УДК 002.6+347,777+343.50/53+35.078+342.7

Цимбалюк В. С.

ПРИЧИНИ ЛАТЕНТНОСТІ КОМП'ЮТЕРНОЇ ЗЛОЧИННОСТІ

Стаття присвячена розглядові окремих питань щодо проблематики латентності комп'ютерної злочинності в Україні та за кордоном.

Будь-яке масове соціальне явище набуває суспільного усвідомлення за наявності відповідної критичної маси інформації (відомостей, даних, знань), що зменшує рівень ентропії (невизначеності) окремих індивідів, соціальних організацій (спільнот), суспільства в цілому, держави, світового співтовариства. Глобальна інформатизація, формування на її основі світової інформаційної цивілізації на рубежі XX—XXI століття породила у злочинному світі нове явище — комп'ютерну злочинність: широкомасштабне, активне пристосування комп'ютерних технологій і телекомунікацій для вчинення "традиційних" злочинів, а також формування нових напрямів використання зазначених технологій для досягнення злочинної мети.

Сьогодні кількість інформації про злочини, що вчиняються з використанням комп'ютерних технологій і телекомунікацій (комп'ютерні злочини), набула такої соціальної критичної маси, що дозволяє виділити її в окремий аспект дослідження. За оцінками експертів, виникає реальна загроза окремим інтересам не тільки конкретної людини, приватних та державних структур, а й національній безпеці окремих держав і людства в цілому.

Згідно з даними Комісії з попередження злочинності та кримінального права Організації Об'єднаних Націй, щорічний економічний збиток від комп'ютерних злочинів, за оцінками експертів, становить мільярди доларів США. (Див.: Юридичний вісник України. 1998. 5—11.03.— С. 7).

Як свідчить практика багатьох країн, зростання комп'ютерної злочинності є однією з характерних і закономірних ознак сучасного стану глобального інформаційного суспільства. У сучасній кримінології щодо комп'ютерної злочинності пропонується визначення її видів.

Одним із проявів комп'ютерної злочинності є нова форма шпигунства із застосуванням комп'ютерних технологій. Відомо, що у більшості економічно заможних господарських організацій левова частка інформації існує в електронному вигляді, в комп'ютерах. Тому сьогодні комп'ютерне шпигунство використовується як універсальний засіб добування інформації про конкурентів і поєднання його з іншими електронними засобами розвідки (радіо, телебачення тощо).

Концентрація в автоматизованих базах даних різної інформації, як правило, означає сприятливі умови для здійснення актів саботажу. Шантаж (у тому числі з метою здирства тощо) за допомогою комп'ютерів здійснюється оперативніше і легше, ніж традиційними методами.

Новим масовим антисоціальним проявом у "кіберпросторі" є несанкціоноване проникнення до автоматизованих (комп'ютерних) систем, що працюють у телекомунікаційній мережі Інтернет. Це соціальне явище набуло умовної назви — "хакерство". Осіб, які вчиняють такі дії називають "хакерами". Однією з причин цього явища є недбале ставлення власників комп'ютерних інформаційних систем до комплексного їх захисту: технічними, організаційними та правовими засобами. Так, наприклад, проведені у Китаї агентствами безпеки дослідження комп'ютерних мереж засвідчили, що 95 % місцевих комп'ютерних систем, підключених до Інтернету, були піддані атакам хакерів. Незахищеними від несанкціонованого доступу опинились майже всі. (Computer World. Київ. 1999. 3 лютого. С. 1,29).

У США офіційні представники американської армії стурбовані тим, що досвідчені хакери ("кіберкриміналітет"), можуть отримати контроль над основними системами зброї (танків, літаків, військових кораблів тощо). Про це було заявлено на конференції Army Directors of Information Management Conference в Х'юстоні. (Computer World Київ. 2000, 29 березня. С. 24).

З проявом організованої злочинності у кіберпросторі окремі проблеми мають особливо негативний для суспільства характер. Дослідження у різних країнах свідчать, що найбільший суспільний резонанс викликають комп'ютерні злочини, що мають ознаки вчинення організованими угрупованнями.

