І.Л. Близнюк

Проблеми комп'ютерної злочинності – правовий аспект

Подальше застосування сучасних інформаційних технологій, пов'язаних з розвитком глобальних комп'ютерних мереж, розширює можливість для різних зловживань, пов'язаних з використанням обчислювальної техніки.

Поряд з цим комп'ютеризація суспільства привела до появи нового, раніш невідомого різновиду злочинності, пов'язаного з крадіжкою, перекрученням або знищенням комп'ютерної інформації, а також іншими, часто надто зухвалими операціями проти комп'ютерних систем або за їх допомогою.

У нашій країні вже сьогодні знаходиться досить розвинута система електронного зв'язку, яка не може бути абсолютно надійною та захищеною. Така ситуація надає можливість злочинцям отримувати несанкціонований доступ до комп'ютерних інформаційних систем для проведення незаконних маніпуляцій у корисливих цілях. Процес комп'ютеризації суспільства приводить до збільшення кількості комп'ютерних злочинів, зростанню їх ваги за розмірами сум, що викрадаються в загальній частині матеріальних витрат, у порівнянні із звичайними видами злочинів.

Як свідчить практика, типовою злочинною метою, для досягнення якої неправомірно використовуються комп'ютери, є крадіжка коштів із грошових фондів; фальсифікація платіжних документів; крадіжка машинного часу; отримання фальшивих дипломів; підробка рахунків і платіжних відомостей; вторинне отримання уже проведених виплат; внесення змін у машинну інформацію; перерахування грошей на фіктивні рахунки; здійснення покупок з фіктивною оплатою; впровадження комп'ютерних вірусів з метою вимагання.

Згідно з даними міжнародного комітету по комп'ютерній злочинності, який займається дослідженням масштабів і видів комп'ютерних злочинів, а також правовими аспектами боротьби з цим видом злочинності, комп'ютерні злочини представляють

Близнюк Ігор Леонідович — кандідат юридичних наук, старший науковий співробітник НДІ НАВСУ, підполковник міліції.

собою загрозу для будь-якої організації, що має комп'ютерну техніку. По існуючим підрахункам, виведення з ладу електронно-обчислювальної системи в результаті виникнення нештатної ситуації або скоєння злочину може привести навіть самий великий банк до повного банкрутства, зруйнування та краху за чотири доби, а більш менше підприємство - за добу.

Згідно з даними комісії з попередження злочинності та кримінального права Організації Об'єднаних Націй щорічний економічний збиток від комп'ютерних злочинів, за оцінками експертів, обчислюється мільйонами доларів США, причому багато злочинів не виявляють або про них не повідомляють з причини високої латентності злочинів даного виду.

Аналіз літературних джерел свідчить про те, що рівень розкриття комп'ютерних злочинів дуже низький. Європейські спеціалісти вважають, що лише 10 % розкритих комп'ютерних злочинів може бути виявлено своєчасно, а про решту 90 % стає відомо лише випадково[1]. Що стосується нашої країни, то тут становище ще гірше. І це не значить, що у нас цих злочинів немає. Вони є, але поки що латентні. Розглянемо деякі особливості й складності, що зустрічаються при розкритті латентних комп'ютерних злочинів.

Найскладнішим є встановлення факту комп'ютерного злочину. Пояснюється це тим, що зовні сам факт здійснення комп'ютерного злочину та його прояв в оточуючому середовищі майже непомітний. Видимого матеріального збитку, здійсненого електронним злодієм, зовні не видно. Наприклад, несанкціонований доступ і незаконне копіювання інформації, або введення вірусу в комп'ютерну систему.

Потерпілі, навіть ті, кому нанесено великі збитки, не поспішають заявляти в правоохоронні органи. Пояснюється це тим, що винуватці або вже залишили місце роботи ще до факту виявлення корисливого злочину, і їх неможливо притягнути до відповідальності, або ж звільняються при їх виявленні, чи переводяться в інші структурні підрозділи і з них стягується збиток в цивільному порядку. Таким чином, кримінальна відповідальність відсутня, а значить відсутня загальна попереджувальна робота з даним видом злочинів.

"Комп'ютерну злочинність" як соціологічну категорію умовно можна поділити на дві великі категорії – злочини, пов'язані з втручанням у роботу комп'ютерів, та злочини, у яких комп'ютери використовують як необхідні технічні засоби.

У вітчизняному кримінальному праві все ще не існує чіткого визначення поняття комп'ютерного злочину, а ті які є, не відповідають реаліям сьогодення. Складність у формулюваннях цих понять існує як унаслідок неможливості виділення єдиного об'єкта злочинного посягання, так і з причин множинності предметів злочинного посягання з точки зору їх кримінально-правового значення.

