Інтернет: протидія кримінальним проявам та боротьба зі злочинністю

На межі тисячоліть людство реально відчуває прихід інформаційної революції, про яку науковці, у тому числі й вітчизняні, писали ще тридцять років тому. Серед основних тенденцій розвитку інформатизації суспільства, що стосується практично всіх сфер життєдіяльності, включаючи економіку, державне управління, науку, мистецтво, слід відзначити стрімкий розвиток інформаційної мережі Інтернет.

Інтернет – це глобальна комп’ютерна мережа, що об’єднує сотні мільйонів користувачів з усього світу, яка почала свій розвиток у 1969 році із замовлення Управління перспективних досліджень (Advanced Research Projects Agency) Міністерства оборони США на побудову мережі, здатної підтримувати обмін інформацією між користувачами за умов ядерної війни. Після прийняття протоколу Transmission Control Protocol/ Internet Protocol (TCP/IP) за стандарт значно зросла швидкість передачі даних по мережі. з 90-х років почалося широке використання Інтернет у комерційних цілях (у 1999 р. світовий прибуток від електронної комерції складав 300 млрд дол.). Сьогодні це важливий фактор, що визначає успіх у бізнесі та науці, це потужний засіб розповсюдження преси, юридичних актів, місце проведення дозвілля та спілкування людей. Послуги Інтернет надають можливість не тільки придбати продукти харчування чи книги, але й брати участь в аукціонах 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 соціально-економічні проблеми ще відстають від потреб сьогодення, наша держава сміливо входить у світовий інформаційний простір. В Україні налічується понад 500 тис. абонентів Інтернет (1 користувач – на 100 громадян, у США, відповідно, 25 користувачів, у Європі – 9). Вже побудовано волоконно-оптичні магістралі, що забезпечують швидкісний доступ в Інтернет до 2 Мб/с. Більше 200 провайдерів (організацій, що забезпечують зв’язок з глобальною мережею) використовують для надання послуг сучасні швидкісні канали доступу, хоча більшість з них знаходиться у Києві [1].

Водночас розбудова інформаційного суспільства вимагає вирішення низки соціальних, організаційних, юридичних та інших проблем, що пов’язані як із впровадженням нових інформаційних технологій у цілому, так і з розвитком структури Інтернет зокрема. Однією із найгостріших з них в умовах глобалізації застосування сучасних комп’ютерних інформаційних технологій практично в усіх сферах життєдіяльності є активне використання злочинним світом наданих їм можливостей для посилення організованості, розширення бандитських зв’язків, поява так званої “комп’ютерної” злочинності, включаючи комп’ютерний тероризм. Сьогодні доходи комп’ютерних злочинців за оцінками фахівців Інтерполу посідають третє місце після доходів наркоділків та постачальників зброї.

Відомий термін “хакер” з’явився в 60-ті роки у Масачусетському технологічному інституті. Так називали людей, здатних ставити перед собою складні завдання та вирішувати їх. Такими були розробники комп’ютерної мережі ARPANET, операційної системи Unix. У 80-х роках не без допомоги журналістів термін “хакер” набув негативного відтінку. Його почали використовувати до людей, які порушують закон за допомогою комп’ютера [2]. Принципово новим видам комп’ютерної злочинності сприяв 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 прошарку, мабуть, є Кевін Митник – програміст з Лос-Анджелеса, який 17-річним хлопчиною був затриманий за крадіжку списку паролей доступу телефонної компанії Pacific Bell. Найвідомішою стала його війна з лабораторією Digital Equipment, яку він у 1995 році програв спеціалісту по безпеці комп’ютерних систем Тсутму Шимомурі [3]. Сума збитків, заподіяних хакером, становить кілька десятків мільйонів доларів.

Використання Інтернету як інструменту в електронних комерційних справах змінює традиційно існуючу практику ведення безготівкових платежів і розрахунків. Сьогодні у світі налічується понад 500 банків (серед них Security First Network Bank, Mark Twain Bank США та ін.), що надають в Інтернеті послуги юридичним і фізичним особам. До 2001 року таких установ налічуватиметься більше 2000. Кібернетичні гроші як платіжний засіб будуть використовуватись замість готівки, причому перекази з пристрою відправника до одержувача передаються, як правило, анонімно. Серед основних причин швидкого поширення використання електронних платежів є те, що оплата послуг через Інтернет обходиться клієнту в 0,01 дол. США, з використанням автоматів – у 0,27 дол. США, надання послуг через телефон – 0,54 дол. США, а надання послуг у касового вікна – у 1,07 дол. США [4]. У той же час згідно з дослідженням компанії Gartner Group кількість фінансових махінацій в Internet у 12 разів більше, ніж у звичайних банківських установах США.

