УДК 343.537:343.346.8:343.974

С.В. Шапочка

КЛАСИФІКАЦІЯ ШАХРАЙСТВА, ЩО ВЧИНЯЄТЬСЯ З ВИКОРИСТАННЯМ КОМП'ЮТЕРНИХ МЕРЕЖ (КІБЕРШАХРАЙСТВА)

У статті описано найбільш розповсюджені способи учинення такого різновиду майнових злочинів, як кібершахрайство. Розкрито питання класифікації шахрайства, що вчиняється з використанням комп'ютерних мереж.

Ключові слова: *шахрайство, Інтернет-шахрайство, кібершахрайство, класифікація, кіберзлочинність, попередження кіберзлочинності.*

В статье описаны наиболее распространенные способы совершения такой разновидности имущественных преступлений, как кибермошенничество. Раскрыты вопросы классификации мошенничества, которое совершается посредством использования компьютерных сетей.

Ключевые слова: *мошенничество, Интернет-мошенничество, классификация, киберпреступность, предупреждение киберпреступности.*

In the paper the most widespread ways of the commission of such kind of property crimes as cyberfraud are described. Issues of classification of fraud committed by means of use of computer networks are revealed.

Keywords: *fraud, Internet fraud, cybercrime, prevention of cybercrime.*

Класифікація злочинів має розкрити їхню кримінально-правову характеристику, сприяти вдосконаленню кримінального законодавства та практики його застосування.

Нині в кримінології не розроблено якоїсь єдиної класифікаційної моделі видів злочинів, і зробити це достатньо складно, якщо врахувати різноструктурний і багатоцільовий аспект подібних класифікацій [1, с. 374], а тим більше стосовно кібершахрайства, яке є порівняно новим для світової науки і практики видом злочинів, має високий рівень латентності, величезну кількість способів учинення, необмежені в часі та просторі можливості [2, с. 63].

Проведенням наукових досліджень окремих аспектів щодо боротьби зі злочинами, що вчиняються з використанням комп'ютерних мереж взагалі та шахрайства зокрема, їх класифікації займаються такі вчені, як І.В. Александров, В.Д. Гавловський, В.Є. Емінов, А.А. Комаров, К.В. Тітуніна, В.В. Чернєй, С.С. Чернявський, В.І. Шакун, В.П. Шеломенцев, О.М. Юрченко та інші.

У попередніх наукових публікаціях ми вивчали різні аспекти шахрайства, що вчиняється з використанням можливостей комп'ютерних мереж – кібершахрайства. Ця стаття є логічним продовженням нашого дослідження і містить спробу зробити його класифікацію.

Науковці пропонують класифікувати шахрайства за різними критеріями. Наприклад, Александров І.В. пропонує таку класифікацію: а) вчинені стосовно знайомих потерпілих; б) вчинені щодо незнайомих осіб; в) такі, що використовуються під час заволодіння майном обох категорій [3, с. 8].

При цьому Волохова О.В. наводить таку класифікацію способів вчинення шахрайства: 1) за потерпілим вчинення – стосовно фізичних осіб; стосовно юридич-

них осіб; 2) за умислом вчиненого – заволодіння майном, придбання права на чуже майно; 3) за суб'єктом злочину – фізична чи юридична особа [4, с. 44–53].

Однією з найбільш поширених класифікацій кібершахрайств, що лягла в основу створеної на початку 90-х рр. автоматизованої інформаційно-пошукової системи, є кодифікатор робочої групи Інтерполу [5, с. 24], за яким: QFC – кібершахрайства, пов'язані з розкраданням готівкових грошей із банкоматів; QFF – кіберпідробки (створення підроблених пристроїв); QFG – шахрайства і розкрадання, пов'язані з ігровими автоматами; QFM – маніпуляції з програмами за допомогою невірного введення-виведення; QFP – кібершахрайства і розкрадання, пов'язані з платіжними засобами; QFT – телефонне шахрайство (доступ до телекомунікаційних послуг шляхом зазіхання на протоколи і процедури комп'ютерів, що обслуговують телефонні системи).

Кібершахрайство є одним з найбільш швидко еволюціонуючих майнових злочинів та налічує найбільшу кількість способів учинення, найбільш розповсюдженими серед яких, на нашу думку, є такі.

1. Шахрайство на Інтернет-аукціонах та фінансовому ринку. Шахраї пропонують купити рідкісні товари за низькою ціною чи спеціальною пропозицією, що діє обмежений час, надсилаючи повідомлення про продаж неіснуючого лота або дешевої підробки за привабливою ціною [6, с. 55–56].

