Ученые записки Таврического национального университета им. В.И. Вернадского
Серия «Юридические науки». Том 26 (65). 2013. № 1. С. 278-283.

УДК : 343. 451 : 343. 982. 3

ІНТЕРНЕТ-ШАХРАЙСТВО: РЕАЛІЇ СУЧАСНОСТІ ТА КРИМІНАЛІСТИЧНІ АСПЕКТИ ПРОТИДІЇ

Сабадаш В. П.

Запорізький національний університет, м. Запоріжжя, Україна

У статті розглядається сучасний стан та криміналістичні аспекти протидіїінтернет-шахрайству.Досліджуються статистичні дані щодо таких злочинних проявів у світі, вказуються способи інтернет-шахрайства, його характерні риси, зазначаються спеціальні організації, які займаються різними аспектами протидії інтернет-шахрайству, у тому числі і реєстрацією скарг на злочинні дії інтернет спрямування у різних державах світу, розкриваються основні напрямки протидії цьому злочинному діянню.

***Ключові слова*:** інтернет-шахрайство, злочин, способи, протидія, інформаційна безпека, сфера високих технологій.

Розвиток та інтенсивне впровадження сучасних інформаційних технологій в різних сферах життєдіяльності обумовлює зростання злочинних проявів в них, що представляє дуже серйозну загрозу як для економіки, так і для інформаційної безпеки держави, складової національної безпеки. Особливо це відчувається з приєднанням до міжнародних систем телекомунікації та підвищення інтелектуального рівня зловмисників, які через мережу Інтернет отримують доступ до комп'ютерної інформації. Високотехнологічні злочини набувають усе більш організованого, транснаціонального характеру [1, с. 106].

Проблема боротьби з високотехнологічним шахрайством особливо гостро стоїть в банківській сфері, телекомунікаціях, ритейлі, електронній торгівлі.

Кожна з організацій цих галузей регулярно зустрічається зі спробами незаконного одержання грошей, товарів або послуг шляхом використання уразливостей в автоматизованих системах або обману клієнтів і обслуговуючого персоналу. Крім постачальників послуг, від дій кібершахраїв страждають клієнти банків, платіжних систем, користувачі телефонних мереж і Інтернет, сервісів електронної й мобільної комерції. Окрему заклопотаність бізнес-співтовариства викликає проблема внутрішнього шахрайства й зловживань, яка приводить до істотних фінансових втрат компаній. Зростаючий збиток від дій зовнішніх і внутрішніх шахраїв створює погрозу розвитку нових перспективних секторів ринку електронних послуг, гальмує впровадження інновацій в економіку й державне управління.

Крім того, захоплення онлайн і мобільним банкінгом обходиться усе дорожче. За даними Української міжбанківської асоціації членів платіжних систем (ЕМА), кількість шахрайських дій в Україні із платіжними картками в Інтернеті за 2012 рік зросла втричі. Тільки внаслідок махінацій у системі "клієнтбанк" фінустановита їх клієнти втратили 116 млн. грн. 75% цих коштів вдалося повернути. Тобто чисті збитки склали порядком 30 млн. грн. У цілому, за статистичними даними Національно-

го банку України, загальна кількість шахрайських операцій з банківськими картами в 2012 році зросла в порівнянні з 2011 роком на 47 %, а обсяг втрат клієнтів - на 20 % [2].

За неповних 2 місяця 2013 року вже зафіксовано 23 випадки несанкціонованого списання коштів (12,5 мільйонів гривень) з рахунків підприємств у результаті втручання в роботу систем віддаленого обслуговування клієнтів. Правоохоронним органам, які тісно співпрацюють із Держфінмоніторингомта банками, вдалося розкрити 15 злочинів та повернути власникам майже 9,2 мільйони гривень [3].

