

Ядром кластера виступає вокзал, оскільки він є пунктом, що забезпечує прийом пасажирів і потягів, їх розміщення, координацію, доступ громадян до станцій, платформ та інших об'єктів інфраструктури залізничного транспорту, є базою для розміщення закладів харчування, медичної допомоги, правоохоронних органів, органів забезпечення безпеки мандрівників. Формування ядра кластера як інституційного середовища для його розвитку, враховуючи особливості територіального розвитку та організаційно-правової форми кластера, є надзвичайно важливим і актуальним.

На нашу думку, співпраця підприємств залізничного кластера може забезпечуватися так званою координаційною радою, що складатиметься з представників усіх учасників кластера. Водночас члени такої координаційної ради мають представляти інтереси конкретних суб'єктів господарювання, вносити пропозиції щодо їх спільної діяльності, формувати стратегію розвитку відповідного кластера й ухвалювати рішення щодо зазначених питань. Зміст діяльності такої координаційної ради становитиме узгодження дій суб'єктів для досягнення мети кластера, а не управління діяльністю конкретного суб'єкта господарювання. Отже, координаційна рада – це орган управління вже сформованого мікрокластера, центр узгодження його розвитку.

Список використаних джерел:

1. Про публічні закупівлі. URL: <https://zakon.rada.gov.ua/laws/show/922-19#Text>.
2. Рудяга І.М. Господарсько-правове забезпечення функціонування залізничного транспорту України в умовах реформування : монографія. Харків : Юрайт, 2017. 196 с.
3. Смирнов І.Г. Процеси транспортно-логістичної кластеризації в Європейському Союзі та Україна: площини взаємодії. URL: http://www.rusnauka.com/29_DWS_2012/Economics/11_120559.doc.htm.
4. Тимоха Д.А. Державне регулювання роботи залізничного транспорту : автореф. дис. ... канд. наук з держ. упр. : 25.00.02. Харків, 2007. 20 с.

References:

1. Pro publichni zakupivli [About public procurement]. URL: <https://zakon.rada.gov.ua/laws/show/922-19#Text>.
2. Rudyaga I.M. (2017) Gospodarske pravove zabezpechennya funkcionuvannya zaliznuchnogo transportu [Economic and legal support for the functioning of railway transport in Ukraine in terms of reform]. Monografiya. Khakiv. 197 p.
3. Smirnov I.G. Procesu transpotno-logistichnoi klasterizacii v Evropekomu Soyuzi ta Ukraini [Processes of transport and logistics clustering in the European Union and Ukraine: planes of interaction]. URL: http://www.rusnauka.com/29_DWS_2012/Economics/11_120559.doc.htm.
4. Tumoha D.A. (2007) Derjavne reguluvannya robotu zaliznuchnogo transportu [State regulation of railway transport]. Author's ref. dis. ... Cand. Sciences of the state. 25.00.02. Khakiv. 20 p.

DOI <https://doi.org/10.51647/kelm.2020.3.2.26>

СПОСОБИ ВЧИНЕННЯ ШАХРАЙСТВ ІЗ ВИКОРИСТАННЯМ ЕЛЕКТРОННО-ОБЧИСЛЮВАЛЬНОЇ ТЕХНІКИ ЯК ЕЛЕМЕНТ ЇХ КРИМІНАЛІСТИЧНОЇ ХАРАКТЕРИСТИКИ

Тетяна Романенко

*ад'юнкт кафедри криміналістики та судової медицини
Національної академії внутрішніх справ (Київ, Україна)
ORCID ID: 0000-0003-2073-3466*

