

4 Забезпечення захисту інформації в системах зв'язку. Технічні засоби системи захисту інформації

УДК 002.6+342.7+347.777+343.50+35.078

ІНФОРМАЦІЙНА БЕЗПЕКА В INTERNET: КРИМІНОЛОГІЧНИЙ АСПЕКТ

Михайло Гуцалюк

Міжвідомчий науково-дослідний центр з проблем боротьби з організованою злочинністю при Координаційному комітеті по боротьбі з корупцією і організованою злочинністю при Президентові України

Анотація: Розглядаються напрямки боротьби з комп'ютерною злочинністю та організаційно-правові проблеми розвитку інформаційних відносин в Україні, пов'язані з використанням глобальної комп'ютерної мережі Internet.

Summary: 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.

Вступ

В сучасних умовах розвитку незалежної держави інформатизацію суспільства слід розглядати як необхідну умову досягнення стратегічної мети – входження України до провідних технологічно розвинутих країн світу, яку визначив Л. Кучма у Посланні Президента України до Верховної Ради [1].

Серед основних тенденцій розвитку інформатизації суспільства, що стосуються практично всіх сфер життєдіяльності, включаючи економіку, державне управління, науку, мистецтво, слід відзначити стрімкий розвиток інформаційної мережі Internet.

Сьогодні Internet стає одним з основних джерел інформації для бізнесу, науки, засобом розповсюдження преси, юридичних актів, місцем проведення дозвілля та спілкування людей. Internet надає світовій спільноті можливість не тільки придбати продукти харчування чи книги, але й приймати участь в аукціонах, отримати грошову позику на основі електронного підпису, чи працювати в електронному офісі, працівники якого знаходяться за тисячі кілометрів один від одного.

Не дивлячись на те, що темпи розвитку інформаційних технологій в Україні через низку соціально-економічних проблем ще відстають від потреб сьогодення, Україна сміливо входить у світовий інформаційний простір (в нашій державі налічується близько 500 тис. абонентів Internet, або 1 користувач на 100 громадян, в США відповідно 25 користувачів, у Європі – 9).

Ефективному використанню можливостей глобальної мережі для розвитку вітчизняної науки, освіти, культури, підприємницької діяльності сприятиме підписаний 31 липня 2000 року Президентом України Указ «Про заходи щодо розвитку національної складової глобальної інформаційної мережі Інтернет та забезпечення широкого доступу до цієї мережі в Україні». Указ зокрема передбачає встановлення та наповнення інформацією до кінця 2000 року Веб-сторінок центральними органами виконавчої влади, створення належних економічних, правових, технічних умов для забезпечення широкого доступу до мережі громадян та юридичних осіб усіх форм власності.

Разом з тим, стрімкий прорив суспільного розвитку в технологічній сфері залишив невирішеними ряд соціальних, організаційних, юридичних та інших проблем, пов'язаних з інформатизацією суспільства в 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 життєдіяльності є активне використання злочинним світом досягнень науково-технічного прогресу для посилення організованості, розширення бандитських зв'язків, поява так званої “комп'ютерної” злочинності, включаючи комп'ютерний тероризм.

Комп'ютерна злочинність

Слід відзначити, що на сьогодні у вітчизняному законодавстві правового визначення “комп'ютерної злочинності” не існує. Це поняття вперше з'явилося в засобах масової інформації США і означало злочини,

що якимсь чином пов'язані з ЕОМ. Пізніше термін багато разів уточнювався і в основному зводився до протиправних чи неетичних дій, пов'язаних з автоматизованою обробкою даних в інформаційних системах. Початок використання електронних банківських розрахунків у тому числі і міжнародних, став новим етапом зростання комп'ютерної злочинності. Цьому сприяв і бурхливий розвиток локальних та глобальних мереж. Серед комп'ютерних злочинців з'явилася спеціалізація, пов'язана з проникненням у віддалені інформаційні системи.

