УДК: 343.98
ORCID: 0000-0003-1861-8354
e-mail: gull_ukr@ukr.net

Larysa P. Grynko,
Associated Professor of the Department of Criminal Law and Criminal Law Disciplines
(Poltava Law Institute of TheYaroslav Mudryi National Law University)

Гринько Лариса Петрівна,
доцент кафедри кримінального права та кримінально-правових дисциплін
(Полтавський юридичний інститут Національного юридичного університету імені Ярослава Мудрого)

ШАХРАЙСТВО В МЕРЕЖІ ІНТЕРНЕТ: СПОСОБИ ВЧИНЕННЯ

ONLINE FRAUD: METHODS OF COMMITTING

Анотація. У статті досліджено особливості способів шахрайств, учинених через мережу Інтернет. Проаналізовано судову практику та позиції вчених-криміналістів з окресленої проблематики. Наголошено, що не існує вичерпного переліку способів досліджуваної тематики, оскільки наявний науково-технічний прогрес породжує виникнення нових способів вчинення шахрайств, злочинці утворюють все більш складні схеми вчинення злочину і, як наслідок, суттєво зростає складність його розкриття та розслідування. Досліджуваний злочин характеризується високою латентністю, насамперед, через різноманітність реалізації шахрайських схем в Інтернеті, складнощів виявлення особи злочинця. Встановлено, що аналізованому шахрайству притаманне одночасно обман та зловживання довірою. За результатами проведеного дослідження виділено способи, які застосовують злочинці при вчинення шахрайств в мережі Інтернет. Найбільшого поширення останнім часом набули такі: використання сайтів двійників; створення або використання інтернет-магазинів та інших сайтів; використання втрачених чи вкрадених карток; отримання інформації на

електронну пошту про виграш в лотерею чи спадкування коштів у великих розмірах; отримання загрози про блокування комп'ютера, телефону чи загроза передання компрометуючої інформації; створення або використання сайтів благодійних організацій; створення фіктивних брокерських сайтів. Вчинення шахрайств через мережу Інтернет є одним з найбільш розповсюджених видів даного кримінального правопорушення. Аналіз існуючих способів надасть можливість розробити практичні рекомендації для подальшого розслідування та розкриття цього різновиду кримінальних правопорушень. Накопичення знань про спосіб вчинення шахрайства через мережу Інтернет дозволить з'ясувати механізм вчинення злочину, слідову картину, дослідити особу злочинця, що є важливим джерелом відомостей про шахрайства, що вчинюються через мережу Інтернет.

Ключові слова: шахрайство, комп'ютерні технології, шахрайство в мережі Інтернет, кіберзлочини, способи вчинення шахрайства.

Summary. The article examines the features of the methods of fraud committed via the Internet. Analyzed judicial practice and positions of criminologists on the outlined issues. Emphasized that there is no exhaustive list of methods of research, as existing scientific and technological progress gives rise to new ways of committing fraud, criminals form increasingly complex schemes of crime and, consequently, significantly increases the complexity of its detection and investigation. The crime that was research is characterized by high level of latency, primarily due to the variety of implementation of fraudulent schemes on the Internet, the difficulty of identifying the offender. It is established that the analyzed fraud is characterized by both deception and abuse of trust. Identified methods that used by criminals in committing fraud on the Internet. In recent years the most common are: the use of duplicate sites; creation or use of online stores and other sites; use of lost or stolen cards; receiving information by e-mail about winning the lottery or inheriting funds in large amounts; receiving a threat of blocking a computer, telephone or threatening to pass compromising

information; creation or use of charity sites; creation of fictitious brokerage sites. Means of committing fraud via the Internet are the most common types of this criminal offense. Analysis of existing methods will provide an opportunity to develop practical recommendations for further investigation and detection of this type of criminal offense. Accumulation of knowledge about the method of committing fraud via the Internet will allow to find out the mechanism of committing a crime, a trace, to investigate the identity of the offender, which is an important source of information about fraud committed via the Internet.

Keywords: fraud, computer technology, Internet fraud, cybercrime, methods of committing fraud.

