спростувати причетність її до злочину (хоча, звичайно, сам собою цей факт ще є недостатнім для висновку про винуватість людини).

Наука і далі, безсумнівно, буде розвиватися, що приведе і до подальшого розширення можливостей експертизи. Тому перед системою підвищення юридичної кваліфікації працівників суду і правоохоронних органів повсякденно стоїть завдання постійного відновлення їх знань у цій сфері. У першу чергу це залежить безпосередньо від самих практиків, від того, наскільки уважно вони знайомляться з новинками спеціальної літератури, консультуються з фахівцями і т.п.

Стаття рекомендована для друку кафедрою кримінального процесу і криміналістики Львівського національного університету імені Івана Франка (протокол № 1 від 28 серпня 2003 р.)

Кравчук С.Й.,
доцент кафедри права Хмельницького державного університету, кандидат юридичних наук

Кравчук О.С.,
інженер-програміст приватної фірми "Система" (м. Хмельницький)

ОСНОВНІ ПРОБЛЕМИ ТА НАПРЯМИ ПРОТИДІЇ ЗЛОЧИННОСТІ В СФЕРІ ЕКСПЛУАТАЦІЇ ЕЛЕКТРОННО-ОБЧИСЛЮВАЛЬНИХ СИСТЕМ

В останні роки відмічається тенденція негативного впливу інформаційних технологій на діяльність окремих економічних суб'єктів та органів влади і управління. Ця проблема є досить актуальною і в останні роки розроблялась багатьма науковцями України та Росії. Зокрема, проблеми злочинності в сфері експлуатації електронно-обчислювальних систем опрацьовувались на теоретичному грунті В.О. Голубєвим, А.А. Барановим, П.Д. Біленчуком, М.А. Зубанем та іншими вченими.

Порівняльний аналіз зарубіжної та вітчизняної практики інформатизації свідчить, що комп'ютерна злочинність несе в собі низку суспільно небезпечних проблем, За повідомленнями засобів масової інформації, тільки в США економічні збитки від комп'ютерних правопорушень складають щорічно близько 100 млрд. дол. США. У Франції тільки втрати банків досягають 1 млрд. франків на рік і кількість подібних злочинів збільшується на 30-40% щорічно. У Німеччині "комп'ютерна мафія" викрадає на рік близько 4 млрд. марок. У Великобританії лише асоціація страхових компаній несе збитки на суму понад 1 млрд. фунтів стерлінгів на рік [5, 85-86].

В той же час, на сьогодні проблеми протидії злочинності у сфері інформаційних технологій потребують досконалого законодавчого врегулювання.

В той же час, по мірі інформатизації в Україні найближчим часом може значно зрости кількість злочинів, вчинених із застосуванням комп'ютерних технологій. Виходячи із тенденцій до зростання таких злочинів, фахівцями прогнозується нанесення Україні економічних збитків на суму близько 10 млрд.грн. щорічно.

Комп'ютерна злочинність має високий рівень латентності. За даними фахівців, лише 10-15% таких правопорушень стають відомими громадськості та правоохоронним органам, оскільки установи та організації, які зазнали шкоди, неохоче повідомляють про них, щоб не створити собі негативної репутації. На думку фахівців, комп'ютери є знаряддям вчинення таких злочинів, як тероризм, шпигунство, шахрайство, крадіжка. Особливої уваги правоохоронних органів заслуговує виявлення, упередження та припинення операцій по легалізації доходів незаконного походження шляхом застосування інформаційних технологій. За їх допомогою вчиняється в Україні більшість злочинів, пов'язаних з викраденням і "відмиванням" коштів за допомогою електронних засобів зв'язку [4, 48].

Основним об'єктом комп'ютерної злочинності є кредитно-фінансова сфера, зокрема банківські установи. Розвиток мережі комерційних банків з великими обсягами фінансових операцій, зростання обсягів переказів коштів між державними і комерційними структурами як у межах України, та і за кордоном, призвели до необхідності вирішення питання про спрощення розрахунків шляхом впровадження у банківську систему комп'ютерних та телекомунікаційних технологій. Введення мережі електронних розрахунків спричинило до зміни техніки вчинення корисливих злочинів у сфері банківської діяльності. З'явилися нові вразливі ланки, як до прикладу система "Банк-Клієнт", міжбанківські мережі, слабку захищеність яких стали використовувати оснащені потужною комп'ютерною технікою шахраї [6, 203]. Про це свідчать виявлені та відвернуті правоохоронними органами за останні 5 років злочини, пов'язані із несанкціонованим проникненням до комп'ютерних мереж фінансових структур України та намаганнями незаконного переведення коштів на власні рахунки окремих господарюючих суб'єктів, жителів України та іноземних громадян [2, 16].

