УДК 343.359:004.056.53

***П.І. Пушкаренко**, канд. екон. наук, доц.,*
Сумська філія Харківського національного університету внутрішніх справ

КІБЕРЗЛОЧИННІСТЬ ЯК НОВІТНІЙ ФЕНОМЕН ТІНЬОВОЇ ЕКОНОМІКИ

Постановка проблеми. Сьогодні вже важко уявити сферу громадського життя, в якій не використовують "диво XXI століття" сучасні інформаційні високі технології та їх ядро – комп'ютеризацію. Користування комп'ютером, вільний доступ до Інтернету, миттєве отримання найрізноманітнішої інформації з усіх можливих сфер людської діяльності, безперечно, відкриває як суспільству в цілому, так і окремим користувачам сучасних благ цивілізації такий простір для творчості, про який наші пращури навіть і мріяти не могли. Для прикладу, у США і Європі зараз налічується по 200 млн. споживачів інформаційних технологій, у Латинській Америці – 20 млн., Африці – шість. Причому йдеться про задоволення не лише власних потреб, а й потреб великих спільнот у виробничій, управлінській, комерційній, військовій, фінансово-банківській та інших сферах діяльності.

Програмне комп'ютерне забезпечення та інша інформація стають товарами широкого вжитку, які, як і всякий товар, можна підробити, незаконно придбати, використовуючи уразливість комп'ютерної мережі, навіть вчиняти такі класичні злочини, як крадіжки, вимагання, шахрайство, "старцювання", відмивання грошей тощо. Немає такої інформації, яка б не цікавила, особливо коли завдяки цій інформації хтось заробляє гроші. Тому високими технологіями активно цікавиться злочинний світ. Уже даються взнаки не лише майже безневинні забави талановитих хакерів покопирсатися у нашому особистому ПК, а й протиправні дії, які мають усі ознаки організаційної злочинності, як комп'ютерний тероризм, інші прояви антагоністичної інформаційної боротьби кримінальних формувань з державною або її правоохоронними органами; крадіжки інформації з баз даних та комп'ютерних програм; шахрайства у сфері міжнародних економічних відносин (насамперед кредитно-фінансовій і банківській системах) тощо. Останні прямо належать до тіньової економіки як одна з найнебезпечніших суспільно-економічних складових глобального характеру.

Аналіз досліджень і публікацій. Світова і вітчизняна економічна і правова наука має чимало здобутків щодо наукової розробки теоретичних основ дослідження тіньової економіки. До вітчизняних і російських дослідників цієї проблеми можна віднести А.В. Базилюка, С.О. Головніна, А. Шохіна, О. Осіпенка [2, 4, 9]. Вони досліджували поняття, структуру й наслідки тіньової економіки. Проблеми кіберзлочинності досліджують також юристи В.О. Голубєв, В.Д. Павловський, Р.А. Калюжний, В.С. Цимбалюк, В.Є. Козлов

[5, 7], розглядаючи її як злочини, яким треба визначити міру відповідальності і міру покарання. Наше ж дослідження проблем кіберзлочинності як новітнього феномену тіньової економіки лежить в комплексній економіко-правовій площині.

Метою статті є визначення економіко-кримінальної природи кіберзлочинності не як окремого явища, а як інституціональної складової (феномену) тіньової економічної діяльності, окреслення основних причин і форм її прояву, наслідків і шляхів протидії.

Наукова новизна полягає у структуризації сучасних тіньових кібертехнологій та обґрунтуванні методологічних положень комплексного підходу до розробки і реалізації державної політики протидії злочинній "світовій павутині", об'єднання зусиль міжнародного співтовариства в боротьбі з кіберзлочинністю, особливо комп'ютерним тероризмом.

Виклад основного матеріалу. Дослідження, вітчизняна та міжнародна практика свідчать, що злочинний світ активно пристосовується до можливостей кіберцивілізації. Серед злочинів, що вчиняються з використанням комп'ютерних технологій і телекомунікацій, особливо зростає комп'ютерна, або кіберзлочинність (від англ. *cyber crime*) у сфері економіки. Економіко-правова актуальність "проблеми кіберзлочинності" обґрунтована нами у спільній праці з В.Б. Чередниченком та Р. Шевченком [1, с. 73-74].

