УДК

Г. В. Загіка, ст. викл.

Одеський національний університет ім. І. І. Мечникова
кафедра кримінального права, кримінального процесу і криміналістики,
Французький бульвар 24/26, Одеса, 65058, Україна

КРИМІНОЛОГІЧНА ХАРАКТЕРИСТИКА КОМП'ЮТЕРНОЇ ЗЛОЧИННОСТІ

Представлено результати кримінологічного дослідження комп'ютерної злочинності. Визначено і охарактеризовано особливості, причини та умови вчинення комп'ютерних злочинів, спрогнозовано основні тенденції їх подальшого розвитку.

Ключові слова: комп'ютерна злочинність, комп'ютерні злочини.

Сьогодні комп'ютерні системи стали основним засобом управління інформацією та її обробки, негативним наслідком цього, однак, є поява комп'ютерних злочинів. Діяльність суб'єктів злочинності у цій сфері спрямована на досягнення великих прибутків при малих затратах, і саме застосування сучасних комп'ютерних технологій дає можливість одержати ці прибутки. Комп'ютерні системи та комп'ютерні мережі створюють різноманітні можливості для вчинення нових видів злочинів, і звичайних традиційних, але більш ефективними засобами. Ці злочини спрямовані на життєво важливі інтереси держави та суспільства, пов'язані зі створенням і використанням новітніх інформаційних технологій та ресурсів, і тому особливо небезпечні.

Відповідно до загальноприйнятого міжнародно-правового визначення, під комп'ютерним злочином слід розуміти будь-які протиправні дії, які спрямовані проти захисту системи даних завдяки електронним операціям [1, 254].

Комп'ютерна злочинність характеризується такими особливостями: використанням сучасних новітніх інформаційних технологій, які потребують спеціальної освіти та високого інтелектуального рівня; високим рівнем латентності; високим ступенем збитку від вчинених комп'ютерних злочинів; складністю своєчасного виявлення та ідентифікації правопорушників; можливістю вчинення злочинів з використанням засобів віддаленого доступу, що обумовлюється відсутністю зловмисника на місці злочину.

Високому рівню *латентності* сприяють такі обставини:

– відсутність достатньої кількості підготовлених фахівців, необхідних технічних засобів для гарантованого виявлення комп'ютерних злочинів та їх розкриття;

– небажання потерпілих у більшості випадків сповіщати про вчинення злочинів у правоохоронні органи;

– утаєний характер цих злочинів, оскільки їх можна вчинити з будь-якої відстані та з будь-якої держави;

– поширенням персональних комп'ютерів у світі та можливість підключення їх до будь-якої інформаційної мережі;

– "розрив" між моментом вчинення комп'ютерних злочинів та проявом їх наслідків [2, 187].

З латентністю тісно пов'язані і труднощі розкриття комп'ютерних злочинів (лише 10-15%).

До найбільш поширених *об'єктів* комп'ютерних злочинів слід віднести:

– комп'ютери військових та розвідувальних організацій;

– комп'ютери компаній та підприємств бізнесу;
– комп'ютери банків та інших фінансових організацій;
– комп'ютери будь-яких організацій, особливо урядових та комунальних.

Комп'ютери військових та розвідувальних організацій відіграють значну роль у забезпеченні національної безпеки, в них зберігається стратегічно важлива інформація, яка має цінність як розвідувальна. Напад на компанії та установи бізнесу перш за все потрібен для знищення конкурентів або для виявлення їх промислових таємниць. Навіть великі компанії (як Apple Computer) теж не захищені від нападу. В грудні 1987 р. ця фірма знайшла вірус у своїй системі електронної пошти. Цьому вірусу вдалося знищити всі мовні повідомлення та відключити систему.

Напад на фінансові організації вчинюється у багатьох випадках її службовцями, які є професіоналами своєї справи. Проведені у США опитування показують, що саме службовці, які мають знання в галузі комп'ютерної техніки, відіграють головну роль у вчиненні комп'ютерних злочинів.

Зарубіжні кримінологи зробили висновок, що при пограбуванні банку матеріальні збитки складають у середньому 20 тисяч доларів, а при комп'ютерному злочині — 560 тисяч доларів. Але шансів бути схопленим у комп'ютерного злочинця значно менше, ніж у грабіжника банку, і при тому шансів понести кримінальну відповідальність значно менше [2, 196].