Така ж ситуація і в Російській Федерації. Так, за даниминачальникаБюро спеціальних технічних заходів МВС РосіїО.М. Мошкова, які він оприлюднив на III Міжнароднійконференції «Борьба с мошенничеством в сфере высоких технологий. Профилактика и противодействие» (AntifraudRussia 2012) у листопаді 2012 року, за 9 місяців 2012 року в Росії кількість розкрадань коштів, зроблених з використанням комп'ютерних і телекомунікаційних технологій зросла на 60%. Лідером за темпами зросту є шахрайства з використанням банківських карт, тенденція до збільшення їх числа спостерігається у світі протягом декількох останніх років[4].

В 2012 році учасники британської багатогалузевоїантіфрод- асоціації CIFAS зафіксували близько 250 тис. випадків шахрайства - рекордне число, яке на 5% перевищило попередній показник.

Згідно зі статистикою CIFAS, половину випадків шахрайств на території Великобританії становить IdentityFraud - обман, що вчиняється від імені законного користувача або вигаданої особи. Кількість таких інцидентів у 2012 році збільшилась на 9%. Більш ніж у півтора рази зросло число випадків викрадення аккаунтів (Facility-TakeoverFraud) - здійснення незаконного доступу до облікового запису й використання його з метою вчинення шахрайських дій. Кількість жертв IdentityFraud і TakeoverFraud у сукупності збільшилась за рік на 24%[5].

Взагалі, згідно з оцінками експертів Євросоюзу, збиток від діяльності кіберзлочинців тільки у 2011 році склав 388 мільярдів доларів США. Жертвами зловмисників стали більш 430 мільйонів людей. Значна частина цих збитків була заподіяна саме в результаті шахрайських дій [4].

Досліджуючи питання розвитку Інтернет-шахрайства у сфері високих технологій, ми можемо зазначити, що найбільшого поширення останнім часом набули наступні способи Інтернет-шахрайства:

1) фішинг та його різновиди: вішинг та смішинг;
2) шахрайство із платіжними пластиковими картками;
3) шахрайство при користуванні мобільними телефонами, зокрема, при здійсненні платежів за допомогою premium-SMS.

Крім того, слід зазначити, що в 2012 році в Україні з'явилися й нові види високотехнологічного шахрайства. Один з них - так званий TransactionReversalFraud (TRF), відомий також як cashtrapping. Суть схеми проста: шахрай запитує видачу готівки по своїй картці, але одночасно заважає банкомату виконати стандартний алгоритм по видачі готівки. Банкомат приймає ситуацію за збій, про що надходить відповідна інформація в банк (reversal), та гроші з рахунку шахрая не списуються. Тим часом злочинець примусово забирає запитувану суму з банкомату, застосовуючи спеціальне механічне обладнання. Поки в нашій країні зафіксовано порівняно

небагато випадків cashtrapping. Однак фінансисти побоюються, що шахраї почнуть діяти з більшим розмахом [2].

Крім того, в 2012 році українські банки зіштовхнулися з масовим впровадженням шкідливого програмного забезпечення сімейства Carberp на домашні й робочі комп'ютери/обладнання власників платіжних карт. Основне призначення цих вірусів - крадіжка й передача реквізитів платіжних карт із інфікованого комп'ютера користувача (власника платіжної карти) на сервер шахраїв.

До найбільш характерних рис інтернет-шахрайства можна віднести наступні:

1. все більша динамічність інтернет-шахрайства та структурованість злочинність об'єднань, які займаються даним видом злочинних посягань. Крім того, деякі злочинні об'єднання можуть мати тимчасовий характер, наприклад, для здійснення однієї незаконної операції, що вчиняється різними особами або угрупуваннями в кількох країнах

2. високий рівень латентності, який дозволяє отримувати великі злочинні доходи з мінімальним ризиком викриття та провокує до вчинення нових видів злочинів. Причин латентності декілька, основними серед яких, на думку експертів, є небажання приватного сектора інформувати про такі злочини через недовіру до потенційних можливостей правоохоронних органів і небажаннявизнати слабкі місця своїх систем безпеки, а також – відсутністьналежної системи моніторингу правоохоронними органами мереж загального користування суб'єктів господарської діяльності, що надають інформаційні послуги;

