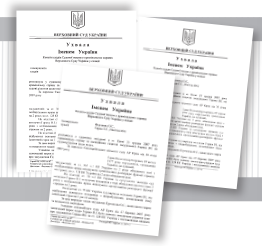

Судова практика розгляду справ про злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), автоматизованих систем та комп'ютерних мереж і мереж електрозв'язку

На сучасному етапі розвитку суспільство стає все більше залежним від роботи комп'ютерних систем для автоматичної обробки інформації. Це стосується різних сфер діяльності людини. Усі найважливіші функції, так чи інакше, здійснюються з використанням комп'ютерів, автоматизованих систем (далі — АС) та комп'ютерних мереж і мереж електрозв'язку.

Завдяки удосконаленню комп'ютерних систем з'являються нові можливості для вчинення невідомих раніше правопорушень, а також традиційних злочинів новими засобами. Останнім часом в Україні наявна стійка тенденція до збільшення кількості злочинів, учинених у сфері використання електронно-обчислювальних машин (комп'ютерів; далі — ЕОМ), АС та комп'ютерних мереж і мереж електрозв'язку (комп'ютерних злочинів).

Комп'ютерна злочинність — це особливий вид злочинів, пов'язаних із незаконним використанням сучасних інформаційних технологій і засобів комп'ютерної техніки. В їх основі можуть бути політичні, хуліганські, корисливі й інші мотиви. Це зумовлює необхідність розвитку й удосконалення правових засобів регулювання суспільних відносин у сфері інформаційної діяльності. Інформаційні відносини, тобто відносини, що виникають при одержанні, використанні, поширенні та зберіганні інформації, регулюються положеннями Конституції України, законами від 2 жовтня 1992 р. № 2657-XII «Про інформацію», від 25 червня 1993 р. № 3322-XII «Про науково-технічну інформацію», від 18 листопада 2003 р. № 1280-IV «Про телекомунікації», від 5 липня 1994 р. № 80/94-ВР «Про захист інформації в інформаційно-телекомунікаційних системах» (в редакції Закону від 31 травня 2005 р. № 2594-IV), а також низкою підзаконних актів, зокрема Положенням про технічний захист інформації в Україні (затверджене Указом Президента України від 27 вересня 1999 р. № 1229/99) та ін.

Згідно з чинним законодавством України кримінальну відповідальність за злочини у сфері використання ЕОМ, АС та комп'ютерних мереж і мереж електрозв'язку передбачено у розд. XVI Кримінального кодексу України (далі — КК).

Аналіз статистичних даних

За даними Державної судової адміністрації України (далі — ДСА), на розгляді в місцевих та апеляційних судах у 2008 р. перебувало 156 [138] [1] кримінальних справ про злочини, відповідальність за які передбачено статтями 361—363[1] КК; це на 13 % більше, ніж у 2007 р. Усього за 2008 р. було розглянуто 112 [114] справ, що на 1,8 % менше, із них з постановленням вироку — 60 [65] справ, або 53,6 % [57 %] від кількості розглянутих.

Відповідно до вироків, що набрали законної сили, у 2008 р. було засуджено за статтями 361—363[1] КК 57 [60] осіб, що на 5 % менше, ніж у 2007 р. Із них за ст. 361 КК — 43 особи, або 75,4 % від кількості осіб, засуджених за ці злочини; за ст. 361[1] КК — три особи, або 5,3 %; за ст. 361[2] КК — чотири особи, або 7 %; за ст. 362 КК — сім осіб, або 12,3 %. У 2007 р. дані щодо засуджених за статтями 361—363[1] КК у статистичних звітах ДСА постатейно не виділялися.

Найчастіше злочини, відповідальність за які передбачена у статтях 361—363[1] КК, вчиняли особи у віці: від 30 до 50 років — 23 особи [20], або 40,4 % [33,3 %] від кількості осіб, засуджених за ці злочини; від 18 до 25 років — 18 осіб [31], або 31,6 % [51,7 %]; від 25 до 30 років — 11 осіб [7], або 19,3 % [11,7 %]; від 50 до 65 років — п'ять осіб [2], або 8,8 % [3,3 %].

