УДК 002.6:342.7:347.777:343.50:35.078

ПРОБЛЕМИ ОРГАНІЗАЦІЙНО-ПРАВОВОГО ЗАБЕЗПЕЧЕННЯ ЗАХИСТУ ІНФОРМАЦІЙНИХ СИСТЕМ В INTERNET

Михайло Гуцалюк

Анотація: **В статті розглядаються напрямки боротьби з комп'ютерною злочинністю та організаційно-правові проблеми розвитку інформаційних відносин в Україні, пов'язаних з використанням глобальної комп'ютерної мережі Internet.**
Summari: **In the article are considered fields of fight against computer crime and organizationally-legal problems of development of information relations in Ukraine coupled to usage of the global computer Internet network.**
Ключові слова: **інформатизація, комп'ютерна злочинність, законодавство, Internet**.

I Україна та Internet: перспективи розвитку

Серед основних тенденцій розвитку суспільства на рубежі тисячоліть слід відзначити глобальну інформатизацію практично всіх сфер життєдіяльності людини, включаючи економіку, державне управління, науку, мистецтво.

Фактично увесь цивілізований світ переходить до технологічно нового виробництва, що побудоване на загальній інформатизації. Про реальне утворення інформаційного суспільства в розвинутих країнах або перманентний розвиток третьої технологічної революції свідчить той факт, що, наприклад, 30% населення США є власниками персональних комп'ютерів. Невпинно зростають темпи росту цифрової економіки, які в декілька разів перевищують показники всіх інших галузей виробництва.[1] Та найбільш вражаючими темпами зростає мережа Internet, що пов'язано з можливістю оперативно отримувати інформацію з терабайтного простору, кількість користувачів якого подвоюється кожні сто днів.

Згідно з статистичним звітом Computer Industry Almanac на кінець 1999 року в Internet було 259 млн. користувачів, до 2002 року доступ в Internet будуть мати 490 млн. чоловік, або 794 чоловіка на 10 тис. населення. До кінця 2005 року кількість користувачів становитиме 118 чоловік на 10 тис. Ресурси мережі Internet розподілені досить нерівномірно. Так 82% користувачів Internet зосереджені в 15 країнах. Лідером тут безперечно є США - 110 млн. американців становлять 43% від загальної кількості користувачів, але до 2002 року їх число впаде до третини, а до кінця 2005 року - до 27%, що означає, звичайно ж, не відхід громадян США з Internet, а інтенсивний розвиток мережі в інших країнах. До кінця 2000 року в світі буде нараховуватися 25 країн, де доступ в Internet буде мати кожний десятий.

Не дивлячись на те, що темпи розвитку інформаційних технологій в Україні через низку соціально-економічних проблем ще відстають від потреб сьогодення, підсумки минулого року свідчать про справжній прорив нашої держави в світовий інформаційний простір. В Україні на початок 2000 року налічувалось близько 1 млн. абонентів Internet. Вже побудовані волоконно-оптичні магістралі, що забезпечують доступ в Internet зі швидкістю до 2 Мб/сек. Багато провайдерів використовують для організації швидкісних каналів доступу супутникові системи.[2]

II Протизаконні дії в Internet

Разом з позитивними тенденціями, стрімкий прорив суспільного розвитку в технологічній сфері залишив невирішеними ряд соціальних, організаційних, юридичних та інших проблем, пов'язаних з інформатизацією суспільства у цілому та з розвитком структури Internet зокрема.

Однією з найгостріших з них в умовах глобалізації застосування сучасних комп'ютерних інформаційних технологій практично в усіх сферах є проблема комп'ютерної злочинності, включаючи комп'ютерний тероризм. Адже інформаційне суспільство суттєво залежить від електронного зберігання, доступу, аналізу та передачі інформації. Військові відомства, правоохоронні органи, енергетичні об'єкти, банки, торгівля, транспорт, наука – всі ті, хто використовує світову інформаційну мережу, можуть стати жертвами інформаційного тероризму, руйнівна сила якого у багато разів перевищує силу будь-яких інших видів зброї, доступних у минулому.

---

[1] Беседин В., Сакали М. Общие тенденции развития мировой экономики // Финансовая консультация. - 1999. - № 41-44. - С. 25-32.

[2] Табаков В. Дорогой, ведущей в сеть // Chip. - 1999. - № 11. - С. 28.

Однак уразливістю держави і суспільства, перш за все, скористаються навіть не терористи, а звичайні злочинці та організовані злочинні групи. Згідно з недавно опублікованим п'ятим щорічним звітом "Дослідження комп'ютерних злочинів і безпеки" ("Computer Crime and Security Survey") в 1999 році втрати приватних і державних структур США від проникнення в їх інформаційні мережі становили $265 млн. (при середньому показнику в $120 млн. протягом трьох попередніх років). Причому різного роду напади були відмічені в 90% (!) відгуків від 600 організацій (корпорацій, банків, урядових агентств) і фахівців з комп'ютерної безпеки, які взяли участь в опитуванні.

