УДК 343.721:004 «364»
DOI https://doi.org/10.32782/klj/2023.3.25

Брисковська О. М.,
кандидат юридичних наук,
старший науковий співробітник,
провідний науковий співробітник наукової лабораторії
з проблем протидії злочинності
навчально-наукового інституту № 1
Національної академії внутрішніх справ

Гелемей М. О.,
кандидат юридичних наук, доцент,
старший науковий співробітник відділу організації наукової діяльності
та захисту прав інтелектуальної власності
Національної академії внутрішніх справ

ОСОБЛИВОСТІ ВЧИНЕННЯ ШАХРАЙСТВА В МЕРЕЖІ ІНТЕРНЕТ В УМОВАХ ВОЄННОГО СТАНУ

Анотація. Стаття присвячена важливій та актуальній на сьогодні темі – особливостям вчинення шахрайства в мережі Інтернет в умовах воєнного стану. Розкрита вагомість та значимість розгляду даної теми, яка має виняткові особливості оскільки шахрайські дії вчиняються онлайн під час воєнних дій на території України. Встановлені особливості шахрайства в мережі Інтернет в умовах воєнного стану. Виявлено та запропоновано типізацію основних індикаторів шахрайських повідомлень. Виокремлені найбільш поширені шахрайські схеми під час війни на теперішній час, зокрема шахрайство щодо збору грошей на ЗСУ або на авто для ЗСУ, фейковий збір коштів на лікування дітей які постраждали від збройної агресії рф, фейкове отримання міжнародної допомоги, фейкове перевезення біженців та допомога з житлом, шахрайство щодо надання інформації про місце перебування безвісти зниклих родичів, фейкові повідомлення на кшталт «ваш син потрапив у полон», продаж неіснуючих товарів і послуг у інтернет-крамницях, шахрайство тощо. Встановлені та розкриті основні індикатори шахрайських повідомлень через мережу Інтернет та класифіковано їх на типи, надана характеристика кожному з них. Розглянуті особливості поведінки осіб, які стали жертвами інтернет-шахрайства та впливають на вразливість до таких злочинів. Зроблено висновок про те, що забезпечення безперервної просвітницької роботи, у тому числі через засоби масової інформації, соціальні мережі, серед усіх верств населення з метою своєчасного інформування про нові види шахрайств, видозмінені та удосконалені способи їх вчинення, характерні особливості шахраїв і криміногенні ситуації-пастки, може значно вплинути на зменшення таких кримінальних правопорушень.

Ключові слова: *шахрай, інтернет-ресурси, онлайн-шахрайство, маніпуляція, кримінальні схеми, умови воєнного часу.*

Bryskovska O. M., Helemei M. O. Peculiarities of committing fraud on the Internet in the conditions of martial law

Abstract. The article is devoted to an important and relevant topic today – the peculiarities of committing fraud on the Internet in the conditions of martial law. The importance and significance of consideration of this topic, which has exceptional features because fraudulent actions are committed online during hostilities on the territory of Ukraine, is revealed. The features of fraud on the Internet in the conditions of martial law have been established. The typification of the main indicators of fraudulent messages was identified and proposed. The most common fraudulent schemes during the war to date have been singled out, including fraud regarding the collection of money for the Armed Forces or cars for the Armed Forces, fake collection of funds for the treatment of children who suffered from the armed aggression of the Russian Federation, fake receipt of international aid, fake transportation of refugees and assistance with housing, fraud regarding the provision of information about the whereabouts of missing relatives, fake messages such as “your son was captured”, sale of non-existent goods and services in online stores, fraud, etc. The main indicators of fraudulent messages via the Internet have been established and disclosed, and they have been classified into types, and the characteristics of each of them have been given. The characteristics of the behavior of persons who have become victims of Internet

fraud and their vulnerability to such crimes are considered. It was concluded that the provision of continuous educational work, including through the mass media, social networks, among all segments of the population in order to timely inform about new types of fraud, modified and improved ways of committing them, characteristic features of fraudsters and criminogenic situations-traps, can significantly affect the reduction of such criminal offenses.

