УДК 343.9
DOI https://doi.org/10.32844/2618-1258.2024.6.31

СЕВРУК І.Ю.

ОКРЕМІ ЗАСАДИ ЗАРУБІЖНОГО ДОСВІДУ ПРОТИДІЇ ПРАВООХОРОННИМИ ОРГАНАМИ ШАХРАЙСТВУ, ЩО ВЧИНЯЄТЬСЯ З ВИКОРИСТАННЯМ МЕРЕЖІ «ІНТЕРНЕТ»

SOME PRINCIPLES OF FOREIGN EXPERIENCE IN COUNTERACTING FRAUD COMMITTED VIA THE INTERNET BY LAW ENFORCEMENT AGENCIES

Актуальність статті полягає в тому, що вивчення іноземного досвіду протидії спеціальними підрозділами поліції шахрайству, що вчиняється з використанням мережі «Інтернет», є неможливим без комплексного аналізу нормативно-правових актів та правозастосовної практики правоохоронних органів різних держав. Мета статті полягає у аналізі досвіду окремих зарубіжних країн щодо протидії правоохоронними органами шахрайству, що вчиняється з використанням мережі «Інтернет». У статті проаналізовано положення нормативно-правових актів і відповідну правозастосовну практику діяльності іноземних правоохоронних органів щодо протидії шахрайству, що вчиняється через мережу «Інтернет». Акцентовано на діяльності суб'єктів окремих держав, які здійснюють протидію шахрайству, що вчиняється через мережу «Інтернет»: США (Управління з боротьби з фінансовими злочинами (Financial Crimes Enforcement Network – FinCEN), Федеральне бюро розслідувань (FBI), Центр скарг на комп'ютерну злочинність (IC3), Федеральна торгова комісія), Бразилія (служба внутрішніх доходів («Receita Federal»), Бразильський підрозділ фінансової розвідки (COAF), Австралії (Державної поліції і Департаменту юстиції). Дослідженням установлено, що більшість іноземних країн не містять спеціальних норм, які регламентують відповідальність за шахрайство, що вчиняється з використанням мережі «Інтернет», відповідно підходи до протидії таким злочинам обумовлені особливостями національного законодавства. Отже, для пошуку ефективних моделей протидії шахрайству, що вчиняється з використанням мережі «Інтернет», було вивчено іноземний досвід та структуру їх спеціальних підрозділів, поліцейських відомств, а також їх функції, що абсолютно різняться за своєю сутністю. Так, у європейських країнах та США функції протидії поступаються місцем запобіганню, на відмінну від вищевказаних країн та США, азіатські держави суворо дотримуються жорстких репресивних заходів. На основі опрацьованого та узагальненого сучасного передового іноземного досвіду розроблено науково обґрунтовані рекомендації щодо протидії правоохоронними органами шахрайству, що вчиняється з використанням мережі «Інтернет».

Ключові слова: *кіберполіція, спеціальні підрозділи, протидія, розслідування, взаємодія, шахрайство, мережа «Інтернет», зарубіжний досвід.*

The relevance of the article lies in the fact that the study of foreign experience in countering fraud committed using the Internet by special police units is impossible without a comprehensive analysis of regulatory legal acts and law enforcement practice of law enforcement agencies of different states. The purpose of the article is to analyze the experience of individual foreign countries in countering fraud committed using the Internet by law enforcement agencies. The article analyzes the provisions of regulatory legal acts and relevant law enforcement practice of foreign law enforcement agencies in terms of combating fraud committed via the Internet. The author emphasizes the activities of entities of certain States engaged in countering fraud committed via the Internet: USA (Financial Crimes Enforcement Network (FinCEN), Federal Bureau of Investigation (FBI), Computer

© СЕВРУК І.Ю. – аспірантка наукової лабораторії з проблем протидії злочинності ННІ № 1 (Національна академія внутрішніх справ)

Crime Complaint Center (IC3), Federal Trade Commission), Brazil (Internal Revenue Service (Receita Federal), Brazilian Financial Intelligence Unit (COAF), Australia (State Police and Department of Justice). The study has found that most foreign countries do not have special rules regulating liability for fraud committed via the Internet, and therefore approaches to combating such crimes are conditioned by the peculiarities of national legislation. Therefore, in order to find effective models for combating fraud committed via the Internet, foreign experience and structure of their special units, police departments, as well as their functions, which are completely different in nature, have been studied. Thus, in European countries and the USA, the functions of counteraction give way to prevention; in contrast to the named countries, Asian States strictly adhere to strict repressive measures. Based on the processed and generalized modern foreign best practices, scientifically sound recommendations for law enforcement agencies to counteract fraud committed via the Internet have been developed.

