5. Програма боротьби з контрабандою та порушеннями митних правив на 2008–2009 роки: Указ Президента України від 4 березня 2008 р. № 195/2008.

УДК 343.9:343.533

П. Д. Біленчук

МІЖНАРОДНА ВИСОКОТЕХНОЛОГІЧНА КІБЕРЗЛОЧИННІСТЬ: ПОНЯТТЯ, СУТНІСТЬ, ШЛЯХИ ПОДОЛАННЯ

У наш час людство переживає бурхливий розвиток автоматизації, інформатизації і комп'ютеризації всіх сфер життя. За даними Nua Internet Surveys, кількість користувачів глобальної мережі Internet з 80 тис. у 1988 р. зросла до 400 млн на кінець 2000 р., і 1 млрд у 2006 р., серед яких станом на 2007 р. близько 4 млн — в Україні. У нашій державі ефективному використанню можливостей глобальної світової мережі для розвитку науки, освіти, культури, підприємницької діяльності сприяє підписаний 31 липня 2000 р. Президентом України Указ «Про заходи щодо розвитку національної складової глобальної інформаційної мережі Internet та забезпечення широкого доступу до цієї мережі в Україні». Указ передбачає встановлення і наповнення інформацією Вебсторінок центральними органами виконавчої влади, створення належних економічних, правових, технічних умов для забезпечення широкого доступу до мережі громадян та юридичних осіб усіх форм власності. Але розвиток і поширення інформаційних технологій має і негативний аспект: відкриває шлях до антисоціальної та злочинної поведінки. Комп'ютерні системи містять у собі нові досконалі можливості для не відомих раніше правопорушень, а також для вчинення традиційних злочинів новітніми високотехнологічними методами, нетрадиційними засобами.

На конференції країн Великої вісімки щодо проблем кіберзлочинності, яка проходила у жовтні 2000 р., зазначалось, що збитки від кіберзлочинів сягають 100 млрд німецьких марок щорічно. А за оцінками Рахункової палати уряду США щорічний збиток від розкрадань і шахрайств, зроблених за допомогою інформаційних технологій тільки через Internet, досягає $5 млрд.

Крім того, що проступки, правопорушення і злочини, які вчиняються з використанням переваг найсучасніших високих технологій, завдають великих економічних збитків, особистість, суспільство, держава все більше стають залежними від роботи автоматизованих комунікаційних систем у різноманітних сферах життя — від управління збройними силами, підприємствами, організаціями, відомствами, рухом літаків і поїздів до медичного обслуговування населення та національної безпеки. Іноді навіть незначний збій у функціонуванні таких систем може призвести до реальної загрози життю людей. Стрімке зростання глобальних комп'ютерних, автоматизованих систем

та телекомунікаційних мереж, а також можливість підключення до них через звичайні телефонні лінії посилюють можливості їх використання для кримінальної діяльності.

Безумовно, найбільше від комп'ютерних (тут і далі він буде використовуватися як умовний термін) високотехнологічних злочинів потерпають розвинуті у технічному відношенні країни, однак і в інших країнах з початком процесу автоматизації, інформатизації і комп'ютеризації створюються сприятливі умови для вчинення таких злочинів. Зокрема, глобальна комп'ютерна мережа Internet надає можливість увійти до будь-якої світової відомчої комп'ютерної системи, у тому числі й військової. До того ж це можна зробити майже з будь-якої точки світу. У порівнянні з Великою Британією, Німеччиною, США, Японією національна безпека України поки що залежить від комп'ютерних мереж значно менше: комп'ютерних злочинів в основному зазнає у нас фінансово-кредитна сфера. Але у недалекому майбутньому такі злочини можуть призвести до глобальних катастроф — екологічних, економічних, транспортних тощо. Введення сучасної системи управління культурою, освітою, наукою, медициною, рухом літаків, поширення телекомунікаційної мережі, впровадження системи електронних платежів, використання комп'ютерів у діяльності органів правопорядку та у військовій справі значно розширили сферу діяльності всіх різновидів комп'ютерних злочинців — хакерів та крекерів, фріккерів та кібершахраїв, колекціонерів та піратів.

Протягом останнього десятиріччя істотно вивчались проблеми, пов'язані з бурхливим розвитком феномена, відомого в усьому світі під назвою «комп'ютерна злочинність», або білокомерційна злочинність у сфері високих технологій. На сьогодні це поняття (досить умовно) включає всі протизаконні дії, при яких електронне опрацювання інформації було знаряддям їх вчинення або їх об'єктом. Таким чином, у це коло проблем потрапили не тільки злочини, безпосередньо пов'язані з комп'ютерами, але й такі, як шахрайство з кредитними магнітними картками, злочини у сфері телекомунікацій (шахрайство з оплатою міжнародних телефонних переговорів), незаконне використання банківської мережі електронних платежів, програмне «піратство», шахрайство з використанням ігрових автоматів та багато інших. До цієї групи проблем належать також ті, що пов'язані з використанням доказів комп'ютерного походження при розслідуванні традиційних злочинів.

