УДК 343:681.302

Г. УСАТИЙ, *кандидат юридичних наук, доцент,*
Національний університет ДПС України

КРИМІНОГЕННА СИТУАЦІЯ У СФЕРІ ЕЛЕКТРОННОГО БАНКІНГУ

Анотація. *Щодо аналізу негативних тенденції та потреби у створенні національної системи кримінально-правового забезпечення ефективної протидії злочинам у сфері електронного банкінгу.*

Аналіз стану криміногенної ситуації у сфері електронного банкінгу* в Україні свідчить про тісний зв'язок злочинності і її залежності від зростання кількості комп’ютерів, підключених до мережі Інтернет. При цьому, чим більшою є комп’ютеризація сучасного суспільства і, відповідно, питома вага осіб, що мають доступ до глобальної інформаційної мережі, тим більшим є ризик негативного впливу комп’ютерної злочинності на сферу електронного банкінгу.

Серед факторів та обставин, які обумовлюють сучасний стан та тенденції злочинності у сфері електронного банкінгу, можна (з певною часткою умовності) виділити наступні.

По-перше, вразливість комп’ютерних систем (у т. ч. електронних платіжних систем). Сюди можна віднести умисні помилки чи помилки з необережності при розробці програмного забезпечення фінансових установ, а також недостатню активність банків з розробки та забезпечення відповідних заходів по запобіганню зовнішнім атакам та внутрішнім посяганням з боку власних працівників.

По-друге, унікальні особливості кіберпростору надають зловмиснику можливість анонімних дій, адже фактично особа, що вчиняє злочин, знаходиться в реальному світі, а злочинною діяльністю займається у віртуальному. Таким чином, “електронні” сліди злочину вітчизняним правоохоронцям надзвичайно складно виявити, зафіксувати та використати у перспективі в межах досудового слідства.

По-третє, просторовий фактор. Адже нерідко комп’ютерного злочинця і жертву розділяють значні відстані, які не обмежуються кордонами однієї держави. Так, наприклад, злочинець може спочатку зайти у мережу з комп’ютера “I” (Україна) і через комп’ютер “II” Інтернет-провайдера, що розміщений у Російській Федерації, заподіяти майнову шкоду або заволодіти майном шляхом незаконного міжбанківського переказу з комп’ютера “III” (США).

По-четверте, надзвичайно високий рівень латентності злочинів у сфері електронного банкінгу. Так, за інформацією Української міжбанківської асоціації членів Europay International “ЕМА”, яка виступає профільною міжбанківською установою та координує спільні заходи щодо запобігання неправомірному використанню карток, загальний обсяг шахрайських операцій перевищив в Україні 500.000 доларів США у 2001 році та 1.000.000 доларів США у 2002 р. Це 1 % загального легального обігу карткових операцій, хоча середньоєвропейське значення – 0,3 % обігу. Але офіційні дані банківських структур та самих платіжних систем на декілька порядків нижчі [1].

* Від ред.: електронний банкінг – це система дистанційного банківського обслуговування клієнта (проведення фінансових операцій (платежів) за допомогою телекомунікаційних каналів (PC-банкінг) і засобів Інтернету (Інтернет-банкінг).

По-п’яте, цьому також сприяє закритість (непрозорість) банківської системи, що дозволяє службовим особам, а інколи навіть і рядовим співробітникам банків вчиняти суттєві зловживання. Керівники кредитних установ (особливо вищої ланки) непідконтрольні практично нікому, окрім засновників банку.

На заваді правоохоронним і контролюючим органам України при проведенні документальних перевірок та ревізій постає правовий інститут банківської (чи комерційної) таємниці. Саме тому можна зрозуміти, чому різноманітні розкрадання у сфері електронного банкінгу вчиняються злочинцями переважно з використанням свого службового становища. Разом з тим, у рекомендаціях ООН з питань формування міжбанківської служби безпеки зазначається, що “для банків життєво важливим є створення механізму ідентифікації особи своїх клієнтів і надання сприяння правоохоронним органам у випадках, коли виникають підозри стосовно тих чи інших вкладів чи операцій. При цьому також необхідне зміцнення механізмів контролю над банківськими операціями і, можливо, навіть централізація такого роду інформації. Державам необхідно заохочувати банки, брати на себе якомога більшу відповідальність за подібний контроль з метою боротьби зі злочинністю” [2].

