УДК 343.13
DOI

А. П. Бегма, О. С. Ховпун

РОЗСЛІДУВАННЯ ЗЛОЧИНІВ В ІТ-СФЕРІ

У сучасному світі подібно до лавини зростає процес цифротизації, комп'ютерні технологій проникли практично в усі сфери людської діяльності – економічну, соціальну, управлінську, культурну та інші, що суттєво впливає на життя соціуму і на видозміну злочинної діяльності загалом. Поряд із виникненням нових видів злочинів у сфері інформаційних технологій (далі – ІТ) практично будь-які злочини, такі як привласнення, крадіжки, шахрайства, злочини у банківській сфері, комп'ютерне шпигунство; комп'ютерні диверсії (у тому числі руйнування операційних систем, створення та використання комп'ютерних вірусів); комп'ютерний тероризм; крадіжку комп'ютерних послуг (зокрема, обчислювальних ресурсів); махінації та маніпулювання системою обробки даних, а також крадіжка фінансових засобів і підробка документів; порушення приватної або державної таємниці; протиправне копіювання програмних продуктів, яке порушує авторське та інші права, тощо [1, с. 59, 60], вчиняються нині за допомогою комп'ютерних засобів та інформаційних систем. Розвиток цифрових технологій постійно породжує нові види злочинів і способи їх вчинення і приховування. У зв'язку з масовим поширенням засобів мобільної комунікації виникли нові види злочинів, такі як створення і поширення шкідливих програм (додатків) для мобільних телефонів, використання мобільних засобів зв'язку для вчинення шахрайства, вимагання, підпалів, вибухів, терористичних актів тощо.

У контексті порушеної проблематики важливо відзначити, що розвиток інформаційних технологій призвів не тільки до появи злочинів нових видів, а й до різкого збільшення наукових досліджень відповідної тематики. Поступово стало зрозуміло, що практично всі вони мають міждисциплінарний характер і використовують досягнення багатьох наук. Темі розслідування та протидії злочинів в ІТ-сфері присвячено низку наукових праць, ці питання були розглянуті у роботах таких науковців: Н.М. Ахтирської, О.А. Баранова, П.Д. Біленчука, Т.В. Варфоломеєвої, В.Д. Гавловського, В.О. Голубєва, В.А. Губанова, Р.А. Калюжного, М.І. Камлика, Б.В. Романюка, М.В. Салтевського, В.М. Смаглюк, О.П. Снігерьова, Є.Ф. Тищенка, В.С. Цимбалюка, О.М. Юрченка та ін. Незважаючи на наявність окремих досліджень із проблем розслідування злочинів в ІТ-сфері, багато питань залишаються невирішеними.

У сучасних умовах практично всі види злочинів можуть бути вчинені за допомогою персонального комп'ютера, за винятком деяких протиправних дій проти життя і здоров'я громадян [2]. Під час вчинення злочинів в ІТ-сфері нерідко здійснюються прямі атаки на комп'ютери або інші пристрої з метою виведення їх із ладу. Іноді атаковані комп'ютери використовуються для поширення шкідливих програм, незаконної інформації, різного роду зображень (наприклад, дитячої порнографії) та інших матеріалів.

В останні роки великого поширення набули такі види злочинів в ІТ-сфері, як: корисливі кіберзлочини (в тому числі фішинг, кібервимагання, фінансове шахрайство тощо), викрадення персональних даних, кібершпіонаж, кібербулінг, порушення авторських прав та інші. Розглядаючи їх, потрібно враховувати, що у сучасних умовах до легального економічного обігу активно залучаються нетрадиційні види майна (у тому числі інтернет-сайти, електронні гроші, технології мобільного зв'язку, інтернет-майно тощо) [3]. Оскільки такі види майна мають здатність приносити високі доходи, на них відповідним чином реагує кримінальне середовище. У результаті з'являються все нові види злочинних посягань, які передбачають використання сучасних інформаційних технологій на умовах раптовості й анонімності [4, с. 15]. Практично всі названі протиправні діяння значно небезпечніші від інших злочинів, скоєних поза кіберпростором, оскільки мають здатність завдавати шкоди всім охоронюваним законом інтересам. Їх діапазон варіюється від приватних немайнових інтересів окремих громадян до інтересів безпеки держави.

Із настанням нової цифрової ери інформаційні технології перетворилися на невід'ємну частину життя суспільства, охопивши практично всі її сфери. Для того щоб об'єктивно оцінити їх безсумнівну користь, потрібно чітко уявляти масштаби шкоди, якої вони здатні заподіяти людству.

