас початку злочинної діяльності, що трасформує типові сліди злочину. Тому ми пристаємо до думки А.М. Кустова, який писав про особливості процесу слідоутворення, які вказують на певні властивості та якості особи злочинця, відображають дію інших осіб, предметів і процесів, що взаємодіють з ним [7, с. 112]. Встановлення таких зв'язків дозволить визначити процес детермінації механізмів традиційних злочинів, що матиме важливе значення для практики розслідування злочинів, вчинених із використання обстановки кіберпростору.

Технологічна складова кіберпростору зробила можливим утворення при вчиненні злочинів із використанням обстановки кіберпростору крім традиційних в криміналістичному сенсі слідів (слідів-відображень, слідів-предметів та сліди-речовини [8; 9]), також й «інформаційних» [1, с. 146], «віртуальних» [10] або «цифрових» слідів, так званих нетрадиційних слідів [11, с. 89].

Криміналісти в більшості випадків як сліди злочину розуміють матеріально фіксовані зміни в середовищі [12, с. 57]. Тобто, це ті сліди, які є об'єктом дослідження галузі криміналістичної техніки – трасології. Але в загальному криміналістичному аспекті зміст слідів охоплює всі матеріальні відображення вчинення злочину. Це більшою мірою відповідає завданням розкриття та розслідування злочину [13, с. 215]. Якщо розглядати поняття слідів у цьому аспекті, то вони є двох видів: ідеальні («відбитки» події у свідомості людині) та матеріальні («відбитки» події на предметах, зміни в обстановці події). Останні своєю чергою поділяють на: сліди-відображення (досліджувані трасологією), сліди-предмети (по суті, можуть бути носіями слідів-відображень – досліджуються трасологією або іншими видами речових доказів, різними видами судових експертиз) та сліди-речовини (що досліджуються різними видами судових експертиз). Ця класифікація сприяє створенню більш повної системи слідів будь-якого злочину, тому багато науковців ставили перед собою мету визначити до якої з груп традиційних слідів віднести інформаційні сліди.

М.В. Салтевський в цьому сенсі, виділяв два види слідів: механічні (які, по суті, є традиційними) та енергетичні, які є результатом фізичного впливу електричного сигналу. Вони динамічні та становлять

енергетичну зміну в конкретній точці магнітного носія [2, с. 12-14]. Далі автор поділяє енергетичні сліди на два види: магнітні та електричні. Магнітний слід – статичний, відносно сталий у часі, локалізований у енергетичному полі. Електричний слід можна приблизно уявити як змінений стан електричного потенціалу в конкретній точці фізичного тіла, тобто як наявність електричного струму, який рухається всередині носія. Енергетичний слід є крапковим накопиченням магнітного, електромагнітного та електричного заряду в результаті електричного впливу. Тому, на думку науковця, за природою енергетичний слід теоретично можна вважати слідом-предметом. Але це стосується не всіх носіїв електронної інформації – наприклад, такого не можна сказати про інформацію на CD-дисках, магнітооптичних носіях, інформацію в комп'ютерній мережі.

Як стверджує В.О. Голубєв, інформаційні сліди, що утворюються в результаті впливу (знищення, модифікації, копіювання, блокування) комп'ютерної інформації шляхом доступу до неї, є будь-яким зміненням комп'ютерної інформації, пов'язаним із фактом злочину [1, с. 146-147]. Тому за своєю природою такі сліди можуть бути слідами-відображеннями., але при цьому вони не є об'єктами трасології. Тож, більш широким терміном, що стосується змін на всіх носіях електронної інформації можна визнати «інформаційні сліди», але вони не повною мірою підпадають під традиційну криміналістичну класифікацію злочинів, тому стосовно них часто використовують термін «нетрадиційні сліди». Через це закономірним постає питання про локалізацію таких слідів.

