

В. П. Бєленький, аспірант

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

СУЧАСНА ІСТОРІЯ ЗЛОЧИНІВ У СФЕРІ КОМП'ЮТЕРНОЇ БЕЗПЕКИ

У статті розглянуті питання виникнення злочинів у сфері комп'ютерної безпеки у західних країнах, їх подальше розповсюдження по всьому світі, у тому числі в СРСР, зазначені перші випадки прояву таких злочинів у незалежній Україні, акцентується увага на сучасній небезпеці цих злочинів. Аналізується сучасний український досвід боротьби із ними.

Ключові слова: поняття злочину, злочини у сфері комп'ютерної безпеки.

Поява в ХХ столітті різних досягнень науки і техніки, таких як: засоби комунікації, телеграф, телефон, радіо, кіно, телебачення, комп'ютер, неминуче тягне за собою і інший процес: багато з різних досягнень науки стали прийматися на озброєння злочинного світу. Проте впровадження в усі сфери людської діяльності комп'ютерної техніки зіграло найбільшу істотну роль у справі технічного озброєння злочинності. Навіть за неповними оцінками експертів, комп'ютерні злочини обходяться мінімум в 200 млрд доларів щорічно. Банківський грабіжник ризикує життям за 10 тис. доларів, електронний, маніпулюючи комп'ютером і нічим не ризикуючи, може отримати 1 млн [1, 3].

В цілому, комп'ютерна злочинність з'явилася порівняно недавно: вперше комп'ютерний злочин було зафіксовано в США в 1966 році. Однак питання про створення комп'ютерної безпеки було поставлено на порядок денний трохи більше десяти років тому, після того, як студент Корнельського університету зумів потрапити в комп'ютерні системи американської розвідки, міністерства оборони та відключив в цих системах кілька тисяч комп'ютерів. Тоді і були зроблені перші заходи протидії: при університеті Карнегі Меллон у Піттсбурзі на кошти Пентагону була створена комп'ютерна група швидкого реагування — CERT (Computer Emergency Response Team), призначена для реєстрації великих «зломів» комп'ютерних мереж і надання допомоги в «латації» дірок, пророблених злочинцями [2].

Суспільна небезпека комп'ютерних злочинів викликана наступними причинами:

— такі злочини ще недостатньо широко відомі, оскільки вони з'явилися наприкінці 60-х років, а звернули на себе увагу і зовсім недавно, на початку 90-х;

— їх складно виявити (іноді навіть постраждалому), оскільки сучасні засоби їх виявлення малоєфективні. Приміром, в експерименті по проникненню в свою ж комп'ютерну мережу, проведенню однієї з американських урядових організацій, з усіх успішних «зломів» вдалося виявити лише 4 %. Мало того, навіть наявні засоби виявлення спроб злому використовуються дуже рідко. Так, за даними одного з опитувань, понад 70 % користувачів мереж у США не мають пристройів, що попереджають про вторгнення в їх комунікаційні та інформаційні системи;

— комп'ютерним злочинам складно запобігти, оскільки засоби і методи захисту постійно відстають від засобів і методів нападу. Причому інформація про останні,

а також програмні продукти для їх реалізації вільно поширяються в Інтернеті, що розшириє коло потенційних злочинців і дозволяє істотно знизити вимоги до рівня їх спеціальних знань;

– комп’ютерні злочини вчиняються в глобальному масштабі, злочинці діють на великій відстані, простежити їх складно, оскільки вони часто прикриваються чужим ім’ям, і слід їх, якщо такий залишається, надзвичайно заплутаний;

– комп’ютерна злочинність приймає організований характер;

– покарати виявленого злочинця не завжди можливо: користуючись неузгодженістю правових баз різних держав, злочинець може здійснювати «зломи» з країни, де подібна діяльність не є протизаконною;

– нейтралізувати наслідки комп’ютерних злочинів надзвичайно складно [3, 40].

