УДК 346.12

Шостко Олена Юріївна –
доктор юридичних наук, професор,
професор кафедри кримінології та кримінально-виконавчого права
Національного юридичного університету
імені Ярослава Мудрого

Olena Yu. Shostko –
doctor of juridical sciences, professor,
professor of criminology and penitentiary law department,
Yaroslav Mudryi National Law University
(77 Pushkinska St., Kharkiv, 61024, Ukraine)

Мак Аліна Олегівна –
студентка 1 курсу магістратури
Інституту прокуратури та кримінальної юстиції
Національного юридичного університету
імені Ярослава Мудрого

Alina O. Mak –
1st year Master's student of
the Criminal Justice and Prosecutors' Training Institute
Yaroslav Mudryi National Law University
(77 Pushkinska St., Kharkiv, 61024, Ukraine)

Шахрайство з використанням електронних платіжних систем: схеми та шляхи запобігання

Стаття присвячена новітньому способу вчинення шахрайств. В роботі наводяться статистичні дані щодо загальної кількості злочинів за статтею 190 Кримінального кодексу України, зокрема, й за частиною третьою цієї статті, об'єктивна сторона якої охоплює вчинення шахрайства з використанням електронних платіжних систем. Зазначаються причини високої латентності цього виду злочину, а також причини складності викриття шахрайств з використанням електронних платіжних систем. Авторами також надаються власні практичні поради, які допоможуть не стати жертвою цього злочину.

Ключові слова: *злочини проти власності, шахрайство, електронні платіжні системи, «QIWI», банківський ідентифікаційний номер, міжнародне співробітництво з правових питань.*

Статья посвящена новейшему способу совершения мошенничеств, а именно, с помощью электронных платежных систем. В работе приводятся статистические данные относительно общего количества преступлений по статье 190 Уголовного кодекса Украины, уточняется также количество преступлений по ч.3 ст.190 УК, объективная сторона которой охватывает совершение мошенничества с использованием электронных платежных систем. Указываются причины высокой латентности этого преступления, а также причины сложности разоблачения мошенничества с использованием электронных платежных систем. Также авторами предоставляются собственные практические советы, которые помогут не стать жертвой такого правонарушения.

Ключевые слова: *преступления против собственности, мошенничество, электронные платежные системы, «QIWI», банковский идентификационный номер, международное сотрудничество по правовым вопросам.*

O.Yu. Shostko, A.O. Mak Frauds with the Use of Electronic Payment Systems: the Schemes and the Ways of Prevention

The article is devoted to the latest method of committing frauds – by use of electronic payment systems. The authors provided official statistical data of the total number of crimes under Article 190 of the Criminal Code of Ukraine - "Fraud", and the number of crimes under Para. 3 of Article 190 of the Criminal Code – "Fraud by Use of Electronic Payment Transaction" (45 735 and 3578 respectively). The total number of frauds has increased by 8 times in 2016 as compared with 1990.

The authors propose their view as to the reasons of high latency of this crime. Among them are distrust in law enforcement bodies efficiency and reluctance to look like a deceived person in the eyes of the immediate surroundings. The reasons of difficulties of detecting this type of frauds are also analyzed. According to the authors, the main reason is an uncomplicated procedure of identifying in electronic payment systems. It should be emphasized the current construction of Para. 3 of Article 190 of the CCU is outdated, because it is not adapted to the realities of the development of technical progress.

The authors give their own practical advices about the prevention of frauds with use electronic payment systems. These advices could help not to become a victim of such an offense. The authors noted about special sites, where a person can find information about the bank, through which the transaction takes place. In conclusion emphasized the need to implement measures to prevent frauds (situational prevention) as well as measures to informing the public about schemes of widespread frauds.

Keywords*: property crimes, fraud, modern fraud schemes, electronic payment systems, «QIWI», Bank Identification Number, international legal cooperation.*

Постановка проблеми. Шахрайство – це злочин проти власності, жертвами якого щорічно стають десятки тисяч осіб в Україні. Специфіка злочину полягає в тому, що злочинці постійно оновлюють схеми вчинення шахрайств, саме тому запобігання даному виду злочину є ускладненим. Розвиток електронно - обчислювальної техніки спричинив створення нових надзвичайно ускладнених схем шахрайства. В контексті цього слід зазначити, що останнім часом надзвичайно популярними стали розрахунки через електронні платіжні системи. За допомогою таких систем можливо проводити транзакції у мережі Інтернет, що значно полегшує здійснення операцій для користувачів. На жаль, електронні платіжні системи досить часто використовуються шахраями для реалізації їх незаконної діяльності. Саму тому надзвичайно актуальним наразі є дослідження таких схем, а також надання порад, які б допомогли громадянам не стати жертвою цього виду шахрайства.

