УДК 002.6+342.7+347.777+343.50+35.078

Гуцалюк М. В.

КРИМІНАЛЬНІ ДЕЛІКТИ В INTERNET

У статті розглядаються напрямки боротьби з комп'ютерною злочинністю та організаційно-правові проблеми розвитку інформаційних відносин в Україні, пов'язані з використанням глобальної комп'ютерної мережі Internet.

На межі тисячоліть ми стали свідками інформаційної революції, вплив якої на розвиток суспільства можна порівняти, наприклад, з винаходом парового двигуна. В свою чергу вона стала закономірним продовженням розвитку технологій обробки та передачі інформації, започаткованих за часів появи писемності та отримавши значного розвитку після винаходу книгодрукування.

Промислова революція у XX СТ. призвела до подальшого зростання обсягів обміну інформацією, що було пов'язано з відкриттями у науці та винаходами в техніці, удосконаленням технологій виробництва. Лавиноподібне зростання інформаційних потоків, необхідність орієнтуватися в них, призвело до неможливості проводити аналіз для прийняття управлінських рішень на основі традиційних методів. Поява електронно-обчислювальних машин та застосування їх для автоматизованої обробки інформації (пошук, передача, обчислення, зберігання і т. п.) дозволили створити так звані "нові інформаційні технології". Використання електронно-обчислювальної техніки в кінці 60-х років досягло таких масштабів, що виникла гостра необхідність організувати віддалений доступ до інформації

окремих наукових та державних організацій, які знаходились на значній відстані одна від одної.

1969 року на замовлення Управління перспективних досліджень (Advanced Research Projects Agency) Міністерства оборони США було розпочато побудову мережі, здатної зберігати обмін інформацією між користувачами за умов ядерної війни; відтоді почала свій розвиток глобальна комп'ютерна мережа Internet.

В кінці 80-х років мережа поєднувала комп'ютери не тільки в США, а й по всьому світу, хоча інформація, що передавалась каналами зв'язку, відображалась на екранах моніторів тільки текстовими символами. В 1989 році, співробітник лабораторії Європейського інституту фізики часток (CERN) Тім Бернерс-Лі запропонував протоколи передачі графічної інформації та започаткував розгалужену гіпермедіа систему World Wide Web (WWW).

З розробкою в середині 90-х років броузерів Netscape та Microsoft Internet Explorer, налагодженням зв'язків між виробниками та споживачами інформації як всередині країн, так і міжнародних і трансконтинентальних почався експоненціальний розвиток глобальної мережі. За даними Nua Internet Surveys (www.nua.ie) кількість користувачів глобальної мережі Internet з 80 тисяч у 1988 році зросла до 400 мільйонів на кінець 2000 року. Серед них близько мільйона в Україні.

В нашій державі ефективному використанню можливостей глобальної мережі для розвитку науки, освіти, культури, підприємницької діяльності сприяє підписаний 31 липня 2000 року Президентом України Указ "Про заходи щодо розвитку національної складової глобальної інформаційної мережі Internet та забезпечення широкого доступу до цієї мережі в Україні" [1]. Указ, зокрема, передбачає встановлення та наповнення інформацією Веб-сторінок центральними органами виконавчої влади, створення належних економічних, правових, технічних умов для забезпечення широкого доступу до мережі громадян та юридичних осіб усіх форм власності.

Разом із позитивними досягненнями широке використання мережі Internet призвело до низки соціальних, організаційних, юридичних та інших проблем.

Засоби комп'ютерної техніки, новітні інформаційні технології почали активно використовувати організовані злочинні угруповання, їхні інтереси передусім спрямовані на отримання конфіденційної комерційної інформації, фінансові махінації, поширення неправдивої інформації тощо. Злочинці у кіберпросторі використовують свої знання для промислового шпигунства, політичних цілей, тероризму. Сьогодні доходи комп'ютерних злочинців, за оцінками фахівців Інтерполу, посідають третє місце після доходів наркоділків і торговців зброєю.

