УДК 343.985 DOI: 10.37025/1992-4437/2024-42-2-63

В. Б. Коба,
кандидат юридичних наук,
начальник Департаменту забезпечення діяльності
Голови Національної поліції України
вул. Богомольця, 10, м. Київ, 01601, Україна
ORCID: https://orcid.org/0009-0002-1201-6205
email: valokt@gmail.com
тел.: +38(093)559-84-50

ЗАСОБИ КРИМІНАЛІСТИЧНОЇ ПРОФІЛАКТИКИ У КРИМІНАЛЬНИХ ПРОВАДЖЕННЯХ ЩОДО ШАХРАЙСТВА У СФЕРІ Е-КОМЕРЦІЇ

Анотація. Висвітлено профілактичні заходи, які безпосередньо здійснює слідчий, зокрема у процесі забезпечення кримінального провадження, проведення окремих слідчих (розшукових) дій, а також тактичних операцій. Наголошено на значенні експертної профілактики, а також профілактичних заходах інформаційно-виховного і віктимологічного характеру тощо. Акцентовано на нагальній потребі створення механізму оперативного реагування на шахрайство у сфері комерційної діяльності через блокування активів шахрайських компаній і зупинення їхньої діяльності. Під час дослідження застосовано такі методи наукового пізнання: формально-логічний, функціональний, системний, статистичний, метод синтезу. Наукова новизна полягає в обґрунтуванні необхідності запровадження функціонування єдиної автоматизованої системи, яка в разі підозрілих дій автоматично спрямовує запит до банківських установ, де встановлюється факт транзакції та відстежується подальший рух коштів до кінцевого рахунку / банківської картки, на яку перераховано кошти, з одночасним блокуванням рахунків. Крім того, запропоновано спеціальні заходи криміналістичної профілактики. Виокремлено складник концепції профілактики онлайн-шахрайства – системну діяльність підрозділів кіберполіції з моніторингу соціальних мереж і медіа. Зосереджено увагу на використанні можливостей інформаційних ресурсів Національної поліції України, у якій створена і тривалий час функціонує система відділів комунікації, які співпрацюють із регіональними та всеукраїнськими медіа, мають власні сайти, вебсторінки в соціальних мережах, виробляють власний аудіовізуальний контент і виявляють високу активність в інших медіа, зокрема й у соціальних мережах та електронних медіа. Практична значущість дослідження полягає в тому, що розроблені пропозиції можуть стати основою методичних рекомендацій щодо застосування заходів криміналістичної профілактики під час розслідування шахрайства у сфері е-комерції.

Ключові слова: онлайн-шахрайство; комерційне інтернет-шахрайство; профілактична діяльність; профілактичні заходи; система «AntiFraud»; досудове розслідування; причини й умови, що сприяють вчиненню шахрайства у сфері е-комерції.

Вступ

Слідчий під час досудового розслідування зобов'язаний виявляти обставини, причини й умови, що сприяли вчиненню кримінального правопорушення, аби був установлений факт об'єктивної дійсності, тобто об'єктивна істина (Havryliuk, 2020; Matviichuk, 2022, s. 14; Dufeniuk, 2023) у кримінальному провадженні, водночас чітко усвідомлюючи необхідність виконання іншої, не менш важливої функції, а саме запобігання кримінальним правопорушенням (Ekici et al., 2022; Melander, 2023; Babenko et al., 2024) у майбутньому. Утім, стосовно змістовного складника профілактичної діяльності в криміналістичному розумінні й досі тривають дискусії (Koba, 2022, s. 291).

Аналіз досліджень і публікацій, у яких започатковано розв'язання окресленої проблеми, свідчить, що окремі аспекти криміналістичної профілактики неодноразово розглядали В. С. Березняк (Berezniak, 2023), І. О. Коновалова (Konovalova, 2021), Л. В. Лефтеров (Lefterov, 2019), Г. В. Недзельська (Nedzelska, 2022), Н. В. Павлова (Pavlova, 2023), А. В. Рейнгольд (Reinhold, 2021), С. В. Томин (Tomyn, 2019), С. О. Харитонов (Kharytonov, 2023).

Їхні праці становлять доволі змістовне та методологічне підґрунтя теорії й практики розслідування шахрайства у сфері е-комерції. Але й дотепер залишається низка дискусійних і невирішених питань, зокрема й щодо профілактичних заходів, які застосовують уповноважені службові особи під час розслідування шахрайства у сфері е-комерції.

Проблема шахрайства у сфері е-комерції останніми роками дедалі більше привертає увагу вітчизняних і зарубіжних науковців і практиків. Вони розглядають різні аспекти порушеного питання, зокрема й такі, як розслідування шахрайства у сфері використання банківських

електронних платежів (e.g., Korshykova, 2021; Kovalenko, 2021; Bondaruk et al., 2023; Chaplynskyi et al., 2024); наукові дискусії щодо проведення різних видів огляду під час розслідування шахрайства у сфері використання банківських електронних платежів (Lepei, 2024); досвід запобігання шахрайству у сфері електронної торгівлі в США (Konovalova, 2021); суб'єкти запобігання шахрайству у сфері електронної торгівлі (Kharytonov, 2023); особливості початкового етапу розслідування шахрайства в кіберпросторі, а також проблеми запобігання таким кримінальним правопорушенням (Reznik et al., 2021); зарубіжний досвід правового регулювання розслідування шахрайства, переконливі аргументи запобігання таким кримінальним правопорушенням (Yefimov et al., 2022); особливості вчинення економічних злочинів із використання інформаційних технологій (Cherniavskyi et al., 2021); захисту прав інтелектуальної власності від кіберзагроз у глобальному інформаційному середовищі (Berezniak, 2023; Chaplynskyi, & Yefimov, 2023; Sopilko et al., 2023); вчинення шахрайства в Інтернеті в умовах воєнного стану (Bryskovska, & Helemei, 2023); питання взаємодії правоохоронних органів України під час розслідування кримінальних правопорушень відповідно до міжнародних стандартів (Chaplynskyi et al., 2023); загрози та сучасні тенденції економічної злочинності (Jakubiec, & Kuliński, 2023); світові тенденції фінансового шахрайства (Dudchenko, 2023); сценарії фінансових злочинів (Snaphaan, & van Ruitenburg, 2024).

А втім, попри достатню кількість праць за напрямом досліджуваної проблематики, деякі актуальні питання щодо криміналістичної профілактики у провадженнях щодо шахрайства у сфері е-комерції потребують додаткового висвітлення.

Матеріали та методи

Мета публікації полягає у висвітленні заходів профілактичної діяльності уповноважених осіб щодо виявлення й усунення причин та умов вчинення шахрайства у сфері е-комерції. Для досягнення цієї мети потрібно вирішити такі завдання: виявити причини та умови, що сприяють вчиненню шахрайства у сфері е-комерції; визначити особливості профілактичної діяльності уповноважених осіб щодо усунення причин та умов вчинення шахрайства у сфері е-комерції; надати відповідні науково-методичні рекомендації в контексті цього дослідження.

Методологію аналізу проблеми становлять загальнонаукові та спеціальні методи наукового пізнання. Методи дослідження: формально-логічний використовувався для аналізу наукових концепцій, що відтворюють особливості дослідження шахрайства; функціональний – для визначення перспективних напрямів застосування криміналістичної профілактики; системний – формування заходів профілактичної діяльності; статистичний – аналізу судово-слідчої практики, узагальнення статистичних даних, матеріалів кримінальних проваджень. На основі синтезу сформульовано загальні висновки за темою дослідження.

Результати та обговорення

Успішне розв'язання проблеми встановлення причин та умов конкретного кримінального правопорушення можливе лише тоді, коли це завдання чітко усвідомлене (Koba, 2022). Утім, не применшуючи значення встановлення причин та умов, які сприяють вчиненню шахрайства, науковці (in particular, Pavlova, 2023, s. 288) вважають, що «не менш важливим завданням є й розробка та застосування спеціальних заходів криміналістичної профілактики».