По-шосте, недоліки у нормативній базі з урегулювання взаємовідносин між господарюючими суб’єктами, у тому числі між банками і їх клієнтами. Відсутність нормативних актів (або їх неналежна якість), що регламентують окремі напрями сфери електронного банкінгу, підсилюється суперечливістю і нечіткістю багатьох законів, інструкцій та розпоряджень, що прийняті поспіхом, без глибинного опрацювання і розуміння сутності проблеми. Так, останніми роками поширеними стають схеми отримання грошових коштів у сфері електронного банкінгу з використанням фіктивних договорів, коли протизаконній діяльності надається формально законний вигляд, що ускладнює втручання та своєчасне реагування на такі факти правоохоронних органів (оскільки взаємовідносини сторін ззовні мають цивільно-правовий чи господарсько-правовий зміст).

Недосконалим, на жаль, у вищезазначеному сенсі є також вітчизняне кримінальне законодавство, яке має суттєві вади та прогалини у забезпеченні ефективної протидії злочинам у сфері електронного банкінгу. Так, ще у 1999 р. Асоціація банків-членів EUROPAY International розробила законопроект, який містив описання складів злочинів у сфері використання банківських платіжних карток. Пропонувалося передбачити покарання за такі діяння: неправомірне використання банківської платіжної картки, її номера, персонального ідентифікаційного коду з метою незаконного отримання доходу або привласнення майна; умисне використання банківської платіжної картки з метою збільшити кредиторську заборгованість, яку особа неспроможна погасити; виготовлення підроблених банківських платіжних карток, їх збут або використання; залучення іншої особи до прийому справжніх або підроблених платіжних карток під час оплати товарів чи послуг з метою незаконного одержання доходу; прийом справжніх або підроблених платіжних карток у рахунок оплати товарів або послуг, якщо особа, яка здійснює такий прийом, знає або підозрює, що картка є підробленою або отримана злочинним шляхом; виготовлення або зберігання інструментів для підробки або копіювання банківських платіжних карток. Під такими інструментами пропонувалось розуміти будь-які матеріали, за допомогою яких можна здійснити штампування, кодування або друкування на платіжних картках [3].

Як бачимо, ухвалюючи Кримінальний кодекс 2001 року, законодавець не сприйняв хоч і не позбавлений недоліків, проте комплексний підхід банкірів у питанні кримінально-правового захисту сфери обігу платіжних карток і обмежився

встановленням кримінальної відповідальності лише за підробку таких платіжних інструментів та за деякі дії з ними.

Серед інших умов, що сприяють вчиненню злочинів у сфері електронного банкінгу, російський правник Астапкіна С.М. [4] виділяє наступні:

а) недостатню взаємодію банківських структур і правоохоронних органів. З одного боку, банки зацікавлені, по-перше, не виносити “бруд з хати” (у даному контексті – інформацію про вчинені проти них “пластикові злочини”) з метою запобігання антирекламі і, по-друге, залучати нову клієнтуру будь-якою ціною (у т. ч. і без достатньої її перевірки), з іншого боку – працівники правоохоронних органів нерідко недооцінюють небезпеку даного виду злочинів і навіть не завжди вносять викрадені картки у списки номерних викрадених речей (тому вони, наприклад, не завжди потрапляють у поле зору працівників міліції при обшуку осіб, затриманих за інші правопорушення);

б) халатне ставлення деяких співробітників банків до збереження службової інформації, а також недбале зберігання чи пересилання пластикових платіжних засобів, бланків суворої звітності, наприклад, сліпів (не говорячи вже про умисне співробітництво зі злочинцями);

в) недоліки в організації роботи торговельних підприємств, що приймають до оплати пластикові картки (наприклад, для економії часу на авторизацію касири нерідко розбивають суму покупки на декілька рахунків, кожен з яких не перевищує ліміту, який не потребує авторизації, стаючи фактично спільниками злочинців);

г) економія на засобах захисту пластикових карток;

г') несвоєчасне і неповне використання стоп-листів з метою попередження шахрайства з картками. Затримки у внесенні втраченої чи викраденої картки до списку заборонених до прийому карток (стоп-лист), а також обмежена територіальність дії стоп-листів (з метою економії) дозволять злочинцям використовувати викрадені чи фальшиві (підроблені) картки тривалий час.

Розглядаючи криміногенну ситуацію у сфері електронного банкінгу, не можна оминути увагою відповідні види (класифікацію) злочинів.

Так, виходячи з вищезазначеного можна виділити найпоширеніші види комп’ютерних злочинів:

- несанкціонований доступ;
- пошкодження комп’ютерних даних;
- комп’ютерний саботаж;
- комп’ютерне розкрадання;
- комп’ютерне шахрайство;
- комп’ютерний підлог (підроблення).

