ПРАВОВИЙ ЗАХИСТ ІНФОРМАЦІЙНИХ РЕСУРСІВ В УКРАЇНІ

Міщенко П., *студент гр. ІК-91*

Українські правознавці мало приділяли увагу законодавчому регулюванню правовому захисту інформаційних ресурсів, що зумовлювалося технічними чинниками: труднощами виявлення місця злочину, ще більшими труднощами фіксування порушення і викриття винних і суб'єктивними: відсутністю необхідних технічних (найчастіше вузькоспеціалізованих) знань у працівників правоохоронних органів, що ставало перешкодою на шляху створення необхідних правових норм.

Єдина норма, що донедавна передбачала відповідальність за комп'ютерні злочини - це стаття 198-1, введена в Кримінальний кодекс у 1992 році, досить широко охоплювала можливі форми і способи таких злочинів. Спроба криміналізації діянь, пов'язаних із зловживаннями комп'ютерами була зроблена на Україні в 1994 р., коли в липні був прийнятий Закон "Про захист інформації в автоматизованих системах".
Однак статті чинного Кримінального кодексу, а також вказані норми, не охоплювали весь спектр суспільно небезпечних діянь, які умовно називаються "злочини в сфері комп'ютерної інформації". Ця проблема вимагала подальшої розробки і вдосконалення кримінально-правових заходів регулювання.

Положення справ кардинально змінилося з прийняттям 5 квітня 2001 року нової редакції Кримінального кодексу України, що вступив у дію 1 вересня 2001 року.

Відповідальність за злочини в сфері комп'ютерної інформації в ньому присвячений розділ XVI "Злочину в сфері використання електронно-обчислювальних машин (комп'ютерів), систем і комп'ютерних мереж", що складає з трьох статей 361, 362, 363.

Під комп'ютерними злочинами розуміються суспільно небезпечні діяння, у яких комп'ютерна інформація являє собою предмет злочинного зазіхання (об'єкт - суспільні відносини з приводу користування, володіння і розпорядження комп'ютерною інформацією).

Треба уточнити, що Кримінальний кодекс України не розшифровує термін "комп'ютерна інформація", для з'ясування його необхідно звернутися до ст. 1 Закону: "Інформація в автоматизованій системі - сукупність усіх даних і програм, що використовуються в АС незалежно від способу їхнього фізичного і логічного представлення". Шляхом аналізу визначення "автоматизованої системи", даної в тій же статті, можна визначити, що комп'ютери відносяться до автоматизованих систем, тому що вони здійснюють автоматичну обробку даних, а в їхній склад входять технічні і програмні засоби.

Така відсильна структура статей КК не зовсім коректна, тому що вона може створити труднощі, як для розуміння норм, так і для їхнього

застосування: у тексті Кримінального кодексу України утримується термін "комп'ютерна інформація", а визначається вона через "автоматизовану систему", визначення якої утримується до того ж в іншому нормативному акті. На наш погляд необхідно ввести в ст. 361 указівку на те, що ж є комп'ютерною інформацією.

Проведене узагальнення практики розгляду судами справ про злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку засвідчило, що при розгляді зазначеної категорії справ окремі суди допускають помилки при кваліфікації дій винних осіб, відмежуванні одних злочинів від інших, вирішенні питань про наявність або відсутність кваліфікуючих ознак вчинених злочинів.

Зокрема, у суддів виникають труднощі при кваліфікації дій винних осіб, коли несанкціоноване втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж здійснювалося з корисливих мотивів, з метою викрадення чи заволодіння чужим майном. Зазначені дії і органи досудового слідства, і суди помилково кваліфікують лише за статтями Кримінального кодексу, якими передбачено відповідальність за вчинення комп'ютерних злочинів, не кваліфікуючи такі дії за сукупністю злочинів, у т. ч. і за відповідний злочин проти власності.

Призначаючи покарання за вчинення такого виду злочинів, суди іноді не застосовують обов'язкове додаткове покарання у виді конфіскації програмних та технічних засобів, за допомогою яких було вчинено злочин.

На наш погляд для покращення захисту інформаційних ресурсів та покращення ефективності боротьби в цій сфері на території України необхідно:

- постійно проводити дослідження проблем захищеності інформаційних систем в наукових працях;
- сприяти удосконаленню правового забезпечення захисту інформаційних систем: зміст законодавства повинен відповідати реальним умовам суспільства та реальному розвитку технічних засобів; поліпшити сам правотворчий процес;
- не повинні визнаватися законними нормативні акти, спрямовані на закріплення свавілля влади, чим би воно не мотивувалося;
- необхідно переймати досвід боротьби зі злочинами в інформацій та комп'ютерній сферах у більш досвідчених країн.

Наук. керівник - Кононенко О.Я., *ст. викладач кафедри права*