сів України та Положення про комісії у справах неповнолітніх Української РСР» //Відомості Верховної Ради. 1994. № 11. Ст. 48. 3. Закон України «Про органи і служби у справах неповнолітніх та спеціальні установи для неповнолітніх» //Відомості Верховної Ради. 1995. № 6. Ст. 36. 4. Дяченко К.І., Шость Н.В. Процесуальні особливості розслідування справ про злочини неповнолітніх. Х., 1997. 5. Указ Президії Верховної Ради СРСР // Відомості Верховної Ради. 1978. № 24. Ст. 359. 6. Кримінально-процесуальний кодекс України. Науково-практичний коментар. К., 1995. 7. Кримінальний кодекс України. Науково-практичний коментар. К., 1994.

Надійшла до редколегії 05.10.98

О.П. Снігерьов, д-р юрид. наук,
В.О. Голубєв

Проблеми класифікації злочинів у сфері комп'ютерної інформації

Проблеми інформаційної безпеки постійно посилюється процесами проникнення практично у всі сфери діяльності суспільства технічних засобів обробки та передачі даних й передусім обчислювальних систем. Це дає підставу поставити проблему комп'ютерного права, одним з основних аспектів якої є так зване комп'ютерне посягання. Про актуальність проблеми свідчить довгий перелік можливих способів скоєння злочинів у сфері комп'ютерної інформації.

У сучасній літературі існують різні точки зору в питаннях виділення та класифікації таких злочинів [1, с.42–74, 2]. «Комп'ютерні злочини» або точніше злочини в сфері комп'ютерної інформації умовно можна поділити на дві великі категорії: злочини, пов'язані з втручанням в роботу комп'ютерів, і злочини, у яких використовуються комп'ютери як необхідні технічні засоби.

На основі аналізу, а також всебічного вивчення спеціальної літератури [1, 2, 3, 4, 5,] можна визначити понад 20 основних способів скоєння злочинів в сфері комп'ютерної інформації і майже 40 їх різновидів, число яких постійно збільшується внаслідок використання злочинцями різних їх комбінацій. Дане явище зумовлене як складністю самих засобів комп'ютерної техніки, так і різноманітністю та постійним нарощуванням інформаційних операцій, багато з яких відображають рух матеріальних цінностей, фінансових і грошових коштів, науково-технічних

розробок тощо, які зумовлюють об'єкт, предмет і знаряддя злочину. Важливим тут є і факт специфічності самих засобів обчислювальної техніки, які беруть участь в інформаційних процесах, виражений в їх подвійності: як предмет, і як засіб скоєння таких злочинів.

У той же час потрібно підкреслити, що практично всі способи скоєння злочинів в сфері комп'ютерної інформації мають свої індивідуальні властивості, за якими їх можна розпізнати і класифікувати в окремі групи. Як правило, їх основою є дії злочинця, направлені на отримання доступу до засобів комп'ютерної техніки. Здебільшого всі ці дії супроводжуються кваліфікованими засобами маскування, що ускладнює процес виявлення та розкриття злочину. У більшості випадків злочинцями використовуються різні комбінації декількох основних способів, які мають досить простий алгоритм виконання і добре відомі вітчизняній юридичній практиці по традиційних видах злочинів. У міру їх модифікації та постійного ускладнення з'являються все нові та нові способи, які із злочину в злочин все більш удосконалюються та модернізуються.

На наш погляд, основні способи скоєння злочинів в сфері комп'ютерної інформації можна класифікувати за шістьма основними групами. При цьому як головна класифікуюча ознака виступає метод використання злочинцем тих або інших дій, направлених на отримання доступу до засобів комп'ютерної техніки з різними намірами.

Керуючись цією ознакою, ми виділили наступні групи: 1) втручання або перехоплення інформації; 2) зміна або пошкодження інформації; 3) комп'ютерне шахрайство; 4) несанкціоноване копіювання; 5) комп'ютерний саботаж; 6) інші злочини, пов'язані з комп'ютером.

До першої групи нами віднесені способи скоєння комп'ютерних злочинів у сфері комп'ютерної інформації, засновані на діях злочинця, направлених на: незаконний доступ; перехоплення; викрадення машинного часу.

До другої групи відносяться злочини, пов'язані з зміною або пошкодженням інформації: «Логічна бомба»; «Троянський кінь»; програми-віруси; «Черв'яки».

