грудня 2005 р. № 12 // Інформаційний сервер Верховного Суду України / [Електронний ресурс]. – Режим доступу: http://www.scourt.gov.ua/.

4. Кримінальне право України. Особлива частина: [підруч.] / М.І. Бажанов, Ю.В. Баулін, В.І. Борисов [та ін.]. / [за заг. ред. М.І Бажанова, В.В. Сташиса, В.Я. Тація]. – [2-е вид., перероб. і доп.]. – К.: Юрінком Інтер, 2005. – 544 с.

5. Караулов В.Ф. Добровольный отказ от совершения преступления / В.Ф. Караулов // Ученые записки Всесоюз. юрид. заочн. ин-та. – 1969. – Вып. 18. Ч. 2. – С. 66–84.

6. Хряпінський П.В. Заохочувальні норми у кримінальному законодавстві України: [моногр.] / П.В. Хряпінський. – Харків: Харків юридичний, 2009. – 840 с.

7. Пинаев А.А. Уголовное право Украины. Общая часть: [учеб. пособ.] / А.А. Пинаев. – Харьков: Харьков юридический, 2005. – 664 с.

8. Ємельянов В.П. Терористичні злочини: кримінально-правова характеристика та вдосконалення антитерористичного законодавства: [моногр.] / В.П. Ємельянов, Л.В. Новікова, М.В. Семикін. – Харків: Кроссроуд, 2007. – 216 с.

9. Баулін Ю.В. Звільнення від кримінальної відповідальності: [моногр.] / Ю.В. Баулин. – К.: Атіка, 2004. – 296 с.

10. Уголовный кодекс Российской Федерации / [Электронный ресурс]. – Режим доступа: www.uk-rf.ru/.

11. Наумов А.В. Российское уголовное право: [курс лекций]: в 3 томах / А.В. Наумов. – [4-е изд., перераб. и доп.]. – М.: Волтерс Клувер, 2007— .—

Т. 2: Особенная часть (Главы I-X). – 2007. – 504 с.

12. Хряпінський П.В. Спеціальні види звільнення від кримінальної відповідальності: порівняльно-правова характеристика / П.В. Хряпінський // Актуальні проблеми формування громадського суспільства та становлення правової держави: [збірн. наук. праць]. – Черкаси: ЧНУ ім. Б. Хмельницького; Видавець Чабаненко Ю.А. – 2010. – С. 320–323.

УДК 343.72 : 334.7:004 (477)

ШАХРАЙСТВО В ЕЛЕКТРОННІЙ КОМЕРЦІЇ: РЕАЛІЇ СЬОГОДЕННЯ

Сабадаш В.П., к.ю.н., доцент

Запорізький національний університет

У статті розглянуто питання протидії шахрайським проявам в електронній комерції на сучасному етапі розвитку даної сфери бізнесу в Україні.

Ключові слова: електронна комерція, електронні платіжні системи, шахрайство, Інтернет, злочин, кіберзлочинність.

Сабадаш В.П. МОШЕННИЧЕСТВО В ЭЛЕКТРОННОЙ КОММЕРЦИИ: РЕАЛИИ СЕГОДНЯШНЕГО ДНЯ / Запорожский национальный университет, Украина

В статье рассмотрены вопросы противодействия мошенническим проявлениям в электронной коммерции на современном этапе развития данной сферы бизнеса в Украине.

Ключевые слова: электронная коммерция, электронные платежные системы, мошенничество, Интернет, преступление, киберпреступность.

Sabadash V.P. FRAUD IN ELECTRONIC COMMERCE: TODAY'S REALITY / Zaporizhzhya national university, Ukraine

In the article were clearly examined the struggle against fraud questions in electronic commerce in the present stage of development of this business sphere in Ukraine.

Key words: electronic commerce, electronic payment systems, fraud, Internet, crime, cybercriminality.

Загальновідомо, що з розвитком всесвітньої мережі Інтернет та технічних ресурсів, а також із розвитком ринку персональних комп'ютерів і збільшенням обсягу Інтернет-аудиторії відповідно збільшується й обсяг електронної комерції, електронного банкінгу та інших складових даного процесу. В усьому світі зростає число людей, які роблять покупки в інтернет-магазинах, користуються онлайновими банківськими послугами – оплачують рахунки, управляють своїми банківськими заощадженнями, розраховують найбільш вигідні для себе умови кредиту.

