А.Ф.Волобуєв, канд.юрид.наук

Проблеми розслідування "комп'ютерних" злочинів

Розвиток в Україні сучасних інформаційних технологій, телекомунікаційних систем, комп'ютеризація суспільства взагалі призводять до появи зовсім нових соціальних проблем, в тому числі і у сфері боротьби зі злочинністю. Розширення мережі комерційних банків, які використовують для спрощення розрахунків у фінансових операціях комп'ютерну техніку, сприяло появі специфічних злочинів, які пов'язані з використанням цієї техніки і завдають великої матеріальної шкоди. У цьому плані перед правоохоронними органами стоїть завдання своєчасного їх виявлення, кваліфікованого розслідування та прийняття заходів для усунення причин та умов, що сприяли здійсненню цих злочинів. І тут дуже важливо використовувати досвід боротьби з комп'ютерною злочинністю, набутий в інших країнах з ринковою економікою, і перш за все в США.

США вважаються батьківщиною не тільки комп'ютерів, але й комп'ютерної злочинності. Вперше термін "комп'ютерний злочин" з'явився більше 30 років тому. Протягом часу цей вид злочинів бурхливо розвивався, набуваючи найрізноманітніших форм. Перш за все, це пояснювалось тим, що комп'ютер, який використовується у фінансових операціях, має дуже великий та спокусливий потенціал для збагачення. Для прикладу, лише один комп'ютер у Нью-Йорк Сіті містить у собі більш 8 млрд. дол. в активах обігових грошово-кредитних документів. Керівники багатьох компаній та банків не приділяли належної уваги контролю за операціями, вважаючи себе недостатньо компетентними у цих питаннях. Тож створюються сприятливі умови для скоєння злочинів персоналом, який обслуговує комп'ютери у цих фірмах. Крім цього, в окремих випадках власники компаній, дізнавшись про подібні операції своїх підлеглих, не тільки не повідомляли про це в поліцію, а й допомагали приховати їх з метою подальшого використання злочинної "методи" у боротьбі зі своїми конкурентами. Цим, а також і деякими іншими причинами пояснюється високий рівень латентності комп'ютерних злочинів. За деякими оцінками тільки 15% злочинів такого виду стають відомі поліції, а притягається до кримінальної відповідальності лише один злочинець з 22 тис. Збитки ж від цих злочинів

становлять величезні суми і обчислюються сотнями мільйонів доларів щорічно [1, с.446].

Але не зважаючи на це, в США все ж накопичено відповідний законодавчий та практичний досвід боротьби з комп'ютерними злочинами, який може бути використаний у діяльності органів внутрішніх справ України. Це є актуальним у зв'язку з тим, що все виразніше виявляється тенденція до розширення кордонів комп'ютерної злочинності, набуття нею транснаціонального характеру.

Американська криміналістична література визначає такі види комп'ютерних злочинів:

1. Крадіжки послуг (крадіжка машинного часу). Цей вид злочину здійснюється службовими особами або персоналом, який обслуговує комп'ютери, для виконання робіт, що не пов'язані з їх службовою діяльністю. Тобто, по своїй суті - це є незаконна експлуатація комп'ютера. Наприклад, використання службовцями фірми часу для обчислювання найбільш вигідних варіантів парі, які укладають на результати футбольних ігор тощо.

2. Інформаційні злочини. Цей вид злочину має два різновиди:

- використання інформації, що зберігається в комп'ютері, у власних інтересах(наприклад, викрадення з комп'ютера фірми, з якою конкурують, списку найбільш вигідних клієнтів);
- внесення до комп'ютера неправильної інформації з метою отримання власної вигоди (наприклад , зміна показників низької кредитоспроможності особи або компанії у кредитних файлах комп'ютера на більш високі).

3. Фінансові злочини. Використання комп'ютерів, що застосовуються для обробки фінансових операцій, з метою незаконного отримання грошей. Цим видом злочинів охоплюються різного роду шахрайські операції, що виконуються за допомогою комп'ютера. Наприклад, керівник одного з офісів брокерської фірми в Нью-Йорку запрограмував комп'ютер таким чином, що той поступово і непомітно "перекачував" грошові активи фірми на його рахунок і на рахунок його дружини. Таким чином за 8 років він викрав приблизно 250 тис. доларів, поки злочин було виявлено.

4. Злочини проти власності. До цього виду злочинів американські джерела відносять втручання у комп'ютерну мережу певної компанії, що

тягне за собою порушення її нормального функціонування, а також псування, руйнування комп'ютерних даних або програм.

