УДК 343.98
DOI https://doi.org/10.32782/pdu.2024.4.94

І. С. Суслікова
доктор філософії з економіки,
фахівець І категорії відділу міжнародних зв'язків
Державного податкового університету
ORCID ID: 0000-0003-3399-020X

ОСОБЛИВОСТІ РОЗСЛІДУВАННЯ КІБЕРШАХРАЙСТВА У ФІНАНСОВІЙ СФЕРІ ПІД ЧАС ВІЙНИ

Проведене дослідження дає підстави стверджувати, що кібершахрайство у фінансовій сфері в умовах воєнного стану набуло якісно нових рис, зумовлених поєднанням високого рівня цифровізації фінансових послуг, зростанням соціально-психологічної вразливості населення та активним використанням злочинцями воєнної тематики як інструменту маніпулятивного впливу. Такі обставини зумовлюють не лише кількісне зростання відповідних кримінальних правопорушень, а й ускладнення їх механізму та підвищення рівня суспільної небезпеки. Встановлено, що практика досудового розслідування кібершахрайства у фінансовій сфері характеризується значними труднощами у частині ідентифікації суб'єкта кримінального правопорушення, доведення його умислу та фактичного контролю над рухом грошових коштів або криптоактивів. Особливу проблему становить допустимість і належність цифрових доказів, що часто зумовлює неможливість притягнення винних осіб до кримінальної відповідальності навіть за наявності підтвердженого факту заподіяння майнової шкоди. Доведено, що чинні процесуальні механізми фіксації та оцінки електронних доказів не повною мірою відповідають потребам розслідування фінансових кіберзлочинів, особливо в умовах обмежених ресурсів і підвищеного навантаження на правоохоронні органи під час воєнного стану. Це обумовлює необхідність їх подальшого вдосконалення з урахуванням технологічних особливостей сучасних злочинних схем. Обґрунтовано, що підвищення ефективності розслідування кібершахрайства у фінансовій сфері можливе лише за умови комплексного підходу, який передбачає спеціалізацію слідчих і прокурорів, посилення міжвідомчої взаємодії з фінансовими установами, удосконалення методик роботи з криптовалютами та активне використання міжнародних механізмів співробітництва. Водночас врахування воєнного соціально-психологічного контексту має істотне значення для правильної кваліфікації та оцінки суспільної небезпеки таких кримінальних правопорушень.

Зроблені у статті висновки та запропоновані прикладні рекомендації можуть бути використані у правозастосовній діяльності органів досудового розслідування, у процесі підготовки методичних матеріалів, а також у подальших наукових дослідженнях, спрямованих на вдосконалення системи протидії фінансовому кібершахрайству в Україні в умовах воєнного стану.

Ключові слова: *кібершахрайство, фінансова сфера, воєнний стан, досудове розслідування, цифрові докази, криптовалюта.*

Актуальність теми. У сучасних умовах цифровізація фінансових послуг, зростання обсягів безготівкових операцій та рух коштів через інтернет-платформи створили як додаткові можливості для економічного розвитку, так і сприятливі умови для кримінальних посягань. Кібершахрайство у фінансовій сфері стало однією з наймасовіших та найбільш розвинутих форм кримінально протиправної діяльності, що завдає значної шкоди як окремим громадянам, так і національній економіці в цілому [1].

Особливо це актуально в умовах воєнного стану, під час якого збройна агресія рф спричинила соціально-економічну нестабільність і значні зміни в звичній поведінці громадян та бізнесу. Психоло-

гічна вразливість населення, зростання благодійних платежів і недостатній рівень цифрової грамотності створили додаткові можливості для шахрайства, у тому числі через соціальну інженерію та фейкові платформи «допомоги» чи «компенсації».