Аналізуючи наукові дослідження і публікації вітчизняних та зарубіжних фахівців з визначеного кола проблем, можна зробити узагальнюючий висновок про те, що нині існують дві основні течії наукової думки. Одні дослідники відносять до комп'ютерних злочинів дії, у яких комп'ютер є або об'єктом, або знаряддям посягання. При цьому, зокрема, крадіжка самих комп'ютерів розглядається як один із способів скоєння комп'ютерних злочинів. Інші дослідники – тільки протизаконні дії у сфері автоматизованої обробки інформації. Вони виділяють це як головну класифікуючу ознаку, що дозволяє віднести ці злочини у відособлену групу, на підставі спільності засобів, знарядь, об'єктів посягання. Законодавство багатьох країн, у тому числі й України, стало розвиватися саме у цьому напрямі.

Як відомо, кримінальне право виходить з матеріального, правового визначення поняття злочину, тобто суть будь-якого злочину полягає в тому, що воно змінює, порушує конкретне суспільне відношення, що являє собою певний зв'язок людей з приводу матеріальних, соціальних та ідеологічних цінностей, які охороняються кримінально-правовими нормами.

У кримінальному праві під предметом злочину мають на увазі всі матеріальні предмети зовнішнього світу, на які безпосередньо спрямовані дії зловмисника при посяганні на об'єкт. Таким чином, предметом злочинного посягання є об'єкт (або елемент об'єкта), впливаючи на який злочинець порушує або намагається порушити конкретне суспільне правовідношення.

В інформаційних правовідношеннях об'єктом злочинного посягання є тільки інформація, а дії злочинця потрібно розгляда-

ти як замах на інформаційні правовідносини у суспільстві. Необхідно враховувати, що якщо інформація є не об'єктом, а засобом замаху на інший об'єкт, то слід зробити диференціацію в тому, чи була інформація продуктом обробки комп'ютерної техніки, або вона мала інший, "некомп'ютерний" зміст. Інформація, оброблена комп'ютерною технікою, - це інформація, яка обертається в обчислювальній системі, зафіксована на фізичному носії, або яка передається по телекомунікаційним каналах: сформована в обчислювальній системі та пересилається за допомогою електромагнітних сигналів з одного комп'ютера на інший, або периферійний пристрій. У першому випадку злочин необхідно відносити до категорії комп'ютерних злочинів, у другому – до категорії тих видів злочинних діянь, які, власне, і визначені в кримінальному кодексі. Поняття термінів "комп'ютерна злочинність" і "комп'ютерний злочин" значно ширше за поняття навмисного втручання у роботу автоматизованих систем, яке виділене в ст. 198-1 Кримінального кодексу України. Нині діючий Кримінальний кодекс України передбачає відповідальність за порушення роботи автоматизованих систем (ст. 198-1, ч.1), а саме "навмисне 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 перекручування або знищення інформації чи то носіїв інформації, – карається позбавленням волі на строк до двох років, або виправними роботами на той же строк, або штрафом у розмірі від ста до двохсот мінімальних розмірів заробітної плати". Частина 2 ст. 198-1 передбачає таку відповідальність: спричинення шкоди у великих розмірах; вчинення злочину повторно або за попередньою змовою групою осіб – караються позбавленням волі на строк від двох до п'яти років.

На наш погляд, треба доповнити чи внести зміни в ст. 198-1 Кримінального кодексу України, де передбачити відповідальність за злочини у сфері застосування автоматизованих електронно-обчислювальних систем. Це дії, які пов'язані з порушенням роботи електронно-обчислювальних машин, незаконним проникненням у комп'ютерні мережі, викраденням, привласнен-

ням або вимаганням комп'ютерної інформації шляхом шахрайства тощо.

Вивчаючи закордонний досвід та виходячи з термінології, що застосовується в розвинутих країнах відносно комп'ютерної злочинності, а також розглядаючи склад злочинів, до проекту Кримінального кодексу України вбачається доцільним внести розділ "Комп'ютерні злочини".

У Законі "Про захист інформації в автоматизованих системах" від 05 липня 1994 року були встановлені основи регулювання правових відносин щодо захисту інформації в автоматизованих системах за умовами дотримання права власності громадян України і юридичних осіб на інформацію та права доступу до неї, права власника інформації на її захист. У розділі п'ятому визначена відповідальність за порушення закону про захист інформації. Особи, винні в порушені порядку і правил захисту оброблюваної в автоматизованій системі інформації, несуть дисциплінарну, адміністративну та кримінальну відповідальність згідно з чинним законодавством України.

