УДК 621.391

Є. РАЩЕНКО, *ад’юнкт* кафедри інформаційних технологій
Київського національного університету внутрішніх справ

КОМП’ЮТЕРНІ ДАНІ ЯК НОСІЙ КРИМІНАЛІСТИЧНОЇ ІНФОРМАЦІЇ ПРО ЗЛОЧИНИ У СФЕРІ КОМП’ЮТЕРНИХ ТЕХНОЛОГІЙ

Анотація. *У статті розкривається сутність комп’ютерних даних з погляду кібернетики та криміналістики, а також їх роль в кримінально-процесуальному провадженні як носіїв доказової інформації про злочини у сфері комп’ютерних технологій.*

У сучасних умовах науково-технічного прогресу чітко вимальовується тенденція до комп’ютеризації, створення розгалужених систем обробки даних, що включають в себе як потужні обчислювальні комплекси, так і персональні комп’ютери. Щодня збільшується кількість комунікаційних локальних, галузевих, загальнодержавних та міждержавних мереж. Комп’ютерні технології впроваджуються практично у всі сфери громадського життя, включно з медициною, зв’язком, транспортом, національною безпекою та багатьма іншими. Ці процеси, безперечно, сприяють розвитку економіки, ведуть до появи “безпаперових” технологій. Зараз наврядчи хтось може уявити діяльність підприємства, організації чи установи без використання комп’ютера.

Разом с тим, удосконалення комп’ютерних технологій призвело до появи нових видів злочинів, так званих “комп’ютерних злочинів”. За своїм механізмом, способами вчинення та укриття ці злочини мають певну специфіку, характеризуються підвищеним рівнем латентності та низьким рівнем розкриття [1].

Питання протидії та розслідування злочинів, вчинених у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж у цілому, розглядалися в роботах П.Д. Біленчука, А.Г. Волеводза, Ю.В. Гавриліна, В.О. Голубєва, Б.В. Романюка, В.В. Козлова, В.П. Паламарчук, В.С. Цимбалюка та ін. Однак, не зважаючи на беззаперечну теоретичну і практичну значимість названих досліджень, питання визначення сутності й ролі комп’ютерних даних як носіїв криміналістичної інформації детально в них не розглядалися.

Відносна новизна для нашої країни вказаних злочинних проявів, повномасштабне та прискорене впровадження інформаційних технологій у життєдіяльність українського суспільства, зростання комп’ютерної грамотності населення та деякі інші фактори виявили неготовність правоохоронних органів до адекватної протидії цим новим деліктним явищам.

Як виявлення, так і розслідування цієї категорії злочинів залишається доволі складним завданням для більшості працівників правоохоронних органів, і пояснюється це, головним чином, їх недостатньою підготовленістю до роботи з новим видом доказової інформації, що міститься на машинних носіях цифрової інформації: жорстких магнітних дисках (вінчестерах), дискетах, CD та DVD, флеш-картах тощо.

Не випадково, що з переходом на новітні інформаційні технології знизилися рівень та якість криміналістичного, судово-експертного забезпечення багатьох інших категорій злочинів, пов’язаних з використанням комп’ютерної техніки, особливо у сфері економіки, бізнесу та підприємництва. З огляду на відсутність методичних рекомендацій з виявлення, фіксації,

вилучення “цифрової” інформації та недостатню розробку експертних методик дослідження даних на машинних носіях використання їх у суді залишається малоефективним [2].

