ми, що розглянуті вище. На нашу думку, ця дисципліна повинна бути комплексною та викладатися декількома кафедрами.

Використана література

1. Закон України "Про захист інформації в автоматизованих системах" від 5.07.94, № 81/94-ВР.
2. Биленчук П.Д., Хахановский В.Г. Компьютерная безопасность // Бюл. по обм. опытом работы ОВД. – 1994. – №115. – С. 48-49.
3. Виявлення та розслідування злочинів, що вчиняються за допомогою комп'ютерних технологій: Посібник / За ред. Я.Ю. Кондратьєва. – К.: НАВСУ, МНДЦ. 2000.
4. Система інформаційного забезпечення ОВС України / Під ред. Л.В.Бородича. – К., РВВ МВС України, 2000.

М. ГУЦАЛЮК, *кандидат юридичних наук*

ЗАХИСТ ІНФОРМАЦІЙНИХ РЕСУРСІВ УКРАЇНИ

Нині всі економічно розвинені країни перейшли на широке використання нових інформаційних технологій у виробничій, комерційній, банківській сферах. Технологічний прогрес надає можливість по-новому організувати процеси обробки, зберігання, пошуку та передавання інформації в будь-якій потрібній формі: усній, письмовій або візуальній – незалежно від відстані, часу та обсягу [1].

Найбільш активно розвиваються технології, пов'язані з глобальною комп'ютерною мережею Інтернет, що призвело до появи таких нових категорій, як е-торгівля, е-бізнес, е-уряд тощо. Це яскраво демонструє графік зростання кількості користувачів Мережі (табл. 1).

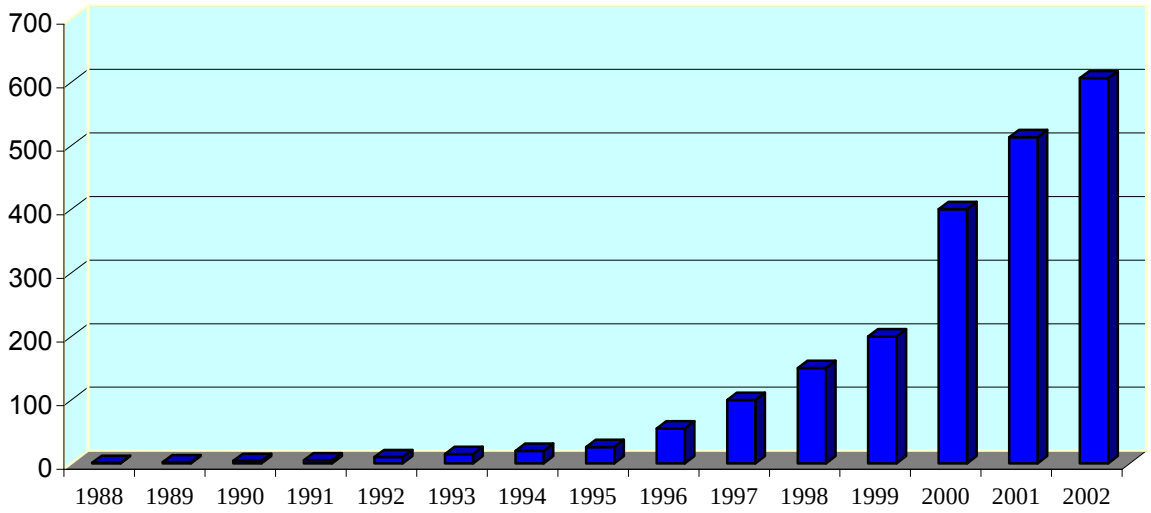
Електронна комерція охопила увесь світ, хоча насиченість електронних засобів у різних країнах є вкрай нерівномірною. Так, за даними Nua Ltd., у США та Європі – по 200 млн користувачів Інтернет, у Латинській Америці – 30 млн, Африці – 6 млн. Цей процес не минув і Україну, фінансові установи якої отримали доступ до міжнародних платіжних систем. Темпи зростання кількості користувачів Інтернет у нашій державі продовжують залишатися високими, на відміну від західних країн. Сьогодні їх приблизно 2 млн. Проте, це тільки 4 зі 100 громадян.

Разом з тим, в інформаційному суспільстві, виникли нові загрози, що стали серйозною перешкодою для інформаційного суспільства. Нові інформаційні технології почали активно використовуватися злочинним світом.

Наприклад, за даними Computer Emergency Response Team (CERT) – міжнародного авторитета в галузі безпеки Internet, заснованого Інститутом розробки програмного забезпечення Пітсбургського університету Карнегі-Мелона (Carnegie Mellon University Pittsburgh), останнім часом стрімко зросла кількість несанкціонованих проникнень до інформаційних систем (див. табл. 2).