5. Злочини проти особистості - загальнокримінальні злочини, які здійснюються з використанням комп'ютера як допоміжного засобу. Наприклад, злочинець відкрив рахунок у банку на фіктивне ім'я і випробував кілька віддалених від банку розподільних автоматів для того, щоб бути впевненим, що він має прихований доступ до свого рахунку. Після цього він викрав маленьку доньку відомого актора і вимагав за неї викуп, який треба було покласти на вказаний рахунок до банку. Зняти ці гроші злочинець міг через один із 348 розподільних автоматів. Завдяки заходам, що були вжиті поліцією, злочинець був затриманий у момент, коли виходив з готівкою з розподільної станції, а дитина неушкодженою була повернена батькам [1, с.447-449].

Зазначимо, що певні види комп'ютерних злочинів скоюються особами з невеликим досвідом роботи з комп'ютером, і більшість їх виявляється при відповідних перевірках. Розслідування у цих випадках включає проведення таких звичайних процесуальних і оперативних дій, як допит персоналу, що обслуговує комп'ютерну техніку, допит підозрюваного, заходи по встановленню його зв'язків і кримінального минулого, обшуки робочого місця підозрюваного і його помешкання, вилучення документів у банках, які використовувались підозрюваним і його співучасниками та ін. Але якщо злочин скоїв висококваліфікований спеціаліст у галузі комп'ютерної техніки, досвідчений і акуратний, то його виявлення може затягнутися на декілька років. Як показує практика, поліцією США виявляються такі злочини найчастіше завдяки кмітливості інформаторів поліції, які працюють на тій чи іншій фірмі, або за повідомленням обділених співучасників злочину. І навіть якщо такий комп'ютерний злочин виявлено, то його розслідування часто пов'язане з серйозними труднощами у доказуванні, тому що його наслідки дуже схожі на технічні неполадки комп'ютера, недоліки в програмному забезпеченні, помилки користувачів. Американські кримінологи виділяють особливий тип комп'ютерних злочинців. Це комп'ютерні хулігани, яких називають хекерами. Хекери - особи, які задля розваги намагаються отримати і отримують незаконний доступ до комп'ютерних систем шляхом відгадування коду (паролю). Отримавши доступ, хекери мають можливість викрадати, перероблювати або знищувати програми і інформацію. Розроблено і соціально-психологічний портрет цих осіб,

який використовується в діяльності поліції. Типові риси хекера: вік 16-17 років; достатньо високий рівень інтелекту, але погана успішність у навчанні (неграмотно пишуть); велика самовпевненість; не користуються популярністю серед однолітків. Переважаючий психологічний тип - інтроверти [6, с.4-5].

Складність виявлення комп'ютерних злочинів, а також їх розслідування диктує необхідність прийняття спеціальних заходів по боротьбі з ними. У США для цього в рамках ФБР створений спеціальний підрозділ, до якого входять поліцейські, що отримали спеціальну освіту і пройшли спеціальну підготовку.

Допомога спеціалістів при розслідуванні комп'ютерних злочинів необхідна, наприклад, для встановлення підозрюваного шляхом визначення того, які знання і технічні навички потрібні для виконання відповідних операцій на комп'ютері, а також для проведення експертиз комп'ютера чи окремих його вузлів. Відповідним обсягом знань в області комп'ютерної техніки повинен володіти і слідчий. Він повинен знати, наприклад, що на одній магнітофонній касеті може бути записано інформації більше, ніж її вміщає книжкова полиця. Повинен знати, що ця інформація може бути легко знищена і не тільки злочинцем, але й самим слідчим у результаті невмілого поводження з нею. Взяти, наприклад, так звану "пастку для дурнів", коли спроба слідчого відтворити запис може потягнути за собою її автоматичне стирання. Використання подібних джерел інформації передбачає постійний контакт слідчого і спеціаліста при розслідуванні комп'ютених злочинів [1, с.451].

У результаті ознайомлення з американськими джерелами щодо проблеми, що розглядається, можна дійти висновку про те, що у понятті "комп'ютерні злочини" поєднуються дуже різноманітні злочини, тим чи іншим чином пов'язані з використанням комп'ютера при їх скоєнні. Під впливом закордонних публікацій такий підхід відображається і у вітчизняній криміналістичній літературі [4, с.6]. При цьому немає чіткого визначення поняття "комп'ютерні" злочини, що відмежовувало б даний вид злочинів від інших. Це дозволяє до категорії комп'ютерних віднести практично будь-який злочин, якщо встановлено, що злочинець при підготовці, скоєнні і приховуванні злочину використовував комп'ютер (наприклад, як засіб накопичення і зберігання інформації).