Анотація. Досліджено особливості способів шахрайств, учинених шляхом незаконних операцій із використанням електронно-обчислювальної техніки. Зроблено висновок, що способи здійснення шахрайств, учинених шляхом незаконних операцій із використанням електронно-обчислювальної техніки, – це сукупність дій злочинця, що полягає в певному порядку, послідовності та конкретному методі діяльності особи шахрая, спрямованих на підготовку, скоєння та приховання конкретного злочину. Не існує вичерпного переліку способів скоєння цього злочину, але найбільшого поширення останнім часом набули такі: обманне заволодіння грошима громадян; створення інтернет-аукціонів шляхом надання недостовірних даних і пропозиції продажу неіснуючих товарів; створення і забезпечення діяльності інтернет-магазину; перерахування коштів із банківських карток шляхом обманного отримання конфіденційних даних; обманне заволодіння грошовими коштами іноземних громадян; обманне заволодіння грошовими коштами шляхом створення або використання сайтів благодійних організацій, створення та діяльність фіктивних фінансових бірж.

Ключові слова: шахрайство, електронно-обчислювальна техніка, незаконні операції, спосіб злочину, криміналістична характеристика.

METHODS OF FRAUD THAT ARE USING ELECTRONIC COMPUTERS AS AN ELEMENT OF THEIR FORENSIC CHARACTERISTICS

Tetiana Romanenko

Associate Professor at the Department Forensics and Forensic Medicine

National Academy of Internal Affairs (Kyiv, Ukraine)

ORCID ID: 0000-0003-2073-3466

Abstract. The peculiarities of the methods of fraud committed by illegal operations using electronic computers have been studied. It is concluded that the methods of fraud committed by illegal operations using electronic computers – is a set of actions of the offender, which consists in a certain order, sequence and specific method of activity of the person of the fraudster aimed at preparing, committing and concealing a specific crime. There is no exhaustive list of ways to commit this crime, but the most widespread in recent years have been the following: fraudulent seizure of citizens' money; creation of online auctions by providing inaccurate data and offers to sell non-existent goods; creation and maintenance of the online store; transfer of funds from bank cards by fraudulently obtaining confidential data; fraudulent seizure of money of foreign citizens; fraudulent misappropriation of funds by creating or using the sites of charitable organizations, the creation and operation of fictitious financial exchanges.

Key words: fraud, computer technology, illegal operations, method of crime, forensic characteristics.

SPOSOBY POPEŁNIANIA OSZUSTW Z WYKORZYSTANIEM TECHNIKI ELEKTRONICZNEJ JAKO ELEMENTU ICH CHARAKTERYSTYKI KRYMINALISTYCZNEJ

Tetiana Romanenko

adiunkt Katedry Kryminalistyki i Medycyny Sądowej

Narodowej Akademii Spraw Wewnętrznych (Kijów, Ukraina)

ORCID ID: 0000-0003-2073-3466

Adnotacja. Zbadano cechy sposobów oszustw popełnianych w wyniku nielegalnych transakcji z wykorzystaniem sprzętu elektronicznego i komputerowego. Stwierdzono, że metody popełniania oszustw popełnionych w wyniku nielegalnych transakcji za pomocą sprzętu elektronicznego i komputerowego są zbiorem czynów przestępstwa, w określonych zasadach, kolejności i konkretnej metodzie działania osobowości oszusta w celu przygotowania, popełnienia i ukrycia określonego przestępstwa. Nie ma wyczerpującej listy sposobów popełnienia ww. przestępstwa, ale ostatnio najbardziej rozpowszechnione były następujące: oszukańcze przejęcie pieniędzy obywateli; tworzenie aukcji internetowych poprzez dostarczanie nieprawdziwych danych i oferowanie sprzedaży nieistniejących towarów; tworzenie i zabezpieczanie działalności sklepu internetowego; przekazywanie środków z kart bankowych poprzez oszukańcze otrzymywanie poufnych danych; oszukańcze posiadanie środków pieniężnych cudzoziemców; oszukańcze posiadanie środków pieniężnych poprzez tworzenie lub korzystanie ze stron organizacji charytatywnych, tworzenie i prowadzenie fikcyjnych giełd finansowych.

Słowa kluczowe: oszustwa, sprzęt elektroniczny, transakcje nielegalne, sposób przestępstwa, charakterystyka kryminalistyczna.