Пильна увага представників "п'ятої влади" до інформаційних технологій пояснюється тим, що сьогодні прибуток від "електронного" бізнесу сягає сотень мільярдів доларів, а списки найпотужніших корпорацій світу очолюють не металургійні чи автомобільні підприємства, а фірми, які спеціалізуються на інформаційних технологіях (рубіж у $100 млрд був подоланий Microsoft). Консалтингова компанія Deloitte & Touche http://www.deloitte.com опублікувала свій щорічний список з 500 технологічних компаній, які найдинамічніше розвиваються — Technology 2000 Fast 500. Цей список очолили Internet-компанії. Інформаційна революція не минула і фінансові установи. Це пояснюється тим, що Internet дозволяє проводити фінансові операції (торгівля акціями, отримання кредитів, страхування і т. п.) без посередників і призводить до зниження комісійних та прискорення обігу фінансових активів. Якщо у 1997 році тільки 5 % фінансових установ надавали доступ через Internet, то в 1998 — їх було 18 %, а в 1999—65 %. В той же час, згідно з дослідженнями компанії Gather Group (http://www.gartner.com), кількість фінансових махінацій в Internet у 12 разів більша, ніж у звичайних банківських установах США.

Широко відома справа Левіна, який подолав систему безпеки Citibank і за допомогою віддаленого комп'ютерного доступу викрав 12 млн. доларів, за що з 1994 року відбуває покарання у США, За аналогічну операцію (несанкціонований доступ у комп'ютерну мережу Китайського банку промисловості) суд східної провінції Жіангсу виніс смертний вирок Гао Жінгвену. Приречено до страти і хакера Фанг Йонга, який у 1990 році, використовуючи комп'ютер, викрав у банку провінції Чжензян 200 тисяч доларів і втік до Канади.

Нині гостро стоїть проблема боротьби з проведенням безподаткових фінансових операцій, відмиванням "брудних" коштів через електронні банківські системи. Для цього глобальна мережа створює принципово нові умови, які сповна використовують кримінальні структури. Маючи розгалужену мережу Internet, створені й успішно функціонують віртуальні підприємства, віртуальна економіка, через яку йдуть цілком реальні гроші. Так, лише в 2000 році, за приблизними підрахунками, із ринку газу, нафти і нафтопродуктів на віртуальні підприємства пішло приблизно 4,5 млрд гривень [2]. За дослідженнями Бюро технологічної оцінки Сполучених Штатів 0,05—0,1 % банківських переказів належать до відмивання грошей. Для оцінки масштабу проблеми необхідно враховувати те, що тільки в США через електронну систему зв'язку щоденно проводяться понад $2000 млрд [3].

На конференції країн Великої вісімки щодо проблем кіберзлочинності, яка проходила у жовтні 2000 року, міністр закордонних справ Німеччини

Йошка Фішер відзначив, що збитки від кіберзлочинів сягають 1ОО мільярдів німецьких марок щорічно. А за оцінками Рахункової палати уряду США щорічний збиток від розкрадань і шахрайств, вчинених за допомогою інформаційних технологій тільки через Internet, досягає $5 млрд.

Перелік комп'ютерних злочинів можна продовжити, згадавши й атаки на військові, космічні комп'ютерні системи, промислове шпигунство, використання компромату в політичних цілях і т. д. У травні 1998 р. "тигри звільнення Тамілу" у Шрі Ланці вперше серед терористичних груп провели кібернетичну атаку, спрямовану проти посольств у столиці [4]. Відомі випадки успішних атак хакерів на сервери Центрального Розвідувального Управління, Федерального Бюро Розслідування, Пентагону, Сенату, інших урядових, комерційних та наукових установ США, які мають неабиякий досвід захисту інформаційних систем. Наприклад, під час проведення виборів президента США хакери змінювали інформацію на сайтах конкуруючої сторони [5].

А ось приклад проникнення до Лабораторій NASA (http://cybercrime.gov). Мері Джо Байт, прокурор Сполучених Штатів у Південному районі Нью-Йорку, заявила, що Раймонд Торрічеллі, "rolex", член групи хакерів, відомий як "конфлікт", визнаний винним Менхетанським федеральним судом у проникненні до двох комп'ютерів, які перебувають у власності й утримуються Федеральною Адміністрацією аеронавтики та космонавтики Лабораторії реактивного руху" ("JPL"), яка розташована в Пазадені, Каліфорнія.

