УДК 002.6+342.7

КООРДИНАЦІЯ БОРОТЬБИ З КОМП'ЮТЕРНИМИ ПРАВОПОРУШЕННЯМИ

Михайло Гуцалюк
Міжвідомчий науково-дослідний центр з проблем боротьби з організованою злочинністю

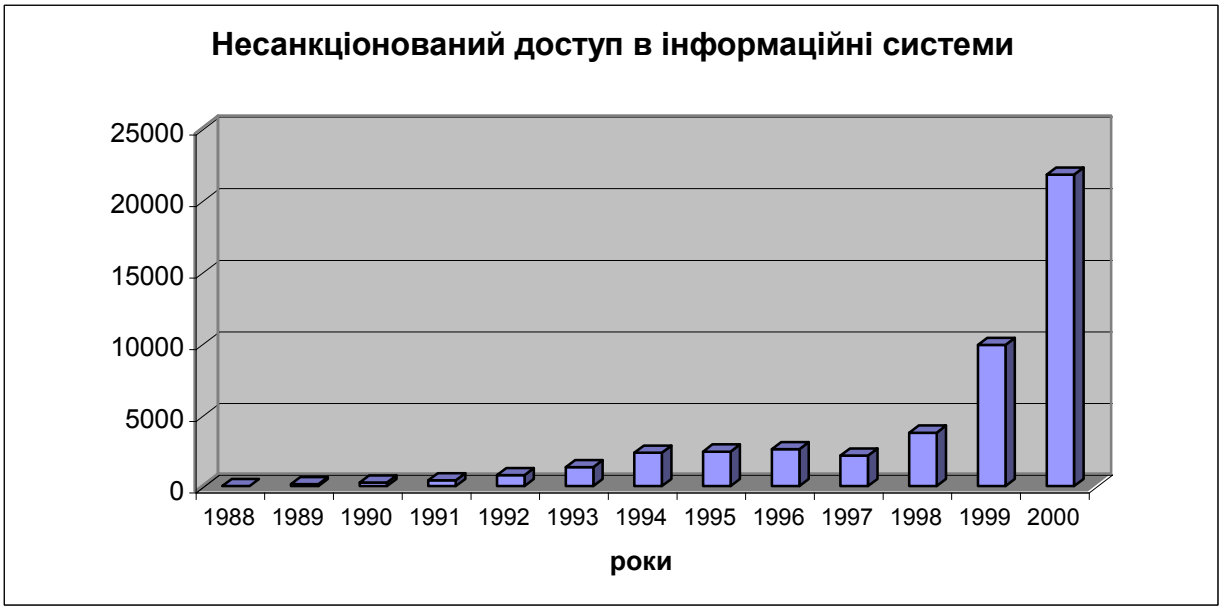
Анотація: **Пропонуються організаційно-правові заходи щодо координації боротьби з комп'ютерними правопорушеннями.**
Summary: **The organization-legal measures on coordination of struggle with computer offences are offered.**
Ключові слова: **Координація, комп'ютерна злочинність, асоціація захисників інформації.**

I Вступ

Сьогодні важко уявити сферу суспільного життя, в якій не використовуються сучасні інформаційні технології. Ефективна діяльність банків, аеропортів, телефонних станцій в значній мірі залежить від рівня використання інформаційних технологій. Особливо великі надії в розбудові інформаційного суспільства у Європі і в цілому світі покладаються на Інтернет та засновану на ньому електронну торгівлю.

Разом з тим високими технологіями почав активно цікавитися злочинний світ. Професійна майстерність деяких його представників, особливо в економічній та фінансовій сфері, викликає подив. Експерти в усьому світі визнають, що міжнародний характер сучасних комп'ютерних і телекомунікаційних технологій приводить до появи нових форм транснаціональної злочинності. Це призвело до появи такого феномену, як "комп'ютерна злочинність" (або "кіберзлочинність" від англ. cyber crime).