Вступ. У сучасному світі, пов'язаному з бурхливим розвитком науково-технічного прогресу, шахрайство набуває все більшого поширення, водночас впливає майже на всі сфери суспільного життя. Через недостатнє наукове дослідження сучасних способів шахрайств, учинених шляхом незаконних операцій із використанням електронно-обчислювальної техніки, виникає багато труднощів як у правоохоронних органів, так і судів у процесі розкриття, розслідування та правильної правової кваліфікації цих діянь.

У криміналістичній науці вважається загальноприйнятим той факт, що спосіб скоєння злочину є основоположним і системоутворювальним елементом криміналістичної характеристики, що характеризує будь-який злочин, зокрема й шахрайство, учинене шляхом незаконних операцій із використанням електронно-обчислювальної техніки. Під час володіння інформацією про спосіб скоєння злочину з'являється можливість висувати обґрунтовані версії про зміст інших елементів криміналістичної характеристики конкретного злочину. Встановлення способу скоєння злочину дасть змогу вибрати необхідний напрям у розслідуванні (Dudnikov, 2017: 42).

Основна частина. Вивченню про спосіб злочину в різний час приділяли увагу в наукових дослідженнях Ю.П. Алєнін, В.П. Бахін, Р.С. Белкін, В.Ф. Єрмолович, Н.І. Клименко, В.О. Коновалова, М.А. Погорецький, М.В. Салтєвський, В.Ю. Шепітько та інші. Проте окремі криміналістичні особливості способів шахрайств, учинених шляхом незаконних операцій із використанням електронно-обчислювальної техніки, розглядали у своїх наукових працях Р.С. Атаманов, С.М. Князєв, Т.А. Пазинич, В.П. Сабадаш, М.М. Федотов, С.С. Чернявський. Незважаючи на те, що проведені ними дослідження є вагомим внеском у вивчення особливостей способу скоєння цього злочину та сприяють його розслідуванню, однак на практиці виникають проблеми в розкритті, розслідуванні та правильній кваліфікації, що потребує більш глибокого та комплексного наукового дослідження способів учинення шахрайств шляхом незаконних операцій із використанням електронно-обчислювальної техніки, що й зумовлює актуальність теми статті.

Метою статті є визначення особливостей такого елементу криміналістичної характеристики шахрайств, учинених шляхом незаконних операцій із використанням електронно-обчислювальної техніки, як спосіб скоєння злочину, розкриття й характеристика його змісту та здійснення класифікації способів скоєння злочинів, передбачених ч. 3 ст. 190 Кримінального кодексу України (далі – КК України).

Спосіб злочину – це спосіб дій злочинця, що виражається в певній системі операцій і прийомів. Як зазначає В.Ю. Шепітько, спосіб злочину являє собою збірне поняття. Його структура охоплює: способи готування до злочинного діяння, способи його вчинення і способи приховання (маскування). Спосіб злочину не завжди має повну структуру, адже існують злочини, які можуть скоюватися без попередньої підготовки або не мають на меті наступного приховання події чи слідів (Panov, Shepitko, Konovalova, 2011: 215).

Дослідження способів учинення шахрайств шляхом незаконних операцій із використанням електронно-обчислювальної техніки, на думку С.С. Чернявського, виступає своєрідним «ключем» до описання інших значущих елементів криміналістичної характеристики (Cherniavskiy, 2010: 9). Проте способи вчинення шахрайств шляхом незаконних операцій із використанням електронно-обчислювальної техніки значно відрізняються від способів учинення інших кримінальних правопорушень, пов'язаних із шахрайством, які потрібно відмежувати, зокрема: завдання майнової шкоди шляхом обману або зловживання довірою (ст. 192 КК України); шахрайства з фінансовими ресурсами (ст. 222 КК України); несанкціоноване втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку (ст. 361 КК України); несанкціонованих дій з інформацією, яка обробляється в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або зберігається на носіях такої інформації, скоєні особою, яка має право доступу до неї (ст. 362 КК України).