Аналіз останніх досліджень та публікацій. Питання кваліфікації шахрайств, їх кримінологічної характеристики в Україні (кількісно-якісні статистичні показники, вивчення особистості злочинця), різні напрями віктимологічної профілактики досліджували у своїх працях такі науковці як І.Г.Богатирьов, Д.В.Верещагин, В.Л.Давиденко, О.О.Дудоров, Б.Д.Завидов, Р.А.Запорожець, Н.Д.Ковбенко, О.В.Кравченко, О.В.Лисоєд, І.С.Мірошніченко, В.О.Навроцький, В.В.Пивоваров, К.Л.Попов, А.В. Савченко.

Невирішені раніше проблеми. У працях зазначених вище науковців увага приділяється, головним чином, традиційним видам шахрайств. На жаль, не є достатньою кількість досліджень, які стосуються новітніх схем шахрайств. Автори, які досліджують сучасні шахрайства, приділяють увагу, головним чином, учиненню шахрайств з використанням банківських карток. Але в той же час детально не аналізуються ризики при альтернативних видах розрахунків, зокрема, з використанням електронних платіжних систем.

Мета роботи: проаналізувати офіційну статистичну звітність, дослідити особливості вчинення шахрайств за допомогою електронних платіжних систем, з'ясувати, чому розкриття таких шахрайств є ускладненим для правоохоронних органів, а також сформулювати низку порад щодо того, як не стати жертвою шахраїв в аналогічних випадках.

Виклад основного матеріалу. Кількість злочинів проти власності в нашій державі є стабільно високою. На підтвердження даного твердження наведемо дані Єдиного звіту про кримінальні правопорушення за 2016 р. (форма №1). Облікована кількість злочинів проти

власності в України за цей рік становила 379 567 тис., серед них найбільшу питому вагу складають крадіжки – 76,9% (304 697 злочинів). Шахрайства становлять 11,5% (45 735 злочинів), грабежі та розбої відповідно 6,4% (25 528 злочинів) та 0,9% (3607 злочинів), 4,3% – інші [1]. Проте слід враховувати, що мова йде лише про злочини, що стали відомі правоохоронним органам і обліковані ними. Достеменно невідомо, скільки випадків шахрайств залишились поза увагою офіційної звітності.

Отже, шахрайство є другим за поширеністю злочином проти власності, саме тому кримінологічне дослідження цього злочину є надзвичайно актуальним. Згідно з офіційними даними Генеральної прокуратури України, із 45 764 облікованих шахрайств, лише у 7 844 кримінальних справах особам було вручено підозру. Це свідчить про те, що у 83% проваджень за ст.190 КК України навіть не було виявлено ймовірно винних у скоєнні злочину.
Але ще більше вражає кількість закритих кримінальних проваджень за цією статтею на стадії досудового розслідування - 41 375 (що становить 90,4 %).

Досить красномовним є порівняння кількості вчинених шахрайств в Україні за останні роки із аналогічними показниками дев'яностих років минулого століття. У 1990 р. було виявлено 5 668 таких злочинів (3,7% серед злочинів проти приватної власності та 1,5% у структурі всієї зареєстрованої злочинності), у 1996 р. – 10 917 (відповідно 4,3 % та 1,8%), у 1997 р. – 18 051 (відповідно 7,6 та 3,1%) [2, 149-152]. Якщо порівняти кількість вчинених шахрайств у 2016 з показниками 1990 р,, то чисельність таких посягань за 25 років незалежності України зросла більш ніж увосьмеро. Звичайно, цьому сприяли економічні проблеми, зокрема, викривлене впровадження елементів ринкової економіки, а розвиток сучасних технологій полегшив процес вчинення шахрайств.

Саме у зв'язку з розвитком новітніх технологій до чинного КК України було включено частину 3 ст. 190, яка виокремлює як самостійний склад злочину шахрайство, вчинене шляхом незаконних операцій з використанням електронно–обчислювальної техніки. Однак досі серед фахівців в галузі кримінального права не існує єдиного підходу щодо тлумачення поняття «електронно- обчислювальна техніка».