На замовлення компанії PreciwaterhouseCoopers фахівцями видання Information Week Research було проведене дослідження потенційного збитку від дій комп'ютерних злочинців та вірусів у 2000 р. У ході цього дослідження було опитано 4900 фахівців з 30 держав світу і зроблено висновок, що близько 50 тисяч американських компаній понесуть великі збитки від цих проблем — їх збиток складе 266 млрд. доларів або близько 2,5 % від валового внутрішнього продукту США, а у світовому масштабі вони досягнуть 1,6 трлн. доларів [3, 22].

Комп'ютерні злочини призводять до великих економічних збитків, а суспільство стає все більш і більш залежним від роботи комп'ютеризованих систем у різноманітних сферах суспільного життя — від керування рухом літаків і поїздів до медичного обслуговування та національної безпеки. Іноді навіть невеличкий збій у функціонуванні таких систем може призвести до реальної загрози життю людей. Стрімке зростання глобальних комп'ютерних мереж, а також можливість підключення до них через звичайні телефонні лінії посилюють можливості їх використання для кримінальної діяльності.

Комп'ютерна злочинність — це міжнародне явище, рівень її тісно пов'язаний з економічним рівнем розвитку суспільства у різних державах та регіонах. Міжнародні комп'ютерні мережі надають користувачам можливість вчиняти певні дії за межами держави, в якій вони знаходяться, та обирати таке правове середовище, яке найбільше відповідає їх цілям. Користувачі обирають такі держави, в яких певні дії в електронному середовищі не спричинять кримінальну відповідальність. Наявність таких держав значно стримує намагання інших держав у боротьбі з комп'ютерною злочинністю.

Для більшості комп'ютерних злочинів характерна корислива мета. Щорічна виручка злочинців у результаті комп'ютерних шахрайств у США оцінюється в 3 мільярди доларів, комерційна школа в Лондоні оцінює збитки Великобританії від цього виду комп'ютерних злочинів більш ніж у 400 млн. фунтів стерлінгів, а деякі експерти вважають, що ця сума досягає 2 мільярдів фунтів. І така тенденція спостерігається у всіх промислово розвинутих країнах. Ця тенденція не обійшла стороною і Україну.

Розвиток мережі комп'ютерних банків з великими обсягами фінансових операцій, зростання обсягів перелічених коштів між державними і комерційними структурами привели до необхідності спрощення банківських розрахунків. З цією метою в Україні було введено систему електронних розрахунків, яка призвела

в свою чергу до нової техніки вчинення корисливих злочинів. Навмисні комп'ютерні злочини складають значну частину злочинів, але зловживань комп'ютерами та помилками ще більше. Як сказав один експерт, "ми втрачаємо через помилки більше грошей, ніж могли б їх викрасти" [4, 197].

Найбільш типовими злочинними засобами для досягнення протиправних цілей (у процесі чого неправомірно використовуються комп'ютери) такі: підробка рахунків та розрахункових відомостей, фальсифікація платіжних документів, розкрадання грошей з грошових фондів, отримання фальшивих дипломів, знищення та перекручення комп'ютерної інформації, порушення роботи комп'ютерів та їх систем і мереж, комп'ютерний саботаж програмного та апаратного забезпечення. Зміни, що відбуваються в економічному житті України, — створення фінансово-кредитної системи, підприємств різноманітних форм власності і т. ін., істотно впливають на проблему захисту інформації, яка знаходиться в комп'ютерах, банках даних та у мережі.

Щороку економічні втрати, викликані комп'ютерними злочинами, обчислюються мільйонами доларів, причому багато втрат не виявляються або про них не повідомляється. Тільки при електронній передачі коштів обсяг операцій указує на те, що потенційні втрати, можливо, перевищують збитки при передачі коштів за допомогою паперових документів.

Дуже часто банки не хочуть, щоб клієнти знали про їхню вразливість і тому не бажають повідомляти про такі злочини. Можна обгрунтовано стверджувати, що майже кожний злочин, пов'язаний з використанням електронної техніки, може призвести до винятково значних утрат протягом дуже короткого періоду часу, майже не залишаючи ніяких слідів злочину. Ряд таких злочинів привернув велику увагу до цієї загрози. Відомі комерційні видання опублікували сотні статей про те, як зробити системи обробки даних більш надійними. Проте серед експертів, що займаються питаннями безпеки використання електронного устаткування, існує єдина думка про те, що величезне число розкрадених коштів, зароблених за допомогою електронної техніки, залишається незнайденими.