На наш погляд, такий підхід не є конструктивним, оскільки породжує багатозначність і неясність, як в теоретичному, так і в практич-

ному аспекті. Є очевидним, що методики розслідування різних злочинів, здійснених з використанням комп'ютера, різноманітні. Немає сумніву, що з розширенням сфери застосування комп'ютерної техніки в Україні з'являться (і вже з'являються) нові види посягань. І бажано в боротьбі з ними використовувати зарубіжний досвід, критично оцінюючи його. Перш за все, необхідно сформулювати чітке поняття "комп'ютерні" злочини і вказати на суттєві ознаки нового виду злочинів.

Аналіз злочинів, які зустрічаються в практиці поліції США, показує, що комп'ютер у механізмі здійснення цих злочинів відіграє різноманітну роль. На нашу думку, ця ознака - роль, що її відіграє комп'ютер у механізмі скоєння злочинів, - повинна бути покладена в основу їх класифікації та відповідної назви. Такий підхід дозволяє виділити три групи злочинів.

Перша група - це злочини, в яких специфічні властивості комп'ютера виступають в якості безпосереднього предмету посягань (розкрадання машинного часу, несанкціоноване втручання в процес обробки інформації, несанкціоноване використання комп'ютерної інформації, знищення комп'ютерних даних чи програм, несанкціоноване копіювання комп'ютерних програм). Названі злочини посягають на специфічний предмет - властивості комп'ютера, окремі елементи комп'ютерної системи, завдаючи тим самим збитків суспільним відносинам по володінню, використанню і розпорядженню комп'ютерною технікою (об'єкт посягань). Як відомо, для розподілу злочинів на види в Кримінальному кодексі України (як і в кодексах інших держав СНД) використовується, перш за все, предмет і об'єкт посягань. Саме тому названу групу злочинів можна віднести до виду комп'ютерних.

Друга група - злочини, скоєні шляхом використання комп'ютерної системи, як засобу досягнення злочинної мети. Як правило, це злочини, направлені на заволодіння грошима чи власністю шляхом присвоєння, зловживання службовим становищем або шахрайством.

Оскільки комп'ютер тут використовується як знаряддя, то, на нашу думку, такі злочини називатися комп'ютерними не можуть. Вони повинні іменуватися відповідно до предмету посягань і засобу заволодіння ним - розкраданням грошей (власності) шляхом присвоєння (зловживання службовим становищем, шахрайства) з використанням комп'ютера. Тобто, це традиційні злочини, у здійсненні яких з'явився новий засіб.

Третя група - злочини, пов'язані з комп'ютером. Перш за все, до цієї категорії слід віднести:

- злочини, в яких комп'ютер виступає як предмет посягання, як матеріальна цінність (наприклад, крадіжка комп'ютера);
- злочини, в яких комп'ютер грає роль допоміжного засобу досягнення зв'язку між співучасниками або сховища певної інформації.

Практично будь-який злочин може бути пов'язаний з використанням комп'ютера, як, наприклад, і автомобіля. Тому немає ніякої підстави називати ці злочини комп'ютерними, як нема підстави називати "автомобільними" злочини, що пов'язані з використанням автомобіля.

Таким чином, поняттям "комп'ютерний злочин", на наш погляд, мають бути охоплені не всі злочини, тим або іншим чином пов'язані з використанням комп'ютерної техніки, а тільки окремий вид (група) злочинів, в яких предметом посягання є специфічні якості комп'ютера або окремі елементи комп'ютерних систем, а об'єктом, відповідно, суспільні відносини по володінню, використанню комп'ютерної техніки.

Поступово комп'ютерний ринок в Україні розширюється. На ньому як товар все більше з'являється різноманітного програмного забезпечення, вартість якого може в десятки і сотні разів перевищувати вартість самого комп'ютера. У зв'язку з цим з'являються і нові злочинні посягання, які вже набули великого поширення в багатьох державах з розвинутою економікою [7]. Тому вважаємо своєчасним доповнення Кримінального кодексу України ст.198., що передбачає кримінальну відповідальність за порушення роботи автоматизованих систем [5, ст.408-409]. Але, як показує зарубіжний досвід, для ведення правової боротьби з комп'ютерною злочинністю однієї норми у Кримінальному кодексі очевидно недостатньо.

Крім суто кримінально-правових проблем боротьби з комп'ютерними злочинами, правоохоронні органи України зустрічаються з труднощами у розслідуванні традиційних розкрадань майна, які скоювалися з використанням ЕОМ.

