М.В. Карчевський,
науковий співробітник Луганського інституту внутр. справ

Удосконалення кримінального законодавства України про комп'ютерні злочини в контексті законодавства зарубіжних країн

Проблема боротьби з комп'ютерними злочинами вже близько 30 років розв'язується у світовій юридичній науці. Для кримінального права України вона відносно нова і недостатньо досліджена. Одне з дискусійних питань – визначення самого поняття "комп'ютерний злочин". Деякі автори вважають, що до комп'ютерної злочинності відносяться всі протизаконні дії, коли електронна обробка інформації є знаряддям їх здійснення і (або) засобом [1, с. 14], "...усі протизаконні діяння, предметом і засобом здійснення яких є процедури і методи, а також процес комп"ютерної обробки даних" [2, с. 72]. Інші до комп'ютерних злочинів відносять "злочини, пов"язані з втручанням у роботу комп'ютерів, і злочини, що використовують комп'ютери як необхідні технічні засоби" [3, с. 11].

Робляться спроби дати більш розширене визначення. Наприклад, П.Д. Біленчук і М.А. Зубань уважають, що комп'ютерна злочинність – це "суспільно небезпечна діяльність або бездіяльність, що здійснюється з використанням сучасних технологій і засобів комп"ютерної техніки з метою спричинення збитку майновим або суспільним інтересам держави, підприємств, відомств, організацій, кооперативів, громадським організаціям і громадянам, а також правам особистості" [4, с. 6; 5, с. 9]. Загальною рисою наведених визначень є об'єднання (поряд з іншими ознаками) протиправних діянь у групу "комп'ютерні злочини" на основі загальної ознаки – використання комп'ютера як засобу здійснення злочину. При такому підході втрачається логічна основа для визначення об'єкта злочину, тому що мова може йти про будь-які злочини, наприклад, розкрадання, шпигунство, незаконне збирання відомостей, що складають комерційну таємницю, і т. ін., якщо вони здійснюються з використанням комп'ютера як знаряддя, засобу або предмета злочину. І теоретично, і практично ці визначення не відповідають суті поняття "комп"ютерний злочин" як новий вид злочинів.

Ймовірно, що визначення нового виду злочинів доцільно будувати з урахуванням ознаки, що служить основою діючої класифікації злочинів. Класифікація – це розподіл предметів якого-небудь роду відповідно до найбільш істотних ознак на взаємозалежні класи. Для злочинів традиційно такою ознакою є їхній об'єкт. Класифікація за об'єктом – це

системоутворюючий фактор сукупності норм Особливої частини КК. У цьому зв'язку має сенс розмежовувати терміни "комп"ютерні злочини" [6] і "злочини у сфері використання комп"ютерної техніки". Очевидно, що остання група ширше. Саме її можна визначати як діяння, у яких комп'ютер є предметом, знаряддям або засобом здійснення злочину. Виділення даної групи, можливо має значення для криміналістики в плані специфіки методики розслідування. Але в кримінальному праві таке відокремлення, на нашу думку, є помилковим.

Як відомо, виготовлення підроблених грошових купюр за допомогою сучасних кольорових ксероксів не змінило кваліфікацію цих діянь, винні притягувалися і продовжують притягуватися до кримінальної відповідальності за статтею 79 КК України разом з тими, хто використовував для підроблення фототехніку або звичайні олівці, фарби й лезо бритви. Комп'ютерна техніка дозволяє довести до найвищого рівня процес виготовлення підроблених документів: перенесені з оригіналу відбитки печатки, підпису, інші реквізити практично ідентичні. Для встановлення підроблення потрібне проведення висококваліфікованої криміналістичної експертизи. Але чи означає це, що таке підроблення документів вимагає особливої, відмінної від існуючої, кваліфікації? Аналогія з наведеним прикладом виготовлення фальшивих купюр на ксероксі приводить до однозначного висновку: модифікація знарядь і засобів здійснення злочину, використання для цих цілей досягнень науково–технічного прогресу не змінює сутності злочину і тому не повинна впливати на його кваліфікацію. Підвищення суспільної небезпечності такого роду діянь вимагає тільки відповідної оцінки у визначенні покарання за їх здійснення. Тому слід погодитися з пропозицією В.В. Голини і В.В. Пивоварова про внесення до Загальної частини Проекту Кримінального кодексу (ст. 63 "Обставини, які обтяжують відповідальність") ознаки "здійснення злочинів із використанням засобів електронно-обчислювальної техніки" [7, с. 64-65].