Скандинавський аукціон. На такому аукціоні товар виставляється за ціною 1–2 дол., учасники роблять мінімальні ставки і за кожну ставку з них знімається певна сума. Далі потерпілі втрачають гроші і не отримують товар.

На фінансовому ринку використовуються інвестиційні схеми в діяльності незареєстрованих брокерських контор (bucket shops), що здійснюють операції з цінними паперами, перепродаючи активи через рахунок іншої компанії або підставний рахунок, не виконуючи чи виконуючи із запізненням замовлення із купівлі-продажу цінних паперів.

На фінансовому ринку України прикладом bucket shops є численні дилінгові центри-організатори торгів на світовому валютному ринку "Forex, з великою кількістю учасників: центробанки, фінкорпорації, інвестиційні компанії, приватні інвестори [7, с. 73–76]. Заявки далі комп'ютера forex dealing центру не йдуть, а угоди є віртуальними.

2. Шахрайства, пов'язані з торгівлею в Інтернет-магазинах, віртуальними електронними платіжними системами (ЕПС) та "проблеми" з їх використанням: фішинг, вішинг, фармінг, кардінг. У результаті комп'ютерної атаки шахраї отримують доступ до персональних даних клієнтів платіжних систем, які після оплати покупки не отримують, неповністю отримують або одержують товар у меншій кількості чи гіршої якості.

Фішинг (phishing) – отримання доступу до конфіденційних даних користувачів, імітуючи роботу сайтів Інтернет-магазину, платіжної системи або перехопивши запит на браузері, шляхом проведення масових спам-розсилок електронних листів від імені популярних брендів, банків, особистих повідомлень всередині різних сервісів, соціальних мереж, переадресація користувача на підроблений сайт (фейкову сторінку), спонукання жертви ввести там свої дані (логін, пароль, дані віртуальної картки, іншу таємну інформацію для отримання доступу до їх акаунтів). Близько 70 % таких атак у соцмережах є успішними.

За даними антифішингової групи компаній із безпеки Anti-Phishing Work Group, найбільша кількість фішингових сайтів знаходиться в доменних зонах Com – більше 50 % і Net – 8,5 % [8]. Наприклад, на e-mail жертви надходить

лист від імені "адміністрації" сервісу Яндекс.Деньги з проханням активувати обліковий запис на точній копії сайта-близнюка сервісу, ввести свої логін і пароль доступу, таким чином шахраї отримують доступ до рахунку на реальному сайті сервісу Яндекс.Деньги.

Вішинг – ідентичний фішингу і відрізняється способом реалізації – замість e-mail обман здійснюється телефоном, але також пов'язаний із платіжними системами в мережі Інтернет.

Фармінг – удосконалена версія фішингу, перенаправлення користувача на інший сайт, але не через підроблені посилання, а через зараження комп'ютера шкідливим програмним забезпеченням, яке, навіть у разі правильного введення потерпілим адреси справжнього сайту, забезпечує потрапляння на фейковий сайт.

Кардінг – злочинці отримують дані потерпілого за банківською картою і здійснюють купівлю товарів, оплату послуг або переводять у готівку шляхом вчинення фішингу, вішингу тощо, а також створюючи Інтернет-магазини, які насправді нічого не продають, а просто збирають дані по картах.

Кіберсквотинг (cybersquatting) – злочинці (сквоттери) аналізують ринок товарів і послуг, визначають нові бренди успішних компаній та продуктів, для яких ще не існує доменних імен, швидко реєструють однойменні домени й можливі їх варіації, звертаються до власників бренду з пропозицією купити їх по більшій вартості, а у разі відмови –шантажують або отримують прибуток від банерної реклами, чи в інший спосіб експлуатують брендові ім'я чужої компанії. Види кіберсквоттингу: галузевий, брендів, географічний, іменний, тайпсквоттинг.

Тайпсквоттинг відрізняється від інших тим, що в реєстрації доменного імені, схожого з назвою популярного ресурсу, близького за написанням, шахраї розраховують на помилку користувачів, які будуть потрапляти на інший сайт, а тайпсквоттери отримають гроші за рекламу, а також можливість здійснення фішингової атаки. Як відомо, людина може прочитати неправильно написане слово і навіть не помітити цього, якщо вірно були поставлені перша й остання букви. Наприклад, http://www.dinseyland.com/ і http://www.disneyland.com/.

Використання ЕПС: на e-mail жертви надходить лист-повідомлення від "адміністрації" платіжної системи, навіть якщо користувач на цю адресу ніколи не реєстрував ні WM-кіпер, ні акаунт E-Gold у інших платіжних системах, із повідомленням про те, що з певного числа поточного року буде заблоковано його акаунти. Але проблему легко вирішити внесенням на рахунок адміністрації заставної суми, яку буде повернуто власнику в разі закриття ідентифікатора.

