

УДК 342.9

М.В. ГУЦАЛЮК, кандидат юридичних наук, доцент, с.н.с.,
виконавчий директор Державного підприємства
“Державний центр персоналізації документів” МВС України

ДЕРЖАВНА СИСТЕМА ПРОТИДІЇ ПРАВОПОРУШЕННЯМ У СФЕРІ КОМП'ЮТЕРНИХ ТЕХНОЛОГІЙ ТА ІНФОРМАЦІЙНИХ МЕРЕЖ

Анотація. Щодо протидії правопорушенням у сфері використання комп'ютерних технологій та створення Міжвідомчого центру боротьби з комп'ютерною злочинністю.

Україна пишається своїми досягненнями в розвитку інформаційних технологій, які пов'язані з іменем засновника школи кібернетиків, всесвітньо відомого науковця і розробника першого персонального комп'ютера В.М. Глушкова. Сьогодні, коли наша держава інтегрується в світове інформаційне суспільство, неможливо навіть уявити не тільки певну галузь народного господарства, а й окрему установу, офіс чи навчальний заклад, які не використовували б комп'ютерну техніку та локальні або глобальні комп'ютерні мережі. Від роботи сучасних програмно-технічних комплексів, які використовуються в медичних закладах, залежить здоров'я і навіть життя людей. Електронно-обчислювальні машини здійснюють фінансові операції, відстежують енергопостачання, використовуються в Збройних Силах та правоохоронних органах, тобто практично все залежить від надійності функціонування програмного забезпечення.

Водночас, разом із зростанням довіри до засобів обчислювальної техніки посилюється і загроза їх використання з метою вчинення правопорушень. Якщо у 70-ті роки минулого століття це були поодинокі випадки, які в основному сприймалися як показник віртуозності програміста, то у новому тисячолітті так звана кіберзлочинність стала однією з найбільших загроз світової спільноти, збитки від якої сягають мільярдів доларів. Набули поширення транскордонні злочини, коли хакер знаходиться в одній країні, банк, що зазнає збитків, – в другій, а кошти “відмиваються” в третій. Організовані злочинні групи та терористичні угруповання почали використовувати інформаційні технології. Відчуття безкарності злочинців, якими керують подібні традиційним злочинам мотиви, такі як помста, жадоба влади, жадібність, стає причиною зростання кількості правопорушень, які все більше характеризуються фінансовими втратами як окремих громадян, так і установ, в першу чергу банківської сфери [1]. Як приклад, можна навести справу Максима Ковальчука, який з 2000 року ошукував громадян США, використовуючи Інтернет-аукціон eBay, зламував сайти відомих фірм, включаючи Microsoft, розповсюджував контрафактну продукцію та вчинив інші правопорушення, чим завдав збитків на суму понад 100 млн. доларів [2].

Зазначене змушує шукати відповідних заходів протидії як окремим країнам, так і світовій спільноті у цілому. В Резолюції Генеральної Асамблеї ООН № 57/53 від 30 грудня 2002 року йдеться про те, що інформаційні технології можуть бути використані в цілях, несумісних із задачами забезпечення міжнародної стабільності та безпеки і негативно впливати на цілісність інфраструктури держав, порушуючи їх безпеку як у цивільній, так і у військовій сферах [3]. ООН закликала держави сприяти розробці заходів з обмеження загроз інформаційній безпеці та вивчення міжнародних конвенцій, що спрямовані на зміцнення безпеки глобальних інформаційних та телекомунікаційних систем.

В цілому, зокрема у Європейському співтоваристві, наприкінці 1990-х років був створений досить об’ємний пакет нормативно-правових актів, які регламентують суспільні відносини у сфері інформаційно-комунікаційних технологій.

Зважаючи на викладене, у грудні 2002 року в Лондоні пройшов Перший міжнародний конгрес по кіберзлочинності (E-Crime Congress), в роботі якого брав участь автор [4]. Під час роботи конгресу правоохоронці з десятків країн світу, працівники Інтерполу та Європолу, фахівці у галузі захисту інформації мали змогу обмінятися думками та налагодити стосунки з питань координації протидії кіберзлочинності. Важливим висновком також стала необхідність плідної співпраці правоохоронців з громадськими організаціями, провайдерами, службами безпеки установ тощо.