Неухильне зростання їх числа і стрімке поширення нових інформаційних технологій не дають можливості повно, об'єктивно, вчасно осмислювати кримінальні нововведення в кіберпросторі та пов'язані з ними ризики. Це не тільки нові віруси, уразливості й закладки, а й реальна загроза несанкціонованого доступу, відсутність приватності, витік персональних даних користувачів мережі, тотальний контроль національного ринку іноземними виробниками тощо. Оцінюючи реальні та потенційні ризики, потрібно розуміти, що всі сучасні девайси – інтернет-сервіси, теле- і радіопристрої, транспорт, зв'язок, промислові комплекси – міцно пов'язані з інтернетом і оновлюються ззовні. Це означає, що і управляються вони таким же шляхом.

Спостерігається стійкий причинно-наслідковий зв'язок між кількісною різноманітністю сучасних інформаційних технологій та якісними змінами у структурі злочинності. Масштабне поширення і досить швидкий розвиток технологій такого роду формує практично безмежні можливості для підготовки, вчинення і приховування злочинів абсолютно новими способами і засобами. Не меншою мірою вони дозволяють розробляти і вдосконалювати методичні основи виявлення, розкриття і розслідування злочинів в ІТ-сфері, скоєних за допомогою різноманітних комп'ютерних та мережевих технологій. Однак із різних причин це відбувається дуже повільно. Значно

швидше прийшло усвідомлення того, що злочинність все більше і більше йде до цифрової сфери. Відповідно, правоохоронним органам держави необхідні нові наукові методи боротьби з нею в кіберпросторі та своєчасного запобігання очікуваних її проявів. Саме це завдання зараз гостро стоїть перед криміналістикою як самостійною галуззю наукового знання.

Слід зазначити, що зараз технології такого роду займають в економіці країни особливе місце, а їх ефективне функціонування є одним із найважливіших факторів, які сприяють вирішенню ключових завдань державної політики. У нашій країні вони є найбільш залежними від використання імпортного програмного забезпечення (до 90% операційних систем і систем управління базами даних). З урахуванням цього факту технологічна незалежність України у сфері інформаційних технологій проголошена основою не тільки інформаційної безпеки, але і безпеки держави загалом, у тому числі від злочинних посягань [5, с. 65].

Крім іншого, інформаційні технології повинні відігравати важливу роль у забезпеченні подальшого поступального розвитку вітчизняної криміналістики. Зараз стало очевидно, що в ній назріла низка питань, які очікують комплексного вирішення. Зокрема, необхідно якомога швидше реалізувати заходи, спрямовані на розроблення та впровадження нових способів виявлення, розкриття і розслідування злочинів, скоєних в IT-сфері.

Поширення комп'ютерних вірусів, шахрайства з платіжними картами, розкрадання грошових коштів із банківських рахунків і різного роду комп'ютерної інформації, порушення правил експлуатації автоматизованих електронних систем – ось далеко не повний перелік злочинів, що вчиняються за допомогою інформаційних технологій. Це явище у наукових публікаціях прийнято називати по-різному: кіберзлочинністю, комп'ютерними злочинами, злочинами у сфері комп'ютерних технологій, злочинами в IT-сфері, злочинами у сфері комп'ютерної інформації тощо. У юридичній літературі, виданій за останнє десятиліття, найбільш часто зустрічаються три терміни: «кіберзлочини», «комп'ютерні злочини», «злочини в IT-сфері». Їх можна вважати рівнозначними, оскільки вони використовуються для позначення групи одних і тих самих суспільно-небезпечних діянь. У криміналістичному аспекті кіберзлочини (або злочини в IT-сфері) – це суспільно небезпечні діяння, для підготовки, вчинення, приховування, а відповідно, виявлення, розкриття і розслідування яких застосовуються різного роду комп'ютерні технології і (або) використовується інформаційно-телекомунікаційна мережа Інтернет.

Існуюча система протидії злочинним посяганням, вчиненим з використанням сучасних інформаційних технологій, поки помітно відстає у своєму розвитку. Такі складнощі зумовлені специфікою вчинення злочинів в IT-сфері, яка, на наш погляд, полягає у такому: у доступності (тобто поширеності і відносній дешевизні) комп'ютерної техніки для найширших верств населення; у дуже великій та фактично транскордонній географії скоєння злочинів; у однозначній досяжності об'єкта злочинного посягання (тобто фактична відстань до нього не має ніякого значення); у комфортності умов, що є супутніми підготовці і скоєнню злочинів (тобто їх підготовка

і скоєння реально можуть здійснюватися практично з будь-якого персонального комп'ютера, що має вихід до Всесвітньої павутини).

