УДК 376:378
О.В. Лаба[1], Р.М. Кузнєцов[2]
[1]Волинський національний університет
імені Лесі Українки
[2]Луцький національний технічний
університет

ДО ПИТАННЯ ВИЗНАЧЕННЯ СУТНОСТІ КОМПЮТЕРНИХ ЗЛОЧИНІВ В УКРАЇНІ

В даній статті досліджуються актуальні питання сутності злочинів у сфері комп'ютерної інформації. Розглянуто елементи складу злочину, проаналізовано предмет, види комп'ютерних злочинів в Україні.
Ключові слова: інформація, комп'ютерні злочини.

Людська цивілізація на межі тисячоліть вступила в еру інформації. Світовою системою комп'ютерних комунікацій щодня користуються сотні мільйонів людей. Інформація стає вирішальним чинником у багатьох галузях народного господарства. Саме вона є продуктом наукової та дослідницької діяльності, необхідним компонентом у ході наукових досліджень. Зростає потреба у засобах структурування, накопичення, зберігання, пошуку та передачі інформації – задоволення саме цих потреб і є метою створення та розвитку інформаційних мереж.

Стрімкий розвиток інформаційних технологій, окрім позитивних моментів, приховує в собі потенційну загрозу. Таким чином, інформаційна сфера сьогодні є одним із основних об'єктів злочинних посягань.

Громадськість усе більше цікавиться даним питанням, оскільки кожний власник або користувач комп'ютера, телефону, модему, пластикової картки є потенційним потерпілим, якого можуть очікувати тяжкі наслідки в разі вчинення злочину, особливо у державному, комерційному та промисловому секторі, де можливі великі фінансові затрати. Тому надзвичайно актуальним є питання щодо визначення сутності комп'ютерних злочинів та розробки ефективних методів боротьби із ними.

Багато явищ соціального життя все більшою мірою знаходить відображення в так званому «віртуальному світі» - в тих інформаційних сферах, носіями яких виступають як засоби масової інформації, так і глобальні комп'ютерні телекомунікаційні мережі та системи. Зокрема С.С. Овчинський відносить до інформаційних сфер засоби масової інформації, телекомунікації та зв'язку, глобальні комп'ютерні мережі, індустрію різних інформаційних послуг [7; 312-313].

Науково-технічна революція призвела, до серйозних змін у суспільстві, найважливішими з яких є поява нового виду суспільних відносин та суспільних ресурсів – інформаційних, які мають свою специфіку:

вони не матеріальні і не залежать від носія інформації;

їх використання дозволяє набагато знизити витрати інших видів ресурсів, що веде до великої економії коштів;

процес їх створення та використання здійснюється за допомогою комп'ютерної техніки [3, 7].

Виходячи з цього, ми можемо визначити поняття нових інформаційних технологій як сукупність методів та засобів реалізації інформаційних процесів у різних галузях людської діяльності, інакше кажучи, засобів реалізації інформаційної діяльності людини. Засобами реалізації цієї діяльності є електронно-обчислювальна техніка, засоби телекомунікації, системи зв'язку,розвиток яких постійно стимулюється прогресом інформаційних відносин.

При характеристиці правопорушень, які вчиняються з використанням нових інформаційних технологій, ми вважаємо доцільним поєднати процес формування інформаційного суспільства з унікальним співіснуванням комп'ютерів та комунікацій. Основною ознакою, яка відносить інформацію до сфери нових технологій є електронна обробка інформації (з метою збереження, передачі, копіювання, переробки, знищення тощо) та використання мереж зв'язку, які в більшості випадків є глобальними.

Першочерговим питанням, яке постало перед суспільством є визначення статусу суспільних інформаційних відносин та шляхів їх правового регулювання з метою уникнення, зменшення, запобігання та подолання юридичними методами негативних проявів інформаційного суспільства

та стимулювання бажаних для людини, держави та суспільства правил поведінки його суб'єктів – учасників інформаційних відносин.