До позбавлення волі засуджено всього дві особи [5], або 3,5 % [8,3 %] від кількості осіб, засуджених за ці злочини. Із них одну особу засуджено за ч. 2 ст. 361 КК та одну особу — за ч. 1 ст. 361[2] КК.

Штраф застосовано до 16 [13] осіб, або 28,1 % [21,7 %] від кількості засуджених за ці злочини, що на 23,1 % більше, ніж у 2007 р., у тому числі за ст. 361 КК — до 13 осіб, за ст. 361[1] КК — до однієї особи, за ст. 361[2] КК — до однієї особи; за ст. 362 КК

* Узагальнення опрацьовано суддею Верховного Суду України М.І. ГРИЦІВИМ та головним консультантом управління вивчення та узагальнення судової практики Верховного Суду України В.В. АНТОЩУКОМ.

[1] Тут і далі в квадратних дужках наведено дані за 2007 р.

також застосовано штраф до однієї особи. За ст. 361 КК засуджено одну особу, до якої застосовано інші види покарання.

Звільнено від покарання з випробуванням 38 [37] осіб, або 66,7 % [61,7 %] від кількості засуджених за ці злочини, що на 2,7 % більше, ніж у 2007 р.

Кількість осіб, щодо яких справи за статтями 361—363[1] КК закрито, становить 35 [35], тобто така ж, як 2007 р. Кількість осіб, справи щодо яких закрито у зв'язку: з дійовим каяттям — 8 [6] осіб; з примиренням винного з потерпілим (за ст. 361 КК) — одна особа; зі зміною обстановки — 11 [9] осіб; з передачею особи на поруки — вісім осіб [3]; з амністією — сім [15] осіб, або 20 % [42,9 %].

Судовий розгляд справ про злочини у сфері використання ЕОМ (комп'ютерів), АС та комп'ютерних мереж чи мереж електрозв'язку

В Україні найбільш поширеним злочином у сфері використання ЕОМ, АС та комп'ютерних мереж і мереж електрозв'язку є злочин, відповідальність за який передбачено ст. 361 КК («Несанкціоноване втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку»). У цій статті передбачено відповідальність за несанкціоноване втручання в роботу ЕОМ, АС, комп'ютерних мереж чи мереж електрозв'язку, що призвело до витоку, втрати, підроблення, блокування інформації, спотворення процесу автоматичної обробки інформації або до порушення встановленого порядку її маршрутизації.

Об'єктом такого злочину є ЕОМ, АС, комп'ютерні мережі та мережі електрозв'язку. Об'єктом такого злочину також може бути право власності на комп'ютерну інформацію.

Для визнання факту вчинення злочину, склад якого передбачено у ст. 361 КК, суд має встановити не лише вчинення діяння, а й настання хоча б одного із зазначених в законі наслідків: витоку, втрати, підроблення, блокування інформації, спотворення процесу її обробки або порушення встановленого порядку її маршрутизації. Тобто між несанкціонованим втручанням в роботу ЕОМ, АС, комп'ютерних мереж чи мереж електрозв'язку має бути причинний зв'язок хоча б з одним із суспільно небезпечних наслідків.

Специфіка розгляду справ цієї категорії полягає у правильному розумінні термінів, визначення яких містяться у наведених вище нормативних документах.

ЕОМ розуміється як комплекс електронних технічних засобів, побудованих на основі мікропроцесорів і призначених для автоматичної обробки інформації при вирішенні обчислювальних та інформаційних завдань.

АС — це організаційно-технічні системи, в яких реалізується технологія обробки інформації з використанням технічних і програмних засобів. Зокрема, такими системами слід вважати сукупність ЕОМ, засобів зв'язку та програм, за допомогою яких ведеться документообіг, формуються, оновлюються та використовуються бази даних, накопичується та обробляється інформація. Оскільки обробка певних даних можлива і в результаті роботи одного комп'ютера, то АС — це й окремо взятий комп'ютер разом з його програмним забезпеченням.

Комп'ютерна мережа — це сукупність програмних і технічних засобів, за допомогою яких забезпечується можливість доступу з однієї ЕОМ до програмних чи технічних засобів інших ЕОМ та до інформації, що зберігається у системі іншої ЕОМ.

