ВИДИ ПРАВОПОРУШЕНЬ У СФЕРІ КОМП'ЮТЕРНИХ ТА ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

Л.В. СОРОКА

Широке впровадження на світовому рівні комп'ютеризованих інформаційно-технологічних систем потребує посилення правового регулювання суспільних відносин у цій сфері. Вони захищаються значним нормативним масивом, у тому числі законами України "Про інформацію", "Про науково-технічну інформацію", "Про національну програму інформатизації" та іншими; правове регулювання інформаційних відносин у частині, пов'язаній зі створенням і використанням комп'ютерних технологій здійснюється законами України "Про авторське право і суміжні права", "Про захист інформації в автоматизованих системах", "Про охорону прав на топографію інтегральних мікросхем".

Найбільш активно розвиваються технології, пов'язані з глобальною комп'ютерною мережею Інтернет, що призвело до появи нових категорій як: е-торгівля, е-бізнес, е-уряд тощо. Разом з тим значні переваги Інтернет-технологій для проведення наукових досліджень, електронного бізнесу та комерції в інформаційному суспільстві несуть із собою загрози, основна з яких – активне використання злочинним світом нових технологій для шахрайства, крадіжок, "відмивання брудних коштів" тощо.

За даними Інституту комп'ютерної безпеки (Computer Security Institute), у другій половині 2002 р. число хакерських атак збільшилося на 32% у порівнянні з аналогічним періодом 2001 р. [1, 114]. А у 2000 р. на конгресі з профілактики злочинності було розповсюджено дані, що загальний прибуток хакерів становить 500 млн. доларів за рік, а збитки від вчиненого середньостатистичного злочину складає майже 560 тис. доларів США [2, 8].

Одними з перших найбільш ґрунтовних праць в цій сфері стали роботи Ю.М. Батурина, в яких розглядається широкий спектр проблем комп'ютерного права, серед яких: комп'ютеризація суспільства і питання теорії права, комп'ютеризація і права особи, комп'ютеризація управління, зобов'язальне право і РЮМ, охорона комп'ютерного права [3, 57]. Особлива увага приділяється комп'ютерній безпеці та комп'ютерній злочинності, кваліфікації комп'ютерних злочинів, порядку їх розкриття [4, 23].

Практичне керівництво з комп'ютерного права розроблено Машуковим В.М. У ньому комп'ютерні програми характеризуються як

об’єкт авторського права, патентного права, договірного права. Право на використання комп’ютерних програм характеризуються через право власності, виключні права, вільне використання [5, 56].

Колективом авторів – Біленчуком П.Д., Романюком В.С., Цимбалюком В.С. та іншими – написаний навчальний посібник “Комп'ютерна злочинність”. У його підготовці брали участь викладачі Національної академії внутрішніх справ України, Центр з проблем боротьби з організованою злочинністю, міжнародні агенції “Бізон”, практичні працівники спецпідрозділів МВС України. Це перший повний навчальний посібник, що висвітлює актуальні проблеми національної безпеки України, пов'язані з комп'ютерною злочинністю. В ньому міститься загальна характеристика комп'ютерної злочинності в світі: проблеми боротьби та перспективи міжнародного співробітництва; висвітлюються основні напрямки комп'ютерної злочинності в США, Канаді, Європі, Азії; дається портрет комп'ютерного злочинця та хакерських організацій; комп'ютерна криміналістика: техніка, тактика, методика [6, 145].

Інтенсивне впровадження обробки інформації в економіку та у сферу кредитно-фінансової системи зумовило появу нового класу злочинів – комп'ютерних. Комп'ютерний злочин – це злочин, де комп'ютер безпосередньо є предметом та (або) знаряддям здійснення правопорушень у суспільних сферах, які пов'язані з використанням комп'ютерної техніки. Комп'ютерні злочини мають багатогранний характер – комп'ютерне піратство, комп'ютерний підлог, комп'ютерне шахрайство з даними і програмами, комп'ютерний саботаж, несанкціонований доступ до систем ЕОМ.