Найяскравішою фігурою цього соціального про шарку мабуть є Кевін Митник - програміст з Лос-Анжелеса, який 17-річним хлопчиною був затриманий за крадіжку списку паролів доступу телефонної компанії Pacific Bell. Найвідомішою стала його війна з лабораторією Digital Equipment, яку він у 1995 році програв спеціалісту з безпеки комп'ютерних систем Тсутму Шимомурі [3]. Сума збитків, заподіяних хакером, становить кілька десятків мільйонів доларів. 21 січня 2000 року Кевіна випустили з в'язниці, заборонивши користуватися не тільки комп'ютерами, але й будь-якими цифровими пристроями, включаючи телефон.

Найвідоміший з пострадянських хакерів – Володимир Левін – який подолав систему безпеки Citibank та за допомогою віддаленого комп'ютерного доступу викрав 12 млн. доларів, за що з 1994 року відбуває покарання у США. За аналогічну операцію (несанкціонований доступ у комп'ютерну мережу Китайського банку промисловості) суд східної провінції Жіангсу виніс смертний вирок Гао Жінгвену. Приречено до страти і хакера Фанг Йонга, який у 1990 році, використовуючи комп'ютер, викрав у банку провінції Чжензян 200 тисяч доларів та втік до Канади.

Впровадження в Україні електронної обробки інформації у банківські системи сприяло виникненню аналогічних злочинів і в нашій державі. За інформацією ГУБОЗ МВС України організоване злочинне угруповання (ОЗУ) у жовтні 1998 р. вчинило крадіжку державних коштів з Вінницького ОУ НБУ України в сумі 80.435.006 грн. Один з членів ОЗУ, працюючи на посаді техника сектора обробки задач регіональної розрахункової палати центра інформатизації і платіжних систем обласного управління НБУ, використовуючи своє службове становище, періодично робив несанкціонований доступ у локальну мережу. Йому вдалося скопіювати цифровий підпис платіжних документів. Одночасно, використовуючи доступ зі свого робочого місця до розрахункових рахунків банку шляхом візуального перегляду через монітор комп'ютера, злочинець встановив, що на спеціальному рахунку вінницького ОУ НБУ знаходиться велика сума грошей. 23. 10. 98 р. техник сформував 9 пачок платіжних документів, підписавши їх за допомогою раніше скопійованого електронного цифрового підпису і направив у систему електронних платежів, незаконно перерахувавши суму зі спеціального рахунку. Далі гроші були переведені по 15 платіжних дорученнях на різні комерційні структури. Внаслідок проведення відповідних заходів, гроші були повернуті державі.

Досить гостро сьогодні стоїть проблема проведення безподаткових фінансових операцій, відмивання “брудних” коштів через електронні банківські системи.

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. Але особливо активно криміналітет використовує останнім часом можливість Internet. Специфічна особливість глобальної мережі – відсутність кордонів. Тому для організації, наприклад, торгівлі наркотиками або зброєю достатньо створити відповідний сайт (Web - сторінку) та чекати на конкретні пропозиції. Причому фізично комп'ютер, на якому розміщується відповідна інформація, знаходиться у третій країні. Обмін пропозиціями між членами злочинних угруповань можливий знову ж таки через анонімні поштові адреси, які після успішного завершення операції закриваються.

Використовують у злочинних цілях Internet і професіонали, які застосовують свої знання для промислового шпигунства, політичних цілей, тероризму. Своїми діями вони здатні посягти фінансову паніку, спровокувати військову катастрофу, пошкодити важливу інформацію на особливо небезпечних об'єктах - адже діяльність енергетичних комплексів, транспорту, банків в значній мірі залежить від надійного зберігання, аналізу та передачі інформації.

Кримінальне переслідування злочинів в сфері високих технологій

Комп'ютерна злочинність викликає занепокоєння світового співтовариства. Усвідомлюючи, що без створення відповідної правової основи ефективна протидія комп'ютерній злочинності неможлива, економічно розвинуті країни прийняли спеціальні законодавчі акти.

Перші закони стосовно комп'ютерних злочинів прийняті у 70-80 роки майже усіма індустріально розвинутими країнами. Серед них 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.