Мережа електрозв'язку — комплекс технічних засобів телекомунікацій та споруд, призначених для маршрутизації, комутації, передавання та/або приймання знаків, сигналів, письмового тексту, зображень та звуків або повідомлень будь-якого роду по радіо, проводових, оптичних чи інших електромагнітних системах між кінцевим обладнанням.

Об'єктивна сторона злочину проявляється у формі несанкціонованого втручання в роботу ЕОМ, їх систем, комп'ютерних мереж чи мереж електрозв'язку, наслідком якого є: 1) витік; 2) втрата; 3) підроблення; 4) блокування інформації; 5) спотворення процесу автоматичної обробки інформації; 6) порушення встановленого порядку її маршрутизації.

Несанкціоноване втручання в роботу ЕОМ, їх систем чи комп'ютерних мереж — це проникнення до цих машин, їх систем чи мереж і вчинення дій, які змінюють режим роботи машин, їх систем чи комп'ютерних мереж або повністю чи частково припиняють їх роботу без дозволу відповідного власника або уповноваженої особи.

Несанкціонованим втручанням в роботу мереж електрозв'язку слід вважати будь-які (окрім втручання в роботу ЕОМ, їх систем чи комп'ютерних мереж, що забезпечують роботу мереж електрозв'язку) вчинені без згоди власника відповідної мережі чи службових осіб, на яких покладено забезпечення її нормальної роботи, дії, внаслідок яких припиняється (зупиняється) робота мережі електрозв'язку або відбуваються зміни режиму цієї роботи.

Комп'ютерна інформація — це текстова, графічна чи будь-яка інша інформація (дані), яка існує в електронному вигляді, зберігається на відповідних носіях і може бути створена, змінена чи використана за допомогою ЕОМ.

Способи несанкціонованого втручання (проникнення) в роботу зазначених систем і мереж у судовій практиці трапляються різні. Як засвідчили матеріали узагальнення, найчастіше вчинення дій, передбачених ст. 361 КК, відбувається з метою безкоштовного доступу до мережі Інтернет.

Наприклад, Сєвєродонецький міський суд Луганської області вироком від 7 червня 2007 р. визнав Г. винним у тому, що він, маючи достатні технічні навики роботи на комп'ютері, використовуючи

останній, не санкціоновано, без дозволу провайдера ТОВ «HomeLAN» втручався в роботу його мережі під чужими мережевими реквізитами. Таке несанкціоноване втручання в роботу комп'ютерних мереж призводило до блокування надходження інформації до офіційних користувачів, унеможливлюючи їм доступ до цих мереж, вносило викривлення в процес обробки інформації, порушувало порядок її маршрутизації.

Дії Г. суд кваліфікував за ч. 1 ст. 361 КК і призначив йому відповідне покарання.

У ч. 2 ст. 361 КК передбачено відповідальність за такі ж самі дії, що й у ч. 1 цієї статті, вчинені повторно або за попередньою змовою групою осіб, або якщо вони заподіяли значну шкоду.

Оскільки вчинення цього злочину за попередньою змовою групою осіб є кваліфікуючою ознакою для ч. 2 ст. 361 КК, то в разі його вчинення за таких обставин дії винних осіб не потребують додаткової кваліфікації за ст. 28 КК. Проте в деяких випадках суди допускали помилки при кваліфікації зазначених дій.

Так, Хмельницький міськрайонний суд Хмельницької області визнав Г. та С. винними за ч. 2 ст. 28, ч. 2 ст. 361 КК і призначив їм відповідне покарання. Г. та С. вироком суду визнано винними у тому, що вони, діючи за попередньою змовою між собою, шляхом несанкціонованого втручання в роботу мереж електрозв'язку порушили встановлений порядок маршрутизації міжнародних телефонних дзвінків.

Міськрайонний суд помилково кваліфікував дії цих засуджених за ч. 2 ст. 28 КК. Виправляючи помилку, Апеляційний суд Хмельницької області ухвалою від 26 грудня 2006 р. змінив вирок суду першої інстанції, виключивши з їх обвинувачення ч. 2 ст. 28 КК.

