УДК 343.98
DOI https://doi.org/10.32782/pdu.2025.2.50

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

ІМПЛЕМЕНТАЦІЯ ПОЗИТИВНОГО ЗАРУБІЖНОГО ДОСВІДУ ЩОДО РОЗСЛІДУВАННЯ КІБЕРЗЛОЧИНІВ, ВЧИНЕНИХ У ФІНАНСОВІЙ СФЕРІ

Статтю присвячено дослідженню можливостей імплементації позитивного зарубіжного досвіду щодо розслідування кіберзлочинів, вчинених у фінансовій сфері, в національну правозастосовну практику України. Актуальність теми зумовлена стрімкою цифровізацією фінансових відносин, зростанням кількості транснаціональних фінансових кіберзлочинів, а також ускладненням процесу доказування у кримінальних провадженнях цієї категорії, особливо в умовах воєнного стану та обмежених ресурсів правоохоронних органів. У статті проаналізовано ключові елементи зарубіжних моделей протидії фінансовим кіберзлочинам на прикладі Франції, Швейцарії, Німеччини та Великої Британії. Встановлено, що спільними рисами ефективних моделей є інституційна спеціалізація правоохоронних органів, активна інтеграція фінансової розвідки у кримінальне переслідування, стандартизація процедур роботи з цифровими доказами, застосування комплексних експертних досліджень та широке використання механізмів міжнародного співробітництва. Окрему увагу приділено ролі Будапештської конвенції про кіберзлочинність, рекомендацій FATF і регіональних механізмів Європейського Союзу у сфері доступу до електронних доказів (e-evidence) як нормативної та методологічної основи доказування у фінансових кіберпровадженнях. На основі узагальнення зарубіжного досвіду сформульовано науково обґрунтовані пропозиції щодо його адаптації до умов України. Обґрунтовано доцільність розвитку інституційної координації, уніфікації стандартів цифрової криміналістики, впровадження механізмів раннього збереження електронних і фінансових даних, посилення ролі фінансового моніторингу та формування методичних підходів до доказування фактичного контролю над цифровими фінансовими інструментами. Зроблено висновок, що системна імплементація позитивного зарубіжного досвіду сприятиме підвищенню ефективності досудового розслідування, допустимості цифрових доказів і забезпеченню належного балансу між інтересами кримінального переслідування та захистом прав людини у сфері фінансових кіберзлочинів.

Ключові слова: *кіберзлочини у фінансовій сфері; фінансове кібершахрайство; цифрові докази; доказування у кримінальному провадженні; розслідування кіберзлочинів; міжнародні стандарти доказування; зарубіжний досвід; фінансова розвідка; цифрова криміналістика; e-evidence; FATF; Будапештська конвенція.*

Актуальність теми. Стрімкий розвиток цифрових технологій та їх активне впровадження у фінансову сферу зумовили суттєві трансформації як легальних фінансових відносин, так і кримінальних практик, пов'язаних із незаконним заволодінням коштами, легалізацією доходів та маніпулюванням фінансовими інструментами. Кіберзлочини у фінансовій сфері набули системного, транснаціонального характеру, поєднуючи елементи класичних майнових і службових кримінальних правопорушень із використанням складних цифрових механізмів, електронних платіжних засобів, криптоактивів і хмарних сервісів. У таких умовах доказування у кримінальних провадженнях цієї категорії справ перетворюється на один із найбільш проблемних елементів кримінального процесу.

Особливої гостроти зазначена проблематика набула в умовах воєнного стану, коли цифровізація фінансових операцій поєднується зі зростанням обсягів онлайн-платежів, благодійних зборів, державних і соціальних виплат, що створює сприятливе середовище для вчинення фінансових кіберзлочинів. Водночас динамічний характер електронних даних, їх розміщення у різних юрисдикціях та залежність від діяльності приватних провайдерів істотно ускладнюють процес збирання, збереження та оцінки цифрових доказів, а також доведення фактичного контролю осіб над фінансовими і цифровими активами.

У цих умовах особливого значення набувають міжнародні стандарти доказування та позитивний зарубіжний досвід розслідування фінансових кіберзлочинів, сформовані в межах універсальних і регіональних механізмів міжнародного співробітництва. Будапештська конвенція про кіберзлочинність, технічні стандарти цифрової криміналістики серії ISO/IEC, рекомендації FATF, а також правовий режим e-evidence Європейського Союзу формують сучасну модель доказування, орієнтовану на забезпечення автентичності й допустимості електронних доказів за одночасного дотримання прав людини.

З огляду на це, наукове осмислення проблем доказування у справах про кіберзлочини у фінансовій сфері та обґрунтування шляхів імплементації позитивного зарубіжного досвіду в національну практику набувають особливої актуальності. Такий підхід дозволяє не лише підвищити ефективність досудового розслідування і судового розгляду, а й сприяти формуванню узгодженої, сучасної системи кримінально-правового захисту фінансових відносин у цифровому середовищі.