Key words: *cyber police, special units, counteraction, investigation, interaction, fraud, Internet, foreign experience.*

Постановка проблеми. Міжнародний досвід боротьби з організованою злочинністю свідчить, що певні державні стратегії можуть значно ускладнити діяльність злочинних угруповань, зробивши її менш ефективною, що може призвести до переміщення кримінальної активності в інші країни. Одним із ключових аспектів державної політики є прийняття законодавства, яке ускладнює отримання незаконного прибутку, спрощує виявлення злочинців і доведення їх вини [1]. В іноземних країнах функції боротьби з організованою злочинністю змінюються, і наразі основну увагу приділяють запобіганню діяльності етнічних злочинних угруповань. Це досягається шляхом усунення причин та умов, що сприяють злочинності, а також впровадженням запобіжних заходів, спрямованих на контроль над злочинністю, з активною підтримкою громадян [2]. Як справедливо зауважує Л. В. Лефтеров, навіть у розвинених економічно країнах існують серйозні труднощі з профілактикою та боротьбою зі шахрайствами, що здійснюються за допомогою комп'ютерних технологій. Це підкреслює актуальність цієї проблеми і вимагає більш глибокого дослідження, аналізу, а також розробки та впровадження ефективних професійних рішень, методичних, юридичних та загальносоціальних заходів для запобігання таким видам шахрайства [3, с. 90–91].

І. М. Охріменко у своєму аналізі процесу запозичення міжнародного досвіду виділяє кілька етапів:

1) збирання інформації про досвід окремих країн чи груп країн;

2) вивчення для виявлення переваг та недоліків певної моделі, поширеної в іншій країні(ах);

3) оцінка можливості адаптації цієї моделі до умов України;

4) розробка наукових основ і методичних рекомендацій для впровадження цього досвіду в Україні;

5) впровадження моделі в реальність з постійним науковим супроводом і моніторингом ефективності інновацій на вітчизняному підґрунті;

6) організація освітнього процесу, від розкладу занять до взаємодії з викладачами та роботи методистів і керівників курсів [4].

Дослідження досвіду інших країн показує, що впровадження і підтримка ефективних програм профілактики злочинності може суттєво сприяти підвищенню рівня безпеки в суспільстві шляхом зменшення рівня злочинності. Ретельно спланованні ініціативи здатні запобігти як злочинам, так і віктимізації, сприяючи загальній безпеці громади та забезпеченню її сталого розвитку [5].

Необхідно прискорити процес впровадження та адаптації міжнародних норм і стандартів до законодавчої системи України в інформаційній сфері. Ключовим є активний обмін даними між правоохоронними органами різних країн щодо кібершахрайств, що вже скоєні або знаходяться на стадії підготовки. Найбільш ефективним способом боротьби з будь-яким видом злочину є його недопущення, запобігання, а також виявлення причин і умов, які сприяють його скоєнню, з подальшим їх обмеженням, нейтралізацією і усуненням, а вже після цього – розслідування та розкриття [6, с. 189; 7, с. 294].

Таким чином, вивчення іноземного досвіду протидії спеціальними підрозділами поліції шахрайству, що вчиняється з використанням мережі «Інтернет», є неможливим без комплексного аналізу нормативно-правових актів та правозастосовної практики правоохоронних органів різних держав, що зумовило **актуальність вибраної теми.**

Аналіз останніх досліджень і публікацій. Окремі засади зарубіжного досвіду протидії правоохоронними органами шахрайству, що вчиняється з використанням мережі «Інтернет» досліджували такі вчені, як: В. С. Березняк, В. В. Вінцук, В. М. Господаренко, М. В. Гуцалюк, М. М. Єфімов, А. Е. Жилін, К. С. Качашвілі, В. Б. Коба, І. О. Коваленко, І. О. Коновалова, Є. В. Кочура, О. І. Кривенко, Л. В. Лефтеров, С. Ю. Лівчук, К. В. Малишев, І. М. Охріменко, С. О. Павленко, Н. В. Павлова, О. М. Петровський, М. В. Підболячний, І. М. Пістунов, Ю. М. Піцик, В. Г. Севрук, Т. Г. Таран, О. О. Хробуст, І. М. Чайка, М. М. Чаплик, С. С. Чернявський, С. В. Шапочка тощо.