Крім того, у цій галузі законодавство часто не встигає за розвитком техніки, а підготування персоналу правоохоронних органів є недостатнім для виконання задач, пов'язаних із виявленням і контролем комп'ютерних злочинів.

Одними з перших з комп'ютерним злочином зіткнулися співробітники управління по боротьбі з організованою злочинністю УВС Дніпропетровської області. В 1994 році ними було попереджено спробу розкрадання 864 млн. карбованців шляхом несанкціонованого проникнення в банківську електронну систему платежів. Ведучий інженер-комп'ютерщик регіонального управління Промінвестбанку Дніпропетровська, маючи доступ до охоронної системи комп'ютерної мережі банку, за допомогою особистого комп'ютера, який був установлений у квартирі, ввійшов до локальної мережі банку. Оформив фіктивний рахунок на 864 млн. крб., "вклав" його до "поштової скринки" комп'ютера банку для відправки на рахунок однієї з дніпропетровських фірм. Після зарахування суми на рахунок фірми зловмисники були затримані [4, 18].

Однак особливий інтерес являють комп'ютерні злочини, вчинені фахівцями по використанню ЕОМ. Представники цієї галузі працюють на грані ентузіазму, вони "грають", перетинаючи системи захисту інформації та "відкриваючи" паролі і коди. Але перетинаючи межі дозволеного, ці професіонали стають комп'ютерними злочинцями, дії яких підпадають під дію кримінального законодавства.

Різні країни мають неоднакові національні законодавчі системи. Деякі з країн уже мають спеціальні норми у кримінальному законодавстві, які передбачають відповідальність за вчинення комп'ютерних злочинів, інші тільки у процесі прийняття відповідних законів. У багатьох країнах відповідальність за вчинення комп'ютерних злочинів настає за традиційними статтями кримінального законодавства (крадіжка, шахрайство, підробка та ін.). Див. таблицю 1.

Таблиця 1

Класифікація комп'ютерних злочинів

Вид злочину	Мета	Об'єкт	Особливість
Незаконний доступ до комп'ютерної системи або мережі	Ознайомлення або копіювання програм та даних	Комп'ютерна система або мережа	Подолання системи захисту
Перехоплення даних за допомогою технічних пристроїв	Перехоплення, тобто прослуховування інформації, даних	Будь-яка форма зв'язку	Незаконними є тільки випадки, передбачені законодавством
Викрадення часу	Ухилення від належної оплати	Будь-яка система зв'язку	
Незаконна заміна комп'ютерних даних: – логічна бомба; – троянський кінь; – троянська матрьошка; – віруси; – черв'яки;			
– часова бомба і т. ін.	Незаконна заміна, знищення або пошкодження комп'ютерних даних	Комп'ютер, комп'ютерна система або мережа	Здійснюються різними засобами, в основному логічними пристроями, які стають активними при виконанні специфічних операцій, при досягненні визначеного моменту часу
Комп'ютерне шахрайство	Отримання фінансового прибутку або іншої вигоди	Комп'ютер, комп'ютерна система або мережа	Використання переваг сучасних комп'ютерних технологій
Телефонне шахрайство	Уникнення від сплати рахунків, підслуховування	Телефонні пристрої	Використання телекомунікаційних мереж
Несанкціоноване копіювання	Отримання фінансового прибутку	Комп'ютерні ігри, програмне забезпечення	Порушення авторських прав
Комп'ютерний саботаж	Перешкодження нормальному функціонуванню комп'ютера	Комп'ютер, комп'ютерна система	Саботаж програмного та апаратного забезпечення

Але це тільки одна з класифікацій комп'ютерних злочинів. Відомий фахівець у даній галузі Ю. М. Батурін розглядає чотири типи комп'ютерних злочинів відносно того, які збитки приносять ці злочини. Це: порушення функцій, втрата вагомих ресурсів, втрата монопольного користування, порушення авторських прав [4, 134-135].

Виявлено можливі чотири види порушення функцій:

- тимчасові порушення, які призводять до хаосу у графіках роботи;
- недоступність системи для користувача;
- пошкодження апаратного забезпечення;
- пошкодження програмного забезпечення.