3. комп'ютерна злочинність усе частіше набуває ознак транскордонності. Відкритість глобальних інформаційних мереж надає можливість злочинцям вибирати таку юрисдикцію, яка відповідає їхнім злочинним цілям. А саме, правопорушники можуть вибирати ті країни, де існують привабливі умови для протиправних дій, які згідно з внутрішнім законодавством не підпадають під кримінальну відповідальність, чи відсутні спеціалізовані підрозділи по боротьбі з комп'ютерною злочинністю взагалі, таІнтернет-шахрайством, зокрема;

4. предметом комп'ютерного шахрайства стають права на об'єкти власності (нерухомість, цінні папери, інші активи);

5. підвищуються професійні навички і технічна забезпеченість злочинців. Інформація щодо реквізитів (персональних даних) сторонніх осіб привласнюється за допомогою методів і засобів соціоінженерії та спеціально розроблених програм для незаконного втручання до комп'ютерів, систем, комп'ютерних мереж і електрозв'язку. У мережі Інтернет розповсюджуються інструменти для здійснення комп'ютерних атак, існують спеціальні програми, що атакують комп'ютерні системи і мережі з метою незаконного доступу до комп'ютерної інформації та отримання можливості керувати комп'ютерною системою;

Так, за повідомленнями прес-центру Служби безпеки України, останнім часом в Інтернеті з'явилась нова шахрайська схема, яка протягом останніх місяців 2012 р. – очатку 2013 р. була застосована більш ніж в 13 країнах світу, у тому числі і в Україні. Згідно наданої інформації, зловмисники поширюють шкідливий програмний засіб Trojan, який блокує роботу операційної системи Windows, при цьому на монітор ураженого комп'ютера виводиться повідомлення про її блокування правоохоронними органами за нелегальну діяльність користувача (використання неліцензійного програмного забезпечення, відвідування порносайтів і т.п.) з вимогою перелічити

гроші на електронні гаманці. Тим більше, що, з метою психологічного впливу на користувачів, правопорушники використовують офіційні логотипи Служби безпеки України, намагаючись створити в громадян враження, що їх програмне забезпечення блокує спецслужба [6].

Звісно, що сплата коштів за зазначеними зловмисниками реквізитами не призводить до розблокування комп'ютера.

6. середовищем вчинення комп'ютерних злочинів стають глобальні інформаційні мережі, де все більшого обсягу набуває використання електронних платіжних систем при шахрайствах та у процесі «відмивання» коштів [1, с. 107-108].

Специфіка проблеми протидії комп'ютерній злочинності взагалі, та комп'ютерному шахрайству, зокрема,на думку багатьох експертів, обумовлена наступними основними факторами:

- недостатнім усвідомленням можливих політичних, економічних, моральних та юридичних наслідків комп'ютерних злочинів;
- слабкістю координації дій по боротьбі з такими злочинами правоохоронних органів, суду, прокуратури та недостатньою підготовленістю їх кадрового складу до ефективного попередження, виявлення та розслідування таких злочинів;
- серйозним відставанням вітчизняної індустрії розробки, впровадження засобів і технологій інформатизації та інформаційної безпеки від розвинутих країн світу [1, с. 106].

Необхідно зазначити, що на сьогоднішній день у світі вже створені спеціальні організації, які займаються різними аспектами боротьби із Інтернет-шахрайством, у тому числі і реєстрацією скарг на злочинні дії Інтернет спрямування.

Так, наприклад, у Великобританії – це Національний підрозділ по боротьбі зі злочинами у сфері високих технологій Королівства Великобританії (National High-Tech Crime Unit).

В Російській Федерації – це Бюро спеціальних технічних заходів МВС Росії, до структури якого увійшло Управління «К». Сьогодні діяльність цього підрозділу направлена на припинення найрізноманітніших видів протиправних діянь, і, в першу чергу, злочинів у сфері інформаційних технологій – таких як злочини у сфері комп'ютерної інформації, електронне шахрайство і т.ін.

Крім того, в Російській Федерації діє «Автономная некоммерческая организация "Центр реагирования на компьютерные инциденты"» або «RU-CERT (Russian Computer Emergency Response Team)». RU-CERT входить до складу міжнародних об'єднань CSIRT/CERT центрів (FIRST, Trusted Introducer), основним завданням яких є зниження рівня загроз інформаційної безпеки для користувачів Інтернет [7].

