Кіберзлочинність як чинник державної інформаційної політики України

У Міжвідомчому науково-дослідному центрі з проблем боротьби з організованою злочинністю (далі – МНДЦ) протягом семи років здійснюється вивчення протидії комп’ютерній злочинності (кіберзлочинності) в Україні. У 2002 році дослідження проводилися з урахуванням положень Указу Президента України № 1193/2001 “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.

У ряді міждержавних нормативно-правових актів визнано, що кіберзлочинність сьогодні становить загрозу не тільки національній безпеці окремих держав, а загрожує людству та міжнародному порядку.

За оцінками Інтерполу, оголошеними на шостому засіданні Робочої групи по співробітництву правоохоронних органів країн Центральної та Східної Європи (м. Мюнстер, 28–30 серпня 2000 р.) з питань боротьби з комп’ютерною злочинністю, прибутки комп’ютерних злочинців у світі посідають третє місце після доходів наркоділків та нелегальних постачальників зброї.

З початку 90-х років ХХ століття зазначеній проблематиці приділяється значна увага в багатьох державах. Окреслені проблеми перебувають і у полі зору Президента України, Верховної Ради та Уряду України. Стимулом цього виступають також взяті Україною зобов’язання щодо інтеграції у світове співтовариство, у тому числі згідно з Програмою інтеграції України до Європейського Союзу (розділ 13 – “Інформаційне суспільство”).

У той самий час в Україні відсутня концепція стратегії реалізації державної політики щодо боротьби з кіберзлочинністю. Стурбованість щодо зазначеної проблематики і розуміння її в контексті державної та міжнародної безпеки на загальнодержавному рівні висловив Президент України у своєму виступі на пленарному засіданні Самміту та Асамблеї тисячоліття, а також Ради безпеки ООН (м. Нью–Йорк, вересень 2000р.).

Проблеми кіберзлочинності у контексті інформаційної безпеки як складової національної безпеки розглядалися неодноразово Радою національної безпеки і оборони України. Про це, зокрема, свідчать укази Президента України: «Про рішення Ради національної безпеки і оборони України від 17 червня 1997 р. “Про невідкладні заходи щодо впорядкування системи здійснення державної інформаційної політики та удосконалення державного регулювання інформаційних відносин”» від 21 липня 1997 р. № 663; «“Про рішення Ради національної безпеки і оборони від 31 жовтня 2001 р. “Про заходи щодо вдосконалення державної політики та забезпечення інформаційної безпеки України”» від 6 грудня 2001 р. № 1193/2001. Окремі заходи визначені Президентом України в указах: “Про заходи щодо зміцнення банківської системи України та підвищення її ролі у процесах економічних перетворень” від 14 липня 2000 р. № 891; “Про заходи щодо розвитку національної складової глобальної інформаційної мережі Інтернет та забезпечення широкого доступу до цієї мережі в Україні” від 31 липня 2000 р. № 928/2000; “Про деякі заходи щодо захисту державних інформаційних ресурсів у мережі передачі даних” від 24 вересня 2001 р. № 891/2001 та ін.

Дослідженням встановлено, що правоохоронними органами з 1994 р. щорічно в Україні офіційно реєструється до десяти злочинів, що вчиняються з використанням комп’ютерних технологій. Однак, статистичні показники не відповідають реальному становищу. З’ясовано, що цей вид злочинів у нашій країні має дуже високий рівень латентності: вони приховані від офіційної статистики. Показники стосовно злочинів, які вчиняються з використанням комп’ютерних технологій, розпорошені у відомчих обліках. За експертними оцінками, рівень латентності кіберзлочинності становить 90–95 %.