Згідно з приміткою до ст. 361 КК, шкода у статтях 361—363[1] КК вважається значною, якщо вона полягає у заподіянні матеріальних збитків, що в 100 і більше разів перевищують неоподатковуваний мінімум доходів громадян. Таким чином, значна шкода може мати і нематеріальний характер. У разі вчинення діянь, передбачених статтями 361—363[1] КК, нематеріальна шкода може полягати у тимчасовому зупиненні (припиненні) роботи або іншому порушенні нормального режиму роботи певного підприємства, організації, установи, їх окремих структурних підрозділів, підриві ділової репутації громадянина чи юридичної особи, заподіянні громадянину моральної шкоди внаслідок втрати, незаконного поширення чи витоку інформації, яка є результатом його наукової чи творчої діяльності, тощо. Значна шкода нематеріального характеру є оціночним поняттям. Отже, питання про те, чи слід визнавати таку шкоду значною, вирішують органи досудового слідства, прокурор або суд з урахуванням конкретних обставин справи.

Матеріали узагальнення свідчать, що збільшилась кількість випадків, коли несанкціоноване втручання в роботу ЕОМ, АС, комп'ютерних мереж здійснювалося з корисливих мотивів з метою викрадення чи заволодіння чужим майном із заподіянням потерпілим матеріальної шкоди і було способом вчинення таких злочинів проти власності, як шахрайство (ст. 190 КК) або привласнення чи заволодіння майном шляхом зловживання службовим становищем (ст. 191 КК). У більшості випадків суди кваліфікували такі дії за сукупністю злочинів: за ст. 361 КК і тією статтею, в якій передбачено відповідальність за конкретний злочин проти власності, способом здійснення якого було несанкціоноване втручання в роботу ЕОМ, АС, комп'ютерних мереж і мереж електрозв'язку.

Наприклад, Печерський районний суд м. Києва вироком від 12 лютого 2007 р. визнав М. винним у тому, що він, працюючи провідним інженером відділу пластикових карток акціонерного комерційного «Промислово-фінансового банку», як службова особа, що виконує адміністративно-господарські функції, в 2006 р., зловживаючи своїм службовим становищем, маючи доступ до бази даних про клієнтів та їхні рахунки, що містилась у його робочому комп'ютері, діючи з метою заволодіння грошовими коштами, виконав операцію з персоналізації сторонньої картки, скопіювавши на неї інформацію одного з клієнтів банку. З використанням картки-дубліката та банкоматів М. зняв і привласнив готівкою з рахунку клієнта грошові кошти на загальну суму 65 тис. 900 грн. Зазначені дії М. суд кваліфікував за ч. 4 ст. 191 КК як заволодіння чужим майном шляхом зловживання службовим становищем, вчинене у великих розмірах.

Крім того, суд правильно кваліфікував дії М. ще й за сукупністю злочинів, склад яких передбачено ч. 3 ст. 362 КК, оскільки М., будучи особою, яка мала право доступу до інформації, що оброблялася на комп'ютерах та зберігалася на носіях, несанкціоновано її скопіював, що призвело до витоку інформації і заподіяло значну шкоду.

Проте в деяких випадках суди кваліфікували зазначені дії лише за тими статтями КК, в яких передбачено відповідальність за вчинення комп'ютерних злочинів.

Так, Красногвардійський районний суд м. Дніпропетровська вироком від 4 грудня 2006 р. визнав Є. винним за ч. 1 ст. 361 КК і призначив йому відповідне покарання. З матеріалів справи вбачається, що Є., діючи з корисливих мотивів, за допомогою спеціальних комп'ютерних програм створив дублікат-макет сайту компанії, яка спільно із закритим акціонерним товариством комерційним банком «ПриватБанк» (далі — ЗАТ КБ «ПриватБанк») надавала послуги з прискореного перерахування платежів за комунальні послуги і мобільний зв'язок через мережу Інтернет. У результаті такої діяльності Є. протягом певного часу викрадав грошові кошти з рахунків клієнтів ЗАТ КБ «ПриватБанк».

Оскільки Є. шляхом обману неодноразово заволодівав грошовими коштами за допомогою незаконних операцій з використанням ЕОМ, а втручання

в роботу ЕОМ є способом вчинення злочину проти власності, то в цьому випадку зазначені дії потребують додаткової кваліфікації ще й за ст. 190 КК (шахрайство).