В Сполучених штатах Америки - це Internet Crime Complaint Center - IC3. IC3 діє у тісній співпраці з Центром дослідження біловоротничкової злочинності (NationalWhiteCollarCrimeCenter -NW3C), з Федеральним бюро розслідування (theFederalBureauofInvestigation - FBI) та з Бюро юридичної допомоги департаменту Юстиції США (BureauofJusticeAssistance - BJA) [8]. Для контролю за діяльністю провайдерів та користувачів у мережі Інтернет у розпорядженні ФБР також існує система Carnivore.

Крім того, у складі Міністерства фінансів США діє Секретна служба США (USSecretService), яка проводить розслідування фінансових злочинів за трьома напрямами:

- злочини проти фінансової системи (злочини проти фінансових установ (банківське шахрайство), шахрайство з використанням електронних засобів доступу (кредитних карток), відмивання грошей);
- злочини з використанням електронної апаратури (комп'ютерне шахрайство, шахрайство проти телефонних компаній);
- шахрайства проти державних фінансових програм (зобов'язання казначейства США, махінації з електронним переказом грошових коштів, інші махінації).

В Україні також створено ефективну національну систему боротьби із правопорушеннями в сфері інформаційно-телекомунікаційних технологій, в складі якої, правоохоронці розглядають і високотехнологічне шахрайство.

На сьогоднішній день питаннями боротьби із Інтернет-шахрайством в Україні займається Управління боротьби з кіберзлочинністю МВС України. Хоча, слід зазначити, що боротьба зі злочинністю у сфері високотехнологічного шахрайства здійснюється не лише цим підрозділом, а й іншими підрозділами органів внутрішніх справ України при тісній взаємодії з підрозділами інших правоохоронних органів.

На нашу думку, основними напрямками протидії Інтернет-шахрайству, на наш погляд, можуть стати:

1) розробка нового програмного обладнання та антивірусних програм;

2) удосконалення нормативно-правової бази у сфері боротьби з Інтернет-шахрайством (жодні технології протидії без відповідної нормативно-правової та методологічної підтримки не зможуть подолати кіберзлочинність).

Так, в Російській Федерації з 10 грудня 2012 року почав діяти новий закон, що закріплює диференціацію ст. 159 КК РФ («шахрайство»). Відповідно до Федерального Закону № 207- ФЗ від 29.11.2012 КК РФбуло доповнено новими статтями 159 зі значками 1, 2, 3, 4, 5, 6, у тому числі "Шахрайство з використанням платіжних карт" (ст. 159^3) і "Шахрайство в сфері комп'ютерної інформації" (ст. 159^6). При цьому останнє трактується як розкрадання майна або придбання права на чуже майно шляхом вводу, видалення, блокування, модифікації комп'ютерної інформації або іншого втручання у функціонування засобів зберігання, обробки й передачі інформації або інформаційно-телекомунікаційних мереж[9];

3) створення системи аутентифікаціїінтернет-адресів для перевірки відповідності введеної користувачем адреси дійсному серверу;

4) підвищення загального рівня грамотності інтернет-користувачів та більш широке поширення інформації про відомі види Інтернет-шахрайства користувачам Інтернету;

5) проведення різного роду науково-практичних конференцій, семінарів, круглих столів за участю теоретиків та практичних працівників.

Так, наприклад, протягом останніх трьох років в Москві було проведено вже 3 міжнародних конференції на тему «Борьба с мошенничеством в сфере високих технологий. Профилактика и противодействие». Наступна конференція запланована на листопад 2013 року, коли пройде 4-та міжнародна конференція по боротьбі із шахрайством у сфері високих технологій «Antifraud Russia – 2013». За роки свого існування конференція зарекомендувала себе як унікальний професійний майданчик для обговорення всього комплексу питань профілактики, запобігання й розслідування

шахрайства з використанням комп'ютерних технологій, юридичних аспектів боротьби з кіберзлочинами, притягнення зловмисників до відповідальності [10]);

6) створення в Україні Бази даннихінтернет-інцидентів та Центру скарг Інтернет-злочинності за аналогією із IC3 (Internet CrimeComplaintCenter - США) та RU CERT (Центр реагування на комп'ютерні інциденти Російської Федерації) та ін.