Донедавна у вітчизняному кримінальному праві системоутворюючою щодо переслідування

комп'ютерних злочинів виступала стаття 198¹ Кримінального Кодексу України “Порушення роботи автоматизованої системи”. У правоохоронній діяльності використовувались також ст. 148⁵ “Шахрайство з фінансовими ресурсами”, ст. 148⁶ “Незаконне збирання з метою використання або використання відомостей, що становлять комерційну таємницю”, ст. 148⁷ “Розголошення комерційної таємниці” та інші [4].

У новому Кримінальному Кодексі, прийнятому Верховною Радою 5 квітня 2001, року комп'ютерним правопорушенням присвячено розділ XVI “Злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж”. В розділі передбачено 3 статті:

ст. 370. “Незаконне втручання в роботу електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж”. Санкція цієї статті передбачає штраф до сімдесяти неоподатковуваних мінімумів доходів громадян, або виправні роботи на строк до двох років, або обмеження волі на той самий строк. У випадку заподіяння шкоди у великих розмірах або вчиненні повторно чи за попередньою змовою групою осіб, – обмеження волі на строк до п'яти років або позбавлення волі на строк від трьох до семи років;

ст. 371. “Викрадення, привласнення, вимагання комп'ютерної інформації або заволодіння нею шляхом шахрайства чи зловживання службовим становищем”. Максимальне покарання, передбачене цією статтею – позбавлення волі на строк від двох до десяти років.

ст. 372. “Порушення правил експлуатації автоматизованих електронно-обчислювальних систем” передбачає відповідальність посадових осіб, якщо це спричинило викрадення, перекручення чи знищення комп'ютерної інформації і карається штрафом до п'ятдесяти неоподатковуваних мінімумів доходів громадян, або позбавленням права обіймати певні посади чи займатися певною діяльністю на строк до п'яти років, або виправними роботами на строк до двох років.

Проте, на нашу думку, Законодавець в цьому напрямку зупинився на півдорозі. Адже з урахуванням входження України до Європейської спільноти, необхідності міжнародного співробітництва щодо переслідування комп'ютерних злочинів настала нагальна потреба реформування чинного законодавства згідно з Європейською угодою щодо комп'ютерних правопорушень, в якій досить чітко визначені види комп'ютерної злочинності та шляхи взаємодії урядів щодо регулювання міждержавного розшуку та боротьби з комп'ютерними правопорушеннями.

Комітет у справах законодавства Ради Європи у проєкті Конвенції щодо кібер-злочинів рекомендує уніфікувати кримінальне законодавство з питань комп'ютерних правопорушень та передбачити відповідальність за такі злочини:

несанкціонований доступ (доступ до інформації без відповідної санкції або з порушенням правил доступу);

незаконне перехоплення інформації (перехоплення технічними засобами комп'ютерної інформації або перехоплення комп'ютерних випромінювань);

пошкодження інформації (модифікація, знищення та ін.);

створення перешкод для функціонування комп'ютерних систем;

розповсюдження програм, паролей чи кодів доступу до інформаційних систем (хакери викрадають паролі та розповсюджують їх, чим створюють загрозу безпеці інформаційних систем);

комп'ютерне шахрайство (втручання в роботу інформаційної системи з метою отримання економічного зиску);

розповсюдження дитячої порнографії;

правопорушення, пов'язані з авторським правом.

Відмова від кримінального переслідування або “частково” уніфіковане законодавство - це серйозні проблеми у боротьбі з кіберзлочинністю. На сьогодні тільки в одній країні – Філіппінах, повністю модифіковане законодавство. Це викликано обставинами, що склалися після руйнівного проходження світом вірусу “Love You”, адже згідно з існуючими законами, студента, що склав вірус не можна було притягнути до суду.

Крім того, на наш погляд, необхідні доповнення до Кодексу про адміністративні правопорушення та Цивільного кодексу з метою регулювання в них сучасних інформаційних відносин. Слід також внести відповідні зміни до Кримінально-процесуального кодексу України, зокрема до ст.ст. 78, 79 які б до об'єктів злочинних дій відносили б і інформацію. Це має посилити правове забезпечення безпеки інформаційних систем, а також відповідальність адміністраторів баз даних та інших посадових осіб, що забезпечують експлуатацію комп'ютерних інформаційних систем.