Втрата вагомих ресурсів означає втрату грошей, інформації, програмного забезпечення, машинного часу. Втрата монопольного використання — втрату цінності інформації для власника, котрий є її монопольним власником.

Найактуальнішим питанням у зв'язку з комп'ютерними злочинами залишаєть-

ся підтримання прав людини та громадянина при використанні комп'ютерних систем та мереж. Нові інформаційно-технічні технології:

– розширюють права громадян шляхом надання швидкого доступу до різноманітної інформації;

– збільшують можливості людей брати участь у процесі прийняття політичних рішень та стежити за діями урядів;

– надають можливість активно створювати інформацію, а не тільки її споживати;

– забезпечують засоби захисту приватного життя й анонімності особистих послань і комунікацій.

У той же час має місце зростання втручання держави в галузь пересилання та шифрування електронних повідомлень, що може загрожувати основним конституційним правам громадян.

Так, голова Служби безпеки України Л. Деркач повідомив, що СБУ має намір контролювати Інтернет-провайдерів України [6, 56]. Це означає, що буде встановлено спеціальне устаткування, яке дозволяє СБУ читати електронну пошту українських громадян і стежити за їхньою інтерактивністю. Але необхідно мати на увазі, що Інтернет — це всесвітня глобальна комп'ютерна мережа, і не тільки повідомлення наших співгромадян проходять через Інтернет-провайдерів України. Адже дуже часто провайдери однієї держави виступають як транзитні бази для пересилки повідомлень для ряду інших держав.

Для попередження комп'ютерних злочинів розробники автоматизованих систем, обчислювальної техніки та засобів передавання інформації передбачають різноманітні засоби захисту інформації та комп'ютерних систем і мереж.

Основними засобами такого захисту є: технічні, програмні, криптографічні, організаційні та правові. Технічні обумовлюють захист даних та систем різними апаратними засобами захисту (екранування приміщень, встановлення джерел безперебійного живлення, засобів розпізнавання користувача та ін.).

Розробка та застосування спеціального програмного забезпечення, яке б не дозволяло стороннім отримувати інформацію із системи, обумовлює програмні засоби захисту даних та програм для комп'ютерів.

Без застосування криптографічних методів захисту інформації практично неможливо реально захистити інформацію. Сучасна криптографія базується на сучасних досягненнях математики, фізики, інженерних дисциплін та досягненнях у галузі розробки і використання комп'ютерних технологій. Крім криптографії, застосовується ще стеганографія, яка приховує сам факт існування таємного повідомлення.

До правових норм слід віднести розробку та прийняття норм, які встановлюють відповідальність за порушення інтелектуальної власності, за комп'ютерні злочини.

Розглянувши в цілому проблему розвитку комп'ютерної злочинності як у нас в країні, так і за кордоном, можна сказати, що робиться дуже багато для вивчення цього негативного соціального явища та пошуку шляхів розв'язання цієї проблеми. Хочеться надіятися, що Україна у новому тисячолітті подолає ці труднощі кінця XX століття.

Література

1. Десятый Конгресс ООН по предупреждению преступности и обращению с правонарушителями: Сборник документов. – М.: Юрлитинформ, 2001. – 496 с.

2. Скоромников К. С. Компьютерное право Российской Федерации. М.: МНЭПУ, 2000. — 224 с.

3. Досье секретных служб// Киев, №9, 2000. — 64 с.

4. Батурин Ю. М. Проблемы компьютерного права. М.: Юридическая литература, 1991, 272 с.

5. Гавриленко И. Компьютерная преступность // Служба безопасности, № 1, 97. — С. 35.

6. Безопасность в Интернете//Досье секретных служб, № 6, 2000. — 64 с.

А. В. Загика

Одесский национальный университет им. И. И. Мечникова,
кафедра уголовного права, уголовного процесса и криминалистики,
Французский бульвар, 24/26, Одесса, 65058, Украина

КРИМИНОЛОГИЧЕСКАЯ ХАРАКТЕРИСТИКА КОМПЬЮТЕРНОЙ ПРЕСТУПНОСТИ

РЕЗЮМЕ

Исследованы цели, объекты и другие особенности компьютерной преступности. Проанализированы основные причины и условия совершения преступлений в сфере компьютерных технологий. Определены основные виды компьютерных преступлений и способы их совершения.

Ключевые слова: компьютерная преступность, компьютерные преступления.