Сказане не означає, що немає і не може бути комп'ютерних злочинів. Тут також доречна аналогія. Досягнення в галузі атомної енергетики, широке використання їх у народному господарстві зумовили формування ядерного права і відповідних доповнень Кримінального кодексу для захисту як суспільства від настання небезпечних наслідків, так і самих користувачів (виробників) атомної енергії від несанкціонованого втручання в їхню діяльність. Аналогічний процес відбувається й у сфері використання комп'ютерної техніки. Комп'ютерні злочини необхідно розглядати як якісно нові злочини, що заподіюють шкоду якісно новим суспільним відносинам, котрі з'явилися завдяки розширенню сфери застосування електронно-обчислювальної техніки. Щоб визначити такі злочини необхідно встановити суть цих відносин (охарактеризувати об'єкт комп'ютерних злочинів). Оскільки дані відносини обумовлені специфічним предметом – інформацією, насамперед варто дати її характе-

ристику. Зауважимо, що комп'ютерну інформацію доцільно також визначати предметом досліджуваних злочинів.

Інформація, будучи необхідною умовою людської діяльності, робить поведінку людини усвідомленою, тому що забезпечує зв'язок людини з людиною, людини з природою і технікою. Досить чітко соціальну значимість інформації сформулював засновник кібернетики Норберт Вінер: "... всякий організм скріплюється наявністю засобів придбання, використання, збереження і передачі інформації" [8, с. 234], тобто інформація як основа результативної, ефективної діяльності конкретної людини в решті решт є обов'язковим фактором розвитку і стабільності суспільства. Ефективність суспільного виробництва зростає за рахунок збільшення масштабів використання інформаційного ресурсу. І в цій якості інформаційний ресурс набуває все більшої економічної та соціальної цінності. Оптимальне використання інформаційних ресурсів вимагало розроблення специфічних – комп'ютерних технологій. Комп'ютерна техніка є засобом для роботи з інформацією. Подання інформації у формі, яку розпізнає машина, забезпечує оперативність передачі, обробки і збереження інформації, що в сучасних умовах і є соціально значимим.

У літературі соціально корисні якості комп'ютерної інформації описуються за допомогою її трьох специфічних властивостей: 1) цілісність (захищеність від несанкціонованих змін і знищення); 2) доступність (захищеність від несанкціонованого утримання інформаційних ресурсів і наявність в осіб, які мають право на інформацію, можливості роботи з нею); 3) конфіденційність (захищеність від несанкціонованого одержання) [9, с. 22]. Таким чином, комп'ютерну інформацію визначимо як *відомості про об'єктивний світ і процеси, що відбуваються у ньому, які сприймаються та використовуються людиною, зафіксовані за допомогою засобів комп'ютерної техніки, що забезпечує її цілісність, конфіденційність і доступність.* Автор у своїх розробках виходить з того, що суспільні відносини з приводу інформації регулюються за допомогою специфічного інституту права власності на неї і тому пропонує таке визначення об'єкту комп'ютерних злочинів: *охоронювана кримінальним законом структурно організована і нормативно врегульована система соціально значимих відносин власності на комп'ютерну інформацію, що забезпечує оптимальну в історичних умовах інформатизації і комп'ютеризації нормативно регламентовану свободу реалізації права кожного учасника на задоволення інформаційної потреби* [10].

Оскільки злочинні посягання на комп'ютерну інформацію є формою посягань на відносини власності, назву глави XVI в проекті КК доцільно змінити на "Злочини проти власності на комп"ютерну інформацію", що дозволить більш конкретно охарактеризувати об'єкт злочину. Безпосередні об'єкти визначаються розподілом інформації за режимом доступу до неї. Ними, отже, будуть відносини власності на відкри-

