розуміти їх створення будь-яким способом. Спосіб виготовлення підроблених недержавних цінних паперів залежить від форми їх існування (документарна чи бездокументарна). Виготовлення підроблених бездокументарних недержавних цінних паперів може бути вчинене шляхом відкриття фіктивного рахунку у цінних паперах у зберігача. Підробкою бездокументарних недержавних цінних паперів слід вважати внесення будь-яких змін до рахунку у цінних паперах у зберігача, які спотворюють зміст зафіксованої у ньому інформації. Такі зміни можуть бути внесені шляхом надання незаконних розпоряджень на здійснення облікових депозитарних операцій (зарахування, списання, переміщення, переказ), наслідком яких може бути зміна кількості цінних паперів на рахунку, обмеження їх в обігу або зняття таких обмежень, чи розпоряджень про внесення змін до реквізитів анкети рахунку у цінних паперах, які не супроводжуються обліковими операціями щодо цінних паперів, наприклад, зміна інформації щодо власника (розпорядника) рахунку тощо.

Виготовлення з метою збуту підроблених бездокументарних цінних паперів, їх підробка чи використання підроблених бездокументарних недержавних цінних паперів, які існують у формі відкритого зберігачем рахунку, здійснюється шляхом внесення неправдивих даних до рахунку в цінних паперах у зберігача на електронних носіях інформації, тобто є одночасно втручанням у роботу автоматизованої системи, якою є така система реєстру. Такі дії одночасно утворюють і склад злочину, передбачений ст. 198^1, і мають кваліфікуватися залежно від того, хто є емітентом цінних паперів за сукупністю злочинів, передбачених ч. 1 чи ч. 9 ст. 79 або ч. 3 чи ч. 4 ст. 148^8 та відповідною частиною ст. 198^1, оскільки при цьому має місце спотворення чи знищення інформації, зокрема, внесення змін в рахунок у цінних паперах, відкритий зберігачем.

З суб'єктивної сторони злочини, передбачені ч. 1 ст. 79 та ч. 3 ст. 148^8, характеризуються лише умисною виною, а мотиви і мета їх вчинення можуть бути різними. При виготовленні підроблених державних та недержавних цінних паперів обов'язковою ознакою їх суб'єктивної сторони є мета збуту. Залежно від конкретних мотивів і мети виготовлення цінних паперів, а щодо недержавних цінних паперів – також мотивів і мети їх використання, дії винного можуть додатково кваліфікуватися за ст. 198^1 (якщо предметом є цінні папери у бездокументарній формі), а також як готування до вчинення інших злочинів чи як замах на їх вчинення (наприклад, розкрадання державного, колективного чи індивідуального майна).

УДК 002.6:342.7:347.777:343.50:35.078

ПРОБЛЕМИ ЛАТЕНТНОСТІ КОМП`ЮТЕРНОЇ ЗЛОЧИННОСТІ

Віталій Цимбалюк

Анонація: **В статті розглядаються питання щодо проблем латентності комп`ютерної злочинності в Україні та за кордоном.**
Summari: **In the article the questions concerning problems of a latence of computer crime in Ukraine and abroad are considered.**
Ключові слова: **комп`ютерна злочинність, інформаційне право.**

Приблизно з середини XX століття у світі з'явилося нове масове соціально-технічне явище, яке знайшло вираз у категорії "комп`ютеризація" та "інформатизація" і, майже одночасно з ними, виникли нові кримінологічні категорії: "комп`ютерні злочини", "комп'ютерна злочинність", "організована комп`ютерна злочинність". В основі сутності останніх категорій полягає практика використання електронно-обчислювальної (комп`ютерної) техніки та заснованих на ній технологій в різних сферах суспільного життя в антисоціальних цілях.

Комп`ютеризація, на сучасному рівні розвитку, ставить перед суспільством та державою, в тому числі перед правоохоронними органами нові, нетрадиційні проблеми. Серед них особливе місце займають проблеми зростання протиправних проявів у сфері використання комп'ютерних технологій в глобальних комп`ютерних мережах.

Як свідчить історія розвитку світового науково-технічного прогресу, будь-яка технічна новація, зокрема щодо засобів комунікації, завжди, неминуче притягувала до себе людей, які намагалися і намагаються використати її для вчинення злочинів.

Сьогодні у злочинному світі спостерігається нова тенденція: організовані злочинні формування активно освоюють "кіберпростір", відчувши тиск правоохоронних органів на "традиційні" сфери злочинного бізнесу. За оцінками експертів, нині комп'ютерна злочинність набуває такого розвою, що при її ігноруванні в подальшому виникає проблема, щодо загрози окремим інтересам не тільки якоїсь конкретної людини, соціальним приватним

та державним структурам, а й національній безпеці окремих держав і безпеці людства в цілому.