Зі звіту також видно, що найбільш поширеною проблемою все ще залишаються комп'ютерні віруси (їх дія була зафіксована 85%-ми респондентів). Далі в "списку популярності" йдуть DoS-атаки (27%) і пошкодження системи захисту (25%). Крім того, 8% учасників визнали випадки крадіжки конфіденційної інформації, а 3% - випадки фінансового шахрайства з використанням Internet.

Одним з найпоширеніших видів незаконного використання глобальної комп'ютерної мережі є несанкціоноване втручання в роботу автоматизованих систем телефонного зв'язку, що дозволяє безкоштовно користуватись послугами міжнародних телефонних переговорів. У Чернігові в січні 2000 року вперше на Україні розпочався судовий процес над групою осіб, які використовували для цього Internet. Управлінням СБУ у Донецькій області цього ж місяця було припинено протиправну діяльність аналогічної групи до якої входили як громадяни України, так і іноземці.[3]

Останнім часом з'явився і такий витончений вид комп'ютерної агресії як бомбардування величезною кількістю запитів інформаційних та комерційних сайтів з метою добитися блокування їх роботи через перевантаження. Масовані атаки небезпечні тим, що в них не використовуються віруси чи інші заборонені програмні продукти. Такої агресії зазнали вже Yahoo, eBay, Amazon.com, Buy.com і CNN.com За оцінками дослідницької компанії Yankee Group, збиток від трьох днів атак на найбільші комерційні Web-сайти, склав як мінімум $1,2 млрд.[4]

Перелік комп'ютерних злочинів можна продовжити згадавши й атаки на військові, космічні комп'ютерні системи, промислове шпигунство, використання компромату в політичних цілях і т.д. Перебігу інформаційних війн засоби масової інформації особливу увагу приділяли під час подій у Косово та Чечні (славнозвісний сайт Kavkaz).

Неухильний розвиток інформаційних технологій та його тісний зв'язок з економічним розвитком, вимагає пошуку нової стратегії та тактики щодо забезпечення інформаційної безпеки суспільства та реалізації Конституційного права на інформацію громадян, юридичних осіб і держави таким чином, щоб вони не порушували громадянські, політичні, економічні, соціальні, духовні, екологічні та інші права, свободи і законні інтереси інших громадян, права та інтереси юридичних осіб.

Інформаційна безпека, захист якої згідно статті 17 Конституції України, поряд з суверенітетом, територіальною цілісністю та економічною безпекою, є найважливішою функцією держави[5], досягається шляхом розробки та впровадження сучасних безпечних інформаційних технологій, побудовою функціонально повної національної інформаційної інфраструктури, формуванням і розвитком інформаційних відносин тощо.

Необхідною умовою цієї роботи повинна стати реальна кількісна оцінка стану комп'ютерної злочинності в Україні. Адже відомо, що більшість жертв комп'ютерних злочинів (комерційні банки, провайдери Internet послуг та ін.) не зацікавлені в їх афішуванні через можливий підрив іміджу та недовіру майбутніх партнерів і користувачів.

Створення статистичного банку даних можна здійснити, використовуючи офіційні та анонімні повідомлення до сайту Міжвідомчого науково-дослідного центру з проблем боротьби з організованою злочинністю, що створюється за сприянням Фонду "Верховенство права". На сайті будуть розміщені прес-релізи, наукові статті, нормативні акти, що регулюють інформаційні відносини в Україні. Важливим фактором підвищення інформаційної безпеки України є формування національного ринку програмних і технічних засобів обробки інформації, впровадження сучасних вітчизняних безпечних інформаційних технологій. На банерах сайту Міжвідомчого центру буде надана можливість прорекламувати подібні продукти.

Планується також і організація проведення електронних наукових конференцій. Комп'ютерні конференції повинні активізувати й формування нормативних актів з питань інформаційної безпеки (у тому числі Кримінального кодексу), які б відповідали сучасним реаліям світового інформаційного простору, сприяли б розробці необхідного, на нашу думку, Інформаційного кодексу.

Усвідомлюючи, що без створення відповідної правової основи ефективна протидія комп'ютерній злочинності неможлива, економічно розвинуті країни прийняли спеціальні законодавчі акти.

---

[3] Фемида против хакеров // Сегодня. 2000. - 13 января. - С. 6.

[4] Computerword Киев. 2000, - 16 февраля. - С. 29.

[5] Конституція України. - К. 1996.