Враховуючи специфіку злочинних посягань у сфері електронного банкінгу, доцільним, на нашу думку, вбачається описання у межах статті наступних його видів:

Комп'ютерне розкрадання. Даний вид злочину включає в себе незаконне привласнення чужої інформації, у т. ч. несанкціоноване перехоплення без дозволу і з використанням технічних засобів повідомлень, які надходять в комп'ютерну систему або мережу, що витікають з комп’ютерної системи або мережі або циркулюють у рамках такої системи або мережі.

Предметом даного злочинного посягання є комп’ютерна інформація, яка може включати конфіденційні відомості про її власника, банківські вклади, номери рахунків, кредитних карток і т. д.

Концептуально крадіжка у фізичному світі не відрізняється від крадіжки у віртуальному просторі. Відмінність полягає лише у тому, що власність в останньому

випадку носить віртуальний характер [5]. Особа здійснює злочин, якщо обертає майно у своє володіння або здійснює незаконний контроль над власністю іншого.

Одному з останніх злочинних діянь подібного роду було надано широкого розголосу (резонансу) у зв'язку з арештом у США двох російських громадян-мешканців м. Челябінська О. Іванова і З. Горшкова, які, за даними ФБР США, впродовж 1999-2001 рр. використовуючи персональні комп’ютери, що знаходяться у Челябінську, шляхом сканування здійснювали в Інтернеті пошук компаній, що використовують уразливе з точки зору захисту програмне забезпечення. Виявляючи такі, вони проникали в комп’ютерні системи і брали їх під свій контроль, “викачуючи” всю необхідну інформацію про клієнтів. В окремих випадках вони входили в контакт з компанією – власником інформації, представляючись членами “групи експертів по захисту від хакерів”, і повідомляли, що їм вдалося проникнути у комп'ютери компанії. Потім вони пропонували за плату усунути недоліки і підвищити безпеку комп'ютерної системи [6].

У ФБР США вважають [7], що заарештовані мають відношення до сотень злочинів, зокрема до справи про розкрадання 15700 номерів кредитних карт компанії з виконання грошових переказів “Western Union” (Денвер, США). У вересні 2000 року та 17 травня 2001 р. у справі відбулися судові слухання. У жовтні 2001 р. Горшков визнаний судом винним за 20 пунктами висунутого проти нього обвинувачення.

Поширеними є випадки, коли злочинець копіює інформацію і забирає копію, залишаючи оригінальну версію законному власникові. У цих випадках жертва часто навіть не знає про злочин, що відбувся. Проте їй заподіяна шкода, яка залежить від характеру власності і, відповідно, кваліфікуватиметься, наприклад, як порушення авторських прав.

Деякі фахівці виділяють окремий вид комп'ютерної крадіжки – крадіжку комп'ютерних послуг. Наприклад, у традиційному сенсі згідно з § 223.7 Типового кримінального кодексу США особа здійснює крадіжку послуг, якщо “шляхом обману або загрози або шляхом пред'явлення фальшивих знаків або інших засобів з метою уникнути платежу за послугу отримує послуги, які свідомо для неї можуть бути надані тільки за умови відшкодування” [8]. У фізичному світі це може бути праця, професійна послуга, перевезення, послуги з телефонного зв'язку, обслуговування в готелі, ресторані, допуск на виставки, користування транспортом або іншим рухомим майном. У віртуальному світі можна вкрасти час користування мережею Інтернет, комп'ютерний час. Правопорушник, у якого немає законного права на використання послуг і який діє з метою позбавлення законного власника власності, таким чином позбавляє жертву цієї власності.

Основними прийомами вчинення злочинів при цьому, на думку Н. Ахтирської [9], можуть бути наступні:

- вилучення засобів обчислювальної техніки, яке здійснюється з метою отримання системних блоків, окремих вінчестерів чи інших носіїв інформації, що містять у пам’яті установчі данні про клієнтів, вкладників, кредиторів банку. Такі дії можуть здійснюватись шляхом викрадення і самі по собі містять склад злочину звичайних, “некомп’ютерних” злочинів;
- перехоплення (негласне отримання) інформації служить для отримання певних відомостей про клієнтів, вкладників, кредиторів банку. Воно може здійснюватися з використанням методів і апаратури аудіо-, візуального і електромагнітного спостереження. Об'єктами, як правило, є канали зв'язку, телекомунікаційне устаткування, службові приміщення для проведення конфіденційних переговорів, паперові і магнітні носії (у тому числі і технологічні відходи);