Зокрема, не допущені спроби незаконного переведення з рахунку Національного банку України до АКБ "Таврія" 10 млн. грн., втручання в електронну систему Мелітопольського відділення АК АПБ "Україна" з метою крадіжки 448 тис. грн., спроби викрадення 182 тис. грн. З використанням електронних міжбанківських розрахунків у Закарпатському відділенні банку "Аваль".

Відмічаються випадки проникнення до банківських рахунків України окремими злочинцями як із-за кордону, так і з території нашої держави у зарубіжні кредитні структури.

Так, через фіктивну київську фірму було викрадено з використанням інформаційних технологій 200 тис. дол. у Московського представництва "American express". Подібним чином намагалися діяти злочинці м. Санкт-Петербурга, які у жовтні 2002 року вчинили "хакерську" атаку на поштовий сервер однієї з філій АППБ "Аваль". При цьому ними вчинялась спроба викачування з основного сервера інформації щодо фінансового стану усіх клієнтів банку.

Одним із методів заволодіння коштами державних установ та колективних підприємств і організацій стало незаконне втручання в роботу комп'ютерних мереж сторонніх осіб.

В середині 2003 року виявлено низку фактів втручання у комп'ютерні системи більш ніж 40 клієнтів (в основному державних установ) через одну із комп'ютерних фірм м. Хмельницького, яка надає інтернет-послуги. Серед них установи, що фінансуються з державного бюджету: виконавчі комітети та правоохоронні органи, а також ряд найбільших підприємств регіону. Для проникнення в їх комп'ютерну мережу зловмисниками використовувався комп'ютерний вірус "TrojanCow 1.0 Cow Client", який розсилався з електронною поштою відповідним адресатам. Вірус проникав до файлів системного адміністратора та копіював "логіни" і паролі доступу до мережі "Інтернет" з ураженого комп'ютера та повертався до свого безпосереднього відправника. Після чого зловмисниками проводилось сканування мережі для пошуку файлів, отриманих за допомогою вірусу. Отримані паролі та "логіни" порушники використовували у власних протиправних цілях.

Після подій 11 вересня 2001 року в США певного розповсюдження набуває використання Інтернету для погроз посадовцям.

Так, два студенти одного із навчальних закладів м. Києва, використовуючи ресурси Інтернет-клубу, підготували та відправили електронною поштою лист з погрозами терористичного характеру на адресу штаб-квартири Міністерства оборони іноземної держави.

Всебічний аналіз вітчизняного законодавства, яке регулює суспільні інформаційні відносини в Україні, дозволяє стверджувати, що наша держава вживає заходів упереджувального характеру, спрямованих на їх вдосконалення, недопущення несанкціонованого використання комп'ютерних технологій.

Зокрема, Кримінальний кодекс України передбачає відповідальність за умисне втручання у роботу автоматизованих систем, що призвело до перекручення чи знищення інформації, або носіїв інформації, чи розповсюдження програмних і технічних засобів, призначених для незаконного проникнення в автоматизовані системи і здатних спричинити до перекручення, знищення інформації чи носіїв інформації [1, 105].

В той же час, введення до Кримінального кодексу України статей, які передбачають відповідальність за вчинення кримінальних злочинів у сфері комп'ютерних технологій, не вирішить проблеми запобігання таким злочинам [3, 8]. Для усунення передумов до вчинення таких злочинів та ефективній протидії комп'ютерної злочинності необхідно прийняти програму по боротьбі з комп'ютерними злочинами, яка повинна передбачати створення:

- правових та організаційних засад для побудови в державі функціонально повної системи по боротьбі з комп'ютерними злочинами;
- спеціалізованих підрозділів в правоохоронних органах по боротьбі з комп'ютерними злочинами та організація їх взаємодії;
- спеціалізованих криміналістичних підрозділів з розслідування комп'ютерних злочинів;
- системи проведення організаційної, пропагандистсько-профілактичної роботи з запобігання комп'ютерним злочинам.

Крім того, в такій програмі окремим розділом необхідно передбачити організацію підготовки та перепідготовки кадрів по боротьбі з комп'ютерними злочинами.

