ЗАХИСТ ІНФОРМАЦІЙНИХ КОМП'ЮТЕРНИХ СИСТЕМ У ПРАВООХОРОННИХ ОРГАНАХ

Р. А. Калюжний,
начальник кафедри теорії і історії держави та права
Київського інституту внутрішніх справ,
доктор юридичних наук, професор;

М. В. Гуцалюк,
старший науковий співробітник
Міжвідомчого науково-дослідного центру
з проблем боротьби з організованою злочинністю,
кандидат юридичних наук

Серед основних тенденцій розвитку суспільства сьогодення слід відзначити глобальну інформатизацію практично всіх сфер життєдіяльності людини, включаючи економіку, державне управління, науку, мистецтво. Як показує досвід інших країн, інформатизація сприяє забезпеченню національних інтересів, поліпшенню керованості економікою, зростанню продуктивності праці, вдосконаленню соціально-економічних відносин, збагаченню духовного життя та подальшій демократизації суспільства [1]. Переваги нових інформаційних технологій широко використовуються для підвищення ефективності боротьби зі злочинністю та її профілактики. Уперше про важливість впровадження нових методів боротьби зі злочинністю, заснованих на досягненні науково-технічного прогресу, було зазначено на п'ятому Конгресі Організації Об'єднаних Націй з попередження злочинності. На шостому Конгресі 1980 року було рекомендовано усім державам активізувати свої зусилля щодо удосконалення систем збору інформації, у тому числі статистичної, для вивчення проблеми злочинності та функціонування систем правосуддя [2].

Інформатизація в правоохоронних органах України вже має певну практику та історію впровадження [3]. Комп'ютери дають змогу швидко опрацьовувати, передавати та зберігати великі обсяги інформації, значно покращувати якість управління, а головне, більш раціонально використовувати час, вивільняти працівників від рутинних операцій, надавати можливість виконувати творчу роботу.

Успішна боротьба зі злочинністю потребує того, щоб правоохоронні органи мали вірогідну інформацію про об'єкти, які потрапили у сферу карно-процесуальної та оперативної діяльності. Чим більше інформації має у своєму розпорядженні слідство про особу, об'єкти та обставини вчиненого злочину, тим швидше він розкривається. Від якісної та своєчасної інформації залежить і точність оцінки оперативної обстановки, і добротність управлінських рішень, і спрямованість планування оперативно-розшукових заходів, і чіткість постановки завдань виконавцям.

Для збору та прийняття такої інформації існують криміналістичні обліки, інакше – система карної реєстрації. Вони формуються спеціалізованими підрозділами правоохоронних органів. Частина інформації централізована в масштабі України, інша – в масштабі міста, області.

Однією з головних вимог, які ставляться до правоохоронної інформації, є її висока вірогідність та своєчасність. Неповна та несвоєчасна інформація позбавляє правоохоронців затримувати злочинців "по гарячих слідах". Налагоджений процес збору та опрацювання інформації дає можливість всебічно аналізувати обстановку, передбачати розвиток негативних тенденцій і приймати відповідні рішення.

Поряд з цим, стає все більш актуальною проблема надійного захисту комп'ютерної інформації, адже прогрес у різних галузях науки і техніки призвів до створення компактних і високоефективних технічних засобів, за допомогою яких можна легко підключатись до ліній телекомунікацій та різноманітних технічних засобів оброблення інформації з метою здобування, пересилання та аналізу інформації, яка становить державну та іншу передбачену законом таємницю конфіденційної інформації.

Злочинців може зацікавити не тільки знищення певної інформації (наприклад, про особу, що розшукується) або її модифікація (номер двигуну на викраденому автомобілі), але і зміст певного документу або ж повністю база даних з відповідного питання.

Усе більше в правоохоронних органах використовуються інформаційні системи, які базуються на Інтернет-технологіях. Зокрема, структурні підрозділи використовують Веб-сторінки для зв'язків з громадськістю. Тут необхідно зауважити, що такі системи є досить уразливими для хакерських атак. Так агентство національної безпеки США класифікує комп'ютери, з погляду їхньої стійкості для проникнення, на класи від D1, D2, D3 і далі до C, B і A. Комп'ютери класу A – це високоякісні комп'ютери, найбільш стійкі для проникнення. В нинішній час комп'ютер типу Windows NT – комп'ютер, що використовує Microsoft Windows NT як оперативне програмне забезпечення, – належить за цією класифікацією до порівняно низького класу C2. Якщо ж він з'єднується з системою Інтернет, то йому взагалі не привласнюється ніякого класу стійкості. Хоча це одна з найбільш розповсюджених комп'ютерних систем в американській військовій структурі [4].