Постановка проблеми. Сьогодні важко уявити світ без комп'ютерної мережі. В інтернеті розміщена величезна кількість інформаційних ресурсів і послуг, які охопили майже всі сфери життя людини. Водночас, така online-активність призвела до зростання великої кількості злочинів, у тому числі й шахрайства. При цьому, найбільшого сплеску злочинна діяльність досягла в період карантину, коли на тлі запровадження он-лайн форми, все більше людей почали використовувати мережу Інтернет, що призвело до зростання кіберзлочинів (різноманітні види шахрайства, крадіжки грошей з банківських рахунків, розповсюдження комп'ютерних вірусів та інші кримінальні правопорушення). За статистичними даними Національної поліції України минулого 2020 року було зареєстровано понад 5 тисяч кіберзлочинів, у яких вдалося оперативно затримати 106 фігурантів кримінальних проваджень, надійшло понад 100 тисяч дзвінків та більше 40 тисяч електронних звернень [1].

Одним з найбільш вчинюваних кримінальних правопорушень через мережу Інтернет є шахрайство. Відповідно до частини першої статті 190 Кримінального кодексу України шахрайство – це заволодіння чужим майном або придбання права на майно шляхом обману чи зловживання довірою [2]. Частина 3 статті 190 Кримінального кодексу України передбачає кримінальну відповідальність за

шахрайство, вчинене у великих розмірах, або шляхом незаконних операцій з використанням електронно-обчислювальної техніки.

Інтернет-шахрайство, з одного боку, є результатом еволюції традиційного шахрайства, оскільки деякі його види зустрічаються в Інтернеті без будь-яких серйозних змін в методиці реалізації злочинного замислу; з іншого боку - це якісно нова група злочинів, оскільки при схожості методів реалізації, конкретні способи мають істотні відмінності [3, с. 41]. Останнім часом, шахрайство, вчинене в мережі Інтернет, набуває все більше обертів, утворюються організовані групи, будуються все більш складні схеми вчинення злочину і, як наслідок, суттєво зростає складність його розкриття та розслідування. Досліджуваний злочин характеризується високою латентністю, насамперед, через різноманітність реалізації шахрайських схем в Інтернеті, складнощів виявлення особи злочинця та встановлення місця вчинення злочину. Тому дослідження способів вчинення досліджуваного виду шахрайства є одним з актуальних питань, яке постає сьогодні.

Стан опрацювання обраної проблематики, аналіз останніх публікацій та досліджень. Дослідженню шахрайства через мережу Інтернет присвятили свої наукові праці А. І. Анапольська, Р. С. Атаманов, С. В. Головкін, С. М. Князєв, Н. Ю. Кириленко, С. М. Князєв, А. В. Крижевський, О. В. Курман, О. Л. Мусієнко, Т. В. Охрімчук, Т. А. Пазинич, В. П. Сабадаш, С.В. Самойлов, М. М. Федотов, С. С. Чернявський та інші. Однак, це питання не втрачає своєї актуальності. Навпаки, розвиток суспільних відносин через мережу Інтернет породжує нові способи шахрайств, що зумовлюють необхідність подальшого наукового пошуку шляхів їх виявлення, розкриття та розслідування.

Метою статті є дослідження способів вчинення шахрайств через мережу Інтернет як ключового елементу криміналістичної характеристики досліджуваного виду злочину.

Виклад основного матеріалу. Шахрайство в мережі Інтернет має істотні відмінності від звичайного шахрайства, оскільки дає перевагу останньому в

виборі місця його вчинення, тактики його дій, вибором жертв та можливостей для підвищення його максимальної анонімності. Безперечно спосіб вчинення цього кримінального правопорушення теж залишається за шахраєм.

На способи вчинення шахрайства неодноразово звертали увагу вчені-криміналісти. Так, Т. Романенко, до способів шахрайства, учиненого шляхом незаконних операцій із використанням електронно-обчислювальної техніки, які нині поширені на території України, відносить: створення інтернет-аукціонів шляхом надання недостовірних даних і пропозиції продажу неіснуючих товарів; перерахування коштів із банківських карток шляхом обманного отримання конфіденційних даних; заволодіння шляхом обману грошовими коштами через створення або використання сайтів благодійних організацій; створення і забезпечення діяльності інтернет-магазину; створення та діяльність фіктивних фінансових бірж [4, с. 146-147].