Комп'ютерна злочинність - це міжнародне явище, рівень якого тісно пов'язаний з економічним рівнем розвитку суспільства у різних державах та регіонах. При цьому менш розвинуті у технічному відношенні країни завдяки діяльності міжнародних правоохоронних організацій мають можливість використати досвід більш розвинутих країн для запобігання та викриття комп'ютерних злочинів. Загальні тенденції, злочинні засоби та заходи запобігання, що ґрунтуються на єдності технічної, програмної та методичної бази цих злочинів, у різні проміжки часу є однаковими у різних країнах [2].

Під час зародження даного явища найбільш поширеним було поняття «комп'ютерний злочин», під яким у більшості випадків розуміли протиправні діяння у сфері комп'ютерної інформації. Проте з розвитком комп'ютерної техніки, телекомунікаційних мереж, технологій обробки, збереження, формування, передачі, кодування інформації визначення «комп'ютерний злочин» поступово трансформувалось у поняття «злочини у сфері сучасних або нових інформаційних технологій». Даний термін підкреслює, що, по-перше, названі правовідносини пов'язані зі створенням інформаційних ресурсів, їх обігом і поширенням, використанням, зберіганням та захистом і регулюються законодавством України у сфері інформаційних відносин. По-друге, галузь цих відносин окреслена особливостями обробки та передачі інформації [4, 17].

Таким чином, під злочинами у сфері нових інформаційних технологій ми розуміємо суспільно небезпечні діяння, які заборонені кримінальним законом під загрозою покарання, скоєні у сфері інформаційних правовідносин, пов'язаних з використанням електронної обробки інформації та (або) засобів комунікації.

Характерними рисами злочинів в галузі нових інформаційних технологій на нашу думку варто виділити:

як правило, міжнародний характер злочину (виходить за рамки кордону однієї держави);

труднощі у визначенні «місця знаходження» злочину;

слабкі зв'язки між ланками в системі до-казів;

неможливість спостерігати і фіксувати докази візуально;

широке використання злочинцями засобів шифрування інформації.

Виходячи з аналізу наукових робіт вітчизняних та закордонних науковців, можна виділити 2 основні напрями наукової думки:

до комп'ютерних злочинів відносять дії, в яких комп'ютер є об'єктом або засобом злочину. При цьому, крадіжка комп'ютера розглядається як один із способів скоєння комп'ютерних злочинів.

до комп'ютерних злочинів відносяться лише протизаконні дії у сфері автоматизованої обробки інформації. Вони виділяють у якості головної класифікуючої ознаки єдність способів, знаряддя, об'єктів посягання [1].

Як відомо, відповідно до Кримінального кодексу України, склад злочину складається з 4 елементів:

суб'єкт злочину

суб'єктивна сторона

об'єкт злочину

об'єктивна сторона.

Суб'єктами комп'ютерної злочинності (комп'ютерним злочинцем) найчастіше є молоді люди, віком від 15 років, більшість з них вчаться у коледжі, інституті, або мають вищу освіту, мають коефіцієнт інтелекту (IQ) вище від середнього. Особистими характеристиками особи злочинця є активна життєва позиція, оригінальність мислення та поведінки, обережність, уважність. Зосереджують увагу на розумінні, передбаченні й управлінні процесами.

Ми пропонуємо виділити три групи злочинців:

а) особи, які не мають трудових, стосунків з організацією, комп'ютерну систему якої вони використовують у злочинних діях, але мають з нею певні зв'язки;

б) співробітники організацій (нерідко займають там відповідальні посади), автоматизовані системи яких вони використовують у злочинних діях;

в) співробітники, які користуються ЕОМ і зловживають своїм становищем/

Суб'єктивна сторона цих злочинів передбачає, як правило, умисну вину. Хоч можлива і необережність — при порушенні правил експлуатації автоматизованих електронно-обчислювальних систем (ст. 363 ККУ) [5].

