



УДК 343.9

О. В. Сіренко,
кандидат юридичних наук,
доцент, професор кафедри
кримінального процесу
та криміналістики
Університету державної
фіскальної служби України

ОСОБЛИВОСТІ РОЗСЛІДУВАННЯ КІБЕРЗЛОЧИНІВ

У статті розглянуто окремі проблемні питання розслідування кіберзлочинів. Досліджено диференціацію підходів до визначення поняття кіберзлочинів. Звернено увагу на криміналістичну характеристику цього виду кримінальних правопорушень.

Ключові слова: комп'ютерні злочини, кіберзлочини, кіберзлочинність, криміналістична характеристика.

В статье рассмотрены проблемные вопросы расследования киберпреступлений. Акцентируется внимание на многоаспектности проблемы расследования данных преступлений.

Ключевые слова: компьютерные преступления, киберпреступления, киберпреступность, криминалистическая характеристика.

The article deals with the problematic issues of the investigation of cybercrime. Attention is focused on the multidimensionality of the problem of investigating these crimes.

Keywords: computer crimes, cybercrime, cybercrime, juvenile forensic characteristics.

Злочинність, яка є невід'ємною частиною нашого суспільства, набуває віртуальних форм, і на сьогодні спостерігається значне розповсюдження комп'ютерних злочинів, що, в першу чергу, пов'язано зі стрімким розвитком новітніх інформаційних технологій.

До комп'ютерних злочинів насамперед належать злочини, передбаченні Кримінальним кодексом України (далі – КК України), який містить самостійний розділ «Злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку».

Як свідчать статистичні дані, в лютому 2017 року обліковано 283 кримінальних правопорушень у сфері використання електронно-обчислювальних машин (далі – ЕОМ) (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку. Із них: несанкціоноване втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку (ст. 361 КК України) становить 156 злочинів; створення з метою використання, розповсюдження або збуту шкідливих програмних чи технічних засобів, а також їхнє розповсюдження або збут (ст. 361-1 КК України) – 3 злочини; несанкціоновані збут або розповсюдження інформації з обмеженим доступом, яка зберігається в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах,

комп'ютерних мережах або на носіях такої інформації (ст. 361-2 КК України), – 2 злочини; несанкціоновані дії з інформацією, яка оброблюється в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або зберігається на носіях такої інформації, вчинені особою, яка має право доступу до неї (ст. 362 КК України), – 121 злочин; порушення правил експлуатації електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку або порядку чи правил захисту інформації, яка в них оброблюється (ст. 363 КК України), – 1 злочин.

Дослідження комп'ютерної злочинності не залишаються поза увагою вчених. Так, кримінально-правові аспекти зазначених злочинів були розглянуті в роботах Д. С. Азарова, М. В. Карчевського, Н. А. Розенфельда та ін. З криміналістичної точки зору комп'ютерні злочини, проблеми їх розслідування та протидії були розглянуті в роботах таких вітчизняних науковців: Н. М. Ахтирської, О. А. Баранова, П. Д. Біленчука, Т. В. Варфоломєєвої, М. С. Вертузаєва, В. Д. Гавловського, В. О. Голубєва, В. Г. Гончаренка, В. А. Губанова, М. В. Гуцалюка, А. В. Іщенко, Р. А. Калюжного, М. І. Камлика, Г. А. Матусовського, Б. В. Романюка, О. Р. Россинської, М. В. Салтевського, А. В. Селюка, В. М. Смаглюк, О. П. Снігерьова, Є. Ф. Тищенко, О. І. Усова, В. Г. Хахановського, В. С. Цимбалюка, О. М. Юрченка та ін.

Незважаючи на наявність окремих досліджень з проблем розслідування комп'ютерних злочинів, багато питань залишаються невирішеними, що і визначає актуальність статті.

Слід погодитися з думкою науковців, які вважають, що оскільки співвідношення термінів «комп'ютерні злочини», «кіберзлочини» використовуються для назви одних і тих самих суспільно-небезпечних діянь, то їх можна вважати синонімами та рівнозначними. Проте у зв'язку з ратифікацією Україною Конвенції про кіберзлочинність 7 вересня 2005 року вважається за доцільне вживати термін «кіберзлочини» [6].