На нашу думку, під комп'ютерним злочином з кримінально-правової точки зору треба розуміти передбачені кримінальним законом суспільно небезпечні дії, в яких об'єктом злочину є інформація, оброблена автоматизованою системою. У даному випадку як предмет або знаряддя злочину буде виступати машинна інформація, комп'ютер, комп'ютерна система або комп'ютерна мережа. При цьому слід враховувати одну особливість – комп'ютер у злочинах може виступати одночасно як предмет і як знаряддя скоєння злочину. Таким чином, під комп'ютерним злочином потрібно розуміти передбачені кримінальним законом суспільно небезпечні дії, скоєні з використанням засобів електронно-обчислювальної (комп'ютерної) техніки. При цьому як основна класифікуюча ознака приналежності злочину до розряду комп'ютерних нами виділяється поняття "використання засобів комп'ютерної техніки", незалежно від того, на якій стадії злочину вона використовувалася: при його підготовці, в ході скоєння або для приховання злочину. Для обґрунтування цього ствердження більш детально розглянемо його складові.

Перша частина визначення, на наш погляд, не вимагає особливих пояснень і залежить лише від того, як будуть кваліфікуватися ті або інші суспільно небезпечні дії згідно з формулюванням кримінального закону. Наприклад, шпигунство з використанням засобів комп'ютерної техніки буде називатися комп'ютерним шпигунством і відноситься криміналістичною наукою до комп'ютерних злочинів (тоді як в кримінально-правовому плані цей злочин буде віднесений до розряду державних злочинів), аналогічно: фальсифікація, комп'ютерна фальсифікація, шахрайство, комп'ютерне шахрайство, розкрадання, комп'ютерне розкрадання, зловживання, комп'ютерне зловживання тощо. Подібні поняття дуже часто вживаються в зарубіжній юридичній практиці при кваліфікації тих або інших комп'ютерних правопорушень. Тому, на нашу думку, можливе використання даної термінології у вітчизняній практиці для позначення схожих за своїм змістом злочинних діянь для виділення їх криміналістичної специфіки. Друга ж частина визначення вимагає, на наш погляд, серйозних пояснень і докладної деталізації.

Наприклад: засоби комп'ютерної техніки за своїм функціональним призначенням представляється можливим поділити на дві основні групи: апаратні засоби (hardware) та програмні засоби (software). Під апаратним засобами комп'ютерної техніки розуміють технічні засоби, що використовуються для обробки даних: механічне, електричне та електронне обладнання для обробки інформації. До них відносяться: персональний комп'ютер – комплекс технічних засобів, призначених для автоматизованої обробки інформації у процесі рішення обчислювальних і інформаційних задач; периферійне обладнання – обладнання, що має підлеглий кібернетичний статус в інформаційній системі: між процесором і користувачем відносно певного центрального процесора; комплекс зовнішніх пристроїв електронно-обчислювальної машини, що не знаходяться під безпосереднім управлінням центрального процесора; фізичні носії машинної інформації.

Програмне забезпечення – сукупність управляючих і обробляючих програм, призначених для планування і організації обчислювального процесу, автоматизації програмування і відладки прикладних задач, що складається з системних програм

(операційні системи, програми технічного обслуговування: драйвери, програми-оболонки, допоміжні програми); прикладних програм (спеціалізованих програм), призначених для вирішення певного класу задач, наприклад, редактори текстів, антивірусні програми, програми захисту від несанкціонованого доступу, табличні процесори, СУБД, графічні редактори, системи ділової і наукової графіки, системи автоматизованого проектування, інтегровані системи, бухгалтерські програми, програми управління технологічними процесами, автоматизовані робочі місця (АРМ), бібліотеки стандартних програм тощо; інструментальних програм (систем програмування), що складаються з мов програмування: Pascal, Microsoft C, Microsoft Basic, Java, Clipper та інші.

Наведене структурування засобів комп'ютерної техніки приводиться нами насамперед для більш чіткого розуміння суті засобів скоєння комп'ютерних злочинів, що розглядаються, предметів та знарядь злочинного посягання, а також для усунення розбіжностей з приводу їх термінології, що мають місце в практичній діяльності органів внутрішніх справ. Наприклад, коли предметом посягання є комп'ютер, то необхідно розглядати його як систему і провести відмінність між його частинами. Адже комп'ютер у вузькому значенні цього слова є просто процесор, реалізований на базі інтегральних мікросхем, але наприкінці він ніколи в основному не використовується самостійно, а тільки в поєднанні з периферійними пристроями, нерідко пов'язаними в єдину мережу, яка може включати в себе й інші комп'ютери та комп'ютерні системи. Програмні засоби можна розглядати і як частину комп'ютерної системи, і як самостійний предмет, для якого комп'ютер є навколишнім (периферійним) середовищем. Цей факт, на наш погляд, повинен встановлюватися програмно-технічною експертизою, виходячи з кожного конкретного випадку.