ту комп'ютерну інформацію і відносини власності на комп'ютерну інформацію з обмеженим доступом. Так, право власності на інформацію, яку суб'єкт надає у відкрите користування, може бути порушене шляхом знищення цієї інформації або здійснення дій, у результаті яких значно погіршується можливість ознайомлення з нею, тобто порушується право розпорядження. Приклади порушення права власності на інформацію з обмеженим доступом утруднень не викликають. Запропоноване рішення може бути основою для побудови ефективного механізму кримінально-правової охорони відносин власності на комп'ютерну інформацію, оскільки дозволяє диференціювати суспільні відносини, які охороняються, за ступенем соціальної значимості й забезпечує чітку градацію дій і наслідків, що складають об'єктивну сторону. Якщо до наслідків при здійсненні злочину проти права власності на комп'ютерну інформацію з обмеженим доступом необхідно відносити порушення конфіденційності, доступності та цілісності, то при аналізі злочинів, предметом яких є відкрита інформація, необхідно враховувати, що суспільно небезпечними наслідками таких злочинів будуть тільки порушення цілісності і доступності. Таким чином, позначивши суспільні відносини, яким заподіюється шкода, видається можливим визначити комп'ютерні злочини як *суспільно небезпечні, карані, винні діяння, що заподіюють шкоду відносинам права власності на комп'ютерну інформацію шляхом порушення її цілісності, конфіденційності або доступності.*

В Україні комп'ютерні технології впроваджено з істотним відставанням у часі й масштабах від передових західних країн, і дефіцит практики позначається на темпах формування законодавства. Однак дана обставина створює також певні переваги в можливості використання західного досвіду правового регулювання. У країнах Західної Європи проблема боротьби зі злочинами у сфері використання комп'ютерної техніки вирішується відповідно до принципів континентальної системи права. Кримінальні кодекси доповнені, по–перше, рядом статей про посягання на традиційні об'єкти злочинів, що здійснюються з використанням комп'ютерної техніки, і, по-друге, новою групою норм, що передбачають відповідальність за посягання на якісно новий об'єкт (комп'ютерні злочини).

Так, розд. 15 Кримінального кодексу ФРН "Порушення недоторканності й таємниці приватного життя" доповнено ст. 202 а "Дії, спрямовані на одержання відомостей", у якій встановлюється відповідальність за незаконне одержання або передачу відомостей, «які можуть бути відтворені або передані електронним, магнітним або іншим способом і не є безпосередньо сприйманими" [11]. У КК Іспанії схожі доповнення зроблено до ст. 197 розд. 10 "Розкриття і поширення таємних відомостей" розд. 10 "Злочини проти недоторканності приватного життя, права на власне зображення і недоторканності житла" [12]. У КК Франції Книга 2 "Про злочини і провини проти людини" містить параграф 2

"Про посягання на таємницю кореспонденції", де в ст. 226-15 установлюється відповідальність за порушення таємниці кореспонденції, переданої за допомогою засобів комп'ютерної техніки, і відділ 5 "Про посягання на права людини, пов"язані з використанням картотек і опрацювання даних на ЕОМ", де в сімох ст. (226-16 – 226-22) встановлюється відповідальність за незаконне оброблення відомостей про особу, неприйняття заходів інформаційної безпеки при проведенні такого оброблення, введення або збереження в ЕОМ без спеціального дозволу інформації, що дозволяє ідентифікувати людину, порушення термінів збереження інформації про особу, незаконне використання такої інформації і т. ін. [13]. Удосконалення традиційних норм про злочини проти власності має місце в Німеччині. Розд. 22 КК ФРН "Шахрайство і злочинне зловживання довірою" доповнено ст. 263а "Комп"ютерне шахрайство", що передбачає відповідальність за незаконне одержання вигоди або заподіяння шкоди майну іншої особи шляхом неправомірного впливу на процес опрацювання даних. Доповнення до системи норм, що охороняє встановлений порядок обігу документів, зроблено у ФРН та Іспанії. У розділі 23 "Підроблення документів" КК ФРН, у ст. 274 "Утаювання документів, зміна знаків, що позначають границю", установлюється відповідальність за знищення, пошкодження або утаювання технічного запису з наміром завдати шкоди іншій особі. Ст. 400 гл. 3 "Загальні положення" розд. 18 "Про фальсифікації" КК Іспанії передбачає відповідальність за розроблення або володіння комп'ютерними програмами, спеціально призначеними для здійснення фальсифікацій. Спеціальні норми про злочини проти держави, що здійснюються з використанням комп'ютерної техніки, містить КК Франції. Кн. 4 КК Франції "Про злочини і провини проти нації, держави і суспільного порядку" містить статті 411-6 – 411-8 (відділ 3 "Про передавання інформації іноземній державі", гл. 1 "Про зраду і шпигунство" розд. 1 "Про посягання на основні інтереси нації"), що передбачають відповідальність за передавання або забезпечення доступності для іноземної держави, іноземного підприємства або організації, підприємства або організації, що знаходяться під іноземним контролем, або їхнім представникам даних, що містяться в пам'яті ЕОМ, використання, поширення або збирання яких може призвести до посягань на основні інтереси нації; збирання й зосередження з метою передавання таких даних і здійснення за рахунок іноземних організацій діяльності, що має метою одержання зазначених даних. У ст. 411-9 відділу 4 "Про саботаж" передбачається кримінальна відповідальність за знищення, псування, або розкрадання, внесення вад в автоматизовані системи опрацювання даних, коли це може призвести до посягання на основні інтереси нації. У ст. 413-9 відділу 2 "Про посягання на секрети національної оборони" гл. 3 "Про інші посягання на національну оборону" цієї ж книги зазначається, що дані, які містяться в пам'яті ЕОМ, що є об'єктом захисних заходів які обмежують їх роз-