Згідно з попереднім обвинуваченням, Торрічеллі використовував один з цих комп'ютерів для заволодіння чат-кімнатою Internet і встановив програми, розроблені для одержання імен користувачів і паролів для входу в інший комп'ютер. Торрічеллі визнав, що в 1998 р. він став комп'ютерним хакером і членом організації хакерів. Торрічеллі підтвердив, що, працюючи у своїй резиденції в Нью Рачеллі, він використовував свій персональний комп'ютер для пошуку в Internet інформаційних систем, вразливих до проникнення. Після виявлення комп'ютер Торрічеллі отримував неправомірний доступ, завантажуючи "rootkit" — програму, яка дозволяє хакерові отримати повний доступ до функцій комп'ютера іншого власника.

Згідно з інформацією та офіційним обвинуваченням, один з комп'ютерів, з якими мав справу Торрічеллі, використовувався NASA для виконання супутникового проекту й аналізів майбутніх космічних місій, інший — використовувався Відділом наземних комунікаційних систем JPL як внутрішній сервер і для електронної пошти.

Торрічеллі визнав, що на такі обговорення він запрошував інших учасників чата відвідати вебсайт, на якому їм буде надана можливість переглянути порнографічні картинки, і, що він заробляв $0,18 з кожної людини, яка відвідувала цей вебсайт. Згідно з офіційним обвинуваченням, Торрічеллі заробляв від цієї діяльності від $300 до $400 за тиждень.

Торрічеллі також визнано винним у перехопленні імен користувачів і паролів проникнення до комп'ютерних мереж комп'ютера, який належить Державному Університетові Сан Хосе, і привласненні перехоплених паролів та імен користувачів, які він використовував для вільного доступу в Internet.

Крім того, Торрічеллі визнаний винним у привласненні захоплених номерів кредитних карток. Він визнав, що використав один такий номер кредитної картки для оплати міжнародних переговорів. Як зазначено в обвинуваченні, Торрічеллі отримував ці номери кредитних карток від інших осіб і зберігав їх на своєму комп'ютері.

Голова окружного суду США Майкл Б. Мукасей повідомив, що вирок буде винесено 7 березня 2001 р. Торрічеллі чекає 10 років тюрми і $250 000 штрафу за кожне шахрайство з кредитною карткою і обвинувачення за володіння паролем; 5 років тюрми і $250 000 штрафу за перехоплення паролю. Крім того 1 рік тюремного ув'язнення та $100 000 штрафу за кожне обвинувачення про неправомірний доступ до двох комп'ютерів NASA.

Як уже зазначалось, величезний потік інформації надходить в Internet з різних держав; користуватися нею можна практично з будь-якого місця світу. Причому, міжнародне спілкування з використанням Internet ніким не регулюється (не існує органу управління мережею, а основний засіб встановлення правил — саморегулювання). Тому протидія злочинним проявам у глобальній мережі лише на національному рівні буде малоефективною.

Усвідомлюючи загрозу комп'ютерної злочинності, міжнародна спільнота шукає шляхи щодо попередження та ефективної боротьби з цим видом правопорушень, що вимагає передусім розбудови відповідної законодавчої бази, підготовки спеціальних правоохоронних підрозділів, а також тісного міжнародного співробітництва.

В Україні за статтею 198[і] КК України (Порушення роботи автоматизованих систем) злочином визнається "умисне втручання у роботу автоматизованих систем, що призвело до перекручення чи знищення інформації або носіїв інформації, чи розповсюдження програмних і технічних засобів, призначених для незаконного проникнення в автоматизовані системи і здатних спричинити перекручення або знищення інформації чи то носіїв інформації, карається позбавленням волі на строк до двох років… Ті ж дії, якщо ними спричинено шкоду у великих розмірах або вчинені повторно чи за попе-

реднім зговором групою осіб, караються позбавленням волі на строк від двох до п'яти років".