Комп'ютерна високотехнологічна злочинність — це міжнародне явище, рівень якого тісно пов'язаний з економічним рівнем розвитку суспільства у різних державах та регіонах. При цьому менш розвинуті у технічному відношенні країни завдяки діяльності міжнародних правоохоронних організацій мають можливість використати досвід більш розвинутих країн для запобігання, протидії та викриття комп'ютерних злочинів. Загальні тенденції, злочинні засоби та заходи запобігання, що ґрунтуються на єдності технічної, програмної та методичної бази цих злочинів, у різні проміжки часу є однаковими у різних країнах.

Таким чином, поняття «комп'ютерна злочинність» разом з розвитком ком-

п'ютерних, телефонних і телекомунікаційних високих технологій поступово трансформувалось у поняття злочинів у сфері високих інформаційних технологій.

Характерні риси злочинності в галузі високих інформаційних технологій мають:

– як правило, міжнародний характер злочину (виходить за рамки кордону однієї держави);

– труднощі у визначенні «місця знаходження» злочину;

– слабкі зв'язки між ланками в системі доказів;

– неможливість спостерігати і фіксувати докази візуально;

– широке використання злочинцями засобів шифрування інформації.

Громадськість усе більше цікавиться цими питаннями, оскільки кожна людина, суспільство чи держава, кожний власник або користувач комп'ютера, телефону, радіотелефону, модему, пластикової картки — це потенційний потерпілий, якого можуть очікувати тяжкі наслідки в разі вчинення злочину, особливо у державному, комерційному та промисловому секторі, де можливі великі фінансові затрати. Комп'ютерні злочинці за допомогою міжнародних комп'ютерних мереж — типу Internet, трансп'ютерних, нейрокомп'ютерних та Grid мереж і технологій — поширюють свій кримінальний досвід, не звертаючи уваги на національні кордони, що вимагає відповідних кроків кооперації від правоохоронних установ, протидіючих цим злочинам, оперативного обміну інформацією про комп'ютерні злочини.

Це обумовлено тим, що кібернетика, нейробіоніка і інформатизація сьогодні ввійшла у четвертий етап свого розвитку. Перший був пов'язаний із появою великих комп'ютерів (мейнфреймів), другий — зі створенням персональних комп'ютерів, третій — із появою Інтернету, який об'єднав користувачів у єдиний інформаційний простір шляхом сумісного доступу до інформації. З XXI століття почався перехід на нові Grid-технології, коли на зміну вже звичному Інтернету з його web-послугами йде всесвітня Grid-мережа як засіб сумісного використання обчислювальних потужностей та сховищ даних, Grid дозволяє вийти за рамки простого обміну даними між комп'ютерами і зрештою перетворити їхню глобальну мережу на свого роду гігантський віртуальний комп'ютер, доступний у режимі віддаленого доступу з будь-якої точки, незалежно від місця розташування користувача.

Таким чином з розвитком глобальних комп'ютерних та телекомунікаційних мереж набула поширення практика промислового шпигунства. Саме тому проблеми розробки систем захисту та збереження державної, приватної, службової та комерційної таємниці набувають сьогодні особливого значення. Багато проблем виникає у зв'язку з крадіжками послуг, зокрема вторгнення до телефонних мереж та незаконна торгівля послугами зв'язку. Також Internet широко використовують торговці піратським програмним забезпеченням, порнографією, зброєю та наркотиками для ведення справ, обміну інформацією, координації дій. Комп'ютерні мережі, окрім усього, можуть стати об'єктом нападу терористів. У травні 1998 р. «тигри звільнення Тамілу» у Шрі-Ланці

вперше серед терористичних груп провели кібернетичну атаку, спрямовану проти посольств у столиці.

Починаючи з 1991 р. при Генеральному секретаріаті Інтерполу діє робоча група з проблем комп'ютерної злочинності, яка вивчає цей вид злочинів у різних країнах світу, розробляє рекомендації, допомагає у стандартизації національних законодавств, напрацьовує методичний досвід розслідування комп'ютерних злочинів, запобігання, протидії їм.

За час існування ця група створила сучасну класифікацію комп'ютерних злочинів, розробила уніфіковану форму повідомлення (запиту) про такі злочини, працює над створенням довідників «Комп'ютери та злочини», намагаючись стандартизувати методи та процедури розслідування у різних країнах, щорічно організовує навчальні курси по підготовці фахівців.