Найбільшу увагу на цьому зосереджують у США. Виникає питання: чому сьогодні саме у США так багато говорять про комп'ютерну злочинність публічно, відкрито і чи завжди це так було? США — батьківщина масової комп'ютеризації та інформатизації, і, звісно, там виникла критична маса соціальної інформації щодо усвідомлення загрози комп'ютерної злочинності для суспільства. Ментальність суспільства цієї країни полягає в тому,

що там розуміють просту істину — колективний розум у відкритому обговоренні дозволить відпрацювати ефективні шляхи подолання суспільних проблем, зменшити негативний вплив останніх на інформаційне суспільство.

А яке суспільне ставлення до комп'ютерної злочинності в Україні? Введення у 1994 році спеціальної норми у статті 198[1] Кримінального кодексу України визначило рівень ентропії органів державної влади щодо суспільної небезпеки комп'ютерної злочинності в країні. Це викликало потребу додаткового переосмислення вітчизняної практики і теорії, кримінально-правових уявлень, зокрема щодо інформаційних (комп'ютерних) злочинів. У свою чергу це стало підставою легального формування кримінологічних та криміналістичних досліджень пов'язаних із протиправним посяганням на суспільні відносини щодо комп'ютеризованих інформаційних систем та на інформацію як предмети делікту (правопорушення).

Щодо нашої країни, то необхідність кримінально-правових заборон у цій сфері передувала визнанню суспільством, а потім і законодавством факту існування інформації в автоматизованих (комп'ютерних) системах як товару, а, отже, як різновиду майна, тобто об'єкта суспільних відносин, різновиду права власності (права інтелектуальної власності). Це зафіксовано у Законах України "Про інформацію", "Про авторське право і суміжні права", "Про захист інформації в автоматизованих системах".

При розгляді проблем комп'ютерної злочинності в кримінологічному аспекті основна увага в цій публікації приділятиметься з'ясуванню причин та умов її латентності (прихованості) — соціального явища, яке не виявляє себе помітними публічно ознаками на певному часовому відтинку. За експертними оцінками, сьогодні латентність комп'ютерної злочинності у світі сягає близько 95—90 %.

При порівнянні показників боротьби з комп'ютерною злочинністю в інших країнах та в Україні викликає підозру низький рівень комп'ютерної злочинності в нашій країні. За офіційними даними, протягом другої половини 90-х років кількість злочинів, що вчиняються за допомогою комп'ютерних технологій, в Україні визначається в межах десятків протягом кожного року. В той же час, із конфіденційних джерел відомо про понад 500 випадків, які можуть бути кваліфіковані як комп'ютерні злочини, але не заявлених до правоохоронних органів.

Звичайно, можна аргументувати це низьким рівнем комп'ютеризації в нашій країні. Але можна аргументувати й рівнем суспільної ентропії у владних структурах (зокрема, в таких правоохоронних органах, як прокуратура, суди та інших) щодо розуміння та усвідомлення комп'ютерної злочинності як суспільне небезпечного явища.

Загальновизнаною є одна причина латентності комп'ютерної злочинності: у більшості випадків через небажання підриву репутації потерпілі неохоче повідомляють (якщо роблять це взагалі) правоохоронні органи про факти злочинних посягань на їхні комп'ютерні системи.

Проте у цього явища існує багато причин другого порядку. Звернемо увагу на когнітологічний (психологічний, пізнавальний, інформаційний) аспект — ентропію (невизначеність через брак знань) щодо сутності явища. У цьому аспекті визначаються такі суб'єкти: персонал, який забезпечує технічний захист інформації в автоматизованих (комп'ютерних) системах, та широкий загал юристів, у тому числі практичних працівників правоохоронних органів, покликаних професійно вести боротьбу зі злочинністю.

Серед працівників підрозділів технічного захисту інформаційних автоматизованих (комп'ютерних) систем (АС) та системних адміністраторів комп'ютерних систем і мереж існує професійний, психологічний феномен, сформований під впливом технічної освіти: фаховий технократичний світогляд, в основі якого лежить сформована думка, що всі проблеми захисту інформації можна розв'язати за допомогою переважно комп'ютерних "замків" — програмно-математичних і технічних засобів, тобто за допомогою технічного захисту інформації. Одразу зазначимо, що при дослідженні проблематики не заперечується значимість технічного захисту комп'ютерних систем.

Визначимо ще одну проблему, яка впливає на латентність комп'ютерної злочинності: більшість технократів забувають чи не знають прописної істини — всі інженерно-технічні засоби захисту, створені розумом і руками одних, з часом (за бажання або потреби) обов'язково будуть зруйновані чи подолані іншими, особливо коли за це береться кілька людей, до того ж, об'єднаних у злочинну організацію.