повсюдження, носять характер секретів національної оборони і на них поширюються норми про посягання на секрети національної оборони. За пунктом 2 ст. 421-1 гл. 1 "Про терористичні акти" розд. 2 "Про тероризм" кваліфікуються як терористичні акти посягання на роботу автоматизованих систем, що мають метою серйозно порушити суспільний порядок шляхом залякування чи терору.

Доповнення про злочини, пов'язані з комп'ютерною технікою у сфері інтелектуальної власності та комерційної таємниці, зроблено до Кримінального кодексу Іспанії. Ст. 270 гл. 11 "Про злочини, пов"язані з інтелектуальною і промисловою власністю, з ринком і споживачами" передбачає відповідальність за порушення авторського права. Дана стаття містить доповнення, відповідно до якого вона може застосовуватися для кваліфікації випадків серійного виробництва або володіння спеціальним засобом, що нейтралізує технічний або програмний захист програм для ЕОМ. У ст. 278 відділу 3 "Про злочини, пов"язані з ринком і споживачами" цієї ж глави встановлено відповідальність за незаконне заволодіння електронними документами з метою розкрити комерційну таємницю. Таким чином, кримінальні кодекси, що аналізуються, містять доповнення про посягання, які вчиняються за допомогою комп'ютерної техніки, на такі традиційні об'єкти: особа (КК ФРН, Франції, Іспанії); власність (КК ФРН); національна безпека (КК Франції); установлений порядок обігу документів (КК ФРН, Іспанії); інтелектуальна власність (КК Іспанії); комерційна таємниця (КК Іспанії).

Норми, що передбачають відповідальність за посягання на якісно новий об'єкт, мають місце в кримінальних кодексах ФРН і Франції. У розд. 26 "Пошкодження майна" КК ФРН установлюється відповідальність за протиправну зміну даних (ст. 303а "Зміна даних") і комп'ютерний саботаж – порушення опрацювання даних, що мають істотне значення для чужого підприємства, організації або органу шляхом зміни даних (ст. 303а) або руйнування, пошкодження, приведення в непридатний стан або зміни установки для опрацювання даних або носія інформації (ст. 303b "Комп"ютерний саботаж") [14]. У ст. ст. 323-1, 323-2 і 323-3 гл. 3 "Про посягання на системи автоматизованого опрацювання даних" розд. 2 "Про інші посягання на власність" кн. 3 "Про злочини проти власності" КК Франції передбачено відповідальність за незаконний доступ до системи автоматизованого опрацювання даних; дії, спрямовані на перешкоджання або порушення правильності роботи такої системи; незаконне введення даних у систему автоматизованого опрацювання даних або знищення, зміну даних, що містяться в ній. Загальною рисою цих законодавчих рішень є те, що злочини проти комп'ютерної інформації у Кримінальних кодексах ФРН і Франції знаходяться в розділах, що передбачають відповідальність за злочини проти власності.

Отже, висловлені пропозиції щодо вдосконалення українського за-

конодавства відповідають тенденціям розвитку кримінального законодавства країн Західної Європи. Вище наводилися пропозиції В.В. Голини і В.В. Пивоварова про внесення до Загальної частини КК України такої обтяжуючої відповідальність ознаки, як скоєння злочину з використанням засобів комп'ютерної техніки. А в країнах Західної Європи норми про посягання на традиційні об'єкти доповнюються положеннями, які дозволяють використовувати ці норми для кваліфікації посягань на такі об'єкти з використанням комп'ютерної техніки.