За даними Національного банку України, частка незаконних операцій із платіжними картками, здійснених в інтернеті, становила 83 % від усіх шахрайських транзакцій у 2024 році, і сума збитків за цими незаконними діями досягла 1,1 млрд грн, що на 37 % більше, ніж у попередньому році. Загалом кількість випадків незаконних операцій із платіжними картками у 2024 році склала близько 270 000 транзакцій, хоча їхня кількість дещо зменшилася, сукупні фінансові втрати значно зросли –з огляду на збільшення середньої суми однієї шахрайської транзакції [4].

Аналіз роботи Департаменту кіберполіції Національної поліції України свідчить, що приблизно 80 % випадків онлайн-шахрайства пов’язані з маніпуляціями з боку зловмисників, які отримують доступ до облікових даних або примушують жертв здійснити платежі через обман [4].

Крім того, дані правоохоронних джерел показують, що за перші вісім місяців 2024 року було знешкоджено 23 організовані групи, що займалися онлайн-шахрайством, що на 6 більше, ніж у минулому році, –це свідчить про активізацію таких злочинних формувань.

Таким чином, кібершахрайство у фінансовій сфері не лише зберігає свою актуальність, але й посилює свої позиції як вагомий криміногенний чинник сучасного цифрового суспільства, особливо в умовах воєнного стану. Це обумовлює необхідність комплексного наукового аналізу, формування ефективних методів розслідування та удосконалення превентивних механізмів протидії таким злочинам.

Аналіз останніх досліджень і публікацій. Проблематику кібершахрайства, фінансових кримінальних правопорушень та кримінальних правопорушень у сфері цифрових технологій у своїх наукових працях досліджували, зокрема, О. М. Литвинов, В. В. Голіна, А. П. Закалюк, С. С. Чернявський, М. І. Хавронюк, В. Я. Тацій, Ю. В. Баулін, а також зарубіжні дослідники кіберзлочинності та фінансової безпеки.

Водночас недостатньо дослідженими залишаються питання специфіки досудового розслідування фінансового кібершахрайства в умовах воєнного стану, процесуальної допустимості та фіксації цифрових і криптовалютних доказів, ефективних моделей міжвідомчої взаємодії правоохоронних органів і фінансових установ, а також впливу воєнних соціально-психологічних чинників на механізм вчинення та викриття таких кримінальних правопорушень.

Метою наукової статті є комплексний аналіз сучасного стану та особливостей розслідування кібершахрайства у фінансовій сфері в умовах воєнного стану, виявлення основних проблем доказування й організації досудового розслідування, а також обґрунтування науково-практичних напрямів удосконалення протидії таким кримінальним правопорушенням в Україні.

Для досягнення поставленої мети у статті передбачається вирішення таких завдань:

1. проаналізувати поняття, ознаки та основні форми кібершахрайства у фінансовій сфері в умовах воєнного стану;
2. охарактеризувати сучасний стан і тенденції поширення фінансового кібершахрайства під час збройної агресії рф;
3. визначити особливості механізму вчинення та типові способи маскування фінансових кібершахрайств;
4. проаналізувати вплив воєнного стану на організацію досудового розслідування та міжвідомчу взаємодію правоохоронних органів і фінансових установ;
5. обґрунтувати напрями вдосконалення правового, організаційного й методичного забезпечення розслідування кібершахрайства у фінансовій сфері.

Виклад основного матеріалу. Кібершахрайство у фінансовій сфері є різновидом кримінальних правопорушень проти власності, що характеризується використанням цифрових технологій з метою незаконного заволодіння грошовими коштами, майновими правами або іншими фінансовими активами шляхом обману чи зловживання довірою.

У широкому розумінні кібершахрайство у фінансовій сфері в умовах воєнного стану доцільно визначати як умисне протиправне заволодіння фінансовими ресурсами фізичних або юридичних осіб шляхом використання цифрових технологій, електронних платіжних інструментів, мережі Інтернет чи телекомунікаційних систем, вчинене з урахуванням або шляхом експлуатації суспільних, економічних і психологічних особливостей, спричинених воєнним станом [1].