Мета статті полягає у аналізі досвіду окремих зарубіжних країн щодо протидії правоохоронними органами шахрайству, що вчиняється з використанням мережі «Інтернет».

Виклад основного матеріалу дослідження. Вивчаючи іноземний досвід і здійснюючи конструктивний аналіз підходів різних держав до питання протидії злочинам, що вчиняються організованими групами і злочинними організаціями, варто констатувати, що у світі за останні десятиліття змінилися підходи, які визначали природу і сутність цього явища, а також концепція правоохоронних органів щодо протидії організованій злочинності [8]. Отже, у рамках комплексної протидії інтернет-шахрайству необхідно забезпечити гармонізацію кримінального законодавства щодо цих злочинів на міжнародному рівні. Це включає розробку та інтеграцію міжнародних стандартів у національне законодавство, які сприяють ефективному розслідуванню кримінальних правопорушень у глобальних інформаційних мережах, а також отриманню, дослідженню та представленню електронних доказів [9, с. 131; 10].

У контексті дослідження проблем протидії шахрайствам у сфері е-комерції, І. М. Пістунов також вважає, що варто вдатися до вивчення досвіду розвинутих іноземних країн у цій сфері [11, с. 33]. О. І. Кривенко наголошує, що однією з основних проблем у боротьбі з інтернет-шахрайствами є те, що підходи до цього питання можуть значно різнитися в залежності від країни [12, с. 210; 10, с. 176].

У травні 2019 року Комісія ООН з питань запобігання злочинності та кримінального правосуддя запропонувала Генеральній Асамблеї прийняти резолюцію, що закликає держави-члени сприяти сталому розвитку потенціалу в боротьбі з кіберзлочинністю на глобальному рівні. Хоча окремі країни активно інвестують у зміцнення своїх кримінально-правових систем, посилення глобальних можливостей у боротьбі з кіберзлочинністю часто вимагає співпраці у форматі «донор – реципієнт», коли країна, що має необхідні знання, технології та досвід, надає підтримку іншим державам у розвитку їхніх можливостей [13, с. 83]. Рада Європи також дотримується такого підходу, визнаючи розбудову потенціалу як важливий інструмент у боротьбі з кіберзлочинністю та класифікує різні типи програм для підвищення спроможностей, які реалізуються по всьому світу. Ці програми можуть включати підтримку розробки стратегій боротьби з кіберзлочинністю, оновлення або створення нових законодавчих актів із забезпеченням верховенства права, створення систем моніторингу кіберзлочинності, формування або зміцнення спеціалізованих підрозділів кіберзлочинності в поліції чи прокуратурі, удосконалення криміналістичних можливостей, проведення тренінгів для правоохоронців, прокурорів та суддів, а також встановлення механізмів державно-приватного співробітництва для ефективного розслідування кіберзлочинів [13, с. 84].

Загалом законодавство ЄС забезпечує захист споживачів при покупках товарів або послуг через інтернет, проте кількість осіб, які стають жертвами інтернет-шахрайства, постійно зростає. Шахрайство в ЄС, відповідно до визначення спільної групи країн ЄС з боротьби з інтернет-шахрайством (на чолі з ECC Lithuania та за участю ECC Ireland, ECC Belgium і ECC Slovenia), є навмисним обманом, спрямованим на особисту вигоду або завдання шкоди іншій особі. Інтернет-шахрайство включає шахрайські дії, що здійснюються через інтернет, зокрема у вигляді обману при електронних покупках або за допомогою інтернет-послуг, таких як чати, електронні листи, дошки оголошень чи програмне забезпечення, які використовуються для маніпулювання жертвами або їх експлуатації. Це може включати підроблені аукціони, неприємні продукти, що не будуть доставлені, шахрайства з кредитними і дебетовими картками, крадіжку особистих даних та фішинг [14]. Враховуючи зазначене, не є дивним, що боротьба з такими злочинами здійснюється за допомогою підрозділів Європейського відділу з протидії шахрайству та Європолу [12, с. 209].

