РОЗДІЛ 15
СУЧАСНІ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНІ ТЕХНОЛОГІЇ У ПРАВОВІЙ СФЕРІ

Ємельянов С. Л.
Національний університет «Одеська юридична академія»,
в. о. завідувача кафедрою інформаційних технологій,
кандидат технічних наук, доцент,
Член-кореспондент Академії зв'язку України

ПРОБЛЕМА БОРОТЬБИ ІЗ КОМП'ЮТЕРНОЮ ЗЛОЧИННІСТЮ В УКРАЇНІ

Досягнення, пов' язані із розвитком інформаційного суспільства та активним впровадженням інформаційно-комунікаційних технологій (ІКТ) в усі сфери життєдіяльності людини, мають не тільки позитивні, але й негативні аспекти.

Фахівці в області ІКТ єдині в думці, що, як свого часу досягнення ядерної фізики викликали небезпеку ядерної війни, так і широка інформатизація (комп'ютеризація) стала джерелом нових загроз суспільству, державі і особі. З'явилися нові терміни і явища «*Інформаційна зброя*», «*Інформаційна війна*», «*Промислове (комерційне) шпигунство*», «***Комп'ютерна злочинність***» тощо. (Емельянов С. Л. Основы информационной безопасности: [конспект лекций] / С. Л. Емельянов. – Вид-во «Юридична література», ОНЮА, 2003. – С.3).

У цьому сенсі досить **актуальною** є проблема боротьби із комп'ютерною злочинністю, яка може мати суттєвий вплив на стан інформаційної безпеки держави, суспільства, окремих юридичних та фізичних осіб, які широко використовують сучасні ІКТ у своїй повсякденній діяльності.

Історично термін «комп'ютерний злочин» (computer crime) уперше з'явився в американській пресі на початку 60-их рр. минулого століття, коли були виявлені перші випадки злочинів, скоєних з використанням ЕОМ. Пізніше цей термін став використовуватися і у правоохоронних органах багатьох країн світу. Також з'явилися інші термінологічні дефініції: інформаційні злочини, злочини у сфері високих технологій, кіберзлочини тощо. З цього моменту почалася наукова полеміка, що йде й понині, стосовно питання, чи має право на життя термін »комп'ютерний злочин« і які саме злочини слід відносити до цієї категорії. При цьому у підході до даної проблеми сформувалися дві протилежні точки зору (Мазуров В. А. Компьютерные преступления: классификация и способы противодействия: Учебно-практическое пособие. – М.: «Палеотип», «Логос», 2002. – С.6).

Одні автори вважають, що використання цього терміну недоречно, адже злочини не прийнято диференціювати по способах та видах технічних засобів, за допомогою яких вони скоюються. При цьому багато традиційних злочинів лише модифікуються через залучення в них засобів обчислювальної техніки, і тому вірніше говорити про комп'ютерні аспекти злочинів, не виділяючи їх у відокремлену групу злочинів.

Також існує думка, що комп'ютерну злочинність слід розглядати як частину «білокомірцевої«, економічної чи організованої злочинності (Гудков П. Б. Компьютерная преступность: возникновение, современное состояние и тенденции / П. Б. Гудков // Защита информации. Конфидент.– 1995. – № 4(2). – С.17– 25.)

Інші науковці визнають правомірність використання цього терміну, адже він вже сприйнят як вітчизняною, так і закордонною наукою та судовою практикою.

Загальноприйнятого визначення комп'ютерної злочинності не існує. Ці злочини тісно пов'язані з ЕОМ та комп'ютерними мережами. Вони часто містять у собі цілу низку незаконних дій, здійснених за допомогою системи обробки даних, або проти неї. Термін охоплює комп'ютер, допоміжне устаткування, програмне забезпечення, засоби зв'язку та телекомунікацій, інформаційні мережі та бази даних, комп'ютерну інформацію тощо. Тому під терміном «комп'ютерна злочинність» зараз розуміються всі злочинні дії, при яких електронне опрацювання інформації було знаряддям їх вчинення або їх об'єктом.

Зазначимо, що український законодавець обрав проміжну позицію між зазначеними вище протилежними точками зору, застосувавши у ККУ назву Розділу XVI «Злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку» (Кримінальний кодекс України від 5 квітня 2001 року // ВВР.– 2001.– № 25-26. – Ст.131). Зараз у кримінальному законодавстві України маємо 6 складів комп'ютерних злочинів (ст. ст.361–3631). Проте аналіз вітчизняної судової практики свідчить, що не всі зазначені норми «працюють» належним чином (Судова практика розгляду справ про злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), автоматизованих систем та комп'ютерних мереж і мереж електрозв'язку. – [Електронний ресурс Верховного Суду України]. – Режим доступу: http://www. scourt. gov. ua/clients/vs. nsf/0/C8EABE11C12BFF3 AC 22576EE004F1E65?OpenDocument).

Звідси бачимо, що в Україні найбільш поширеним в цій сфері є злочини, відповідальність за які передбачено ст.361 ККУ («Несанкціоноване втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку»), та ст.362 ККУ, в якій передбачено відповідальність за несанкціоновані дії з інформацією, яка оброблюється в ЕОМ, АС, комп'ютерних мережах або

зберігається на носіях такої інформації, вчинені особою, яка має право доступу до неї.

Проте у 2007–2008 рр. суди не розглядали кримінальних справ про злочини, передбачені статтями 363 («Порушення правил експлуатації ЕОМ, АС, комп'ютерних мереж чи мереж електрозв'язку або порядку чи правил захисту інформації, яка в них оброблюється») та 3631 ККУ. («Перешкоджання роботі ЕОМ (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку шляхом масового розповсюдження повідомлень електрозв'язку»), що є певним свідоцтвом недосконалості цих норм.

Таким чином, 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 ККУ, якими передбачено відповідальність за вчинення комп'ютерних злочинів, не кваліфікуючи такі дії за сукупністю злочинів, у тому числі й за відповідний злочин проти власності.

Якутко В. Ф.

Национальный университет «Одесская юридическая академия», доцент кафедры информационных технологий, кандидат технических наук, доцент

ИСПОЛЬЗОВАНИЕ ВИДЕОКОНФЕРЕНЦСВЯЗИ В СУДЕБНОМ ПРОЦЕССЕ

Эффективность судебной заключается не только в беспристрастном и справедливом рассмотрении дела судом, но и в оперативности такого рассмотрения. Оперативность может быть достигнута, в первую очередь, путем технической модернизации судебного процесса.

Важным техническим решением является использование во время судебных заседаний системы видеоконференцсвязи, которая позволит избежать затягивания судебного рассмотрения дела, в связи с невозможностью того или иного участника процесса прибыть в зал судебного заседания.