Підробка ЕПС шляхом створення фейкових доменних імен. Жертва отримує лист, у якому зазначається про поширення шахрайства і необхідність усім користувачам пройти верифікацію, для якої увійти в акаунт й клікнути підтвердження чи закачати файли ключів і акаунт не буде заблоковано. Отримавши пароль і ключі, шахраї використовують кошти на власний розсуд чи з двох платежів, перерахованих на рахунок жертви, зараховується лише один.

3. "Нігерійські листи чи "Схема 419", допомога у відмиванні коштів чи листи щастя (за номером відповідної статті КК Нігерії). Одержувач email-листа приймає участь у переказі чи переведенні в готівку великої суми коштів, що належить спадкоємцям африканських президентів, диктаторів, королів із нігерійського, ганського, лівійського банку в банк інших держав та розраховує отримати частину суми, для чого жертві пропонується перевести кілька тисяч доларів (транспортні чи інші витрати) на рахунок шахраїв.

Листи щастя. Користувач отримує спам-лист із повідомленням про виграш у великому Інтернет-проекті – лотереї, конкурсі, акції, для отримання якого

потрібно оплатити наперед податок, комісію, внести певну суму, щоб пройти онлайн-реєстрацію, для переходу на інший рівень, в супергру.

4. Ділові пропозиції на безкоштовних дошках оголошень, форумах, спеціальних сайтах, у спам-розсилках з явно завищеною оцінкою очікуваного прибутку: пропозиція високоприбуткової роботи вдома (збирання інформації з метою її аналізу, узагальнення, дизайн веб-сайтів, створення програмних продуктів, набір тексту, переклад за вигідним тарифом тощо), працевлаштування в компанію зі світовим ім'ям [6, с. 44–45]. Жертва здійснює передоплату витратних матеріалів, відшкодовує витрати на їх доставку, робить гарантійний чи вступний внесок, який повернуть через тиждень або частину часу працює безкоштовно на випробувальному терміні. Купує спеціальні HOAX-програми, які автоматично збирають бонуси у вигляді грошей або самі генерують криптовалюту Bitcoin, коди платіжних карт, за допомогою яких можна здійснити злам системи, аканту, імітатори антивірусів. При цьому зазначені програми не працюють.

Також можуть запропонувати дешеву програму для зламу WebMoney Keeper, використання якої є злочином, а вона може містити ще й вірус-троян, який допоможе злочинцям отримати паролі від гаманців жертви.

5. Шахрайство в соціальних мережах: використовуючи можливості соціальної інженерії, вчиняється фішинг, sms-шахрайство, розсилаючи від імені друзів зі зламаних акаунтів прохання поповнити рахунок мобільного телефону, відправити sms тощо.

SMS-шахрайство. Пропозиції відправити повідомлення на короткий номер містяться в значній частині спаму під приводом: блокування облікового запису жертви чи ускладнення роботи системи через розсилки спаму за допомогою вірусів типу Trojan.Winlock (банери з порнографічними зображеннями поверх вікон), для підтвердження особистості та номера телефону, зазначеного при реєстрації на сайті, у зв'язку з виграшем призу, отриманням подарунку, платного доступу до "порно-архівів", вартість якого виявляється значно вищою заявленої. Майже всі сайти "знайомств для сексу" є шахрайськими.

6. Пільгові позики. Фізичним особам часто пропонують пільгові кредити, для отримання яких необхідно зробити вступний внесок або в які закладено приховані занадто високі відсотки.

7. Шахрайство під час гри онлайн: створення сайтів онлайн-казино, реклама яких розповсюджується за допомогою листів-спаму, а хостинг здійснюється в країнах, де гральний бізнес є легальним, казино доступне користувачам у всьому світі. Потенційній жертві випадає можливість отримати гроші, а щоб скористатися "удачею" потрібно завантажити програмне забезпечення для гри – вірус.

Шахрайство під час гри в онлайн-покер. Адміністрація й деякі "привілейовані" гравці можуть бачити всі карти, які знаходяться в момент гри на руках учасників, а злочинець реєструється на одному і тому ж покер-румі під кількома акаунтами, успішно беручи участь у турнірах.