Так, наприклад, у західних країнах, за підсумками нещодавнього опитування, проведеного Symantec, споживачі ставлять банківські онлайн-послуги на перше місце серед усіх видів діяльності в Інтернеті, які полегшують їм життя. Із них 86% респондентів вважають, що банківські онлайн-послуги заощаджують їм не менш 5-ти годин на тиждень, а більш ніж кожний п'ятий (21%) вважає за можливе взагалі обійтися без особистого відвідування банку завдяки банківським онлайн-послугам. Опитування також показало, що коли споживачам потрібна порада або допомога щодо захисту персональної інформації, вони, у першу чергу, звертаються до своїх фінансових установ (54%), а потім – у компанії, що спеціалізуються на безпеці, такі як Symantec (29%) [1].

Необхідно зазначити, що початок становлення електронної комерції безпосередньо пов'язаний з появою та розвитком Інтернету. До 2000-х років глобальна мережа в Україні майже не розвивалася, а більшість населення навіть не підозрювала про її існування. Станом на 2000 р. у країні налічувалось тільки 200 тисяч користувачів Інтернету. Високі ціни доступу разом із низькими швидкостями були нездоланним бар'єром для розвитку онлайн-торгівлі. У 2000 р. в Україні діяло лише близько 100 інтернет-магазинів. Проте в наступні роки ситуація почала змінюватись. Вже на середину 2000-х років Інтернет перестав бути екзотикою для українців. У 2005 р. аудиторія уанету перевищила 5 млн. користувачів, а на сьогоднішній день інтернет-користувачів вже майже 15 млн. Це і стало основою для динамічного зростання онлайн-торгівлі. У 2010 році 7,5% обсягу української роздрібної торгівлі припадало на покупки у світовій павутині. На сьогоднішній день ринок інтернет-торгівлі України перебуває на етапі бурхливого розвитку. За останні 10 років кількість інтернет-магазинів зросла приблизно в 60 раз, а обіг онлайн-торгівлі перевищив 1 млрд. дол. [2].

Актуальність теми статті обумовлена тим, що зростання науково-технічного прогресу обумовлює не тільки прогресивні зміни в розвитку електронного сегмента ринкових відносин, але й негативні тенденції розвитку злочинного світу, призводить до появи нових форм і видів злочинних зазіхань. Це проявляється в тому, що злочинні групи в електронній комерції все активніше використовують новітні досягнення науки й техніки, застосовують усілякі комп'ютерні пристрої та нові інформаційно-обробні технології тільки задля того, щоб за допомогою шахрайських дій отримувати прибутки.

Вивчення стану наукової розробленості проблеми протидії комп'ютерній злочинності та впливу шахрайства на розвиток електронної комерції в Україні показало, що на сучасному етапі спеціального дослідження із цих проблем не проводилося. Проте необхідно зазначити, що окремі аспекти протидії комп'ютерній злочинності розглядалися в роботах Д.С. Азарова, Ю.М. Батурина, П.Д. Біленчука, М.С. Вертузаєва, В.Б. Вєхова, В.О. Голубєва, М.Д. Дихтяренко, Є.І. Панфілової, О.М. Попова, Н.А. Селіванова й деяких ін.

Метою даної статті є комплексне вивчення проблем, пов'язаних із сучасним етапом розвитку електронної комерції в Україні, впливом шахрайства на розвиток цього сегмента ринкових відносин та на базі цього розробка пропозицій, спрямованих на підвищення ефективності кримінально-правового регулювання боротьби з комп'ютерною злочинністю.

На сьогоднішній день ми можемо назвати кілька основних електронних платіжних систем, за допомогою яких українські споживачі роблять інтернет-платежі: WebMoney, LiqPay, Portmone, FlashCheque. Кожна із цих систем приділяє велику увагу безпеці електронних платежів. Традиційно інтернет-платежі поділяються на моментальні, регулярні, а також P2P-переклади і C2B. Моментальні платежі – це, в основному, оплата всіляких послуг телекома (мобільний зв'язок, Інтернет і т.п.), саме вона робить левову частину обороту. Регулярні платежі – по суті те же саме, але здійснюються вони на регулярній основі шляхом надання відповідних повноважень платіжній системі розпоряджатися вашими грошима від вашого імені. P2P-платежі – це переклади грошей від користувача до користувача. Таким способом найчастіше здійснюють оплату праці фрілансерів, трудові відносини з якими ніяк не врегульовані. C2B – це оплата товарів в інтернет-магазинах. Більшість систем електронних платежів охоплюють

відразу всі ці напрямки, однак деякі з них більш строго сегментовані. Платіжними ж засобами виступають переважно електронні гроші, банківські платіжні картки та електронні засоби керування безготівковим розрахунком [3].