До характерних ознак кібершахрайства у фінансовій сфері в умовах війни належать:

1. Цифровий спосіб вчинення –кримінальне правопорушення вчиняється через інтернет-ресурси, мобільні застосунки, платіжні сервіси, електронні гаманці, месенджери, соціальні мережі або криптовалютні платформи.

2. Обман або маніпуляція довірою потерпілого –використання неправдивої інформації, фейкових повідомлень, підроблених сайтів, псевдоофіційних звернень від імені банків, державних органів, військових формувань чи благодійних організацій.

3. Фінансова спрямованість –безпосереднім предметом посягання є грошові кошти, безготівкові активи, криптовалюта або права вимоги на фінансові ресурси.

4. Високий рівень латентності –значна частина таких злочинів не реєструється через невеликі суми збитків, недовіру потерпілих до можливостей розслідування або складність ідентифікації злочинців.

5. Транснаціональний характер –використання серверів, платіжних систем, криптогаманців та виконавців, розміщених за межами України, що істотно ускладнює юрисдикційні та процесуальні аспекти розслідування.

6. Експлуатація воєнних чинників –використання тем війни, допомоги ЗСУ, компенсацій за зруйноване житло, соціальних виплат, евакуації або полону як інструменту психологічного впливу на потерпілих.

У період дії воєнного стану спостерігається істотна трансформація класичних схем фінансового шахрайства, що відбувається шляхом їх адаптації до нових соціальних, економічних і психологічних реалій воєнного часу. Найбільш поширеними формами кібершахрайства у фінансовій сфері є такі:

Фішингове кібершахрайство, що реалізується через створення підроблених вебсайтів банківських установ, державних електронних сервісів або платіжних платформ, які імітують надання соціальної допомоги внутрішньо переміщеним особам, військовослужбовцям чи громадянам, які постраждали внаслідок бойових дій.

Шахрайство, пов’язане з благодійними зборами, яке проявляється у функціонуванні фейкових благодійних фондів, сторінок у соціальних мережах або автоматизованих ботів у месенджерах, що здійснюють збір коштів нібито на потреби Збройних Сил України, лікування поранених або відновлення зруйнованого житла.

Компрометація банківських облікових записів, що здійснюється шляхом застосування методів соціальної інженерії, зокрема телефонного чи онлайн-контакту з потерпілими під виглядом працівників банків, волонтерів або представників органів державної влади.

Інвестиційне кібершахрайство, яке полягає у пропозиціях вкладення коштів у так звані «військові проєкти», «воєнні облігації» або криптоактиви, що фактично не мають реального економічного підґрунтя та використовуються виключно як інструмент заволодіння коштами потерпілих.

Варто зазначити, що використання криптовалют для заволодіння та легалізації незаконно отриманих коштів, що значно ускладнює відстеження фінансових потоків, встановлення кінцевих бенефіціарів і доведення походження активів у кримінальному провадженні.

Мультикомпонентні організовані шахрайські схеми, які поєднують елементи фішингу, соціальної інженерії, використання підставних осіб (так званих «дропів») та транснаціональних платіжних інструментів, що свідчить про високий рівень організованості та адаптивності злочинної діяльності.

Практика досудового розслідування кримінальних правопорушень, пов’язаних із кібершахрайством у фінансовій сфері,

свідчить, що переважна більшість таких проваджень є складними з погляду встановлення суб'єкта кримінального правопорушення, збирання доказів та доведення причинно-наслідкового зв'язку між діями зловмисників і заподіяною шкодою. Це зумовлено як цифровою природою кримінального правопорушення, так і особливостями воєнного часу [5;6].