Аналіз численних випадків впливу на інформацію і несанкціонованого доступу до неї доводить, що їх можна розділити на випадкові і навмисні. Навмисні загрози можуть бути виконані шляхом довготривалого втручання несанкціонованими запитами або вірусами. Це може привести до руйнування чи втрати інформації, її модифікації чи ознайомлення з нею сторонніх. Попередження таких наслідків в автоматизованій системі і є основною метою створення системи безпеки інформації.

До випадкових впливів при експлуатації автоматизованої системи можна віднести:

– перешкоди на лініях зв'язку від впливу зовнішнього середовища;

– відмови і збої апаратури;

– помилки людини як ланки системи;

– схемні та системотехнічні помилки розробників;

– структурні, алгоритмічні і програмні помилки;

– аварійні ситуації;

– інші впливи.

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 застосовуються в інформаційних процесах, виражений в їх подвійності: як предмет, і як засіб скоєння таких злочинів.

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

Існуючі способи скоєння комп'ютерних злочинів можна класифікувати на чотири основні групи:

– *перехоплення інформації;*

– *несанкціонований доступ до засобів комп'ютерної техніки;*

– *маніпуляція даними та командами;*

– *комплексні способи.*

Головною класифікуючою ознакою виступає метод використання злочинцем інших дій, спрямованих на отримання доступу до засобів комп'ютерної техніки з різними намірами.

До першої групи можна віднести способи скоєння комп'ютерних злочинів, засновані на діях злочинця, що спрямовані на отримання даних та машинної інформації за допомогою використання методів аудіовізуального та електромагнітного перехоплення, широко впроваджених в оперативно-розшукову діяльність правоохоронних органів.

Безпосередні перехоплення здійснюються за допомогою прямого підключення до телекомунікаційного обладнання комп'ютера, комп'ютерної системи або мережі, наприклад, принтера або телефону, що використовуються для передачі даних та сигналів комп'ютерної техніки безпосередньо або через відповідний порт персонального комп'ютера. У зв'язку з цим розрізнюють:

– форсоване перехоплення – перехоплення повідомлень, що направляються робочим станціям (ЕОМ), які мають неполадки в обладнанні або каналах зв'язку;

– перехоплення символів, які набираються користувачем на клавіатурі ЕОМ;

– перехоплення повідомлень – несанкціоноване підключення до лінії зв'язку, прийом повідомлень, які циркулюють між сервером та робочими станціями.

Електромагнітне перехоплення полягає в тому, що не всі перехоплюючі пристрої необхідно підключати до системи. Дані та інформація можуть бути перехоплені не тільки в каналах зв'язку, але і з приміщень, в яких знаходяться засоби комунікацій.

Аудіоперехоплення або зняття інформації по віброакустичному каналу є найбільш небезпечним і досить поширеним. Захист інформації від аудіоперехоплення дуже складний.

Відеоперехоплення – це дії злочинця, спрямовані на отримання необхідних даних та інформації шляхом використання різної відеооптичної техніки.

"Прибирання сміття" полягає у використанні злочинцем технологічних відходів інформаційного процесу, залишених користувачем після роботи з комп'ютерною технікою. Він здійснюється в двох формах: фізичній та електронній. Зазначимо, що

в цій та інших групах засоби комп'ютерної техніки будуть виступати і як знаряддя скоєння злочинів.

До другої групи скоєння комп'ютерних злочинів ми відносимо дії, спрямовані на отримання несанкціонованого доступу до комп'ютерної техніки.

Спосіб ***"за дурнем"*** часто використовується злочинцями для проникнення в такі заборонні зони, як виробничі приміщення, інформаційні системи.

Спосіб перехоплення інформації ***"за хвіст"*** полягає в тому, що злочинець підключається до лінії зв'язку законного користувача (з використанням засобів комп'ютерного зв'язку) і терпляче чекає сигналу про закінчення роботи, перехоплює його, а потім, коли законний користувач виходить з активного режиму, здійснює доступ до системи.

Подібні властивості мають телефонні апарати з функцією утримання номера абонента, якого викликали.

"Комп'ютерний абордаж" здійснюється злочинцем шляхом випадкового підбору (або заздалегідь здобутого) абонентського номера комп'ютерної системи з використанням, наприклад, звичайного телефонного апарату.