В Україні, на жаль, відсутня офіційна державна статистика, яка б містила відомості про кіберзлочини, що негативно позначається на запобіжних заходах, які здебільшого мають фрагментарний характер, зумовлюючи складнощі у протидії та боротьбі з таким видом суспільно небезпечних діянь.

Причини таких дивних кількісних розбіжностей різні, але нам вони вбачаються у тому, що абсолютна більшість злочинів у сфері комп'ютерної інформації – латентні. Фахівці правильно стверджують, що до 90% кримінальних актів цього різновиду не знаходять відображення в офіційній кримінальній статистиці [6, с. 135]. Найбільш поширеною причиною такого стану справ, на нашу думку, є небажання практично всіх комерційних структур (у тому числі банків) оприлюднювати відомості про викрадення у них комп'ютерної інформації та грошових коштів шляхом віртуальних зломів систем їх захисту. Пояснення цьому просте – всі вони вважають за краще дорожити репутацією і бояться втратити клієнтів, а доведення фактів вчинення таких злочинів – досить складна і витратна справа.

Сам процес виявлення, розкриття і розслідування злочинів, скоєних із використанням сучасних інформаційних технологій, також має низку істотних особливостей. Помилки, допущені при цьому слідчими і дізнавачами, здебільшого є наслідком їх незадовільної професійної підготовки саме для цього сегменту криміналістичної діяльності. Однією з найбільш істотних причин низької якості досудового розслідування злочинів, скоєних в ІТ-сфері, у наукових публікаціях справедливо визнається відсутність якісних методичних розробок, у реалізації яких були би повною мірою задіяні сучасні інформаційні технології. За таких умов об'єктивні складнощі виявлення, фіксації та вилучення криміналістично-значущої інформації з метою її подальшого використання як доказів у кримінальній справі нерідко стають нездоланними. Більше того, тут як ніде висока ймовірність того, що ті докази, що все ж таки були виявлені, можуть бути ненавмисно змінені і навіть втрачені як у результаті допущених помилок під час їх фіксації або, наприклад, вилученні, так і в процесі їх дослідження. Підготовка у процесі досудового розслідування у кримінальній справі доказів такого роду для подальшого подання їх до суду вимагає не тільки обов'язкової наявності рунтовної фахової підготовки, а й регулярного оновлення наявних знань у слідчих, дізнавачів, оперативних працівників і, зрозуміло, у фахівців і експертів тощо.

У науках кримінального права та кримінології спостерігається приблизно така ж картина. Висновок невтішний: відсутність системного та інституційного характеру в дослідницькій роботі на цьому напрямі відчутно ускладнює боротьбу зі злочинами в сфері ІТ, що насамперед пов'язано із постійним удосконаленням комп'ютерних та мережевих технологій. Сама ж інформація виступає об'єктом злочинної діяльності у цій сфері. Її розкрадання, зміна, неправомірне використання так чи інакше вносять дисонанс у функціонування економічних систем. Більш того, на відміну від організованої злочинності, корупції, багатьох проявів тероризму та

екстремізму діяльність кіберзлочинців не узгоджується з відомими і звичними в суспільстві моделями поведінки. По суті, це означає, що вона індивідуальна, ірраціональна, анонімна й інтернаціональна, а кожна людина у сучасному світі, від пересічного громадянина до великої компанії, банку і держави, ризикує у будь-який момент стати жертвою зловмисників у кіберпросторі, які постійно винаходять нові, складні та різноманітні схеми шахрайських операцій.

Що ж до характерних рис злочинів в ІТ-сфері, то у 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 цифрованої інформації [7, с. 1–4].

Під криміналістичною методикою розкриття і розслідування злочинів в ІТ-сфері розуміється сукупність наукових положень і рекомендацій, розроблених на їхній основі, тобто науково обгрунтованих і апробованих на практиці порад щодо розкриття та розслідування цих злочинів [8, с. 65].