Комітет у справах законодавства Ради Європи у проекті Конвенції щодо кібер-злочинів http://conventions.coe.int/treaty/en/projets/cybercrime.htm рекомендує уніфікувати кримінальне законодавство з питань комп'ютерних правопорушень та передбачити відповідальність за такі злочини:

несанкціонований доступ (доступ до інформації без відповідної санкції або з порушенням правил доступу);

незаконне перехоплення інформації (перехоплення технічними засобами комп'ютерної інформації або перехоплення комп'ютерних випромінювань);

пошкодження інформації (модифікація, знищення та ін.);

створення перешкод для функціонування комп'ютерних систем;

розповсюдження програм, паролей чи кодів доступу до інформаційних систем (хакери викрадають паролі та розповсюджують їх, чим створюють загрозу безпеці інформаційних систем);

комп'ютерне шахрайство (втручання в роботу інформаційної системи з метою отримання економічного зиску);

розповсюдження дитячої порнографії;

правопорушення, пов'язані з авторським правом.

Визнаючи загрозу безпеці та добробуту народів, яку несе у собі транснаціональна комп'ютерна злочинність, Президент України на Саміті Тисячоліття у вересні 2000 року в Нью-Йорку виступив з ініціативою про розробку Міжнародної конвенції про боротьбу з комп'ютерним тероризмом [6].

Для протидії інформаційній агресії в ряді країн почалося формування спеціальних підрозділів, у завдання яких входить не тільки захист від хакерських атак, а й кібернетичний наступ на власників кіберзброї. На думку американського генерала Едварда Андерсена, "готовність до бойових дій у кіберпросторі з точки зору національної безпеки так само важлива, як ядерні ракети та контроль над космосом [7].

В МВС Російської Федерації для боротьби з комп'ютерними злочинами (мережевий злом, поширення комп'ютерних вірусів), з незаконним оборотом заборонених радіоелектронних і спеціальних технічних засобів та із загрозою проникнення в міжміські та міжнародні канали зв'язку створено спеціальний підрозділ — Управління по боротьбі зі злочинами в сфері високих технологій. На створення спеціального підрозділу по боротьбі з комп'ютерними злочинами у міністерстві внутрішніх справ Великобританії на 2001 рік виділено $35 млн.

Незважаючи на те, що в США вже створені та діють центри інформаційної безпеки в Міністерстві оборони, ЦРУ, ФБР і в інших федеральних відомствах, у 2000 році було розроблено "Національний план захисту інформаційних систем", покликаний стати початком довгострокової програми федерального уряду на національному рівні в галузі інформаційної безпеки. Основна мета плану — створення системи захисту до травня 2003 р. [8].

В Україні завдання у сфері захисту державних інформаційних ресурсів у мережах передачі даних покладено на Службу Безпеки України (Департамент спеціальних телекомунікаційних систем та захисту інформації), йде формування спеціальних підрозділів електронної розвідки та протидії комп'ютерним злочинам як в МВС так і в СБУ. Специфіка розслідування злочинів у сфері високих технологій вимагає розробки принципово нової стратегії, тактики та методики, наявності спеціальних технічних засобів, внесення змін до чинного законодавства, створення центрів з підготовки відповідних фахівців, спеціалізованих інформаційних систем оперативного оповіщення. Без проведення такої роботи важко говорити про надійний інформаційний захист національної інфраструктури [9].

Безперечним міжнародним авторитетом у галузі безпеки Internet є Computer Emergency Response Team (CERT) (www.cert.org), заснований інститутом розробки програмного забезпечення Пітсбургського університету Карнегі-Мелона (Carnegie Mellon University Pittsburgh). Працівники CERT допомагають користувачам Internet виявляти випадки проникнення в інформаційні системи, розробляти й розповсюджувати посібники з інформаційної безпеки.

Міжнародна спільнота дійшла висновку, що організація захисту інформаційної інфраструктури тільки на національному рівні буде малоефективною. Водночас, організація протидії кримінальним проявам лише засобами правоохоронних органів не завжди буває ефективною. Тому на початку 90-х років була створена організація FIRST — форум команд реагування на інциденти, який об'єднує 80 бригад реагування з 19 країн світу. Ці бригади представляють державні, комерційні, промислові та навчальні установи [10].