Комп'ютерна мережа (зокрема, Інтернет) становить сукупність територіально розосереджених систем опрацювання даних, засобів і (або) систем зв'язку та передавання даних, що забезпечує користувачам дистанційний доступ до її ресурсів і колективне використання цих ресурсів [3]. Відповідно проведення транзакцій через електронну платіжну систему, вхід та операції в якій відбувається саме за допомогою Інтернету, становить використання інформаційного ресурсу шляхом дистанційного доступу до нього, забезпечене засобами електронно-обчислювальної техніки, тобто є операцією з використанням ЕОМ.

Але частина науковців в галузі кримінального права, а також практичних працівників, не визнають використання комп'ютерної мережі та суміжної з нею мережі Інтернет як використання електронно-обчислювальної техніки. Мотивується така позиція тим, що комп'ютерна мережа не є електронно-обчислювальною технікою, а лише електронною. На наш погляд, більш доцільною видається перша позиція, а другий підхід слід визнати надто обмеженим з огляду на тлумачення поняття «електронно-обчислювальна техніка». Одночасно слід наголосити на застарілості конструкції ч. 3 ст. 190 ККУ, адже вона не пристосована до реалій розвитку технічного прогресу.

Що стосується кількості виявлених злочинів за цим складом злочину, то згідно з офіційними даними Генеральної прокуратури України, у 2016 році за ч. 3 ст. 190 ККУ було обліковано 3578 кримінальних правопорушень, підозра була оголошена особам у 878 кримінальних правопорушеннях. Закрито кримінальних проваджень в цьому році – 630, що складає 17,6 % від загальної кількості виявлених злочинів за ч.3 ст.190 ККУ.

Але фактична кількість вчинених шахрайств із використанням електронно-обчислювальної техніки є набагато більшою. Це пояснюється високою латентністю саме цього виду шахрайства, яка пов'язана з тим, що потерпілі особи переважно не повідомляють про такі випадки правоохоронним органам, а останні вибирають найлегший шлях, кваліфікуючи суперечливе кримінальне провадження за ч.1 ст.190 ККУ. Таким чином, в офіційній

статистиці не відображається реальна кількість вчинених шахрайств із використанням електронно-обчислювальної техніки.

Можна зробити висновок, що ефективність роботи правоохоронних органів щодо розкриття цього злочину є надзвичайно низькою. Слідчі, зазвичай, не бажають займатись складними справами. Типовою є ситуація, коли, наприклад, покупець через електронний платіж перерахував певну суму коштів на рахунок продавця, а останній не передав товар, привласнив кошти, заблокувавши будь-який доступ до своїх засобів зв'язку. Співробітники правоохоронних органів в таких випадках дуже часто вважають, що мають місце «цивільно-правові відносини» та невиконання зобов'язання у вигляді договору купівлі-продажу, тому слід звертатись до суду в рамках цивільного судочинства. Очевидно, що такі діяння цілком вписуються в диспозицію ч.3 статті 190 КК України, а посадові особи правоохоронних органів мають нести юридичну відповідальність за бездіяльність.

Така поведінка правоохоронців пояснюється, зокрема, й тим, що вони недостатньою обізнані з правилами кваліфікації за ч.3 ст. 190 ККУ. З огляду на конструкцію даної частини дискусійними залишаються питання щодо віднесення до електронно – обчислювальної техніки певних інформаційних ресурсів. Відсутність єдиного погляду науковців щодо цієї проблеми негативно впливає на правозастосовну практику. Один із можливих шляхів зменшення латентності злочину за ч. 3 ст. 190 ККУ – прийняття нової редакції статті, яка б враховувала новації науково - технічного прогресу.

Далі зауважимо, що зараз досить поширеною є практика замовлення товарів через онлайн - крамниці або онлайн-майданчики, в яких зібрані оголошення від приватних осіб – продавців. Сучасні шахраї використовують в своїй незаконній діяльності саме електронні платіжні системи, оскільки є очевидним, що використовувати звичайні банківські розрахунки є більш ризикованим, адже правоохоронні органи можуть встановити особу злочинця під час проведення негласних слідчий дій. Найбільш поширеними електронними платіжними системами є PayPal, Neteller, Egold, StormPay, PayAce, E-gold, WebMoney, «QIWI», Яндекс. Деньги та інші.