Слушною є думка про припинення випадків комерційного інтернет-шахрайства і запобігання їм саме технічними засобами. Приміром, дослідження технічних можливостей електронно-обчислювальної техніки й особливостей функціонування Інтернету дає змогу виявляти певні факти, що можуть говорити про шахрайські дії, запобігати подальшій їх реалізації. Науковці (Yarovenko et al., 2018; Reinhold, 2021) із метою профілактики шахрайства навіть розробили концептуальну модель виявлення ознак кіберзагроз у транзакціях користувачів мобільного та інтернет-банкінгу. Зокрема, ґрунтуючись на аналізі статистичних даних, можна виокремити такі показники, що свідчать про можливе виникнення кіберзагрози в процесі виконання банківської операції, а саме:

транзакція має ознаки кіберзагрози, якщо її ініційовано на території іншої країни. У більшості банків узвичаєно практику, коли клієнт повідомляє банк про його виїзд за кордон і зазначає відвідувані країни. Інакше служба безпеки банку може заблокувати картку, якщо за нею ініціюватимуть транзакції з іншої країни. Адже хакери, зламуючи доступ до мобільного або інтернет-банкінгу та привласнюючи чужі кошти, застосовують спеціальні програми для шифрування їх місцеположення;

на ймовірність виникнення кіберзагрози впливає тип пристрою, з якого виконувалася транзакція. Послуговуються різними способами злому мобільних пристроїв і комп'ютерів, за допомогою яких зловмисники з легкістю отримують доступ до мобільного та інтернет-банкінгу користувачів банківських послуг. Також банк не в змозі контролювати, хто є користувачем і де він застосовує пристрій. Здебільшого такі операції можуть містити ознаки кіберзагроз;

тип транзакції впливає на ймовірність виникнення ознак кіберзагрози. Зловмисники через розмаїття типів банківських транзакцій вдаються до нових заходів, спрямованих на заволодіння чужими коштами та порушення безпеки інформації в банку;

обнуління рахунків клієнтів банку свідчить про ймовірні ознаки кіберзагроз. Оскільки сьогодні доволі поширені безготівкові розрахунки, на банківських рахунках завжди є якісь кошти. Якщо під час транзакції відбувається зняття всієї суми, можливо, це порушення користування рахунком або несанкціоноване зняття коштів.

Серед розмаїття підсистем криміналістичної профілактики та великої кількості суб'єктів, що реалізують окремі напрями превентивної діяльності, вирізняють (Filipenko et al., 2019, s. 155) і експертну профілактику, що вважають складним системним утворенням, основою якого є діяльність експертів на базі своїх спеціальних знань, які виявлятимуть обставини, що сприяли вчиненню кримінальних правопорушень. Виявлення таких обставин, наголошують науковці, може стати основним експертним завданням, для вирішення якого і призначалася експертиза, або це може бути супутній «продукт» експертної діяльності, що «з'являється», коли вирішують інші експертні завдання, які не ставили за мету виявлення криміногенних чинників. Допустимим є також виявлення криміногенних чинників та обставин, що сприяють вчиненню кримінальних правопорушень, у процесі узагальнення напрацьованої експертної практики в окремій судово-експертній установі або в разі підготовки відповідних оглядів, звітів, аналітичних довідок.

Так, саме висновки експертів, засвідчив аналіз кримінальних проваджень щодо шахрайства у сфері е-комерції, значною мірою позначаються на рівні запобігання подальшим спробам шахрайських дій, що їх вчиняли окремі особи (група осіб). До того ж у 67 % проваджень завдяки ідентифікаційним експертним дослідженням встановлено аналогічні факти, що, як наслідок, складали один ланцюг шахрайських операцій у сфері е-комерції (Koba, 2022, s. 292–293).

У разі коли встановлені причини кримінальних правопорушень можуть сприяти вчиненню аналогічних правопорушень на інших підприємствах, в установах чи організаціях, зокрема й в інших сферах життєдіяльності людини, керівник експертної служби має, наголошують фахівці (e.g., Filipenko, 2020, s. 226), безпосередньо повідомляти відповідні правоохоронні органи, щоб запобігти їх вчиненню. Водночас проблему експертної ініціативи зумовлено не лише межами кримінального провадження, а й обставиною, яка полягає в тому, що праву експерта фактично не відповідає нічий обов'язок реалізувати ту додаткову інформацію, яку з власної ініціативи отримує експерт. Тож може статися, що ініціатива експерта буде нереалізованою, а його висновки – невикористані. Найчастіше трапляються ситуації, коли з ініціативи експерта розробляють ті чи ті профілактичні рекомендації.

Коли йдеться про профілактичні заходи, які безпосередньо здійснює слідчий, напрямами їх реалізації, як вважають фахівці (Berezniak, 2020; Koba, 2022, s. 293), є заходи забезпечення кримінального провадження (затримання особи, арешт майна, тримання під вартою), окремі слідчі (розшукові) дії (огляд, допит, ін.), а також тактичні операції. Застосування запобіжних заходів спрямоване не тільки на забезпечення виконання підозрюваним покладених на нього обов'язків, а й на запобігання спробам вчинити інше кримінальне правопорушення чи продовжувати кримінальне правопорушення, у якому його підозрюють. Крім того, «саме під час ознайомлення з матеріалами кримінального провадження слідчий може виявити обставини криміногенного характеру, які вже попередньо зафіксовані у документах (актах ревізій, висновках експертів, довідках, поясненнях та показаннях інших осіб тощо)» (Tomyn, 2019, s. 323).

Слід наголосити, що запобіганню фактам шахрайства у сфері е-комерції сприяють інформаційно-аналітична забезпеченість і можливості різноманітних обліків, баз даних тощо.

До того ж профілактичні функції виконують й оперативні підрозділи кіберполіції. Зокрема, Департамент кіберполіції Національної поліції України відповідно до покладених на нього завдань (Bakaianova et al., 2020, s. 92; Reinhold, 2023, s. 119): визначає, розробляє та забезпечує реалізацію комплексу організаційних і практичних заходів, спрямованих на запобігання та протидію кримінальним правопорушенням у сфері протидії кіберзлочинності; у межах своїх повноважень вживає необхідних оперативно-розшукових заходів щодо викриття причин і умов, які призводять до вчинення кримінальних правопорушень у сфері протидії кіберзлочинності; уживає передбачених чинним законодавством заходів щодо збирання й узагальнення інформації стосовно об'єктів, зокрема й об'єктів сфери телекомунікацій, інтернет-послуг, банківських установ і платіжних систем для запобігання кримінальним правопорушенням, їх виявлення та припинення; організовує та контролює діяльність підпорядкованих підрозділів кіберполіції щодо виконання вимог законодавства України у сфері протидії кіберзлочинності; провадить серед населення роз'яснювальну

роботу з питань дотримання законодавства України у сфері використання новітніх технологій, а також захисту та протидії кіберзагрозам у повсякденному житті; вивчає позитивний вітчизняний і зарубіжний досвід боротьби з кримінальними правопорушеннями у сфері протидії кіберзлочинності та вносить пропозиції керівництву Національної поліції України щодо його впровадження; згідно з чинним законодавством збирає, узагальнює, систематизує й аналізує інформацію про криміногенні процеси та стан боротьби з кримінальною протиправністю за напрямом діяльності департаменту на загальнодержавному та регіональному рівнях, оцінює результати за окремими показниками службової діяльності, надає згідно із законодавством України звіти про результати роботи та відповідну інформацію керівництву Національної поліції України, Міністерства внутрішніх справ України, органів державної влади з питань запобігання та протидії кіберзлочинам.

А втім, профілактична діяльність правоохоронних органів під час розслідування кримінальних правопорушень дає максимальний ефект лише тоді, коли вона, варто погодитися з науковою думкою (Volobuiev (Uklad.), 2003, s. 12), органічно поєднується з економічними, соціальними, правовими й організаційними заходами запобігання кримінальній протиправності в масштабах країни.

