Круль С.М

ЗЛОЧИНИ У СФЕРІ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ: НАЦІОНАЛЬНИЙ ТА МІЖНАРОДНИЙ АСПЕКТИ

УДК 343.9

Протягом останнього двадцятиріччя в світі триває про¬цес формування інформаційного суспільства, а тому все більше розвиваються обчислювальні та інформаційні мере¬жі — унікальний симбіоз комп'ютерів і комунікацій. З кож¬ним днем активніше розвиваються сучасні інформаційні тех¬нології і в Україні. Людська цивілізація на межі тисячоліть вступила в еру інформації. Світовою системою комп'ютер¬них комунікацій щодня користуються сотні мільйонів людей... Це надає нових можливостей розвитку національної культури, освіти, науки й економіки. Але поширення інформаційних технологій має і негативний аспект: відкриває шлях до антисоціальної та злочинної поведінки. Комп'ютерні системи містять в собі нові, дуже досконалі можливості для невідомих раніше правопорушень, а також для скоєння традиційних злочинів, але нетрадиційними засобами [1, с.8].

Крім того, що злочини, які вчинені з використанням переваг найсучасніших технологій, завдають великих економічних збитків, суспільство стає все більш залежним від роботи автоматизованих 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 і телекомунікаційних мереж, а також можливість підключення до них через звичайні телефонні лінії посилюють можливості їх використання для кримінальної діяльності.

Безумовно, найбільше від таких злочинів потерпають розвинуті в технічному відношенні країни, однак і в інших країнах з початком процесу комп'ютеризації створюються сприятливі умови для скоєння таких злочинів. Зокрема, глобальна комп'ютерна мережа Internet надає можливість увійти до будь-якої світової відомчої комп'ютерної системи, у тому числі і військової. До того ж це можна зробити майже з будь-якої точки світу. Порівняно з Великобританією, 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 в недалекому майбутньому такі злочини можуть призвести до глобальних катастроф – екологічних, економічних,

транспортних тощо. Введення сучасної системи управління культурою, освітою, наукою, медициною, рухом літаків у повітрі, поширення телекомунікаційної мережі, впровадження системи електронних платежів, використання комп'ютерів у діяльності правоохоронних органів та у військовій справі значно розширили сферу діяльності всіх різновидів комп'ютерних злочинців (хакерів та крекерів, фріків та кібершахраїв, колекціонерів та піратів).

Упродовж років науковцями вивчались проблеми, пов'язані з бурхливим розвитком феномену, відомого в усьому світі під назвою «комп'ютерна злочинність». Загальноприйнято, що це поняття включає всі протизаконні дії, при яких електронне опрацювання інформації було знаряддям їх скоєння або їх об'єктом.

Отже, комп'ютерна злочинність – це міжнародне явище, рівень якої тісно пов'язаний з економічним рівнем розвитку суспільства в різних державах та регіонах. При цьому менш розвинуті в технічному відношенні країни завдяки діяльності міжнародних правоохоронних організацій мають можливість використати досвід більш розвинутих країн для запобігання та викриття комп'ютерних злочинів. Загальні тенденції, злочинні засоби та заходи запобігання є в різні відрізки часу однаковими для різних країн, що базується на єдності технічної, програмної та методичної бази цих злочинів [3, с.137].

Таким чином, поняття «комп'ютерна злочинність» разом з розвит¬ком комп'ютерних, телефонних технологій поступово трансформу¬валось у поняття злочинів у сфері інформаційних технологій.

Характерні риси злочинності в галузі інформаційних технологій:

1. як правило, міжнародний характер злочину (виходить за межі однієї держави);

2. труднощі у визначені «місцезнаходження» злочину;

3. слабкі зв'язки між ланками в системі доказів;

4. неможливість спостерігати і фіксувати докази візуально;

5.широке використання злочинцями засобів шифрування інформації. [2, с.211]

Громадськість усе більше цікавиться цими питаннями, оскільки кожний власник або користувач комп'ютера, телефону, модему, пластикової картки – це потенційний потерпілий, якого можуть очікувати тяжкі наслідки в разі вчинення злочину, особливо в державному, комерційному та промисловому секторах, де можливі великі фінансові втрати. Комп'ютерні злочинці за допомогою міжнародних комп'ютерних мереж – типу Інтернет – широко розповсюджують свій кримінальний досвід, не звертаючи уваги на національні кордони, що вимагає відпо-

відних кроків кооперації від правоохоронних установ, що протидіють цим злочинам. Усе це вимагає оперативного обміну інформацією про комп'ютерні злочини.