Слід зазначити проблему державного статистичного забезпечення досліджень комп`ютерної злочинності в Україні. Взагалі прояви комп`ютерної злочинності в нашій країні розпорошені, приховані переважно в статистиці економічної злочинності, що не дає змоги дослідження динаміки комп`ютерної злочинності, як специфічного соціального явища у державі.

Народна мудрість говорить, що краще вчитися на помилках інших, а тому для ілюстрації загроз інформаційній безпеці пропонується звернутися до світової практики.

Офіційні представники американської армії стурбовані тим, що досвідчені хакери, "кіберкриміналітет" можуть отримати контроль над основними системами зброї, на зразок танків, літаків, військових кораблів. Про це було заявлено на конференції Army Directors of Information Management Conference в Хьюстоні. Така можливість була продемонстрована офіцером армії США, який знаходячись в готелі в Бостоні, за допомогою портативного комп`ютера зумів ввести дезінформацію в систему управління кораблями ВМС у морі. На щастя - це була тільки контрольна перевірка надійності захисту військових комп`ютерних систем. (Computerworld Київ, 2000, 29 березня. С. 24).

Комп`ютеризація різних сфер суспільного життя викликала ряд проблем щодо інформаційної безпеки в господарських правовідносинах, зокрема підприємництва. Так за експертними оцінками спеціалістів США, зняття елементів захисту інформації з комп'ютерних систем приводить до розорювання 20% середніх компаній на протязі декількох годин, 48% зазнають крах через декілька днів, а інших розорення настане в цьому проміжку. Суттєвіші втрати спостерігаються в банківській сфері. Близько 33% банків «лопне» через декілька годин, 50% - через декілька днів. Середні збитки від одного комп'ютерного злочину в США складають 450 тис доларів, щорічні втрати деяких американських фірм в загальній сумі досягають 5 мільярдів доларів. (Див.: Фатьянов А.А. Проблеми защиты конфиденциальной информации, не составляющей государственную тайну //Информационное общество. 1997. №1. С.55).

Поряд із зазначеними проблемами інформаційної безпеки в умовах інформатизації звернемо увагу на таку яка існує, не тільки в Україні, але й у всьому світі - латентність комп`ютерної злочинності: її прихованість; соціальне явище, яке не виявляє себе видимими ознаками на певному часовому проміжку. За оцінками експертів сьогодні комп`ютерна злочинність досягає близько 90%.

Загально відомою є одна її причина: у більшості випадків, через небажання підриву репутації потерпілі неохоче повідомляють (якщо роблять це взагалі) правоохоронні органи про факти злочинних посягань на їх комп`ютерні системи.

Проте у цього явища існує багато причин другого порядку. Пропонується звернути увагу на такі, що мало висвітлені у публікаціях: когнітологічний (психологічний, пізнавальний, інформаційний) аспект, та пов`язану з цим ентропію (невизначеність через відсутність знань) персоналу, який забезпечує технічний захист інформації в автоматизованих (комп`ютерних) системах та широкого загалу юристів, в тому числі практичних працівників правоохоронних органів, покликаних вести боротьбу зі злочинністю.

Серед працівників підрозділів технічного захисту приватних та деяких державних відомчих інформаційних автоматизованих (комп`ютерних) систем (АС), деяких провайдерів у трансграничних комп`ютерних мережах (на зразок Інтернет), системних адміністраторів локальних АС існує професійний, психологічний феномен сформований під впливом технічної освіти: фаховий технократичний світогляд в основі якого полягає думка, що всі проблеми захисту інформації в АС можна вирішити за допомогою переважно комп`ютерних "замків" - програмно-математичних та технічних засобів, тобто за допомогою технічного захисту інформації в АС.

Зазначимо ще одну проблему, що впливає на латентність комп`ютерної злочинності: більшість технократів забувають чи не знають прописної істини - всі інженерно-технічні засоби захисту, що створені розумом і руками одних, з часом, при бажанні або потребі, обов'язково будуть зруйновані чи подолані іншими, особливо коли за це береться декілька людей, зокрема, об`єднаних у злочинну організацію.

Як свідчить практика, отримавши опір технічної системи захисту щодо несанкціонованого проникнення в комп`ютерну систему злочинці шукають нових знань і шляхів вчинення злочину, зупинити їх може тільки державний суд (покарання), чи загроза суду (загроза покарання). Нерідко, злочинці знаючи психологію "захисників" комп`ютерних систем, служб технічного захисту, нахабніють на стільки, що гублять пильність, адже мають переконання, що про наміри несанкціонованого проникнення повідомлення у правоохоронні органи не буде, а отже вони не будуть покарані.