У більшості кримінальних проваджень розслідування кібершахрайства у фінансовій сфері розпочинається з подання потерпілим заяви про незаконне списання грошових коштів або введення його в оману шляхом фішингу чи застосування методів соціальної інженерії. Аналіз слідчої практики свідчить, що до первинних слідчих (розшукових) дій у таких провадженнях, відповідно до положень Кримінального процесуального кодексу України, належать: витребування від банківських установ інформації щодо руху коштів за рахунками (ст. 159–166 КПК України –тимчасовий доступ до речей і документів); аналіз платіжних операцій і фінансових транзакцій; отримання відомостей від мобільних операторів та інтернет-провайдерів (ст. 93 КПК України); фіксація цифрових слідів злочину –електронних повідомлень, лог-файлів, IP-адрес, доменних імен (ст. 84, 99 КПК України); встановлення та допит так званих «дропів» –осіб, на рахунки яких надходили незаконно отримані кошти (ст. 224 КПК України) [2; 3].

Водночас правозастосовна та судова практика засвідчує, що значна частина таких кримінальних проваджень ускладнюється або фактично зупиняється на етапі встановлення кінцевого вигодонабувача, що зумовлено швидким переміщенням коштів через багаторівневі ланцюжки рахунків, використанням підставних осіб, а також конвертацією фінансових ресурсів у криптовалюту, що істотно ускладнює їх подальше відстеження, арешт і доказування контролю над активами.

Аналіз судової практики, зокрема позицій Верховного Суду, свідчить, що у справах про кібершахрайство у фінансовій сфері ключовою проблемою залишається допустимість і належність цифрових доказів, а не сам факт завдання майнової шкоди. Суди неодноразово наголошували, що електронні дані можуть визнаватися доказами лише за умови дотримання вимог щодо їх належного отримання, фіксації та збереження відповідно до положень Кримінального процесуального кодексу України.

Так, у своїх рішеннях Верховний Суд послідовно виходить з того, що скріншоти листування, електронні повідомлення, дані з мобільних пристроїв або вебресурсів не можуть автоматично визнаватися допустимими доказами, якщо сторона обвинувачення не довела джерело їх походження, цілісність та відсутність втручання в їх зміст. У низці рішень Суд звертав увагу, що фіксація таких відомостей без участі спеціаліста або без використання процесуально передбачених механізмів (огляд, тимчасовий доступ, експертиза) істотно знижує їх доказове значення [7].

Окрему проблему становить доведення умислу та ролі конкретної особи у вчиненні кібершахрайства. Судова практика демонструє, що сам по собі факт надходження коштів на банківський рахунок особи (так званого «дропа») не є достатнім для визнання її співучасником кримінального правопорушення без доведення усвідомлення протиправного характеру дій та контролю над подальшим рухом коштів. У зв'язку з цим значна кількість проваджень завершується перекваліфікацією дій або закриттям за недоведеністю складу кримінального правопорушення.

Особливої складності набувають провадження, у яких незаконно отримані кошти конвертуються в криптовалюту. Судова практика засвідчує, що без належного експертного дослідження та аналітики блокчейн-транзакцій орган досудового розслідування не спроможний довести належність криптогаманця конкретній особі, а отже - встановити фактичний контроль над цифровими активами. Відсутність таких доказів судами розцінюється як істотний недолік доказової бази.

Таким чином, судова практика підтверджує, що основні труднощі розслідування фінансового кібершахрайства полягають не лише у складності викриття кримінально протиправних схем схем, а й у недостатньому рівні процесуальної

якості зібраних цифрових доказів, що безпосередньо впливає на результати судового розгляду [8].

Зазначені проблеми обумовлюють необхідність удосконалення методики фіксації та оцінки цифрових доказів, підвищення рівня спеціалізації слідчих і прокурорів, а також розроблення єдиних стандартів взаємодії між правоохоронними органами, фінансовими установами та провайдерами цифрових сервісів.

Результати аналізу слідчої та судової практики свідчать про необхідність удосконалення організаційних, процесуальних і методичних підходів до розслідування кібершахрайства у фінансовій сфері, особливо в умовах дії воєнного стану. З огляду на це доцільно сформулювати низку прикладних рекомендацій, спрямованих на підвищення ефективності досудового розслідування зазначеної категорії кримінальних правопорушень.