Далі розглянемо конкретний приклад, пов'язаний із можливостями ошукування громадян через відому російську електронну платіжну систему «QIWI», яка офіційно заборонена в Україні, але яка реально працює і якою користуються тисячі українських споживачів. Які ризики чекають на осіб, які хочуть скористатись нею?

Щоб розпочати роботу, перш за все, необхідно знайти сайт цієї платіжної системи. Для цього достатньо зазначити в пошуку назву й потім перейти по першому посиланню. Для авторизації необхідно зазначити свій номер телефону, далі на цей номер приходить смс-оповіщення з необхідним кодом. Після його зазначення, особа має доступ до абсолютно всіх можливостей платіжної системи. На цьому ідентифікація особи закінчується. Непотрібно, за аналогією з банками, надавати паспорт, ідентифікаційний код, фотографуватись із банківською карткою тощо. Для того, щоб дізнатись реквізити своєї карти, достатньо ввімкнути послугу відправки таких реквізитів на телефон. Необхідно зазначити, що номер такого розрахунку буде містити 16 цифр як і у звичайній банківській картці.

Досить важливим є питання: чим українських шахраїв приваблює використання цієї платіжної системи?

По-перше, юридичною адресою цієї організації зазначається місто Москва, мікрорайон Чертаново Севєрноє. У випадку, коли ошукана особа звернеться до правоохоронних органів України, останні мусять підготувати клопотання про тимчасовий доступ до речей та документів в рамках міжнародного співробітництва. Зрозуміло, що таку інформацію можна вилучити тільки у Москві. З формального боку така процедура є досить складною і довготривалою, тим паче враховуючи сучасну політичну ситуацію, пов'язану із збройною агресією Росії проти України. Саме тому правоохоронні органи визнають такі випадки шахрайства «цивільно-правовими відносинами» та закривають провадження. На що шахраї, власне кажучи, й сподіваються.

По - друге, процедура ідентифікації особистості є надзвичайно простою. Все, що необхідно від клієнта - це номер мобільного

телефону. Зазначимо, що в Україні більшість номерів не пов'язані із конкретною особою. Найчастіше шахраї для проведення своїх злочинних оборудок спеціально купляють нову картку та періодично змінюють її. Тобто, навіть якщо правоохоронні органи встановлять номер телефону такої особи – знайти її буде майже нереально, оскільки цілком можливо, що номер мобільного телефону вже давно є неактивним.

Слід звернути увагу і на те, що більшість громадян не обізнані з особливостями в номерах платежів. Як вже зазначалось, однакову кількість цифр необхідно ввести як під час розрахунку через звичайний банк, так і через платіжну систему. Особа найчастіше навіть не підозрює про те, що буде перераховувати свої кошти на «QIWI».

З урахуванням вищезазначеного, наведемо деякі рекомендації, як не стати жертвою шахрайства, використовуючи електронну платіжну систему «QIWI». 1. Особа, яка збирається здійснювати Інтернет - покупки, в першу чергу, повинна запитати у продавця, через який банк буде здійснюватися оплата. Якщо у відповідь вам повідомлять, що, скажімо, через ПАТ КБ «Приватбанк», тоді слід пам'ятати, що після введення номера картки повинно висвітиться прізвище та ім'я держателя картки. Можливо й таке: шахрай зазначає, що є користувачем банку, який під час транзакції не надає особисті дані отримувача грошей, що, насправді, не відповідає дійсності. Така ситуація можлива під час перерахунку коштів саме в платіжній системі «QIWI». Тому не слід бути занадто довірливими стосовно інформації, яку повідомляє продавець щодо переказу грошей.

2. Необхідно розуміти також, що комбінація цифр в номері картки не є випадковою. Число, за допомогою якого можливо визначити банк, називається БІН - банківський ідентифікаційний номер. БІН платіжної картки визначається за першими 6 цифрами її номера. Існують спеціальні програми, за допомогою яких після введення цих даних стає доступною детальна інформація про рахунок. Серед найбільш ефективних слід назвати сайт, який є в загальному доступі - www.bindb.ua. Між іншим, цей веб ресурс створювався саме для запобігання шахрайствам. Тому в разі сумнівів, доцільно скористатись цим або іншими сервісами.

