

Комп'ютерна злочинність: нормативно-правове врегулювання

Куліш А. М., Тютюнник В. В.
Сумський державний університет, юридичний факультет
д.ю.н., проф.; студентка гр. Ю-74
e-mail: kafedraprivasumdu@ukr.net

Author of the report explores the question of legal regulation of this phenomenon as «computer crime», examines the stages of development of national legislation on matters related to settlement of relations in the field of Internet.

ВСТУП

Internet стає одним з основних джерел інформації для бізнесу, науки, засобом розповсюдження преси, юридичних актів, місцем проведення дозвілля та спілкування людей. Internet надає світовій спільноті можливість не тільки придбати продукти харчування чи книги, але й приймати участь в аукціонах, отримати грошову позику на основі електронного підпису, чи працювати в електронному офісі, працівники якого знаходяться за тисячі кілометрів один від одного.

ОСНОВНИЙ ТЕКСТ

Не дивлячись на те, що темпи розвитку інформаційних технологій в Україні через низку соціально-економічних проблем ще відстають від потреб сьогодення, Україна сміливо входить у світовий інформаційний простір. Разом з тим, стрімкий прорив суспільного розвитку в технологічній сфері залишив невирішеними ряд соціальних, організаційних, юридичних та інших проблем, пов'язаних з інформатизацією суспільства в цілому та з розвитком структури Internet зокрема. Інформаційний розвиток суспільства та запровадження на державному рівні в Україні використання мережі Internet та інших комп'ютерних систем в усіх сферах суспільного життя, поряд із позитивними здобутками, супроводжується і негативними явищами.

Особливу занепокоєність викликає збільшення кількості злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), комп'ютерних систем та мереж, як в світі, так і в Україні, оскільки такі злочини не лише гальмують позитивні тенденції розвитку, а й завдають шкоди суспільству, державі, суб'єктам інформаційних відносин в усіх сферах господарювання та окремим громадянам.

Потрібно зазначити, що наукові розвідки, присвячені цій проблематиці, вже започатковані такими авторами, як П.П. Андрушко, Ю.М. Батурін, О.І. Бойцов, О.Г. Волеводз, Б.В. Волженкін, В.Д. Гавловський, М.В. Гуцалюк, А.М. Жодзішський, В.О. Копилов, Ю.І. Ляпунов, В.Ю. Максимов, М.І. Панов, О.І. Панфілова, А.М. Попов, А.М. Ришелюк, В.С. Цимбалюк та іншими [1]. Надзвичайно цікавою є статистика, яку отримали американські експерти. В США середня вартість збитку складає: від одного фізичного пограбування банку - 3,2 тис. дол.; від одного шахрайства - 23 тис. дол.; від однієї комп'ютерної крадіжки - 500 тис. дол. [2]. І все це ускладнюється недосконалістю законодавства, передусім кримінального, а також недосконалістю державної системи боротьби з комп'ютерними злочинами. Разом з тим, з розвитком високих технологій, визначення «комп'ютерний злочин» поступово трансформувалося у поняття «злочини у сфері інформатизації», під котрим розуміються злочини, електронна обробка інформації при яких була знаряддям їх вчинення або їх об'єктом. У коло проблем, об'єднаних таким

поняттям, потрапили: шахрайство з кредитними магнітними картками, злочини у сфері телекомунікацій (шахрайство з оплатою міжнародних телефонних розмов), незаконне використання банківської мережі електронних платежів, програмне «піратство», шахрайство з використанням ігрових автоматів тощо. До цієї групи належать також й ті, що пов'язані з використанням доказів комп'ютерного походження при розслідуванні традиційних злочинів.

Комп'ютерна злочинність викликає занепокоєння світового співтовариства. Усвідомлюючи, що без створення відповідної правової основи ефективна протидія комп'ютерній злочинності неможлива, економічно розвинуті країни прийняли спеціальні законодавчі акти.

Перші закони стосовно комп'ютерних злочинів прийняті у 70-80 роки майже усіма індустріально розвинутими країнами. Серед них Computer Fraud and Abuse Act 1984 Сполучені Штати Америки, які найбільше страждають через комп'ютерні злочини. Але процес вдосконалення чинного законодавства не припиняється і сьогодні, що пояснюється стрімким розвитком інформаційних технологій [3].

В Україні інформаційна безпека закріплена в статті 17 Конституції України, поряд із суверенітетом, територіальною цілісністю та економічною безпекою, є найважливішою функцією держави і досягається шляхом розробки та впровадження сучасних безпечних інформаційних технологій, побудовою функціонально повної національної інформаційної інфраструктури, формуванням і розвитком інформаційних відносин тощо. Необхідною умовою цієї роботи повинна стати реальна кількісна оцінка стану комп'ютерної злочинності в Україні. Адже відомо, що більшість жертв комп'ютерних злочинів (комерційні банки, провайдери Internet послуг та ін.) не зацікавлені в їх афішуванні через можливий підрив іміджу та недовіру майбутніх партнерів і користувачів.