По-перше, першочергового значення набуває питання належної фіксації цифрових доказів на початковому етапі кримінального провадження. Саме на стадії первинного реагування формується основа доказової бази, яка в подальшому визначає перспективи судового розгляду. У зв'язку з цим доцільним є запровадження уніфікованих підходів до процесуальної фіксації електронних даних із використанням механізмів, передбачених кримінальним процесуальним законодавством, а також обов'язкове залучення спеціалістів у сфері цифрової криміналістики під час огляду електронних пристроїв, вебресурсів і мережевих сервісів.

По-друге, ефективність розслідування фінансового кібершахрайства безпосередньо залежить від оперативності та повноти взаємодії органів досудового розслідування з банківськими та іншими фінансовими установами. Доцільним є вдосконалення процедур обміну інформацією, зокрема шляхом стандартизації запитів про тимчасовий доступ до банківської таємниці, а також скорочення строків реагування на звернення щодо блокування рахунків і зупинення підозрілих транзакцій. Особливого значення в цьому контексті набуває використання інструментів фінансового моніторингу для раннього виявлення ознак шахрайської діяльності.

По-третє, практика свідчить про необхідність поглибленої спеціалізації слідчих і прокурорів, які здійснюють розслідування фінансових кіберзлочинів. Універсальний підхід до ведення таких кримінальних проваджень не відповідає їх складності та технологічному характеру. З огляду на це доцільно формувати спеціалізовані слідчі групи, забезпечувати системне підвищення кваліфікації з питань цифрових доказів, платіжних технологій та криптоактивів, а також залучати до розслідування фахівців з фінансового аналізу та інформаційних технологій.

По-четверте, окремої уваги потребує удосконалення методик роботи з криптовалютами, які дедалі частіше використовуються у схемах фінансового кібершахрайства як засіб приховування походження коштів та ускладнення їх відстеження. Доцільним є ширше використання експертних досліджень у сфері блокчейн-аналітики, а також нормативне уточнення підходів до доведення фактичного контролю особи над криптогаманцем як елементу суб'єктивної сторони кримінального правопорушення.

По-п'яте, з огляду на транснаціональний характер фінансового кібершахрайства, необхідним є посилення міжнародного співробітництва у сфері кримінального судочинства. Це передбачає активніше використання механізмів міжнародної правової допомоги, удосконалення процедур отримання інформації від іноземних платіжних сервісів, хостинг-провайдерів та криптобірж, а також розширення співпраці з міжнародними правоохоронними інституціями.

По-шосте, при розслідуванні фінансового кібершахрайства в умовах воєнного стану доцільно враховувати специфічний соціально-психологічний контекст, у межах якого вчиняються такі правопорушення. Використання воєнної тематики, апеляція до патріотичних почуттів або експлуатація стану підвищеної тривожності населення істотно підвищують суспільну небезпеку діяння та мають бути належним чином відображені як у процесі доказування, так і під час кваліфікації кримінально протиправних дій.

Висновки. Узагальнюючи результати проведеного дослідження, слід констатувати, що кібершахрайство у фінансовій сфері в умовах воєнного стану характеризується підвищеною динамічністю, технологічною складністю та адаптивністю до соціально-економічних реалій воєнного часу. Активне використання інформаційно-комунікаційних технологій, криптоактивів і методів соціальної інженерії, поєднане з експлуатацією психологічної вразливості населення, істотно ускладнює як виявлення, так і розслідування таких кримінальних правопорушень, а також знижує ефективність традиційних підходів кримінального переслідування.