Варто відзначити, що для боротьби з кіберзлочинністю, яка включає шахрайство через Інтернет, ряд іноземних країн створили спеціалізовані органи, метою яких є розробка та реалізація політики у сфері кібербезпеки. Формування національної політики з кібербезпеки здійснюють як органи загальної компетенції, так і спеціально створені структури. Серед органів загальної

компетенції можна виділити Комітет з питань безпеки Фінляндії, Центр захисту національної інфраструктури Великобританії, Управління національної безпеки Чехії, Національне управління з питань безпеки та контртероризму і Міністерство адміністрації та впровадження цифрових технологій Польщі. У Франції діє Національна служба безпеки інформаційних технологій, у Великобританії – Управління кібербезпеки та інформаційного забезпечення, а в Австрії функціонує Керівна група з кібербезпеки [15, с. 56; 10, с. 172].

У Сполучених Штатах Америки (далі – США) боротьба з досліджуваним видом злочинності здійснюється через Федеральне бюро розслідувань, яке має в своєму складі Центр скарг на інтернет-злочинність. Цей Центр приймає онлайн-скарги про злочини, подані безпосередньо потерпілими або третіми особами [16; 12, с. 210]. На веб-сайті ФБР регулярно оновлюються переліки найпоширеніших видів інтернет-шахрайств, а також інформація про фізичних та юридичних осіб, які підозрюються або підозрювались у вчиненні таких злочинів. Крім того, публікуються рекомендації щодо захисту від інтернет-шахраїв та списки шкідливих програм для комп'ютерної та мобільної техніки [12, с. 210].

Згідно з доповіддю ФБР США за 2017 рік щодо злочинів в інтернеті, Центр скарг на комп'ютерні злочини (IC3) отримав близько 300 тисяч звернень від жертв онлайн-шахрайства, загальна сума збитків перевищила 1,4 мільярда доларів. Це означає, що щодня понад 800 осіб у США ставали жертвами інтернет-шахрайств, загальна сума яких складала більше 3,5 мільйона доларів на день. Зазначені дані включають тільки зареєстровані випадки правопорушень [17; 3, с. 90].

За звітом ФБР «Про інтернет-злочини» (Internet Crime Report) за 2020 рік [18], найпоширенішим типом кіберзлочинів є інтернет-шахрайство (фішинг, вишінг, смішинг). Це ж підтверджує українська компанія «Опендатабот», яка на підставі аналізу даних основних публічних реєстрів країни вважає шахрайство найпопулярнішою категорією кіберзлочинів [19; 20; 21, с. 449]. Статистичні дані щодо інтернет-шахрайства збираються як на міжнародному, так і на національному рівнях. Наприклад, Федеральна торгова комісія США опублікувала звіт, в якому зазначено, що в 2021 році шахраї викрали майже $770 млн у користувачів соціальних мереж. Всього ж жертвами цих правопорушників стали 95 млн осіб. Також варто відзначити, що у 2020 році шкода від шахрайських дій становила $258 млн, що значно менше в порівнянні з 2021 роком [22; 23, с. 190]. Так, у США у 2020 р. загальний обсяг транскордонного шахрайства склав 33 968 випадків, із заявленими збитками у розмірі 91,95 млн дол. США, у порівнянні з 14 797 заявами та зі збитками, у розмірі 40,83 млн дол. США, 5 років тому. Ці скарги включали шахрайство при покупках в інтернеті, спотворення інформації про товари, випадки, коли товари не були доставлені, та проблеми із поверненням коштів. Сполучені Штати посіли перше місце серед десяти країн з розвиненою електронною торгівлею за кількістю поданих заяв та скарг на шахрайство в мережі «Інтернет» [24; 25].

Наразі ФБР доповідає американському уряду про зусилля щодо контролю за боротьбою з організованими злочинними групами, виділяючи три основні категорії: італійську мафію, близькосхідні та африканські злочинні угруповання. Проте, на думку керівництва ФБР, етнічний характер цих груп поступово стає менш виразним, оскільки вони прагнуть інтегруватися в легальний бізнес. Це призводить до створення «вільних конфедерацій» злочинних осередків, які пов'язані не родинними зв'язками, а винятково економічними інтересами [26]. Така зміна структури допомагає злочинцям успішно організовувати нелегальну торгівлю наркотиками, контрафактними алкоголем і паливом, проституцією, нелегальною міграцією, шахрайствами з кредитними картками та наданням кредитів під високі відсотки [27].