Розглядаючи способи вчинення шахрайств, учинених із використанням мережі інтернет, С.В. Самойлов поділяє їх за наступними підставами: а) шахрайства, які пов’язані із купівлею/продажом у мережі «Інтернет»; б) шахрайства, сутність яких полягає в отриманні коштів (майна) шляхом надсилання листів чи повідомлень; в) шахрайства, які для заволодіння коштами (майном) потребують розробки та розміщення в мережі «Інтернет» дублікатів або вузькоспеціалізованих сайтів для надання псевдопослуг; г) шахрайства, які спрямовані на отримання персональних (реєстраційних) даних (так званий «фішинг»); д) шахрайства, пов’язані з обігом електронних грошей; є) шахрайства, для вчинення яких використовується спеціалізоване та/чи шкідливе програмне забезпечення; е) «комбіновані способи» шахрайств [5, с. 7].

Крім того, про способи шахрайства, пов’язаного з комп’ютерами (комп’ютерне шахрайство) мова йде і в Конвенції про кіберзлочинність від 23 листопада 2001 р. Відповідно до ст. 8 цієї Конвенції, шахрайство, пов’язане з комп’ютерами, – це навмисне вчинення, без права на це, дій, що призводять до втрати майна іншої особи шляхом: а) будь-якого введення, зміни, знищення чи

приховування комп'ютерних даних; б) будь-якого втручання у функціонування комп'ютерної системи, з шахрайською або нечесною метою набуття, без права на це, економічних переваг для себе чи іншої особи [6].

Аналіз судової практики по справам про шахрайства, що здійснювалося через всесвітню павутину, свідчить про те, що 80% досліджуваного злочину вчинювалось шляхом обману і лише 20% - зловживання довірою.

Обман і зловживання довірою як способи шахрайства усвідомлюються як досягнення певних проміжних результатів перед остаточним отриманням чужого майна або отриманням права на нього, а саме введення в оману власника майна таким чином, щоб злочинець згодом сам отримав майно від жертви [7, с. 54].

Обман при шахрайстві - це повідомлення завідомо неправдивих даних або приховування певних обставин, зловживання довірою – недобросовісне використання довіри потерпілого. Обман, так само як і зловживання довірою використовується для заволодіння майном чи придбання права на майно. З цього приводу, Т. А. Пазинич правильно зазначає, що обман під час шахрайства – це поведінка особи, яка свідомо спрямована на те, щоб будь-якими засобами сформувати в іншої людини уявлення, яке не відповідає дійсності, й спонукати її до передачі майна або права на нього [8, с. 7]. Зловживання довірою під час шахрайства виникає у тому разі, коли потерпілий і злочинець мають взаємовідносини, які породжують довіру між ними.

Проаналізував слідчу практику, а також дослідивши наукові праці, до найбільш розповсюджених способів шахрайств, вчинених через мережу Інтернет, слід віднести наступні.

Використання сайтів двійників. Такими сайтами, як правило, є сайти двійники відомих товариств, фірм та магазинів. Сторінка візуально виглядає як справжня. При цьому застосовують ту ж саму кольорову гаму, що й офіційний сайт. Гіперпосилання на сайт приблизно таке ж, однак містить зайві букви або цифри. Оплативши товари чи вказавши власні персональні дані на сайті-

двійнику, ви потрапляєте у пастку шахраїв. Найбільш вразливими є сайти з великою кількістю відвідувачів. Так, останнім часом все більше зустрічається інформація про сайт-двійник, який обманним шляхом списує кошти з відвідувачів сайту OLX, при замовленні послуги доставки. Зловмисник розміщує на сайті OLX оголошення про продаж популярного товару за привабливою ціною, але додатково, «на навантаження», пропонує якусь малокорисну річ. Покупець починає торгуватись, оскільки хоче купити лише основний товар, без додаткового. Обидві сторони домовляються про прийнятну ціну. Продавець створює нове оголошення, вже без товару «на навантаження», з обумовленою раніше ціною, і повідомляє покупцю у листі пряме посилання на товар, ніби-то щоб ніхто не «перехопив товар» і не купив його першим. Обман у тому, що покупцеві посилають посилання на фішинговий сайт, інтерфейс якого зовні ідентичний на сторінці оплати товару на OLX.ua. Наприклад, в одному з нещодавно зафіксованих випадків шахрайства було використано домен http://safdeal.online/olx.ua_payment. До того ж фішинговий сайт повністю повторював сторінку оплати товару через «OLX доставка» оригінального сайту, що ввело покупця в оману. Коли жертва проводила транзакцію на фішинговій сторінці ніби-то з метою покупки товару на умовах «OLX доставки», насправді вона просто переказувала гроші зі своєї картки на карту шахраїв [9].