Key words: *swindler, Internet resources, online fraud, manipulation, criminal schemes, wartime conditions.*

Постановка проблеми. Варто визнати, що в умовах воєнного стану значною мірою полегшується вчинення кримінально протиправного діяння, зростає ризик особи стати потерпілою, а правоохоронні органи мають обмеженні ресурси для адекватного кримінально-правового реагування [1, с. 315]. Зловмисники, удосконалюючи способи вчинення та приховання кримінальних правопорушень, часто використовують для злочинної діяльності торгівельні площадки мережі Інтернет. На жаль, війна відкрила нові «горизонти та можливості» для шахрайської діяльності зловмисників, користуючись вразливим емоційним станом співвітчизників, маніпулюючи почуттями людей які перебувають у розпачі та гніві, зловмисники будують шахрайські схеми, пристосовуючись до ситуації. На сьогодні більше 70% українців не мають впевненості у своїй здатності розпізнати ознаки онлайн-шахрайства. Менша половина співвітчизників перевіряє у повідомленнях правильність логотипу компанії та її електронну адресу відправника [2]. 7 із 10 українців переймаються, що їх рідні чи друзі можуть з легкістю відреагувати на шахрайське повідомлення, а 68% українців самі не впевнені у своїх можливостях щодо спроможності розпізнати онлайн-шахрайство. Така ж кількість респондентів занепокоєні, що жертвами інтернет-шахраїв можуть стати літні люди, а майже чверть опитаних не впевнена у пильності дітей та підлітків. За результатами останнього дослідження Visa Stay Secure – кожен другий українець принаймні раз потрапляв на гачок шахраїв, а 17% ставали жертвами обману неодноразово [2].

Аналіз останніх досліджень і публікацій. Загальні питання вчинення інтернет-шахрайства в Україні розглядали такі вітчизняні вчені О.В. Бишевець, О.С. Белицький, Т.С. Вайда, В.В. Винник, А.С. Габуда, В.М. Галунько, Л.П. Гринько, Н.О. Думанський, О.М. Джужа, Л.М. Івашко, О.О. Кіпа, О.В. Клювак, О.І. Кривенко, І. Метельський, А.Б. Мізерак, Л.М. Прудка, Ю.О. Полукаров, Д.В. Перепелиця, Т.В. Романенко, Я.П. Руденко, В.П. Сабадаш, О.А. Самойленко, І.В. Сабадаш, С.С. Чернявський, В.І. Шакун, С.В. Шапочка, О.М. Юрченко та інші. В наукових працях приділялась увага загальним аспектам злочинів у мережі Інтернет, а також інтернет-шахрайствам в мирний час.

Вивченням окремих питань шахрайства в мережі Інтернет в умовах воєнного стану переймалися науковці О.М. Брисковська, Я.В. Левківська, М.Є. Собаченко, В.Г. Телійчук. Незважаючи на суттєвий внесок вітчизняних вчених у вивчення означеної проблематики, особливості вчинення шахрайства в мережі Інтернет в умовах воєнного стану на сьогодні потребує подальшого наукового дослідження.

Метою статті є дослідження особливостей вчинення онлайн-шахрайств в умовах воєнного часу.

Виклад основного матеріалу. Як тільки в Україні почали користуватися мережею Інтернет та розвиватися різні інтернет-ресурси, шахраї почали їх використовувати як можливість та засіб для своєї злочинної діяльності [3, с. 522]. Привабливі умови щодо неможливості безпосередньо бачити особу та контактувати з нею притягують зловмисників та надихають на вигадування різних злочинних схем з заволодіння майном, коштами, цінностями інших осіб.