Мотиви і цілі можуть бути різними — помста, заздрість, прагнення до володіння інформацією. Якщо ж, наприклад, викрадення інформації, вчиняється з корисливих мотивів і містить ознаки складу шахрайства, вчинене слід кваліфікувати за сукупністю злочинів — за статтями 362 і 190 ККУ [5].

Родовим об'єктом цих злочинів є суспільні відносини у сфері безпеки комп'ютерної інформації і нормального функціонування електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж.

У складі злочину інформація на наш погляд може виступати у двох аспектах: як предмет злочину та як засіб його вчинення.

До предметів злочину ми пропонуємо віднести:

електронно-обчислювальна машина (ЕОМ) — комп'ютер — комплекс технічних засобів, призначених для автоматичної обробки інформації в процесі вирішення обчислювальних та інформаційних задач;

автоматизовані комп'ютерні системи (АКС) — сукупність взаємопов'язаних ЕОМ, периферійного обладнання та програмного забезпечення, призначених для автоматизації прийому, зберігання, обробки, пошуку і видачі інформації споживачам. Комп'ютерні системи можуть бути регіонального та галузевого характеру;

комп'ютерні мережі (мережа ЕОМ) — це з'єднання декількох комп'ютерів (ЕОМ) та комп'ютерних систем, що взаємопов'язані і розташовані на фіксованій території та орієнтовані на колективне використання загальномережових ресурсів. Комп'ютерні мережі передбачають спільне використання ресурсів обчислювальних центрів (ОЦ), запуск загальних програм, які входять до комп'ютерних систем;

носії комп'ютерної інформації — фізичні об'єкти, машинні носії, призначені для постійного зберігання, перенесення і обробки комп'ютерної інформації. До них відносяться гнучкі магнітні диски (дискети), жорсткі магнітні диски (вінчестери), касетні магнітні стрічки (стримери), магнітні барабани, магнітні карти тощо;

комп'ютерна інформація — це текстова, цифрова, графічна чи інша інформація (дані, відомості) про осіб, предмети, події, яка існує в електронному виді, зберігається на відповідних електронних носіях і може використовуватися, оброблятися або змінюватися за допомогою ЕОМ.

Об'єктивна сторона цих злочинів може виражатися в активних діях (наприклад, в незаконному втручанні в роботу автоматизованих електронно-обчислювальних машин (комп'ютерів), їх систем чи комп'ютерних мереж, в розповсюдженні комп'ютерного вірусу), а також в злочинній бездіяльності, наприклад, при порушенні правил експлуатації автоматизованих електронно-обчислювальних машин, їх систем чи комп'ютерних мереж.

Кримінальним кодексом України передбачено такі види злочинів:

Незаконне втручання в роботу електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж (ст. 361 ККУ).

Об'єктивна сторона даного виду злочину виражається в 2 формах:

1) незаконне втручання в роботу автоматизованих електронно-обчислювальних машин, їх систем чи комп'ютерних мереж.

Втручання полягає у проникненні до цих машин, їх систем чи мереж і вчиненні дій, які порушують режим роботи ЕОМ, припиняють (частково чи у повному обсязі) їх роботу.

2) розповсюдження комп'ютерного вірусу шляхом застосування програмних і технічних засобів, призначених для незаконного проникнення в ці машини, системи чи комп'ютерні мережі та здатних спричинити перекручення або знищення комп'ютерної інформації чи носіїв такої інформації.

Викрадення, привласнення, вимагання комп'ютерної інформації або заволодіння нею шляхом шахрайства чи зловживання службовим становищем (ст. 362 ККУ), що передбачає активні дії, які виражаються у викраденні, привласненні, вимаганні комп'ютерної інформації або у заволодінні нею шляхом шахрайства чи зловживання службовою особою своїм службовим становищем. Внаслідок вчинення цих дій власник чи інша особа, яка володіє комп'ютерною інформацією, позбавляються такої інформації, вона вибуває з їх володіння і не може ними використовуватися.