У грудні 2011 р. в Україні створено Департамент з боротьби із кіберзлочинністю МВС України. Цей підрозділ покликаний володіти не лише знаннями законодавчих норм, які стосуються комп'ютерних злочинів (кіберзлочини), але й інформаційними технологіями, використовуючи останні розробки у сфері ІТ-індустрії. Загалом особливість комп'ютерних злочинів (кіберзлочинів) полягає у тому, що їхнє розслідування неможливе без знань комп'ютерних технологій.

Що ж таке кіберзлочини і які саме злочини належать до цього виду?

Кіберзлочини досить різноманітні, у зв'язку з чим існує безліч класифікацій зазначених злочинів. Як відмічають науковці, найбільш поширена класифікація кіберзлочинів ґрунтується на структурі Конвенції про кіберзлочинність [8].

Відповідно до згаданої Конвенції та Додаткового протоколу до неї існують такі види кіберзлочинів:

- 1) правопорушення проти конфіденційності, цілісності та доступності комп'ютерних даних і систем: незаконний доступ, нелегальне перехоплення, втручання у дані, втручання у систему, зловживання пристроями;
- 2) правопорушення, пов'язані з комп'ютерами: підробка, пов'язана з комп'ютерами, шахрайство, пов'язане з комп'ютерами;
- 3) правопорушення, пов'язані зі змістом – правопорушення, пов'язані з дитячою порнографією;
- 4) правопорушення, пов'язані з порушенням авторських та суміжних прав [8];
- 5) дії расистського та ксенофобного характеру, вчинені через комп'ютерні системи [7].

На думку Б. М. Дердюка, криміналістична класифікація комп'ютерних злочинів має такий вигляд:

- 1) знищення (руйнування) інформації;
- 2) неправомірне заволодіння інформацією чи порушення права її використання:
 - а) неправомірне заволодіння інформацією як сукупністю відомостей, документів – порушення права володіння;
 - б) неправомірне заволодіння інформацією як алгоритмом (методом перетворення);
 - в) неправомірне заволодіння інформацією як товаром;
- 3) дія або бездіяльність щодо створення (генерації) інформації із заданими властивостями:
 - а) поширення за телекомунікаційними каналами інформаційно-обчислювальних мереж інформації, що наносить збиток абонентам;
 - б) розробка і поширення комп'ютерних вірусів й інших шкідливих програм для ЕОМ;
- 4) неправомірна модифікація інформації:
 - а) неправомірна модифікація інформації як сукупності фактів, відомостей;
 - б) неправомірна модифікація інформації як алгоритму;
 - в) неправомірна модифікація інформації як товару з метою скористатися її корисними властивостями [5, с. 225–234].

Що ж стосується безпосередньо кіберзлочину, то на сьогодні чіткого визначення цього терміна не існує. Так, на думку В. Бутузова, комп'ютерні злочини та кіберзлочини є різними видами злочинів у сфері високих інформаційних технологій, класифікація яких відбувається за такими ознаками: 1) ознакою віднесення певних злочинів до комп'ютерних є знаряддя вчинення злочину – комп'ютерна техніка; 2) об'єктом посягання є суспільні відносини у сфері автоматизованої обробки інформації; 3) ознакою віднесення злочинів до кіберзлочинів є специфічне середовище вчинення злочинів – кіберпростір (середовище комп'ютерних систем та мереж) [2].

М. Погорецький вважає, що загальною ознакою протиправних діянь, передбачених Конвенцією та Додатковим протоколом до неї, є те, що їхнє вчинення на різних стадіях безпосередньо пов'язане з використанням ресурсів комп'ютерних систем (вчинення за допомогою комп'ютерних систем або через комп'ютерні системи), які, у свою чергу, є середовищем вчинення кіберзлочинів. Кіберзлочинами слід вважати ті, що вчиняються за допомогою або через комп'ютерні системи чи пов'язані саме з комп'ютерними системами, тобто із сукупністю пристроїв, із яких один чи більше, відповідно до певної програми, виконують автоматичну обробку даних [12, с. 89–96].

О. Копатін та Є. Скулишин надають такі підходи до поняття «кіберзлочин»:

1. Кіберзлочин – злочин, пов'язаний із використанням кібернетичних комп'ютерних систем, та злочин у кіберпросторі.