• несанкціонований доступ до засобів обчислювальної техніки, тобто активні дії по створенню можливості розпоряджатися інформацією без згоди власника, що здійснюється з використанням наступних основних прийомів:

1) “за дурнем” – фізичне проникнення у виробничі приміщення. Зловмисник чекає у закритого приміщення, тримаючи в руках предмети, пов'язані з роботою на комп'ютерній техніці (елементи маскування), поки не з'явиться хто-небудь, що має легальний доступ до нього, потім залишається тільки увійти всередину разом з ним або попросити його допомогти занести нібито необхідні для роботи на комп'ютері предмети.

Інший варіант – електронне проникнення у засоби обчислювальної техніки – підключення додаткового комп'ютерного терміналу до каналів зв'язку з використанням шлейфу “шнурка” у той момент часу, коли законний користувач короткочасно покидає своє робоче місце, залишаючи свій термінал або персональний комп'ютер в активному режимі;

2) “за хвіст” – зловмисник підключається до лінії зв'язку законного користувача і терпляче чекає сигналу, що позначає кінець роботи, перехоплює його на себе, а потім, коли законний користувач закінчує активний режим, здійснює доступ до банківської системи; подібними властивостями володіють телефонні апарати з функцією утримання номера, що викликається абонентом;

3) “комп'ютерний абордаж” – зловмисник вручну або з використанням автоматичної програми підбирає код (пароль) доступу до банківської системи з використанням звичайного телефонного апарату;

4) “неспішний вибір” – зловмисник вивчає і досліджує систему захисту, використовувану у банківській комп'ютерній системі, її слабкі місця, виявляє ділянки, що мають помилки або невдалу логіку програмної будови, розриви програми (пролом, люк), і вводить додаткові програми, що вирішують доступ;

5) “маскарад” – зловмисник проникає в банківську комп'ютерну систему, видаючи себе за законного користувача із застосуванням його кодів (паролів) та інших ідентифікуючих шифрів;

6) “містифікація” – зловмисник створює умови, коли законний користувач банківської системи здійснює зв'язок з нелегальним терміналом, будучи абсолютно упевненим у тому, що він працює з потрібним йому законним абонентом. Формуючи правдоподібні відповіді на запити законного користувача і підтримуючи його помилки якийсь час, зловмисник здобуває коди (паролі) доступу або відгук на пароль;

7) “аварійний” – зловмисник створює умови для виникнення збоїв або інших відхилень у роботі засобів обчислювальної техніки банківської комп'ютерної системи. При цьому включається особлива програма, що дозволяє в аварійному режимі діставати доступ до найбільш цінних даних. У цьому режимі можливе “відключення” всіх наявних у банківській комп'ютерній системі засобів захисту інформації, що полегшує доступ до них зловмисника.

Комп'ютерне шахрайство. Відповідно до рекомендацій Ради Європи даний злочин включає введення, зміну, стирання або поглинання комп’ютерних даних чи комп'ютерних програм або інше втручання у процес обробки даних, що завдає іншій особі економічного збитку або веде до втрати її майна, з метою отримання незаконної економічної вигоди для себе або на користь іншої особи. Аналізуючи даний вид злочину у сфері комп'ютерної інформації, слід відокремлювати його від шахрайства, здійсненого з використанням комп'ютера як інструменту, а інформаційного простору – як середовища скоєння злочину.

Здійснюючи комп’ютерне шахрайство, правопорушник несанкціоновано або з дозволу втручається у процес належного функціонування обробки даних комп'ютером таким чином, що це призводить до наслідків, що підпадають під визначення шахрайства.

Так, згідно з § 263а Кримінального кодексу ФРН під комп'ютерним шахрайством розуміється діяння, що полягає у завданні шкоди чужому майну через дію на результат обробки даних шляхом неправильного створення програм, використання неправильних даних або неправомочного використання даних чи іншого впливу на результат обробки даних з наміром отримати для себе або третьої особи майнову користь [10].

В одному з відомих випадків у 1997 – 1998 рр. громадянин Ш., знаходячись за місцем свого проживання, за допомогою програми згенерував номер кредитної картки платіжної системи VISA. Знаючи адресу електронного магазину “PC Teach” в Інтернеті, він провів замовлення різних товарів на суму понад 20 тисяч доларів США, ввівши магазин в оману відносно своєї платоспроможності шляхом надання відомостей про номер кредитної картки [11], що був згенерований ним.