Часто злочинці, знаючи таку психологію "захисників" комп'ютерних систем (служб технічного захисту, адміністраторів комп'ютерної мережі), нахабніють такою мірою, що втрачають пильність, оскільки переконані, що притягуватись до відповідальності за законодавством не будуть, а, отже, не будуть покарані.

Як свідчить практика, отримавши опір технічної системи захисту щодо несанкціонованого доступу до комп'ютерної системи, злочинці шукають нову інформацію для подолання своєї ентропії — нових знань щодо способів і шляхів вчинення злочину. Зупинити їх може лише покарання через державний суд чи реальна загроза покарання у суді.

Великого значення у попередженні, виявленні та боротьбі з комп'ютерними злочинами має виявлення і дослідження причин їх вчинення та напра-

цювання відповідних рекомендацій протидії, зокрема, за участю правоохоронних органів. Але коли потерпілі мовчатимуть про напади на їхні комп'ютерні системи, чи можна вести мову про ефективну боротьбу зі зловмисниками юридичними засобами? З цього випливає інша проблема: як подолати ентропію у працівників правоохоронних органів, якщо їм не давати інформації і не формувати стимулів до отримання знань та навичок боротьби з комп'ютерною злочинністю.

Дослідження, проведені в Україні, свідчать, що широкий загал фахівців, чия діяльність пов'язана з комп'ютерними технологіями, не мають не тільки відповідних навичок, а й правових знань: як правильно документувати дії порушника; як діяти до втручання у справу правоохоронців тощо. Це зумовлено тим, що в більшості неюридичних ВНЗ правова підготовка, як правило, обмежується єдиною юридичною навчальною дисципліною — "Основи права". До того ж, часто ця навчальна дисципліна не містить тем, які б розкривали юридичну сутність та особливості змісту комп'ютерних правопорушень, зокрема таких, що визначаються як злочини. З цим пов'язана ще одна проблема — відсутність широкого загалу фахівців-юристів, які б могли кваліфіковано, комплексно донести проблематику комп'ютерної злочинності та правових засобів протидії їй. Таким чином, формується замкнене коло щодо подолання соціальної ентропії до протидії комп'ютерній злочинності.

Наступний аспект — це формування правосвідомості окремих індивідів, учасників суспільних інформаційних відносин. Недостатній обсяг юридичних знань про особливості суспільних відносин в умовах інформатизації створює інформаційний вакуум при формуванні правосвідомості програмістів-математиків, інженерів-електронників, інженерів-програмістів комп'ютерних (електронно-обчислювальних) систем. Необхідно звернути увагу на те, що це саме те середовище, з якого, переважно, виходять не тільки фахівці з технічного захисту інформації в АС, а й висококваліфіковані хакери — зловмисники (фрікери, крекери, кракери тощо), особи, які часто-густо є центральними фігурами вчинення найбільш соціальне небезпечних правопорушень із використанням комп'ютерних технологій.

Наступна проблема має відношення до правознавства. Юридичні знання, сформовані за часів, коли комп'ютер був екзотикою, створили комплекс суспільної ентропії в колах правознавців (у тому числі в середовищі працівників правоохоронних органів, суду, прокуратури) до особливостей нових інформаційних правовідносин в умовах комп'ютеризації, інформатизації. Сьогодні критична маса правової інформації до світового емпіричного матеріалу (зокрема, щодо порушення роботи комп'ютерних автоматизованих інформаційних систем) потребує відповідно цілеспрямованого, комплексного, системного наукового осмислення на міжгалузевому науковому рівні, адаптації до сучасних умов інформаційного суспільства.

В основному наукові розробки, предметом яких є суспільні інформаційні відносини, в нашій країні проводяться переважно в межах таких традиційних юридичних інституцій, як право інтелектуальної власності, авторське право, антимонопольне право та недопущення недобросовісної конкуренції у підприємницькій діяльності. Це породжує ще одну проблему: недостатній рівень комплексних вітчизняних наукових напрацювань щодо боротьби з комп'ютерними правопорушеннями в межах традиційних провідних галузей правознавства: цивільного, адміністративного, кримінального, трудового. Вузькогалузевим підходом до з'ясування сутності комп'ютерних правопорушень створено ентропію у юристів-практиків щодо інформатизації та ентропію і недовіру технократів щодо можливостей права у боротьбі з такими правопорушеннями.