Так, у результаті спільної роботи правоохоронних органів, представників електронного бізнесу, громадськості та науковців у США були офіційно розроблені стабільні механізми захисту інтернет-магазинів від різноманітних видів шахрайства, які включають впровадження превентивних заходів для зменшення ризиків у сфері електронної комерції. До таких заходів належать: регулярні аудити безпеки сайту для перевірки відповідності стандарту PCI DSS, постійний моніторинг сайту на наявність підозрілої активності, а також використання сервісу перевірки адрес (AVS); використання кодів CVV2, CVC2 – захисного коду платіжних карток, який закодований у магнітній смузі. Цей код потрібний для того, щоб банк міг ідентифікувати клієнта при оплаті товарів та послуг карткою онлайн та офлайн; зберігання обмеженої кількості інформації; введення обмежень на кількість покупок і загальну суму, які онлайн-магазин може прийняти від одного користувача протягом доби; перевірку відповідності IP-адреси і адреси кредитної картки; а також використання програмного забезпечення для боротьби з шахрайством, таких як Kount, Riskified, Forter, Signifyd, ClearSale, CyberSource, Feedzai, Ravelin, Sift, Fraud.net, Nethone,

Precognitive, SEON, FraudLabs Pro. Ці програми автоматизують процеси перевірки на шахрайство під час здійснення платежів, блокують підозрілі пристрої, скасовують шахрайські замовлення та виконують інші функції для забезпечення безпеки [28; 25, с. 221–223].

На прикладі США виділимо щонайперші завдання запобігання електронному комерційно-торгівельному шахрайству в Україні: 1) створення Єдиної інформаційної системи профілактики шахрайства у сфері електронної комерції та торгівлі, яка поєднуватиме різноманітні інформаційні ресурси, платформи та бази даних про шахраїв; 2) запровадження політики належного корпоративного управління; 3) упровадження дієвих законодавчих ініціатив щодо належного регулювання комерційної реклами та / або просування комерційних продуктів або послуг; установлення кримінальної відповідальності за злом та крадіжку в мережі, знищення приватної та / або секретної інформації; 4) реформування інституту кримінальної відповідальності за електронне торговельно-комерційне шахрайство; 5) використання новітніх електронних систем та досягнень штучного інтелекту у запобіганні електронному комерційному шахрайстві; 6) популяризація електронної комерції через онлайн та офлайн-магазини; 7) посилення міжнародного співробітництва та залучення громадськості до соціально-виховної роботи з профілактики шахрайства в сфері електронної торгівлі [25].

Низка науковців вказують на те, що через обмеженість ресурсами малий бізнес може бути особливо спустошений втратою коштів від шахрайства. Автори зазначають, що такі обмеження в більшості малих організацій часто означають мінімум інвестицій для боротьби з шахрайством, що робить ці організації більш вразливими до економічних зловживань [29, с. 161]. М. М. Єфімов підкреслює, що у 2015 році компанія «Ubiquiti Networks», що спеціалізується на комп'ютерних мережах та базується в США, стала жертвою фішингової атаки, внаслідок якої було втрачено 46,7 млн доларів. Зловмисник, який видавав себе за виконавчого директора компанії та її адвоката, наказав головному бухгалтеру здійснити низку переказів для закриття секретної угоди. За 17 днів компанія перерахувала 14 банківських трансакцій на рахунки в Росії, Угорщині, Китаї та Польщі. Інцидент став відомим компанії лише після того, як ФБР повідомило, що її банківський рахунок у Гонконзі, ймовірно, став жертвою шахрайства. Це дозволило компанії зупинити подальші перекази та спробувати повернути якнайбільше з вкрадених 46,7 млн доларів, що становило близько 10% її готівкових активів [30, с. 120; 31, с. 97].

Цікавим є досвід Китайської Народної Республіки. Кожен користувач китайського сегменту інформаційного простору при реєстрації в соціальних мережах і на інших сайтах зобов'язаний вводити паспортні дані, інакше доступ до таких сайтів для цього користувача буде закритий. Такі заходи були викликані поширенням шахрайства в кіберпросторі КНР. Вони суттєво вплинули на зовнішній вигляд кіберпростору Китаю, фактично знищивши свободу спілкування. Однак свій внесок у протидію кіберзлочинності ці нововведення зробили – рівень кіберзлочинності в соціальних мережах Китаю різко знизився [32, с. 110].

В Японії діє Закон «Про несанкціоноване проникнення в комп'ютерні мережі» 2000 року. Він не виділяє комп'ютерне шахрайство як самостійний вид злочинів, але встановлює відповідальність за несанкціоноване проникнення в комп'ютерні мережі з метою викрадення [32, с. 110].