Вивчення справ про комп'ютерні злочини показало, що значна кількість їх пов'язана із несанкціонованим втручанням в роботу мереж електрозв'язку шляхом використання емуляторів — телефонних карток, що дають змогу безкоштовно здійснювати з таксофонних автоматів дзвінки в будь-якому напрямку, у тому числі за межі України. Такі дії завдають значних збитків телекомунікаційним компаніям, за рахунок яких здійснюються дзвінки у віддалені регіони; при цьому вчинювані телефонні виклики, як правило, не прослідковуються, і за них компанія не в змозі виставити рахунок користувачеві.

Наприклад, Центральний районний суд м. Сімферополя вироком від 20 вересня 2006 р. визнав С. винним за ч. 2 ст. 361 КК і призначив йому відповідне покарання. З матеріалів справи вбачається, що С., діючи повторно, з метою отримання матеріальної вигоди для здійснення безкоштовних дзвінків придбав емулятор таксофонної картки із впаяним у нього запрограмованим чіпом. Використовуючи зазначений емулятор, С. надавав послуги міжміського та міжнародного телефонного зв'язку стороннім особам, а кошти, одержані за ці послуги, привласнював. Таким чином, було здійснено 1 тис. 177 незаконних безоплатних телефонних дзвінків, у тому числі й за кордон, та завдано збитків відкритому акціонерному товариству «Укртелеком» (далі — ВАТ «Укртелеком») на суму 11 тис. 980 грн.

Згідно з висновком судово-технічної експертизи, вилучений у С. технічний пристрій є емулятором телефонної картки для несанкціонованого доступу до послуг ВАТ «Укртелеком». Емулятор таксофонної картки був виготовлений шляхом видалення електронного модуля із пластикової картки і встановлення на це місце мікропроцесора, в якому записано програмне забезпечення, що емулює роботу електронної картки.

У цьому випадку грошові кошти у вигляді оплати за міжміські та міжнародні розмови, які мали б надійти в розпорядження власника телефонної мережі, отримував зловмисник, тому ця грошова сума є неодержаним прибутком власника. Неодержаний прибуток є предметом злочину ст. 192 КК (заподіяння майнової шкоди шляхом обману або зловживання довірою). Отже, дії С. слід було б додатково кваліфікувати ще й за ч. 1 ст. 192 КК.

Створення з метою використання, розповсюдження або збуту, а також розповсюдження або збут шкідливих програмних чи технічних засобів, призначених для несанкціонованого втручання в роботу ЕОМ, АС, комп'ютерних мереж чи мереж електрозв'язку, тягне відповідальність за ст. 361[1] КК. Як предмет цього злочину комп'ютерні програми (програмні засоби) мають бути шкідливими, тобто здатними забезпечити несанкціонований доступ до інформації, а також змінити, знищити, пошкодити, заблокувати інформацію — комп'ютерну чи ту, яка передається мережами електрозв'язку. Різновидом шкідливих комп'ютерних програм є комп'ютерні віруси [2]. Їх призначення — несанкціоноване втручання в роботу ЕОМ, АС, комп'ютерних мереж чи мереж електрозв'язку. Зазначений злочин (ч. 1 ст. 361[1] КК) має формальний склад, і для наявності його об'єктивної сторони не потрібне настання суспільно небезпечних наслідків.

Так, Дрогобицький міськрайонний суд Львівської області вироком від 7 серпня 2006 р. призначив А. кримінальне покарання, в тому числі й за ч. 1 ст. 361[1] КК. З матеріалів справи вбачається, що А. з метою безкоштовного доступу до мережі Інтернет створив та використав шкідливу комп'ютерну програму, призначену для сканування мережі провайдера й отримання логінів та паролів, для модемного доступу до мережі Інтернет, які містилися на сервері провайдера. В подальшому А. незаконно використовував логіни та паролі для доступу до мережі Інтернет.

Несанкціоновані збут або розповсюдження інформації з обмеженим доступом, яка зберігається в ЕОМ, АС, комп'ютерних мережах або на носіях такої інформації, створеної та захищеної відповідно до вимог чинного законодавства, утворюють склад злочину, передбачений ст. 361[2] КК. Ознакою комп'ютерної ***інформації з обмеженим доступом*** є те, що вона повинна бути створена та захищена відповідно до положень чинного законодавства, зокрема положень відповідних законів чи підзаконних нормативно-правових актів, у яких регламентується порядок її створення і захисту.