У Кримінальному Кодексі комп'ютерним правопорушенням присвячено розділ XVI «Злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж». З урахуванням входження України до Європейської спільноти, необхідності міжнародного співробітництва щодо переслідування комп'ютерних злочинів настала нагальна потреба реформування чинного законодавства згідно з Європейською угодою щодо комп'ютерних правопорушень, в якій досить чітко визначені види комп'ютерної злочинності та шляхи взаємодії урядів щодо регулювання міждержавного розшуку та боротьби з комп'ютерними правопорушеннями.

Характерними особливостями «комп'ютерних» є наступні:

- складність визначення розміру заподіяних збитків;
- значні фінансові витрати на проведення розслідування.

Слід зазначити, що сьогодні існує потреба у фахівцях, які мають необхідні для розкриття «комп'ютерних злочинів» навички та кваліфікацію, а також врегулювання національним законодавством багатьох питань, які виникають під час збору і документування інформації про «комп'ютерні злочини», а також у процесі проведення слідчих дій (наприклад, обшук комп'ютера, пошук слідів у комп'ютері, порядок зняття копій з машинних носіїв даних тощо).

«Комп'ютерні злочини» являють собою передбачені законодавством суспільно небезпечні дії, що посягають на встановлений в суспільстві порядок інформаційних відносин і скоєння їх відбувається з використанням електронно-обчислювальних машин, тобто комп'ютерів, систем та комп'ютерних мереж. Таким чином об'єктом злочину зазначених правопорушень виступають інформаційні відносини у суспільстві, що охороняються законом, а предметом – електронно-обчислювальні машини (комп'ютери), системи та комп'ютерні мережі, а також комп'ютерна інформація, що обробляється за їх допомогою.

В залежності від виду правопорушення особи, винні у вчиненні «комп'ютерних злочинів», несуть кримінальну, адміністративну, цивільно-правову, дисциплінарну або матеріальну відповідальність.

Щодо кримінальної відповідальності за «комп'ютерні злочини», то вона може наступати за шахрайство з використанням пластикових платіжних засобів (ч. 3 ст. 190 КК України); порушення авторського права і суміжних прав тощо (ст. 176 КК України).

Скоєння певних видів правопорушень, які можна класифікувати за «комп'ютерні злочини», спричиняють настання адміністративної відповідальності. Так, санкції у вигляді штрафу передбачено, наприклад, за поширення, використання, розголошення комерційної, конфіденційної інформації з метою спричинення збитків діловій репутації або майну підприємця (ст. 1643 Кодексу України про адміністративні правопорушення). Цивільно-правова відповідальність настає у разі, коли відповідні неправомірні діяння завдають матеріальної або моральної шкоди особі, але не мають ознак діянь, що переслідуються у кримінальному порядку (ст. 440, 4401 Цивільного кодексу України). Важливим етапом розвитку законодавства, що прискорив розвиток національної складової Internet, стало прийняття Закону України «Про телекомунікації», Закону України «Про захист персональних даних», Закону України «Про захист інформації в інформаційно-телекомунікаційних системах», «Про електронний підпис», а також Закону «Про інформацію».

Важливим етапом є проведення електронних наукових конференцій. Комп'ютерні конференції повинні активізувати й формування нормативних актів з питань інформаційної безпеки (у тому числі Кримінального кодексу), які б відповідали сучасним реаліям світового інформаційного простору, сприяли б розробці необхідного Інформаційного кодексу.

ВИСНОВКИ

Тільки в останні роки з'явилися роботи з проблем правової боротьби з комп'ютерною злочинністю і зовсім недавно вітчизняне законодавство стало на шлях боротьби з комп'ютерною злочинністю. І тому, представляється досить важливим розширити правову і законодавчу інформованість фахівців і посадових осіб, зацікавлених у боротьбі з комп'ютерними злочинами. Оскільки, високий ступінь залежності України від імпортичних комп'ютерів та інших інформаційних систем (з програмним забезпеченням включно), що вже сьогодні створює додаткові ризики організованих хакерських атак, здатних серйозно пошкодити урядові, банківські, енергетичні, транспортні та інші інформаційно-комунікаційні мережі, правове реагування на проблеми посилення комп'ютерної злочинності є надзвичайно важливим. Стимулом цього є також взяті Україною зобов'язання щодо інтеграції в світове співтовариство, в тому числі згідно з Програмою інтеграції України до Європейського Союзу.

ЛІТЕРАТУРА

- [1] Режим доступу: <http://media.parlament.org.ua/uploads/files/f945.RTF>
Петриченко О. Проблеми вдосконалення кримінального законодавства в сфері комп'ютерних технологій // Центр дослідження комп'ютерної преступности [Електронний ресурс]. – Режим доступу: <http://www.crime-research.ru/library/Oleg03.html>
Гуцалюк М. Проблеми організаційно-правового забезпечення захисту інформаційних систем в Internet [Електронний ресурс]. – Режим доступу: <http://www.bezpeka.com/ru/lib/spec/law/legal-protection-information-systems-Internet.html>