Як приклад, звернемо увагу на дослідження Американського міністерства оборони, воно провело широкомасштабні навчання з інформаційної атаки на власних комп'ютерних мережах. Результат був вражаючим. У США 99% військових засобів зв'язку вдаються до цивільних мереж Internet; 88% атак на ділянку з 3000 комп'ютерів завершились успіхом; з них 4% було виявлено, а повідомлено всього про 0,5%.

Як зазначають спеціалісти, складності цього виду злочинів полягає в тому, що вразливість військових і цивільних систем тісно пов'язана, і електронний «бліцкриг» одночасно міг би позначитися на всій інфраструктурі будь якої країни (Див.: Політі А. Нові транснаціональні ризики і європейська безпека. - К. 1997).

При дослідженні проблематики не заперечується значимість технічного захисту комп`ютерних систем,

технічний захист потрібний без сумніву. Поряд з цим, нагадаємо народну мудрість: замки роблять для порядних людей, злочинцю вони надають тільки додаткового клопоту для досягнення злочинної мети.

Дослідження в Україні свідчать, що широкий загал фахівців, діяльність яких пов`язана з комп`ютерними технологіями, не мають не тільки відповідних навичок, але й правових знань: як правильно документувати дії порушника; в які правоохоронні органи слід звертатися в разі виявлення порушення; як діяти до втручання у справу правоохоронців, тощо.

Це зумовлено тим, що в більшості технічних вузів юридична підготовка, як правило, обмежується єдиною юридичною навчальною дисципліною - «Основи права», на вивчення якої відводиться приблизно до 20 аудиторних годин. До того ж у багатьох технічних вузах ця навчальна дисципліна не містить тем, які б розкривали сутність та особливості змісту комп`ютерних правопорушень, зокрема таких що визначаються як злочини. З цим пов`язана ще одна проблема - відсутність широкого кола серед фахівців - юристів, таких, хто міг би кваліфіковано комплексно донести до студентів проблематику комп`ютерної злочинності та правових засобів протидії їй.

Обсяг подання юридичних знань щодо особливостей суспільних відносин в умовах інформатизації у навчальних закладах є недостатнім, в тому числі і щодо формування правосвідомості майбутніх фахівців: програмістів-математиків, інженерів-електронників, інженерів-програмістів комп`ютерних (електронно-обчислювальних) систем тощо. Слід звернути увагу, що це саме те середовище, з якого, переважно, виходять не тільки експерти технічного захисту інформації в АС, а й висококваліфіковані хакери - особи, що вчиняють правопорушення з використанням комп`ютерних технологій, несанкціонований доступ до АС.

Наступна проблема. Юридичні знання, сформовані за часів коли комп`ютер був екзотикою створили комплекс суспільної ентропії до особливості нових інформаційних правовідносин: в умовах комп`ютеризації, інформатизації. Сьогодні, критична маса правової інформації до емпіричного матеріалу, зокрема щодо несанкціонованого проникнення в АС потребує відповідного цілеспрямованого, комплексного та системного наукового осмислення на міжгалузевому науковому рівні.

У зв`язку з цим виникла потреба формування у теорії права концепції синтетичних міжгалузевих комплексних систем (інституцій) права. Назвемо умовно їх субінститутами права чи гіперінститутами права. На базі цієї концепції пропонується виділити соціальні інформаційні відносини у спеціальні синтетичні міжгалузеві комплексні наукові дисципліни: інформаційне право та правову інформатику. Серед наукової громадськості України ця ідея ще тільки набуває поширення. В основному наукові розробки 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, інформаційна безпека. (Щодо інформаційної безпеки, як наукової дисципліни автор вважає, що вона повинна складатися з двох складових: інформаційне право та правова інформатика).

Існує думка, що доцільним є в технічних та юридичних навчальних закладах де готують висококваліфікованих фахівців з навичками роботи на комп`ютері, впровадити додатково, як обов’язкову навчальну дисципліну «Інформаційне право». Як альтернатива, в межах більш вузького коло питань можлива така навчальна дисципліна «Правове регулювання захисту інформації в автоматизованих системах». За структурою такі навчальні дисципліни повинні в комплексі охоплювати вивчення тем конституційного, адміністративного, цивільного, трудового та кримінального законодавства щодо регулювання суспільних інформаційних відносин.