Інструментом знищення інформації є так звані програми-віруси. Комп'ютерні віруси (від лат. VIRUS - отрута) - вид комп'ютерних програм, здатних без відома користувача та поза його волею спонтанно розмножуватися і поширюватися. Комп'ютерний вірус вносить зміни в існуючі програми, що призводить до несанкціонованого знищення, блокування, модифікації чи копіювання інформації, порушення роботи ВОМ чи їх мереж, у зв'язку з чим і його назва виникла за аналогією з медичним вірусом. Для боротьби із комп'ютерними вірусами розробляють та створюють спеціальні антивіруси! програми, призначення яких полягає у виявленні та знищені комп'ютерних вірусів [7, 198]. Загальну класифікацію комп'ютерних вірусів, способів їх розповсюдження та структуру, опис каталогу, юридичні та інші способи захисту інформації в комп'ютерних системах у своїй роботі дає Коваленко М.М [8, 45].

Комп'ютерній злочинності в юридичній літературі приділяється все більше уваги. Так, міфи і реальність комп'ютерної злочинності аналізує Раденький В. Міфом він називає думку щодо всемогутності хакерів та цілковитої незахищеності комп'ютерних систем, яка насаджується

засобами масової інформації. Не дивлячись на серйозні проблеми з безпекою комп'ютерних технологій, прорив у цьому напрямку таки є. Галузі, що потребують забезпечення вищим рівнем захисту та секретності – військова, атомна енергетика, – користуються захищеними системами, ізольованими від мереж загального користування. Несанкціонований віддалений доступ до них ззовні неможливий [9, 5].

З іншого боку, вказує Раденький В., розкриття правоохоронцями комп'ютерних злочинів ускладнюється тим, що хакери ретельно "замітають" свої сліди. Майже всі вони використовують міжнародні супутникові мережі телезв'язку, тобто можуть перебувати на значній відстані від об'єкту посягання і витрачати на скоєння злочину лічені долі секунди. В той же час розслідування займає тижні, якщо не місяці, а це дає злочинцям додаткові можливості захистити себе [9, 6].

Предметом комп'ютерної крадіжки крім інформації, можуть бути також гроші та інші матеріальні цінності. Причому їх розкрадання відбувається не у звичному для нас розумінні, у безготівковому вигляді, за допомогою комп'ютера. Дані гроші є фактично комп'ютерною інформацією, а не майновими правами, для віднесення таких грошей до майнових прав немає достатніх підстав [10, 87].

Питаннями кваліфікації комп'ютерних злочинів займається Лісовий В. Він відзначає, що різні країни пішли неоднаковими шляхами при кримінально-правовому регулюванні комп'ютерних злочинів. У багатьох державах відповідальність за вчинення злочинів у сфері інформатизації настає за традиційними статтями кримінального законодавства (крадіжка, шахрайство тощо). Деякі держави мають спеціальні норми в кримінальному законодавстві. Під комп'ютерними злочинами автор розуміє передбачені кримінальним законом суспільно-небезпечні діяння, вчинені переважно з використанням комп'ютерної техніки, у яких електронна обробка інформації є або засобом, або об'єктом злочинного посягання [11, 34-35].

Узагальнюючи різні концепції, можна стверджувати, що до правопорушень у сфері комп'ютерних технологій відносяться всі протизаконні дії, при яких електронна обробка інформації була знаряддям їх вчинення або предметом. В цілому це:

- незаконне використання комп'ютера з метою аналізу або моделювання злочинних дій для їх здійснення в комп'ютерних системах;
- несанкціоноване проникнення в інформаційно-обчислювальну мережу або масиви інформації з корисливою метою;
- розкрадання системного і прикладного програмного забезпечення;
- несанкціоноване копіювання, зміна або знищення інформації;
- шантаж, інформаційна блокада та інші методи комп'ютерного тиску;
- комп'ютерний шпіонаж і передання комп'ютерної інформації особам, які не мають права доступу до неї;

- фальсифікація комп'ютерної інформації;
- розробка і розповсюдження комп'ютерних вірусів в інформаційно-обчислювальних системах і мережах;
- несанкціонований перегляд або розкрадання інформації з банків даних баз знань і автоматизованих систем;
- недбалість при розробленні, створенні інформаційно-обчислювальних мереж і програмного забезпечення, що призводить до небажаних наслідків і втрати ресурсів;
- механічні, електричні, електромагнітні та інші види впливу на інформаційно-обчислювальні системи та лінії телекомунікації, що викликають їх пошкодження [6, 63]. Але цей перелік на сьогоднішній день є невичерпним і постійно збільшується.