Законодавцем поняття інформації формулюється таким чином: *інформація – це документовані або публічно оголошені відомості про події та явища, що відбуваються у суспільстві, державі та навколишньому природному середовищі* [3]. Відносно інформації, яка обробляється в електронно-обчислюваних машинах, таке визначення не в повному обсязі відповідає дійсності та звужує зміст такої інформації. Специфіка комп’ютерної інформації полягає в тому, що вона може слугувати засобом керування електронно-обчислюваною машиною або окремими її частинами, знаходячись у вигляді комп’ютерних програм та файлів, не містячи при цьому відомостей ані про події, ані про явища. Ніби врахувавши вказані розбіжності, законодавець згодом у статті 2 Закону Україні “Про захист інформації в автоматизованих системах” від 5 липня 1994 р. закріпив таке поняття, як інформація в автоматизованій системі – сукупність усіх даних і програм, які використовуються в автоматизованій системі незалежно від засобу їх фізичного та логічного представлення [4]. Відповідно до цього визначення дані – це інформація у формі, придатній для автоматизованої обробки її засобами обчислюваної техніки, а програми – послідовність інструкцій, команд для здійснення певного процесу, яка надається в такій формі, що вона може бути виконана електронно-обчислюваною машиною (комп’ютером) або може бути перетворена в таку форму. Виходячи з наведених дефініцій можна стверджувати, що комп’ютерні дані, поряд з комп’ютерними програмами, є складовою частиною комп’ютерної інформації і співвідносяться між собою як частина та ціле. Але існує дещо інший погляд на сутність комп’ютерних даних, який був зазначений у міжнародному документі – Конвенції про кіберзлочинність. Відповідно до вказаної конвенції комп’ютерні дані – це будь-яке представлення фактів, інформації або концепцій у формі, яка є придатною для обробки у комп’ютерній системі, включаючи програму, яка є придатною для того, щоб забезпечити виконання певної функції комп’ютерною системою. Таким чином, міжнародно-правові норми суперечать вітчизняним, стверджуючи той факт, що комп’ютерні дані є більш широким поняттям, яке включає в себе як інформацію, так і комп’ютерні програми.

На нашу думку, виходячи з наведених дефініцій такі поняття, як комп’ютерна інформація та комп’ютерні дані можуть використовуватися в науковій літературі як взаємозамінні і як такі, що відбивають сутність одного і того ж об’єкта.

Переходячи до ролі комп’ютерних даних як носіїв криміналістичної інформації, слід з насамперед з’ясувати сутність самої криміналістичної інформації.

Термін “криміналістична інформація” визначається більшістю науковців як будь-які відомості, отримані процесуальним та непроцесуальним шляхами під час розслідування злочину слідчим або працівником органу дізнання відповідно до рекомендацій, розроблених криміналістикою [5, 6]. Тобто можна стверджувати, що криміналістичною інформацією є вся інформація, яку використовують для розслідування. Інші науковці, такі як Г.А. Матусовський, А.А. Дудніков, Р.С. Бєлкін, не радять використовувати цей термін, оскільки, на їх думку, коли говорять про криміналістичну інформацію, здебільшого йдеться про “криміналістичнозначимі явища”, “криміналістичні ознаки” або “криміналістичнозначущу інформацію”. На наш погляд використання терміна “криміналістична інформація” цілком доцільно в тому значенні, яке було зазначено вище. Але не слід ототожнювати такі поняття, як криміналістична та доказова інформація. Як

відомо, в ході розслідування кримінальної справи інформація, що має відношення до вчинення злочину, може бути отримана оперативним шляхом і тому не завжди може використовуватися як доказ. Такий вид криміналістичної інформації прийнято називати орієнтуючою.

Зміст криміналістичної інформації становлять різноманітні дані, які використовуються для розслідування злочинних діянь, встановлення особи злочинця, причин та умов вчинення злочину, попередження протиправної поведінки. У разі правильного процесуального їх закріплення – утворюють доказову базу. Розглядаючи такий вид злочинів, як злочини у сфері комп’ютерних технологій, необхідно зазначити, що дані та відомості, які становлять зміст криміналістичної інформації по цих злочинах, мають певні особливості [7]. Пов’язане це в першу чергу з предметом, на який вони посягають, – комп’ютерною інформацією або комп’ютерними даними. Своєрідність комп’ютерної інформації, а також її носіїв та засобів обробки зумовлює особливості слідової картини, яка умовно поділяється на два види. До першого належать матеріальні сліди, що залишаються у електронно-обчислювальній машині, сліди відображення, документація, сліди-речовини). Такі сліди можуть залишатися на комп’ютерній техніці, носіях інформації та іншому обладнанні. Другий вид слідів є специфічним для цього виду злочинів – комп’ютерна інформація та інформаційні сліди. Ці сліди відбиваються на носіях інформації у вигляді сигналів, кодів, зарядів, полів і повинні вилучатися або з носієм інформації, або шляхом копіювання з використанням спеціальних програмних продуктів, бажано із залученням спеціалістів.