8. Шахрайство-здирництво. Жертва отримує повідомлення про те, що користуючись послугами різних Інтернет-сервісів, відвідуючи сайти сумнівного чи злочинного змісту, вона вчиняє злочин, чи веде аморальний спосіб життя, про що стане відомо правоохоронним органам, ЗМІ, рідним, діловим партнерам. З метою запобігання зазначеному необхідно перерахувати гроші на рахунок злочинця.

У іншому випадку – потерпілого повідомляють про можливість безкоштовно отримати від невідомої особи чи родича колекційну або високої вартості річ, тварину тощо, лише оплативши за пересилку половину від реальної вартості товару.

9. Зловживання співчуттям. Жебрацтво. Шахраї через спам-розсилку тиражують листи жалісливого змісту, в яких описують неіснуючі власні проблеми-потреби, вирішити які можна, надіславши на їх рахунок невеликі кошти (від 1 цента до кількох дол.). Сума зібраного залежить від активності шахрая та рівня емпатії жертв [9, с. 44].

Збирання пожертвувань. 90 % американців жертвують великі суми на різні благодійні цілі. Цим користуються шахраї, створюючи фальшиву благодійну організацію й абсолютно відкрито збираючи пожертвування. Так, шахраї збирали кошти для надання допомоги дітям, постраждалим від теракту в м. Беслані, через електронну платіжну систему WebMoney.

Зазначений спосіб обману набув популярності й в Україні. Кібершахраї збирають кошти під різними благодійними гаслами: починаючи від пожертв на операцію для спасіння життя чи відновлення здоров'я дитини із зазначенням номеру мобільного телефону, банківських реквізитів чи електронного гаманця "мами" до допомоги внутрішнім мігрантам та мешканцям України з АР Крим, територій проведення антитерористичної операції, власне бійцям АТО, а також збирають кошти на чисельні "відновлювальні" роботи зруйнованих споруд культового призначення, дитячих будинків тощо.

10. Фінансові інвестиційні "піраміди" (pyramid scheme) – шахрайство, що вчиняється під прикриттям організації, членство в якій набувається в разі внесення коштів потерпілими, причому розмір прибутків зростає прямо пропорційно кількості вкладників та місцю розпорядника коштів у ієрархії цієї організації [10, с. 22–23]. Прикладами фінансових Інтернет-пірамід є: програми Бінар (MyBinar), NewPRO, SuperProgik, проекти Мавроді МММ-2011 та МММ-2012, Emgoldex, Swissgolden. Фінансовими пірамідами є також більшість хайп-проектів (HYIP – High Yield Investment Program) – інвестиційних фондів із високою прибутковістю: швидкі, середньострокові, довгострокові. Нині це, в основному, онлайн-проекти, які працюють з електронними валютами.

Наприклад, за електронною адресою http://josephpetercamposjr.info/ Костянтин Фєлатов пропонує заробити на бінарних опціонах з торгівлі валютами, дорогоцінними металами, акціями, індексами або товарами на міжнародних фінансових ринках і біржах до 500 дол. США на день, стверджуючи, що на відміну від торгівлі на фондових біржах або ринку Forex, тут все максимально спрощено, необхідно лише зробити ставку курсу на певний період часу, зазначаючи, що спочатку необхідно зареєструватися і внести депозит [11].

Кібершахрайство із криптовалютами. У лютому поточного року в спеціальному адміністративному районі КНР Гонконзі було вчинено кібершахрайство, внаслідок якого на місцевій біржі злочинці заволоділи криптовалютою Bitcoin у кількості 386,9 млн. Це найбільша сума втрат від кібершахрайства з використанням криптовалют, оскільки загальна кількість Bitcoin у світі не перевищує 3 млрд.

11. Чарівні (золоті) гаманці, подвоєння коштів – вид кібершахрайства, що полягає в спонуканні жертви до переведення коштів на технічний рахунок платіжної системи, а електронний гаманець нібито автоматично повертає їх назад у подвоєному або потроєному розмірі. Шахраї здійснюють злам платіжних систем Яндекс і WebMoney або нібито знаходять і використовують таємні тестові гаманці цих систем, які повертають надіслані на них гроші збільшеними в кілька разів. Або розповсюдження неправдивої інформації, що чарівні гаманці не повертають тільки великі суми від 10 дол. і вище, а більш дрібні – приходять, причому подвоєні або потроєні і можна покарати шахраїв всім разом і викачати, посилаючи маленькі суми, всі гроші з гаманців "шахраїв" – втрата коштів потерпілими.

12. Страхове шахрайство. “Страхова” компанія пропонує рекордно низькі розцінки за свої послуги, існуючи лише на папері, або вона закладає в договір із клієнтом умови, які унеможливлюють одержання страховки.