Комп'ютерні правопорушення в юридичній літературі групуються по-різному, найчастіше в три групи. До першої групи належать правопорушення, де сам комп'ютер чи інформація у ньому є предметом вчинення протиправних дій. До другої групи відносять правопорушення, де комп'ютер виступає як знаряддя вчинення злочину. До третьої групи входять правопорушення, доказом яких є інформація, що міститься в комп'ютерних системах [12, 22].

Шахрайство є досить великим нелегальним бізнесом. Є декілька видів електронного шахрайства, суть якого полягає у тому, що як оплата за товари і послуги використовуються підроблені кредитні картки, у тому числі і пластикові. Цей вид шахрайства вирізняє простота, відсутність насильства, а також та обставина, що ні банк, ні законний власник картки, як правило, не бачить зловмисника. Статистичні дані свідчать, що шахрайство з пластиковими платіжними картками становить три відсотки від загального обсягу здійснених операцій [2, 3].

Інший вид шахрайства - це несанкціонований доступ до електронно-банківських рахунків і модифікація інформації, що знаходиться в них. Так відбувається перерахування коштів на рахунки злочинців. Наприклад, у США збитки від шахрайства з магнітними кредитними картками у 1992 р. перевищили 1 трильйон доларів. Доходи злочинців стоять на третьому місці після доходів від торгівлі наркотиками і зброєю. Коли фінансовими установами Канади було випущено близько 25 мільйонів кредитних карток, правоохоронними органами було встановлено, що з них більше 55 тисяч використовувалося виключно шляхом обману [13, 47-48].

Дослідження комп'ютерної проблематики свідчить про появу транснаціональної міжнародної комп'ютерної злочинності. Вона характеризується такими негативними явищами, як кібервійни, комп'ютерний тероризм, комп'ютерне хуліганство, комп'ютерне піратство та інше [6, 93-94].

За характером їх умовно можна поділити на дві основні групи: воєнно-політичні і економічні. До першої групи слід віднести кібервійни,

обумовлені комп'ютеризацією ракетно-ядерного арсеналу кожної держави. До другої – трансграничне "нелегальне інформаційне брокерство" (злам комп'ютерних систем з наступним продажем інформації як самим потерпілим, так і конкурентам); організоване промислове (комерційне, підприємницьке) шпигунство; організоване "комп'ютерне піратство".

Періодична преса постійно повідомляє про вражаючі за обсягом масштаби комп'ютерної злочинності і, насамперед, комп'ютерного піратства. Високим рівнем таких злочинів вирізняються країни Східної Європи, третього світу, Південної Африки. Наприклад, середній рейтинг комп'ютерного піратства на теренах Східної Європи становив 80-85%. У грошовому обчисленні це щорічно становить збитки розробників комп'ютерних програм у розмірі 750 млн. доларів США [14, 4].

Однією з підстав кіберзлочинності є відсутність належного законодавчого регулювання в рамках міжнародного права, так як національним законодавством окремо взятої країни усіх проблем охорони комп'ютерних технологій не вирішити.

Перші спеціальні закони по боротьбі з комп'ютерною злочинністю було прийнято в 1973 році у Швеції та у 1976 році в США. Згодом і в інших країнах світу були затверджені законодавчі акти стосовно цієї категорії злочинів. До боротьби з комп'ютерними злочинами, виходячи з їх широких масштабів та багатоманітних втрат, підключились міждержавні і громадські організації [9, 37].

Європейський комітет з проблем злочинності Ради Європи у 1990 році підготував рекомендації з метою визначення в Європі правопорушень, пов'язаних з комп'ютерами, і ввів їх до "Мінімального списку" та "Необов'язкового списку" комп'ютерних злочинів, які були рекомендовані для включення до законодавств європейських країн [6, 167].

До Мінімального списку входять такі види протиправних діянь: комп'ютерне шахрайство, комп'ютерний підлог, знищення комп'ютерної інформації та комп'ютерних програм, комп'ютерний саботаж, несанкціонований доступ до комп'ютерних мереж; несанкціоноване копіювання захищених комп'ютерних програм; незаконне виробництво типографічних копій.

Необов'язковий список включає в себе: зміна інформації чи комп'ютерних програм, комп'ютерне шпигунство, протизаконне застосування комп'ютера, несанкціоноване застосування захищених комп'ютерних програм.

Також Радою Європи була прийнята Конвенція про кіберзлочинність, яку 23 листопада 2001 р. Україна ратифікувала. Конвенція являє собою комплексний документ, який містить норми, призвані вплинути на різні галузі права: кримінальне, кримінально-процесуальне, авторське, цивільне, інформаційне. Вона базується на основних принципах міжнародного

права: поваги прав людини, співробітництва і добросовісного виконання зобов'язань.

