УДК 658.1

В.Ф. Столбов[1], О.Г. Зима[2]

[1]*Інститут підготовки юридичних кадрів для СБ України Національної юридичної академії України ім. Я. Мудрого, Київ*
[2]*Харківський національний економічний університет, Харків*

АНАЛІЗ БОРОТЬБИ З КОМП'ЮТЕРНОЮ ЗЛОЧИННІСТЮ

Нові інформаційні технології дали не тільки унікальні можливості для більше активного й ефективного розвитку економіки, політики, держави й суспільства, але й стимулювали виникнення й розвиток негативних процесів. Одним з них є поява комп'ютерної злочинності.

Цьому сприяє і постійний ріст користувачів персональних комп'ютерів і мережі Інтернет. Це в свою чергу призвело до виникнення нових негативних явищ: атак хакерів на web-ресурси, Інтернет-шахрайств, поширення комп'ютерних вірусів і СПАМів, розповсюдження дитячої порнографії і виникнення кібертероризму.

По оцінках експертів з питань боротьби з комп'ютерною злочинністю правоохоронних органів країн Центральної й Східної Європи, прибутки від злочинної діяльності у сфері використання електронно-обчислювальних машин (назва із ст. 361 КК) посідають третє місце після доходів від наркоторгівлі і продажу зброї, а нанесені збитки уже зараз оцінюється мільярдами доларів. Тільки в США щорічно економічні збитки від такого роду злочинів становлять біля $100 млрд.

Характерною рисою комп'ютерних злочинів є їх дуже висока латентність й надмірно великі розміри нанесених збитків. Інформація про комп'ютерні злочини не завжди стає загальновідома, як свідчать наукові дослідження, тільки 10 – 15% комп'ютерних злочинів стають надбанням гласності тому, що організації, які постраждали в їх наслідок, із боязні втратити репутацію чи його повторного вчинення у їх відношенні, досить неохоче надають інформацію про такі протиправні дії. Тому, мабуть, ніхто у світі не має сьогодні повної картини комп'ютерної злочинності. Зрозуміло, що державні й комерційні структури, які піддалися нападам, не дуже схильні афішувати наслідки, заподіяні нападами, і "ефективність" своїх систем захисту. Але й ті факти, які стали відомими, роблять сильне враження.

Однієї із серйозних причин низького розкриття такого виду злочинів є й транснаціональна (трансгранична) складова, тобто коли злочинець, перебуваючи в одній державі, вчиняє протиправні діяння відносно об'єкта, який знаходиться в іншій державі за багато тисяч кілометрів.

Останнім часом все частіше чується слово "Кібертероризм".

Аналізуючи суспільну небезпеку кіберзлочинності, необхідно відзначити появу високотехнологічного тероризму - особливо комп'ютерного тероризму або кібертероризму. Ця форма тероризму викликає особливу занепокоєність в експертів у зв'язку з високою уразливістю комп'ютерних систем керування інфраструктурою (транспорт, атомні електростанції, водопостачання й енергетика), підключених до Інтернету.

Кібертероризм являє собою серйозну соціально небезпечну загрозу для людства, порівнянну з ядерною, бактеріологічною й хімічною зброєю. Причому ступінь цієї загрози в силу своєї новизни ще не до кінця усвідомлена й вивчена. Наявний досвід світового співтовариства у цій області з усією очевидністю свідчить про безсумнівну уразливість будь-якої держави, тим більше, що кібертероризм не має державних кордонів й кібертерорист здатний рівною мірою загрожувати інформаційним системам, розташованим практично в будь-якій точці земної кулі. Виявити й нейтралізувати віртуального терориста досить складно через занадто малу кількість слідів, які залишаються ним, на відміну від реального світу. Особливу заклопотаність у правоохоронних органів викликають терористичні акти, пов'язані з використанням глобальної мережі Інтернет.

Резюмуючи із приводу проблеми кібертероризму, можна сміло затверджувати, що це суспільне небезпечне явище не міф, а реальність як для всього світового співтовариства, так і для нашої держави. Масовий перехід на методи електронного керування технологічними процесами у виробництві приведе нашу країну, як уже привів розвинені держави, до принципово нових видів злочинів, у тому числі до електронного тероризму.

Аналіз світових тенденцій розвитку електронного тероризму дозволяє сьогодні зробити з великою часткою ймовірності висновок про те, що загроза з кібернзлочинності з кожним роком буде зростати.

Таким чином, проблему боротьби з комп'ютерною злочинністю сьогодні вже треба ставити на один рівень із традиційним тероризмом і організованою злочинністю. Для її подолання чи, принаймі, зменшення негативних наслідків, необхідно здійснювати комплексний підхід на міжнародному рівні.