Необхідно зазначити, що, незважаючи на те, що на сьогоднішній день в Україні зареєстровано приблизно 15 млн. інтернет-користувачів, а кількість інтернет-магазинів зросла приблизно в 60 раз за останні 10 років, електронні гроші у вітчизняних споживачів великим попитом не користуються, та взагалі електронна комерція ще розвинена недостатньо. Причинами, які гальмують розвиток електронної комерції в Україні, фахівці називають: а) низький ступінь довіри рядових користувачів до електронних платіжних систем та інтернет-магазинів, б) низький розвиток культури інтернет-шопінгу, в) перешкоди з боку банків-емітентів пластикових карток, г) нерозуміння і небажання розуміти, що таке "електронні гроші", д) нерозвиненість системи захисту прав споживачів [4]. Хоча переваги електронних платежів перед усіма іншими видами готівкових та безготівкових платежів очевидні. Застосування електронних грошей може стати гарним рішенням як для компаній, так і для споживачів. Перша (і основна) перевага – моментальність оплати. У споживача немає необхідності кудись ходити, стояти в чергах і заповнювати масу документів. Компанія може спростити свій бухгалтерський облік і відійти від роботи з готівкою.

Тим більше, що практично будь-яка електронна платіжна система додає максимум зусиль щодо забезпечення безпеки платежів своїх користувачів. Так, наприклад, у системі LiqPay безпека керування рахунком забезпечується технологією OTP (One-time Password – одноразовий пароль), тобто транзакції підтверджуються динамічним одноразовим паролем, що висилається в SMS на номер рахунку. Portmone використовує стандарт SSL-шифрування з використанням стійкої криптографії (довжина ключа 128 біт). Система ж FlashCheque вирішує проблему безпеки принципово іншим способом. Вона не зберігає й не передає через Інтернет дані про платіжні реквізити користувачів. Акт здійснення платежу тут нагадує скоріше не переклад коштів з одного рахунку на інший, а виписку іменного векселя, завіреного особистим підписом. При цьому одержувач платежу (або зловмисник) не може виявити ні номер рахунку платника, ні дані його банку.

Однак все рівно час від часу виникають прикрі інциденти, і провиною всьому, як правило – людський фактор. Якщо базу не можна зламати, її можна купити. Так, відповідно до результатів закордонних досліджень, на першому місці серед кібер-злочинців – колишні банківські співробітники та технічні фахівці. Спокуса продати наявні в розпорядженні дані за великі гроші виявляється занадто великою. Тому користуючись сервісом, що зберігає платіжні дані користувачів, навряд чи можна бути на 100% спокійним за їхню схоронність: або хакери зацікавляться, або звільнений адмін продасть.

До речі, електронні платіжні системи завжди цікавили різного роду інтернет-злочинців та найбільш небезпечним видом шахрайства в електронній комерції залишається фішинг. Перша відома фішингова атака на електронну платіжну систему зафіксована в червні 2001 року, коли атаці піддалася платіжна система e-gold, другою стала атака, що відбулася незабаром після теракту 11 вересня 2001 року. Ці перші спроби були лише експериментом, перевіркою можливостей. А вже в 2004 році фішинг став найбільшою небезпекою для компаній, що займаються електронною комерцією, і з тих пір він постійно розвивається й нарощує потенціал [5].

Метою фішерів сьогодні є клієнти банків і електронних платіжних систем. У США, маскуючись під Службу внутрішніх доходів, фішери зібрали значні дані про платників податків. І якщо перші листи відправлялися випадково, у надії на те, що вони дійдуть до клієнтів потрібного банку або сервісу, то зараз фішери можуть визначити, якими послугами користується жертва, і застосовувати цілеспрямоване розсилання. Частина останніх фішингових атак була спрямована безпосередньо на керівників і інших людей, що займають високі пости в компаніях [6].