Стурбованість щодо появи цього небезпечного соціального явища помітна в усьому цивілізованому суспільстві. Ця гостра проблема обговорювалася на багатьох міжнародних форумах. Так, на конференції країн Великої вісімки щодо кіберзлочинності, яка проходила у жовтні 2000 року, міністр закордонних справ Німеччини Йошка Фішер відзначив, що збитки від кіберзлочинів сягають 100 мільярдів німецьких марок ($ 45 млрд.) щорічно! За оцінками Рахункової палати уряду США щорічний збиток від розкрадань і шахрайств, вчинених за допомогою інформаційних технологій тільки через Інтернет, досягає $ 5 млрд. Кількість комп'ютерних злочинів має тенденцію до зростання, що яскраво видно з аналізу одного з його видів – несанкціонованого доступу (дані Computer Emergency Response Team (CERT) – міжнародного авторитета в галузі безпеки Internet).



З іншого боку, статистичні дані свідчать, що кількість зареєстрованих та розкритих злочинів у нашій державі (за ст. 198-1 Кримінального кодексу України, що діяв донедавна) не перевищує десяти на рік та має

тенденцію до зниження. За повідомленням Національного центрального бюро Інтерполу в Україні, куди згідно з п. 4 Наказу МВС України № 572 від 17 серпня 1996 року надходить узагальнена інформація про вчинення комп'ютерних злочинів з ГУМВС–УМВС України в Криму, областях, містах Києві та Севастополі, ***у 2000 році "...фактів, де комп'ютерна техніка виступала як об'єкт скоєння злочину, в тому числі фактів несанкціонованого проникнення до локальних відомчих комп'ютерних мереж та банків даних зареєстровано не було***" [1].

Для порівняння наведемо дані МВС Росії, згідно з якими кількість злочинів у сфері високих технологій збільшилася на 60 відсотків з 1999 р. до 2000 р. до загальної кількості 1375. Серед них 584 – неправомірних доступів до комп'ютерних систем, 284 – пошкодження комп'ютерної інформації, 210 – використання комп'ютерів для шахрайства (WJIN).

Національне поліцейське управління Японії повідомило, що у першому півріччі 2001 року кількість злочинів, вчинених з використанням Інтернет, збільшилася на 60 відсотків (News.Battery.Ru).

Як видно з наведених прикладів, існує чітка тенденція зростання числа комп'ютерних правопорушень разом із ростом кількості користувачів глобальної інформаційної мережі. Якщо ж враховувати ту обставину, що темпи зростання кількості користувачів Інтернету в Україні, на відміну від насиченого ринку заходу, продовжують зростати високими темпами, то постає закономірне питання щодо неадекватної оцінки загрози комп'ютерної злочинності в нашій державі. Адже масштаби такої злочинності зростають разом з ростом числа потенційних правопорушників і жертв, що використовують комп'ютерні системи.

Чому ж існує невідповідність між офіційною статистикою та реальною загрозою інформаційній безпеці суспільства?

II Протидія комп'ютерній злочинності

У **Міжвідомчому науково-дослідному центрі** при Координаційному комітеті по боротьбі з корупцією і організованою злочинністю при Президентові України проблеми комп'ютерної злочинності досліджуються більше 5 років.

Результати роботи дозволяють зробити наступні висновки.

Правопорушення, пов'язані з комп'ютерами, слід розглядати за трьома основним групами.

До першої групи належать правопорушення, де сам комп'ютер чи інформація у ньому є предметом вчинення протиправних дій (сьогодні оперативне отримання інформації навіть без порушення роботи інформаційної системи може завдати мільйонних збитків).

До другої групи слід віднести правопорушення, де комп'ютер виступає як знаряддя вчинення злочину. Особливо широко такі правопорушення виникають у фінансово-банківській сфері. Серед резонансних слід відзначити так звану Вінницьку справу, де зловмисник, використовуючи систему електронних платежів незаконно перевів більше 80 млн. грн. на кореспондентський рахунок одного з латвійських банків.