Наприклад, у 1995 році агенти ФБР заарештували молодого американця Кевіна Мітника. Його охрестили найнебезпечнішим хакером в світі за те, що він зламав системи захисту комп’ютерних мереж більше десятка відомих компаній. У цей список входять «Моторола», «Фуджіцу», «Ейр тач», «Пасифік bell» і безліч інших. Мітник першим розкрив деякі з хакерських секретів правоохоронним і законодавчим органам США. Його діяльність змусила сенат терміново внести зміни до законодавства про захист авторських прав. До речі, Кевін стверджував, що найслабшою ланкою в будь-якої комп’ютерної системи є ... людина. Він розповідав, що часто користувався простим трюком: дзвонив в яку-небудь компанію, представлявся одним з її співробітників і просив «колег» нагадати йому пароль, що відкриває доступ до мережі. Трюк спрацьовував майже завжди! Мітника засудили до п’яти років тюремного ув’язнення. Він вийшов на волю в січні 2000 року. Проте американська влада так боялася Кевіна, що заборонила йому користуватися будь-якими видами комп’ютерів та іншими засобами комунікацій, крім звичайного телефону. Хакер так і не визнав себе винним. Він щоразу підкреслював ту обставину, що нічого не вкрав. «Я міг би стати мільйонером, скористайся в корисливих цілях отриманою інформацією, зламуючи комп’ютерні мережі! Але я робив це лише заради розваги ...» — затверджує і сьогодні Мітник. Йому дозволили знову сісти за комп’ютер в січні нинішнього року. Кевін заснував консалтингову компанію і розмістив в Інтернеті її сайт. Через кілька днів його кілька разів зламали інші хакери! Вони визнали за честь подолати систему безпеки, створену самим Кевіном Мітником.

Однак далеко не всі хакери настільки ж безкорисливі, як містер Мітник. У 1998 році в штаті Флорида росіянин Володимир Левін зламав комп’ютерну мережу «Сітібанку» і вкрав з рахунків клієнтів 12 мільйонів доларів. ФБР вдалося його заарештувати. Після цього випадку федерали стали все частіше звертати увагу на хакерів з колишніх радянських республік. Виявилося, що саме вони завдають найбільшої шкоди американським компаніям [4,10].

Це відчувається незважаючи на те, що на території колишнього Радянського Союзу злочини у сфері комп’ютерних технологій виникли трохи пізніше. Вважається, що перший злочин у сфері високих інформаційних технологій було скоміюто у 1979 році у Вільнюсі. Збитки державі тоді склали 80 тисяч рублів — на ці гроші можна було придбати 8 автомобілів «Волга» [5].

У 1983 р. на автомобільному заводі в Тольятті «ВАЗ» був викритий програміст, який з помсті до керівництва підприємства умисно внес зміни в програму ЕОМ, що керувала подачею деталей на конвеєр. В результаті події збою заводу було завдано істотної матеріальної шкоди: не зійшли з конвеєра понад сотні автомобілів. Програміст був притягнутий до кримінальної відповідальності. Справа дійшла до суду. Підсудний звинувачувався за ст. 98 ч. 2 Кримінального кодексу РРФСР «Умисне знищення або пошкодження державного чи громадського майна».

При цьому обвинувачуваний стверджував, що нічого натурально пошкоджено не було — порушенім виявився лише порядок роботи, тобто дії, які не підпадають

ні під одну статтю чинного на той час законодавства. З наукової точки зору цікавий вирок суду: «... три роки позбавлення волі умовно; стягнення суми, виплаченої робітникам за час вимушеної простою головного конвеєра; переведення на посаду складальника головного конвеєра ...» [6, 17].

Перші корисні злочини з використанням комп'ютерної техніки в Росії з'явилися в 1991 р., коли були викрадені 125,5 тис. доларів США у Зовнішекономбанку СРСР. Весь світ облетіла інформація про кримінальну справу за обвинуваченням Левіна та інших осіб, які вчинили розкрадання грошей з банківських рахунків на великий відстані з використанням ЕОМ [7].

Цей процес не минув і Україну, державні та приватні установи, якої отримали доступ до мережі Інтернет, у тому числі до міжнародних платіжних систем, де рівень злочинності з використанням комп'ютерів досить високий. Хоча в Україні комп'ютерна злочинність ще не набула значних масштабів, оскільки, серед населення України доступ до Інтернету мають лише жителі міст з розвинutoю інфраструктурою, так по даним на 2010 рік, лише 1/3 всіх українців користується мережею Інтернет [8], але її прояви вже зафіксовані. Також рівень забезпеченості наших державних та приватних установ значно нижче, порівняно з розвинutoю Європою та США. Тому не дивно, що українські хакери-злочинці зазіхались у першу чергу на власність громадян та установ США та Європи.