Широко поширені схеми обману людей за допомогою таких електронних звернень або повідомлень через Інтернет, як пропозиції про продаж акцій за привабливою ціною; інвестиції у нерухомість в іноземній державі; надання позик на умовах, що забезпечують винятково високу норму прибутку; передоплата недостатньо ретельно охарактеризованих товарів або запрошення приєднатися до фінансової піраміди. Комп'ютер у таких випадках використовується як допоміжний інструмент для скоєння злочину, а віртуальне середовище є альтернативою фізичного світу, в якому також можна здійснити аналогічні операції. Правопорушник використовує Інтернет або будь-яку іншу мережу, щоб спілкуватися з потенційними жертвами не безпосередньо, а віртуально, свідомо убезпечивши себе, приховавши свою особу. Спілкування може відбуватися за допомогою веб-сайтів або електронної пошти. Шахраї переконують переслати грошові кошти на їх адресу в обмін на послуги, які вони ніколи не нададуть.

У останньому випадку це не комп'ютерне, а традиційне шахрайство, де комп'ютер – тільки інструмент для скоєння злочину, оскільки немає безпосередніх маніпуляцій з комп'ютерною інформацією. В цьому випадку повинні застосовуватися традиційні норми, що стосуються шахрайства.

На основі узагальнення і аналізу судово-слідчої практики способи здійснення шахрайства з платіжними картками представляється доцільним класифікувати на п'ять основних груп [12]:

1. Способи шахрайства з використанням підробленої платіжної картки. При скоєнні злочинів можливо використання як підроблених платіжних карток (матеріальна підробка), так і платіжних карток, належно виготовлених, але які містять помилкові відомості (інтелектуальне підроблення). Виготовленням підроблених платіжних карток визнається як їх повне відтворення, так і часткова підробка (наприклад, зміна реквізитів – номери рахунку, підписи, перекодування інформації на магнітному носієві). Способи їх виготовлення такі: поліграфічний, репрографічний, анастатичний, малюванням і комбінований.

2. Способи шахрайства з використанням сліпів (квитанції електронного терміналу). Підроблені сліпи для здійснення злочину можуть бути отримані при виробництві несанкціонованих відбитків як із справжньої, так і з підробленої платіжних карток. Сліпи виготовляються шахраями за допомогою набірних друкарських форм або шляхом застосування підроблених кліше з використанням інформації із справжніх пластикових карток.

3. Способи шахрайства, реалізовані з використанням слабких місць технології обробки платежів за платіжними картками. Це способи, засновані на недосконалості каналів зв'язку між торговими точками і банками, а також на непрофесіоналізмі працівників торгівлі, що оформляють платежі по картці. У зв'язку з тим, що для скоєння злочинів вказаними способами необхідний значний обсяг знань, спеціальні технічні засоби, а сам процес здійснення розкрадання досить тривалий (час на розшифровку і перекодування інформації) і трудомісткий, випадки скоєння таких злочинів зустрічаються рідко.

4. Способи шахрайства з використанням справжньої платіжної картки, законно або незаконно отриманої злочинцями. Сюди можна віднести: овердрафт з шахрайським використанням платіжної картки, передачу картки шахраям її власником за певну винагороду, отримання платіжних карток у банках по викрадених документах з подальшим перевищенням ліміту кредитування, операції з краденою або втраченою карткою.

5. Способи шахрайства з використанням інформації про платіжну картку у сфері телекомунікацій. Найбільш латентний і небезпечний спосіб скоєння злочинів у сфері обороту платіжних карток – це скоєння злочинів через всесвітню мережу Інтернет. Проблема полягає у тому, що більшість співробітників СБУ і МВС, зокрема слідчих підрозділів, мають дуже узагальнене уявлення про комп'ютерні технології, навіть на рівні користувачів, тому їм складно використовувати у доведенні роздруківки з рядом IP-адрес. Крім того, несанкціоновані проникнення в комп'ютерні мережі можуть мати дуже обширну географію, і тому локалізувати місце скоєння злочину практично неможливо. Хакер, що знаходиться в Україні, може, наприклад, розплатитися з американським магазином платіжною карткою громадянина Італії, що відкрив рахунок в австралійському банку.

Комп'ютерний підлог (підроблення). Комп'ютерний підлог (підроблення) – це всілякі маніпуляції, що включають введення, зміну, стирання або поглинання комп'ютерних даних чи комп'ютерних програм з метою здійснення фальсифікації у класичному сенсі.