Серед тем інформаційного права пропонуються, як обов`язкові, теми з питань застосування норм права у боротьбі з комп`ютерними правопорушеннями - юридична деліктологія в інформаційних відносинах (в спектрі провідних галузей права розвивається система публічного правового захисту суспільних інформаційних відносин в умовах інформатизації України). Тобто, поряд з іншим, увага повинна звертатися щодо з`ясування деліктних відносин (правопорушень) в інформаційній сфері, особливо відповідальності за злочинні дії предметом посягання та вчинення яких є інформація в автоматизованих (комп`ютерних) системах.

Апробація навчальної дисципліни "Інформаційне право" проводиться автором в одному з київських вузів на протязі вже двох років. Також проблематика інформаційного права введена автором до навчальних дисциплін, методичні матеріали яких готувалися за його участю і викладалися чи викладаються ним в різних вузах міста Києва та Київської області: "Захист електронних засобів від несанкціонованого доступу", "Правове регулювання відносин власності", "Господарське право", "Правове регулювання підприємницької діяльності", "Цивільне право", "Теорія держави та права".

Враховуючи трансграничність суспільних інформаційних відносин в умовах інформатизації, автором введено до навчальної дисципліни "Міжнародне приватне право", що викладається на юридичному факультеті Національного технічного університету України "КПІ", тему "Міжнародне інформаційне право та право інтелектуальної власності".

Ведення тематики інформаційного права, поряд з іншими юридичними навчальними дисциплінами покликано зменшити ентропію у майбутніх юристів щодо правового регулювання інформаційних правовідносин в умовах інформатизації світу, а також відпрацювати зі студентами (на умовах партнерства) питання

проблематики інформаційного права, зокрема його складової, яка у Західних країнах отримала умовну назву "комп`ютерне право".

Існує також ще проблема: недостатній рівень вітчизняних наукових напрацювань боротьби з комп`ютерними правопорушеннями в межах традиційних провідних галузей правознавства: цивільного, адміністративного, кримінального, трудового. Галузевий підхід щодо з`ясування сутності комп`ютерних правопорушень, створили ентропію у юристів щодо інформатизації та ентропію технократів щодо можливостей права у боротьбі з такими правопорушеннями.

Ця проблема існує не тільки у нас. З наукових джерел відомо, що в американському суспільстві проблема деліктів пов`язаних з використанням комп`ютерних технологій, були сформовані у 1979 році на Конференції Американської асоціації адвокатів у м. Далласі. Але тільки через 10 років вона остаточно знайшла вирішення в законодавстві США.

Нема сумніву, що категорії "інформаційне право" (або, як його називають на Заході, "комп`ютерне право") та "правова інформатика" стануть звичними категоріями в лексиконі юристів та інформатиків щодо захисту інформації в автоматизованих системах. Адже історія науки знає, що саме на межі і в поєднанні різних галузей знань, що досягли за кількістю і якістю критичної маси, виникають нові наукові дисципліни, які з часом стають автономними науками. Наприклад, на межі правознавства та медицини існує судова медицина, судова психіатрія. Кримінологію та криміналістику також можна вважати науками, які виникли на межі інших наук: перша - на межі соціології, психології та кримінального права, друга - на межі права і технічних наук.

Недостатність теоретичних розробок у вітчизняній науці щодо боротьби з комп`ютерною злочинністю, особливо організованими її проявами створюють ентропію (невизначеність) серед практичних працівників правоохоронних органів України. Поки що, у нас налічуються одиниці "гучних", з великим суспільним резонансом, кримінальних справ щодо злочинів вчинених з використанням комп`ютерних технологій.

Наступна проблема, на яку хочеться звернути увагу, це те, що кожний факт спроби зазіхання, зокрема, на несанкціонований доступ до автоматизованої (комп`ютерної) системи (в широкому розумінні цієї категорії) повинен бути відомий правоохоронним органам, тобто бути офіційно зареєстрованим. Це дасть змогу на основі емпіричного матеріалу відпрацьовувати оптимальні моделі виявлення та розкриття злочинів, що в свою чергу забезпечить наукове обгрунтування боротьби з комп`ютерною злочинністю.

Комп'ютерна злочинність - це соціальне явище, якому можна протистояти тільки спільними зусиллями - громадою, спільним розумом фахівців науковців і практиків різних галузей знання. Сьогодні, на межі цих галузей в Україні, як і в інших цивілізованих країнах, існує потреба та формуються нові міжгалузеві комплексні наукові інституції: інформаційне право та правова інформатика (в складі останньої існує нагальна потреба формування розділу криміналістичної інформатика, чи інформаційної криміналістики).

На цій «ниві», як і в будь-якій сфері суспільних відносин вистачить роботи всім. Але потрібна чітка скоординована взаємодія фахівців. Конкуренції бути не може і не повинно бути. У кожного з них свої методи і засоби боротьби з комп`ютерною злочинністю, але мета одна.