До третьої групи належать правопорушення, доказом про які є інформація, що міститься в комп'ютерних системах. Так організована злочинна група кілерів з Дніпропетровська отримувала "замовлення" на свої жертви через Інтернет. Комп'ютерна інформація може також свідчити про торгівлю наркотиками або, наприклад, відмивання коштів.

Потрібно відмітити, що злочини, пов'язані з використанням інформаційних технологій, як ніякі інші характеризуються високою латентністю (до 90 %). Це в першу чергу пояснюється небажанням фінансово-кредитних установ, де широко використовуються новітні технології, надавати інформацію про факти "злому" автоматизованих систем через побоювання втрати потенційних клієнтів. Це саме стосується адміністраторів систем захисту інформацій, які не інформують своє керівництво через можливість втрати роботи внаслідок визнання своєї професійної некомпетентності. Водночас, користувачі інформаційних систем можуть навіть і не підозрювати, що вони стали жертвами комп'ютерних злочинів. Не останню роль відіграють також недовіра до правоохоронних органів в можливості розкриття таких злочинів, або побоювання, що під час слідчих дій виявляться інші фінансові правопорушення.

На нашу думку, для комплексного вивчення комп'ютерної злочинності передовсім необхідно організувати оперативну систему збору інформації про їх вчинення.

Аналіз кримінальних справ, проведений науковцями Міжвідомчого НДЦ, свідчить про те, що мільйонних збитків завдає сьогодні внесення завідомо неправдивих даних у корпоративні інформаційні системи з метою розкрадань коштів. В особливо великих розмірах проводяться операції в так званих конвертаційних центрах. Комп'ютери використовуються для виготовлення фальшивих документів та валюти. Досить важко отримати інформацію щодо шкоди, яку завдають комп'ютерні віруси в Україні. Ось тільки деякі з вершин айсберга комп'ютерної злочинності сьогодення.

Відсутність міждержавних кордонів у глобальних інформаційних мережах є однією з основних особливостей, які потрібно враховувати при протидії та профілактиці комп'ютерних правопорушень. Це вимагає координації національних і міжнародних заходів, а саме:

- уніфікації кримінального законодавства щодо комп'ютерних злочинів;
- налагодження ефективної оперативної взаємодії між спеціальними правоохоронними підрозділами;
- співробітництва між державним та комерційним сектором;
- широкого залучення спеціальних освітніх програм як для вищої, так і загальної освіти.

Восьмий Конгрес Організації Об'єднаних Націй, що проходив у Гавані 27 серпня – 7 вересня 1990 року, розглянув проблему злочинів, вчинених із застосуванням комп'ютерів. Він рекомендував уніфікувати внутрішні законодавства про склади злочинів і поширити їх дію на злочини, вчинені з використанням комп'ютерів, а також узгодити процедури розслідування, правила доведення, умови видачі правопорушників, взаємної правової допомоги. Без такого узгодження відповідні міри можуть виявитися неефективними в боротьбі зі злочинністю і навіть мати негативні наслідки [2].

Наприклад, через побоювання комп'ютерних злочинів в Україні не розвивається система Інтернет-банків, яка набула значного поширення у світі. Це, в свою чергу, створює розрив у конкурентоспроможності з іноземними фінансовими установами.

Стосовно найбільш серйозних видів правопорушень в інформаційній сфері в даний час формується міжнародний консенсус. Однак деякі з них, в основному пов'язані з правами інтелектуальної власності, несанкціонованим копіюванням програмного забезпечення, а також інформації непристойного змісту – розглядаються як злочини не всіма країнами.

Комітет експертів з кіберзлочинів (Committee of Experts on Crime in Cyber-Space), який був організований за рішенням Ради Європи у 1996 році, у вересні 2001 року надав для затвердження Комітету Міністрів остаточну – двадцять сьому версію Конвенції щодо комп'ютерних правопорушень, в якій досить чітко визначені види комп'ютерної злочинності та шляхи взаємодії урядів щодо боротьби з комп'ютерними правопорушеннями.