Комп'ютерна інформація з обмеженим доступом може бути ***конфіденційною і таємною***, зокрема такою, що містить банківську чи комерційну таємницю.

Наприклад, Індустріальний районний суд м. Дніпропетровська вироком від 26 червня 2006 р. визнав Д. винним за ч. 1 ст. 361[2] КК і призначив йому відповідне покарання. З матеріалів справи вбачається, що Д. відповідно до своїх службових повноважень мав доступ до комп'ютерної інформації про наступну переоцінку товарів у мережі магазинів, що було комерційною таємницею підприємства, в якому він працював. Цю інформацію він через мережу Інтернет розповсюдив серед осіб, які не були співробітниками цього підприємства і не мали права доступу до неї.

У ст. 362 КК передбачено відповідальність за несанкціоновані дії з інформацією, яка оброблюється в ЕОМ, АС, комп'ютерних мережах або зберігається на носіях такої інформації, вчинені особою, яка має право доступу до неї.

Об'єктивна сторона такого злочину полягає у вчиненні щодо відповідної комп'ютерної інформації несанкціонованих: 1) зміни; 2) знищення; 3) блоку-

[2] Див.: Кримінальний кодекс України: Наук.-практ. коментар / За заг. ред. В.В. Сташиса, В.Я. Тація. — К., 2006. — С. 969.

вання; 4) перехоплення; 5) копіювання. У двох останніх випадках обов'язковим елементом об'єктивної сторони злочину є наслідки у вигляді витоку інформації.

Суб'єктом цього злочину може бути особа, яка має право доступу (на підставі трудових чи договірних правовідносин або з інших юридичних підстав) до комп'ютерної інформації чи носіїв такої інформації.

Суди при розгляді справ цієї категорії допускають помилки при кваліфікації дій винних осіб, які, маючи право доступу до комп'ютерної інформації, вчинювали щодо неї несанкціоновані дії.

Так, Заводський районний суд м. Миколаєва вироком від 14 березня 2007 р. визнав С. винним за ч. 1 ст. 361[1] та ч. 2 ст. 15, ч. 1 ст. 361 КК і призначив йому відповідне покарання. З матеріалів справи вбачається, що С., працюючи інженером супроводження програмного забезпечення відділення ЗАТ КБ «ПриватБанк», відповідно до своїх службових обов'язків через локальну мережу мав доступ до всіх ЕОМ відділення банку. С. був незадоволеним розміром заробітної плати, з помсти за це керівництву банку, використовуючи наданий йому комп'ютер, за допомогою локальної комп'ютерної мережі зайшов на сервер банку і з метою використання створив у ньому шкідливий програмний засіб. Маючи намір запустити його та знищити інформацію, що містилася в ЕОМ відділення банку, напередодні свого звільнення розмістив його в активному стані у каталогах операційної системи серверу банку. Але реалізувати до кінця свій умисел, спрямований на несанкціоноване втручання в роботу сервера, яке могло призвести до втрати інформації, не зміг, оскільки в день подання заяви про звільнення йому було відмовлено в допуску до робочого місця і сервера.

Районний суд, кваліфікуючи дії С. за ч. 2 ст. 15, ч. 1 ст. 361 КК, припустився помилки, оскільки С. як відповідальна за експлуатацію АС особа намагався умисно знищити інформацію, яка в них оброблялася. У цьому випадку його дії слід було кваліфікувати за ч. 2 ст. 15, ч. 1 ст. 362 КК.

За несанкціоноване перехоплення або копіювання інформації, яка оброблюється в ЕОМ, АС, комп'ютерних мережах або зберігається на носіях такої інформації, вчинене особою, яка має право доступу до такої інформації, якщо ці дії призвели до її витоку, настає відповідальність, передбачена ч. 2 ст. 362 КК.

Наприклад, Жовтневий районний суд м. Дніпропетровська вироком від 27 липня 2007 р. визнав С. винною за ч. 2 ст. 362 КК та призначив їй відповідне покарання. С., працюючи у відділенні ЗАТ КБ «ПриватБанк» спеціалістом відділу кредитування фізичних осіб і маючи доступ до бази даних клієнтів та їхніх рахунків, скопіювала інформацію, що стосувалася рахунку одного з клієнтів банку (трансфер та комп'ютерні паролі входу до рахунку). Використовуючи зазначену інформацію, С. через мережу Інтернет поповнювала рахунок свого мобільного телефону та сплачувала рахунки за комунальні послуги.