Водночас профілактичні заходи у правовому полі спрямовані на вдосконалення нормативно-правової бази, що становить підґрунтя єдиної державної політики забезпечення інформаційної безпеки та її реалізації. Першим кроком до досягнення цієї мети дослідниця (Kachashvili, 2019, Cherven 7, s. 130) вважає «визначення кібернетичної безпеки як самостійної сфери національної безпеки. Це дасть змогу формувати засади державної політики у сфері забезпечення кібернетичної безпеки України шляхом визначення основних реальних загроз національній безпеці, основних напрямів державної політики та основних функцій суб'єктів щодо забезпечення національної безпеки в цій сфері». Крім того, запобігання кіберзлочинності ґрунтується на заходах, скерованих на зниження ризику вчинення таких кримінальних правопорушень і нейтралізацію шкідливих наслідків для суспільства (Kachashvili, 2019, Cherven 7, s. 131; Bortnyk, 2022, Traven 27, s. 16).

В організаційному аспекті серед основних проблем профілактики шахрайства постають питання спеціалізації підрозділів МВС України при організації та здійсненні профілактики таких кримінальних правопорушень, слабкої взаємодії між суб'єктами профілактики, утворення єдиного координаційного органу, ефективної системи контролю за виявленням і розслідуванням організованих кримінальних правопорушень. У цьому контексті дослідниця (Nedzelska, 2022, s. 212) з-поміж заходів запобігання комп'ютерному шахрайству виокремлює: створення спеціалізованих центрів збирання й аналізування інформації про факти шахрайства в Інтернеті. Їхня діяльність має орієнтуватися не так на констатацію кримінально протиправних посягань, як на вироблення дієвих профілактичних заходів. Серед напрямів діяльності цих центрів – збирання інформації про потенційно небезпечні об'єкти та їх блокування; організація підбору, навчання й інструктажу працівників служб комп'ютерної (інформаційної) безпеки суб'єктів господарювання; упровадження програми навчання громадян основ комп'ютерної безпеки під час фінансових операцій через інформаційні мережі, спілкування в соціальних мережах та ін., інформування через медіа про нові види комп'ютерного шахрайства; розроблення та використання спеціального програмного забезпечення, зокрема й антивірусних програм або програм ідентифікації користувача; розширення системи з протидії кримінальним правопорушенням у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку та формування єдиної державної бази інтернет-шахраїв.

Розгляньмо заходи профілактики шахрайства, пов'язаного з комерційною діяльністю в онлайн-режимі. У цьому аспекті, убачається, варто повести мову насамперед:

про нагальну потребу створення механізму оперативного реагування на шахрайство у сфері комерційної діяльності через блокування активів шахрайських компаній і зупинення їхньої діяльності, а також ведення податковими органами інформаційної бази про раніше судимих за шахрайство підприємців, зазначення таких відомостей у виписці з Єдиного державного реєстру юридичних осіб, а також розвиток системи громадських порталів, що ведуть реєстр неблагонадійних суб'єктів комерційної діяльності (Nedzelska, 2022, s. 212), зокрема й в онлайн-режимі;

профілактичні заходи інформаційно-виховного та віктимологічного характеру, приміром, через медіа та інші інформаційні ресурси, якими реалізується метод поширення інформаційного контенту. Правоохоронні органи, наголошують фахівці (e.g., Lefterov, 2019, s. 97), також можуть брати участь у таких заходах через спеціалізовані підрозділи та пресцентри Національної поліції України;

комплекс ефективних заходів у протидії інтернет-шахрайству, що їх мають вживати юридичні особи. Для убезпечення банківських операцій компанії необхідно, радять фахівці (Berezniak,

2023, s. 192), виокремити комп'ютери, що міститимуть фінансові дані та реквізити юридичної особи, а для вирішення решти питань, зокрема небанківських операцій, передбачити іншу комп'ютерну техніку з доступом до Інтернету – комп'ютери загального користування. Крім того, за умови виведення комп'ютера з матеріально-технічної бази юридичної особи, слід пам'ятати про необхідність створення резервної копії наявної інформації й очищення твердого магнітного диска тощо;

заборону інтернет-торгівлі суб'єктам, які не розкривають реєстраційної інформації, та гармонізацію законодавчої бази України з міжнародно-правовими стандартами, щоб не виникало непорозумінь під час е-комерції.

Отже, зважаючи на тенденції до значного збільшення кількості зареєстрованих фактів онлайн-шахрайства під час дії воєнного стану, убачається доцільним (Koba, 2024, s. 164–165) рекомендувати Національній поліції України, слідчі (дізнавачі) якої відповідно до ст. 216 КПК України уповноважені на здійснення досудового розслідування кримінальних правопорушень, передбачених ст. 190 КК України, розгорнути «агресивну» інформаційно-роз'яснювальну кампанію серед населення. Її сутність полягає в активній взаємодії Національної поліції України та її територіальних підрозділів з органами місцевого самоврядування, громадськими організаціями, державними та недержавними медіа, закладами вищої та середньої освіти, представниками бізнесу щодо виготовлення та доведення до відома якнайбільшої кількості громадян інформаційних матеріалів профілактичного характеру. Для охоплення максимальної кількості населення убачається доцільним розміщення інформаційно-роз'яснювальної інформації на білбордах і сітілайтах. Виготовлені постери, плакати та листівки вивішуються у громадському транспорті, на вокзалах, у торговельно-розважальних центрах, на автозаправних комплексах. Не мають залишатися поза увагою місця масового перебування громадян: медичні заклади, поштові відділення, навчальні заклади, магазини, приміщення органів влади та органів місцевого самоврядування.

Певний потенціал закладений і у використанні можливостей інформаційних ресурсів самих правоохоронних органів, насамперед Національної поліції України, у якій створено й тривалий час функціонує система відділів комунікації, що співпрацюють із регіональними та всеукраїнськими медіа, мають власні сайти, сторінки в соціальних мережах, виробляють власний аудіовізуальний контент, проявляють високу активність зокрема й у соціальних мережах та електронних медіа (Koba, 2024, s. 165).

Як окремий складник концепції профілактики фактів онлайн-шахрайства, найпоширенішою схемою яких залишається непостачання замовлених товарів, убачається (Koba, 2024, s. 165–166), слід виокремити діяльність працівників правоохоронних органів із моніторингу соціальних мереж і медіа. Зокрема, аналізуючи цифровий контент на наявність скарг громадян щодо дій або бездіяльності посадових осіб під час прийняття та розгляду заяв про вчинені шахрайства, працівники правоохоронних органів можуть запобігти подальшим фактам приховування кримінальних правопорушень від обліку, а їх органи досудового розслідування – реалізувати принцип невідворотності покарання через установлення та притягнення шахраїв до кримінальної відповідальності за всі епізоди їхньої кримінально протиправної діяльності.

Варта уваги й діяльність кіберполіції, яка з метою запобігання та протидії фактам шахрайства надає відвідувачам свого офіційного сайту можливість перевірити підозрілу інформацію за такими параметрами: номер банківської картки, телефон або посилання на сайт (доступ за посиланням https://cyberpolice.gov.ua/stopfraud/), а також корисні поради, як не стати жертвою шахраїв. Крім того, на сайті передбачено зворотний зв'язок для тих, хто зазнав моральної чи матеріальної шкоди від дії шахраїв і бажає звернутися до правоохоронних органів з електронним зверненням, не виходячи з власної домівки. Зазначена послуга від кіберполіції, набувши подальшого розвитку, має інтегрувати в сервіси «Дія» – мобільного застосунку, вебпорталу і бренду цифрової держави в Україні, розробленого Міністерством цифрової трансформації України. Це доступний для більшості українців портал, де громадяни отримуватимуть державні послуги онлайн. Сервіси «Дії», якими наприкінці 2023 р. послуговувалися майже 20 млн користувачів (Koba, 2024, s. 167), можуть містити розділи, доступні й користувачам сайту кіберполіції.