Таблиця 1

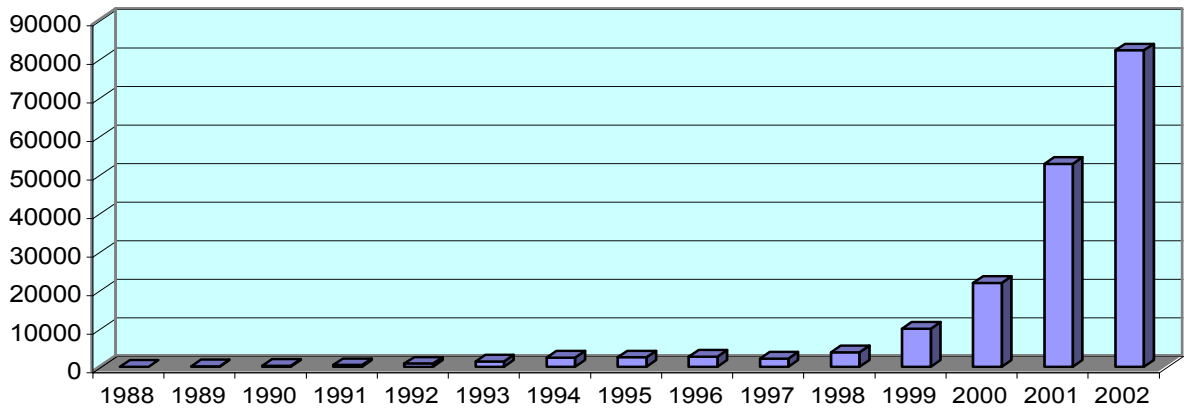
Кількість користувачів у глобальній мережі Internet, млн



У складі комп'ютерної злочинності найбільшу небезпеку для особи, держави, суспільства в цілому становлять такі злочини, що мають ознаки організованої злочинності: комп'ютерний тероризм; диверсії, інші прояви антагоністичної інформаційної боротьби кримінальних формувань з державою, правоохоронними органами; крадіжки інформації з баз даних та комп'ютерних програм; шахрайства з використанням комп'ютерних технологій, особливо у сфері міжнародних економічних відносин (кредитно-фінансова, банківська) і т. ін. Це одна з найбільш серйозних проблем багатьох держав, щорічні збитки від якої становлять понад 100 млрд дол. США. Кількість правопорушень вказаного виду має тенденцію до зростання.

Таблиця 2

Несанкціонований доступ до інформаційних систем



У грудні 2002 року в Лондоні проходив Перший міжнародний стратегічний конгрес „E-CRIME CONGRESS 2002", присвячений проблемі електронної злочинності. Серед інших доповідачів віце-президент групи страхових компаній Вільям Барр виклав такі факти:

- 90 % організацій виявляють порушення інформаційних систем щороку;
- 80 % з них підтверджують фінансові збитки;
- тільки один вірус NIMDA призвів до збитків понад 1,8 млрд фунтів;

- у жовтні 2002 року кібератака протязом 1 години вивела з ладу 9 з 13 головних комп'ютерів, які керують глобальним рухом у мережі Інтернет;
- щороку викрадається приватної інформації на суму понад 38 млрд фунтів.

Підготовку та проведення Конгресу взяв на себе Національний центр по боротьбі зі злочинами у сфері високих технологій (National Hi-Tech Crime Unit – NHTCU) – перша в історії Великобританії національна правоохоронна організація, мета якої – боротьба з комп'ютерною злочинністю та співробітництво з іншими правоохоронними структурами.

NHTCU створений на виконання Національної стратегії, яка була представлена до Парламенту Великобританії у листопаді 2000 року. Стратегія „Project Trawler" була розроблена Асоціацією поліцейських офіцерів (ACPO) та Робочою групою з питань комп'ютерної злочинності й була опублікована Національним бюро кримінальних розслідувань (NCIS) у 1999 році. В стратегії йшлося про потенційні загрози комп'ютерної злочинності.

Після діяльності робочої групи, створеної у березні 2000 року, на виконання Стратегії з державного бюджету було виділено 25 млн фунтів на три роки, 10 млн з яких було виділено на розвиток відповідних відділів на місцях, та 15 млн на створення Національного центру по боротьбі зі злочинами у сфері високих технологій.

У роботі Конгресу „E-CRIME" взяли участь близько 400 делегатів з усього світу, у тому числі з Австралії, Нової Зеландії, Кореї, Гонконгу, Росії, Латвії, США та ін. Вони представляли державні, комерційні, наукові та правоохоронні органи, що займаються проблемами захисту інформації та розслідуванням комп'ютерних злочинів. Зокрема, своїх делегатів представляли Міністерство внутрішніх справ Великобританії, Інтерпол, Європол, ФБР, Управління "Р" (Росія), Microsoft, Symantec, IBM, Sun Microsystems Ltd., VISA, MasterCard, eBay, Bank of New York, Swedbank та ін.