2. Кіберзлочин – найбільш небезпечне кіберправопорушення, за яке законодавством встановлюється кримінальна відповідальність [13].

На думку В. М. Болгова, кіберзлочини – це сукупність передбачених чинним законодавством кримінально караних суспільно небезпечних діянь (дій чи бездіяльності), що посягають на право захисту від несанкціонованого поширення і використання інформації, негативних наслідків впливу інформації чи функціонування інформаційних технологій, а також інші суспільно небезпечні діяння, пов'язані з порушенням права власності на інформацію та інформаційні технології, права власників або користувачів інформаційних технологій вчасно одержувати або поширювати достовірну й повну інформацію [1].

Таким чином, узагальнюючи вищезазначене, кіберзлочин – це кримінальне правопорушення, що вчиняється за допомогою або через комп'ютерні системи, посягає на право захисту від несанкціонованого поширення і використання інформації, негативних наслідків впливу інформації чи функціонування інформаційних технологій, а також інші суспільно небезпечні діяння, пов'язані з порушенням права власності на інформацію та інформаційні технології, права власників або користувачів інформаційних технологій вчасно одержувати або поширювати достовірну й повну інформацію і за яке передбачено кримінальну відповідальність.

Що стосується характерних рис кіберзлочинів, то в науковій літературі виділяють такі:

- 1) має міжнародний характер (виходить за рамки кордону однієї держави);
- 2) труднощі у визначенні «місцезнаходження злочину»;
- 3) слабкість зв'язку між ланками в системі доказів;
- 4) неможливість спостерігати і фіксувати докази візуально;
- 5) широке використання злочинцями засобів цифрової інформації [3, с. 1–4].

Під криміналістичною методикою розкриття і розслідування комп'ютерних злочинів розуміється сукупність наукових положень і рекомендацій, розроблених на їхній основі, тобто науково обґрунтованих і апробованих на практиці порад щодо розкриття та розслідування цих злочинів [4, с. 65].

Серед особливостей методики розкриття і розслідування комп'ютерних злочинів науковці вказують такі:

– ряд традиційних елементів окремих криміналістичних методик виявляються неінформативними чи малоінформативними стосовно категорії комп'ютерних злочинів і структури окремих її елементів; до їхнього числа можна віднести особливості використання допомоги громадськості у розкритті злочинів, особливості особистості потерпілого;

– особливу роль відіграє інформація про особливості використання спеціальних знань при розкритті і розслідуванні злочинів, що розглядаються, про особливості безпосереднього предмета злочинного посягання і можливостях захисту закритих інформаційних ресурсів криміналістичними методами, прийомами і засобами [11, с. 315].

При цьому виділяють такі елементи криміналістичної характеристики, як типові слідчі ситуації, спосіб вчинення злочину, типові матеріальні сліди злочину, характеристика особистості обвинуваченого й потерпілого, спосіб приховання злочину, обстановка злочину.

Узагальнюючи існуючі позиції, бачення щодо особливостей методики розкриття і розслідування комп'ютерних злочинів, елементів їхньої криміналістичної характеристики, В. О. Голубев зазначає, що під криміналістичною характеристикою незаконного втручання в роботу електронно-обчислювальних машин (комп'ютерів), систем і комп'ютерних мереж слід розуміти систему узагальнених даних про типові сліди, способи здійснення і механізми злочину, особистість злочинця та інші істотні риси, властивості та особливості злочину й обставин, які йому сприяють, що допомагає оптимізації розслідування і практичному застосуванню засобів, прийомів і методів криміналістики в розкритті та розслідуванні цього злочину. Її становлять такі основні дані про: способи здійснення злочину і механізм протиправного діяння; способи приховання незаконного втручання в роботу електронно-обчислювальних машин (комп'ютерів), системи і комп'ютерні мережі; знаряддя (засоби) вчинення протиправного діяння; обставини і місце вчинення злочину; сліди злочину; предмет

злочинного посягання; осіб, які вчинили незаконне втручання в роботу ЕОМ (комп'ютерів), систем і комп'ютерних мереж тощо [4, с. 69].