Перші закони стосовно цієї категорії злочинів прийняті Швецією (1973 р.). Пізніше вони з'явилися у Німеччині, Австралії, Італії, Франції, Іспанії, Канаді та інших країнах світу. Мабуть все ж таки найрозвинутішою є система нормативних актів (в тому числі й відомий Computer Fraud and Abuse Act 1984) Сполучених Штатів Америки, які найбільше страждають через комп'ютерні злочини. Але процес вдосконалення чинного законодавства не припиняється і сьогодні, що пояснюється стрімким розвитком інформаційних технологій.

В Китаї, побоювання впливу, який Internet може надати на китайське суспільство, політику і комерцію призвів до появи цілого потоку регулюючих актів уряду країни, які охоплюють широке коло питань, включаючи передачу через мережу не схваленої урядом інформації, використання технології шифрування даних і випуск акцій Internet-фірмами в Китаї. До 31 січня 2000 р. компанії повинні були повідомити урядовим органам імена, домашні адреси, e-mail та іншу інформацію про всіх нових користувачів ПО, які використовують можливості шифрування. [6]

У Кримінальному кодексі Російської федерації, який був прийнятий у травні 1996 року введено главу 28, яка містить три статті: неправомірний доступ до комп'ютерної інформації; створення, використання та розповсюдження шкідливих програм для ЕОМ і порушення правил експлуатації ЕОМ, системи ЕОМ або їх мережі.

Європейський комітет з проблем злочинності Ради Європи підготував рекомендації з метою визначення правопорушень, пов'язаних з комп'ютерами для включення їх у законодавство європейських країн. Тому, прийняту у 1994 році "комп'ютерну" статтю 198[1] Кримінального кодексу України, що передбачає відповідальність за дії, які призводять до перекручення чи знищення інформації в автоматизованих системах або за розповсюдження таких програмних чи технічних засобів слід доповнити й іншими, які б розширили дію кримінальної відповідальності за протиправне використання можливостей Internet (розповсюдження нелегального матеріалу, несанкціоноване перехоплення інформації, комп'ютерний саботаж та ін.). Крім того, на наш погляд, необхідні доповнення і до Адміністративного та Цивільного кодексів з метою регулювання в них сучасних інформаційних відносин. Це повинно посилити правове забезпечення безпеки інформаційних систем, а також відповідальність адміністраторів баз даних та інших посадових осіб, що забезпечують експлуатацію комп'ютерних інформаційних систем.

Специфіка виявлення та проведення слідчо-криміналістичних дій в Internet просторі вимагає розробки спеціальних методик, глибоких знань сучасних інформаційних технологій, наявності відповідного апаратного та програмного забезпечення.

В МВС Російської Федерації для боротьби з комп'ютерними злочинами (мережевий злом, поширення комп'ютерних вірусів), з незаконним оборотом заборонених радіоелектронних і спеціальних технічних засобів та із загрозою проникнення в міжміські та міжнародні канали зв'язку створено спеціальний підрозділ - Управління по боротьбі зі злочинами в сфері високих технологій.

Для дослідження проблеми незаконного використання Internet, у серпні 1999 року Президентом США Біллом Клінтоном була створена Робоча група в складі Міністра юстиції, директора ФБР, керівника офісу управління та бюджету, секретаря освіти та інших зацікавлених осіб. А на нараді, присвяченій безпеці в Internet, що проходила 15 лютого 2000 р. він запропонував створити національний центр безпеки та звернувся до Конгресу з проханням виділити на його утворення 9 млн. доларів.[7] В ФБР Сполучених Штатів створено National Computer Crime Squard, San Jose Resident Agency, San Francisco Division. Відповідні підрозділи створені і в міністерстві юстиції США.

На нашу думку своєчасним є рішення про створення в системі МВС спеціальних підрозділів "Інформаційної електронної розвідки та протидії комп'ютерним злочинам". Відповідних фахівців до них можна підготувати з числа осіб з вищою освітою суміжних спеціальностей. Це може бути друга освіта або перепідготовка кадрів. Для забезпечення навчального процесу у добрій нагоді став би посібник Б.В.Романюка, М.І.Камлика та ін. "Виявлення та розслідування злочинів, що вчиняються за допомогою комп'ютерних технологій"[8]. Вразливим місцем вітчизняних інформаційних систем є використання неліцензійного програмного забезпечення, в тому числі і державними органами (за оцінками Business Software Alliance рівень піратства перевищує 90%.). Серед комплексу заходів, що проводить держава для виправлення такої ситуації, знешкодження "тіньових" виробників програмного забезпечення є створення "групи по боротьбі з посяганням на інтелектуальну власність" в МВС України. Постійно вдосконалюється і інформаційне забезпечення самих правоохоронних органів, адже це важливий фактор забезпечення ефективної протидії злочинному світу. Значна увага при цьому приділяється кваліфікованому кадровому забезпеченню, адже за сучасних умов для правоохоронних органів несприйнятна

[6] Пекин ужесточает правила работы в Internet // Computerword Киев. 2000. - 16 февраля. - С. 28.