Стосовно саме комп'ютерних злочинів теж маємо певну відповідність. Комп'ютерні злочини в європейському законодавстві відносяться до злочинів проти власності. Вище пропонувалося об'єктом комп'ютерних злочинів в українському законодавстві визначити право власності на комп'ютерну інформацію. Хоч слід зазначити що запропоноване рішення відрізняється від французького визначення родового об'єкту комп'ютерних злочинів (відносини щодо систем автоматизованого опрацювання даних) та німецького (загальні майнові відносини). У США проблему кримінальної відповідальності за злочини у сфері використання комп'ютерної техніки розв'язано інакше. Рішення американського законодавця більш відповідають тим поглядам на комп'ютерні злочини, які критикувалися на початку статті. Відповідальність за злочини у сфері використання комп'ютерної техніки передбачено в параграфі 1030 "Шахрайство і подібні злочини, пов"язані з комп'ютерами" (Fraud and Related Activity in Connection with Computers) титулу 18 Зводу законів США. У цьому параграфі передбачається відповідальність за здійснення таких дій: 1. Одержання особою доступу до охоронюваної комп'ютерної інформації і здійснення дій, спрямованих на передачу такої інформації особам, що не мають права доступу до неї, чим створюється небезпека заподіяння шкоди США або утруднюється використання такої інформації владою (1030 (a) (1)). 2. Одержання особою, яка не має на це права, комп'ютерної інформації, що знаходиться в комп'ютері фінансової установи (1030 (a) (2) (A)), інформації будь-якого міністерства або відомства США (1030 (a) (2) (B)) або інформації, що знаходиться в захищеному комп'ютері [15] якщо дія включала використання міжнародної комунікації або комунікацію між штатами (1030 (a) (2) (3)). 3. Одержання особою, яка не має на це права, доступу до комп'ютера, який використовується урядом США, та утруднення такими діями його використання (1030 (a) (3)). 4. Одержання незаконної вигоди або заподіяння шкоди шляхом впливу на комп'ютерну інформацію (1030 (a)(4)). 5. Незаконна передача коду, що заподіює шкоду [16] захищеному комп'ютерові (1030 (a) (5) (A)). 6. Навмисний незаконний доступ до захищеного комп'ютера і необережне заподіяння шкоди в результаті таких дій (1030 (a) (5) (B)). 7. Навмисний незаконний доступ до захищеного комп'ютера і заподіяння шкоди в результаті таких дій (1030 (a) (5) (C)). 8. Незаконна торгівля паролями або будь-якою іншою інформацією, що дозволяє здійснити неправо-

мірний доступ (1030 (а) (6)). 9. Погроза з метою одержання незаконної вигоди заподіянням шкоди захищеному комп'ютерові (1030 (а) (7)) [17].

Крім параграфа 1030, відповідальність за злочини, пов'язані з комп'ютерною технікою, передбачають параграфи: 1029 – незаконна торгівля пристроями доступу, 2511 – розголошення повідомлень, переданих телеграфом, усно або електронним способом, і параграф 2701, що спеціально охороняє конфіденційність електронної пошти і мовної кореспонденції на сервері, – навмисне одержання або видозміна повідомлень, що зберігаються в електронній пам'яті, створення перешкод для санкціонованого доступу до таких повідомлень [18, с.18-19]. Отже, у США спостерігається зовсім інший підхід до організації кримінально-правової відповідальності за злочини у сфері використання комп'ютерної техніки, ніж у європейських країнах. У новому розділі Зводу законів США об'єднано злочини з різними об'єктами: шпигунство (1030 (а) (1)), використання комп'ютера для розкрадань (1030 (а) (4)), незаконне одержання інформації (1030 (а) (2)), вимагательство (1030 (а) (7)) і т. ін. Дану розбіжність можна пояснити несхожістю підходів до систематизації норм кримінального законодавства в континентальній і американській правових системах. Принципи систематизації відображають специфіку розуміння злочинного у тій чи іншій державі, яка обумовлена історичними, економічними та соціальними особливостями. Тому використання розроблених в рамках певної правової системи рішень для охорони суспільних відносин у державі, яка не відноситься до цієї системи, не завжди обґрунтоване. Останнє відноситься і до проблеми комп'ютерних злочинів.