Ще одним прикладом шахрайства є створення сайтів-двійників брендових товарів. Продавці незаконно використовують товарні знаки, копіюють дизайн магазинів або видають себе за офіційний аккаунт бренду, хоча насправді не є таким.

В іншому випадку створювалися сайти-двійники, які пропонували скидки на товари чи послуги, при цьому користувач повинен відповісти на декілька незначних питань, тим самим надаючи персональні дані, які в подальшому використовувалися проти нього. Отримавши талон зі скидкою, користувач пред’являв його в магазині, однак одержував негативну відповідь з зазначенням інформації, що ніякої акції магазин не проводив. Мета фішингу - отримання

персональних даних користувача, які можуть бути продані або використані в подальшому для викрадення грошей або особистих даних.

Створення або використання інтернет-магазинів та інших сайтів. Створюються інтернет-магазини, які пропонують різноманітні товари та послуги за ціною, яка менша ніж у інших продавців. Головна мета діяльності такого магазину - отримання часткової або повної передоплати. Після отримання передоплати магазин або перестає функціонувати, або постійно обіцяє вислати неіснуючий товар найближчим часом.

Надання послуг через мережу Інтернет останнім часом також набуває популярності й серед громадян. Шахраї на сайтах розміщують інформацію щодо надання послуг з ремонту, купівлі/продажу товару, передачі майна безкоштовно тощо. Після цього, заволодівши грошима чи відповідним майном потерпілих, шахраї не мають наміру їх повертати. Так, Вироком Волинського апеляційного суду по справі № 166/938/17 був засуджений Особа_1, якого визнано винуватим та засуджено за те, що він в квітні 2017 року, з метою заволодіння чужим майном, шляхом обману, з використанням електронно-обчислювальної техніки, під виглядом безкоштовної передачі через мережу Інтернет товару, якого у наявності не було, використовуючи власний мобільний телефон марки «Fly» з IMEI 868455016264142, IMEI 868455016463041 зареєструвався в Інтернет-ресурсі «Вконтакте», шляхом створення сторінки з вигаданим псевдонімом «Алена Кучурина», на яку інсталював фотознімки товарів, якими в дійсності не володів. 13 квітня 2017 року ОСОБА_2 ознайомившись з інформацією в Інтернет-ресурсі «Вконтакте» на сторінці «Алена Кучурина» про товари, будучи введеним в оману, замовив ноутбук, за пересилання якого ОСОБА_1 перерахував гроші на електронний гаманець WebMoney U986025696068, у розмірі 160 грн., якими обвинувачений заволодів [10].

Вироком Стрийського мійськрайонного суду Львівської області по справі № 456/2818/15-к був засуджений ОСОБА_2 за ст.190 ч.3 Кримінального кодексу України, який зареєструвався на сайті aukro.ua, що належить ТзОВ «Аукро

Україна» і являє собою електронний аукціон, створив обліковий запис під логіном «ІНФОРМАЦІЯ_2», з НОМЕР_3 вказавши при цьому свої власні реєстраційні дані: ім'я користувача ОСОБА_2, з логіном на aukro.ua «ІНФОРМАЦІЯ_2» за адресою місця свого проживання АДРЕСА_2. 24.12.2014 року ОСОБА_2, маючи умисел на заволодіння чужим майном, будучи учасником електронного аукціону, користуючись логіном «ІНФОРМАЦІЯ_2», під приводом продажу, розмістив оголошення про продаж жіночого взуття «UGGY» за ціною 190 гривень, на інтернет-аукціоні aukro.ua. Під час електронного спілкування по електронній пошті ОСОБА_3 замовила у ОСОБА_2 виставлене на продаж взуття. ОСОБА_2 надав необхідні дані для здійснення грошового переказу - реквізити пластикової картки ПАТ КБ «ПриватБанк» НОМЕР_2, запевнивши при цьому, що після перерахування коштів перешле взуття протягом доби з часу їхньої домовленості, хоча достовірно знав, що цих умов він виконувати не буде, тобто зловживаючи довірою ввів в оману потерпілу ОСОБА_3. 24.12.2014 року, о 17:27:14 год., виконуючи зазначені умови усної домовленості, ОСОБА_3 перерахувала на пластикову картку ПАТ КБ «Приват Банк» НОМЕР_2, зареєстровану на ОСОБА_2, грошові кошти у сумі 190 грн. Однак, ОСОБА_2, шляхом обману та зловживання довірою заволодів 24.12.2014 року перерахованими ОСОБА_3 грошовими коштами, знявши 190 гривень в банкоматі у м. Стрий, які витратив на власні потреби, а всього завдав ОСОБА_3 матеріальної шкоди на суму 190 гривень [11].