В. Левін – найвідоміший з пострадянських хакерів, який подолав систему безпеки Citibank і за допомогою віддаленого комп’ютерного доступу викрав 12 млн дол., 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 тис. дол. і втік до Канади.

Впровадження в Україні у банківські системи електронної обробки інформації сприяло виникненню аналогічних злочинів і в нашій державі. Так, 24 січня 1994 року співробітник Г. АКБ “Україна” сформувала фіктивний електронний платіж на суму 450 млн крб. та перерахувала його на рахунок Севастопольського товариства “Орбі” для подальшої конвертації. Злочинну групу у складі чотирьох чоловік було затримано, і 31 січня 1994 року порушено кримінальну справу. У червні 1994 року УБОЗом МВС України в Дніпропетровській області припинено спробу викрадення злочинним угрупованням 864 млн крб. з Промінвестбанку м. Дніпропетровська [5].

На сьогодні гостро стоїть проблема боротьби з проведенням безподаткових фінансових операцій, “ відмиванням брудних” коштів через електронні банківські системи. Для цього глобальна мережа створює принципово нові умови, які повністю використовують кримінальні структури. Так, з доповіді Бюро технологічної оцінки Сполучених Штатів, у день 0,05 ‑0,1% банківських переказів відносяться до “відмивання” грошей. Для оцінки масштабу проблеми необхідно враховувати те, що через електронну систему зв’язку тільки у США щоденно проводяться понад 2 000 млрд дол. [6]. Усім відомий політичний скандал після проведення у 1999 році численних транзакцій з “відмиванням” коштів на суму близько 10 млрд дол. до американського банку Bank of New York.

Перелік комп’ютерних злочинів можна продовжити, згадавши й атаки на військові, космічні комп’ютерні системи, промислове шпигунство, використання компромату в політичних цілях і т.ін. У травні 1998 р. “тигри звільнення Тамілу” у Шрі-Ланка вперше серед терористичних груп провели кібернетичну атаку, спрямовану проти посольств у столиці [7]. Відомі випадки успішних атак хакерів на сервери Центрального розвідувального управління, Федерального бюро розслідування, Пентагону, Сенату, інших урядових, комерційних, наукових установ США, що мають неабиякий досвід захисту інформаційних систем.

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

Безпосередньо на комп’ютерні системи спрямовані дії так званих “кракерів”, які, на відміну від “хакерів”, є менш кваліфікованими фахівцями інформаційних систем, проте своїми вчинками – зміною текстів чи зображень в Інтернет-системах – завдають значної шкоди. Прикладом їх протиправних дій може бути поява порнографічних зображень на сайтах, розрахованих на школярів, а незначна зміна в банку даних групи крові пацієнтів медичного закладу може призвести до катастрофи.

Одним із 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. Таких нелегальних користувачів називають “фрікерами”. Організовані злочинні групи цього спрямування в Україні останнім часом завдають значної шкоди як окремим громадянам, так і телекомунікаційним установам.

Але найнебезпечнішими злочинцями у кіберпросторі є професіонали, які використовують свої знання для промислового шпигунства, політичних цілей, тероризму. Своїми діями вони здатні посіяти фінансову паніку, вивести з орбіти супутник, змінити важливу інформацію на особливо небезпечних об’єктах, діяльність яких значною мірою залежить від надійного зберігання, аналізу та передачі інформації. Президентська комісія США по захисту критичної інфраструктури (PCCIP) у звіті за 1997 р. визначила уразливість до кібернетичних атак таких інфраструктур, як телекомунікації; банківські та фінансові системи; електро- і енергопостачання; розподіл і збереження нафти й газу; водопостачання; транспортні системи; аварійно-рятувальні служби; державні установи [[7]](#гуц1).

Організація успішної боротьби з комп’ютерною злочинністю на магістралях глобальної мережі вимагає, перш за все, розбудови відповідної законодавчої бази, постійного аналізу криміногенної ситуації, кримінологічного дослідження проблеми, відповідної підготовки спеціальних правоохоронних підрозділів.

Перші закони стосовно комп’ютерних злочинів були прийняті Швецією (1973 р.), пізніше – у Німеччині, Австралії, Італії, Франції, Іспанії, Канаді, Сполучених Штатах Америки, які найбільше страждають від злочинів у сфері високих технологій. з кінця 80-х рр. з’явилися перші нормативно-правові акти, що регулюють інформаційні відносини в глобальній мережі. Але процес удосконалення чинного законодавства не припиняється і сьогодні, що пояснюється стрімким розвитком інформаційних систем. Для дослідження проблеми незаконного використання Інтернет у серпні 1999 року Президентом США Б. Клінтоном було створено Робочу групу у складі міністра юстиції, директора ФБР, керівника офісу управління та бюджету, секретаря освіти та інших зацікавлених осіб.