Деякі криміналісти пишуть про кіберпростір в контексті місця вчинення злочину як місця, де не діють географічні та юридичні категорії [14, с. 23]. Вважаємо, що це не зовсім відповідає дійсності. Фактично інформаційні сліди як сліди-відображення у вигляді будь-яких змін інформації містяться в предметах матеріального світу – конкретних технічних або комбінованих засобах автоматизованої обробки інформації. Звертаючи увагу на віддаленість доступу до предмета посягання як особливість кіберпростору, завдяки якій він активно використовується при вчиненні злочину, аксіомою варто визнати той факт, що сліди злочину в електронному середовищі відбиваються одночасно в багатьох апаратних засобах комп'ютерної техніки, комп'ютерної мережі або телекомунікаційної мережі, мережі електрозв'язку. Останні ж фізично знаходяться на чітко визначеній географічній території під юрисдикцією певної держави та у власності конкретної особи.

В цьому контексті В.В. Крилов свого часу виділяв три групи слідів: сліди на машинних носіях, за допомогою яких діяв злочинець на своєму робочому місці; сліди на «транзитних» машинних носіях, за допомогою

яких злочинець здійснював зв'язок з інформаційними ресурсами, що піддалися нападу; сліди на машинних носіях інформаційної системи, до якої здійснено неправомірний доступ [15, с. 180].

А.А. Протасович, Л.П. Зверянська, виходячи з сучасних умов функціонування кіберпростору, виділили чотири місця вчинення кіберзлочину, відповідно місць знаходження слідів: 1) робоче місце, робоча станція – робоча станція – місце обробки інформації, що стала предметом посягання; 2) місце постійного зберігання або резервирування інформації – сервер або стример; 3) місце використання технічних засобів для неправомірного доступу до комп'ютерної інформації, яка знаходиться в іншому місці (може співпадати з робочим місцем, але знаходитись поза організації, наприклад, при сторонньому зламі шляхом віддаленого мережевого доступу); 4) місце підготовки злочину (розробки вірусу, програм зламу, підбору паролів) або місце безпосереднього використання інформації (копіювання, поширення, модифікації), що була отримана в результаті неправомірного доступу до даних, які зберігалися) [14].

Аналіз матеріалів кримінальних проваджень відкритих за ознаками злочинів у кіберпросторі свідчить про те, що ці місця знаходяться не тільки на території України. За результатами узагальнення відзначаємо, що на території України у 70 % злочинів, вчинених із використанням обстановки кіберпростору, знаходиться місце (комп'ютер, сервер або стример) обробки інформаційного продукту як предмета посягання; 70 % таких злочинів – місце використання технічних засобів для неправомірного доступу до комп'ютерної інформації; 10 % таких злочинів – місце підготовки злочину, якщо воно не співпадає з іншими позиціями місця злочину (розробки вірусу, програм зламу, підбору паролів).

Нагадаємо, що для суб'єкта кіберпростору як споживача телекомунікаційних послуг само обладнання виступає лише кінцевим елементом у мережі. Такі послуги надаються оператором або провайдером телекомунікацій, які в Україні для здійснення своєї діяльності повинні бути внесені до відповідного реєстру, який веде Національна комісія, що здійснює державне регулювання у сфері зв'язку та інформатизації (НКДРЗІ) [16]. Відповідно ч. 2 ст. 27 Закону України «Про телекомунікації» право власності на телекомунікаційну мережу та право на її технічне обслуговування і експлуатацію належить будь-якій фізичній особі-суб'єкту підприємницької діяльності або юридичній особі, які є резидентами України, незалежно від форм власності [17]. Національні оператори та провайдери, на відміну від закордонних, зобов'язані здійснювати діяльності у сфері телекомунікацій відповідно до законодавства України, в тому числі з метою сприяння проведенню оперативно-розшукових заходів,

досудового та судового розгляду. Цю обставину вдало використає злочинець, обираючи як знаряддя вчинення злочину інформаційні ресурси іншої держави.

Вважаємо, що якщо інформаційні сліди злочину свідчать про те, що доступ злочинця до інформаційного продукту/ресурсу, який є предметом або знаряддям злочинної діяльності, забезпечував закордонний оператор/провайдер, то можна висновувати про специфічні характеристики особи злочинця як-от професійна, географічна або соціальна мобільність, про його роль у складі організованої злочинної групи, кількість учасників такої групи. Локалізація інформаційних слідів злочину може свідчити також про спосіб вчинення злочину або технологію злочинної діяльності. Наприклад, на території України типово містяться зміни у файловій системі комп'ютера, який використовувався для вчинення злочину, на з'ємних його носіях, а також на сервері національного оператора або провайдера (спеціальні файли реєстрації, де протоколюється технічна інформація, яка містить відомості про технічний обмін) при вчиненні злочинцем простої вольової дії як-от розміщення в мережі Інтернет інформації певного змісту з насильницько-егоїстичних, антидержавно-політичних або дискримінаційних мотивів. Цього не можна сказати за умови діяльності злочинця шляхом складної вольової дії з корисливих мотивів, коли аналогічні інформаційні сліди злочину як правило виявляються лише на місці підготовки до злочину (розробки вірусу, програм зламу, підбору паролів), іноді на місці (комп'ютері сервері) обробки інформаційного продукту як предмета посягання.