Так, злочинні угруповання різного етнічного складу, такі, наприклад, як нігерійці та румуни, об'єдналися для створення міжнародних мереж, які займаються інтернет-шахрайством і схемами відмивання грошей. Для приховування своїх дій вони використовують передові технології, зокрема метод «Фаст Флукс» (Fast Flux) – технологію, яка дозволяє приховувати команди та контроль ботнетів (мереж комп'ютерів, заражених автономним програмним забезпеченням) [33].

У Стратегії попередження злочинності штату Новий Південний Уельс (Австралія) на 2015–2017 роки також було заплановано включення стратегії, що передбачала можливість для громадян надсилати повідомлення про злочини через мобільні телефони, планшети та інші пристрої. Для цього необхідно було пройти реєстрацію та отримати доступ до заповнення спеціально розроблених анкет з детальною інформацією щодо таких злочинів, як крадіжки, грабежі, шахрайство тощо [34; 35, с. 148]. В Австралії зокрема наголошують на важливості регулярного оприлюднення інформації про випадки шахрайства та накладені покарання [36]. Поліція Квінсленда зазначає, що значна частина шахрайських операцій з кредитними картками в країні здійснюється злочинцями з Румунії [37], причиною цього є те, що багато з них мають технічну освіту, зокрема в галузі математики та інформатики (як програмісти чи працівники обчислювальних центрів) [38].

Цікавою є думка С. С. Чернявського, згідно з якою аналіз вітчизняного та міжнародного досвіду у проведенні судово-бухгалтерських, фінансово-економічних, почеркознавчих, техніко-криміналістичних та комп'ютерно-технічних експертиз є важливим кроком для вдосконалення

методик розслідування фінансових шахрайств [39, с. 19]. І дійсно, для удосконалення методики розслідування шахрайства, що вчиняється через мережу «Інтернет», необхідно розглянути питання призначення окремих видів експертиз [40, с. 162].

Слушно з цього приводу відзначає К. В. Малишев, О. О. Хробуст та І. М. Чайка, що вивчення міжнародного досвіду у сфері запобігання шахрайству є важливим для розвитку вітчизняної системи попередження злочинів і включає кілька ключових аспектів: передові методи боротьби з кримінальними правопорушеннями повинні бути застосовані при формуванні інституційних, правових, організаційних та інформаційних компонентів реформ; для боротьби з транскордонною злочинністю критично важливе співробітництво з правоохоронними органами інших країн; ресурсне забезпечення правоохоронних органів України ще не досягло рівня, який забезпечив би ефективну протидію злочинності, охорону громадського порядку та безпеку соціальних систем [41, с. 144; 42, с. 70–71].

Висновки. Отже, підсумовуючи вище викладене, дослідженням установлено, що більшість іноземних країн не містять спеціальних норм, які регламентують відповідальність за шахрайство, що вчиняється з використанням мережі «Інтернет», відповідно підходи до протидії такому злочину обумовлені особливостями національного законодавства. Отже, для пошуку ефективних моделей протидії шахрайству, що вчиняється з використанням мережі «Інтернет», було вивчено іноземний досвід та структуру їх спеціальних підрозділів, поліцейських відомств, а також їх функції, що абсолютно різняться за своєю сутністю. Так, у європейських країнах та США функції протидії поступаються місцем запобіганню, на відмінну від вищевказаних країн та США, азіатські держави суворо дотримуються жорстких репресивних заходів. На основі опрацьованого та узагальненого сучасного передового іноземного досвіду розроблено науково обґрунтовані рекомендації щодо протидії правоохоронними органами шахрайству, що вчиняється з використанням мережі «Інтернет».

Список використаних джерел:

1. Вінцук В. В. Шляхи удосконалення протидії організованій злочинності за часів Незалежності України. *Вісник Луганського державного університету внутрішніх справ імені Е. О. Дідоренка.* 2013. Спецвип. № 6. С. 293.

2. Підболячний М. В. Запобігання корисливим насильницьким злочинам, що вчиняються етнічними організованими злочинними групами: автореф. дис. ... канд. юрид. наук: 12.00.08 / ПрАТ «ВНЗ «Міжрегіон. акад. упр. персоналом». Київ, 2019. 21 с.

3. Лефтеров Л. В. Загальносоціальні заходи запобігання шахрайству, що вчиняється шляхом використання засобів електронних комунікацій. LEX PORTUS. № 1 (15). 2019. С. 89-101. DOI 10.26886/2524-101X.1.2019.6.