Слід також зазначити, що в січні 2023 р. Департаментом кіберполіції Національної поліції України розроблено концепцію Національної системи обміну даних і блокування банківських карток (система «AntiFraud»), задіяних у шахрайських схемах. За результатами робочої зустрічі з представниками юридичних і безпекових департаментів банківських установ і платіжних систем України досягнуто спільної позиції щодо необхідності запровадження такої системи та заявлено про готовність приєднання до неї з боку провідних банків, що становлять 80 % банківського сектору України (Koba, 2024, s. 167).

Як перспективний напрям планується (Koba, 2024, s. 167) розроблення нормативно-правового

акта, який забезпечить правову основу для функціонування Національної системи «AntiFraud» на період дії воєнного стану та шести місяців після його закінчення.

За цієї концепцією вже зареєстрована інформація та зазначені потерпілим відомості (номер картки, сума збитку, дата і час транзакції) надходять до системи «AntiFraud». Після цього запит автоматично спрямовується до банківських установ, де і встановлюється факт транзакції, відстежується подальший рух коштів потерпілого до кінцевого рахунку / банківської картки, на яку правопорушник переказав кошти, з одночасним блокуванням рахунку на їх вивід. Банківська установа, отримавши зазначені відомості, дає автоматичний припис через API іншим банкам – отримувачам коштів щодо блокування банківських рахунків шахраїв і грошових коштів, з яких здійснено «обготівкування», терміном до 48 годин (Koba, 2024, s. 167).

Не менш важливим профілактичним складником боротьби з шахрайством у сфері е-комерції вбачається передбачений системою «AntiFraud» механізм блокування банківських рахунків не лише активних виконавців кримінального правопорушення, так званих шахраїв, а й їхніх імовірних співучасників, так званих дропів, реквізити платіжних карток яких використовуються у схемі протиправного заволодіння грошовими коштами потерпілих. Наслідком активної співпраці Національної поліції України та Національного банку України стали відповідні Зміни до Правил зберігання, захисту, використання та розкриття банківської таємниці, затверджені постановою Правління Національного банку України від 18 березня 2024 р. № 33 (набрали чинності з 20 березня 2024 р.). Зокрема, доповнено перелік відомостей, що мають право отримати в банківській установі правоохоронні органи, які мають відповідні повноваження, можливість отримання інформації про номер платіжної картки клієнта банку. «Інформація про номер платіжної картки допоможе правоохоронцям розслідувати кримінальні провадження про платіжне шахрайство, зокрема виманювання коштів методами соціальної інженерії, фішингу тощо. Адже платіжні операції можуть здійснюватися фактично і без використання номера рахунку, лише за номером платіжної картки» (*Dostup do bankivskoi taiemnytsi*, 2024, Berezen 20; *NBU onovyv pravyla*, 2024, Berezen 20).

Департаментом кіберполіції Національної поліції України 1 квітня 2024 р. на базі чинної системи обміну інформацією між Департаментом, банківськими установами та Українською міжбанківською асоціацією членів платіжних систем «ЄМА» «Crimechek» запроваджено оновлену її версію з удосконаленими механізмами отримання та оброблення інформації. Оновлення під назвою «AntiFraud-2024» набуло розширеного функціоналу і здатність опрацювання інформації від 85 % банківського сектору держави. Попередні її випробування працівниками Департаменту кіберполіції та 64 банківськими установами протягом квітня – серпня 2024 р. засвідчили зменшення часу оброблення запитів на 50 %. Водночас середній час надання відповіді на запит зменшився з дванадцяти до чотирьох годин, що суттєво підвищує оперативність та якість реагування правоохоронних органів на повідомлення про кримінальні правопорушення цієї категорії, а також істотно мінімізує негативні наслідки для заявника (потерпілого) у вигляді заподіяння йому реальних матеріальних збитків.

Не менш ефективним може стати прийняття Верховною Радою України у другому читанні та в цілому законопроєкту № 11043 щодо удосконалення функцій Національного банку України з державного регулювання ринків фінансових послуг (*Verkhovna Rada Ukrainy*, 2024, Liutyi 28), яким уносяться зміни до ст. 62 Закону України «Про банки і банківську діяльність» і до ст. 31 Закону України «Про платіжні послуги», якими передбачено обов'язок банківських установ розкривати банківську таємницю не пізніше 24 годин після отримання письмового (електронного) запиту від органу Національної поліції України, завданням якого є реалізація державної політики у сфері протидії кіберзлочинності. Серед переліку таких відомостей, викладених в одинадцяти пунктах, передбачені, наприклад, такі, як геопросторові дані, IP-адреса, адреса засобу дистанційної комунікації (зокрема й платіжний застосунок) або платіжного пристрою, що використовувався для платіжної операції; унікальний ідентифікатор отримувача та/або повний номер електронного платіжного засобу та/або рахунку отримувача; найменування та код еквайра (за наявності) тощо.

Сьогодні доволі актуальним є розроблення концепції протидії онлайн-шахрайству через її профілактичний складник із використанням можливостей соціальних мереж, а також національних і регіональних медіа, насамперед електронних, із застосуванням сервісів «Дії» тощо.

Висновки

Заходами профілактичної діяльності уповноважених осіб щодо виявлення й усунення причин та умов вчинення шахрайства у сфері е-комерції є: а) взаємодія Національної поліції України з органами місцевого самоврядування, громадськими організаціями, закладами освіти, представниками бізнесу щодо виявлення осіб, схильних до

антисуспільної поведінки у сфері використання комп'ютерних технологій і подальше їх узяття на облік кіберполіції; б) використання можливостей інформаційних ресурсів Національної поліції України, де створена і функціонує система відділів комунікації, які співпрацюють із медіа, мають власні сайти, сторінки в соціальних мережах, виробляють власний аудіовізуальний контент, проявляють високу активність в інших медіа, зокрема й у соціальних мережах; в) діяльність правоохоронних органів із моніторингу соціальних мереж і медіа; г) розміщення на сайті кіберполіції інформації, що надає можливість громадянам перевірити підозрілу інформацію за такими параметрами: номер банківської картки, телефон або посилання на сайт. Зазначений напрям роботи кіберполіції має набути подальшого розвитку та інтегруватися в сервіси «Дія» – мобільного застосунку, вебпорталу; ґ) створення механізму оперативного реагування на шахрайські прояви через блокування активів комерційних об'єктів; д) використання можливостей різноманітних обліків та інформаційних баз даних щодо шахрайства в Інтернеті. Крім того, наголошено на необхідності підвищення ефективності профілактичної діяльності уповноважених осіб у кримінальних провадженнях за фактами шахрайства через внесення змін до КПК України, які полягають у визначенні їхнього обов'язку виявляти причини й умови, що сприяли вчиненню кримінального правопорушення.

Подяки

Немає.

Конфлікт інтересів

Немає.

References

[1] Babenko, A. M., Chekmarova, I. M., & Palii, M. V. (2024). Viktymolohichne zapobihannia kryminalnym pravoporushenniam proty vlasnosti [Victimology prevention of criminal offenses against property]. *Yurydychnyi naukovyi elektronnyi zhurnal*, (3), 630–633 [in Ukrainian].
DOI: https://doi.org/10.32782/2524-0374/2024-3/152

[2] Bakaianova, N. M., Kubaienko, A. V., & Svyda, O. H. (2020). *Orhanizatsiia diialnosti Natsionalnoi politsii Ukrainy ta operatyvnykh pidrozdiliv*: navchalno-metodychnyi posibnyk. Odesa: Feniks. 251 s. [in Ukrainian].
https://dspace.onua.edu.ua/server/api/core/bitstreams/78ab9a6e-6934-40aa-86dd-726ea0f479d3/content

[3] Berezniak, V. S. (2020, Zhovten 17). Osnovni napriamy kryminalistychnoi profilaktyky pid chas rozsliduvannia kryminalnykh pravoporushen u sferi nerukhomosti. V *Operatyvno-rozshukova diialnist Natsionalnoi politsii: problemy teorii ta praktyky*: materialy vseukrainskoi naukovo-praktychnoi konferentsii (s. 5–8). Dnipro: Dnipropetrovskyi derzhavnyi universytet vnutrishnikh sprav [in Ukrainian].