При розслідуванні кіберзлочинів дослідження комп'ютерної техніки, на думку науковців, доцільно проводити в умовах криміналістичної лабораторії, де цю роботу виконують фахівці з необхідною професійною підготовкою. Адже докази, пов'язані з комп'ютерними злочинами, які були вилучені з місця події, можуть бути легко змінені як у результаті помилок при їхньому вилученні, так і у процесі самого дослідження [10, с. 81–85].

Саме тому, на думку О. М. Миколенко, з якою погоджуємося, незважаючи на де-юре, відсутність законодавчої вимоги про обов'язкове призначення експертизи в цих провадженнях, де-факто, без призначення і проведення експертизи не можна говорити про ефективне розслідування таких справ [9, с. 155–157].

Що ж стосується проведення окремих слідчих та негласних слідчих (розшукових) дій під час досудового розслідування, то тут також існує певна специфіка. Оскільки зазначені дії пов'язані із використанням певних технічних засобів, то слідчі та оперативні працівники повинні володіти як навичками роботи з комп'ютерною технікою, так і знати та розуміти механізм вчинення кіберзлочину, а це означає необхідність здійснення комплексної підготовки фахівців відповідного рівня.

Враховуючи вищевикладене, можна зробити висновок про багатоаспектність проблеми розслідування кіберзлочинів, широкі можливості для їхнього дослідження та розроблення напрямів їхнього вирішення.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Болгов В. Організаційно-правове забезпечення протидії кримінальним правопорушенням, що вчиняються з використанням інформаційних технологій : наук.-практ. посіб. / В. М. Болгов, Н. М. Гадіон, О. З. Гладун та ін. – К. : Національна академія прокуратури України, 2015. – 202 с.
2. Бутузов В. Протидія комп'ютерній злочинності в Україні (системно-структурний аналіз) : монографія / В. Бутузов. – К. : КИТ, 2010. – 148 с.
3. Голубев В. Комп'ютерна злочинність / В. Голубев // Юридичний вісник України. – 2012. – № 6(9). – С. 1–4.
4. Голубев В. О. Розслідування комп'ютерних злочинів : монографія / В. О. Голубев. – Запоріжжя : Гуманітарний університет «ЗІДМУ», 2003. – 296 с.
5. Дердюк Б. Поняття та теоретичні основи криміналістичної класифікації комп'ютерних злочинів / Б. Дердюк // Прикарпатський юридичний вісник. – 2014. – № 3(6). – С. 225–234.
6. Довбиш М. Кіберзлочинність в Україні / М. Довбиш [Електронний ресурс]. – Режим доступу : <https://www.science-community.org/ru/node/16132>
7. Додатковий протокол до Конвенції про кіберзлочинність, який стосується криміналізації дій расистського та ксенофобного характеру, вчинених через комп'ютерні системи [Електронний ресурс]. – Режим доступу : http://zakon2.rada.gov.ua/laws/show/994_687
8. Конвенція про кіберзлочинність [Електронний ресурс]. – Режим доступу : http://zakon2.rada.gov.ua/laws/show/994_575
9. Миколенко О. М. Деякі особливості розслідування злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку / О. М. Миколенко // Кібербезпека в Україні: правові та організаційні питання :

матеріали Всеукр. наук.-практ. конф., м. Одеса, 21 жовтня 2016 р. – Одеса : ОДУВС, 2016. – 233 с.

10. Моїсєєв О. М. Залучення спеціаліста до розслідування комп'ютерних злочинів / О. М. Моїсєєв // Правові основи захисту комп'ютерної інформації від протиправних посягань : матеріали міжвузівської науково-практичної конференції, м. Донецьк, 22 грудня 2000 р. – Донецький інститут внутрішніх справ, 2001. – С. 81–85.

11. Мухин Г. Н. Структура и содержание методики расследования преступлений, связанных с посягательством на информационные ресурсы / Г. Н. Мухин // Управление защитой информации. – 1999. – Т. 3, № 3. – С. 315.

12. Погорецький М. Кіберзлочини: до визначення поняття / М. Погорецький, В. Шеломенцев // Вісник прокуратури. – 2012. – № 8. – С. 89–96.

13. Словник термінів з кібербезпеки / за заг. ред. О. Копатіна, Є. Скулишина. – К. : Аванпост - Прим, 2012. – 214 с.