Список літератури:

1. Правові та організаційні засади протидії злочинам у сфері використання платіжних карток. Науково-практичний посібник / В.М. Бутузов, В.Д. Гавловський, К.В. Тітуніна, В.П. Шоломенцев; За ред. І.В. Бондаренка. – К., 2009. – 182с.

2. Очимовская Т. Новые уловки интернет-мошенников // [Электронный ресурс]. – Режим доступа: http://smi.liga.net/articles/2013-02-12/8306060-novye_ulovki_internet_moshennikov.htm

3. Княжанский В. На темной стороне Интернета // [Электронный ресурс]. – Режим доступа: http://smi.liga.net/articles/2013-02-22/8440309-na_temnoy_storone_interneta.htm

4. Мошков А.Н. Современные подходы к борьбе с электронным мошенничеством [Электронный ресурс]. – Режим доступа: http://antifraudrussia.ru/

5. Никитина Т. Британцев атакуют мошенники, использующие чужие данные [Электронный ресурс]. – Режим доступа: http://www.securelist.com/ru/blog/207764448/Britantsev_atakuyut_moshenniki_ispolzuyushchie_chuzhie_dannye

6. СБУ призывает не поддаваться на вымогание средств в Интернете [Электронный ресурс]. – Режим доступа: http://for-ua.com/

7. Центр реагирования на компьютерные инциденты Российской Федерации: сайт // [Электронный ресурс]. – Режим доступа: http://www.cert.ru/

8. The Internet Crime Complaint Center (IC3) // [the Electronic resource] – the Mode of access: http://www.ic3.gov

9. О внесении изменений в Уголовный кодекс Российской Федерации и отдельные законодательные акты Российской Федерации: федеральный закон от 29.11.2012 № 207-ФЗ (принят ГД ФС РФ 23.11.2012) [Электронный ресурс]. – Режим доступа: http://duma.consultant.ru/page.aspx?1635181

10. Борьба с мошенничеством в сфере высоких технологий // [Электронный ресурс]. – Режим доступа: http://antifraudrussia.ru/news/339.html

Сабадаш В.П. Интернет-мошенничество: реалии современности и криминалистические аспекты противодействия / В.П. Сабадаш // Ученые записки Таврического национальногоуниверситета им. В. И. Вернадского. Серия : Юридические науки. – 2013. – Т. 26 (65). № 1. – С. 278-283.

В статье рассматривается современное состояние и криминалистические аспекты противодействияинтернет-мошенничеству. Исследуются статистические даннные относительно таких преступных проявлений в мире, указываютсяспособы интернет-мошенничества, его характерные особенности, отмечаются специальные организации, которые занимаются разными аспектами противодействияинтернет-мошенничеству, в том числе и регистрацией жалоб на преступные действия интернет направленности в разных государствах мира, раскрываются основные направления противодействия этому преступному действию.

Ключевые слова: интернет-мошенничество, преступление, способы, противодействие, информационная безопасность, сфера высоких технологий.

Sabadash, V.Internet fraud: realities of the present and criminalistic aspects of counteraction / V. Sabadash // Scientific Notes of Tavrida National V. I. Vernadsky University. – Series : Juridical sciences. – 2013. – Vol. 26 (65). № 1. – P. 278-283.

In article the current state and criminalistic aspects of counteraction to Internet fraud is considered. Statistical data concerning such criminal manifestations in the world are investigated, ways of Internet fraud, its characteristics are specified, the special organizations which are engaged in different aspects of counteraction to Internet fraud including registration of complaints to criminal acts the orientation Internet in the different states of the world, the main directions of counteraction to this criminal act reveal are noted.

Keywords:Internet fraud, crime, ways, counteraction, information security, sphere of high technologies.