[7] Не допустим Перл-Харбора в Internet // Computerworld Киев. 2000. - 23 февраля .

[8] Б.В.Романюк, М.І.Камлик, В.Д.Гавловський В.С.Цимбалюк, В.Г.Хахановський Виявлення та розслідування злочинів, що вчиняються за допомогою комп'ютерних технологій: Посібник / За заг. ред. проф. Я.Ю.Кондратьєва. -К.: Національна академія внутрішніх справ України, 2000.

практика, яку використовували деякі західні фірми - вони призначали на посади консультантів з інформаційної безпеки "хакерів", які проникли через систему захисту.

III Висновок

Звичайно, зазначені вище напрямки організації захисту інформаційних систем в Internet не в змозі в повному обсязі вирішити проблему. Це складне завдання вимагає не тільки системного підходу та координації діяльності державних структур та правоохоронних органів, а й усіх, хто зацікавлений в подальшому розвитку як Internet-культури взагалі, так і Internet-комерції зокрема.

Тому тільки скоординованими зусиллями організацій та відомств незалежно від форм власності, шляхом налагодження міжнародного співробітництва, використовуючи сучасні технології захисту інформації можна отримати переваги не тільки електронного бізнесу, а й інформаційної революції в цілому, не забуваючи при цьому про інформаційну безпеку як нашої держави, так і її окремих громадян.

УДК 681.3:34

ПРОБЛЕМИ ТА ПЕРСПЕКТИВИ ПРАВОВОГО ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ ІНФОРМАЦІЇ З ОБМЕЖЕНИМ ДОСТУПОМ, ЩО НЕ СТАНОВИТЬ ДЕРЖАВНОЇ ТАЄМНИЦІ

Ростислав Калюжний, Дарія Прокоф'єва

Національна Академія Внутрішніх справ України, Національний технічний університет України "КПІ"

Анотація: **стаття присвячена сучасним проблемам вдосконалення правового регулювання обігу конфіденційної інформації, а також таємної інформації, що не становить державної таємниці.**

Summary: **this article is about the contemporary problems of impruving law regulation of the circulation of confidential and the secret information, which is not forming the state secrets.**

Згідно із Законом України "Про інформацію" [2] інформація поділяється на відкриту та інформацію з обмеженим доступом. Остання поділяється на таємну, яка, в свою чергу, складається з державної таємниці та іншої таємної інформації, та конфіденційну інформацію [2-3]. Якщо державна таємниця на сьогоднішній день охоплена ефективним правовим захистом, то цього, на жаль, не можна констатувати щодо іншої інформації з обмеженим доступом. "Інша таємна інформація", яка становить систему видів таємної інформації, що не становить державної таємниці, не має навіть чітко закріпленої в законодавстві структури (однак потребує вичерпної визначеності, осільки її існування фактично є обмеженням права на інформацію), хоча ця структура й може бути визначена виходячи зі змісту правових норм, присвячених окремим видам такої інформації, які містяться в законах, що контекстно не належать до інформаційного законодавства. Не кращою є ситуація і з правовим регулюванням обігу конфіденційної інформації [2, 4, 5]. Наслідком такої невизначеності є відсутність у суб'єктів правотворення та правозастосування адекватного уявлення про структуру інформації з обмеженим доступом, ототожнення конфіденційної інформації та таємної інформації, що не становить державної таємниці, "аморфний стан" нових видів таємної інформації, що з'являються поза нормами інформаційного законодавства (наприклад, професійна таємниця [6] або відомості про заходи безпеки та осіб, взятих під захист [7]). Все це негативно відбивається на якості створюваних підзаконних нормативно-правових актів, зокрема з питань захисту інформації, бо інформація не може бути належним чином захищена без визначення ступеню безпеки, якого вона потребує, та його аргументації тими чи іншими властивостями інформації. Досі відсутня також єдина термінологічна база інформаційного законодавства, неврегульовані суперечності між нормами його окремих актів.

Виходом з цього *circuluc vitiosus* представляється вдосконалення правового регулювання обігу інформації з обмеженим доступом (конфіденційної та таємної), що не становить державної таємниці, та її правового захисту. Таку спробу було зроблено НДЦ «Тезіс» НТУУ "КПІ", яким на замовлення Держкомсекретів України в 1998-1999 роках був розроблений проект Закону України "Про інформацію з обмеженим доступом, що не становить державної таємниці" [8] відповідно до завдань другого етапу роботи "Щит-3". Підгрунтям його розробки стало вивчення інформаційного законодавства України та дослідження функціонування інформації з обмеженим доступом відповідно до чинного законодавства України. Проект було дороблено спільно з Управлінням експертиз, реєстрації державних секретів, нормативного забезпечення та професійної підготовки