На Конгресі відзначалося, що високотехнологічна злочинність зростає високими темпами, Інтернет дозволяє організованим злочинним групам швидко отримувати прибуток з відносно невеликим ризиком бути упійманими. Знаходячись у Мережі, можна порушувати закон на відстані, швидко і незалежно від громадянства і місця перебування. Злочинцям легко ошукувати безліч людей, приховувати докази і награбоване. Вони стали значною загрозою для критичної інфраструктури розвинених держав. Так, за повідомленням інформаційного агентства Washington ProFile, з посиланням на газету The Washington Times, терорист номер один – Усама Бен Ладен одержав у своє розпорядження комп'ютерну програму Promis (виробник – компанія Inslaw Inc.), що дозволяє йому проникати в урядові інформаційні мережі США.

Інтегруючись у світове інформаційне суспільство Україна перш за все повинна подбати про надійний захист своїх інформаційних ресурсів. Вагомим внеском у цьому напрямі було прийняття нової Конституції України ст. 17 якої визначає забезпечення інформаційної безпеки як одну з найважливіших функцій держави, справою всього Українського народу [2].

Не зупиняючись на питаннях щодо визначення самого терміну „інформаційний ресурс", дискусія відносного чого продовжується серед вітчизняних науковців [3], відзначимо, що Законом України „Про основи національної безпеки України" від 19 червня 2003 р. № 964-IV загрозами національній безпеці України в інформаційній сфері серед інших визначені комп'ютерна злочинність та комп'ютерний тероризм.

Протидія комп'ютерній злочинності передбачає перш за все створення відповідної законодавчої бази, комплексу організаційних заходів, у тому числі підготовку кадрів високої кваліфікації, а також спеціальне технічне забезпечення цієї діяльності.

Перш за все, хотілося б зупинитися на самому понятті „комп'ютерний злочин". Як відомо, ця проблема привернула до себе увагу криміналістів провідних зарубіжних країн, коли почався розквіт комп'ютерної техніки, який спричинив цілий комплекс негативних наслідків, які загострили ситуацію із захистом інформації, що міститься в базах даних комп'ютерів і комп'ютерних систем.

Статистика таких злочинів велася з 1958 року. Тоді під ними малися на увазі випадки псування і розкрадання комп'ютерного устаткування; крадіжка інформації; шахрайство або крадіжка грошей, здійснені із застосуванням комп'ютерів; несанкціоноване використання комп'ютерів або крадіжка машинного часу. Записи велися у Стенфордському дослідницькому інституті та тривалий час не представляли великого інтересу. До речі, у 1966 році комп'ютер уперше був використаний як інструмент для пограбування банку. Сталося це в Міннесоті. У 1968 році у всіх Сполучених Штатах було зафіксовано 13 злочинів; у 1978 році – 85, а в 1975 році інститут припинив ведення і публікацію статистики через складність визначення вірогідності подій, кількість яких швидко зростала [4].

У новому Кримінальному кодексі комп'ютерним злочинам присвячено Розділ XVI Злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку (Розділ із змінами, внесеними згідно із Законом України від 05.06.2003 р. № 908-IV), який складається з трьох статей:

Стаття 361. Незаконне втручання в роботу електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку

Стаття 362. Викрадення, привласнення, вимагання комп'ютерної інформації або заволодіння нею шляхом шахрайства чи зловживання службовим становищем

Стаття 363. КК Порушення правил експлуатації автоматизованих електронно-обчислювальних систем

Статтями передбачено максимальну санкцію - позбавленням волі на строк до п'яти років.

Поряд з цим існують також і інші злочини, передбачені статтями Кримінального кодексу, де в якості знаряддя вчинення злочину може використовуватися комп'ютер.

9 – 13 червня 2003 р. Міжвідомчим НДЦ з проблем боротьби з організованою злочинністю спільно зі співробітниками ФБР за сприянням посольства США на базі Національної академії внутрішніх справ України був проведений Міжнародний міжвідомчий навчальний семінар з питань розслідування злочинів, що вчиняються у сфері використання комп'ютерних технологій.

У роботі семінару приймали участь співробітники Міжвідомчого НДЦ, ДСБЕЗ МВС, ГСУ МВС, НЦБ Інтерполу, Київського науково-дослідного інституту судових експертиз, СБУ, органів прокуратури, суддів.

Під час роботи семінару були вивчені питання розслідування комп'ютерних злочинів, практично опрацьовані методи пошуку правопорушників у кіберпросторі, обговорені питання законодавства та міжнародної взаємодії у протидії кіберзлочинності.

Водночас під час проведення круглого столу, який проходив в рамках роботи семінару, було зазначено, що існує низка питань, які потребують невідкладного вирішення. Зокрема, це питання удосконалення чинного законодавства, розробки стратегії та тактики протидії кіберзлочинності, профілактики правопорушень в інформаційній сфері, подальшого посилення технічного захисту інформації тощо.