Розширення сфери діяльності робочої групи викликало її перейменування у 1996 р. в Європейську робочу групу з проблем злочинності у сфері інформаційних технологій. Були визначені три пріоритетні напрямки діяльності робочої групи:

1) Internet — аналіз ситуації, дослідження питань правового і поліцейського характеру;

2) шахрайства з використанням електронних засобів платежу;

3) шахрайства з використанням різних засобів зв'язку і телекомунікацій.

Особлива увага приділяється саме питанням міжнародного співробітництва, партнерства, порозуміння під час розслідування комп'ютерних злочинів. У багатьох країнах світу для боротьби з цим видом злочину створені спеціалізовані підрозділи, кіберкоманди, які займаються виявленням, розслідуванням комп'ютерних злочинів та збиранням іншої інформації з цього питання на національному рівні. Саме спеціалізовані національні поліцейські підрозділи утворюють головне ядро сил протидії міжнародній комп'ютерній злочинності. Такі підрозділи вже створені і діють тривалий час у Сполучених Штатах Америки, Канаді, Великій Британії, Німеччині, Швеції, Швейцарії, Бельгії, Португалії, Австрії, Польщі та багатьох інших країнах світу.

Беззаперечним міжнародним авторитетом у галузі безпеки Internet є служба Computer Energency Response Team (CERT), заснована Інститутом розробки програмного забезпечення Пітсбурзького університету Карнегі-Мелона (Carnegie Mellon University Pittsburgh, США). Працівники FIRST допомагають користувачам Internet виявляти випадки проникнення в інформаційні системи, розробляти та розповсюджувати посібники з інформаційної безпеки тощо.

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 1990-х рр. 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.

Для того щоб інформація з інших країн швидко і в доступній формі (мова

повідомлення, специфічні терміни, коди злочинів тощо) надходила до національних спеціалізованих підрозділів (якщо їх немає, то до інших компетентних органів), для оперативного обміну такою інформацією між країнами, Генеральний секретаріат Інтерполу ще у 1994 р. рекомендував усім країнам — членам організації створити національний центральний консультативний пункт з проблем комп'ютерної злочинності (national central reference point) і закріпити конкретних співробітників для роботи з інформацією про комп'ютерні злочини. Ці пункти створені, як правило, в апараті національних бюро Інтерполу або у спеціалізованих підрозділах, які займаються комп'ютерною злочинністю й економічними злочинами. На базі НЦБ Інтерполу в Україні такий пункт був створений 17 вересня 1996 р.

Це дало можливість накопичити матеріал про законодавче регулювання та організаційний досвід розкриття і розслідування комп'ютерних високотехнологічних злочинів, запобігання їм у різних країнах світу, підготувати низку аналітичних оглядів і публікацій з актуальних питань, ознайомити співробітників МВС, СБУ, МО, МНС, прокуратури, суду з цим новим для України видом злочинів, внести конкретні пропозиції по вдосконаленню чинного кримінального і кримінально-процесуального законодавства України.

Сьогодні спеціалізовані команди, установи і органи правопорядку України на партнерських засадах активно і тісно співпрацюють, взаємодіють та знаходять порозуміння з такими відомими відомствами, установами і організаціями світу, як спеціальні комітети Організації Об'єднаних Націй (ООН). Група з розробки фінансових заходів боротьби з відмиванням коштів (FATF), Єгмонтська група підрозділів фінансової розвідки, Рада Європи / Європейська комісія, Спеціальний комітет експертів Ради Європи із взаємної оцінки заходів протидії відмиванню коштів (MONEYVAL), МАГАТЕ, Міжнародна організація з міграції, Інтерпол, Європол, Секретаріат Співдружності націй, Європейський банк реконструкції і розвитку (EBRD), Центральний європейський банк (ECB), Міжнародна асоціація страхових спостерігачів (IAIS) Міжнародний валютний фонд, Міжнародна організація цінних паперів (IOSCO), Світовий банк, Офшорна група банківських спостерігачів (OGBS), Світова митна організація (WCO) та інші, що дозволяє ефективно діяти і сприяти швидкому розслідуванню нових загроз та викликів третього тисячоліття, запобіганню, протидії їм — високотехнологічній інтелектуальній білокомірцевій комп'ютерній злочинності, міжнародному тероризму, біологічному тероризму, радіаційному тероризму, міжнародним фінансово-економічним злочинам, легалізації (відмивання) ресурсів, кримінальних капіталів, брудних коштів та доходів, отриманих злочинним шляхом, корупції, ухиленню від сплати податків і шахрайству (включаючи махінації з приватизацією, білого, сірого і чорного рейдерства), контрабанді, злочинам із торгівлею людьми, зброєю, наркотичними та радіоактивними речовинами, тінізації економік ряду країн світу тощо.