Нажаль, у новому Кримінальному кодексі, який має значні новації щодо кваліфікації традиційної злочинності, існує певна невідповідність рекомендаціям європейських експертів [3].

Підгрупа експертів із комп'ютерних злочинів Ліонської групи старших експертів з транснаціональної організованої злочинності країн великої вісімки підготувала ряд ініціатив. Зокрема, були узгоджені принципи отримання правоохоронними органами електронних даних, що знаходяться в іноземних державах [4]. Це пов'язано з тим, що в більшості країн операції щодо пошуку та виїмки електронних даних проводяться під судовим наглядом. У свою чергу, при вчиненні транснаціональних злочинів унаслідок необхідності направляти запити, наприклад, каналами Інтерполу, ця процедура займає певний термін. Цією обставиною і користуються злочинці, які встигають знищити усі докази. Тому слід налагоджувати спрощену систему оперативного сповіщення для миттєвого збереження інформації.

Для сприяння оперативному співробітництву між правоохоронними органами в транснаціональному контексті Ліонська група рекомендувала створити в кожній державі мережу органів з контактів, до яких можна звертатися в будь-який час доби протягом семи днів у тиждень із проханням про надання допомоги в проведенні компетентного розслідування. Спочатку в цю мережу входили держави – члени Групи восьми, однак у даний час вона охоплює 19 країн. Одночасно змінюються правила з захисту інформації, щоб забезпечити правоохоронним органам доступ до електронної кореспонденції. Передбачається зберігати архівні записи Інтернет-трафіку терміном до семи років, що збільшить можливості з відстеження телекомунікацій.

Генеральна Асамблея ООН у своїй резолюції № 55/63 від 4 грудня 2000 року відзначила важливість зусиль по боротьбі зі злочинами у сфері використання інформаційних технологій та визначила наступні необхідні заходи: ліквідація притулків для правопорушників; співробітництво правоохоронних органів у розслідуванні трансграничних злочинів; обмін інформацією; навчання та оснащення персоналу; захист конфіденційності; забезпечення охорони даних, що мають відношення до розслідування злочинів і швидкого доступу до них; забезпечення належних режимів взаємної правової допомоги; підвищення поінформованості громадськості; розробка інформаційних систем для попередження злочинів і сприяння їхньому розслідуванню; необхідність захисту приватного життя при збереженні в урядів можливості боротися зі злочинним використанням інформаційних технологій.

Була висловлена думка про те, що важливими елементами рішення даної проблеми є прийняття законодавства на національному рівні, а також міжнародного договору. Однак у той же час було висловлено занепокоєння відносно небезпеки передчасної розробки відповідних нормативних документів. Ця проблема може бути також частково вирішена шляхом вживання профілактичних заходів, наприклад, на основі

забезпечення технічної безпеки, просвітницької діяльності і розробки етичних норм стосовно використання нових технологій.

У своїй резолюції 55/25 від 15 листопада 2000 року Генеральна Асамблея прийняла Конвенцію Організації Об'єднаних Націй проти транснаціональної організованої злочинності і два Протоколи до неї (резолюція 55/25, додатки I – III). Конвенція застосовується в тих випадках, коли комп'ютер чи телекомунікаційні мережі використовуються злочинцями в рамках більш традиційних форм транснаціональної організованої злочинності.

Зокрема в ст. 29 Конвенції говориться, що кожна держава-учасник у необхідних рамках розробляє або вдосконалює програми підготовки правоохоронних органів. Такі програми можуть включати відрядження співробітників та обмін ними. Зазначені програми стосуються методів, що використовуються у боротьбі з транснаціональними організованими злочинами, які вчиняються з використанням комп'ютерів, телекомунікаційних мереж та інших видів сучасної технології [5].