Необхідно відмітити, що, за прогнозами провідних науковців у галузі інформаційної безпеки, вже найближчими роками можливе стрімке зростання кількості кіберзлочинів. Так, за розрахунками компанії Gartner, вже у кінці 2004 року економічні збитки від них збільшаться у десятки разів. Це змушує і уряд США і європейське співтовариство терміново вжити відповідних заходів як на законодавчому так, і організаційному рівні. Зокрема, урядом США була нещодавно прийнята нова Стратегія щодо захисту інформаційних систем в Інтернет (бюджетом планується виділення близько $ 60 млрд), в Раді Європи створюється спеціальний Комітет „Агентство інформаційної безпеки", відповідні заходи вживаються на рівні ООН. Тому, обравши свій шлях розбудови інформаційного суспільства, Україна також повинна здійснювати відповідні кроки щодо своєї інформаційної безпеки.

У червні цього року народним депутатом України Кириловим В.Д. було зареєстровано законопроект „Про внесення змін до Закону України „Про організаційно-правові основи бо-

ротьби з організованою злочинністю", яким передбачається аналітичне та науково-методичного забезпечення боротьби з комп'ютерною злочинністю покласти на Міжвідомчий центр з проблем боротьби з організованою злочинністю. Відповідне рішення підтримується і Кабінетом міністрів України, якому Указом Президента України „Про рішення Ради національної безпеки і оборони України від 31 жовтня 2001 року "Про заходи щодо вдосконалення державної інформаційної політики та забезпечення інформаційної безпеки України" від 6 грудня 2001 року № 193/2001 надавалися повноваження щодо його організації. Залишилося невирішеним, нажаль, одне питання – фінансування відповідних досліджень.

У цьому зв'язку залишається лише зазначити, що сучасні технології та глобальні інформаційні системи надають небачених раніше можливостей організованим злочинним угрупованням щодо вчинення незаконних фінансових операцій. Якщо враховувати, що щоденний обсяг електронних переказів перевищує 2 трильйона доларів США [5], та подальше ускладнення методів та масштабів фінансових операцій (в Україні вже функціонують віртуальні системи WebMoney, PayCash, e-port та ін.), а тільки по одній справі громадянину України Максиму Височанському було висунуте обвинувачення в нанесенні збитків американським банкам на суму понад 100 мільйонів доларів, то на мій погляд, зволікання щодо відповідного розв'язання проблем захисту інформаційних ресурсів може призвести до не передбачуваних наслідків.

Використана література

1. Європа на шляху до інформаційного суспільства. Матеріали Європейської комісії 1994-1995 рр. – К. – 2000. – С. 11.
2. Конституція України. – К. – 1996.
3. Див. Інформатизація управління соціальними системами: організаційно-правові питання теорії і практики: Навч. посіб./ В.Д. Гавловський, Р.А. Калюжний, В.С. Цимбалюк, Ю.В. Ящуринський, М.В. Гуцалюк. За заг. ред. М.Я. Швеця, Р.А. Калюжного. – К.: МАУП, 2003. – С. 12-19.
4. Див. Компьютерные террористы: Новейшие технологии на службе преступного мира (Энциклопедия преступлений и катастроф) /Автор-составит. Т. И. Ревяко. - Мн.: Литература, 1997. – 640 с.
5. Диканова Т.А., Осипов В.Е. Борьба с таможенными преступлениями и отмыванием «грязных» денег. М., 2000. – С. 157.
6. http://www.liga.net: 29.07.2003, 16:08

ВІД НАУКОВОЇ РАДИ

ПРОБЛЕМИ РОЗБУДОВИ ІНФОРМАЦІЙНОГО СУСПІЛЬСТВА В США, ЄВРОПІ ТА УКРАЇНІ

Серед кардинальних політичних, економічних і структурних змін у світі за останні десятиріччя особливо помітним є стрімкий за темпами і глобальний за масштабом перехід від індустріального до Інформаційного суспільства. Інформаційне суспільство, як це було зазначено у Білій книзі Європейської Комісії "Розвиток. Конкуренція. Зайнятість", – це суспільство, в якому діяльність людей здійснюється на основі використання послуг, що надаються за допомогою інформаційно-комп'ютерних технологій та телекомунікаційних мереж.

Інформаційні технології, інфраструктура інформатизації відіграють сьогодні вирішальну роль у забезпеченні адміністративного і господарського управління, в розширенні інформаційної взаємодії між людьми, в більшій відкритості органів державної влади, в підготовці і розповсюдженні масової інформації, у процесі інтелектуалізації суспільства, в розвитку освіти, науки, культури, охорони здоров'я, захисту навколишнього середовища.