Останнім часом у зв'язку зі збільшенням обсягів, кількості користувачів, видів випадкових впливів збільшується ймовірність несанкціонованого доступу до інформації. Так, не зважаючи на створення найбільш безпечної системи, поліція США має серйозні проблеми від кібер-атак, кількість яких значно зросла в останні місяці 2002 року. За словами Хізаши Сонода (Hisashi Sonoda), професора кримінального права Канзайського Університету національного Агентства поліції США (National Police Agency – NPA), в 57 поліцейських комп'ютерних мережах національного масштабу були встановлені цілодобові системи виявлення кібер-атак.

У трьохмісячний термін було зафіксовано 51 104 кібер-атак, що в середньому складає – 10 нападів на добу [5].

Для протидії витоку інформації по технічних каналах створюється комплексна система захисту, яка передбачає використання фізичних, апаратних, програмних і криптографічних засобів захисту інформації.

Означені системи дозволяють реалізувати такі методи захисту інформації:

- обмеження доступу;
- розмежування доступу;
- розподіл доступу;
- криптографічне перетворення інформації;
- контроль і облік доступу.

Слід відзначити, що технології, які необхідні для забезпечення надійного захисту, постійно ускладнюються. Наприклад, криптографічні методи, що оцінювалися як "відмінні" десятиліття назад, нині застаріли, оскільки комп'ютери, що використовуються правопорушниками, стали більш потужними і менш дорогими. Тому необхідно постійно стежити за досягненнями в цій галузі.

На жаль, через значну вартість в правоохоронних органах практично не застосовуються такі засоби виявлення несанкціонованого доступу, як "CyberPatrol", або, наприклад, ручні ідентифікатори для персоналізації доступу до інформаційних систем.

Необхідно повсякденно приділяти увагу захисту приміщень, що є складовою частиною загальних заходів для захисту комп'ютерної інформації. Адже комп'ютер, не з'єднаний з іншими комп'ютерами, забезпечує досить надійне збереження інформації, хоча слід не розповсюджувати інформацію про кількість, типи і навіть розміщення електронних пристроїв.

Важливою умовою успішного захисту комп'ютерних систем є відповідне правове забезпечення як інформаційних систем зокрема, так і інформаційних відносин у суспільстві в цілому. Сьогодні необхідність реформування інформаційного законодавства не викликає сумнівів. Однак, на наш погляд, масив законів і підзаконних актів досяг такої критичної межі, яка об'єктивно вимагає кодифікації. Стратегія реформування знайшла своє відображення у Концепції реформи інформаційного законодавства України, розробленої ініціативною групою науковців. З текстом Концепції можна ознайомитись на сайті Міжвідомчого науково-дослідного центру з проблем боротьби з організованою злочинністю – http://mndc. naiau. kiev. ua [6].

Безумовно, проблема захисту інформаційних ресурсів не буде вирішена в повному обсязі без кримінального переслідування комп'ютерних правопорушень. Специфіка розслідування злочинів у сфері високих технологій вимагає розробки принципово нової стратегії, тактики та методики, наявності спеціальних технічних засобів, створення центрів з підготовки відповідних фахівців, спеціалізованих інформаційних систем оперативного сповіщення. Без проведення такої роботи важко говорити про надійний інформаційний захист національної інфраструктури [7].

На відміну від західних, формування вітчизняних спецпідрозділів по боротьбі з комп'ютерними злочинами проходить в умовах реформування правоохоронних органів. Не зважаючи на певні труднощі, співробітниками створеного 2001 р. Управління по боротьбі зі злочинами у сфері високих технологій за рік розкрито так званих "комп'ютерних" злочинів у декілька разів більше, ніж за всі попередні роки, коли була введена відповідна норма до Кримінального кодексу України (ст. 198-1).