Необхідно зазначити, що соціальні мережі також становлять великий інтерес для фішерів, дозволяючи збирати особисті дані користувачів: так, у 2006 році комп'ютерний вірус розмістив на MySpace безліч посилань на фішингові сайти, націлені на крадіжку реєстраційних даних; у травні 2008 року перший подібний вірус поширився й у популярній російській мережі ВКонтакте. За оцінками фахівців, більше 70 % фішингових атак у соціальних мережах – успішні [7].

Більше того, на сьогодні фішинг виходить за межі інтернет-шахрайства, а підроблені веб-сайти стали лише одним з безлічі його напрямків. Листи, які нібито відправлені з банку, можуть повідомляти користувачам про необхідність подзвонити за певним номером для вирішення проблем з їхніми банківськими рахунками. Ця техніка називається вішинг (голосовий фішинг). Подзвонивши на зазначений номер, користувач заслуховує інструкції автовідповідача, які вказують на необхідність ввести номер свого рахунку та PiN-код. До того ж вішери можуть самі дзвонити жертвам, переконуючи їх, що вони спілкуються із представниками офіційних організацій, використовуючи фальшиві номери.

Набирає свої оберти й SMS-фішинг, також відомий як смішинг (англ. SMiShing – від "SMS" і "фішинг"). Шахраї розсилають повідомлення, що містять посилання на фішинговий сайт, – входячи на нього і вводячи свої особисті дані, жертва аналогічним чином передає їх зловмисникам. У повідомленні також може говоритися про необхідність подзвонити шахраям по певному номеру для вирішення "проблем, що виникли".

Так, відповідно до щомісячного огляду вірусної активності, що проводиться фахівцями "Лабораторії Касперського", січень 2011 року був відзначений ростом кількості шахрайських схем, які застосовувалися зловмисниками, при цьому ключовим елементом більшості схем роботи кібершахраїв також стали SMS-повідомлення. Так, на ряді сайтів користувачам пропонувалася можливість обновити популярний браузер Internet Explorer, однак процес "установки" зненацька завершувався необхідністю "активувати" ПО за допомогою SMS-повідомлення, відправленого на зазначений преміум-номер. Відправивши SMS-повідомлення згідно з вказаним тарифом, користувач одержував посилання на офіційний ресурс, з якого Internet Explorer 8 поширюється зовсім безкоштовно.

Крім того, отримати легкі гроші намагалися й шахраї, що вирішили скористатися популярністю продуктів "Лабораторії Касперського": на сайті, назва якого відрізнялася від kaspersky.ru усього на одну букву, користувачам пропонувалося скачати "новорічний подарунок" – безкоштовний Kaspersky Internet Security 2011. Однак замість подарунка в систему попадала програма, що перезавантажувала комп'ютер і після цього показувала "щасливчикові" повідомлення про виграш телефону Samsung Galaxy S. Для одержання "призу" необхідно також було відправити SMS-повідомлення, що, природно, виявлялося платним.

Взагалі, досить часто наприкінці 2010 та на початку 2011 року жертвами зловмисників ставали власники мобільних телефонів. Пройшовши по отриманому в SMS-повідомленні посиланню на "віртуальну листівку", користувач активував троянську програму, що відправляла SMS на номер, який використовується оператором зв'язку для перекладу грошей з одного рахунку на інший. У результаті подібної операції користувач також втрачав деяку суму грошей [8].

Розкручування ще однієї афери за допомогою SMS-повідомлення можна було спостерігати восени 2010 року. На мобільний телефон абонентів МТС приходили повідомлення приблизно такого змісту: «Ви стали переможцем розіграшу автомобіля «KIA RIO»». Звичайно деяких абонентів зацікавлювало таке повідомлення. Коли вони телефонували на номер, з якого було надіслано повідомлення, то чули приблизно таке повідомлення: «Доброго дня, це оператор мобільного зв'язку МТС. Ви стали переможцем акції і маєте можливість отримати безкоштовно автомобіль, за умови виконання певних вимог», – приємним голосом відповіла дівчина. А для отримання автомобіля потрібно було купити картки поповнення рахунку на певну суму на оператор Київстар та продиктувати «оператору» коди карток поповнення. Що деякі абоненти і робили, та в результаті залишилася без грошей та «виграного автомобіля». Коли правоохоронці надсилали запит до компанії МТС про проведення акції по розіграшу автомобіля «KIA RIO», то там відповідали, що така акція компанією не проводилася.