Як показує аналіз слідчої та судової практики, для шахрайств, учинених шляхом незаконних операцій із використанням електронно-обчислювальної техніки, більш характерна така форма вчинення, як заволодіння грошовими коштами. В інших випадках шахраї спонукають потерпілого передати своє майно шляхом обману.

Власний практичний досвід, аналіз слідчої та судової практики, а також наукових досліджень дав змогу виділити кілька типових способів шахрайств, учинених шляхом незаконних операцій із використанням електронно-обчислювальної техніки, які нині поширені на території України.

Створення інтернет-аукціонів шляхом надання недостовірних даних і пропозиції продажу неіснуючих товарів. Завзвичай злочинці реєструються на вебсайтах інтернет-аукціонів, найчастіше на «Aukro.ua», «Емаркет Україна» (olx.ua). Водночас шахраї використовують анкетні дані близьких або сторонніх осіб. Після цього на сайті під своїм доменним іменем розміщують лот, до якого завантажують фото товару з максимальною вартістю та початковою ставкою, де учасники інтернет-аукціону, потенційні жертви, дистанційно ставлять ставки на сайті вказаного товару. Після завершення торгів шахрай зв'язується з жертвою на сайті інтернет-аукціону, однак часто спілкування може здійснюватися через листування електронною поштою або мобільний зв'язок. Після домовленості в ціні шахрай надає жертві реквізити банківського рахунку для оплати товару та послуг пересилання, однак у кінцевому результаті після перерахування коштів жертва товару не отримує. Шахрай із метою приховання процесу злочинних дій і самовикриття може використовувати банківські картки інших осіб та надалі переводить у готівку шляхом зняття коштів із банкомату. Більш досвідчені злочинці з метою приховання свого місця знаходження постійно змінюють IP-адреси, що створює труднощі у встановленні місця перебування шахрая (Schemes “Out-of-OLX” fraud + infographics, <https://www.ema.com.ua/citizens/cyber-safety-school/shemi-out-of-olx-shahrajstva-infografika>).

Перерахування коштів із банківських карток шляхом обманного отримання конфіденційних даних. Для вчинення вказаного виду шахрайства шляхом незаконних операцій із використанням електронно-обчислювальної техніки злочинці на сайтах інтернет-торгівлі підшукують жертв. Знайшовши інформацію потенційної жертви про продаж товарів, шахраї встановлюють з нею контакт. Під час розмови з жертвою шахраї неправдиво повідомляють, що будуть здійснювати купівлю товарів, та для перерахунку грошових коштів за покупку дізнаються номер її банківського карткового рахунку. Після чого шахрай телефонує жертві та назвавшись працівником банку, повідомляє інформацію про неможливість перерахунку коштів на картку потерпілої. Після цього під час телефонної розмови неправдиво повідомляють, що для зарахування грошових коштів їй необхідно повідомити конфіденційні дані банківської картки (анкетні дані жертви, захисний код картки та дівоче прізвище матері) або підійти до терміналу банкомата й виконати необхідні операції для нібито зарахування коштів на її банківську картку. Під час розмови телефоном із жертвою шахрай диктує відповідні комбінації, які остання виконує, та шляхом обману і незаконних операцій із використанням електронно-обчислювальної техніки отримує грошові кошти.

Надалі шахрай, використовуючи електронні платіжні системи мережі Інтернет («Портмоне», ГлобалМані, EasyPay, LiqPay, iPay.ua, Простір), перераховує грошові кошти з карткового рахунку потерпілої на свій банківський рахунок або рахунок третіх осіб, яким навіть не відомо, що з їхніми банківськими картками проводяться злочинні операції. Для того щоб жертва відразу не дізналась, що щодо неї вчинено шахрайство, злочинці надсилають на її мобільний номер SMS про зарахування коштів на банківську картку (Skachko, 2017).

Обманне заволодіння грошовими коштами шляхом створення або використання сайтів благодійних організацій. Під час використання благодійних сайтів злочинці надсилають листи від імені благодійних організацій або людей, яким потрібна допомога. Водночас посилання можуть належати реальним благодійним фондам, але реквізити для перерахування коштів належать шахраям.

