Удосконалення боротьби зі злочинами у сфері використання автоматизованих електронно-обчислювальних систем

Боротьба зі злочинністю у сфері використання автоматизованих електронно-обчислювальних систем[\*](#_ftn1) (далі – комп’ютерні злочини), вже сьогодні є одним з важливіших державних завдань. Для того, щоб ця боротьба була максимально ефективною, безумовно необхідно дослідження цієї ще нової для нашого суспільства форми злочинності, її складових, виявлення закономірності і тенденцій, а також глибоке вивчення організаційно-правових та інших можливих заходів, що перешкоджають її поширенню, розробка заходів попередження і розслідування таких видів злочину.

При недостатній практиці розслідування комп’ютерних злочинів (далі – КЗ) і судового розгляду таких справ, необхідних для розробки їх криміналістичної характеристики, можливе застосування порівняльного аналітичного і прогностичного підходів. Джерелами їх здійснення є:

стан, структура, характеристика КЗ в країнах, де поширено ці діяння і розроблено засоби боротьби з ними;

досвід правового регулювання боротьби з цим видом злочинів;

практика виявлення, розслідування і профілактики;

діяльність правоохоронних структур щодо збору, накопичування та аналізу інформації, що стосується КЗ.

Стан КЗ характеризується наявністю діянь, предметом зазіхання яких є комп’ютерна інформація, її носії, або протиправними діями, для здійснення яких комп’ютер використовується як знаряддя.

У багатьох публікаціях зазначається значне зростання КЗ на Заході. Це підтверджують документи міжнародних організацій (Європейський комітет з проблем злочинності Ради Європи, Інтерпол), що дають підставу розглядати КЗ як транснаціональну проблему.

На такій небезпечній тенденції наголошувалося і у виступах учасників X конгресу ООН Щодо попередження злочинності і поводження з правопорушниками, який відбувся у Відні (Австрія) 10-17 квітня 2000 р. [1]

Вперше склад КЗ було сформульовано у 1979 р. на Конференції американської асоціації адвокатів в м. Далласі (США), де було запропоновано наступні формулювання:

використання або спроба використання комп’ютера, обчислювальної системи або мережі комп’ютерів з метою отримання грошей, власності або послуг, прикриваючись фальшивими прийменниками, помилковими обіцянками або видаючи себе за іншу особу;

навмисна несанкціонована дія, що має на меті зміну, пошкодження, знищення або викрадення комп’ютера, обчислювальної системи, мережі комп’ютерів або систем математичного забезпечення, що містяться в них, програм або інформації;

навмисне несанкціоноване порушення зв’язку між комп’ютерами, обчислювальними системами або мережами комп’ютерів.

Однак, ці пропозиції знайшли відображення в американському законодавстві лише через декілька років.

До сучасного складу КЗ включаються все нові види протиправних діянь, хоч і не скрізь досить оформлені у правовому відношенні. Так, на сьогодні до цього переліку вже відносять:

несанкціоноване проникнення в автоматизовані електронно-обчислювальні системи;

розкрадання системного і прикладного програмного забезпечення;

несанкціоноване копіювання, модифікацію або знищення комп’ютерної інформації;

блокування комп’ютерної інформації, шантаж та інші методи комп’ютерного тероризму;

комп’ютерне шпигунство;

підробку і фальсифікацію комп’ютерної інформації;

розробку і поширення комп’ютерних вірусів і програмних закладок;

несанкціонований перегляд або розкрадання інформації з банків даних і баз знань;

халатну недбалість при розробці, створенні автоматизованих електронно-обчислювальних систем і програмного забезпечення, що призводить до тяжких наслідків і втрати інформації;

механічні, електричні, електромагнітні та інші види впливу на автоматизовані електронно-обчислювальні системи;

мережеве шахрайство;

шахрайство з використанням пластикових платіжних карток;

використання глобальної інформаційної мережі Internet для вчинення віддалених атак проти електронно-обчислювальних систем.