Отже, інформаційні сліди злочину із використанням обстановки кіберпростору утворюють інформаційну основу, що використовується для пізнання механізму вчинення конкретного злочину у кіберпросторі. Вони мають кореляційні зв'язки з характеристикою особи злочинця, способом та технологією його вчинення. Їх встановлення сприятиме у практичній роботі слідчим та співробітникам кіберполіції в контексті встановлення комплексу злочинів, вчинених із використанням обстановки кіберпростору.

Література

1. Голубєв В.О. Інформаційна безпека: проблеми боротьби з кіберзлочинністю. Запоріжжя, 2003. 250 с.

2. Салтевський М.В. Основи методики розслідування злочинів, скоєних з використанням ЕОМ: Навч. посібник. Харків, 2000. 35 с.

3. Салтевський М.В., Губанов В.А. Использование следов сети интернет в раскрытии экономических пре ступлений. *Вісник Луганського інституту внутрішніх справ.* Спеціальний випуск. 1999. Частина 1. С. 67-74.

4. Мазниченко Ю.О., Шведова О.В. Методологічні аспекти автоматизованого дослідження матеріалів та засобів цифрового звукозапису. *Криміналістика і судова експертиза.* Мінюст України, Київський НДІ судових експертиз; редкол.: О. Г. Рувін (голов. ред.) та ін. К., 2015. Вип. 60. С. 299-308.

5. Хакановський В.Г. Можливості і перспективи використання інформаційних технологій в експертній практиці. *Криміналістика і судова експертиза*. Київський НДІ судових експертиз; редкол.: О. Г. Рувін (голов. ред.) та ін. К., 2017. Вип. 62. С. 330-343.

6. Лук'янчіков Є.Д. Інформаційне забезпечення розслідування злочинів : дис... докт. юрид. наук **:** 12.00.09. Київ, 2005. 429 с.

7. Кустов А.М. Криминалистика и механихм преступления. Цикв лекцій. Москва, 2002. 304 с.

8. Криминалистика: Учебник для вузов. Т.В. Аверьянова, Р.С. Белкин и др. Москва, 1999. 971 с.

9. Белкин Р.С. Курс криминалистики: В 3 т. М.осква, 1997. Т.2.: Частные криминалистические теории. 464 с.

10. Мещеряков В.А. Преступления в сфере компьютерной информации: основы теории и практики расследования : монография. Воронеж, 2002. 407с.

11. Самойленко О. А. Особливості розслідування викрадень майна, вчинених із використанням комп'ютерних технологій : монографія. Київ, 2009. 328 с.

12. Белкин Р.С. Курс криминалистики: В 3 т. М.: Юристъ, 1997. Т.2.: Частные криминалистические теории. 464 с.

13. Криминалистика: Учебник для вузов. Под ред. Р.С. Белкина, Г.Г. Зуйкова. Москва, 1969. Т.1. 376 с.

14. Протасевич А.А., Зверянская Л.П. Особенности осмотра места проишествия по делам о киберпреступлениях. *Известия Иркутской государственной экономической академии (Байкалский гос університет экономики и права)*. 2013. № 2. С. 23-26.

15. Крылов В.В. Расследование преступлений в сфере информации. Москва, 1998. 264 с.

16. Реєстр операторів, провайдерів телекомунікацій. URL: http://nkrzi.gov.ua/index.php?r=site/index&pg=55&language=uk

17. Про телекомунікації: Закон України від 18.11.2003 року за № 1280-IV. URL: http://zakon0.rada.gov.ua/laws/show/1280-15/page2?text=%F0%E5%E7%E8%E4%E5%ED%F2#w15