В Україні феномен створення інформаційного суспільства і необхідну його складову – інформаційну безпеку почали активно досліджувати з 90-х років минулого століття. Серед вітчизняних науковців, які вивчали проблему протидії правопорушенням у сфері використання інформаційних технологій, слід зазначити Д. Азарова, Н. Ахтирську, В. Бутузова, В. Гавловського, В. Голубева, Р. Калюжного, М. Швеця та ін. Серед безумовних досягнень – прийняття Закону України від 9 січня 2009 р. № 537-V “Про Основні засади розвитку інформаційного суспільства в Україні на 2007-2015 роки”, нового розділу у Кримінальному кодексі, який передбачає покарання відповідно до Європейської конвенції про кіберзлочинність, яка була ратифікована Верховною Радою України 2002 р., розробка проекту Концепції боротьби з кіберзлочинністю, роботи по створенню проекту Інформаційного кодексу.

Разом з тим, як свідчить аналіз співвідношення статистики виявлених злочинів темпам розвитку інформаційних технологій, більшість правопорушень залишаються невиявленими, а значна частина з порушених кримінальних справ не доходить до суду. Як відомо, ефективна протидія як “традиційним” правопорушенням, так і „комп’ютерним” можлива лише за умови створення державної комплексної системи, яка передбачала б існування відповідної нормативно-правової бази, в першу чергу кримінальної та адміністративної відповідальності, спеціальних підрозділів, співробітники яких могли б оперативно відстежувати правопорушення та ефективно реагувати на них, скажімо, як працівник ДАІ, систему спеціальних технічних пристроїв для документування правопорушень та постійне навчання і підвищення кваліфікації особового складу, адже новітні технології змінюються надзвичайно інтенсивно.

Першу комплексну підготовку працівників правоохоронних органів було проведено у 2003 році в Національній академії МВС України за участі закордонних фахівців. На спеціалізованих тренінгах питання виявлення злочинів, документування, особливостей слідчих дій вивчали десятки співробітників МВС, СБУ, експертно-криміналістичних установ, Генеральної прокуратури, судді. На практичних семінарах були представлені всі регіони України, а слухачі мали змогу обмінятися досвідом із закордонними фахівцями, включаючи найбільш досвідчених у цій галузі співробітників ФБР.

На сьогодні, незважаючи на ратифікацію 7 вересня 2005 р. Конвенції про кіберзлочинність від 23 листопада 2001 року, в Україні ще не створено спеціалізований підрозділ, мета якого – надання цілодобової допомоги для розслідування кримінальних правопорушень, пов’язаних з комп’ютерними системами, зокрема, надання технічних порад, збереження електронних даних для компетентних органів, ідентифікація правопорушника, надання даних про рух інформації тощо. Слід зазначити, що п. 2а ст. 27 Конвенції передбачено забезпечення кожною стороною кваліфікованим персоналом

та відповідним обладнанням. Ці завдання ще належить виконати вітчизняним правоохоронцям. А розпочати свою діяльність відповідний підрозділ повинен з аналізу криміногенної ситуації, адже за деякими дослідженнями латентність цих видів злочинів становить понад 90 відсотків.

Крім того, настала нагальна потреба ввести у вищих навчальних закладах правоохоронних органів спеціалізовані дисципліни, у яких вивчалися б не тільки основи виявлення та розслідування злочинів у сфері інформаційних технологій, а й використання комп’ютерної техніки для протидії традиційній злочинності, що започатковано учнем В.М. Глушкова, М.Я. Швецом та вихованими ним науковцями.

Використана література

1. Комп’ютерний тероризм: суперхакери, кібертерористи, кібер-криміналісти: монографія ; за заг. ред П.Д. Біленчука. – К. : Наука і життя, 2008. – 291 с.
2. Карнаухов С., Козлов И.. Америка требует выдачи арестованного в Бангкоке 25-летнего жителя Тернополя, утверждая, что он один из наиболее опасных хакеров в мире и нанес ведущим компьютерным компаниям в США ущерб в размере 100 миллионов долларов / “Факты и комментарии” от 31 мая 2003 г.
3. Резолюція Генеральної Асамблеї ООН № 57/53 від 30 грудня 2002 року. – (Досягнення в сфері інформатизації і телекомунікацій в контексті міжнародної безпеки).
4. Гуцалюк М. Перший міжнародний стратегічний конгрес “E-CRIME 2002” / Крок. – 2002. – № 24. – С. 7.

~~~~~ \* \* \* ~~~~~