Іншим видом шахрайства є продаж товарів неналежної якості через інтернет-магазин. Після отримання товару особа розуміє, що їй не надали товар, який вона розраховувала або продали підробку. Після чого номер телефону інтернет-магазин змінює, якщо особа висуває претензії, або магазин включає покупця в чорний список чи посилається на те, що на сайті є чітка інформація, що товар не оригінальний, хоча така інформація відсутня. Деякі продавці контрафакту в описі товару зазначають, що товар є копією, однак така репліка не виділяється в характеристики товару, а написана в кінці опису чи через

посилання. З кожним роком проблема контрафакції в інтернет-роздробі відчувається дедалі гостріше. Особливо вона помітна там, де інтернет найбільше глибоко проникає в ритейл – у США, Китаї та Індії. Так, за даними компанії Red Point, на які посилається Forbes, з 2018 до 2019 року, обсяги контрафактної продукції збільшились на 40% [12].

Деякі великі платформи, які надають послуги по розміщенню товарів, не мають уявлення, що на їх сайтах розміщають контрафактну продукцію. Так, компанія Amazon уникла відповідальності за продаж контрафактної продукції на своїй платформі – таке рішення ухвалив Суд Європейського Союзу у справі, порушеній косметичним брендом Coty. Справа була порушена німецькою філією американської косметичної компанії Coty, яка стверджувала, що Amazon порушує закон про товарні знаки, зберігаючи флакони парфумів Davidoff у своєму дистриб'юторському центрі для незаконного продавця. Amazon наголошує, що продовжує вкладати значні кошти у боротьбу з шахрайськими продавцями [13].

Останнім часом шахраї використовують сайти купівлі/продажу товарів чи соціальні сайти з метою отримання коштів незаконним шляхом. Суть такого виду шахрайства полягає у тому, що вибираючи товар, вони зв’язуються с продавцем і стверджують, що бажають купити товар. При цьому, як правило, вони мало цікавляться характеристиками товару. Шахраї пропонують оплатити товар зразу по повній передоплаті. Продавець надає дані картки і номер телефону, який прив’язаний до власної банківської карти. Найближчим часом кошти списуються не з карти покупця, а з карти продавця.

Ще одним розповсюдженим видом шахрайства є здійснення покупки через сайт законним власником картки, а потім її оскарження. Особа-шахрай оплачує покупку товару, забирає товар, як правило, безпосередньо у продавця, а потім телефонує в банк і стверджує про те, що вона не отримала куплений товар. Банк повертає кошти шахраю та блокує картку продавця.

Використання втрачених чи вкрадених карток. Цей тип шахрайства використовує вкрадені дані картки для здійснення покупки в мережі Інтернет. Продавець відправляє товари або надає послуги шахраю з припущенням, що платіж є законним. При цьому власник картки не знає, що дані картки використані, тому платежі можуть бути успішно оброблені. У разі використання картки шахрайським шляхом, платіж може бути оскаржений власником картки.

Як тільки суперечка буде вирішена на користь власника картки, бізнес зазнає збитків у розмірі суми платежу, вартості будь-яких уже наданих товарів чи послуг, а також додаткової комісії за спір.