Історично термін "комп'ютерна злочинність" вперше з'явився в американській літературі на початку 60-х років, коли були виявлені перші випадки злочинів, зроблених з використанням ЕОМ. Основні ознаки комп'ютерних злочинів були сформульовані на Конференції Американської асоціації адвокатів у Далласі в 1979 році: а) використання або спроба використання комп'ютера, обчислювальної системи або мережі комп'ютерів з метою одержання грошей, власності або послуг, під прикриттям фальшивих приводів або помилкових обіцянок, або видаючи себе за іншу особу; б) навмисна несанкціонована дія, що має на меті зміну, ушкодження, знищення або викрадення комп'ютера, обчислювальної системи, мережі комп'ютерів або комп'ютерів, що мають системи математичного забезпечення, програм або інформації; в) навмисне несанкціоноване порушення зв'язку між комп'ютерами, обчислювальними системами або мережами комп'ютерів.

Визначення кіберзлочинності у різних авторів неоднакові. Найбільш поширеним є наступне визначення комп'ютерного злочину: "здійснення карного суспільно небезпечного протиправного діяння з використанням інформаційно-обчислювальних систем, або з впливом на них". Таке визначення відповідає економіко-кримінологічному розумінню комп'ютерної злочинності, однак, на нашу думку, потребує уточнення. Беручи до уваги погляди законодавців ряду країн, практику протидії комп'ютерній злочинності ми вважаємо, що до числа комп'ютерних злочинів доцільно віднести "злочини в сфері комп'ютерної інформації, або її захисту, та злочини, вчинені з використанням комп'ютерних технологій". Все більшого розмаху набуває також піратський контроль за сотферним ринком і

програмним забезпеченням, нелегальний продаж через Інтернет аудіо записів (щороку 500 тис.) фільмів та ін.

Більшість західних дослідників пов'язують причини виникнення й існування кіберзлочинності як новітнього феномену тіньової економіки з порушенням певного, підтримує мого державою, розглянутого державою, "розгорнутого порядку людської кооперації" (Ф. Хайєк), тобто загальної суми усіх правил, норм, цінностей і прийнятих взірців поведінки, що дозволяють індивідам співпрацювати у ринковому господарстві. Вважають, що витоки цього феномену закладені у самій людині, мотивах її вчинків, інтересах, специфіці та унікальності соціальної психології індивіду. Водночас загально відомо, що найбільший вплив на поведінку людини, як біосоціальної істоти, має не її внутрішній морально-психологічний стан, а безпосереднє соціальне оточення. "Ненависть і жадоба руйнування... (протиправних дій – *прим. авт.*) зароджуються не в людині, а в її оточенні" [6, с. 62]. Як зауважує у своїй статті Д. Ронг, якби людські істоти повністю складалися з норм і обмежень, то як би тоді можна було зрозуміти способи, якими індивіди щось винаходять і стають підприємцями, новаторами або злочинцями [16, с. 189]. Сучасна неокласична економіка, заснована на моделі раціональної поведінки людини, яка забезпечує максимальну вигоду, надає її вибору центральну роль. Отже, люди приймають рішення щось робити тому, що мають у цьому власний раціональний інтерес (Ф. Фукцяма). Звідси виникає ситуація, за якої невиконання закону стає нормою. Тому тут повинні діяти не лише визначені суспільством правила і норми господарської поведінки, але й ідеологічні та етичні.