У Китаї побоювання впливу, який Інтернет може завдати китайському суспільству, політиці й комерції, призвів до появи цілого потоку регулюючих актів уряду країни, що охоплюють широке коло питань, включаючи заборону передачі через мережу не схваленої урядом інформації. Новини розміщуються тільки на державних сайтах під контролем Держкомітету по інформації (State Council Information Office).

У країнах Європи з 90-х років теж з’являються нормативні акти, що стосуються регулювання відносин в Інтернеті. В них визнається основний принцип Інтернет-індустрії – саморегуляція. У той же час чітко визначено відповідальність перед законом за протиправні дії. Європейський комітет з проблем злочинності Ради Європи підготував рекомендації із метою визначення правопорушень, пов’язаних з комп’ютерами для включення їх у законодавство європейських країн. Враховуючи рішення щодо гармонізації законодавства України із законодавством Європейського Союзу, необхідно до ст. 1981 Кримінального кодексу України додати й інші, які б розширили дію кримінальної відповідальності за протиправне використання можливостей Інтернет (розповсюдження нелегального матеріалу, несанкціоноване перехоплення інформації, комп’ютерний саботаж тощо). Крім того, необхідно внести статті стосовно регулювання сучасних інформаційних відносин до Кодексу про адміністративні правопорушення та Цивільного кодексу, що має посилити правове забезпечення безпеки інформаційних систем, а також відповідальність адміністраторів баз даних та інших посадових осіб, які забезпечують експлуатацію комп’ютерних інформаційних систем.

Важливим етапом розвитку чинного законодавства, що має прискорити розвиток національної складової Інтернету, повинно стати прийняття Закону України “Про телекомунікації”, а також нормативного акта про використання електронного підпису. Спираючись на міжнародний досвід, необхідно розробити такий механізм державного регулювання, який би не перешкоджав розвитку ринкових відносин у цій відносно молодій галузі.

З метою вчасного виявлення та профілактики таких видів злочинної діяльності в Інтернеті, як розповсюдження порнографії, расистських лозунгів чи антидержавної інформації, необхідно широко використовувати асоціативні фільтри, проводити заходи з врегулювання перегляду електронної інформації, фіксації Web-серфінгу (пошуку інформації в Інтернеті) відповідними спеціальними підрозділами, що потребує відповідного законодавчого врегулювання.

Як уже зазначалось, величезний потік інформації надходить в Інтернет із різних держав; користуватися нею можна практично з будь-якого куточка світу. Причому міжнародне спілкування з використанням Інтернет ніким не регулюється (не існує органу управління мережею, а основний засіб встановлення правил – саморегулювання). Тому протидія злочинним проявам у глобальній мережі тільки на національному рівні буде малоефективною. У зв’язку з цим необхідні розробки і прийняття таких норм, що будуть пристосованими до законодавств інших держав.

Специфіка виявлення та проведення слідчо-криміналістичних дій в Інтернет – 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.

У Міністерстві внутрішніх справ 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 у сфері високих технологій. У США створено Національний центр захисту інфраструктури (NIPC), завданням якого є попередження та розслідування комп’ютерних злочинів та координація роботи інших центрів, таких, як National Computer Crime Squad, San Jose Resident Agency, San Francisco Division, Cyber Emergency Support Team та ін.

В Україні здійснюється формування спеціальних підрозділів електронної розвідки та протидії комп’ютерним злочинам як у МВС, так і у СБУ. Проте, на наш погляд, слід приділяти увагу і питанням спеціальної підготовки щодо використання нових інформаційних технологій оперативних працівників правоохоронних органів, адже в сучасних умовах комп’ютерна техніка може фіксувати докази злочинів не тільки в Інтернет-мережі. Під час обшуків будуть постійно виникати питання стосовно доцільності вилучення електронних пристроїв з діючих автоматизованих систем. Невдалі підходи до вирішення цих питань можуть призвести до знищення доказів, порушення роботи цих систем, а це, у свою чергу, до законних судових позовів. Інша причина необхідності поглиблених знань – складність виявлення комп’ютерних злочинів, а також значна вартість комп’ютерної експертизи при обмеженості коштів у правоохоронних органах, чим і користуються злочинці. з такою метою доцільно використовувати сучасні методи та методики викладання [8].