Високий рівень латентності кіберзлочинності серед інших чинників зумовлено:

низьким рівнем спеціального технічного оснащення правоохоронних органів сучасними засобами комп’ютерної техніки та комп’ютерними технологіями;

відсутністю знань та навичок виявлення, розкриття та розслідування кіберзлочинів через обмеження доступу до відповідних методик, тактики та техніки;

низьким рівнем інформаційної культури, підготовленості широкого кола кадрів правоохоронних органів та суддів щодо притягнення винних до кримінальної відповідальності

недовірою потерпілих до правоохоронних органів (пов’язане з вищезазначеними чинниками) і т. ін.

Аналіз змісту вітчизняних підручників з кримінології, криміналістики, кримінального та кримінально-процесуального права свідчить, що зазначеній проблематиці не приділялося належної уваги. Це, у свою чергу, зумовлено тим, що у навчальних закладах, що готують працівників правоохоронних органів, та інших вузах юридичного профілю в нашій країні питання боротьби з кіберзлочинністю практично не розглядалися.

Ґрунтовному дослідженню проблем боротьби з кіберзлочинністю також перешкоджала відсутність показників у державній кримінальній статистиці. Більшість виявлених злочинів, що вчиняються з використанням комп’ютерних технологій, розпорошені у звітності різних підрозділів правоохоронних органів серед показників економічної та інших видів злочинності.

Порівняльний аналіз досліджень зарубіжного досвіду боротьби з кіберзлочинністю свідчить, що вона має тенденцію до зростання. Однією з умов її зростання є ускладнення технічних систем глобального зв’язку (телефонного, радіо- та супутникового, їх взаємоінтеграція) і спрощення доступу до використання комп’ютерних технологій широкого кола користувачів через персональні комп’ютери.

У провідних, економічно розвинутих країнах (США, ФРН та ін.) рівень кіберзлочинності вимірюється кількісно тисячами, економічні збитки становлять мільярди доларів США.

Дослідження проблем боротьби з кіберзлочинністю показало, що орієнтація тільки на технічні та технологічні засоби забезпечення інформаційної безпеки (технічного захисту інформації) в умовах інформатизації, у тому числі профілактики кіберзлочинів, не має значного успіху. Особливо це відчувається з часу приєднання до міжнародних систем телекомунікації нових країн та підвищення інтелектуального рівня користувачів комп’ютерної техніки.

Парадокс полягає в тому, що чим складніше стає комп’ютерне програмно-математичне забезпечення, тим вразливішими виявляються традиційні організаційні заходи та засоби інженерно-технічного захисту інформації в автоматизованих (комп’ютерних) системах, зокрема щодо несанкціонованого доступу.

Проблемою наступного порядку також є і те, що з розвитком сучасних електронних засобів інформації розвиваються технічні засоби перехоплення та доступу до інформації, яка обробляється і передається в електронних системах телекомунікації. Доступ до цих засобів не створює проблеми для злочинних формувань.

Найбільшу небезпеку для суспільства, держави становить транскордонна організована кіберзлочинність: комп’ютерний тероризм; диверсії, інші прояви антагоністичної інформаційної боротьби кримінальних формувань з державою, правоохоронними органами; крадіжки інформації з комп’ютеризованих баз даних та порушення права інтелектуальної власності на комп’ютерні програми; шахрайства з використанням комп’ютерних технологій, особливо у сфері міжнародних економічних відносин (кредитно-фінансова, банківська) і т. ін.

Серед державних організаційно-правових заходів, спрямованих на протидію кіберзлочинності, можна визначити такі:

1. Урядом України створено спеціальні організаційні структури з питань координації напрацювання державної політики у сфері організаційно-правового забезпечення входження нашої держави у світове інформаційне суспільство.

1.1. Урядова комісія з питань інформаційно-аналітичного забезпечення органів виконавчої влади. Комісією, серед інших проектів нормативно-правових актів, розглянуто розроблений науковцями МНДЦ спільно з науковцями НАВСУ та НДЦ правової інформатики Академії правових наук України проект Концепції реформування законодавства України у сфері суспільних інформаційних відносин шляхом розробки Кодексу про інформацію. За своїм змістом зазначена Концепція спрямована на системну, комплексну організаційно-правову реалізацію на законодавчому рівні державної політики у сфері суспільних інформаційних відносин. Кодифікація інформаційного законодавства сприятиме, поряд з іншим, правовому забезпеченню боротьби з кіберзлочинністю.