Важливим етапом розвитку чинного законодавства, що прискорить розвиток національної складової Internet, має стати прийняття Закону України “Про телекомунікації”, а також нормативний акт про використання електронного цифрового підпису. При підготовці законопроекту щодо телекомунікацій гострі дебати чиняться навколо статей 21–24 та 45, що стосуються ліцензування, сертифікації та контролю якості надання послуг. Спираючись на міжнародний досвід необхідно виробити такий механізм державного

регулювання, який би не став на шляху розвитку ринкових відносин у цій відносно молодій галузі.

Для забезпечення інформаційної безпеки держави актуальним є законодавче врегулювання перегляду електронної інформації, фіксація Web-серфінгу (пошуку інформації в Internet) відповідними спеціальними підрозділами. Ці заходи необхідно проводити з метою вчасного виявлення правопорушень.

Вирішення в комплексі зазначених проблем можливо за умови кодифікації інформаційного законодавства України на рівні Кодексу України про інформацію.

Вже сьогодні з проектом концепції Кодексу можна ознайомитися на сайті (<http://mndc.naiu.kiev.ua/KONC/ST-TL.htm>). Це має сприяти адекватності процесу правотворення у сфері суспільних інформаційних відносин потребам практики (зокрема, на законодавчому рівні), комплексному, системному вирішенню проблем удосконалення інформаційної діяльності суспільних інституцій нашої країни.

Виявлення та розслідування злочинів в Internet

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, налагодження міжнародного співробітництва для розслідування комп'ютерних злочинів та ліквідації злочинних угруповань. Наприклад, для проведення обшуку у справах щодо комп'ютерних злочинів необхідно користуватись спеціальними технічними засобами та додержуватись відповідної тактики проведення пошуку інформації у зв'язку з тим, що на сьогодні існує багато програмних та апаратних методів захисту від несанкціонованого доступу, у тому числі і від правоохоронців.

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. В ФБР Сполучених Штатів створено National Computer Crime Squared, Computer Investigation and Infrastructure Threat Assesmtnt Centre, San Jose Resident Agency, San Francisco Division. Відповідні підрозділи створені і в Міністерстві юстиції США. Аналогічні підрозділи існують і в інших державах світу.

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

Відповідно до Указу Президента України № 582/2000 від 10 квітня 2000 року реалізація державної політики у сфері захисту державних інформаційних ресурсів покладена на Департамент спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України.

В системі МВС України йде розбудова спеціальних підрозділів. До учбових дисциплін курсантів вносяться відповідні зміни [5]. На наш погляд доцільно було б створити WEB-сторінку підрозділу, яка б містила у собі крім сервісу для передачі відповідних повідомлень від жертв інформаційних правопорушень ще й нормативні акти, рекомендації фахівців, роз'яснення правил поведінки у кіберпросторі, в тому числі і для дітей та підлітків.

Крім спец підрозділів, безпеку в Internet-мережі повинні всіляко підтримувати Internet-провайдери та власники інформаційних систем. Зокрема, керівники служб безпеки банків, інших критичних в інформаційному відношенні установ перш за все повинні зважено підійти до питання доцільності використання Internet-послуг. При позитивному вирішенні необхідно спланувати хто, коли і з якою метою повинен користуватися мережею, забезпечити технічний захист інформаційних систем ("firewall"), використовувати криптографічний захист інформації. Як показує практика, особливу увагу необхідно приділяти конфліктним ситуаціям у колективі, через те, що в більшості протиправних дій, пов'язаних з порушенням інформаційних систем, буває задіяна організована злочинна група, один з членів якої, як правило, знаходиться в потерпілій групі. Іноді достатнє матеріальне та моральне стимулювання своїх працівників коштує набагато дешевше, ніж значні витрати на програмно-технічні комплекси захисту.

На наш погляд слід активніше використовувати Internet і для боротьби із традиційними злочинами. Наприклад, у відповідь на утворення сайту Колумбійської повстанської армії, яка використовувала Internet для обговорення питань транспортування, виробництва, маркетингу наркотиків, служба розвідки Колумбійської армії створила свою сторінку для отримання інформації про наркоділків. За словами представників армії за перші дві доби дії сайту ним скористалися більше тисячі чоловік [6].