Не варто забувати, що інформаційні системи правоохоронних органів теж можуть піддаватися атакам хакерів. Тому постійно слід вести кропітку роботу щодо технічного та криптографічного захисту інформаційної інфраструктури. Зупинимося на проблемі кадрового забезпечення інформаційних підрозділів, адже інформаційна безпека значною мірою залежить від підбору та розстановки кадрів, постійного підвищення їх професійного рівня. Неприпустимим є призначення на керівні посади працівників без відповідної кваліфікації в надії на засвоєння ними основ інформаційних технологій у подальшій роботі. Це може призвести до неефективної роботи інформаційних систем та зниження рівня інформаційної безпеки у цілому.

На наш погляд, слід активніше використовувати Інтернет і для боротьби з традиційними злочинами. Наприклад, у відповідь на утворення сайту Колумбійської повстанської армії, яка використовувала Інтернет для обговорення питань транспортування, виробництва, маркетингу наркотиків, Служба розвідки Колумбійської армії створила свою сторінку для отримання інформації про наркобаронів. За словами представників армії, за перші дві доби дії сайту ним скористалися більше тисячі чоловік [9].

Інтернет – ідеальний засіб щодо розшуку як злочинців, так і викрадених предметів. При цьому слід використовувати не тільки сайти правоохоронних органів, але й електронні засоби масової інформації (практично кожна центральна газета сьогодні має Інтернет-видання). При відповідному законодавчому забезпеченні використання можливостей Інтернет щодо відеоконференцій для проведення слідчих дій могло б значно заощадити кошти правоохоронних органів (у деяких випадках зникає необхідність виїзду у відрядження чи етапування засудженого).

Важливе значення щодо правового виховання населення мають комп’ютерні правові системи. У цьому аспекті не варто не згадати позитивний досвід найпотужнішого в Україні пошуковоого правовового сервера LIGA ONLINE. Потужним засобом у боротьбі з корупцією повинно стати інформування населення через сайти центральних виконавчих органів стосовно підзаконних нормативних актів.

З метою оперативного інформування населення та правоохоронних органів про стан та проблеми боротьби з організованою злочинністю і корупцією у Міжвідомчому науково-дослідному центрі відкрито WEB-сторінку за адресою: http://mndc.naiau.kiev.ua з наданням наступних матеріалів:

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 Президентові України “Крок”;

огляд регіональної преси;

бібліографічна база даних з проблем боротьби зі злочинністю (понад 2000 праць, статей, монографій);

форум для обговорення актуальних проблем сьогодення.

Звичайно, далеко не всі вищезазначені питання пов’язані з безпечним функціонуванням інформаційних систем в Інтернеті. Наприклад, проблема розповсюдження вірусів (з моменту виходу “черв’яка” Морріса до появи змінних сигнатур) чи використання неліцензійного програмного забезпечення (прозорість вітчизняних інформаційних систем) потребує окремого дослідження. Інші, невідомі на сьогодні правопорушення в Мережі, можливо будуть порушувати цивільне, адміністративне законодавство. Зрозуміло й те, що відносини в інформаційній сфері будуть постійно ускладнюватись. Тому розбудова вітчизняного інформаційного права вимагає системного підходу та координації діяльності не тільки державних структур та правоохоронних органів, а й усіх, хто зацікавлений у подальшому розвитку як Інтернет-культури взагалі, так й Інтернет-комерції зокрема.

Враховуючи постійне зростання правопорушень у кіберпросторі, крім розбудови відповідного законодавства та чіткої роботи правоохоронних органів, необхідна координація зусиль усіх громадян, організацій та установ незалежно від форм власності, налагодження тісного міжнародного співробітництва, використання сучасних технологій захисту інформації для отримання переваг не тільки електронного бізнесу, а й інформаційної революції в цілому.

1. Табаков В. Дорогой, ведущей в сеть //Chip.–1999.– № 11.– С. 28.

2. Любивый Д. Мастера компьютерного взлома //Chip.–1999. – № 10. – С. 78-80.

3. Айков А., Сейгер К., Фонсторх У. Компьютерные преступления. – М.: Мир, 1999. – С. 27.

4. Kriminalistik, 1998. – № 2. – P. 109.

5. Коваленко М. Комп’ютерні віруси і захист інформації. – К.: Наук. думка, 1999.

6. Information Technologies for the Control Money – laundering. Washington, Government Printing Office. –1995. – Sept.

7. International Police Review. –1998. – Nov./Dec. – P. 56.

8. Гуцалюк М.В. Інформаційні технології у професійній підготовці працівників правоохоронних органів // Науковий вісник Національної академії внутрішніх справ України.– К., 2000.– № 1. – С. 145-147.

9. Jane’s Defence Weekly. – 1997. – 16 July. – P. 10.