Мабуть, цей перелік не є повним, а буде з часом поповнюватися, але щодо структури КЗ в узагальненому виді можна дотримуватися рекомендацій, що були наданими ще у 1990 р. Європейським комітетом з проблем злочинності Ради Європи для включення в законодавство європейських країн списку протиправних діянь у сфері комп’ютерної інформації:

1) комп’ютерне шахрайство;

2) комп’ютерна підробка;

3) пошкодження комп’ютерної інформації або комп’ютерних програм;

4) комп’ютерний саботаж;

5) несанкціонований доступ до комп’ютерних систем;

6) несанкціоноване перехоплення інформації;

7) несанкціоноване копіювання захищених комп’ютерних програм;

8) незаконне виробництво копій напівпровідникової продукції.

Робоча група Інтерполу, що була створена з січня 1991 р., теж прагне знайти шляхи розв’язання цієї проблем, які вже виникають не тільки на національному але й на міжнародному рівнях. Зарубіжними фахівцями було розроблено різні класифікації засобів здійснення КЗ. Однією з подібних класифікацій є кодифікатор робочої групи Інтерполу, що у 1991 р. був інтегрований в автоматизовану систему пошуку інформації і в цей час є доступним більш ніж для 100 країн.

Особливе значення має той факт, що відповідно до рекомендацій Європейського комітету з проблем злочинності Ради Європи на базі Національного центрального бюро Інтерполу в Україні створено Національний центральний консультативний пункт (НЦКП) з пробем КЗ, який здійснює збір і накопичення інформації стосовно КЗ, скоєних на території країни, і узагальнює практику їх розслідування; взаємодіє з НЦКП інших країн; здійснює інформаційне супроводження конкретних кримінальних справ, що мають транснаціональний характер.

Соціальна небезпека КЗ визначається негативними тенденціями, що мають відношення до КЗ на сучасному етапі. До них, на наш погляд, необхідно віднести:

високий ступінь їх розповсюдження;

дуже високий ступінь суспільної небезпеки (збитки від них часто не піддаються обчисленню);

ступінь латентності (чи не самий високий порівняно з іншими видами злочинів);

високий рівень професійної або “білокоміркової” злочинності;

транснаціональний характер їх окремих видів.

Певне уявлення масштабу КЗ дають експертні дані, і, насамперед, дані про злочини.

Відповідно до офіційної статистики у США з 90% опитаних, чиї комп’ютерні системи піддалися в 1999 році атакам у Internet, 74% стверджували, що проникнення в їх систему було пов’язане з розкраданням конфіденційної інформації через фінансове шахрайство (розкрадання інформації і фінансове шахрайство завдало шкоди на 68 млн дол. і 56 млн дол. відповідно). Фінансові втрати у 273 опитаних склали понад в 265 млн дол. Збитки від атаки типу “відмовлення в обслуговуванні” тільки у 1998 році склали 77 тис. дол., а у 1999 р. зросли до 116 тис. дол [2]. У лютому 2000 р. були атаковані відомі в усьому світі Web-сайти Yahoo. com, Amazon. com, CNN. com, eBay. com та ін., збиток від трьох днів атаки на ці сайти склав понад 1,2 млрд дол. США [3].

Постійне зростання КЗ і, насамперед, її транснаціональної складової як найбільш небезпечної, свідчить, що боротьба з нею ще не достатньо ефективна і не приносить позитивних наслідків.

Ця тенденція має відношення не тільки до України, але й стосується всього світу.

Причинами недостатньої ефективності боротьби, на наш погляд, є:

відсутність комплексного підходу до розробки заходів попередження і обмеження КЗ;

недосконалість українського законодавства;

використання виключно іноземного програмно-технічного забезпечення;

відсутність необхідних методик розслідування КЗ;

відсутність програм підготовки високоякісних фахівців-практиків в галузі боротьби з КЗ;

відсутність міжнародної взаємодії, міжвідомче розмежування діяльності правоохоронних органів з питань попередження і розслідування КЗ.