Такі науки, як правова інформатика, криміналістика, інформаційне право дозволяють об'єднати зусилля, пояснити фахівцям різних галузей науки, один - одному, специфічні терміни, категорії, тощо, все, що напрацьовано практикою і знайшло розробку у вузьких наукових галузях знань. Завдання сьогодення - спільно відпрацювати методики і тактику боротьби з комп'ютерними правопорушеннями, особливо такими, що вчиняються організованими формуваннями.

Відомчі амбіції вирішити самотужки проблеми несанкціонованого проникнення в комп`ютерні системи повинні чітко узгоджуватися з суспільними інтересами, потребами. Саме і для цього в Україні існує державне (публічне) право, його провідні галузі: конституційне, адміністративне, цивільне, трудове і кримінальне, на межі яких формується міжгалузева комплексна інституція - інформаційне право.

Подолання суспільної правової ентропії в галузі соціальних інформаційних відносин в умовах інформатизації, зокрема, щодо засобів та методів боротьби з комп`ютерною злочинністю є нагальне завдання юридичної науки, як один із засобів зниження латентності комп`ютерної злочинності, в тому числі її різновиду організованої комп`ютерної злочинності.

Більш детально окремі аспекти результатів багаторічних досліджень за участю автора з проблематики інформаційного права та правової інформатики висвітлені у таких публікаціях:

Братков И.С., Цимбалюк В.С. Психолого-педагогическая подготовка сотрудников ОВД к работе с ЭВМ. //Социально-психологические проблемы ОВД /Межвузовский сборник научных трудов. -К. УАВД. 1993. С.80-84.

Братков І.С., Цимбалюк В.С. Деякі організаційно-правові питання формування концепції удосконалення комп'ютеризації ОВС (адміністративно-правовий аспект) //Удосконалення адміністративної діяльності ОВС. -К. УАВС. 1994 С.28-30.

Калюжний Р.А., Цимбалюк В.С. Інформатизація державного управління і національна безпека України. //Розбудова держави. 1993. №8 С.20-21.

Калюжний Р.А., Цимбалюк В.С. Вдосконалення інформатизації ОВС України - передумова покращення їх діяльності в боротьбі зі злочинністю //Правова система України: теорія і практика. -К. 1993. С.397-399.

4. Калюжний Р.А., Цимбалюк В.С. Розбудова держави та інформатизація державного управління. //Розбудова держави. 1994. №2 С.31-36.

Ящуринский Ю.В., Цымбалюк В.С. Использование новых информационных технологий в учебной и исследовательской работе слушателей учебных заведений правоохранительных органов. //К вопросу о концепции управленческой деятельности (ДСП). -К. ИПК СБУ. 1994. С.68-74.

Ящуринський Ю.В., Цимбалюк В.С. Нові комп'ютерні технології - в навчальну та науково-дослідну роботу навчальних закладів. //Інформаційний бюлетень РНМЦ, УАВС. -К. 1995. №2. С.39-44.

Гавловський В.Д., Цимбалюк В.С. Щодо проблем боротьби зі злочинами, що вчиняються з використанням комп'ютерних технологій //Боротьба з контрабандою: проблеми та шляхи їх вирішення. - К. НДІ "Проблем людини".1998. С.148-154.

Гавловський В.Д., Цимбалюк В.С., Корочанський О.Е. Проблеми юридичної деліктології в інформаційних відносинах //"Бизнес и безопасность". 1998 № 6. С. 19-21

Гавловський В., Цимбалюк В., Кашпур В. Державно-правове регулювання соціальних інформаційних відносин //Українське право. 1998 №1. С. 173-176. (укр. і англ. мовами).

Цимбалюк В.С. Захист електронних засобів від несанкціонованого доступу. Навчально-методичний посібник. Ірпінь. УФЕІ. 1998.

11. Організована злочинність в Україні. /Камлик М.І., Романюк Б.В., Сущенко В.Д. Гавлорвський В.Д., Цимбалюк В.С. та ін.; За ред. Я.Ю. Кондратьєва. -К. НАВСУ. 1999. -124с.

Гавловський В.Д., Цимбалюк В.С., Інформаційне право. Навчально-методичний комплекс. -К. 1999. 183 с.

13. Романюк Б.В. Камлик М.І., Гавлорвський В.Д., Хахановський В.Г. Цимбалюк В.С. Виявлення та розслідування злочинів, що вчиняються за допомогою комп`ютерних технологій. Посібник /За ред. Я.Ю. Кондратьєва. - К. НАВСУ. 2000. - 64с.