За іншою теорією, яка знайшла своє відображення у працях нобелівського лауреата І. Пригожина [12, с. 25], причини виникнення тіньової економіки та кіберзлочинності лежать у загальних законах хаосу, який породжує організовані структури, насамперед, кримінальні, що перебирають на себе певні функції держави. Адже функціонування ринкової економічної системи носить не "детермінований", а імовірний, стохастичний характер. Глобальні соціальні проблеми нерівності, масове поширення безробіття і бідності, незахищеність населення від навколишнього світу, падіння цінності людського життя призводять до згуртування людей у товариства, часто заради особистого збагачення шляхом порушення законів, паразитування на державному устрої; значної криміналізації суспільства, яка спостерігається уже майже сто років. Тьєрі Годен, наприклад, пророкує через 25 років захоплення кібермафією усієї галузі озброєння у світі [15].

Ми вважаємо, що генезис тіньової економіки та її небезпечного прояву – кіберзлочинності – не можна пояснити окремими причинами чи факторами. Він своїм корінням сутнісного походження сягає в неправильні, неадекватні існуючій політико-економічній системі дії суб'єктів господарювання, соціально-психологічні створення їхньої господарсько-правової поведінки, які входять у суперечність з об'єктивними економічними законами, цивілізованим господарським механізмом і не відповідають інтересам переважної більшості населення.

На основі аналізу наукових публікацій на паперових і електронних носіях та існуючого моніторингу комп'ютерної інформаційної практики нами відокремлюються і обґрунтовуються такі схожі для багатьох країн головні технології кібертінізації і, відповідно, привласнення величезних тіньових доходів у сучасній "світо-павутині": 1) комп'ютерні віруси для знищення машинної пам'яті; 2) комп'ютерне піратство нелегальної експлуатації авторських програм і типологій інтегральних мікросхем; 3) крадіжки грошей (прямі або за допомогою техніки "салямі") та інтелектуальної власності "електронним" шляхом; 4) шахрайство з магнітними кредитними картками; 5) інформаційні війни, які можуть призвести до електронного "бліцкригу"; 6) комп'ютерний саботаж та економічний шантаж; 7) індустріальне шпигунство; 8) маніпулювання на серверах під час виробничих компаній; 9) організована комп'ютерна злочинність; 10) загроза контролю кіберкриміналітету над основними військовими комп'ютерними системами управління, комп'ютерний тероризм та багато інших.

Вважається, що перший у світі комп'ютерний злочин був здійснений у Міннесоті (США), а на території колишнього СРСР зареєстрований в 1979 р. у Вільнюсі, внаслідок якого була нанесена шкода державі у розмірі 80 тис. крб. За повідомленням БІ-БІ-СІ, у штаті Вірджинія вперше в історії засуджений на дев'ять років тюремного ув'язнення 30-річний Джерелі Джейн, здавалося б, за безневинні пустощі розсилань близько 10 млн. електронних листів, так званого рекламного спаму для продажу усяких підробок і щомісячний заробіток від цього 750 тис. дол.

Значного резонансу набула справа жителя Санкт-Петербурга Левіна, який подолав систему безпеки Citibank і за допомогою віддаленого комп'ютерного доступу викрав близько 10 млн. дол. Серед вітчизняних слід відзначити, так звану, вінницьку справу 1998 р., коли зловмисник, використовуючи систему електронних платежів, незаконно переказав понад 80 млн. грн. (на той час близько 20 млн. дол.) на кореспондентський рахунок одного з латвійських банків [8, с. 89, 118]. Проте на відміну від "справи Левіна", яка стала хрестоматійною у працях, присвячених комп'ютерній злочинності, "вінницька" через недосконалість вітчизняного законодавства до комп'ютерних не віднесена.

В сучасних умовах кіберзлочинність стає одним із найнебезпечніших суспільно-економічних явищ глобального характеру, яке турбує весь цивілізований світ. На конференції країн Великої вісімки щодо проблем кіберзлочинності, яка проходила у жовтні 2000 р., тодішній міністр закордонних справ Німеччини Йошка Фішер зазначив, що збитки від кіберзлочинів сягають 100 млрд. німецьких марок (45 млрд. дол.) щорічно. За оцінками Рахункової палати уряду США щорічний збиток від розкрадань і шахрайств, вчинених з використанням комп'ютерних технологій тільки через Інтернет досягла 5 млрд. дол. Один лише комп'ютерний вірус NIM DA обійшовся британській економіці сумою понад 1,8 млрд. фунтів. До того ж, за допомогою "світової павутини" здійснюється зв'язок між терористичними організаціями, координується їхня діяльність, вербуються нові учасники,