У випадках зміни, знищення, блокування інформації злочин вважається закінченим з моменту фактичної зміни, знищення чи блокування відповідної інформації, а в разі перехоплення чи копіювання інформації — з моменту настання наслідків, спеціально передбачених законом.

Проте деякі суди при відмежуванні закінченого складу цього злочину від замаху на його вчинення допускали помилки.

Наприклад, вироком Ленінського районного суду м. Миколаєва від 29 травня 2006 р. за ч. 2 ст. 15, ч. 2 ст. 362 КК засуджено П., який, працюючи спеціалістом технічної підтримки канадської компанії та маючи доступ до інформації, яка оброблялась і зберігалася в комп'ютерній мережі компанії, вчинив несанкціоноване копіювання трьох шаблонів сайтів, які продав за 30 доларів США, що призвело до витоку цієї інформації. В цьому випадку суд помилково кваліфікував дії П. як замах на вчинення злочину, передбаченого ч. 2 ст. 362 КК, хоча в результаті його дій зазначена інформація стала відомою та доступною стороннім особам, тобто наявний закінчений склад злочину.

Крім того, дії П. слід було додатково кваліфікувати за ч. 1 ст. 361[2] КК, оскільки він також здійснив несанкціонований збут інформації з обмеженим доступом.

Кримінальна відповідальність за порушення правил експлуатації ЕОМ, АС, комп'ютерних мереж чи мереж електрозв'язку або порядку чи правил захисту інформації, яка в них оброблюється (ст. 363 КК), настає, якщо цими діями заподіяно значну шкоду особою, яка відповідає за їх експлуатацію, за умови, що це спричинило викрадення, перекручення чи знищення комп'ютерної інформації, засобів їх захисту, або незаконне копіювання комп'ютерної інформації, чи істотне порушення роботи таких машин, їх систем чи комп'ютерних мереж.

Правилами експлуатації ЕОМ, АС, комп'ютерних мереж чи мереж електрозв'язку слід розуміти будь-які технічні правила, що регламентують порядок використання таких машин і автоматичної обробки в них інформації, а також забезпечення засобів захисту їх програмного забезпечення. У вироку суд має вказати, які конкретно правила були порушені винною особою. Саме ж порушення правил може бути як ***умисним***, так і ***необережним***. Між діями, що утворюють об'єктивну сторону цього злочину, і суспільно небезпечними наслідками має бути причинний зв'язок.

Порушення правил експлуатації ЕОМ, АС чи комп'ютерних мереж визнаються злочином лише в разі, коли їх наслідком було заподіяння значної шкоди, розмір якої визначено у примітці до ст. 361 КК. При цьому шкода, що береться до уваги при кваліфікації злочину, може стати значною як результат одного із допущених порушень або як сукупний результат усіх допущених порушень.

Суб'єкт зазначеного злочину спеціальний — особа, яка відповідає за експлуатацію ЕОМ, АС та комп'ютерних мереж.

Порушення правил експлуатації може виявлятися як в активних діях, коли особа вчинює дії всупереч розпорядженням, закріпленим у правилах, так і у формі бездіяльності — це невиконання або неналежне виконання обов'язків із технічного забезпечення захисту комп'ютерної інформації.

У ст. 363[1] КК передбачено відповідальність за умисне масове розповсюдження повідомлень електрозв'язку, здійснене без попередньої згоди адресатів, що призвело до порушення або припинення роботи ЕОМ, АС, комп'ютерних мереж чи мереж електрозв'язку. Засобом вчинення такого злочину є повідомлення електрозв'язку, які розповсюджуються через систему ЕОМ, АС, комп'ютерні мережі чи мережі електрозв'язку, в тому числі через мережу Інтернет. Суспільно небезпечними наслідками злочину, склад якого передбачено ст. 363[1] КК, є порушення або припинення роботи ЕОМ, АС, комп'ютерних мереж чи мереж електрозв'язку.