Об'єктивні ознаки викрадення, привласнення, вимагання комп'ютерної інформації, заволодіння нею шляхом шахрайства потрібно трактувати так само, як і в злочинах проти власності — за статтями 185, 186, 189, 190 і 191 ККУ.

Порушення правил експлуатації автоматизованих електронно-обчислювальних систем (ст. 363 ККУ).

Правила експлуатації ЕОМ — технічні правила, які регламентують порядок використання таких машин, збереження комп'ютерної інформації, а також забезпечення засобів захисту автоматизованих електронно-обчислювальних машин. Порушення правил може виражатися як в активних діях, коли особа діє всупереч розпорядженням, закріпленим в правилах, так і у формі бездіяльності — невиконання обов'язків з належного використання (обслуговування) ЕОМ.

Об'єктивна сторона цього злочину передбачає не тільки вчинення діяння (порушення правил експлуатації ЕОМ), а й настання суспільно небезпечних наслідків у вигляді: викрадення, перекручення чи знищення комп'ютерної інформації, засобів її захисту, або незаконного копіювання комп'ютерної інформації, або істотного порушення роботи таких машин, їх систем чи комп'ютерних мереж [6].

Підсумовуючи вищесказане, слід наголосити, що усі протиправні діяння у сфері нових інформаційних технологій, передбачені і класифіковані в міжнародному праві як комп'ютерні, слід розуміти під терміном «злочини у сфері нових інформаційних технологій».

До них слід відносити: комп'ютерне шпигунство, комп'ютерні диверсії, комп'ютерний тероризм, крадіжка комп'ютерних послуг, махінації та маніпулювання системою обробки даних, а також крадіжка фінансових засобів і підробка документів, порушення державної і приватної таємниці, протиправне копіювання програмних продуктів, яке порушує авторське та інші права тощо.

Стосовно інформації, як головного об'єкта посягань даного виду правопорушень, слід зазначити, що в сучасних поглядах науковців на її роль і сутність буде доцільним розуміти під терміном «комп'ютерна інформація» усі дані та програми, що використовуються в електронно-обчислювальних машинах (комп'ютерах), системах та комп'ютерних мережах та мають власника, що встановлює правила її використання.

1. Батурин Ю. М., Жодзинский А. М. Компьютерная преступность и компьютерная безопасность. – М.: Юрид. литература, 1999. – 158 с.
2. Біленчук П.Д. Організована транснаціональна комп'ютерна злочинність: глобальна проблема третього тисячоліття. – К: Національна академія внутрішніх справ України. – 2002.
3. Вехов Б. В. Компьютерные преступления: способы совершения и раскрытия. – М.: Право и закон, 1996. – 182 с.
4. Використання оперативно-технічних засобів у протидії злочинам, що вчиняються у сфері нових інформаційних технологій: монографія / І. Я. Харабержош, В. Я. Мацюк, В. А. Некрасов, О. І. Харабержош. – К.: КНТ, 2007. – 196 с.
5. Кримінальне право України: Особлива частина: Підручник / М. І. Бажанов, Ю. В. Баулін, В. І. Борисов та ін.; За ред. проф. М. І. Бажанова , В. В. Сташиса, В. Я. Тація. - 2-е вид., перероб. і доп. — К.: Юрінком Інтер, 2005. — 544 с.
6. Кримінальний кодекс України. – К.: ВЕЛЕС, 2006. – 152 с.
7. Овчинський С. С. Оперативно-розыскная информация / Под. ред.. А. С. Овчинского и В.С. Овчинского. – М.:ИНФРА-М, 2000. – 367 с.
8. Юридична енциклопедія: В 6 т. /Редкол.: Ю. С. Шемшученко (голова редкол.) та ін. — К.: «Укр. енцикл.», 1998. – Т.3