Заходи стосовно розробки остаточного варіанту і реалізації зазначеної Концепції включено до завдань Національної програми інформатизації України. Проте, реалізація зазначеної Концепції не здійснюється через ряд організаційних, бюрократичних чинників.

1.2. Питаннями удосконалення правового регулювання, визначення та організації реалізації державної політики у сфері інформаційних відносин займаються також Міжвідомчий комітет з проблем захисту прав на об’єкти інтелектуальної власності, Міжвідомча робоча група з розроблення та узгодження Концепції легалізації програмних продуктів та боротьби з їх нелегальним використанням.

1.3. Згідно з Розпорядженням Уряду України від 6 травня 2001 р. № 181-р створено Міжвідомчу робочу групу щодо розробки проекту Концепції інформаційної безпеки та Програми боротьби зі злочинами у сфері інформаційних технологій. На жаль, повідомлень стосовно діяльності зазначеної групи у засобах масової інформації до сьогодні немає.

Результативність діяльності державних структур визначається введенням економічних санкцій США стосовно нашої країни за неналежну боротьбу з порушеннями права інтелектуальної власності, переважно, щодо комп’ютерних програмних продуктів та включення України Міждержавною групою розробки фінансових заходів боротьби з “відмиванням” грошей до списку країн, що не співробітничають.

Аналіз емпіричного матеріалу дозволяє зробити прогноз, що у разі невирішення проблем щодо боротьби з організованою кіберзлочинністю, особливо у сфері міжнародних економічних відносин, до України з боку міжнародного співтовариства буде посилений інформаційний, політичний та економічний тиск.

2. Відповідно до Указу Президента України від 6 грудня 2001 р. № 1193 Уряду доручено ініціювати ряд нормативно-правових актів: подати проект Концепції національної інформаційної політики та інформаційної безпеки України; а також проект Стратегії впровадження національної інформаційної політики на розгляд Верховної Ради України.

Правові засади щодо протидії комп’ютерній злочинності на національному рівні вже визначено у прийнятому новому Кримінальному кодексі України (КК). У Кримінальному кодексі окремі види комп’ютерних злочинів (кіберзлочинів) виділено в окремий розділ VI Особливої частини – Злочини у сфері використання електронно-обчислювальних машин (комп’ютерів), систем та комп’ютерних мереж (ст. 361, 361, 363). Окремі види злочинів, у яких комп’ютерні продукти визначено як засіб злочину, розміщені в інших розділах Особливої частини: Розділ V – Злочини проти виборчих, трудових та інших особистих прав і свобод людини і громадянина (ст. 163, 176, 177); Розділ VII – Злочини у сфері господарської діяльності (ст. 200). Комп’ютерні засоби можуть виступати предметом злочинного посягання і предметом вчинення злочинів і в інших окремих видах злочинів, об’єктом (предметом) суспільних відносин яких є інформація, наприклад ст. 109–111, 113–114, 120, 129, 132, 138, 142, 145, 156–162, 168, 170–172, 172, 182, 183, 185–199, 201–212, 215–236, 238, 255, 256, 258, 259, 266, 276, 277, 279–285, 290, 292–296, 300, 301, 304, 306, 312, 313, 318,319, 328–330, 338, 340, 343–347, 349–360, 364–370, 373, 374, 376–378, 380, 381, 383–387, 396–399, 401, 405, 409–413, 422–424, 426, 427, 435, 435–437, 439, 440, 445.