Розглянемо найбільш відомі способи скоєння комп'ютерних злочинів, які використовуються злочинцями ***та відносяться до групи методів маніпуляції даними та керуючими командами засобів комп'ютерної техніки.***

"Підміна даних" – найбільш простий і тому дуже часто застосовуваний спосіб скоєння злочину. Дії злочинців у цьому випадку спрямовані на зміну або введення нових даних, які здійснюються, як правило, при введенні-виведенні інформації. Зокрема, даний спосіб скоєння злочину застосовується для модифікації даних в автоматизованій системі банківських операцій, що призводить до появи в системі сум, які реально на даний рахунок не зараховувалися.

"Троянський кінь" – це спосіб, що полягає в таємному введенні в чуже програмне забезпечення спеціально створеної програми, яка, потрапляючи в інформаційно-обчислювальну систему, починає виконувати нові, не заплановані розробником дії, з одночасним збереженням працездатності основної програми (комп'ютерні віруси).

Питаннями наукового вивчення комп'ютерних вірусів у наш час займається спеціально створена нова наука – комп'ютерна вірусологія. З погляду цієї науки ***всі програми-віруси поділяються на дві групи***:

а) за способом зараження засобів комп'ютерної техніки: ***резидентні і нерезидентні***;

б) за алгоритмом їх побудови і виявлення: ***"вульгарний вірус" і "роздроблений вірус"***.

Спосіб скоєння злочину ***"асинхронна атака"*** дуже складний і вимагає хорошого знання операційної системи.

Залежно від завдань, що вирішуються, використовують ті або інші операційні системи. Організація останніх настільки складна, що їх розробкою займаються авторські колективи професійних програмістів іноді протягом кількох років. Тому такі складні програмні продукти практично неможливо перевірити на предмет достовірності роботи та логічної досконалості. Інакше кажучи, особливості функціонування операційної системи за всіх умов залишаються невідомими. Цим і користуються злочинці при організації "асинхронних атак".

Для скоєння комп'ютерних злочинів усе більш характерним стали використання злочинцем способу ***комп'ютерного моделювання:*** моделювання поведінки пристрою або системи за допомогою програмного забезпечення. Моделюються як процеси, в які злочинці втручаються, так і плановані способи скоєння злочину. Наприклад, останнім часом злочинці з метою відходу від оподаткування все частіше починають використовувати так звану "чорну", або "подвійну бухгалтерію", засновану на існуванні двох одночасно працюючих програм автоматизованого бухгалтерського обліку. У даному випадку одна з них функціонує в легальному (законному) режимі, а інша - в нелегальному для проведення незаконних (тіньових) бухгалтерських операцій.

Моделювання в кримінальних цілях, на нашу думку, буде поширюватися по мірі зниження вартості персональних комп'ютерів і збільшення кількості моделюючих програмних засобів. Так, у вільному продажу з'явилися спеціальні системи моделювання GPSS та аналогічні, які дозволяють створювати повноцінні програмні продукти користувача, у тому числі і для кримінальних цілей.

Спосіб ***подолання програмних засобів захисту***. є допоміжним і призначений для підготовки скоєння комп'ютерного злочину способами, розглянутими нами вище. Він полягає в діях злочинця, спрямованих на умисне подолання програмних засобів захисту комп'ютерної техніки і має кілька різновидів.

Незаконне створення ключової дискети є одним із способів подолання засобів захисту комп'ютерної техніки. Здійснюється злочинцем шляхом перенесення всієї структури й інформації, розташованої на ключовій дискеті-оригіналі, захищеній від копіювання програмними засобами, на дискету-копію. Для отримання працездатної дискети-копії достатньо повторення дискети-оригіналу з усіма характеристиками, які перевіряються системою захисту. Вибір правильного методу їх копіювання є головним завданням, яке вирішується злочинцем у даному випадку.

Вирішення у цьому випадку завдань для кожної системи захисту вимагає певного професійного досвіду. Ці завдання можуть бути вирішені тільки двома способами: програмним та програмно-апаратним.

До четвертої та останньої групи способів скоєння комп'ютерних злочинів ми відносимо комплексні способи, під якими розуміють використання злочинцем двох та більше способів. а також їх різні комбінації при скоєнні злочину. Ці способи ми детально розглянули в перших трьох групах. Деякі з них виявляються допоміжними, такими, які працюють на основний спосіб, виходячи з конкретної злочинної мети та ситуації.

---

[1] *Матеріали* Комісії ООН з попередження злочинності та кримінального правосуддя. – Відень, 13-23 квітня, E/CN. 15/1993/3.