На сайті Міжвідомчого науково-дослідного центру з проблем боротьби з організованою злочинністю (<http://mndc.naiu.kiev.ua>) розміщено матеріали щодо правоохоронної діяльності в Україні та за кордоном:

законодавство з питань боротьби з організованою злочинністю та корупцією;
міжнародний досвід боротьби з організованою злочинністю;
газета Координаційного комітету по боротьбі з корупцією і організованою злочинністю при Президентіві України "Крок";
науково-практичний журнал "Боротьба з організованою злочинністю і корупцією (теорія і практика)";
огляд регіональної та центральної преси;
форум (обговорення актуальних питань законодавства).

Висновки

Вище розглянуто далеко не всі питання, пов'язані з безпечним функціонуванням інформаційних систем в Internet. Кожне з них, наприклад, розповсюдження вірусів чи використання не ліцензійного програмного забезпечення, потребує окремого дослідження. Вітчизняне інформаційне право знаходиться ще на стадії формування. В цілому це завдання вимагає системного підходу та координації діяльності не тільки державних структур та правоохоронних органів, а й усіх, зацікавлених 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.

Література: 1. Послання Президента України до Верховної Ради "Україна: поступ у XXI сторіччя. Стратегія економічного та соціального розвитку на 2000-2004 роки" // Урядовий кур'єр. – 2000. - № 16. – С. 7. 2. Указ Президента України Про заходи щодо розвитку національної складової глобальної інформаційної мережі Інтернет та забезпечення широкого доступу до цієї мережі в Україні № 582 від 31 липня 2000 року. 3. Компьютерные преступления / Айков А., Сейгер К., Фонсторх У. - М., "Мир". - 1999. - С. 27. 4. Виявлення та розслідування злочинів, що вчиняються за допомогою комп'ютерних технологій Б. В. Романюк, М. І. Камлик, В. Д. Гавловський, В. Г. Хахановський, В. С. Цимбалюк за заг. ред. Я. Ю. Кондратьєва. -К., - 2000. 5. Криміналістика П. Д. Біленчук, В. В. Головач, М. В. Салтевський. К. – 1997. 6. *Jane's Defence Weekly.*— 1997.— 16 July.— P. 10.

УДК 681.322:621.395

АСПЕКТИ ПОЛІТИКИ БЕЗПЕКИ СИСТЕМИ

УПРАВЛІННЯ ТЕЛЕКОМУНІКАЦІЙНИМИ МЕРЕЖАМИ

Микола Тардаскін, Володимир Кононович

Одеський регіональний центр технічного захисту інформації ВАТ "УКРТЕЛЕКОМ"

Анотація: Розглядається демонстраційний приклад політики безпеки інформації у системах управління телекомунікаційними мережами (СУТ). Охоплені питання, що мають бути застосовані при реалізації політики безпеки об'єктів СУТ.

Summary: Demonstrative examples of security policy in the Telecommunication Management Network (TMN) are considered. The aspects, which must application in security policy realization of the object of TMN examine.

Ключові слова: Політика безпеки, система технологічного управління, інформація, адміністратори, програмне забезпечення.

Інформація, що використовується у системах управління телекомунікаційними мережами (СУТ), є критично важливою для галузі телекомунікацій [1]. Розміри та складність побудови СУТ великі і вона забезпечує обмін інформації між значною кількістю операторів [2]. Це призводить до збільшення ризиків і вимагає застосування більш сильних механізмів захисту, порівняно з тими, що потрібні при роботі з окремими персональними комп'ютерами (ПК). Посилені вимоги до захисту в обчислювальному середовищі СУТ зумовлюють необхідність даної політики.

І Мета і загальні положення політики безпеки

Метою роботи є розвиток нормативно-правової бази для реалізації комплексної системи захисту інформації СУТ [3, 4]. Політика безпеки є ключовим компонентом плану захисту СУТ. У той же час,