[4] Berezniak, V. S. (2023). Zapobihannia shakhraistvu v Interneti [Prevention of fraud on the Internet]. *Naukovyi visnyk Dnipropetrovskoho derzhavnoho universytetu vnutrishnikh sprav*, (1), 190–196 [in Ukrainian].
DOI: https://doi.org/10.31733/2078-3566-2023-1-190-196

[5] Bondaruk, T. H., Bohrinovtseva, L. M., & Bondaruk, O. S. (2023). Shakhraistvo iz vykorystanniam bankivskykh platizhnykh kartok yak sposib finansuvannia teroryzmu ta separatyzmu [Fraud Using Bank Payment Cards: A Way for Financing of Terrorism and Separatism]. *Statystyka Ukrainy, 101*(2), 4–13 [in Ukrainian].
DOI: https://doi.org/10.31767/su.2(101)2023.02.01

[6] Bortnyk, S. M. (2022, Traven 27). Okremi aspekty protydii lehalizatsii dokhodiv, oderzhanykh u rezultati vchynennia kiberzlochyniv. U *Protydiia kiberzlochynnosti ta torhivli liudmy*: zbirnyk materialiv mizhnarodnoi naukovo-praktychnoi konferentsii (s. 16–17). Kharkiv: Kharkivskyi natsionalnyi universytet vnutrishnikh sprav [in Ukrainian].
https://dspace.univd.edu.ua/server/api/core/bitstreams/e791062b-5b16-4bad-bf11-7a48eece6693/content

[7] Bryskovska, O. M., & Helemei, M. O. (2023). Osoblyvosti vchynennia shakhraistva v merezhi Internet v umovakh voiennoho stanu [Peculiarities of committing fraud on the Internet in the conditions of martial law]. *Kyivskyi chasopys prava*, (3), 174–180 [in Ukrainian].
DOI: https://doi.org/10.32782/klj/2023.3.25

[8] Chaplynskyi, K. O., & Yefimov, M. M. (2023). Naukovi dysputy shchodo sutnosti vzaiemodii orhaniv dosudovoho rozsliduvannia ta operatyvnykh pidrozdiliv kiberpolitsii u protsesi dokazuvannia pry rozsliduvanni zlochyniv u sferi intelektualnoi vlasnosti [Scientific disputes regarding the essence of interaction between prejudicial investigation bodies and cyberpolice operational units in the process of evidence in the investigation of crimes in the sphere of intellectual property]. *Yurydychnyi naukovyi elektronnyi zhurnal*, (4), 630–633 [in Ukrainian].
DOI: https://doi.org/10.32782/2524-0374/2023-4/152

[9] Chaplynskyi, K., Yefimov, M., Pletenets, V., Harashchuk, D., & Demchenko, I. (2023). Features of interaction between law enforcement agencies during the investigation of criminal offenses according to international standards. *Cuestiones Políticas, 41*(76), 469–481.
DOI: https://doi.org/10.46398/cuestpol.4176.27

[10] Chaplynskyi, K. O., Zhylin, A. E., & Yefimov, M. M. (2024). *Metodyka rozsliduvannia shakhraistva u sferi vykorystannia bankivskykh elektronnykh platezhiv*: monohrafiia. Odesa: Yurydyka. 218 s. [in Ukrainian].

[11] Cherniavskyi, S., Babanina, V., Vartyletska, I., & Mykytchyk, O. (2021). Peculiarities of The Economic Crimes Committed with the Use of Information Technologies. *European Journal of Sustainable Development, 10*(1), 420–431. DOI: https://doi.org/10.14207/ejsd.2021.v10n1p420

[12] *Dostup do bankivskoi taiemnytsi, yak ranishe, zalyshaietsia obmezhenym*. (2024, Berezen 20). bank.gov.ua [in Ukrainian]. https://bank.gov.ua/ua/news/all/dostup-do-bankivskoyi-tayemnitsi-yak-ranishe-zalishayetsya-obmejenim

[13] Dudchenko, N. (2023). Svitovi tendentsii finansovoho shakhraistva [Global trends of financial fraud]. *Tsyfrova ekonomika ta ekonomichna bezpeka, 5*(05), 86–92 [in Ukrainian]. DOI: https://doi.org/10.32782/dees.5-13

[14] Dufeniuk, O. M. (2023). Poliarnist ta konverhentsiia obiektyvnosti ta subiektyvnosti u kryminalnomu provadzhenni [Polarity and convergence of objectivity and subjectivity in criminal proceedings]. *Prykarpatskyi yurydychnyi visnyk, 1*(48), 110–116 [in Ukrainian]. DOI: https://doi.org/10.32782/pyuv.v1.2023.22

[15] Ekici, N., Akdogan, H., Kelly, R., & Gultekin, S. (2022). A meta-analysis of the impact of community policing on crime reduction. *Journal of Community Safety and Well-Being, 7*(3), 111–121. DOI: https://doi.org/10.35502/jcswb.244

[16] Filipenko, N. Ye., Uhrovetskyi, O. P., & Sharapova, O. V. (2019). Teoretychni osnovy ekspertnoi profilaktyky [Theoretical bases of expert prevention: concept and tasks]. *Teoriia ta praktyka sudovoi ekspertyzy, 20*(2), 151–162 [in Ukrainian]. DOI: https://doi.org/10.32353/khrife.2.2019.11

[17] Filipenko, N. Ye. (2020). *Kryminolohichna diialnist sudovo-ekspertnykh ustanov Ukrainy*: monohrafiia. Kharkiv: Kollehium. 391 s. [in Ukrainian]. https://files.znu.edu.ua/files/Bibliobooks/Inshi73/0054302.pdf

[18] Havryliuk, R. A. (2020). Sotsialna tsinnist dyskusii pro hnoseolohichni zasady vstanovlennia istyny u sudovii spravi [The social value of the discussion abot the epistemological fundations of establishing the truth in a court case]. *Aktualni problemy prava: teoriia i praktyka, 2*(40), 76–84 [in Ukrainian]. DOI: https://doi.org/10.33216/2218-5461-2020-40-2-76-84

[19] Jakubiec, W., & Kuliński, M. (2023). The phenomenon of economic crime: threats and contemporary trends. *Scientific Journal of Bielsko-Biala School of Finance and Law*, *27*(3), 55–58. DOI: https://doi.org/10.19192/wsfip.sj3.2023.8

[20] Kachashvili, K. S. (2019, Cherven 7). Problematyka internet-shakhraistva v Ukraini ta sposoby borotby z nym. U *Tradytsii ta innovatsii rozvytku pryvatnoho prava v Ukraini: osvitnii vymir*: materialy VIII Vseukrainskoi naukovo-praktychnoi konferentsii (s. 129–132). Poltava: Poltavskyi universytet ekonomiky i torhivli [in Ukrainian]. 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

[21] Kharytonov, S. O. (2023). Subiekty zapobihannia shakhraistvu u sferi elektronnoi torhivli [Fraud prevention subjects in the sphere of electronic commerce]. *Analitychno-porivnialne pravoznavstvo*, (5), 502– 505 [in Ukrainian]. DOI: https://doi.org/10.24144/2788-6018.2023.05.90

[22] Koba, V. B. (2022). Zasoby kryminalistychnoi profilaktyky, shcho zastosovuiutsia upovnovazhenymy osobamy pry rozsliduvanni shakhraistva u sferi e-komertsii [Means of criminal prevention used by authorized persons in the investigation of fraud in the sphere e-commerce]. *Pravo ta derzhavne upravlinnia*, (3), 291–295 [in Ukrainian]. DOI: https://doi.org/10.32782/pdu.2022.3.44