До головних ознак інтернет-шахрайства можна віднести: 1) високий ступінь латентності; 2) багатоманітність способів учинення шахрайства (пов’язано із широким спектром послуг у мережі Інтернет); 3) глобальний характер (інформаційний простір, на відміну від фізичного, не має чітких кордонів й обмежень); 4) складнощі виявлення та запобігання [4, с. 226].

Шахрайства в мережі Інтернет в умовах воєнного стану мають свої особливості:

– шахрайські дії вчиняють онлайн;

– шахрайство вчиняють під час воєнних дій на території України;

– використовують вразливість емоційного стану через спекуляцію на почуттях людей: співпереживання (фейкові рахунків на допомогу постраждалим від збройної агресії, допомога військовим), гнів (донати на зброю, дрони і т.д.);

– користуються попитом на життєво необхідні послуги (вивезення з зони бойових дій, тимчасово окупованих територій, оренда житла, придбання бронежилетів, пального або запчастин для автомобілів, програмами виплат внутрішньо переміщеним особам та інше).

В умовах збройної агресії рф у українців підвищилась вразливість емоційного стану, зловмисники реагують на такі зміни і використовуючи наявні обставини та актуальні питання сьогодення використовують у своїх шахрайських схемах нові умови суспільного життя.

До засобів вчинення онлайн-шахрайства доцільно віднести комп'ютерну техніку, мобільні пристрої, а також інші мультифункціональні пристрої, за допомогою яких можна збирати, отримувати або зчитувати конкретні дані [5, с. 191]. На нашу думку до засобів їх вчинення доцільно віднести і наявність мережі Інтернет та пристрої для отримання і передачі Інтернета (маршрутизатори або роутери), банківські рахунки підставних осіб та картки.

Географія інтернет-шахрайства в умовах воєнного стану дуже широка і охоплює всі області країни. Такі кримінальні правопорушення переважно вчинюють чоловіки 80% від 21 до 55 років, найбільша кількість припадає на вік від 30 до 42 років, траплялися поодинокі випадки вчинення неповнолітніми,. Жінки на яких припадає 20% вчинення інтернет-шахрайства, в переважній більшості, використовують платформу для оголошення в соціальних мережах про продаж і доставку товарів або здачу в оренду житла розміщуючи фейкові оголошення.

Розглянемо *основні індикатори шахрайських повідомлень* та класифікуємо їх на типи:

Маніпуляція прискоренням: шахраї дуже часто користуються термінами «не зволікаючи», «терміново», «негайно»:заохочують до дій осіб щодо відповіді на електронний лист або перехід за посиланням. В більшості випадків – це повідомлення від шахраїв, вони надсилаються наче б то від імені банків, відомих брендів, друзів чи знайомих. Зазвичай, вони повідомляють про негаразди з банківським рахунком, обіцяють грошову винагороду, закликають до пожертв тощо. Майже 27 % громадян можуть піддатися схемам, що несуть повідомлення про загрозу безпеки щодо зламання паролів. Також 32% жителів нашої країни можуть бути обмануті повідомленнями,начебто, від урядових органів.

Маніпуляція повідомленням «вам пощастило це ціна ще за старим курсом», «вітаємо, гарні новини», «виграші дорогих товарів, за доставлення яких не потрібно платити»: майже половина опитуваних готові виконати запропоновані дії якщо у повідомленні міститься позитивна інформація. 35% респондентів позитивно відкликнулися та клацнули б на лінк чи надали відповідь на лист у якому розписані фінансові переваги та переконливі обіцянки їх отримати.

Пред'явлення вимог: в більшості випадків пред'являють вимоги з обмеженням часу для їх виконання 35% респондентів відгукнулися б на повідомлення, яке вимагало від них конкретних дій. Але щодо отримання запитів на зміну паролів українці виявилися найбільш обережні.