Підставою для такого підходу є застосування законодавцем у КК таких категорій, як “майно”, “власність”, “інформаційна безпека”, “таємниця”, “конфіденційна інформація”, “відомості”, “дані”, “знання”, “документи”, “гроші”, “приватизаційні папери”, “засоби зв’язку”, “незаконні дії”, “інші дії”, а також – положень теорії кримінального права щодо застосування бланкетності у нормах кримінального законодавства та посилань на кримінальну відповідальність в іншому галузевому законодавстві України.

В Указі 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”» № 1193/2001 від 6 грудня 2001 р. ініційоване встановлення кримінальної відповідальності за незаконне втручання до роботи телекомунікаційного обладнання, що потребує додаткового переосмислення вітчизняної практики і теорії, кримінально-правових уявлень щодо інформаційних (комп’ютерних) злочинів. У свою чергу, це стало підставою легального формування кримінально-правових, кримінологічних та криміналістичних досліджень, пов’язаних із протиправним посяганням на суспільні відносини щодо комп’ютеризованих інформаційних систем та на інформацію (комп’ютерну інформацію) як на предмети делікту (правопорушення).

Звичайно, можна збільшувати кількість статей Особливої частини КК відносно тих, що вже існують, і таким чином створити ентропію (невизначеність) у практиків, що є неминучим при великій кількості подібних за сутністю і змістом диспозицій. Але існує й альтернативний шлях, за допомогою якого можна комплексно вирішити проблему не тільки кримінально-правової кваліфікації злочинів, але й юридичної (кримінологічної) статистики. Це введення до Загальної частини КК спеціальної норми (статті):

розділ III – Злочин, його види та стаді –ї доповнити ст. 121 такого змісту:

“Злочини з використанням комп’ютерних інформаційних технологій”.

За вчинення злочинів проти основ національної безпеки (конституційного устрою України): проти життєво важливих інтересів особи, суспільства держави, громадської безпеки, чи вчинення інших злочинів, передбачених цим Кодексом, з використанням функціональних можливостей (технологій) комп’ютерних систем, комп’ютерних мереж, комп’ютерних інформаційних ресурсів та інших електронних інформаційних технологій, покарання призначається за статтями Особливої частини, в яких передбачається відповідальність за такий злочин. При цьому робиться посилання на цю статтю.

Такий правовий захід дозволить забезпечити здійснення організаційних та інших заходів, у тому числі об’єктивного моніторингу та статистику комп’ютерних злочинів і комп’ютерної злочинності в Україні.

Серед інших організаційних заходів в Україні на урядовому рівні створено багато робочих груп, що розробляють проекти законодавчих та підзаконних актів у сфері суспільних інформаційних відносин, які прямо чи опосередковано відображають питання боротьби з кіберзлочинністю та взаємодію з різними транснаціональними організаційними структурами.

Аналіз різних ініціатив щодо створення проектів нормативно-правових актів свідчить, що між зазначеними та іншими державними структурами не має взаємодії, координації діяльності. На законодавчому рівні лобіюються суперечливі антидержавні потреби та інтереси на фоні сповідування ідей правового нігілізму до чинного законодавства, що провокує масовий правовий хаос, у тому числі у правотворчій діяльності. Сьогодні у сфері інформаційного законодавства створено умови, які дозволяють злочинцям “законно” уникати відповідальності на використанні конфліктів різних юридичних норм. Зазначений чинник можна розглядати як додаткову ознаку латентності кіберзлочинності.

За результатами науково-дослідної роботи науковцями Міжвідомчого науково-дослідного центру з проблем боротьби з організованою злочинністю спільно з науковцями Національної академії внутрішніх справ та Науково-дослідного центру правової інформатики АПрН України розроблено проект Концепції стратегії реалізації державної політики щодо боротьби з кіберзлочинністю. Зазначений проект обговорено у ряді зацікавлених органів центральної виконавчої влади (у тому числі у СБУ, МВС та ін.), у наукових і вищих закладах освіти України, на науково-практичних конференціях. 25 грудня 2001 року зазначена Концепція розглянута і схвалена вченою радою Національної академії внутрішніх справ України.