Так, відповідно до обвинувального акту - обвинувачений ОСОБА_1 15 червня 2020 року, приблизно об 11 годині, перебуваючи за місцем свого мешкання, по АДРЕСА_1 , та, маючи умисел на заволодіння чужим майном шляхом обману (шахрайство), за допомогою Інтернет-мережі та мобільного телефону, надавши до ТОВ «МАНІВЕО ШВИДКА ФІНАНСОВА ДОПОМОГА» - заявку на отримання он-лайн кредиту, у сумі 600 гривень, попередньо створивши у зазначеній фінансовій установі, використовуючи паспортні дані ОСОБА_2 , електронний особистий кабінет на ім`я останнього, та, отримавши відкритий кредитний рахунок з перерахуванням грошових коштів, у сумі 600 гривень, на картку АТ КБ «Приватбанк» за № НОМЕР_1 , емітовану на ім`я ОСОБА_2 , здійснив зняття грошових коштів того ж дня, об 11 годині 57 хвилин, з банківського терміналу АТ КБ «Приватбанк», по вулиці імені Д.І. Менделєєва, 56, міста Лисичанська, спричинивши ТОВ «МАНІВЕО ШВИДКА ФІНАНСОВА ДОПОМОГА» майнову шкоду на вказану суму. Таким чином, обвинувачений ОСОБА_1 скоїв кримінальне правопорушення, передбачене ст.190 ч.3 КК України, а саме, - заволодіння чужим майном шляхом обману (шахрайство), вчинене шляхом незаконних операцій з використанням електронно-обчислювальної техніки [14].

Отримання інформації на електронну пошту про виграш в лотерею чи спадкування коштів у великих розмірах. Для того, щоб отримати виграш чи приз,

шахраї просять заповнити дані особи, яка виграла з метою переказати їй приз. Потім ці дані продаються чи використовуються в подальшому для викрадення грошей з банківських карток. Ще одним способом шахрайства при отриманні інформації про виграш, є умова перерахування певної суми коштів для сплати податку чи збору за оформлення документів. Оплативши, жертва в подальшому залишається без коштів, сплачених на податок чи збори та звичайно і без призу.

Отримання загрози про блокування комп'ютера, телефону чи загроза передання компрометуючої інформації. Шахраї розсилають інформацію на електронну пошту, що комп'ютер буде заблоковано, якщо Ви не надіслали кошти протягом доби або буде розповсюджена конфіденційна інформація чи продана конкурентам. Це доволі розповсюджений вид шахрайства. Також при відвідуванні сайту, блокується телефон чи комп'ютер і шахраї надсилають номер картки чи телефону, на які жертва повинна сплатити кошти для розблокування. Після сплати коштів телефон не розблоковується і потерпілому треба звертатися в сервісний центр для видалення вірусу.

Створення або використання сайтів благодійних організацій. Під час використання благодійних сайтів злочинці використовують електронну пошту, соціальні сайти чи надсилають повідомлення на телефон з проханням надати матеріальну допомогу. Шахраї видаються за агентів благодійних організацій або створюють власну благодійну назву. Це може включати благодійні організації, які проводять медичні дослідження або допомагають хворим та їхнім родинам, мають форму реагування на справжні катастрофи чи надзвичайні ситуації, такі як повені, землетруси, лісові пожежі тощо. Шахраї можуть використовувати назви реальних благодійних фондів, реальні фотографії та історію хвороби хворих люде, однак розміщувати шахрайські реквізити.

Створення фіктивних брокерських сайтів. Метою створення таких сайтів є заволодіння коштів у великих розмірах. Брокери створюють сайти та розміщують інформацію про свою компанію та діяльність, яку вони здійснюють. Однак дані про ліцензію та регулятори відсутні на сайті, але це не заважає деяким

брокерським компаніям обслуговувати 100+ країн. Компанії пропонують інвестувати у фіат, монети, сировинну продукцію, акції світових брендів, індекси та енергоносії. Послуги надаються від імені офшорної контори, місце знаходження якої невідомо або, як правило, знаходиться в іншій державі, юридична адреса такої компанії знаходиться в офшорній зоні. Функції учасників таких компаній чітко визначені. Зловмисники використовують психологічні методи агітаційного характеру з метою інвестування коштів у торгівлю на фінансових ринках. Разом з тим, кошти жертв не попадають на фінансовий ринок, а залишаються в брокера-шахрая. Злочинці імітують відкриття рахунку на Meta Trader, не даючи безпосереднього доступу до платформи. Головна мета – витягнути всі кошти з жертви. Як тільки особа перестає перераховувати кошти в свій особистий кабінет або забажає їх забрати, компанія перестає брати слухавку або торгівля на біржі обнулюється.