Серед особливостей методики розкриття і розслідування злочинів в ІТ-сфері науковці виокремлюють, зокрема, те, що:

– низка 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 під час розкриття і розслідування злочинів, що розглядаються, про особливості безпосереднього предмета злочинного посягання і можливості захисту закритих інформаційних ресурсів криміналістичними методами, прийомами і засобами [9, 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 кіберзлочинів, елементів їхньої криміналістичної характеристики, В.О. Голубєв 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 [9, с. 69].

На думку О.М. Миколенко, саме тому, 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 [6, 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 з використанням певних технічних засобів, то слідчі та оперативні працівники повинні володіти навичками роботи з комп'ютерною технікою, знати та розуміти механізм вчинення злочину в ІТ-сфері, а це означає необхідність здійснення комплексної підготовки фахівців відповідного рівня.

Висновки. Таким чином, більшість змін, що виникли із причини розвитку інформаційних технологій, принесли користь суспільству насамперед у медицині, інженерії, управлінні ресурсами (у тому числі фінансовими). Однак вони ж і визначили появу нових можливостей для заподіяння шкоди інтересам суспільства і держави, оскільки з появою технологічних новацій виникли нові види злочинів, що грунтуються на них, такі, наприклад, як злочини проти конфіденційності, цілісності та доступності комп'ютерних даних і систем, шахрайство та підробка, що пов'язані з використанням комп'ютерів, злочини, пов'язані з розміщенням у мережах протиправної інформації, злочини щодо авторських і суміжних прав, вимагання за допомогою мережі інтернет, кібертероризм та багато інших. Головною особливістю, що визначає те чи інше протиправне діяння як злочини в ІТ-сфері, на нашу думку, найправильніше вважати його вчинення за допомогою комп'ютерних і мережевих технологій.

Враховуючи вищевикладене, можна зробити висновок про багатоаспектність проблеми розслідування злочинів в ІТ-сфері, широкі можливості для їхнього дослідження та розроблення напрямів їхнього вирішення.

Боротьба зі злочинами в ІТ-сфері є проблемою міжнародного масштабу, оскільки заходи щодо запобігання, виявлення, розкриття і розслідування злочинів, скоєних з використанням сучасних інформаційних технологій, не можуть бути результативними лише на національному рівні в силу транснаціонального та транскордонного характеру самої мережі інтернет. Більш того, не припиняється збільшення чисельності її користувачів, що закономірно породжує їх залежність від інформаційного співтовариства і вразливість від різного роду кіберпосягань.

Література

1. Ботвінкін О.В. Проблеми забезпечення національної безпеки в інформаційній сфері // Юридичний журнал. 2007. № 2. С. 59–60.

2. Гавловський В.Д. Аналіз стану кіберзлочинності в Україні // Інформація і право. 2019. № 1(28). С. 108–117.

3. Карчевский Н.В. «Киберпреступление» или преступление в сфере использования информационных технологий? // Кібербезпека в Україні:

правові та організаційні питання : матеріали Всеукр. наук.-практ. конф. (м. Одеса, 21 жовтня 2016 р.). Одеса : ОДУВС, 2016. С. 10–14.

4. 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.

5. Ткачук Т.Ю. Правове забезпечення інформаційної безпеки в умовах євроінтеграції України. Кваліфікаційна наукова праця на правах рукопису. Дисертація на здобуття наукового ступеня доктора юридичних наук за спеціальністю 12.00.07 – адміністративне право і процес; фінансове право; інформаційне право (081 – Право). ДВНЗ «Ужгородський національний університет», Ужгород, 2019. С. 65.

6. Миколенко О.М. Деякі особливості розслідування злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку // Кібербезпека в Україні: правові та організаційні питання : матеріали Всеукр. наук.-практ. конф., м. Одеса, 21 жовтня 2016 р. Одеса : ОДУВС, 2016. 233 с.

7. Голубєв В. Комп'ютерна злочинність // Юридичний вісник України. 2012. № 6(9). С. 1–4.

8. Голубєв В.О. Розслідування комп'ютерних злочинів : монографія / В. О. Голубєв. Запоріжжя : Гуманітарний університет «ЗІДМУ», 2003. 296 с.

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

10. Моїсеєв О.М. Залучення спеціаліста до розслідування комп'ютерних злочинів // 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.

Анотація

Бегма А. П., Ховпун О. С. **Розслідування злочинів в ІТ-сфері.** – Стаття.

Комп'ютерні технологій проникли у сфери людської діяльності – економічну, соціальну, управлінську, культурну та інші. Діяльність впливає на життя соціуму та на злочинну діяльність. До злочинів у сфері інформаційних технологій слід віднести: привласнення, крадіжку, шахрайство, комп'ютерне шпигунство, крадіжка комп'ютерних послуг, злочини у банківській сфері, підробку документів, маніпулювання системою обробкою даних, протиправне копіювання програмних продуктів.