В цілому проблема комп'ютерних злочинів є для України достатньо новою. В той же час, на думку фахівців, якщо зараз не створити відповідну фінансово-правову, організаційну, технічну та технологічну інфраструктуру протидії цим проявам, то з часом в Україні ситуація стане набагато складнішою, ніж на Заході. Хоча комп'ютерна злочинність тут почала розвиватись пізніше, однак недосконалість, а з певних криміногенних аспектів – відсутність комплексу необхідної організаційно-правової та матеріальної бази створює сприятливі умови для розвитку такої злочинності. Разом з тим гальмується робота з виявлення і локалізації подібних некримінальних, але небезпечних діянь.

Тому правоохоронним органам, особливо Службі безпеки України, до компетенції якої входить розслідування подібних злочинів, доцільно вивчити та узагальнити досвід іноземних країн по боротьбі із незаконним і протиправним використанням інформаційних технологій, особливо для "відмивання" та привласнення незаконно отриманих коштів, систематизувати і досліджувати дані види злочинів в Україні і за її межами (у випадках, якщо це стосується "відмивання" українських грошових коштів).

Для вирішення цього питання необхідно створити відповідний центр із дослідження та розробки цього питання, що підвищить результативність боротьби із злочинністю в сфері експлуатації електронно-обчислювальних систем та її проявами.

Література

1. Кримінальний кодекс України. // Офіційний вісник України. – 2001. –С. 105-106.
2. Голубєв В.О. Комп'ютерні злочини в банківській діяльності. – З.: Павел., 1997. – С. 16-18.
3. Баранов А.А. Уголовная ответственность за компьютерные преступления // Безопасность информации. –1996. – № 2. – С. 4-9.
4. Біленчук П.Д., Зубань М.А. Комп'ютерні злочини: соціально-правові і криміналістичний аспекти: Навч. посібник. – К.: Українська академія внутрішніх справ. 1999. – 71 с.
5. Крутских А. Информационный вызов безопасности на рубеже XX1 века// Международная жизнь. –1999. – № 2. – С. 83-89.
6. Яровий Б.Д. Злочинність у сфері інформаційних технологій: проблеми та напрями боротьби із нею // Актуальні проблеми кримінального і кримінально-процесуального законодавства та практики його застосування. – Хмельницький: Хмельницький інститут регіонального управління та права. –2003. –С. 242-245.

Стаття рекомендована до друку кафедрою права
Технологічного університету Поділля
(протокол № 1 від 29 серпня 2003 р.)

Саінчин О.С.,
декан юридичного факультету
Міжнародного гуманітарного
університету, кандидат юридичних наук,
доцент

ОСОБЛИВОСТІ ПРИВАТНОЇ МЕТОДИКИ РОЗКРИТТЯ УБИВСТВ, СКОЄНИХ ІЗ ЗАСТОСУВАННЯМ ВОГНЕПАЛЬНОЇ ЗБРОЇ, ВИБУХОВИХ ПРИСТРОЇВ І ВИБУХОВИХ РЕЧОВИН

У ст. 3 Конституції України проголошено, що людина, її життя і здоров'я, честь і воля, недоторканність і безпека визнаються в Україні найвищою соціальною цінністю. Кожна законослухняна людина має бути впевнена, що з метою реалізації цієї, мабуть, найважливішої конституційної норми, державою має бути вироблений визначений кримінально-правовий механізм, який захищає й охороняє життя і здоров'я людини від зазіхань, під страхом суворого покарання.

Проблемам розкриття убивств у випадку відсутності трупа видатними вченими-криміналістами О.Я. Баєвим[1], Л.Г. Відоновим[2], Ю.П. Дубягіним[3], В.П. Колмаковим[4],

[1] Баев О.Я. Одиноких А.С. Расследование убийств, сопряженных с сокрытием трупа // Расследование отдельных видов преступлений. Воронеж: Изд-во Ворон. - Ун-та, 1986.

[2] Видонов Л.Г. Криминалистическая характеристика убийств и системы типовых версий о лицах, совершивших убийства без очевидцев: Метод. рекоменд. к использованию систем типовых версий. - Горький, 1978.

[3] Дубягин Ю.П. Как не пропасть без вести. - СПб.: Питер-Пресс, 1996.

[4] Колмаков В.П. Расследование убийств: Лекция для студентов. - М.: ВЗЮИ, 1958.