[23] Koba, V. B. (2024). *Teoretychni ta prakseolohichni zasady metodyky rozsliduvannia shakhraistva u sferi e-komertsii [Theoretical and praxeological foundations of fraud investigation methods in the field of e-commerce]* [Dysertatsiia kandydata yurydychnykh nauk, Dnipropetrovskyi derzhavnyi universytet vnutrishnikh sprav]. Dnipro. 262 s. [in Ukrainian]. https://dduvs.edu.ua/wp-content/uploads/files/Structure/science/rada/new_d0872702/2023/4/3/d3.pdf

[24] Konovalova, I. O. (2021). Dosvid zapobihannia shakhraistvu v sferi elektronnoi torhivli v SShA [Experience of prevention e-commercial fraud in the USA]. *Naukovyi visnyk Uzhhorodskoho natsionalnoho universytetu. Seriia: Pravo*, (68), 220–224 [in Ukrainian]. DOI: https://doi.org/10.24144/2307-3322.2021.68.38

[25] Korshykova, T. V. (2021). *Rozsliduvannia shakhraistv, uchynenykh z vykorystanniam elektronno-obchysliuvalnoi tekhniky [Investigation of fraud committed with the use of computer technology]* [Dysertatsiia doktora filosofii, Natsionalna akademiia vnutrishnikh sprav]. Kyiv. 255 s. [in Ukrainian]. https://elar.naiau.kiev.ua/server/api/core/bitstreams/91e29df8-f347-4437-b46d-266bf4909664/content

[26] Kovalenko, I. O. (2021). Obstavyny, shcho pidliahaiut vstanovlenniu pid chas rozsliduvannia shakhraistva u sferi vykorystannia bankivskykh elektronnykh platezhiv [Circumstances to be established during the investigation of fraud in the use of electronic bank payments]. *Prykarpatskyi yurydychnyi visnyk, 1*(36), 98–101 [in Ukrainian]. DOI: https://doi.org/10.32837/pyuv.v0i1.741

[27] Lefterov, L. V. (2019). Zahalnosotsialni zakhody zapobihannia shakhraistvu, shcho vchyniaietsia shliakhom vykorystannia zasobiv elektronnykh komunikatsii [General social measures which prevent frauds commited by using of electronic communications]. *Lex Portus, 1*(15), 89–101 [in Ukrainian]. https://dspace.onua.edu.ua/server/api/core/bitstreams/4ea3793b-8257-48ca-9860-d91a903c9efc/content

[28] Lepei, M. V. (2024). Naukovi dyskusii shchodo provedennia riznykh vydiv ohliadu pid chas rozsliduvannia shakhraistva u sferi vykorystannia bankivskykh elektronnykh platezhiv [Scientific discussions on conducting different types of examination during the investigation of fraud in the field of electronic payments]. *Visnyk Kharkivskoho natsionalnoho universytetu vnutrishnikh sprav, 105*(2(1), 158–166 [in Ukrainian].
DOI: https://doi.org/10.32631/v.2024.2.15

[29] Matviichuk, V. K. (2022). Subiektyvna storona kryminalnoho pravoporushennia proektuvannia chy ekspluatatsiia sporud bez system zakhystu dovkillia: teoretychni ta praktychni problemy [The subjective side of the criminal offense of designing or operating buildings without environmental protection systems: theoretical and practical problems]. *Chasopys Kyivskoho instytutu intelektualnoi vlasnosti ta prava*, (2), 12–17 [in Ukrainian].
DOI: https://doi.org/10.32782/chasopyskiivp/2022-2-2

[30] Melander, S. (2023). Preventive turn in criminal law. *Peking University Law Journal, 11*(1), 11–23.
DOI: https://doi.org/10.1080/20517483.2023.2223843

[31] NBU onovyv pravyla zberihannia, zakhystu, vykorystannia ta rozkryttia bankivskoi taiemnytsi. (2024, Berezen 20). *Sudovo-yurydychna hazeta* [in Ukrainian].
https://sud.ua/uk/news/ukraine/296164-nbu-obnovil-pravila-khraneniya-zaschity-ispolzovaniya-i-raskrytiya-bankovskoy-tayny

[32] Nedzelska, H. V. (2022). Spetsialno-kryminolohichni zakhody zapobihannia shakhraistva, shcho vchyniaietsia orhanizovanoiu hrupoiu [Special criminological measures to prevent fraud by an organized group]. *Yurydychnyi naukovyi elektronnyi zhurnal*, (3), 211–213 [in Ukrainian].
DOI: https://doi.org/10.32782/2524-0374/2022-3/48

[33] Pavlova, N. V. (2023). Osnovni profilaktychni zakhody pry rozsliduvanni kryminalnykh pravoporushen, vchynenykh shliakhom shakhraistva [Basic preventive measures in the investigation of criminal offenses committed through fraud]. *Naukovyi visnyk Luhanskoho derzhavnoho universytetu vnutrishnikh sprav im. E. O. Didorenka, 1*(101), 288–298 [in Ukrainian].
DOI: https://doi.org/10.33766/2524-0323.101.288-298

[34] Reinhold, A. V. (2021). Kryminalistychna profilaktyka u provadzhenniakh za faktamy vchynennia shakhraistva v internet-komertsii [Forensic prevention in proceedings for fraud in internet commerce]. *Naukovyi visnyk publichnoho ta pryvatnoho prava, 2*(2), 162–167 [in Ukrainian].
DOI: https://doi.org/10.32844/2618-1258.2021.2.2.28

[35] Reinhold, A. V. (2023). *Osnovy metodyky rozsliduvannia shakhraistva v internet-komertsii* [Dysertatsiia kandydata yurydychnykh nauk, Dnipropetrovskyi derzhavnyi universytet vnutrishnikh sprav]. Dnipro. 253 s. [in Ukrainian].

[36] Reznik, O., Fomenko, A., Melnychenko, A., Pavlova, N., & Prozorov, A. (2021). Features of the initial stage of investigating fraud with financial resources in cyberspace. *Amazonia Investiga, 10*(41), 141–150.
DOI: https://doi.org/10.34069/AI/2021.41.05.14

[37] Snaphaan, T., & van Ruitenburg, T. (2024). Financial Crime Scripting : an Analytical Method to Generate, Organise and Systematise Knowledge on the Financial Aspects of Profit-Driven Crime. *European Journal on Criminal Policy and Research*.
DOI: https://doi.org/10.1007/s10610-023-09571-9

[38] Sopilko, I., Filinovych, V., Pankova, L. O., Obshalov, S. V., & Chaplynskyi, K. O. (2023). Protection of Intellectual Property Rights from Cyber Threats in the Global Information Environment. *Novum Jus, 17*(1), 237–258.
DOI: https://doi.org/10.14718/NovumJus.2023.17.1.10

[39] Tomyn, S. V. (2019). Vykorystannia taktychnykh pryiomiv dopytu z metoiu profilaktyky kryminalnykh pravoporushen [Using the tactical methods of inquest for the crime prevention]. *Kryminalistyka i sudova ekspertyza*, (64), 319–331.
DOI: https://doi.org/10.33994/kndise.2019.64.28

[40] Verkhovna Rada Ukrainy. (2024, Liutyi 28). *Proiekt Zakonu pro vnesennia zmin do deiakykh zakoniv Ukrainy shchodo udoskonalennia funktsii Natsionalnoho banku Ukrainy z derzhavnoho rehuliuvannia rynkiv finansovykh posluh* (No 11043) [in Ukrainian].
https://itd.rada.gov.ua/billInfo/Bills/Card/43742

[41] Volobuiev, A. F. (Uklad.). (2003). *Profilaktychna diialnist slidchoho pry rozsliduvanni zlochyniv*: lektsiia dlia vsikh form navchannia. Kharkiv: Natsionalnyi universytet vnutrishnikh sprav. 24 s. [in Ukrainian].