У цьому зв'язку цікавим представляється аналіз пропозицій Ради Європи щодо вдосконалення законодавства про комп'ютерні злочини 1989 і 2000 рр. 13 вересня 1989 р. Радою Європи були прийняті рекомендації, розроблені Комітетом експертів з комп'ютерних злочинів Союзу Європи. Даний документ містить два списки дій: мінімальний і додатковий. У мінімальний список включені визначення комп'ютерних злочинів з яких досягнуто загальної згоди й у відповідність до яких повинні бути приведені карні законодавства держав членів Союзу Європи. У додатковому списку знаходяться діяння, криміналізовані в окремих державах, але з приводу криміналізації яких усіма державами, що входять у Союз Європи згоди досягнуто не було. Мінімальний список: комп'ютерне шахрайство [19], комп'ютерне підроблення, пошкодження комп'ютерних даних або програм, комп'ютерний саботаж, неправомірний доступ, неправомірне перехоплення, неправомірне відтворення комп'ютерних програм, неправомірне відтворення топологій напівпровідникової продукції. Додатковий список складають такі дії: зміна комп'ютерних даних або програм, комп'ютерне шпигунство, несанкціоноване використання комп'ютерів, несанкціоноване використання захищених комп'ютерних програм [20].

У проекті угоди з комп'ютерних правопорушень Ради Європи 2000

р., яку запропоновано для публічного обговорення, пропонується така класифікація даних злочинів: порушення конфіденційності, цілісності та придатності комп'ютерних даних і систем (незаконний доступ, незаконне перехоплення, перекручування даних, перешкоди роботі системи, нелегальні пристрої); правопорушення, зв'язані з комп'ютером (фальсифікація даних, шахрайство зв'язане з комп'ютером); правопорушення, зв'язані зі змістом інформації (злочини, зв'язані з дитячою порнографією); авторське право і зв'язані з ним порушення (незаконне відтворення і поширення за допомогою комп'ютерної системи об'єктів авторського права) [21]. Отже, перші рекомендації Ради Європи 1989 р. більшою мірою відповідають американському підходу до вирішення проблеми комп'ютерних злочинів. Це можна пояснити тим, що в США вперше у світі комп'ютерна техніка набула значного поширення, там же вперше було поставлено питання про комп'ютерні злочини, а рішення Ради Європи 1989 р. являє собою запозичення цього рішення без оцінки специфіки систематизації континентального законодавства. Однак уже в проекті останнього рішення Ради Європи з комп'ютерних злочинів ми виявляємо відповідну континентальним правовим традиціям класифікацію злочинів, пов'язаних із комп'ютерною технікою. В цьому проекті відокремлюється група злочинів з якісно новим об'єктом (порушення конфіденційності, цілісності та придатності комп'ютерних даних і систем) й визначаються злочинні посягання на традиційні об'єкти, що скоюються з використанням комп'ютерної техніки.

Таким чином, висловлені на початку пропозиції щодо вдосконалення кримінального законодавства України з питань комп'ютерних злочинів відповідають тенденціям розвитку законодавств Західної Європи, законопроектній діяльності в цьому регіоні та принципам систематизації кримінального законодавства в континентальній правовій системі. Їх використання дозволить: створити в Україні ефективну нормативно–правову базу для боротьби з комп'ютерними злочинами; проводити роботу щодо гармонізації українського законодавства з законодавством зарубіжних країн, що з огляду на тенденції інтернаціоналізації комп'ютерної злочинності видається актуальним завданням.