Так, 21 травня в Бангкоку (Тайланд) місцева поліція за підтримки агентів американських спецслужб заарештувала 25-річного громадянина України Максима Ковальчука. Йому було пред'явлено цілу низку серйозних звинувачень: злом сайтів провідних комп'ютерних компаній, незаконні операції з відмивання трьох мільйонів доларів, отриманих від продажу контрафактних дисків з банківськими програмами, і ще більше десяти фінансових злочинів. Арешт відбувся в кафе, розташованому в одному з універмагів Бангкока. Ковальчук опору не чинив. При ньому були знайдені піратські копії комп'ютерних програм від виробників зі світовим ім'ям, — «Майкрософт», «Автодеск», «Едоб», «Макромедіа». На деяких підробках були фірмові написи і етикетки. Як стверджують представники тайської поліції, приблизна вартість вилученої у Ковальчука піратської продукції становить 3 мільйони доларів. Американські правоохоронні органи оголосили Максима Ковальчука в розшук ще в 2000 році — після великої афери в Північній Каліфорнії. Прокуратура США стверджує, що Ковальчук використовував Інтернет-аукціон eBay для обману величезної кількості громадян США та інших країн. Жертви українського хакера платили гроші за товари, які так ніколи і не отримали. Керівництво eBay було змушене звернутися до спецвідділу поліції Сан-Франциско, що займається комп'ютерними злочинами. Після цього встановили, що Ковальчук зумів зламати комп'ютерні системи «Майкрософт» і «Едоб». Американці підрахували, що своєю незаконною діяльністю хакер з України завдав компаніям збитків у розмірі більше 100 мільйонів доларів, і його ім'я включили до списку найбільш небезпечних хакерів в світі.

1 травня влада Таїланду, за вимогою США, приступила до широкомасштабної кампанії з боротьби з комп'ютерним піратством і хакерами. Так уже збіглося, що Максим та його дружина приїхали до Бангкока в самий розпал цієї операції. Причому Ковальчук прибув під чужим прізвищем. Тайська влада стверджує, що в паспорти, з яким він перетнув кордон, значиться прізвище Височанський. Максим поки заперечує всі пред'явлені йому звинувачення. США вимагають його видачі. Якщо екстрадиція відбудеться, то Максима будуть судити в Америці. Йому загрожує тюремне ув'язнення терміном до 20 років і штраф у розмірі 500 тисяч доларів.

У 2000 році 21-річного студента Київського державного лінгвістичного університету Максима Попова з Житомира запросила на стажування лондонська фірма. А вже в травні наступного року Максим опинився в США в американській в'язниці поблизу міста Сент-Луїс (штат Міссурі). Попова звинуватили у зломі даних банку «Вестерн Юніон» і вимаганні 50 тисяч доларів.

16–20 листопада 2001 р. зазнала вірусної атаки обчислювальна мережа Генеральної дирекції ВАТ «Укртелеком», яка налічує понад 700 комп’ютерів та десятки серверів. Як наслідок — це спричинило тимчасове відключення комп’ютерів від Інтернету, а також виведення з ладу системи корпоративної електронної пошти. Збитки від атаки становили понад 1 млн грн [9]. Резонансні справи стосуються та-ж фінансово-банківської системи [10]. Тенденція зростання цього виду злочинів в Україні повторює світову — щорічне збільшення у 2–3 рази (тільки у 2002 р., за даними Департаменту інформаційних технологій МВС України, виявлено 681 злочин, вчинений у сфері високих технологій).

Тому реалії сьогодення вимагають активного формування відповідних підрозділів у МВС, СБУ, ДПА України. Наприклад, створення у 2001 р. Управління по боротьбі зі злочинами у сфері високих технологій МВС України уможливило викриття злочинів та порушення кримінальних справ щорічно у декілька разів більше, ніж за всі попередні роки з моменту введення кримінальної відповідальності за них (1994 р.) [11, 121]. Але діяльність цих підрозділів потребує координації з боку спеціально створеного органу, адже кіберзлочини стосуються і неправомірного доступу до таємної інформації, і крадіжок коштів з пластикових карток та електронних рахунків банків, і ухилення від сплати податків, а також — використання електронних засобів терористами.

Виходячи з актуальності зазначеного питання для України, у МНДЦ з проблем боротьби з організованою злочинністю при Координаційному комітеті при Президентові України за останні роки накопичено досвід щодо дослідження наведених проблем. Так, за результатами дослідження науковцями МНДЦ підготовлено проект Концепції стратегії реалізації державної політики щодо боротьби з кіберзлочинністю. Рішенням Урядової комісії з питань аналітичного забезпечення органів виконавчої влади 6 жовтня 2000 р. прийнято за основу проект Концепції реформування законодавства України у сфері суспільних інформаційних відносин. Основні положення названих документів викладено у аналітичних довідках, доповідних, Стратегії та рекомендаціях щодо тактики боротьби з організованою злочинністю і корупцією тощо, які надіслані до Координаційного комітету по боротьбі з корупцією і організованою злочинністю. З метою ефективної протидії кіберзлочинності Указом Президента України «Про рішення Ради національної безпеки і оборони України від 31 жовтня 2001 р. «Про заходи щодо вдосконалення державної інформаційної політики та забезпечення інформаційної безпеки України» № 193/2001 від 6 грудня 2001 р. передбачено створення Міжвідомчого центру з питань боротьби з комп’ютерною злочинністю (далі — МЦПБКЗ). Підтримуючи пропозицію Кабінету Міністрів України щодо його відкриття, вважаю за необхідне зазначений підрозділ створити у структурі Координаційного комітету по боротьбі з корупцією і організованою злочинністю, який відповідно до ст. 8 Закону «Про організаційно-правові основи боротьби з організованою злочинністю» від 30 червня 1993 р. координує діяльність всіх державних органів, що здійснюють боротьбу з організованою злочинністю, у тому числі з комп’ютерною. Наукове, аналітичне та інформаційне забезпечення слід покласти на Міжвідомчий НДЦ з проблем боротьби з організованою злочинністю за умови відповідного штатного та фінансового забезпечення.