З впровадженням у систему міжбанківських розрахунків електронних засобів у різних регіонах України зареєстровано розкрадання грошей в особливо великих розмірах, учинене з використанням комп'ютерів (формування фіктивних електронних розрахунків, перерахування грошей на фіктивні рахунки з наступним їх вилученням). Розмір збитку в доларовому еквіваленті обчислюється десятками тисяч доларів у кож-

ному конкретному випадку (Дніпропетровська, Донецька обл., Автономна Республіка Крим). Це свідчить про появу нового способу розкрадання майна. ЕОМ стає багатообіцяючим засобом скоєння корисливих злочинів. Розслідування подібних злочинів пов'язане з великими труднощами, які обумовлені такими факторами:

- складністю виявлення злочинів, скоєних з використанням комп'ютерів (часто ці злочини виявляються і розкриваються випадково);
- небажанням потерпілих від злочину (найчастіше ними є великі комерційні банки та інші комерційні структури) співпрацювати з слідчими органами через страх викриття компрометуючих їх фактів;
- складнощами в розумінні порядку роботи комп'ютера в деяких технологічних ситуаціях;
- неможливістю використання звичайних методів фінансової ревізії, оскільки для передавання інформації використовуються електронні імпульси, а не фінансові документи;
- можливістю зацікавлених осіб миттєво знищити інформацію, яка зберігається в пам'яті комп'ютера.

При вирішенні проблем у ході розслідування цих злочинів отримують особливості такі традиційні слідчі дії, як огляд, допит свідків, обвинувачених (підозрюваних), обшук, вилучення та інші, які потребують участі спеціалістів у галузі комп'ютерної техніки. Особливо важливу роль у розслідуванні таких злочинів відіграє експертиза засобів комп'ютерної техніки - новий вид експертиз, методика проведення якої розроблена в Харківському науково-дослідному інституті судових експертиз [2, с.213-215; 3, с.205-207].

Поява нових засобів розкрадання грошових коштів з використанням комп'ютера як знаряддя злочину потребує відповідних заходів реагування. Яку небезпеку становлять ці злочини, показує закордонний досвід, а також досвід, що накопичується органами внутрішніх справ України (величезні суми збитків, складнощі у виявленні та розслідуванні таких злочинів). Для успішної боротьби з ними, на наш погляд, необхідно вжити заходи у трьох напрямках.

Перший - законодавчий. Вважаємо необхідним при розробці нового Кримінального кодексу України врахувати появу "комп'ютерних" злочинів, у боротьбі з ними використовувати закордонний досвід.

Другий - науково-прикладний. Розробку методик розслідування злочинів, пов'язаних з використанням комп'ютерної техніки, а також розвиток експертизи електронних засобів та програмного забезпечення розглядати як один із пріоритетних напрямків розвитку наукових досліджень у криміналістиці та судовій експертизі.

Третій - організаційний. Вважаємо за необхідне створити в органах внутрішніх справ спеціалізовані підрозділи по розкриттю та розслідуванню злочинів, які учиняються з використанням комп'ютерної техніки (за прикладом постійно діючих слідчо-оперативних груп по розслідуванню пожеж, дорожньо-транспортних пригод).

На наш погляд, є всі підстави вважати, що злочини з використанням комп'ютерної техніки в Україні будуть мати тенденцію до розвитку та розширення. Тому здійснення заходів, названих вище, націлене якщо не на попередження, то, принаймні, на своєчасне реагування держави на зміни в структурі злочинності.

Список літератури:

1. *Gharles H. Swanson, Hell C. Chamerlin, Leonard Ferrito.* Criminal investigation. New-York, 1988. 2. *Ясинов И.И., Манько И.Г., Зубова Н.О., Чугурова И.Н.* О предмете экспертизы средств электронно-вычислительной техники и программного обеспечения //Актуальные проблемы судебной экспертизы и криминалистики : Тез. науч.-практич. конф. К., 1993. 3. *Салтевский М.В., Эрнест А.В., Ясинов И.И.* К вопросу о методике судебно-экспертного исследования программного продукта для ЭВМ с целью установления автора программ// Роль судебной экспертизы и криминалистики в раскрытии и профилактике преступлений: Тез. науч.-практич. конф. Одесса, 1994. 4. *Біленчук П.Д., Зубань М.А.* Комп'ютерні злочини: соціально-правові і кримінолого-криміналістичні аспекти. К., 1994. 5. Закон України "Про внесення змін і доповнень до Кримінального кодексу України та Кримінально-процесуального кодексу України//Відомості Верховної Ради України. 1994. № 45. 6. Материалы семинара по борьбе с экономическим мошенничеством и изготовлением фальшивых денег (Combating ekonomic Fraud and counterfeiting ceminar). Вашингтон-Киев, 1995. 7. Борьба с компьютерной преступностью за рубежом: Научно-аналистический обзор. М., 1995.

Надійшла до редколегії 12.10.95 р.