За результатами дослідження, опитувані які вважали себе як обізнаними попадалися на шахрайські хитрощі. Це особи які обізнані 54% та 42% відгукуються на «термінові дії». Доцільно наголосити, що 85% респондентів вважають найбільш підозрілими повідомлення про зміну пароля [2].

Найбільш поширеними шахрайськими схемами під час війни є наступнна теперішній час:

Шахрайство щодо збору грошей на ЗСУ або на авто для ЗСУ. Приміром, на Одещині від імені керівництва військових адміністрацій десять шахраїв просили «допомогу для ЗСУ» у бізнесменів кількох міст, включаючи

Одесу. Організатор злочинної схеми – іноземець, який відбуває покарання в одній із колоній на окупованій території Луганщини. Його спільники – мешканці Києва та півдня України, координація дій яких здійснювалася телефоном. Користуючись особистими зв'язками, вони знаходили компанії, яким під час війни вдалося вціліти. Бізнесменам пропонували зробити благодійний внесок – від 20 тис. до 100 тис. грн. Отримавши кошти, учасники групи переказували їх на свої рахунки або знімали у банкоматах у різних регіонах країни. Загалом потерпіло від угруповання 60 комерсантів-благодійників. За такою ж схемою діяв житель міста Ізмаїл 29-річний чоловік. У соцмережах він оприлюднив відеозвернення, в якому оголосив збір грошей для військових, які несуть службу на блокпостах. Так чоловік зібрав 30 тис. грн. – на «допомогу бійцям» встигли скинутися 26 осіб [6].

Фейковий збір коштів на лікування дітей які постраждали від збройної агресії рф. Така злочинна схема набула широкого розповсюдження. Фейкові волонтерські та благодійні організації створюють фіктивні сайти, сторінки у соціальних мережах, канали в телеграм та привласнюють кошти громадян.

Фейкове отримання міжнародної допомоги. Зловмисники через спеціально створений чат-бот розсилали листи людям, які постраждали від вторгнення РФ. У посланнях шахраї пропонували постраждалим отримати міжнародну допомогу. Зокрема, у повідомленнях: «Дія. Допомога від ООН» містилася рекомендація щодо того, як зробити запит на виплату 2,2 тис. грн. Довірливі люди йшли за посиланням та потрапляли на фішинговий сайт з інтерфейсом, схожим на «Приват24». Цей фейковий веб-ресурс і виманював реквізити платіжних карток [2].

Фейкові оголошення в Інтернеті про продаж автомобілів. Шахраї розміщували фото авто з його параметрами, пробігом та іншим. Оголошення робили максимум реалістичними, що важко запідозрити про їх фейковість. Зловмисники використовували фейкові акаунти. Пропонували переважно пікапи, які, як відомо, мають попит серед військових. Зацікавлених переконували, що нібито вже домовилися з іншими покупцями, але за умови передоплати товар зможуть «притримати». Таким чином, за даними поліції, шахраї виманювали гроші у волонтерів та бійців ЗСУ [6].

Фейковий захист рахунків. Зловмисники, під виглядом працівників банків, телефонували громадянам та переконували надати інформацію про фінансові номери нібито для захисту їх рахунків. Отримавши конфіденційні дані, аферисти здійснювали несанкціонований доступ до SIM-карток шляхом їх перевипуску та дублювання. У подальшому шахраї без відома власників здійснювали переказ грошей на підконтрольні банківські рахунки. Для цього використовували унікальний номер-пароль клієнтів банку, який є засобом ідентифікації переказу [7].

Фейкове перевезення біженців та допомога з житлом. Тисячі українців (більше на території сходу нашої країни) постраждали від найбільш поширених схем онлайн-шахрайства – імітації перевезення з прифронтових або з окупованих територій до безпечних міст та допомоги в розміщенні. Шахраї розміщували в інтернет-мережі оголошення з пропозицією безпечного та швидкого доставлення до західних регіонів України або навіть за кордон. Під час спілкування шахраї намагалися виманити передоплату за запропоновані послуги, обґрунтовуючи це підвищеною небезпекою, необхідністю резервування місць тощо. Здебільшого за свої «послуги» зловмисники вимагали від 500 до 1000 грн авансу з особи. Отримавши передоплату, шахраї зникали та переставали виходити на зв'язок [8].