До третьої групи злочинів в сфері комп'ютерної інформації нами віднесені комп'ютерне шахрайство, яке відрізняється від звичайного тільки тим, що злочинці використовують переваги сучасних комп'ю-

терних технологій та мереж. Шахрайства, пов'язані з комп'ютерами, через відсутність специфічних правових норм підпадають під існуючі в кримінальному законодавстві визначення шахрайських дій, і відповідальність може наступати за цими статтями. Такі злочини спрямовані на отримання фінансового прибутку або іншої вигоди і засновані на діях злочинця, направлених на:

шахрайство з автоматами для видачі готівки;

комп'ютерна підробка;

шахрайство з ігровими автоматами;

шахрайство шляхом неправильного вводу/виводу або маніпуляції програмами;

шахрайство з платіжними засобами;

телефонне шахрайство.

До четвертої групи злочинів в сфері комп'ютерної інформації нами віднесені способи скоєння комп'ютерних злочинів, засновані на діях злочинця, направлених на:

несанкціоноване тиражування комп'ютерних ігор;

несанкціоноване тиражування програмного забезпечення;

несанкціоноване тиражування напівпровідникової продукції;

інші випадки несанкціонованого копіювання.

П'ята група – це способи скоєння злочинів у сфері комп'ютерної інформації, засновані на діях злочинця, направлених на:

саботаж технічного забезпечення;

саботаж програмного забезпечення.

До шостої групи належать злочини в сфері комп'ютерної інформації, засновані на діях злочинця, направлених на:

незаконне використання INTERNET та дошки електронних оголошень (BBS);

викрадення комерційної таємниці;

зберігання або розповсюдження матеріалів, які є об'єктом судового переслідування.

Для того, щоб зупинити «комп'ютерного злочинця», необхідно визначити можливі точки прикладення його зусиль до комп'ютерної інформації і встановити на його шляху систему відповідних перешкод достатньої міцності. Вирішення проблеми буде значно полегшене, якщо

для безлічі різних видів скоєння таких злочинів буде прийнята єдина узагальнена класифікація злочинів у сфері комп'ютерної інформації.

Список літератури:

1. Голубєв В.О. Програмно-технічні засоби захисту інформації від комп'ютерних злочинів. Запоріжжя. 1998. 2. Computer and crime. Interpol. 1997. 3 Announcing the Guideline for the Use of Advanced Authentication Technology Alternatives. – Federal Information Processing Standards Publication 190, 1994. 4. Announcing the Standard for Automated Password Generator. – Federal Information Processing Standards Publication 181, 1993. 5. Біленчук П.Д., Зубань М.А. Комп'ютерні злочини: соціально- правові і кримінолого- криміналістичні аспекти. Навч. посібник. К., 1994.

Надійшла до редколегії 29.05.98

А.Ф. Волобуєв, кано. юрид. наук

ЕТАПИ РОЗСЛІДУВАННЯ В КРИМІНАЛІСТИЧНІЙ МЕТОДИЦІ

Однією з проблем, яка залишається не вирішеною остаточно в теорії криміналістичної методики, є поняття етапів розслідування. Найбільш відоме визначення цього поняття дав І.М. Лузгін, який вважав, що етап розслідування – це такий його елемент, який являє собою певну систему дій, об'єднаних єдністю задач, умовами розслідування, специфікою криміналістичних прийомів [1, с.86]. Таке визначення певною мірою вплинуло на те, що окремі вчені-криміналісти в методиках розслідування злочинів не тільки називають різну кількість етапів, але і порізному трактують їх зміст.

У зв'язку з цим треба звернути увагу, що з етимологічної точки зору поняття «етап» (від франц. etape) означає «перехід, місце зупинки» Кримінально-процесуальний закон у структурі попереднього розслідування злочину не виділяє будь-яких етапів. Акцент робиться на процесуальних рішеннях (порушенні кримінальної справи, вибір запобіжного заходу, притягнення особи як обвинуваченого та ін.). Але в криміналістичній методиці процес розслідування злочину розглядається перш за все як система внутрішньо взаємопов'язаних та скоординованих процесуальних дій, спрямованих на виявлення, фіксацію, вилучення та використання доказів. На певних проміжках розслідування у кримінальній