Комп’ютерні сліди утворюються внаслідок впливу на комп’ютерні дані і пов’язані зі змінами, які відбуваються у самій інформації, порівняно з початковим її станом [8]. Серед багатьох науковців поширена думка про те, що здійснити вплив на комп’ютерну інформацію можливо лише за допомогою іншої комп’ютерної інформації. Виходячи з цього тезису вони зазначають, що обов’язковою ознакою “кіберзлочинів” є таке знаряддя їх вчинення, як комп’ютерна інформація. На наш погляд, внести зміни у комп’ютерні дані (пошкодити) можна не тільки за допомогою програмних засобів, а також використовуючи технічні прилади, наприклад, генератори магнітних полів.

Слід також розуміти, що комп’ютерні дані можуть або безпосередньо виступати слідами вчинення злочину, або містити такі сліди. Як вірно вказав Крилов В.В., для «цифрових» слідів характері специфічні якості, що визначають перспективи їх реєстрації, вилучення і використання як доказів під час розслідування злочину [9]. По-перше, комп’ютерна інформація існує на певних носіях, але недоступна для безпосереднього спостереження. Тобто для її виявлення та дослідження необхідне використання технічних та програмних засобів, що ставить під загрозу її подальше доказове значення, адже вказані засоби повинні бути сертифікованими і використовуватися відповідними спеціалістами. По-друге, комп’ютерна інформація не змінюється з плином часу, а також при багаторазовому копіюванні. Ця якість машинних даних пояснюється тим, що вони представлені в числовій формі за допомогою знаків “1” і “0”, а вся інформація іншого характеру, яка вноситься в комп’ютер (тексти, графіка, відео, аудіо), перетворюється у форму, зрозумілу для ЕОМ, – цифрову. По-третє, така інформація, хоча і є стабільною за змістом, може бути по-різному сприйнята залежно від засобів зчитування, декодування та відображення. Наприклад, використання невірного засобу декодування тексту особою, що бажає ознайомитись з електронним документом, призведе до виводу на дисплей або принтер незрозумілого набору символів.

Джерелами комп’ютерної інформації можуть слугувати:

- фізичні носії комп’ютерної інформації (жорсткі диски, компакт-диски, флеш-карти, накопичувачі на гнучких магнітних дисках та ін.);
- оперативний запам’ятовуючий пристрій комп’ютера;
- оперативний запам’ятовуючий пристрій периферійних пристроїв;
- комп’ютерна мережа.

Розглядаючи джерела комп’ютерної інформації, слід зазначити, що самі носії інформації не можуть розглядатися як об’єкти криміналістичних досліджень, якщо вони не містять в собі слідів вчиненого злочину [10]. У разі присутності таких цифрових слідів існує ще одна проблема − яким чином пред’явити таку інформацію в суді, щоб не виникало сумнівів в її оригінальності та щоб вона не втратила процесуальної сили доказу. Відносно цього питання існують декілька методик, але найпоширенішою є методика, запропонована американськими криміналістами, які після вилучення носія інформації, використовуючи спеціальне легітимне програмне забезпечення, знімають точну копію цієї інформації, а оригінальний носій опечатують і більше не використовують його. Вивчення потрібної їм інформації вони здійснюють зі знятої копії, а в суд пред’являють роздрукований варіант інформації (на так званому “твердому носії”). У разі виникнення підозри щодо достовірності пред’явленої в суді інформації суддя може витребувати оригінальний носій цієї інформації для звірки. Але це тільки одна з можливих проблем з доказами, тому що комп’ютерна інформація може бути зашифрована злочинцем або частково знищена, і подальші дії з її відновлення чи розшифрування правоохоронними органами будуть доволі суперечливими з погляду чинного кримінально-процесуального законодавства.