Список літератури:

1. Калюжный Р.А. Теоретические и практические проблемы использования вычислительной техники в системе органов внутренних дел (организационно–правовой аспект): Автореф. дис... д-ра юрид. наук, 12.00.02 / АН Украины Институт государства и права им. В.М. Корецкого. – К., 1992. – С. 14. 2. Азаров Д. Порушення роботи автоматизованих систем – злочини у сфері комп'ютерної інформації // Право України. – № 12. – 2000. – С. 72. 3. Батурин Ю.М., Жодзишский А.М. Компьютерная преступность и компьютерная безопасность. – М.: Юридическая литература, 1991. – С. 11. 4. Біленчук П.Д., Зубань М.А. Комп'ютерні злочини: соціально–правові та кримінолого–криміналістичні аспекти: Навчальний посібник. – К.: Ук-

раїнська академія внутрішніх справ, 1994. – С. 6. 5. Шилан Н.Н., Кривонос Ю.М., Бирюков Г.М. Компьютерные преступления и проблемы защиты информации: Монография – Луганск: РИО ЛИВД, 1999. – С. 9. 6. Злочини, які є предметом дослідження, будемо називати "комп"ютерні злочини". Хоч цей термін має недоліки (ще у 1974 році в Німеччині під час слухань однієї справи було відзначено, що злочинець не комп'ютер, злочинець – людина, тому термін "комп"ютерний злочин" є невдалим), його використання видається доцільним з урахуванням його значної поширеності. 7. Голина В.В., Пивоваров В.В. Проблемы компьютерной преступности // Фінансова злочинність: Зб. матеріалів міжнар. наук.–практ. семінару, 12-13 лют. 1999 р./ Ред. кол.: В.І. Борисов (голов. ред.) та ін.]. – Х.: Право, 2000. – С. 64 – 65. 8. Винер Н. Кибернетика или управление и связь в животном и машине. – М.: Советское радио, 1968. – С. 234. 9. Воройский Ф.С. Систематизированный толковый словарь по информатике. (Вводный курс по информатике и вычислительной технике в терминах) – М.: Киберия, 1998. С. 22. 10. Докладніше про об'єкт і предмет комп'ютерних злочинів у статті: Карчевский Н.В. Преступления против собственности на компьютерную информацию: определение, объект и предмет // Вісник ЛІВС МВС України. – № 1. – 2001. 11. Приводиться за: Уголовный кодекс ФРГ / Пер. с нем. А.В. Серебренникова. – М., 1996. 12. Приводиться за: Уголовный кодекс Испании / Под ред. Н.Ф. Кузнецовой, Ф.М. Решетникова. – М., 1998. 13. Приводиться за: Новый уголовный кодекс Франции / Науч. ред. Н.Ф. Кузнецова, Э.Ф. Побегайло. – М. 1994. 14. Зауважимо, що у КК Франції схожий склад злочину віднесено до злочинів проти нації. 15. Під захищеним комп'ютером американський законодавець розуміє комп'ютер, що використовується виключно фінансовим закладом чи урядом США або комп'ютер невиключного використання, який використовується фінансовим закладом чи урядом США або для нього та дії, які складають порушення утруднюють це використання; або комп'ютер, який використовується в торгівлі між штатами, або міжнародній торгівлі, або зв'язку (1030 (e)(2)(A)). 16. Шкода в даному випадку розуміється як будь-яке погіршення цілісності або доступності даних, програми, системи, яке призвело до шкоди еквівалентної не менш ніж 5000 доларів на рік одній або декільком особам; або зміні чи пошкодженню або створенню небезпеки зміни чи пошкодження судово–медичної експертизи, діагнозу, одного або декількох осіб або спричиняє фізичну шкоду людині або створює небезпеку охороні здоров'я чи безпеці (1030 (e)(8)). 17. Приводиться за: The National Information Infrastructure Protection Act of 1996 Legislative Analysis By The Computer Crime and Intellectual Property Section United States Department of Justice. http://www.usdoj.gov/criminal/cybercrime/1030_anal.html. 18. Панфилова Е.И., Попов А.Н. Компьютерные преступления: Серия «Современные стандарты в уголовном праве и уголовном процессе» / Науч. редактор проф. Б.В. Волженкин. – СПб., 1998. С. 18–19. 19. Слід відзначити, що використання європейськими фахівцями терміну «шахрайство» (fraud), в контексті комп'ютерних злочинів, представляється не зовсім вдалим. Тому що це вимагає визнання як істинних таких висловлювань як «обман комп'ютера» або «зловживання довірою комп'ютера». 20. Приводиться за International review of criminal policy – United Nations Manual on the prevention and control of computer–related crime, paragraph 191–197, http://www.ifs.univie.ac.at/~pr2qq/rew4344.html. 21. Crime in Cyberspace. First Draft of International Convention Released for Public Discussion. http://bezpeka.com / library /asp / asp_33.html.

Надійшла до редколегії 01.10.2000