[42] Yarovenko, H. M., Skovronska, A. I., & Boiadzhian, M. M. (2018). Modeliuvannia vyiavlennia oznak kiberzahroz v bankakh iz vykorystanniam intelektualnoho analizu [Modeling the detect signs of the cyber threats in the banks with using data mining]. *Efektyvna ekonomika*, (7) [in Ukrainian].
http://www.economy.nayka.com.ua/pdf/7_2018/39.pdf

[43] Yefimov, M., Pavlova, N., Fedchenko, V., Pletenets, V., & Kryvopusk, O. (2022). Foreign experience in legal regulation of fraud investigation. *Journal of the University of Zulia, 13*(38), 159–168.
DOI: https://doi.org/10.46925//rdluz.38.11

Список використаних джерел

[1] Бабенко А. М., Чекмарьова І. М., Палій М. В. Віктимологічне запобігання кримінальним правопорушенням проти власності. *Юридичний науковий електронний журнал*. 2024. № 3. С. 630–633.
DOI: https://doi.org/10.32782/2524-0374/2024-3/152

[2] Бакаянова Н. М., Кубаєнко А. В., Свида О. Г. Організація діяльності Національної поліції України та оперативних підрозділів : навч.-метод. посіб. Одеса : Фенікс, 2020. 251 с.
URL: https://dspace.onua.edu.ua/server/api/core/bitstreams/78ab9a6e-6934-40aa-86dd-726ea0f479d3/content
[3] Березняк В. С. Основні напрями криміналістичної профілактики під час розслідування кримінальних правопорушень у сфері нерухомості. *Оперативно-розшукова діяльність Національної поліції: проблеми теорії та практики :* матеріали всеукр. наук.-практ. конф., Дніпро, 17 жовт. 2020 р. / Дніпропетр. держ. ун-т внутр. справ. Дніпро, 2020. С. 5–8.
[4] Березняк В. С. Запобігання шахрайству в Інтернеті. *Науковий вісник Дніпропетровського державного університету внутрішніх справ*. 2023. № 1. С. 190–196.
DOI: https://doi.org/10.31733/2078-3566-2023-1-190-196
[5] Бондарук Т. Г., Богріновцева Л. М., Бондарук О. С. Шахрайство із використанням банківських платіжних карток як спосіб фінансування тероризму та сепаратизму. *Статистика України*. 2023. № 101(2). С. 4–13.
DOI: https://doi.org/10.31767/su.2(101)2023.02.01
[6] Бортник С. М. Окремі аспекти протидії легалізації доходів, одержаних у результаті вчинення кіберзлочинів. *Протидія кіберзлочинності та торгівлі людьми :* матеріали міжнар. наук.-практ. конф. Харків, 27 трав. 2022 р. / Харків. нац. ун-т внутр. справ. Харків, 2022. С. 16–17.
URL: https://dspace.univd.edu.ua/server/api/core/bitstreams/e791062b-5b16-4bad-bf11-7a48eece6693/content
[7] Брисковська О. М., Гелемей М. О. Особливості вчинення шахрайства в мережі Інтернет в умовах воєнного стану. *Київський часопис права*. 2023. № 3. С. 174–180.
DOI: https://doi.org/10.32782/klj/2023.3.25
[8] Чаплинський К. О., Єфімов М. М. Наукові диспути щодо сутності взаємодії органів досудового розслідування та оперативних підрозділів кіберполіції у процесі доказування при розслідуванні злочинів у сфері інтелектуальної власності. *Юридичний науковий електронний журнал*. 2023. № 4. С. 630–633.
DOI: https://doi.org/10.32782/2524-0374/2023-4/152
[9] Chaplynskyi K., Yefimov M., Pletenets V., Harashchuk D., Demchenko I. Features of interaction between law enforcement agencies during the investigation of criminal offenses according to international standards. *Cuestiones Políticas*. 2023. No 41(76). P. 469–481.
DOI: https://doi.org/10.46398/cuestpol.4176.27
[10] Чаплинський К. О., Жилін А. Е., Єфімов М. М. Методика розслідування шахрайства у сфері використання банківських електронних платежів : монографія. Одеса : Юридика, 2024. 218 с.
[11] Cherniavskyi S., Babanina V., Vartyletska I., Mykytchyk O. Peculiarities of The Economic Crimes Committed with the Use of Information Technologies. *European Journal of Sustainable Development*. 2021. No 10. P. 420–431.
DOI: https://doi.org/10.14207/ejsd.2021.v10n1p420
[12] Доступ до банківської таємниці, як раніше, залишається обмеженим. *bank.gov.ua.* 2024. 20 берез.
URL: https://bank.gov.ua/ua/news/all/dostup-do-bankivskoyi-tayemnitsi-yak-ranishe-zalishayetsya-obmejenim
[13] Дудченко Н. Світові тенденції фінансового шахрайства. *Цифрова економіка та економічна безпека*. 2023. № 5(05). С. 86–92.
DOI: https://doi.org/10.32782/dees.5-13
[14] Дуфенюк О. М. Полярність та конвергенція об'єктивності та суб'єктивності у кримінальному провадженні. *Прикарпатський юридичний вісник*. 2023. № 1(48). С. 110–116.
DOI: https://doi.org/10.32782/pyuv.v1.2023.22
[15] Ekici N., Akdogan H., Kelly R., Gultekin S. A meta-analysis of the impact of community policing on crime reduction. *Journal of Community Safety and Well-Being*. 2022. No 7(3). P. 111–121.
DOI: https://doi.org/10.35502/jcswb.244
[16] Філіпенко Н. Є., Угровецький О. П., Шарапова О. В. Теоретичні основи експертної профілактики. *Теорія та практика судової експертизи*. 2019. № 20(2). С. 151–162.
DOI: https://doi.org/10.32353/khrife.2.2019.11
[17] Філіпенко Н. Є. Кримінологічна діяльність судово-експертних установ України : монографія. Харків : Колегіум, 2020. 391 с.
URL: https://files.znu.edu.ua/files/Bibliobooks/Inshi73/0054302.pdf
[18] Гаврилюк Р. А. Соціальна цінність дискусії про гносеологічні засади встановлення істини у судовій справі. *Актуальні проблеми права: теорія і практика*. 2020. № 2(40). С. 76–84.
DOI: https://doi.org/10.33216/2218-5461-2020-40-2-76-84
[19] Jakubiec W., Kuliński M. The phenomenon of economic crime: threats and contemporary trends. *Scientific Journal of Bielsko-Biala School of Finance and Law*. 2023. No 27(3). P. 55–58.
DOI: https://doi.org/10.19192/wsfip.sj3.2023.8
[20] Качашвілі К. С. Проблематика інтернет-шахрайства в Україні та способи боротьби з ним. *Традиції та інновації розвитку приватного права в Україні: освітній вимір :* матеріали VIII Всеукр. наук.-практ. конф., Полтава, 7 червня 2019 р. / Полтав. ун-т економіки і торгівлі. Полтава, 2019. С. 129–132.
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