Висновки та пропозиції. У підсумку зазначимо, що вчинення шахрайств через мережу Інтернет є одним з найбільш розповсюджених видів даного кримінального правопорушення. На сьогодні способи його вчинення не є вичерпними, що зумовлює актуалізацію досліджуваного питання. Це пояснюється наявністю науково-технічного прогресу, різноманітністю впровадження комп'ютерних програм та сайтів, що дає платформу для виникнення нових способів вчинення шахрайств в мережі Інтернет. Разом з тим, аналіз існуючих способів надасть можливість розробити практичні рекомендації для подальшого розслідування та розкриття цього різновиду кримінальних правопорушень. Накопичення знань про спосіб вчинення шахрайства через мережу Інтернет дозволить з'ясувати механізм вчинення злочину, слідову картину, дослідити особу злочинця, що є важливим джерелом відомостей про шахрайства, що вчинюються через мережу Інтернет.

Література

1. Звіт Національної поліції України про результати роботи у 2020 році. URL: https://www.kmu.gov.ua/storage/app/sites/1/17-civik-2018/zvit2020/npu-zvit-2020.pdf. (дата звернення до ресурсу: 20.11.2021).

2. Кримінальний кодекс України. URL: https://zakon.rada.gov.ua/laws/show/2341-14#Text. (дата звернення до ресурсу: 20.11.2021).

3. Веліканов С.В., Волобуєв А.Ф., Журавель В.А. Криміналістична профілактика економічних злочинів: Науково-практичний посібник. Х.: Харків юридичний, 2006. 236 с.

4. Романенко Т. Способи вчинення шахрайств із використанням електронно-обчислювальної техніки як елемент їх криміналістичної характеристики. Knowledge, Education, Law, Management. 2020. № 3 (31). P. 144-148.

5. Самойлов С.В. Розслідування шахрайств, учинених із використанням мережі «Інтернет»: автореф. дис.… канд. юрид. наук. Донецьк. 2014. 18 с.

6. Конвенція про кіберзлочинність від 23.11.2001 р. (ратифікована Україною із застереженнями і заявами від 7 верес. 2005 р.). URL: http://zakon.rada.gov.ua/cgi-bin/laws/main.cgi?nreg=994_575. (дата звернення до ресурсу: 20.11.2021).

7. Білоус В.Т. Координація боротьби з економічною злочинністю: Монографія. Ірпінь: Академія державної податкової служби України, 2002. 449с.

8. Пазинич Т. А. Криміналістична характеристика шахрайств та основні положення їх розслідування: автореф. дис. ... канд. юрид. наук. Харків, 2007. 20 с.

9. Кибермошенники изобрели новый способ обмана покупателей на OLX. URL: https://uapay.ua/ru/cyberswindlers-found-new-way-to-cheat-olx-buyers/. (дата звернення до ресурсу: 20.11.2021).

10. Вирок Волинського апеляційного суду від 24 квітня 2019 року, судова справа № 166/938/17. URL: https://reyestr.court.gov.ua/Review/81413651. (дата звернення до ресурсу: 20.11.2021).

11. Вирок Стрийського мійськрайонного суду Львівської області від 01 лютого 2016 року, судова справа № 456/2818/15-к. URL: https://reyestr.court.gov.ua/Review/56043653. (дата звернення до ресурсу: 20.11.2021).

12. Рыбачук С. Контрафакт в e-commerce: победить, нельзя смириться. Retail.Ru. 20 сентября 2020 г. URL: https://www.retail.ru/articles/kontrafakt-v-e-commerce-pobedit-nelzya-smiritsya/. (дата звернення до ресурсу: 20.11.2021).

13. Amazon избежала ответственности за продажу контрафактной продукции. 08 апреля 2020 г. Портал о розничной и торговой платформы TradeMaster.UA. URL: https://trademaster.ua/news/24259. (дата звернення до ресурсу: 20.11.2021).

14. Вирок Лисичанського міського суду Луганської області від 08 квітня 2021 року, судова справа № 415/1311/21. URL: https://reyestr.court.gov.ua/Review/97914992. (дата звернення до ресурсу: 20.11.2021).