збираються кошти для забезпечення терактів. До чого це може призвести – можна судити вже по тому, яка трагедія сталася у США 11 вересня 2001 р., коли оператори авіарейсів та протиповітряної оборони цієї країни внаслідок кібератаки на систему управління польотами не змогли своєчасно зреагувати на нештатну ситуацію та оголосили тривогу.

За незалежним дослідженням, проведеним на замовлення виробника антивірусу McAfee на європейській базі доктором Пітером Трокслером, експертом і дослідником з федерального технологічного інституту в Цюріху кіберзлочини політико-економічного характеру сьогодні вчиняються не одинаками, а справжніми злочинами організованими структурами, які перебувають на утриманні історичних злочинних співтовариств типу італійської мафії [3, с. 13]. До таких нових феноменів "справжніх кібермафій" дослідники відносять *bot-net*, використання дитячої праці та шахрайство; *script kiddies*, молоді комп'ютерні таланти; акціонерні шахрайства та ін.

Поліція Палермо в ході слідчих заходів виявила факти акціонерного шахрайства в обсязі 474 млн. євро, в яких були задіяні брудні гроші мафії і законні доходи, пов'язані котируванням акцій деяких підприємств. За даними швейцарського дослідження, групи комп'ютерних найманців пропонують свої мережі злочинним організаціям по 150 євро за годину. У США відмивання грошей від наркоторгівлі за допомогою комп'ютерних технологій становить від 30 до 100 млрд. дол.

За останні п'ятнадцять років кількість несанкціонованих проникнень до інформаційних систем зросла від поодиноких випадків у 1988 р. до 140 тис. – у 2004 р. Що ж до збитків, яких зазнає через це щорічна світова економіка, то вони становлять понад 100 трлн. дол. [10, с. 11]. За оцінкою Інтерполу прибутки кіберзлочинців займають третє місце після доходів наркоділків та нелегальних постачальників зброї. Приміром, тільки за допомогою карток систем Visa та Europay у світі щороку зникає наліво майже 2 млрд. дол. [13, с. 14]. Кримінологічні прогнози свідчать, що кіберзлочинність (особливо організована та транскордонна) у XXI ст. динамічно зростатиме.

Враховуючи загрозу безпеці та добробуту народів, яку несе в собі транснаціональна комп'ютерна злочинність, на Саміті Тисячоліття (Нью-Йорк, 2001 р.) розроблена і прийнята Міжнародна конвенція про боротьбу з комп'ютерним тероризмом, а в Україні для цього створений відповідний міжвідомчий центр.

В Україні до певного часу економічні та правові науки особливо не переймалися дослідженнями проблем комп'ютерної злочинності. Воно й зрозуміло: рівень життя, соціально-економічного розвитку та комп'ютеризації ще років десять тому не давали приводу для занепокоєння. Однак сьогодні, коли, кількість споживачів Інтернету в нашій країні перевалила за 2 млн. і темпи її зростання продовжують збільшуватися, постало питання захисту інформаційних систем як у технологічному, так і в правовому аспекті.

Адже хоч Україна ще не перейшла межі кіберепідемії, ознаки хвороби вже досить відчутні. Чого тільки варта, скажімо, вірусна атака 16-20 листопада 2001 р. на обчислювальну мережу гендирекції ВАТ "Укртелеком", яка налічує понад 700 комп'ютерів та десятки серверів, із збитками 700 млн. грн. Або, за оцінкою фахівців, за два останніх роки через 5 тис. банкоматів вітчизняних банків викрадено в еквіваленті понад 5 млн. дол. Причому кількість кіберзлочинів і збитків від них з кожним роком зростає. Якщо у 2002 р. році викрито 32 таких випадки, то в 2003 – вже 52, а в 2004 р. вони збільшилися ще на 20 % [10, с. 11]. За прогнозами фахівців, цей показник може навіть у найближчий період зрости у десятки разів.