Коли питання не стосуються обробки комп'ютерних даних, як у випадку з підробкою, комп'ютер використовується як інструмент для зміни або створення фальшивого письмового або електронного документа. Об'єктивний бік злочину становить зміна, створення, доповнення, випуск, передача і збут фальшивих документів, записів, чеків, кредитних карток та інших предметів.

У зв'язку з цим слід підкреслити суміжність віртуальних і традиційних форм шахрайства і комп’ютерного підлогу (підроблення). Перший з них стосується декількох форм шахрайства у зв'язку з телекомунікаційними послугами. У таких випадках злочинець намагається отримати послуги без оплати за допомогою технічних маніпуляцій з пристроями або електронними елементами пристроїв. Така поведінка зазвичай криміналізується за допомогою конкретних кримінально-правових положень, проте у ряді випадків її можна віднести до категорії, відповідної класичним положенням, що характеризують шахрайство чи комп’ютерний підлог (підроблення). Друга група пов'язана із зловживанням платіжними документами. Злочинець, здійснюючи махінації з електронною банківською карткою або використовуючи підроблені картки чи помилкові коди, намагається отримати незаконну фінансову вигоду. Такі діяння можуть охоплюватися конкретними кримінально-правовими положеннями або класичними положеннями, що характеризують шахрайство і комп’ютерний підлог (підроблення), до яких можуть вноситися поправки.

В якості **висновків** можна зазначити наступне.

Проаналізовані негативні тенденції засвідчують, що вже зараз суспільство і держава відчувають нагальну потребу створення національної системи кримінально-правового забезпечення ефективної протидії злочинам у сфері електронного банкінгу, їх запобігання та криміналістичного захисту банківської (грошової) системи не лише від “традиційних” злочинних посягань у сфері власності, господарської діяльності тощо, але й від новітніх, вкрай складних та надзвичайно досконалих способів шахрайства, які безпосередньо пов’язані з науково-технічним прогресом у цій галузі (у т. ч. злочини з використанням пластикових карток).

Використана література

1. Бутузов В.М., Василинчук В.І., Шеломенцев В.П. Правові та організаційні засади протидії злочинам у сфері використання платіжних карток: навчальний посібник. – К.: Типографія ТОВ “СТ-Стиль”, 2006. – С. 45.

2. Практические меры борьбы с организованной преступностью : материалы семинара ООН. – Суздаль, 21-25 октября 1991. – С. 31.

3. Дудоров О.О. Злочини у сфері господарської діяльності: кримінально-правова характеристика: монографія. – К.: Юридична практика, 2003. – С. 78.

4. Астапкина С.М., Максимов С.В. Криминальные расчёты: уголовно-правовая охрана инвестиций. – М., 1995. – С. 80-82.

5. Brenner S.W. California Criminal Law Review. 2001, vol. 4.

6. Russian National Arrested and Indicted for Penetrating U.S. Corporate Computer Networks, Stealing Credit Card Numbers, and Extorting the Companies by Threatening to Damage Their Computers // Press Release for Immediate Release. U.S. Department of Justice, United States Attorney, District of Connecticut. 2001, May 7.

7. Садчиков А. Как ФБР устроило “подставу” хакерам Леше и Васе / Комсомольская правда. 2001, 24 мая; Георгиев В. Судебные слушания в Сиэтле по делу челябинских хакеров состоялись, но решение пока не оглашено / Урал-Пресс. 2001, 23 мая; Трудолюбов М. Хакеров выловили на приманку / Ведомости. 2001, 25 апреля; Куклев С. Агент Мадлер поймал хакера Иванова / Челябинский рабочий. 2001, 25 апреля.

8. Примерный уголовный кодекс США. – М.: Прогресс, 1969. – С. 153.

9. Ахтырская Н. Способы хищений в банковских информационно-вычислительных системах / Компьютерная преступность и кибертерроризм: сб. научных статей. – Запорожье, 2004. – Вып. 1. – С. 117.

10. Уголовный кодекс ФРГ ; [пер. с нем.]. – М.: Зерцало, 2000.

11. Кесарева Т.П. Криминальная паутина. Мошенничество в системе электронной торговли через Интернет / Интерпол в России, 2000. – № 3. – С. 26-27.

12. Реуцкий А.В. Способы совершения мошенничества с платёжными карточками / Відповідальність за злочини у сфері господарської діяльності: матер. НПК. – Х., 2006. – С. 197-198.

~~~~~~~~~~~~~ * * * ~~~~~~~~~~~~~
~~~~~~~~~~~~~