Координації зусиль з протидії комп'ютерній злочинності потребують не тільки правоохоронні органи, але й потенціальні жертви комп'ютерних атак, а також виробники апаратного та програмного забезпечення.

Проте їхні мотиви, як правило, носять комерційний, а не політичний характер і методи їхньої діяльності мають скоріше технічний, а не правовий характер, а тому мають бути враховані і по можливості погоджені з зусиллями урядів на внутрішньо державному і міжнародному рівнях, а також сприяти мобілізації грошових ресурсів і технічної допомоги з боку компаній у рамках глобальної стратегії проти комп'ютерної злочинності.

Для протидії загрозам інформаційній безпеці нашої держави необхідно провести комплексне вивчення такого соціально-небезпечного явища, як комп'ютерна злочинність. Це передбачає, перш за все, налагодження централізованої звітності щодо зазначених груп правопорушень. При аналізі такої інформації відразу визначаться масштаби комп'ютерної злочинності в Україні, яка сьогодні непомітна внаслідок змішування з традиційною.

Боротьба з комп'ютерною злочинністю вимагає високої кваліфікації кадрів, відповідного спеціального технічного забезпечення, наявності дієвої законодавчої бази.

Формування відповідних підрозділів в Міністерстві внутрішніх справ, Службі безпеки, Державній податковій адміністрації координує Координаційний комітет по боротьбі з корупцією і організованою злочинністю при Президентові України. Проте специфіка комп'ютерних злочинів потребує створення спеціального підрозділу, який би здійснював аналітично-інформаційну діяльність щодо боротьби та попередження правопорушень в інформаційній сфері. На базі такого підрозділу можливою була б організація інформаційних систем, до яких можна звертатися в будь-який час доби із проханням про надання допомоги в проведенні компетентного розслідування.

Але, як показують наші дослідження, тільки правозастосовчими заходами неможливо реально вирішити зазначену проблему. Тут необхідний комплекс заходів, який передбачає широке залучення громадськості, міністерств та відомств, навчальних закладів, засобів масової інформації по формуванню у населення відповідного правового менталітету.

Вирішенню цього питання могла б сприяти громадська організація – Асоціація захисників інформації, яка проводила б координацію роботи з забезпечення інформаційної безпеки згідно зі ст. 17 Конституції України.

Для вирішення цього завдання в рамках Асоціації пропонується приймати участь у виробленні державної політики щодо інформаційної безпеки шляхом:

- обговорення законопроектів з питань інформаційної безпеки з подальшим внесенням пропозицій до органів влади та управління;
- координації і методичного забезпечення освіти населення щодо інформаційної безпеки;
- організації презентацій розробок програмно-технічних систем захисту інформації;
- популяризації літератури у сфері інформаційної безпеки;
- координації зусиль фахівців з технічного захисту інформації у розробці та впровадженні технічних засобів захисту інформації;
- міжнародного співробітництва з організаціями, науковими установами з питань інформаційної безпеки.

III Висновок

Як уже зазначалося, сьогодні розпочалось активне формування спеціальних підрозділів по боротьбі з комп'ютерними злочинами. Їхня робота знаходить підтримку як в урядових, так і приватних структурах. Налагоджується співробітництво з організаціями, які здійснюють захист інформації на комерційній основі.

Висловлюю надію, що становлення асоціації захисників інформації сприятиме подальшій координації зусиль організацій та відомств незалежно від форм власності, міжнародному співробітництву у сфері надійного забезпечення інформаційної безпеки України.