Висновки. Кіберзлочинці, як правило, мають досить високу кваліфікацію та глибоке знання сучасних технологій організації електронного обертання коштів та платіжних карток. Не випадково цей вид злочинів віднесений до високоінтелектуальних, а також таких, що важко розкриваються. Адже насилля при його скоєнні майже відсутнє, а злочинця жертви не бачать, оскільки в момент пограбування він може перебувати за тисячі кілометрів від місця злочину. Тому у створеному відділі боротьби з правопорушеннями у сфері високих технологій в структурі Департаменту по боротьбі з економічними злочинами МВС України повинні працювати спеціалісти особливо високої фахової підготовки. Назріло також істотне вдосконалення законодавчої бази, особливо в галузі економічної кримінології, об'єднання зусиль у профільній робочій групі представників МВС, СБУ, НБУ та ін. для розв'язання нагальних проблем кіберзлочинної афери.

Досить реальною для нашої країни є й перспектива апробації проекту ООН для СНД "Боротьба з організованою злочинністю шляхом попередження махінацій з банківськими кредитними картками та інших фінансових злочинів, пов'язаних з комп'ютерними технологіями". Пропонуємо також розробити та прийняти міжвідомчий нормативний документ, у якому вирішити питання координації досліджень та обміну досвідом між науково-дослідними установами та вищими навчальними закладами з цієї проблематики.

Список літератури

1. Актуальні проблеми сучасної науки: Матеріали підсумкової наукової конференції. – Харків: Вид-во Нац. ун-ту внутр. справ, 2005. – 260 с.
2. Базилюк А. В., Коваленко С. О. Тіньова економіка в Україні. – К.: НДЕІ Мінекономіки України, 1998. – 206 с.
3. В Інтернет прийшла кібермафія // Урядовий кур'єр. – 11.03.2005. – № 44.
4. Головнин С., Шохин А. Теневая экономика: за реализм оценок// Коммунист. – 1990. – № 1.
5. Голубєв В.О., Гавловский В.Д., Цимбалюк В.С. Інформаційна безпека: проблеми боротьби зі злочинами у сфері використання комп'ютерних технологій / За заг. ред. док. юрид. наук Р.А. Калюжного. – Запоріжжя, 2002.
6. Дегальдо Х. Мозг и сознание. – М.: Прогресс, 1971.
7. Козлов В.Е. Теория и практика борьбы с компьютерной преступностью. – М.: Горячая линия – Телеком, 2002.
8. Комп'ютерна злочинність. Навчальний посібник. – Київ: Атіка, 2002. – 232 с.

9. Осипенко О. Теневая экономика: попытка политико-экономического анализа // Экономические науки. – 1989. – № 8.
10. Підводні рифи високих технологій // Урядовий кур'єр. – 01.06.2005. – № 100.
11. Попович В. М. Тіньова економіка як предмет економічної кримінології. – К.: Правові джерела, 1998.
12. Пригожин И., Стенгерс И. Порядок из хаоса – М.: Прогресс, 1986. – 202 с.
13. Самсоненко Л. Чи омине нас кіберзлочинна афера // Урядовий кур'єр. – 21 грудня 2005 р. – № 243.
14. Турчинов О. В. Тіньова економіка: теоретичні основи дослідження. – К.: Артек, 1995.
15. Gaudin T. 2100, Our Species Odyssey, Fondation 2100. – Paris, 1998.
16. Wrong D. The Oversocialized Conception of Man in Modern Sociology. "American Sociological Review" № 26. – 1961. – P. 183-196.
Отримано 13.04.2006

Пушкаренко, П.І. Кіберзлочинність як новітній феномен тіньової економіки [Текст] / П.І. Пушкаренко // Проблеми і перспективи розвитку банківської системи УкраїниУкраїни: зб. наук. праць. – Суми: УАБС НБУ, 2006. - Т. 17. - С. 75-82.