13. Обмін електронних грошей, валюти. Шахраї пропонують усім бажаючим обмінювати електронні валюти і отримувати прибуток завдяки істотній різниці курсів у обмінних пунктах різних держав.

Широкого розповсюдження в Україні набула рекламна компанія заробітку грошей на ринку міжбанківського обміну валюти за вільними цінами, на якому котирування формується без обмежень або фіксованих значень – Forex (FOReign EXchange, FX – “закордонний обмін”) чи Forex market, FX-market. У зв’язку з відсутністю в переважної кількості громадян відповідної освіти для здійснення операцій на FX-market, багато з них шукають варіант довірчого управління, залучаючи досвідчених трейдерів, трейдер-шахрай отримує свою частку.

14. Лотереї, спорт-прогнози. На e-mail потерпілого приходить повідомлення про те, що він виграв велику суму грошей чи коштовний подарунок у лотереї, про яку він навіть й не чув, і потрібно перерахувати гроші для оформлення переказу та активації рахунку або пересилання виграшу.

Ставки на спорт. На сайтах букмекерських контор, які часто і самі є шахрайськими, та в спам-розсилках кібершахраї пропонують купити прогнози спортивних результатів від “професіоналів” або взагалі “знають” все про договірні матчі в футболі й поділяться цим за гроші.

15. Скаммеринг – обдзвонювання жертв від імені корпорацій Microsoft, Dell, McAfee, повідомляючи про серйозне зараження ПК потерпілих небезпечними вірусами, що можуть призвести до псування комп’ютера, пропонуючи “лікування” за грошову винагороду [12]. Жертва, діючи за вказівками шахрая, завантажує вірус, що дозволяє злочинцям отримати повний доступ до ПК. Також злочинці розміщають рекламу в пошуковій роздачі Google за запитами “McAfee”, “PC support”, і “fix MS Office”, залишаючи в ній свої псевдоніми та безкоштовні телефони як служби підтримки компанії-виробника антивірусних продуктів.

Ми зібрали дані, проаналізували та дослідили близько 40 видів кібершахрайства, які виділили і об’єднали в 15 груп, розподіливши їх за способами вчинення чи об’єктами посягання. У наступних працях докладніше розглянемо деякі з них.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. *Эминов В.Е.* Криминологическая классификация и характеристика преступлений / В.Е. Эминов // LEX RUSSICA (РУССКИЙ ЗАКОН). – 2006. – № 2. – С. 374–377.

2. *Shapochka S.* Preventing Fraud Using Computer Networks / S.V. Shapochka // Internal Security. – 2013. – № 2. – P. 63–75.

3. *Александров И.В.* Криминалистическая характеристика и особенности расследования мошеннических посягательств на личную собственность граждан : автореф. дис. ... канд. юрид. наук / И.В. Александров. – Свердловск, 1985. – 20 с.

4. *Волохова О.В.* Современные способы совершения мошенничества : особенности выявления и расследования / О.В. Волохова, под ред. проф. Е.П. Ищенко. – М. : Издательство “Юрлитинформ”, 2005. – 128 с.

5. *Комаров А.А.* Криминологические аспекты мошенничества в глобальной сети Интернет : дис. ... канд. юрид. наук : 12. 00. 08 / А.А. Комаров. – Саратов, 2011. – 262 с.

6. *Смирнова Л.* 100 способов удачного мошенничества, или как избежать ловушки / Л. Смирнова. – Мн. : Современный литератор, 2005. – 96 с.

7. *Глушков В.О.* Шахрайство на фінансових ринках у біржовій торгівлі. Правовий та кримінологічний аналіз / В.О. Глушков, П.М. Коваленко. – К. : Ін Юре, 2008. – 280 с.

8. Кибермошенничество в эпоху глобализации [Электронный ресурс]. – Режим доступа : http : // univer-nn.ru/it/flood.php.

9. *Корнєєв О.О.* Обережно! Шахраї, аферисти, злодії / О.О. Корнєєв. – Х. : Прапор, 1997. – 158 с.

10. Розслідування шахрайств, учинених способом фінансової піраміди : навч. посіб. / С.С. Чернявський, О.Ю. Татаров, В.В. Чернєй та ін. ; за заг. ред. В.В. Коваленка. – К., 2013. – 180 с.

11. *Константин Фелатов* (Моя методика заработка в интернете до 500 $ в день / К. Фелатов [Электронный ресурс]. – Режим доступа : http : // josephpetercamposjr.info/.

12. Новый вид Интернет-мошенничества [Электронный ресурс]. – Режим доступа : http : // www.mywebs.su/blog/safety/10946.html.

Отримано 02.03.2015