Об'єктом кіберзлочинності, відповідно до Конвенції, є широкий спектр суспільних відносин, що що охороняються нормами права. Ці відносини виникають при здійсненні інформаційних процесів із приводу виробництва, збору, обробки, накопичення, збереження, пошуку, передачі, розповсюдження і споживання комп'ютерної інформації, а так само в інших областях, де використовуються комп'ютери, комп'ютерні системи і мережі. Серед них, з огляду на підвищену суспільну значимість, відокремлюються правовідносини, що виникають у сфері забезпечення конфіденційності, цілісності комп'ютерних даних і систем, законного використання комп'ютерів і комп'ютерної інформації (даних), авторського і суміжного прав.

Об'єктивна сторона кіберзлочинності характеризується виділенням чотирьох груп суспільно небезпечних діянь, а саме:

А) проти конфіденційності, цілісності та доступності комп'ютерних даних і систем, до них відносяться:

- протизаконний доступ, тобто одержання доступу до комп'ютерної системи в цілому чи будь-якої її частини без права на це, що може розглядатися як злочин, якщо він зроблений в обхід мір безпеки та з метою заволодіти комп'ютерними даними чи іншим злочинним наміром, або по відношенню до комп'ютерної системи, яка з'єднана з іншою комп'ютерною системою;

- протизаконне перехоплення даних, здійснюване з використанням технічних засобів без права на це;

- порушення цілісності даних (ушкодження, стирання, псування, зміна чи блокування комп'ютерних даних) без права на це, якщо такі діяння потягли за собою серйозні наслідки;

- втручання у функціонування системи, тобто створення серйозних перешкод функціонуванню комп'ютерної системи шляхом введення, передачі, ушкодження, видалення, псування, зміни чи блокування комп'ютерних даних;

- протиправне використання пристроїв: а) виробництво, продаж, придбання для використання, імпорт, оптовий продаж чи інші форми представлення у використання: 1) пристроїв, включаючи комп'ютерні програми, розроблені чи адаптовані, насамперед для цілей здійснення злочинів; 2) комп'ютерних паролів, кодів доступу чи інших подібних даних, за допомогою яких може бути отриманий доступ до комп'ютерної системи в цілому чи будь-якої її частині, з наміром використовувати їх з метою здійснення злочинів; б) володіння одним із предметів, що згадуються вище, з наміром використовувати його з метою здійснення злочинів;

Б) пов'язані з використанням комп'ютерів:

- підробка з використанням комп'ютерів – введення, зміна стирання, блокування комп'ютерних даних, що призводять до порушення автентичності даних з наміром, щоб вони розглядалися чи використовувалися в юридичних цілях, начебто вони залишаються справжніми, незалежно від того, чи є ці дані зрозумілими;

- шахрайство з використанням комп'ютерів - позбавлення іншої особи його власності шляхом введення, зміни, стирання, приховування комп'ютерних даних чи втручання у функціонування комп'ютера чи системи з метою неправомірного одержання економічної вигоди для себе чи для іншої особи;

В) пов'язані із змістом даних:

- правопорушення, пов'язані з дитячою порнографією (порнографічні матеріали, що візуально відображають участь неповнолітнього чи такого, який удавав себе неповнолітньою особою, у сексуально відвертих діях, а так само реалістичні зображення, що представляють неповнолітніх, що беруть участь у сексуально відвертих діях), а саме: виробництво з метою поширення через комп'ютерні системи; пропозиції чи представлення через комп'ютерні системи; придбання через комп'ютерну систему для себе чи для іншої особи; володіння дитячою порнографією, що знаходиться у комп'ютерній системі чи в середовищі для збереження комп'ютерних даних.

Г) пов'язані з порушенням авторських і суміжних прав:

- порушення авторського права, передбаченого нормами внутрішньодержавного законодавства, з урахуванням вимог Паризького акта від 24 липня 1971 року до Бернської конвенції про захист творів літератури і мистецтва, договори про авторське право Всесвітньої організації інтелектуальної власності (ВО1В), за виключенням будь-яких моральних прав, наданих цими конвенціями, коли такі дії навмисно відбуваються в комерційному масштабі і за допомогою комп'ютерної системи;

- порушення прав, пов'язаних з авторським правом (суміжних прав), передбачених нормами внутрішньодержавного законодавства, з урахуванням вимог: Міжнародної конвенції про захист прав споживачів, виробників звукозаписів і радіомовних організацій (Римська конвенція), Договору ВОІВ про виконавців і звукозаписи, за винятком будь-яких моральних прав, що представляються цими конвенціями, коли такі дії відбуваються навмисно в комерційному масштабі і з використанням комп'ютерної системи.