Крім того, злочинці шляхом незаконних операцій із використанням електронно-обчислювальної техніки створюють сайти благодійних організацій, на яких публікують оголошення з проханням про матеріаль-

ну допомогу на лікування хворим дітям. Також шахраї на вказаних сайтах можуть розміщувати вигадану інформацію стосовно хвороби, водночас розміщують чужі фотографії людей, які потребують фінансової допомоги на лікування, або копіюють оголошення із сайтів благодійної допомоги, які належать реальним людям, змінюючи реквізити для перерахування грошей (Pazynych, 2006: 78).

Створення і забезпечення діяльності інтернет-магазину. Під час створення сайту інтернет-магазину шахрай може діяти як самостійно, так і у складі злочинної групи. Це більш складний спосіб, ніж продаж товарів на інтернет-аукціоні, і складається з декількох етапів.

Спочатку шахраї створюють у мережі Інтернет сайти у вигляді інтернет-магазинів – аналогів вебсайтів, що діяли на території України чи інших держав та які функціонували б на території України. На вказаних сайтах розміщують завідомо неправдиву інформацію у вигляді оголошень щодо продажу товарів, яких у наявності ніколи не було.

Наступним етапом є створення та отримання контролю над фіктивними підприємствами, відкриття банківських рахунків, на які замовники/клієнти фіктивних інтернет-магазинів надалі здійснюють передоплату у вигляді грошового переказу за придбання замовленого товару за реквізитами належних їм пластикових карток, відкритих у банках України. Водночас назви фіктивних підприємств повинні бути схожими до назв фіктивних інтернет-магазинів, щоб викликати довіру в користувачів.

Після цього здійснюється оформлення договорів з операторами телефонного зв'язку про надання послуг зв'язку та інтернет-зв'язку так званої «Сіп-телефонії», телефонні номери яких слугують для зворотного зв'язку із замовниками інтернет-магазинів. Водночас у вхідних дзвінках на телефони замовників фіктивних інтернет-магазинів відображаються міські номери телефонів, що викликає довіру в користувачів.

Надалі вчиняються дії зі створення, організації та забезпечення діяльності структурної частини злочинної групи, а саме «кол-центру», оператори якого спілкуються з клієнтами, імітуючи діяльність кол-центрів справжніх інтернет-магазинів, приймають замовлення та надають реквізити для перерахування грошових коштів. Крім того, шахраї розробляють спеціальну веб-сторінку з базою даних для роботи організаторів та операторів «кол-центру», за допомогою якої злочинці приймають і ведуть облік замовлень. Після вчинення шахрайських дій так звані оператори «кол-центру» заносять телефонні номери ошуканих клієнтів до «чорного списку», щоб вони не заважали роботі «кол-центру» та якнайдовше не здогадувалися, що щодо них було скоєно шахрайство.

На завершальному етапі підготовки до скоєння злочину та під час безпосередньої протиправної діяльності здійснюється добір учасників злочинної групи для вчинення шахрайств шляхом незаконних операцій із використанням електронно-обчислювальної техніки (Judgment of the Primorsky District Court of Odessa of September 15, 2016 № 63418296).

Створення та діяльність фіктивних фінансових бірж. Діяльність таких бірж забезпечується діяльністю злочинної групи, яка складається та маскується за офіційно зареєстрованими підприємствами. Зловмисники використовують методи агітаційного характеру для залучення громадян до інвестування коштів у торгівлю на фінансових ринках. Шахраї пропонують потенційним клієнтам купувати цінні папери для отримання прибутку. Використовуючи бренди «hqbroker» та «trade12», злочинці задіюють різні вебресурси для імітації добросовісної ділової репутації. Після цього так звані брокери створюють у потерпілого помилкове уявлення про процес здійснення торгів на світових біржах. Для цього вони використовують уже встановлене на комп'ютері потерпілого спеціальне програмне забезпечення для проведення торгів, яке фактично надає можливість здійснювати віддалений контроль за його комп'ютером. Такі компанії створюють уявлення в потерпілих про співпрацю з іноземними компаніями, які торгують цінними паперами та які є учасниками фондового ринку й мають відповідні дозволи та ліцензії на здійснення зазначеної діяльності у світі. Такими діями злочинці спонукають потерпілого вносити свої кошти на рахунок шахрайського торговельно-сервісного підприємства, переслідуючи мету – заволодіння його коштами під приводом укладання угод із купівлі-продажу цінних паперів.