4. Охріменко І. М. Компаративістика у дидактичному проектуванні процесу підготовки поліцейських. *Світовий досвід підготовки кадрів поліції та його впровадження в Україні:* матеріали Міжнар. наук.-практ. конф. (Дніпропетровськ, 17 берез. 2016 р.). Дніпропетровськ: Ліра ЛТД, 2016. С. 66−67.

5. Таран Т. Г. Запобігання шахрайству, що вчиняються жінками в Україні: дис. канд. юрид. наук: 12.00.08. Київ, 2019. 235 с.

6. Шапочка С.В. До питання боротьби з шахрайством, яке вчиняється з вико-ристанням можливостей мережі Інтернет. Інформаційна безпека та кібершахрайство: матеріали Міжнар. наук.-практ. конф. Внутрішні та зовнішні загрози національній безпеці держави, (Київ, 2 квітня 2013 р.), НАВС. Київ : ТОВ «Три К», 2013. С.188-191.

7. Павлова Н. В. Основні профілактичні заходи при розслідуванні кримінальних правопорушень,вчинених шляхом шахрайства. Вісник ЛДУВС ім. Е.О. Дідоренка. 2023. Вип.1(101). С. 288-298. DOI:10.33766/2524-0323.101.288-298.

8. Севрук В. Г. Протидія злочинам, що вчиняються організованими групами і злочинними організаціями, які сформовані на етнічній основі: теорія та практика: монографія. Київ: «Видавництво Людмила», 2022. 1092 с.

9. Качашвілі К. С. Проблема інтернет-шахрайства в Україні та способи боротьби із ним. URL: http://dspace.puet.edu.ua/bitstream/123456789/9520/1/%D0%9A%D0%B0%D1% 87%D0%B0%D1%88%D0%B2%D1%96%D0%BB%D1%96%20%D0%9A.%D0 %A1..pdf.

10. Коба В. Б. Теоретичні та праксеологічні засади методики розслідування шахрайства у сфері е-комерції. Дисертація на здобуття наукового ступеня кандидата юридичних наук за спеціальністю 12.00.09 – кримінальний процес та криміналістика; судова експертиза;

оперативно-розшукова діяльність. – Дніпропетровський державний університет внутрішніх справ, Дніпро, 2024. 266 с.

11. Пістунов І. М., Кочура Є. В. Безпека електронної комерції : навч. посіб. Дніпропетровськ : НГУ, 2014. 125 с.

12. Кривенко О. І. Міжнародний досвід протидії шахрайствам, що вчиняються через мережу Інтернет (на прикладі Європейського Союзу та Сполучених Штатів Америки). Форум права: електрон. наук. фахове вид. 2017. № 5. С. 208–212.

13. Гуцалюк М.В. Шляхи посилення спроможностей правоохоронних та інших державних органів у сфері боротьби з кіберзлочинністю. Інформація і право. 2020. № 3(34). С. 75-87.

14. Fraud in cross-border e-commerce. URL: http://ecc-croatia.hr/resources/files/Fraud%20in%20crossborder%20e-commerce.pdf.

15. Петровський О. М., Лівчук С. Ю. Проблеми боротьби з кіберзлочинністю: міжнародний досвід та українські реалії. Молодий вчений. 2019. № 12/1. С. 55-59.

16. Scams and Safety. Internet Fraud. URL: https://www.fbi.gov/scams-and-safety/common-fraudschemes/internet-fraud.

17. Smith, S.S. (2017). Internet crime report. https://www.ic3.gov/Home/AnnualReports?redirect=true.

18. Internet crime report 2020. *Federal bureau of investigation. Internet crime complaint center.* URL: https://www.ic3.gov/Media/PDF/AnnualReport/ 2020_IC3Report.pdf.

19. За п'ять років кіберзлочинність в Україні виросла вдвічі. URL: https://www.epravda.com.ua/news/2019/10/21/652782/.

20. Чаплик М. М. Український вимір кіберзлочинності крізь призму окремих типів кіберзлочинців. *Науковий журнал Габітус.* 2020. Вип. 11 С. 83–87. DOI: https://doi.org/10.32843/2663-5208.2020.11.14.

21. Павленко С. О. Основи оперативно-розшукової тактики : монографія. Київ : Людмила, 2022. 624 с.

22. Шахраї обікрали користувачів соцмереж на $770 млн у 2021 році: як не стати жертвою. ФОКУС. URL : https://focus.ua/uk/digital/504782-moshennniki-obokrali-polzovateleysocseteyna-770-mln-v-2021-godu-kak-ne-stat-zhertvoy.