Як шкідливі наслідки перерахованих діянь проектом Конвенції визнається порушення прав законних користувачів комп'ютерної інформації, комп'ютерів, їхніх систем чи мереж. Встановлення як обов'язкової ознаки більш тяжких наслідків (матеріального збитку, протиправного використання отриманої комп'ютерної інформації і т.д.)

проектом залишено на розсуд держав. У цілому норми проекту не передбачають обов'язковість настання шкідливих наслідків.

Суб'єктом кіберзлочинів може бути фізична особа, що скоїла вказані вище дії. Виходячи з практики, що складається в різних країнах, стаття 12 проекту Конвенції вимагає встановлення відповідальності юридичних осіб за правопорушення, передбачені нею.

Суб''єктивна сторона кіберзлочинів характеризується прямим умислом.

Для України, яка має значний потенціал передових наукових знань, новітніх технологій, проблеми їх захисту від несанкціонованого доступу є надзвичайно актуальними. До недавнього часу, а саме до 1 вересня 2001 року, дати вступу в дію нового Кримінального кодексу України (ККУ), в Україні була відсутня можливість ефективно боротися з комп'ютерними злочинами. Не дивлячись на явну суспільну небезпеку, дані посягання не були протизаконними, тобто вони не згадувалися нашим кримінальним законодавством. Хоча ще до прийняття нового ККУ, в Україні була усвідомлена необхідність правової боротьби з комп'ютерною злочинністю.

Комп'ютерним злочинам присвячено розділ XVI "Злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж". І хоча, на відміну попереднього Кодексу, досягнуто певного прогресу щодо кваліфікації зазначеного виду злочинів, входження України до Європейського Співтовариства, виникла нагальна потреба реформування чинного законодавства. Тому, обравши свій шлях розбудови інформаційного суспільства, Україна також повинна здійснювати відповідні кроки щодо своєї інформаційної безпеки, яка згідно з Конституцією є невід'ємною складовою національної безпеки нашої держави.

ДЖЕРЕЛА ТА ЛІТЕРАТУРА

1. Гуцалюк М. Протидія комп'ютерній злочинності //Право України. – 2003. – №6. – С.114-117.

2. Ралемська І. Комп'ютерна злочинність: міфи і реальність //Міліція України. – 2001. - №18.

3. Батурин Ю.М. Проблемы копьютерного права. – М.: Юридическая литература, 1991.

4. Батурин Ю.М., Жодзишский А.М. Компьютерная преступность и компьютерная безопасность. - М.: Юридическая литература, 1991.

5. Машуков В.М. Компьютерное право: практическое руководство. – Львлв: Аверс, 1998.

6. Комп'ютерна злочинність: Навчальний посібник. – К.: Атіка, 2002.

7. Стефанчук Р.О. Комп'ютерний вірус //Юридична енциклопедія. Т.3. – К., 2001.

8. Коваленко М.М. Комп'ютерні віруси і захист інформації. – К., 1999.

9. Демешко О.В., Манжул К.В., Сорока Л.В. Охорона комп'ютерних технологій: Навчальний посібник. – Кіровоград, 2002.

10. Кузнецов В.Комп'ютерна інформація як предмет крадіжки //Право України. –

1999. - №7.

11. Лісовий Г. Кримінальна відповідальність за комп'ютерні злочини //Юридичний вісник України. – 2001. - №29.

12. Романюк Б., Гуцалюк М. Координація боротьби з комп'ютерною злочинністю – нагальна вимога сьогодення //Міліція України. – 2001. - №11.

13. Юрченко О.М. Зарубіжний досвід попередження шахрайства з використанням пластикових карт //Інформаційні технології та захист інформації. Збірник наукових праць. – Запоріжжя. – 1998. - №5

ВІДОМОСТІ ПРО АВТОРА

Сорока Лариса Володимирівна – кандидат правознавчих наук, доцент кафедри правознавства Кіровоградського державного педагогічного університету імені Володимира Винниченка.