Важливим аспектом профілактики комп'ютерної злочинності є формування відповідної правосвідомості користувачів Internet. Цьому повинно сприяти введення до навчального процесу таких дисциплін як інформаційне право та правова інформатика [11]. В цьому аспекті слід зазначити, що в Україні існує ряд проблем щодо правового регулювання інформаційних відносин. Серед них: брак легальної чіткої, ієрархічної єдності законів, що викликає суперечливе тлумачення для застосування норм у практиці; термінологічні неточності, різне тлумачення однакових за назвою та формою понять і категорій призводить до їх неоднозначно-

го розуміння і застосування на практиці; багато законів та підзаконних нормативних актів в сфері інформаційних відносин ускладнює їх пошук, аналіз та узгодження для практичного застосування; нові правові акти у сфері суспільних інформаційних відносин, часто не узгоджені концептуально з раніше прийнятими, що призводить до правового хаосу тощо [12].

Зазначені проблеми сформували практичну потребу визначення методології систематизації права, розробки її концепції. Ініціативна група науковців та консультантів Міжвідомчого науково-дослідного центру з проблем боротьби з організованою злочинністю розробила Концепцію щодо реформування системи інформаційного законодавства України. 6 жовтня 2000 року на засіданні Урядової комісії з питань інформаційно-аналітичного забезпечення діяльності органів виконавчої влади проект Концепції було прийнято за основу. З проектом Концепції можна ознайомитися на сайті Міжвідомчого науково-дослідного центру з проблем боротьби з організованою злочинністю (http://mndc.naiau.kiev.ua) [13].

Незалежно від того, які технології використовуються для захисту інформаційних систем, що мають доступ в Internet, вони завжди будуть під загрозою вчинення комп'ютерних злочинів. Ефективна організація інформаційної безпеки вимагає значних коштів та часу. Тому тільки скоординованими зусиллями організацій та відомств незалежно від форм власності, шляхом налагодження міжнародного співробітництва, комплексним розв'язанням проблем удосконалення інформаційної діяльності в нашій країні, використовуючи сучасні технології захисту інформації, впроваджуючи відповідні спеціальні дисципліни у вищих навчальних закладах, можна отримати переваги не тільки електронного бізнесу, а й інформаційної революції в цілому, не забуваючи при цьому про інформаційну безпеку як окремих громадян так і держави.

1. Указ Президента від 31 липня 2000 року № 928 / 2000 Про заходи щодо розвитку національної складової глобальної інформаційної мережі Інтернет та забезпечення широкого доступу до цієї мережі в Україні
2. З виступу Голови Державної податкової адміністрації України Миколи Азарова на розширеному засіданні Координаційного комітету по боротьбі з корупцією і організованою злочинністю // Крок.— 2000.— № 8.— С. 7.
3. Information Technologies for the Control Money — laundering. Washington, Government Printing Office, September 1995.
4. International Police Review.— 1998.— November / December. P. 56
5. Инвестиционная газета.— 2000.— 14 ноября.— С. 5.
6. Виступ Президента України Леоніда Кучми на пленарному засіданні Генеральної асамблеї ООН // Крок.— № 17—18.— 2000. Вересень.
7. Пентагон в киберпространстве // Известия.— 2000.— 28 ноября.
8. *Леваков А.* США готовятся к защите информационных систем // Известия.— 2000. 15 ноября.
9. *Гуцалюк М.* Проблеми організаційно-правового забезпечення захисту інформаційних систем в Internet // Збірник "Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні". К.: НТУУ "КПГ, Міносвіти і науки України, СБУ.— К.— 2000.— С. 24—27.
10. *М. Вест-Браун, К. Коссаковский.* Международная инфраструктура за глобальную безопасность и реагирование в сфере информационных технологий.— 1999.— 4 июля.
11. *Гуцапюк М. В.* Інформаційні технології у професійній підготовці працівників правоохоронних органів // Науковий вісник Національної академії внутрішніх справ України.— К.—2000.—№ 1.—С. 145—147.
12. Питання концепції реформування інформаційного законодавства України / Р. Калюжний, В. Гавловський, В. Цимбалкж, М. Гуцалюк // Збірник "Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні". К.: НТУУ "КПІ", Міносвіти і науки України, СБУ.— К.—2000.—С. 17—21.
13. *Гуцалюк М.* Інтернет у боротьбі з корупцією та організованою злочинністю // Крок.— 2000.—№21.— С. 3.

Gutcaljuk M. V.

INTERNET'S CRIMINAL OFFENCES

In the article are considered fields of fight against computer crime and organizationally-legal problems of development of information relations in Ukraine related with usage of the global computer Internet network.