Взагалі, необхідно зазначити, що платежі за допомогою premium-SMS в історично недовірливому до кредитних карток та інших електронних методів оплати послуг українському суспільстві стають не тільки самим популярним способом витратити електронні гроші, але й самим небезпечним.

Так, зловмисники обманюють користувачів, пропонуючи їм скачати контент і вказуючи ціну, що менше реальної вартості SMS у 10-15 разів, заражають мобільні телефони користувачів вірусами, які згодом самі розсилають повідомлення на premium-номери, кодують файли, що містяться на жорсткому диску, а то й зовсім блокують функціонал операційних систем, вимагаючи в обмін на лікування відіслати SMS на який-небудь із premium-номерів. Іншими словами, шахраї невпинно винаходять нові способи відібрання грошей у населення, і у всіх цих способів є як мінімум одна загальна ознака: короткі мобільні номери з дуже дорогими SMS.

Прагнення мережних злочинців є зрозумілим: якщо при інших способах Інтернет-шахрайства зловмисникові потрібно пройти досить довгий шлях від моменту обману користувача до одержання живих грошей (наприклад, роздобути дані кредитної картки за допомогою підробленого сайту, витратити гроші на товари в інтернет-магазинах і тільки потім перетворити товари в гроші, продавши речі за непридатною ціною), то у випадку з premium-SMS реальні гроші зловмисники можуть одержати вже буквально через тиждень. Infox.ru неодноразово називав цю форму комерції золотою жилою для мережних зловмисників [9].

Таким чином, дослідивши сучасний стан розвитку електронної комерції в Україні, ми можемо зазначити, що цей сегмент ринку все частіше піддається нападам інтернет-шахраїв, які використовують задля цього новітні досягнення науки й техніки, застосовують усілякі комп'ютерні пристрої та нові інформаційно-обробні технології з метою отримання злочинних прибутків. І тільки знання способів боротьби та профілактики зможе зупинити вал шахрайських проявів в Інтернеті.

Так, основними напрямками протидії шахрайству в Інтернеті, на наш погляд, можуть стати:

– розробка нового програмного обладнання та антивірусних програм;

– створення системи аутентифікації інтернет-адресів для перевірки відповідності введеної користувачем адреси дійсному серверу;

– більше широке поширення інформації про відомі види Інтернет-шахрайства користувачам Інтернету та ін.

ЛІТЕРАТУРА

1. Онлайн-банкинг облегчает пользователям жизнь / [Электронный ресурс]. – Режим доступа: http://e-commerce.com.ua/5827.

2. Огляд ринку Інтернет-торгівлі в Україні / [Електронний ресурс]. – Режим доступу: http://www.ukrbiznes.com/analitic/marketing/10614.html.

3. Майданик А. Насколько безопасны платежи в Уанете? / [Электронный ресурс]. – Режим доступа: http://www.internetua.com/naskolko-bezopasni-plateji-v-uanete1.

4. Станут ли виртуальные деньги реальным платежным средством украинца? / [Электронный ресурс]. – Режим доступа: http://www.internetua.com/stanut-li-virtualnie-dengi-realnim-platejnim-sredstvom-ukrainca.

5. Фишинг / [Электронный ресурс]. – Режим доступа: http://ru.wikipedia.org/wiki/Фишинг#cite_note-7.

6. Markus Jakobsson, Tom N. Jagatic, Sid Stamm. Phishing for Clues / [Electronic resource]. – Access mode: https://www.indiana.edu/~phishing/browser-recon/.

7. Пользователи сайта "В Контакте.Ру" стали жертвами компьютерного вируса / [Электронный ресурс]. – Режим доступа: http://www.webcitation.org/5w9YfvFNN.

8. Киберитоги января: новые схемы работы мошенников / [Электронный ресурс]. – Режим доступа: http://www.internetua.com/kiberitogi-yanvarya--novie-shemi-raboti-moshennikov.

9. Мобильные мошенники пока неуловимы / [Электронный ресурс]. – Режим доступа: http://www.internetua.com/mobilnie-moshenniki-poka-neulovimi.