Іншою проблемою є відсутність фахівців-практиків у галузці попередження і боротьби з КЗ. Суб’єктами КЗ, як вже зазначалося раніше, виступають фахівці дуже високого рівня, злочинці-інтелектуали. Правоохоронні органи, на жаль, ще не можуть ефективно їм протидіяти. Матеріали перевірок і порушені кримінальні справи (якщо їх вдається порушити) втрачаються, а злочинці уникають відповідальності. Треба невідкладно, на рівні вузівської освіти готувати вузьких фахівців щодо боротьби з КЗ. Програма підготовки таких спеціалістів повинна включати в себе поглиблене вивчення інформатики та обчислювальної техніки і отримання практичних навичок щодо попередження і розслідування КЗ. Для вирішення цієї проблеми на кафедрі кримінального процесу і криміналістики Гуманітарного університету (“Запорізький інститут державного і муніципального управління”) з 1 вересня 2001 року планується викладання дисципліни “Попередження і розслідування злочинів у сфері використання автоматизованих електронно-обчислювальних систем”. Метою цієї дисципліни є ознайомлення студентів з поняттям і сутністю комп’ютерної інформації, основними засобами її зберігання та захисту, з кримінально-правовою і криміналістичною характеристикою таких видів злочину, особливостями розкриття і розслідування злочинів у сфері використання автоматизованих електронно-обчислювальних систем. Передбачена також тема стосовно попередження КЗ, в якій розглядаються питання безпеки автоматизованих електронно-обчислювальних систем і попередження КЗ при використанні глобальної інформаційної мережі Internet.

У рамках вирішення цієї проблеми необхідна не тільки вузівська підготовка таких фахівців, але й реалізація програм щодо підвищення кваліфікації практичних співробітників правоохоронних органів, які спеціалізуються у боротьбі з КЗ.

Ще однією, дуже важливою проблемою, залишається і неузгодженість зусиль правоохоронних органів на міжнародному рівні щодо попередження та розслідування транснаціональних КЗ, що отримали на Заході назву “кіберзлочини” (cyber crime).

Одним із серйозних кроків, спрямованих на врегулювання цієї проблеми, є прийняття Радою Європи (Council of Europe) 24 квітня 2000 р. проекту Конвенції щодо попередження киберзлочинів [4]. з огляду на складність проблеми, Рада Європи підготувала і опублікувала проект Конвенції щодо боротьби зі злочинами у кіберпросторі, який планується остаточно прийняти у вересні 2001 року. Реалізуючи положення цього документа, на національному рівні необхідна гармонізація кримінального законодавства з урахуванням рекомендацій Ради Європи і норм міжнародного права. Така необхідність викликана тим, що часто при вчиненні таких видів злочинів об’єкт і суб’єкт знаходяться в різній юрисдикції, існує дуже великий ризик того, що злочинці будуть здійснювати свої протиправні дії з території держав, де такі діяння не віднесено до кримінальних. Тому, на наш погляд, підписання і прийняття Україною запропонованої Конвенції щодо попередження кіберзлочинів сприятиме зміцненню міжнародного співробітництва у боротьбі з цими видами злочинів.

Криміногенна ситуація у сфері використання автоматизованих електронно-обчислювальних систем потребує комплексного підходу стосовно вирішення проблем попередження і розслідування КЗ. Застосування системи заходів завжди є більш ефективним, ніж вплив на злочинність окремими діями. Коли при розробці заходів дотримується комплексний системний підхід, що включає у себе різні рівні, тоді отримання позитивних результатів стає реальним.

Комплекс заходів щодо боротьби з КЗ повинен спиратися на єдину державну політику в цій галузі. Для цього, на наш погляд, повинна бути розроблена науково обґрунтована програма, яка включатиме заходи державного, політичного, економічного, соціального, правового та іншого характеру.

1. Golubev V.. Creating conditions for constructive international cooperation in combating the transnational computer crime - is the demand of the time // The Tenth United Nations Congress on the Prevention of Crime and the Treatment of Offenders, to be held in Vienna, Austria, from 15 April 2000. http://www. networkremotemonitor. com/articles/vienna. html

2. Statement for the Record of Louis J. Freeh, Director Federal Bureau of Investigation on Сybercrime Before the Senate Committee on Judiciary Subcommittee for the Technology, Terrorism and Government Information Washington, D. C. – 2000. – March 28.

3. http://www. fbi/gov/nipc/compcrime. html.

4. Computerword., - Киев., 2000. – 16 февраля. – С.29.

5. Draft Convention on Cyber-crime. – Strasbourg, 27.04.2000, Council of Europe. http://conventions. coe. int/treaty/en/projets/cybercrime. htm

[\*](#_ftnref1) У Проекті Кримінального кодексу України, прийнятому у другому читанні, передбачено Розділ 16. Злочини у сфері використання автоматизованих електронно-обчислювальних систем.