Розглядаючи комп’ютерні дані як джерело криміналістичної інформації, не можна оминути і питання її безпосереднього вилучення. Таке вилучення може проводитись в ході обшуку, огляду місця події, виїмки або навіть відтворення обстановки і обставин події [11]. При цьому суб’єкту доказування слід додержуватись спеціальних правил, які не характерні для вилучення речових доказів по інших категоріях злочинів. Головними завданнями при такому вилученні є: не втратити і не пошкодити інформацію, що знаходиться в оперативній пам’яті ЕОМ та на інших носіях інформації, правильно з процесуальної точки зору вилучити обладнання, а також виявити всі пристрої та носії інформації, які можуть мати доказове значення у справі. Також не слід забувати про дуже широке на теперішній час коло носіїв цифрової інформації, які навіть без додаткового маскування з боку злочинця, можуть мати зовнішній вигляд ручки, іграшки, брелока або будь-якого іншого предмета, в який вбудована flash-карта або інший носій інформації*.

Також слід зазначити, що до криміналістичної інформації по злочинах у сфері комп’ютерних технологій належить інформація, отримана під час застосування спеціальних знань: проведення експертних досліджень, інших досліджень комп’ютерної інформації, враховуючи її пошук та виїмку, консультації спеціалістів. Але у будь-якому випадку, коли слідчий чи інша процесуальна особа має справу з комп’ютерною інформацією, бажано залучати до цього процесу відповідних спеціалістів, тому що всіх аспектів поводження з цифровими даними не може знати навіть найобдарованіший юрист,

* flash-карта представляє собою відносно новий вид енергонезалежної пам’яті, виконаний у вигляді невеликого розміру мікрочіпу та групи контактів для з’єднання з іншими пристроями. До інших носіїв інформації можна віднести: міні-диски (зменшені CD); мініатюрні жорсткі дики, якими в наш час комплектуються MP3- та мультімедіаплеєри, та багато інших накопичувачів цифрових даних.

а втратити або пошкодити такий вид джерела криміналістичної інформації надзвичайно легко.

Висновки. На основі вищевикладеного можна зазначити, що комп’ютерні дані безперечно можуть виконувати роль джерел криміналістичної інформації як відносно злочинів у сфері використання комп’ютерних технологій, так й інших видів злочинів, де вони присутні. Сліди злочину, залишені на цифровій інформації, мають певні особливості, які повинні бути враховані під час їх збирання, закріплення та дослідження. У зв’язку з вищевикладеним вбачається необхідність подальшого дослідження кримінально-процесуальних властивостей комп’ютерної інформації та впровадження його результатів в практичну діяльність правоохоронних органів.

Використана література

1 Гаврилин Ю. В. Расследование неправомерного доступа к компьютерной информации: Автореф. дис. …канд. юрид. наук. 12.00.09. – М., 2000. – 23 с.

2. Яковлев А.Н. Теоретические и методические основы экспертного исследования документов на машинных магнитных носителях информации: Автореф. дис. …канд. юрид. наук. 12.00.09. – Саратов, 2000. – 24 с.

3. Закон України “Про інформацію” // Відомості Верховної Ради України. – 1992. – № 48. – С. 3

4. Закон України “Про захист інформації в автоматизованих системах” // Відомості Верховної Ради України. – 1994. – № 31. – С. 2

5. Лук’янчиков Б.Є., Лук’янчиков Є.Д., Поняття і види криміналістичної інформації // Вісник НАВС України. – К., 2000. – № 1. – С. 72-77.

6. Хлынцов М.Н. Криминалистическая информация и моделирование при расследовании преступлений. – Саратов: Изд-во Сарат. ун-та, 1982. – С. 38

7. Паламарчук Л.П. Криміналістичне забезпечення розслідування незаконного втручання в роботу електронно-обчислюваних машин (компютерів), систем та комп’ютерних мереж: Автореф. дис. …канд. юрид. наук, 12.00.09. – К., 2005. – 24 с.

8. Біленчук П.Д., Романюк Б.В., Цимбалюк В.С. та ін. Комп’ютерна злочинність: Навчальний посібник. – К.: Атика, 2002. – 240 с.

9. Крылов В. В. Информационные компьютерные преступления. – М., 1997. – С. 27.

10. Волеводз А.Г. Противодействие компьютерным преступлениям: правовые основы международного сотрудничества. – М.: ООО Издательство “Юрлитинформ”, 2002. – 154 с.

11. Голубєв В.О. Комп`ютерні злочини в банківській діяльності. – З.: Павел, 1997. – С. 125.

~~~~~~~~~~~~~ * * * ~~~~~~~~~~~~~
~~~~~~~~~~~~~