Розвиток мережі Інтернет призвів до того, що однією з основних проблем користувачів став надлишок інформації. Це стосується передусім так званого «спаму», тобто масового розповсюдження попередньо не обумовлених електронних листів. Через масовий характер спамових повідомлень останні утруднюють роботу інформаційних систем і ресурсів, створюючи для них зайве перевантаження, що може бути причиною їх виходу з ладу. «Спам» також може стати носієм шкідливих програм і комп'ютерних вірусів, поширених із метою отримання доступу до комп'ютерних систем, виведення їх із ладу або отримання конфіденційної інформації.

Однією з характерних особливостей цього виду злочинів є їхня латентність, яка спричинена небажанням користувачів мережі інформувати про такі злочини через недовіру до потенційних можливостей правоохоронних органів, а також небажанням публічно визнати слабкі місця у власних системах безпеки.

Згідно зі статистичною інформацією ДСА, у 2007—2008 рр. суди не розглядали кримінальних справ про злочини, передбачені статтями 363 та 363[1] КК.

Призначення покарання

Вивчення зазначеної категорії кримінальних справ засвідчило, що суди, призначаючи покарання, здебільшого дотримуються передбаченого законом принципу індивідуалізації покарання залежно від характеру і ступеня тяжкості вчиненого злочину. Однак при призначенні покарань ще мають місце недоліки, на які необхідно звернути увагу. Зокрема, у деяких випадках сумнівними є рішення суду щодо призначення більш м'якого покарання, ніж передбачено законом, та звільнення осіб від відбування покарання з випробуванням. Згідно з вимогами ст. 69 КК суд може призначити більш м'яке покарання, ніж передбачено законом, лише за наявності декількох обставин (тобто не менше двох), що пом'якшують покарання та істотно знижують ступінь тяжкості вчиненого злочину, з урахуванням особи винного.

Однак мали місце випадки необґрунтованого призначення судами більш м'якого покарання, ніж передбачено законом.

Наприклад, Павлоградський міськрайонний суд Дніпропетровської області вироком від 30 квітня 2007 р. визнав П. винною за ч. 3 ст. 362 КК та із застосуванням ст. 69 цього Кодексу призначив їй покарання у виді двох років обмеження волі. Призначаючи П. покарання, суд у вироку зазначив лише про наявність позитивної характеристики підсудної, а обставин, які пом'якшують покарання, не навів.

У деяких випадках суди при призначенні покарання не враховують, що від конфіскації майна як виду додаткового покарання необхідно відрізняти спеціальну конфіскацію, яка полягає у вилученні у засудженого програмних або технічних засобів, за допомогою яких було вчинено злочин. Оскільки законом не передбачено можливості звільнення від такої конфіскації, спеціальна конфіскація має застосовуватися судами незалежно від застосування статей 69, 75 КК.

Так, Шевченківський районний суд м. Києва вироком від 10 березня 2006 р. визнав Я. винним у вчиненні злочину, передбаченого ч. 1 ст. 361 КК, та призначив йому покарання у виді трьох років обмеження волі з конфіскацією телефонного шлюзу «Audio codes», який є власністю винної особи та за допомогою якого він вчинив несанкціоноване втручання у мережу електрозв'язку. На підставі ст. 75 КК суд звільнив його від відбування покарання з випробуванням, зазначивши у вироку про звільнення його від конфіскації технічного засобу, за допомогою якого було вчинено несанкціоноване втручання.

Апеляційний суд м. Києва вирок районного суду скасував у частині призначення Я. покарання та постановив свій вирок, яким призначив йому відповідне покарання із застосуванням конфіскації телефонного шлюзу.

Проведене узагальнення засвідчило, що при розгляді зазначеної категорії справ суди допускають помилки при кваліфікації дій винних осіб, розрізненні одних злочинів від інших, вирішенні питань про наявність або відсутність кваліфікуючих ознак та призначенні кримінального покарання.

Труднощі також виникають при кваліфікації дій винних осіб, коли несанкціоноване втручання в роботу ЕОМ, АС, комп'ютерних мереж здійснювалося з корисливих мотивів із метою викрадення чи заволодіння чужим майном. Зазначені дії суди помилково кваліфікують лише за статтями КК, в яких передбачено відповідальність за вчинення комп'ютерних злочинів.

Призначаючи покарання за вчинення такого виду злочинів, суди іноді не застосовують обов'язкову конфіскацію програмних та технічних засобів, за допомогою яких було вчинено злочин.