23. Березняк В. Запобігання шахрайству в Інтернеті. Науковий вісник Дніпропетровського державного університету внутрішніх справ. 2023. № 1. С. 190-196.

24. E-Commerce and Consumer Protection in India. Journal of Business Ethics, 2021. URL: https://link.springer.com/ article/10.1007/s10551-021-04884-3.

25. Коновалова І. О. Досвід запобігання шахрайству в сфері електронної торгівлі в США. Науковий вісник Ужгородського Національного Університету, Серія ПРАВО. 2021. Випуск 68. С. 220-224. https://visnyk-juris-uzhnu.com/wp-content/uploads/2022/03/40.pdf.

26. 200th Anniversary of the Office of the Attorney General, 1789–1989. Wash.: U. S. Department of Justice, 1991. II. P. 117.

27. Господаренко В. М. Державна кримінальна політика США і боротьба проти організованої злочинності. *Правова позиція.* 2016. № 2. С. 187.

28. Merchant Fraud Journal: eCommerce Fraud News Publication. URL: https://www.merchantfraudjournal.com/topecommerce-fraud-protection-solutions/.

29. Yefimov M., Pavlova N., Fedchenko V., Pletenets V., Kryvopusk O. Foreign experience in legal regulation of fraud investigation. Revista De La Universidad Del Zulia. 2022. 13 (38). P. 159–168.

30. Єфімов М. М. Криміналістичний аналіз окремих сучасних видів шахрайства: проблемні питання. Збірник наукових праць «Науковий вісник публічного та приватного права». 2021. Випуск 5. С. 116–121.

31. Жилін А. Е. Теоретичні та праксеологічні засади методики розслідування шахрайства у сфері використання банківських електронних платежів. Дисертація на здобуття наукового ступеня кандидата юридичних наук (доктора філософії) за спеціальністю 12.00.09 – кримінальний процес та криміналістика; судова експертиза; оперативно-розшукова діяльність (081 – Право). – Науково-дослідний інститут публічного права; Дніпропетровський державний університет внутрішніх справ, Київ, 2023.226 с.

32. Піцик Ю. М. Міжнародний досвід у сфері протидії злочинам проти власності, що вчиняються у кіберпросторі. Прикарпатський юридичний вісник. 2016. Вип. 4(13). С. 107-111.

33. Оцінка загроз організованої злочинності в Європейському Союзі. *OCTA: звіт.* 2011. 52 с.

34. Crime prevention strategy 2015–2017. URL: https://www.police.nsw.gov.au/__.../ Crime_ Prevention_Strategy_2.

35. Бугера О. Сучасні кримінологічні стратегії запобігання злочинності з використанням мережі інтернет: зарубіжний досвід. Підприємництво, господарство і право. 2019. № 1. С. 146-149.

36. Prenzler Tim. Responding to welfare fraud: The Australian experience, AIC Report in Research and Public Policy Series No. 119. URL: http://www.aic.gov.au/media_library/publications/ rpp/119/rpp119. pdf.

37. Romanian scammers targeting Sydney ATMs. 2013. 15 August. URL: https://www.theaustralian.com.au/news/nation/romanian-scammers-targeting-sydney-atms/story-e6frg6nf-1226697744244.

38. Why Romanians specialise in ATM skimming. URL: https://www.smh.com.au/national/ why-romanians-specialise-in-atm-skimming-20111215-1ow7w.html.

39. Чернявський С. С. Теоретичні та практичні основи методики розслідування фінансового шахрайства : автореф. дис. … д-ра юрид. наук : 12.00.09 / Національна академія внутрішніх справ. Київ, 2010. 36 с.

40. Коваленко І. О. Розслідування шахрайства у сфері використання банківських електронних платежів. Дисертація на здобуття наукового ступеня доктора філософії за спеціальністю 081 – Право. – Дніпропетровський державний університет внутрішніх справ. Дніпро, 2022. 229 с.

41. Малишев К.В., Хробуст О.О. Особливості правоохоронної діяльності в зарубіжних країнах. Вчені записки ТНУ імені В.І. Вернадського. Серія: Державне управління. 2020. Том 31 (70). № 5. С. 143-150.

42. Чайка І.М. Кримінологічна характеристика та запобігання шахрайству в Україні. Дисертація на здобуття ступеня вищої освіти доктора філософії за спеціальністю 081 – Право. – Донецький державний університет внутрішніх справ Міністерства внутрішніх справ України, Кропивницький. 2023. 296 с.