[21] Харитонов С. О. Суб'єкти запобігання шахрайству у сфері електронної торгівлі. *Аналітично-порівняльне правознавство*. 2023. № (5). С. 502–505.
DOI: https://doi.org/10.24144/2788-6018.2023.05.90
[22] Коба В. Б. Засоби криміналістичної профілактики, що застосовуються уповноваженими особами при розслідуванні шахрайства у сфері е-комерції. *Право та державне управління*. 2022. № 3. С. 291–295.
DOI: https://doi.org/10.32782/pdu.2022.3.44
[23] Коба В. Б. Теоретичні та праксеологічні засади методики розслідування шахрайства у сфері е-комерції : дис. … канд. юрид. наук : 12.00.09. Дніпро, 2024. 265 с.
URL: https://dduvs.edu.ua/wp-content/uploads/files/Structure/science/rada/new_d0872702/2023/4/3/d3.pdf
[24] Коновалова І. О. Досвід запобігання шахрайству в сфері електронної торгівлі в США. *Науковий вісник Ужгородського національного університету. Серія : Право*. 2021. № 68. С. 220–224.
DOI: https://doi.org/10.24144/2307-3322.2021.68.38
[25] Коршикова Т. В. Розслідування шахрайств, учинених з використанням електронно-обчислювальної техніки : дис. … д-ра філософії : 081 – Право. Київ, 2021. 255 с.
URL: https://elar.naiau.kiev.ua/server/api/core/bitstreams/91e29df8-f347-4437-b46d-266bf4909664/content
[26] Коваленко І. О. Обставини, що підлягають встановленню під час розслідування шахрайства у сфері використання банківських електронних платежів. *Прикарпатський юридичний вісник*. 2021. № 1(36). С. 98–101.
DOI: https://doi.org/10.32837/pyuv.v0i1.741
[27] Лефтеров Л. В. Загальносоціальні заходи запобігання шахрайству, що вчиняється шляхом використання засобів електронних комунікацій. *Lex Portus.* 2019. № 1(15). С. 89–101.
URL: https://dspace.onua.edu.ua/server/api/core/bitstreams/4ea3793b-8257-48ca-9860-d91a903c9efc/content
[28] Лепей М. В. Наукові дискусії щодо проведення різних видів огляду під час розслідування шахрайства у сфері використання банківських електронних платежів. *Вісник Харківського національного університету внутрішніх справ*. 2024. № 105(2(1). С. 158–166.
DOI: https://doi.org/10.32631/v.2024.2.15
[29] Матвійчук В. К. Суб'єктивна сторона кримінального правопорушення проектування чи експлуатація споруд без систем захисту довкілля: теоретичні та практичні проблеми. *Часопис Київського інституту інтелектуальної власності та права.* 2022. № 2. С. 12–17.
DOI: https://doi.org/10.32782/chasopyskiivp/2022-2-2
[30] Melander S. Preventive turn in criminal law. *Peking University Law Journal*. 2023. No 11(1). P. 11–23.
DOI: https://doi.org/10.1080/20517483.2023.2223843
[31] НБУ оновив правила зберігання, захисту, використання та розкриття банківської таємниці. *Судово-юридична газета.* 2024. 20 берез.
URL: https://sud.ua/uk/news/ukraine/296164-nbu-obnovil-pravila-khraneniya-zaschity-ispolzovaniya-i-raskrytiya-bankovskoy-tayny
[32] Недзельська Г. В. Спеціально-кримінологічні заходи запобігання шахрайства, що вчиняється організованою групою. *Юридичний науковий електронний журнал.* 2022. № 3. С. 211–213.
DOI: https://doi.org/10.32782/2524-0374/2022-3/48
[33] Павлова Н. В. Основні профілактичні заходи при розслідуванні кримінальних правопорушень, вчинених шляхом шахрайства. *Науковий вісник Луганського державного університету внутрішніх справ ім. Е. О. Дідоренка.* 2023. № 1(101). С. 288–298.
DOI: https://doi.org/10.33766/2524-0323.101.288-298
[34] Рейнгольд А. В. Криміналістична профілактика у провадженнях за фактами вчинення шахрайства в інтернет-комерції. *Науковий вісник публічного та приватного права*. 2021. № 2(2). С. 162–167.
DOI: https://doi.org/10.32844/2618-1258.2021.2.2.28
[35] Рейнгольд А. В. Основи методики розслідування шахрайства в інтернет-комерції : дис. … канд. юрид. наук : 12.00.09. Дніпро, 2023. 253 с.
[36] Reznik O., Fomenko A., Melnychenko A., Pavlova N., Prozorov A. Features of the initial stage of investigating fraud with financial resources in cyberspace. *Amazonia Investiga.* 2021. No 10(41). P. 141–150.
DOI: https://doi.org/10.34069/AI/2021.41.05.14
[37] Snaphaan T., van Ruitenburg T. Financial Crime Scripting : an Analytical Method to Generate, Organise and Systematise Knowledge on the Financial Aspects of Profit-Driven Crime. *European Journal on Criminal Policy and Research.* 2024.
DOI: https://doi.org/10.1007/s10610-023-09571-9
[38] Sopilko I., Filinovych V., Pankova L. O., Obshalov S. V., Chaplynskyi K. O. Protection of Intellectual Property Rights from Cyber Threats in the Global Information Environment. *Novum Jus.* 2023. No 17(1). P. 237–258.
DOI: https://doi.org/10.14718/NovumJus.2023.17.1.10
[39] Томин С. В. Використання тактичних прийомів допиту з метою профілактики кримінальних правопорушень. *Криміналістика і судова експертиза.* 2019. № 64. С. 319–331.
DOI: https://doi.org/10.33994/kndise.2019.64.28

[40] Проєкт Закону про внесення змін до деяких законів України щодо удосконалення функцій Національного банку України з державного регулювання ринків фінансових послуг від 28.02.2024 № 11043.
URL: https://itd.rada.gov.ua/billInfo/Bills/Card/43742
[41] Профілактична діяльність слідчого при розслідуванні злочинів : лекція для всіх форм навчання / уклад. А. Ф. Волобуєв. Харків : Національний ун-т внутр. справ, 2003. 24 с.
[42] Яровенко Г. М., Сковронська А. І., Бояджян М. М. Моделювання виявлення ознак кіберзагроз в банках із використанням інтелектуального аналізу. *Ефективна економіка*. 2018. № 7.
URL: http://www.economy.nayka.com.ua/pdf/7_2018/39.pdf
[43] Yefimov M., Pavlova N., Fedchenko V., Pletenets V., Kryvopusk O. Foreign experience in legal regulation of fraud investigation. *Journal of the University of Zulia*. 2022. No 13(38). P. 159–168.
DOI: https://doi.org/10.46925//rdluz.38.11

Стаття надійшла до редакції 16.07.2024

V. Koba,
Cand. Sc. (Law),
Head of the Department for Ensuring the Activities
of the Head of the National Police of Ukraine
10 Bohomoltsia St., Kyiv, 01601, Ukraine
ORCID: https://orcid.org/0009-0002-1201-6205
email: valokt@ gmail.com
phone: +38(093) 559-84-50

MEANS OF CRIMINAL PREVENTION IN CRIMINAL PROCEEDINGS REGARDING FRAUD IN THE SPHERE OF E-COMMERCE

Abstract. Preventive measures directly carried out by the investigator are highlighted, in particular in the process of ensuring criminal proceedings, carrying out individual investigative (search) actions, as well as tactical operations. Emphasis is placed on the importance of expert prevention, as well as preventive measures of an informational, educational and victimological nature, etc. Emphasis is placed on the urgent need to create a mechanism for prompt response to fraud in the field of commercial activity by blocking the assets of fraudulent companies and stopping their activities. During the study, the following research methods were applied: formal-logical, functional, systemic, statistical, synthesis method. The scientific novelty consists in justifying the need to introduce a single automated system, which in case of suspicious actions automatically sends a request to banking institutions, where the fact of the transaction is established and the further movement of funds to the final account / bank card to which the funds were transferred is tracked, with simultaneous blocking of accounts. In addition, special forensic prevention measures are proposed. A component of the online fraud prevention concept is singled out – the systematic activity of cyber police units monitoring social networks and media. Attention is focused on the use of the information resources of the National Police of Ukraine, which has created and has been operating for a long time a system of communication departments that cooperate with regional and all-Ukrainian media, have their own websites, web pages in social networks, produce their own audiovisual content and are highly active in other media, including social networks and electronic media. The practical significance of the study lies in the fact that the developed proposals can become the basis of methodological recommendations for the application of forensic prevention measures during the investigation of fraud in e-commerce.

Keywords: online fraud; commercial internet fraud; preventive activities; preventive measures; "AntiFraud" system; pre-trial investigation; causes and conditions that contribute to fraud in the field of e-commerce.