Література: 1. Аналітичний огляд стану комп'ютерної злочинності та інформаційної безпеки в Україні у 2000 році. // Національне Центральне бюро Інтерполу в Україні. – К. – 2001. – С. 6. 2. Международное сотрудничество в борьбе с транснациональной преступностью // Организация Объединенных наций. Экономический и социальный Совет. Комиссия по предупреждению преступности и уголовному правосудию. – Вена. – 2001. – 17 мая. 3. М. Гуцалюк Інформаційна безпека в Інтернет: кримінологічний аспект // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. – К. – 2001. № 2. – С. 230–234. 4. Коммюнике Конференции министров стран Группы восьми по проблемам борьбы с транснациональной организованной преступностью. – М. 1999. – 20 октября. 5. Ст. 29 (h) Конвенции ООН против транснациональной организованной преступности. – 2000. 18 ноября. 6. В. Д. Гавловський, М. В. Гуцалюк, В. С. Цимбалюк Удосконалення інформаційного законодавства як засіб оптимізації протидії комп'ютерній злочинності // Науковий вісник Національної академії внутрішніх справ України. – 2001. № 3. – С. 20–24. 7. М. Гуцалюк Інтернет: протидія кримінальним проявам та боротьба зі злочинністю // Боротьба з організованою злочинністю і корупцією (теорія і практика). – 2001.– № 3. – С. 183–191.

УДК 002.6 + 347,777 + 343.50/53 + 35.078 + 342.7

ПИТАННЯ КОДИФІКАЦІЇ ЗАКОНОДАВСТВА УКРАЇНИ ПРО ІНФОРМАЦІЮ З ОБМЕЖЕНИМ ДОСТУПОМ

Ростислав Калюжний, Владислав Гавловський, Віталій Цимбалюк
Міжвідомчий науково-дослідний центр з проблем боротьби з організованою злочинністю

Анотація: **Розглядаються питання теорії інформаційного права, правової інформатики щодо інформаційної безпеки. Подаються зауваження до проекту Закону України "Про інформацію з обмеженим доступом, що не становить державної таємниці".**
Summary: **In the article the questions of the theory of the information right concerning information safety are considered. The remarks to the project of the law " About the information with the limited access are shined{*covered*} which does not constitute the state secret ".**
Ключові слова: **Інформаційна безпека, інформація з обмеженим доступом, конфіденційна інформація, таємниця.**

Поступ України до інформаційного суспільства та інтеграція її до глобальної інформаційної мережі викликали необхідність формування адекватного публічного права у сфері суспільних інформаційних відносин. Чільне місце в інформаційному законодавстві займає регулювання суспільних відносини щодо інформаційної безпеки людини, суспільства, держави. Одним із важливих чинників підтримки інформаційної безпеки є кодифікація суспільних відносин щодо інформації з обмеженим доступом. У зазначеному контексті заслуговує на увагу наукової громадськості винесений на обговорення проект Закону України "Про інформацію з обмеженим доступом, що не становить державної таємниці" (далі – законопроект).

Критичний, системно-комплексний правовий аналіз зазначеного законопроекту свідчить, що його розробники глибоко дослідили проблеми суспільних відносин щодо інформації з обмеженим доступом. Законопроект має чітко визначену структуру, логічне викладення формулювань науковою літературною мовою. В той же час окремі положення законопроекту є дискусійними і потребують з'ясування.

Щодо назви законопроекту. Пропонується для обговорення наступна: Закон України "Про інформацію з обмеженим доступом". Розширення її словами "що не становить державної таємниці" є дискусійним. Логічно, що у законопроекті йде мова і про державну таємницю і про відмежування законопроекту від Закону України "Про державну таємницю". У зв'язку з цим виникає питання: навіщо давати розширення у назві?

Розглянемо основні засади Розділу І. (ЗАГАЛЬНІ ПОЛОЖЕННЯ) законопроекту. Логічно для нормативно-правового акту на рівні законодавства законопроект починається з визначення у статті 1 мети та завдання Закону.

На наш погляд конструкція статті надто складна. З часів стародавнього римського права латинами була відпрацьована (і запозичена багатьма правовими доктринами) універсальна техніка правотворення, що знайшла відображення у народній мудрості – словам тісно – думкам просторо. Складні конструкції сьогодні