Нова цифрова ера інформаційних технологій перетворила на невід'ємну частину життя суспільства, охопивши практично всі її сфери. Для того щоб об'єктивно оцінити їх безсумнівну користь, потрібно чітко уявляти масштаби шкоди, якої вони здатні заподіяти людству.

Розвиток цифрових технологій постійно породжує нові види злочинів і способи їх вчинення та приховування. Злочини в ІТ-сфері набули поширення, а їх зміст охоплює весь спектр суспільно-небезпечних діянь у сфері використання інформаційних технологій. Практично всі види злочинів можуть бути вчинені за допомогою персонального комп'ютера, за винятком деяких протиправних дій проти життя і здоров'я громадян.

Під час вчинення злочинів в ІТ-сфері здійснюються прямі атаки на комп'ютери або інші пристрої з метою виведення їх з ладу. Іноді атаковані комп'ютери використовуються для поширення шкідливих програм, незаконної інформації, зображень.

У сучасних умовах до легального економічного обігу активно залучаються нетрадиційні види майна (інтернет-сайти, електронні гроші, технології мобільного зв'язку, інтернет-майно). Види майна мають здатність приносити високі доходи, на них відповідним чином реагує кримінальне середовище.

Масштабне поширення формує безмежні можливості для підготовки, вчинення і приховування злочинів абсолютно новими способами і засобами. Вони дозволяють розробляти і вдосконалювати методичні основи виявлення, розкриття і розслідування злочинів в ІТ-сфері, скоєних за допомогою різноманітних комп'ютерних та мережевих технологій, але це відбувається повільно.

Особливості методики розкриття і розслідування злочинів полягає у використанні допомоги громадськості у розкритті злочинів, особливості особистості потерпілого; використання спеціальних знань під час розкриття і розслідування злочинів.

Боротьба зі злочинами в ІТ-сфері є проблемою міжнародного масштабу, заходи щодо запобігання, виявлення, розкриття і розслідування злочинів, скоєних з використанням сучасних інформаційних технологій, не можуть бути результативними через масштабність мережі Інтернет. Збільшення чисельності користувачів не припиняється, що породжує залежність від інформаційного співтовариства і вразливість від посягань.

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

S u m m a r y

Begma A. P., Khovpun O. S. **Crime investigation into the IT sphere.** – Article.

Computer technology has penetrated into the spheres of human activity – economic, social, managerial, cultural and others. Activities affect the life of society and criminal activity. Crimes in the field of information technology include: embezzlement, theft, fraud, computer espionage, theft of computer services, crimes in the banking sector, forgery of documents, manipulation of the data processing system, illegal copying of software products.

The new digital age of information technology has become an integral part of society, covering almost all areas. In order to objectively assess their undoubted benefits, it is necessary to have a clear idea of the extent of the damage they can cause to humanity.

The development of digital technologies is constantly generating new types of crimes and ways to commit and conceal them. Crimes in the IT sphere have become widespread, and their content covers the full range of socially dangerous acts in the use of information technology. Virtually all types of crimes can be committed with the help of a personal computer, with the exception of some illegal actions against the life and health of citizens.

When IT crimes are committed, direct attacks are carried out on computers or other devices in order to disable them. Sometimes attacked computers are used to spread malware, illegal information, images.

In modern conditions, non-traditional types of property (Internet sites, electronic money, mobile communication technologies, Internet property) are actively involved in legal economic circulation. Types of property have the ability to generate high incomes, and the criminal environment responds accordingly.

Large-scale spread creates endless opportunities for the preparation, commission and concealment of crimes in completely new ways and means. They allow the development and improvement of methodological frameworks for the detection, detection and investigation of crimes in the field of IT, committed using a variety of computer and network technologies, but this is slow.

Features of the methodology of detection and investigation of crimes is the use of public assistance in the detection of crimes, the personality of the victim; use of special knowledge in the detection and investigation of crimes.

The fight against IT crimes is an international problem, and measures to prevent, detect, detect and investigate crimes committed with the use of modern information technology cannot be effective due to the scale of the Internet. The increase in the number of users does not stop, which creates dependence on the information community and vulnerability to encroachments.

Key words: computer crimes, cybercrime, cybercrime, juvenile forensic characteristics.