У цих умовах протидія фінансовому кібершахрайству потребує комплексного переосмислення організаційних, процесуальних і методичних засад досудового розслідування, посилення спеціалізації правоохоронних органів, удосконалення механізмів фіксації та оцінки цифрових доказів, а також розвитку міжвідомчої й міжнародної співпраці. Реалізація зазначених підходів сприятиме підвищенню рівня захисту майнових прав громадян, стабільності фінансової системи та ефективності кримінально-правового реагування на виклики, зумовлені воєнним станом.

Список використаної літератури:

1. Самойлов С. Розслідування шахрайств, учинених із використанням мережі «Інтернет» : автореф. дис. … канд. юрид. наук : 081. Донецьк, 2014. 18 с. URL: https://dspace.nlu.edu.ua/handle/123456789/14174.
2. Кримінальний кодекс України: від 05.04.2001 № 2341-III (зі змін. і допов.). URL: https://zakon.rada.gov.ua/laws/show/2341-14#Text
3. Кримінальний процесуальний кодекс України: від 13.04.2012 № 4651-VI (зі змін. і допов.). URL: https://zakon.rada.gov.ua/laws/show/4651-17#Text
4. CERT-UA. Звіт про кіберінциденти в Україні. URL: https://cip.gov.ua/ua/news
5. Interpol. Global Financial Fraud Assessment 2024. URL: https://www.interpol.int/en/News-and-Events/News/2024/INTERPOL-Financial-Fraud-assessment-A-global-threat-boosted-by-technology
6. Deloitte. Cybersecurity requirements for financial institutions during wartime. URL: https://www.deloitte.com/ua/en/services/tax/perspectives/updated-cybersecurity-requirements-for-non-bank-financial-institutions.html
7. Верховний Суд. Огляд судової практики щодо допустимості електронних доказів у кримінальному провадженні. URL: https://supreme.court.gov.ua/supreme/pokazniki-diyalnosti/uzagalnennya-sudovoyi-praktiki.
8. Чаплинський К.О., Рейнгольд А. В., Павлова Н. В. Методика розслідування шахрайства в інтернет-комерції: теорія та практика : монографія Одеса : Видавництво «Юридика», 2024. 242 с.

Suslikova I. S. Features of investigating cyberfraud in the financial sphere during war

The conducted research gives grounds to assert that cyber fraud in the financial sector under martial law has acquired qualitatively new features, caused by a combination of a high level of digitalization of financial services, an increase in the socio-psychological vulnerability of the population and the active use of military themes by criminals as a tool of manipulative influence. Such circumstances lead not only to a quantitative increase in the number of relevant criminal offenses, but also to a complication of their mechanism and an increase in the level of public danger. It has been established that the practice of pre-trial investigation of cyber fraud in the financial sector is characterized by significant difficulties in identifying the subject of a criminal offense, proving his intent and actual control over the movement of funds or crypto assets. A particular problem is the admissibility and relevance of digital evidence, which often makes it impossible to bring the guilty parties to criminal liability even in the presence of a confirmed fact of causing property damage. It has been proven that the current procedural mechanisms for recording and evaluating electronic evidence do not fully meet the needs of investigating financial cybercrimes, especially in conditions of limited resources and increased burden on law enforcement agencies during martial law. This necessitates their further improvement, taking into account the technological features of modern criminal schemes. It is substantiated that increasing the efficiency of investigating cyberfraud in the financial sector is possible only with a comprehensive approach, which

involves the specialization of investigators and prosecutors, strengthening interagency cooperation with financial institutions, improving methods of working with cryptocurrencies, and active use of international cooperation mechanisms. At the same time, taking into account the military socio-psychological context is essential for the correct qualification and assessment of the social danger of such criminal offenses. The conclusions drawn in the article and the proposed practical recommendations can be used in the law enforcement activities of pre-trial investigation bodies, in the process of preparing methodological materials, as well as in further scientific research aimed at improving the system of combating financial cyber fraud in Ukraine under martial law.

Key words: *cyber fraud, financial sphere, martial law, pre-trial investigation, digital evidence, cryptocurrency.*