У зв’язку із зазначеним варто ще раз звернутися до практики функціонування відповідного Центру у Великобританії. На нього покладено виконання таких завдань: діяльність проти організованої злочинності у сфері високих технологій і транснаціонального характеру; проведення стратегічних прогнозів; проведення розслідувань; координація діяльності правоохоронних органів; розроблення рекомендацій для правоохоронних органів. До Центру входять чотири відділи: розслідування — проводить розслідування та підтримує інші правоохоронні органи у розслідуванні тяжких та вчинених організованими групами злочинів з викорис-

танням високих технологій; розвідки — забезпечує стратегічну і тактичну розвідку та співробітництво із зарубіжними партнерами; тактичної і технічної підтримки — забезпечує консультативну підтримку та допомогу місцевим правоохоронним агентствам, міжнародним правоохоронним організаціям, уряду і промисловості; цифрових доказів — забезпечує судову підтримку при розгляді злочинів у сфері високих технологій. І, врешті-решт, необхідно зазначити, 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 р. економічні збитки від них збільшаться у 10—100 разів [12]. Це змушує і уряд США, і Європейське Спітвовариство терміново вжити відповідних заходів як на законодавчому, так і організаційному рівнях. Зокрема, урядом США нещодавно прийнята нова Стратегія щодо захисту інформаційних систем у Інтернеті (бюджетом планується виділення близько 60 млрд дол.), у 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, яка згідно з Конституцією є невід'ємною складовою національної безпеки нашої держави.

Література

1. Проблемы развития цифровых информационных технологий в органах внутренних дел // Компьютерные технологии в криминалистике и информационная безопасность. Труды академии МВД РФ. — М., 1997. — С. 3.
2. Иксар В. Компьютерные преступления [електронний ресурс]. — Режим доступу до документа: <http://www.comprice.ru/articles/detail.php?ID=42319>
3. Крылов В. В. Расследование преступлений в сфере информации. — М.: Издательство «Городец», 1998. — С. 264.
4. Козлов И., Карнаухов С. Америка требует выдачи арестованного в Бангкоке 25-летнего жителя Тернополя // Факты и Комментарии. — 31-Май-2003. — С. 10.
5. Карпинский О. Защита информации, виртуальные частные сети (VPN). Технология ViPNet / По материалам компании Infotechs // Gazeta.Ru. — 2001. — 18 июня.
6. Наумов В. Отечественное законодательство в борьбе с компьютерными преступлениями // Computer World Россия. — 1997. — № 8. — С. 17–18.
7. Сайтарлы Т. Россия: статистика компьютерной преступности [електронний ресурс]. — Режим доступу до документа: <http://www.crime-research.ru/news/12.03.2004/2004-03-1202/>
8. За даними маркетингової дослідженувальної компанії InMind, [електронний ресурс]. — Режим доступу до документа: <http://itnews.com.ua/analytics/277.html>
9. Хроніка вірусної атаки на Укртелеком, [електронний ресурс]. — Режим доступу до документа: <http://www.ukrtel.net>
10. Гуцалюк М. Безпека банківських інформаційних систем // Страхова справа. — 2002. — № 2(6). — С. 68–70.
11. Гуцалюк М. Координація боротьби з комп'ютерною злочинністю // Право України. — 2002. — № 5. — С. 121–126.
12. Інтерпол, [електронний ресурс]. — Режим доступу до документа: <http://www.interpol-assembly2001.com>

B. П. Беленький, аспирант

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

СОВРЕМЕННАЯ ИСТОРИЯ ПРЕСТУПЛЕНИЙ В СФЕРЕ КОМПЬЮТЕРНОЙ БЕЗОПАСНОСТИ

РЕЗЮМЕ

Статья посвящена истории компьютерных преступлений. Автор приходит к выводу, что преступления в сфере информационных технологий очень часто являются международными, то есть преступники действуют в одном государстве, а их жертвы находятся в другом государстве. Поэтому для борьбы с такими преступлениями особое значение имеет международное сотрудничество.

Ключевые слова: компьютерные преступления, компьютерная безопасность.