Шахрайство з орендою житла. Через війну багато людей переїжджають з місця на місце, шукаючи прихисток. Найчастіше шахраї використовують мережу Інтернет на різних платформах для розміщення оголошень про товари та послуги. Під приводом здачі в оренду житла, в безпечних регіонах України, шахраї просять переказати перший платіж або певну частину від вартості оренди. Проте після перерахування коштів потерпілі приїздять на місце і, як правило, виявляють, що в оселі або хтось проживає, або оголошення вже неактуальне. Шахраї блокують

у соціальних мережах своїх жертв, міняють номера телефонів та продовжують свою шахрайську діяльність [8].

Фейкові повідомлення «ваш син потрапив у полон». Зловмисники телефонують родичам зниклих називаючи прізвище та ім'я, що нібито він перебуває в полоні, для того щоб визволити потрібна певна сума грошей.

Шахрайство щодо надання інформації про місце перебування родичів які безвісти зникли. Зловмисники використовують розміщені у Інтернеті оголошення про розшук безвісти зниклих осіб. Шахраї зв'язуються з рідними, та повідомляють, що за винагороду можуть надати інформацію про місце знаходження безвісти зниклого родича.

Продаж неіснуючих товарів і послуг у інтернет-крамницях. Цей вид шахрайства можна поділити на три умовні підвиди:

– шахрай пропонує покупцеві що-небудь, бере з нього повну або часткову передоплату і зникає;

– шахрай продає замовнику товар, але неналежної якості, такий, що не відповідає стандартам, на які той розраховував і які оголошував продавець;

– шахрай підмінює товар, тобто надсилає те, чого людина не замовляла [6].

Причиною активізації таких схем є масовий перехід суб'єктів господарювання на віртуальні майданчики, де можна зекономити на оренді приміщення і зробити ринкові ціни на товари та послуги привабливішими для покупців.

Особливості поведінки осіб які стали жертвами інтернет-шахрайства, що впливає на вразливість до таких злочинів.

Респонденти, які вважають себе знавцями щодо тактик онлайн-зловмисників, з більшою імовірністю натиснуть на фальшиве посилання або повірять шахрайській пропозиції. Так, 53% «знавців» українців повірять повідомленням, що містить позитивні новини з фінансовими бонусами а 38% відреагують на прохання виконати термінові дії, тоді як серед тих, хто сумнівається у своїй пильності, так само вчинять 47%.

Надмірна довірливість через нестачу знань або досвіду. Шахраї використовують некомпетентність в якійсь сфері, наприклад, фінансові консультації, пропозицію вкласти гроші в нову технологію або продукт.

Цікавість до привабливих заголовків, які змушують користувача Інтернету натиснути на нього. Злочинці використовують клікбейт – привабливі пропозиції або інтригуючі повідомлення, щоб заманити клієнта або встановити шкідливе програмне забезпечення.

Менша кількість опитаних вірять проханням перевстановити пароль із-за потенційного витіку даних: для 83% опитаних повідомлення такого змісту – найбільш підозріла. Набагато менше занепокоєння викликають СМС про статус відправлення, що доставляється (лише 25% включили такі повідомлення, що змушують насторожитися), електронні листи з оголошенням про розпродаж або появу нового продукту (29%) або лист з прохання залишити відгук про отриманий нещодавній досвід (18%) – таким усім можуть скористатися шахраї.

Майже кожен другий (47%) опитуваний повідомив, що переконується, що листа надіслано з дійсної електронної адреси, тоді як лише 41% перевірятимуть, чи прикріплено до повідомлення назву або логотип компанії. Менше половини респондентів шукатимуть у листі номер свого замовлення (39%) або банківського рахунку (32%), а 40% перевірятимуть правильність написання слів.