3. Слід пам'ятати і таке: якщо споживач буде намагатись перевести на рахунок платіжної системи «QIWI» занадто маленьку суму, то на дисплеї висвітиться досить дивне повідомлення про те, що сума операції не повинна буде меншою, ніж 10 доларів США. Зазвичай, надійні банки подібних вимог не висувають, тому така вимога є свого роду індикатором можливих шахрайських дій.

Чому так важливо встановити, що транзакція буде здійснюватися через електронну платіжну систему? Якщо ви купуєте товари в мережі Інтернет з повною або частковою передоплатою та особа надає вам реквізити для оплати рахунку, який належить до електронної платіжної системи, то є надзвичайно висока ймовірність того, що вас хочуть ошукати. Через зазначені вище причини встановити особу злочинця та розкрити такий злочин буде надзвичайно складно, шахраї це враховують при плануванні своїх незаконних дій.

Висновки. Використання певних електронних платіжних систем не слід завжди розглядати як шахрайство. Через них проводиться досить значна кількість законних операцій. Але, в той же час, полегшена процедура ідентифікації особи в цих системах робить їх сприятливим середовищем для вчинення шахрайських дій. Тому особливу увагу необхідно приділити саме ситуаційному запобіганню даному виду злочину. Важливим у цьому контексті є робота із зменшення можливостей (або ускладнення) використання легальних (економічних) ресурсів, за допомогою яких вчинюються злочини, Перед тим, як розробляти і впроваджувати запобіжні заходи, слід провести оцінку ризиків (risk assessment) вчинення шахрайств того чи іншого виду. [4, 98-101]

Нагальною потребою є інформування найбільш широкого кола осіб щодо подібних схем шахрайства шляхом виготовлення і розповсюдження відповідних інформаційних матеріалів, проведення лекцій та «круглих столів» з цього приводу. Можливо, через певний час такі платіжні системи взагалі замінять всі інші, тому цей напрямок потребує детального кримінологічного аналізу.

Список використаних джерел:

1. Єдиний звіт про кримінальні правопорушення по державі за грудень 2016 року [Електронний ресурс]. – Режим доступу : http://www.gp.gov.ua/ua/stst2011.html?dir_id=112755&libid=100820&c=edit&_c=fo#.

2. Лисодєд О. В. Про сучасне шахрайство та шляхи його попередження / О. В. Лисодєд // Актуальні проблеми формування правової держави в Україні (до 50-ї річниці Конвенції про захист прав людини та основних свобод) : тези доп. та наук. повідомл. Всеукр. наук.-практ. конф. молодих учених. – Харків, 2000. – С. 149–152.

3. Системи оброблення інформації. Основні положення. Терміни та визначення: ДСТУ 2938-94. (Чинний від 1996-01-01). – К. : Держспоживстандарт України, 1996. – 20 с.

4. Шостко О. Ю. Деякі аспекти ситуаційного запобігання організованій злочинності в Європейських країнах / О. Ю. Шостко // Науковий вісник Ужгородського національного університету. Серія «Право». – Вип. 20. – Ч. 1. – Т. 4. – 2012. – С. 98–101.

References:

1. Yedynyi zvit pro kryminalni pravoporushennia po derzhavi za hruden 2016 roku [Elektronnyi resurs]. – Rezhym dostupu : http://www.gp.gov.ua/ua/stst2011.html?dir_id=112755&libid=100820&c=edit&_c=fo#.

2. O. V. Lysodied, Pro suchasne shakhraistvo ta shliakhy yoho poperedzhennia / O. V. Lysodied // Aktualni problemy formuvannia pravovoi derzhavy v Ukraini (do 50-i richnytsi Konventsii pro zakhyst prav liudyny ta osnovnykh svobod) : tezy dop. ta nauk. povidoml. Vseukr. nauk.-prakt. konf. molodykh uchenykh. – Kharkiv, 2000. – Pp. 149–152.

3. Systemy obroblennia informatsii. Osnovni polozhennia. Terminy ta vyznachennia: DSTU 2938-94. (Chynnyi vid 1996-01-01). – K. : Derzhspozhyvstandart Ukrainy, 1996. – 20 p.

4. O. Yu. Shostko, Deiaki aspekty sytuatsiinoho zapobihannia orhanizovanii zlochynnosti v Yevropeiskykh krainakh / O. Yu. Shostko // Naukovyi visnyk Uzhhorodskoho natsionalnoho universytetu. Seriia “Pravo”. – Vyp. 20. – Ch. 1. – T. 4. – 2012. – Pp. 98–101.