Але навіть спеціалізоване обладнання та підготовлений персонал повністю не вирішать проблеми надійного захисту (у відомих зарубіжних програмних продуктах існують незадокументовані можливості для отримання потрібної інформації). Більш комплексно питання слід вирішувати базуючись на вітчизняних розробках. Тому, необхідно розробити Концепцію розвитку вітчизняного інформаційного забезпечення. В першу чергу, це стосується органів державного управління та, зокрема, правоохоронних органів. Слід також активніше використовувати досвід українських фахівців у галузі захисту інформації, сміливіше впроваджувати в навчальний процес такі дисципліни, як інформаційне право, правова інформатика, розслідування злочинів, що вчиняються за допомогою комп'ютерних технологій [8].

У цілому, надійний захист інформаційних комп'ютерних систем у правоохоронних органах можливо забезпечити з урахуванням системного підходу [9], шляхом координації дій, починаючи від виявлення правопорушень та накопичення відповідних статистичних даних для наукових досліджень, закінчуючи проведенням кримінологічних експертиз і систем оперативного сповіщення відповідних міжнародних організацій [10].

Приділяючи належну увагу інформаційній безпеці, Конгрес США схвалив триразове збільшення фінансування досліджень в області запобігання комп'ютерних злочинів. Протягом наступних п'яти років Національному дослідницькому фонду і Національному інституту стандартизації і технологій будуть виділені 900 мільйонів доларів, у першу чергу, на підготовку наукових кадрів [11].

У Міжвідомчому НДЦ з проблем боротьби з організованою злочинністю при Координаційному комітеті наявний відповідний досвід дослідження зазначених проблем. У рамках теми "Координація діяльності органів влади у боротьбі з кіберзлочинністю" науковцями МНДЦ підготовлено проект Концепції стратегії реалізації державної політики щодо боротьби з кіберзлочинністю. Підготовлені навчальні посібники розіслано у практичні підрозділи. Зазначені питання розглядаються на лекціях і семінарах у відомчих навчальних закладах та у системі службової підготовки правоохоронних органів. Постійно здійснюється моніторинг комп'ютерної злочинності. Тому, підтримуючи пропозицію МВС стосовно створення відповідного міжвідомчого центру, передбаченого Указом Президента України "Про рішення Ради національної безпеки і оборони України від 31 жовтня 2001 р. "Про заходи щодо вдосконалення державної інформаційної політики та забезпечення інформаційної безпеки України" від 6 грудня 2001 р. № 193/2001 вважаємо за доцільне створення відповідного підрозділу у структурі Міжвідомчого НДЦ з проблем боротьби з організованою злочинністю за умови відповідного штатного та фінансового забезпечення, оскільки створення підрозділу з питань боротьби з комп'ютерною злочинністю на базі Міжвідомчого НДЦ буде значно дешевшим за створення ще одного самостійного Міжвідомчого центру.

Література:

1. Інформатизація, право, управління (організаційно–правові питання): Монографія / Р. А. Калюжний, О. Д. Крупчан, В. Д. Гавловський, М. В. Гуцалюк, В. С. Цимбалюк, М. Я. Швець. – К., 2002. – С. 33.
2. Руководство по компьютеризации информационных систем в области уголовного правосудия // ООН. Методологические исследования. — Нью-Йорк, 1992. – Серия F. – № 58. – С. 3.
3. Швец Н. Я. Автоматизированные системы управления органами внутренних дел. – К., 1983.
4. Jane's Intelligence Review. – 1999. – № 1. – P. 50-54.
5. http://www.crime-research.org.
6. Питання концепції реформування інформаційного законодавства України / Р. Калюжний, В. Гавловський, В. Цимбалюк, М. Гуцалюк // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні: Збірник. – К.: НТУУ"КПІ"; Міносвіти і науки України; СБУ. – К., 2000. – С. 17-21.
7. Гуцалюк М. Інтернет & Закон // Форпост. – 2001. – № 2. – С. 18-20.
8. Комп'ютерна злочинність: Навчальний посібник / П. Д. Біленчук, В. В. Бут, В. Д. Гавловський, М. В. Гуцалюк, Б. В. Романюк, В. С. Цимбалюк – К.: Атіка, 2002. – 240 с.
9. Гуцалюк М. В., Ящуринский Ю. В. Системный подход и формально-математические направления в теории управления // Сборник материалов методологического семинара 2. Системный подход как методологический базис формирования системного мышления: – К.: Академия СБУ, 1995. – С. 59-61.
10. М. Гуцалюк Координація боротьби з комп'ютерною злочинністю // Право України. – 2002. – № 5. – С. 121–126.
11. http://www.compulenta.ru.