Кіберзлочинці повсякчас підвищують рівень професіоналізму, удосконалюючи способи вчинення та приховування злочинів [9, с. 75]. Успішне запобігання інтернет-шахрайствам, їх викриття і притягнення винних осіб до відповідальності сьогодні є досить рідкісним явищем, якщо порівнювати з їх кількістю [10, с. 223].

Висновки. Через хибну впевненість осіб посилюється вразливість до обману. Зловмисники використовують повідомлення, які не викликають підозру, містять безпечний, нейтральний текст оголошення з необхідністю перейти за посиланням, а тому особи нехтують перевіркою інтернет-майданчиків, не перевіряють відгуки про товари та продавців, без перевірки відразу оплачують товар, забираючи з поштового відділення. Також багато випадків, коли особи не перевіряють благодійні фонди чи навіть правдивість

інформації від своїх друзів, знайомих про необхідну їм допомогу, на яку збирають гроші невідомі їм особи. При оренді житла заздалегідь пересилають кошти, керуючись тільки фотографіями приміщення в Інтернеті.

Усе це потребує запровадження нових, нерідко нетрадиційних підходів з організації і здійснення протидії організованим злочинним проявам [11, с. 7]. Важливо також пам'ятати, що система заходів індивідуального запобігання повинна бути циклічною: розпочинатися із заходів усунення причин і умов учинення суспільно небезпечних діянь, продовжуватись заходами їх відвернення та припинення і завершуватися знову-таки заходами усунення причин і умов учинення суспільно небезпечних діянь [12, с. 7].

Забезпечення безперервної просвітницької роботи, охоплюючи всі соціально-демографічні верстви населення, через засоби масової інформації (соціальні мережі,сайти,пресу, радіо, телебачення, смс-повідомлення тощо), бесіди, лекції (колективам, працівникам на підприємствах, в установах, організаціях, студентам у вишах, учням у школі, пенсіонерам, соціально незахищеним верствам населення за місцем проживання і т. ін.) з метою своєчасного інформування про нові види інтернет-шахрайства в умовах воєнного стану [13, с. 48]. Про ознаки інтернет-шахрайств, криміногенні ситуації-пастки, які створюються шахраями для вчинення своїх злочинних посягань. Все це є ефективними заходами профілактики такої злочинності.

Доцільно пояснити, що навіть якщо особа стала жертвою шахрайства і вже перераховувала кошти на телефонні чи банківські рахунки, такий процес ще можна зупинити. Необхідно, не зволікаючи, звернутися до банку з проханням скасування такого платежу та блокування карти. Жертвам інтернет-шахрайства потрібно акумулювати всю інформацію і звернутися до поліції, вказавши свій номер телефону та номер телефону, з якого телефонував шахрай, а також номери банківських рахунків, з яких переведені кошти і рахунки, на які були перераховані. Таку ж інформацію необхідно повідомити на «гарячу лінію» управління по боротьбі з кіберзлочинністю.

Крім того, своєчасно оновлена інформація про нові види онлайн-шахрайств, способи їх учинення та приховання, особливості поведінки шахраїв і криміногенні ситуації-пастки, які створюються ними для вчинення злочинних посягань, розроблення та поширення роз'яснювальних інструкцій щодо розпізнання схем аферистів в Інтернеті, поради щодо протидії цим злочинам також можуть істотно вплинути на зменшення рівня таких кримінальних правопорушень.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ:

1. Вознюк А. А. Воєнний та надзвичайний стан як обставини, що впливають на кваліфікацію кримінального правопорушення або призначення покарання. *Юридичний науковий електронний журнал*. 2022. № 6. С. 308–317.DOI: https://doi.org/10.32782/2524-0374/2022-6/69