Поступ України до інформаційного суспільства зумовив необхідність формування нових багатоаспектних комплексних наукових дисциплін. Серед таких на провідну роль сьогодні претендують: інформаційне право; правова інформатика, у складі якої криміналістична інформатика; тектології (теорії організації соціальних систем) інформаційної безпеки.

Щодо інформаційної безпеки, вітчизняна наукова думка схиляється до концептуального визначення її як складного міжгалузевого об'єкта дослідження, у якому домінують три взаємопов'язані провідні наукові дисципліни: право, інформатика і теорія управління соціальними системами. У складі теорії управління соціальними системами особливу, значну роль відіграє її складова — організація соціальних систем (тектологія).

Поки що в Україні інформаційна безпека, як наукова дисципліна, переважно формується у технічному (технократичному) напрямі. Наукове обгрунтування організаційно-правових аспектів відіграє вторинну роль, виражену в окремих нормативних актах, підготовлених фахівцями з технократичним світоглядом та освітою. Такі нормативно-правові акти породжують у широкого загалу учасників інформаційних відносин розширення ентропії, хоча кожен нормативно-правовий акт покликаний зменшувати невизначеність у суспільстві.

Інформаційне суспільство потребує адекватного правого забезпечення. Існує думка, що доцільно додатково впровадити у технічних навчальних закладах (особливо в тих, де готують висококваліфікованих фахівців з навичками роботи на комп'ютері) та юридичних вузах, як обов'язкову навчальну дисципліну "Інформаційне право". (Така дисципліна

вже кілька років викладається автором цієї статті в одному з вузів міста Києва).

У межах вужчого кола питань можлива навчальна дисципліна "Правове регулювання захисту інформації в автоматизованих системах" та ширша за змістом — "Інформаційна безпека" або "Основи тектології інформаційної безпеки".

Існує думка, що за структурою тематики така навчальна дисципліна, як "Основи тектології інформаційної безпеки" повинна комплексно охоплювати у рівномірному співвідношенні викладання і вивчення наступних тематичних блоків: тем щодо загальних положень теорії інформаційної безпеки як соціального явища; тем конституційного, адміністративного, цивільного, трудового та кримінального законодавства щодо регулювання суспільних інформаційних відносин в умовах інформатизації, тем інженерно-технічного, криптографічного захисту; а також теми з тектології захисту інформації, у тому числі в автоматизованих (комп'ютерних) інформаційних системах. У такому ж комплексі пропонується формування і відповідної наукової дисципліни, як міжгалузевої комплексної інституції.

Зазначимо, що перші кроки на державному рівні вже зроблено Урядом України. Розпорядженням Прем'єр-міністра (яке покладено в основу відповідних нормативних актів міністерств і відомств) у відомчих вузах правоохоронних органів зазначені дисципліни рекомендовані до введення у навчальні плани. Сьогодні можна ставити питання про введення зазначених навчальних дисциплін і в інші ВНЗ України.

Введення тематики інформаційного права в юридичні ВНЗ, поряд з іншими юридичними навчальними дисциплінами, покликано зменшити ентропію у майбутніх правоохоронців щодо правового регулювання інформаційних правовідносин та протидії комп'ютерній злочинності.

Введення навчальних дисциплін щодо інформаційного права в технічних ВНЗ дозволить зменшити вплив проблем щодо формування правової культури фахівців з технічною освітою і взаємодію їх з юристами щодо боротьби з комп'ютерною злочинністю.

Існує також нагальна потреба залучення широкого кола фахівців у галузі інформатики, комп'ютерних технологій до формування інформаційних ресурсів у науці криміналістиці її наукового напрямку — криміналістичної інформатики — щодо напрацювання методик проведення судових експертиз по комп'ютерних злочинах, техніки, методики і тактики їх виявлення та розкриття.

Одним із шляхів подолання соціальної та індивідуальної ентропії є систематизація та удосконалення національного законодавства у сфері суспільних інформаційних відносин. Цей захід дозволяє правовими методами знизити ентропію суспільства щодо комп'ютерних правопорушень, визначити межу дозволеної поведінки особи у суспільстві.

Tcimbaljuk V. S.

THE PROBLEMS OF A LATENCY OF COMPUTER CRIME

In the article the questions concerning problems of a latency of computer crime in Ukraine and abroad are considered.