Починаючи з 1991 року при Генеральному Секретаріаті Інтерполу діє Робоча група з проблем комп'ютерної злочинності, яка вивчає цей вид злочинів у різних країнах, розробляє рекомендації, допомагає в стандартизації національних законодавств, напрацьовує методичний досвід розслідування комп'ютерних злочинів.

За час існування Робоча група створила сучасну класифікацію комп'ютерних злочинів, розробила уніфіковану форму повідомлення (запиту) про такі злочини, працює над створенням довідника «Комп'ютери та Злочини», намагаючись стандартизувати методи й процедури розслідування в різних країнах, щорічно організує навчальні курси з підготовки національних кадрів фахівців.

Розширення сфери діяльності Робочої групи привело її до перейменування 1996 року в Європейську робочу групу з проблем злочинності у сфері інформаційних технологій, та було визначено три пріоритетні напрямки діяльності даної 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 при розслідуванні комп'ютерних злочинів. У багатьох країнах для боротьби з цим видом злочину створені спеціалізовані підрозділи, які займаються виявленням, розслідуванням комп'ютерних злочинів та збором 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, Великобританії, Німеччині, Швеції, Швейцарії, Бельгії, Португалії, Австрії, Польщі та багатьох інших країнах. [3, с.139]

Для того, щоб інформація з інших країн швидко та в доступній формі (мова повідомлення, специфічні терміни, коди злочинів тощо) надходила до національних спеціалізованих підрозділів (якщо їх немає, то до інших компетентних органів), а також для оперативного обміну такою інформацією між країнами, Генеральний Секретаріат Інтерполу ще 1994 року рекомендував усім країнам – членам орга¬нізації створити національний центральний консультативний пункт з проблем комп'ютерної

злочинності (National Central Reference Point) та закріпити конкретних співробітників для роботи з інформацією про комп'ютерні злочини. На даний час 18 європейських країн уже створили такі пункти й надіслали інформацію до Генерального Секретаріату. Ці пункти створені, як правило, в апараті Національних бюро Інтерполу або в спеціалізованих підрозділах, які займаються комп'ютерною злочинністю або економічними злочинами.

На базі НЦБ Інтерполу в Україні такий пункт був створений 17 вересня 1996 року. Це дало можливість накопичити матеріал про законодавче регулювання та організаційний досвід попередження, розкриття і розслідування комп'ютерних злочинів у різних країнах, підготувати низку аналітичних оглядів і публікацій з цих питань, ознайомити співробітників МВС, прокуратури, суду з цим, порівняно новим для України, видом злочинів, внести конкретні пропозиції щодо удосконалення кримінального законодавства України [2, с.211].

1. Інформаційна діяльність в правознавстві: Монографія. – К.: Наука і життя, 2007. – 244 с.
2. Криміналістика: підручник – за ред. П.Д. Біленчука – К.: Право, 1997 – 256 с.
3. П.Д. Біленчук, М.Т. Задояний. Основи криміналістики: інноваційні технології та основи організації розслідування злочинів: навчальний посібник. – Черкаси: Східноєвропейський ун-т економіки і менеджменту, 2008. – 193 с.

Krul S.M.

Crimes in the Sphere of informative Technologies: the national and international Aspects

The author opens the question of crimes in the sphere of informative technologies, he defines this kind of crime and gives its features. The activity of European working group in the sphere of informative technologies is analyzed.

Key words: crimes in the sphere of informative technologies, the computer crimes, European working group in the shpere of informative techmologies, Internet.