2. Якобчук А. Половина українців потрапили на гачок шахраїв у мережі URL: https://slovoproslovo.info/polovina-ukraintsiv-potrapili-na-gachok-shahraiv-u-merezhi

3. Левківська Я.В. Вплив воєнного стану на трансформування та розвиток інтернет-шахрайства в Україні *Європейський вибір України, розвиток науки та національна безпека в реаліях масштабної військової агресії та глобальних викликів XXI століття* (до 25-річчя Національного університету «Одеська юридична академія» та 175-річчя Одеської школи права) : у 2 т. : матеріали Міжнар.наук.-практ. конф. (Одеса, 17 черв. 2022 р.). Одеса : Видавничий дім «Гельветика», Т. 2.2022. С. 521–523.

4. Чернявський С.С. Інтернет шахрайство як об'єкт дослідження правових наук. Протидія злочинності у сфері інтелектуальної власності та комп'ютерних технологій органами внутрішніх справ: стан, проблеми та шляхи вирішення : матеріали Всеукр. наук.-практ. конф., (Донецьк, 12 листоп. 2010 р.). Донецьк : ДЮІ ЛДУВС, 2010. С. 100–103.

5. Березняк В. Запобігання шахрайству в Інтернеті. *Науковий вісник Дніпропетровського державного університету внутрішніх справ.* № 1 2023. С. 190–196. DOI: 10.31733/2078-3566-2023-1-190-196

6. Козова Л. Було вашим, стало нашим: як шахраї під час війни на чужому горі «заробляють». URL: https://www.unian.ua/society/bulo-vashim-stalo-nashim-yak-shahraji-pid-chas-viyni-na-chuzhomu-gori-zaroblyayut-12179187.html#id--1117563139

7. Привласнили близько пів мільйона гривень: кіберполіція викрила групу зловмисників, які діяли за схемою перевипуску SIM-карт URL: https://cyberpolice.gov.ua/news/pryvlasnyly-blyzko-piv-miljona-gryven-kiberpolicziya-vykryla-grupu-zlovmysnykiv-yaki-diyaly-za-sxemoyu-perevypusku-sim-kart-6582/

8. Реальні історії шахрайства в Інтернеті в умовах війни. URL:https://it-kharkiv.com/realni-istoriyi-shahrajstva-v-interneti-v-umovah-vijny/

9. Брисковська О. М. Соціально-психологічна характеристика особи, яка вчиняє шахрайство в мережі Інтернет. *Науковий вісник Національної академії внутрішніх справ*. 2020. № 1 (114), С. 70–78. doi: https://doi.org/10.33270/01201141.70

10. Брисковська О. М., Пустовіт В. А. Організовані форми інтернет-шахрайства на сучасному етапі *Вісник Запорізького національного університету (Юридичні науки).* № 4. (Т. 1). 2020. С. 219–225. DOI: https://doi.org/10.26661/2616-9444-2020-4.1-32

11. Мороз В.П., Чаплинський К.О., Богуславський М.Г., Волошина М.О. Протидія організованій злочинності в Україні: сучасність та перспективи : монографія. Дніпро : Дніпроп. держ. ун-т внутр. справ, 2023. 236 с.

12. Вознюк А. А. Концептуальні засади запобігання суспільно небезпечним діянням. *Науковий вісник Національної академії внутрішніх справ*. 2016. № 2 (99). С. 156–165.

13. Брисковська О.М. Окремі види фінансового шахрайства з використанням мережі інтернет в умовах воєнного стану. *Злочинність і протидія їй в умовах війни: глобальний, регіональний та національний виміри* : матеріали наук.-практ. конф. (Вінниця, 12 квіт. 2023 р.) МВС України, Харків. Нац. ун-т внутр. справ, Кримінол. асоц. України, Наук. парк «Наука та безпека». Вінниця : ХНУВС, 2023. С. 46–49.