Крім того, аналогічним способом учасники групи організують діяльність офісів для «операторів», «технічних працівників» і «брокерів». Такі офіси можуть розміщувати в різних містах. Свою діяльність шахраї «прикривають» офшорною компанією. Для здійснення злочинної діяльності злочинці використовують спеціально створений для цього онлайн-ресурс (інтернет-майданчик), де нібито відбувалися успішні онлайн-торги валютними парами (бінарні опціони). За схемою потенціальному клієнту пропонують узяти участь у торгах шляхом відкриття спеціального демо-рахунку, де організаторами створюється імітація успішних торгів. Після цього особу шляхом обману скеровують на відкриття реального рахунку. Водночас із потерпілими працюють «оператори» офісу, які націлюють їх на внесення якомога більших внесків. Аргументують це більшою вірогідністю виграшу. Для досягнення цієї мети зловмисники використовують заздалегідь прописану схему психологічного впливу на жертву. Вклавши гроші, потерпілі не мають можливості їх «зняти». У цьому випадку вони можуть лише поповнювати рахунки. Система працює так, що всі торги призводять до повної втрати грошей користувачів (Samoilov, 2014: 7).

Висновки. Підбиваючи висновки, зазначимо, що способи здійснення шахрайств, учинених шляхом незаконних операцій із використанням електронно-обчислювальної техніки, – це сукупність дій злочинця, що полягає в певному порядку, послідовності та конкретному методі діяльності особи шахрая, спрямованих на підготовку, скоєння та приховання конкретного злочину. Не існує вичерпного переліку способів скоєння цього злочину, але найбільшого поширення останнім часом набули такі: обманне заволодіння грошима

громадян; створення інтернет-аукціонів шляхом наданням недостовірних даних і пропозиції продажу неіснуючих товарів; створення й забезпечення діяльності інтернет-магазину; перерахування коштів із банківських карток шляхом обманного отримання конфіденційних даних; обманне заволодіння грошовими коштами іноземних громадян; обманне заволодіння грошовими коштами шляхом створення або використання сайтів благодійних організацій, створення та діяльність фіктивних фінансових бірж. Вказаний перелік способів не є вичерпним, що зумовлює потребу в подальшому науковому дослідженні.

Зі свого боку, дослідження способів учинення шахрайств шляхом незаконних операцій із використанням електронно-обчислювальної техніки доцільно використовувати в практичній діяльності правоохоронних органів, оскільки воно сприятиме швидкому, повному та всебічному розкриттю і розслідуванню цієї категорії злочинів.

Список використаних джерел:

1. Вирок Приморського районного суду м. Одеси від 15 вересня 2016 р. № 63418296. *Єдиний державний реєстр судових рішень*. URL: <http://www.reyestr.court.gov.ua/Review/63418296>.
2. Дудніков А.Л. Спосіб злочину у сфері економічної діяльності як системоутворюючий елемент криміналістичної характеристики. *Теорія та практика судової експертизи і криміналістики*. 2017. Вип. 17. С. 39–47.
3. Настільна книга слідчого : Наук.-практ. видання для слідчих і дізнавачів / Панов М.І., Шепітько В.Ю., Коновалова В.О. та ін. Київ : Видавничий Дім «Ін Юре», 2011. 728 с.
4. Пазинич Т.А. Криміналістична характеристика шахрайств та основні положення їх розслідування : дис. ... канд. юрид. наук : 12.00.09. Харк. нац. ун-т внутр. справ. Харків, 2006. 215 с.
5. Самойлов С.В. Розслідування шахрайств, учинених із використанням мережі «Інтернет» : автореф. дис. ... канд. юрид. наук : 12.00.09; Донецьк. юрид. ін-т МВС України. Донецьк, 2014. 18 с.
6. Скачко Є.Ю. Топ-5 новин в сфері шахрайства з платіжними інструментами. 26.05.2017. URL: <https://pingvin.pro/gadgets/article-gadget/top-5-novyn-v-sferi-shahrajstva-z-platizhnymy-instrumentamy-13.html>.
7. Схеми «Out-of-OLX» шахрайства + інфографіка. *Український сайт міжбанківської асоціації членів платіжних систем ЄМА*. URL: <https://www.ema.com.ua/citizens/cyber-safety-school/shemi-out-of-olx-shahrajstva-infografika>.
8. Чернявський С.С. Теоретичні та практичні основи методики розслідування фінансового шахрайства : автореф. дис. ... д-ра юрид. наук : 12.00.09. Нац. акад. внутр. справ. Київ, 2010. 21 с.

References:

1. Vyrok Prymorskoho raionnoho sudu m. Odesy vid 15 veresnia 2016 r. № 63418296 [Judgment of the Primorsky District Court of Odessa of September 15, 2016 № 63418296]. *Yedynyi derzhavnyi reiestr sudovykh rishen*. URL: <http://www.reyestr.court.gov.ua/Review/63418296>.
2. Dudnikov A.L. (2017) Sposib zlochynu u sferi ekonomichnoi diialnosti yak systemoutvoriuiuchy element kryminalistychnoi kharakterystyky [The method of crime in the field of economic activity as a system-forming element of forensic characteristics]. *Teoriia ta praktyka sudovoi ekspertyzy i kryminalistyky*. Vyp. 17. P. 39–47.
3. Panov M.I., Shepitko V.Yu., Konovalova V.O. (2011) Nastilna knyha slidchoho [Investigator's desk book]. Nauk.-prakt. vydannia dlia slidchykh i diznavachiv. K. : Vydavnychy Dim "In Yure". 728 p.
4. Pazynych T.A. (2006) Kryminalistychna kharakterystyka shakhraistv ta osnovni polozhennia yikh rozsliduvannia [Forensic characteristics of fraud and the main provisions of their investigation]: dys. ... kand. yuryd. nauk: 12.00.09. Khark. nats. un-t vnutr. sprav. Kh. 215 p.
5. Samoilov S.V. (2014) Rozsliduvannia shakhraistv, uchynenykh iz vykorystanniam merezhi "Internet" [Investigation of fraud committed using the Internet] : avtoref. dys. ... kand. yuryd. nauk : 12.00.09. Donetsk. yuryd. in-t MVS Ukrainy. Donetsk. 18 p.
6. Skachko Ye. Yu. (2017) Top-5 novyn v sferi shakhraistva z platizhnymy instrumentamy [Top 5 news in the field of fraud with payment instruments.]. URL: <https://pingvin.pro/gadgets/article-gadget/top-5-novyn-v-sferi-shahrajstva-z-platizhnymy-instrumentamy-13.html>.
7. Skhemy "Out-of-OLX" shakhraistva + infografika [Schemes "Out-of-OLX" fraud + infographics]. *Ukrainskyi sait mizhbankivskoi asotsiatsii chleniv platizhnykh system YeMA* URL: <https://www.ema.com.ua/citizens/cyber-safety-school/shemi-out-of-olx-shahrajstva-infografika/>.
8. Cherniavskiy S.S. (2010) Teoretychni ta praktychni osnovy metodyky rozsliduvannia finansovoho shakhraistva [Theoretical and practical bases of methods of investigation of financial fraud]: avtoref. dys. ... d-ra yuryd. nauk: 12.00.09. Nats. akad. vnutr. sprav. K. 21 p.