Аналіз останніх досліджень і публікацій. Проблематику впровадження позитивного зарубіжного досвіду розслідування у справах про кіберзлочини, вчинені у фінансовій сфері, у своїх наукових працях досліджували Томас Дж. Холт, Адам М. Босслер, Девід С. Волл, Іган Кейсі, Орін С. Керр, Росс Андерсон, Джонатан Клаф, Сьюзен В. Бреннер, Ендрю Мюррей, а також вітчизняні науковці М. А. Погорецький, Т. Г. Фоміна, І. Г. Каланча, А. В. Гутник, А. Я. Хитра, А. Є. Жилін, К. О. Чаплинський, М. І. Хавронюк, С. С. Чернявський.

Попри наявний науковий доробок, недостатньо дослідженими залишаються: уніфікація стандартів допустимості цифрових доказів у справах про фінансові кіберзлочини та їх узгодження з вимогами міжнародного й національного кримінального процесу, механізми доказування фактичного контролю особи над цифровими фінансовими інструментами (банківськими рахунками, платіжними засобами, криптогаманцями) за відсутності формального правового зв'язку, процесуальні та доказові аспекти транскордонного доступу до електронних доказів, зокрема імплементація інструментів e-evidence та положень Будапештської конвенції у національну практику, стандартизація та межі використання комплексних експертних досліджень у фінансових кіберпровадженнях, забезпечення балансу між ефективністю кримінального переслідування та захистом прав людини під час збирання й використання цифрових доказів у фінансовій сфері.

Метою наукової статті є комплексне дослідження проблем розслідування у справах про кіберзлочини, вчинені у фінансовій сфері, з урахуванням міжнародних стандартів та позитивного зарубіжного досвіду, а також обґрунтування науково і практично виважених напрямів їх імплементації у національну практику досудового розслідування і судового розгляду з метою підвищення ефективності протидії фінансовим кіберзлочинам та забезпечення належного захисту прав людини.

Виклад основного матеріалу. Варто почати з дослідження позитивного зарубіжного досвіду окремих європейських держав. У цьому аспекті цікавою є Французька Республіка, яка належить до держав, у яких сформовано комплексну та інституційно розвинену модель протидії кіберзлочинам у фінансовій сфері, що поєднує спеціалізацію правоохоронних органів, розвинену систему цифрової криміналістики та активне використання міжнародних стандартів доказування.

Позитивний досвід Франції є показовим з огляду на високий рівень цифровізації фінансового сектору та значну кількість транснаціональних фінансових кіберінцидентів [1].

Ключовим елементом французької моделі є інституційна спеціалізація. Розслідування фінансових кіберзлочинів здійснюється спеціалізованими підрозділами Національної жандармерії та Національної поліції, зокрема кіберпідрозділами Gendarmerie nationale та Police nationale, які тісно співпрацюють із фінансовими слідчими та органами фінансового моніторингу. Така модель дозволяє поєднувати кримінально-правовий, технічний і фінансово-аналітичний підходи на ранніх стадіях розслідування.

Особливу роль у забезпеченні якості доказування відіграє Національне агентство з безпеки інформаційних систем - ANSSI, яке, хоча і не є органом досудового розслідування, формує технічні стандарти реагування на кіберінциденти та методичні рекомендації щодо фіксації цифрових слідів. Використання уніфікованих технічних протоколів забезпечує дотримання принципів автентичності та цілісності цифрових доказів, що безпосередньо впливає на їх допустимість у судовому провадженні [1].

Франція активно імплементує положення Будапештської конвенції про кіберзлочинність та регіональні механізми Європейського Союзу у сфері e-evidence. Практика французьких правоохоронних органів свідчить про пріоритетність механізмів термінового збереження електронних даних і прямої взаємодії з провайдерами цифрових і фінансових послуг. Це дозволяє оперативно отримувати дані щодо транзакцій, руху коштів, облікових записів і телекомунікаційних метаданих без застосування тривалих процедур класичної міжнародної правової допомоги.

Окремою перевагою французької моделі є інтеграція фінансових розслідувань із стандартами FATF. Доказування у справах про фінансові кіберзлочини орієнтується не лише на фіксацію факту незаконного доступу або шахрайства, а й на встановлення походження коштів, трасування фінансових потоків та доведення фактичного контролю над активами, у тому числі цифровими. Значна увага приділяється взаємодії слідчих із банківськими установами та фінансовими аналітичними підрозділами.

Таким чином, позитивний досвід Франції характеризується системним підходом до розслідування фінансових кіберзлочинів, поєднанням спеціалізації, стандартизації доказування та ефективного міжнародного співробітництва. Імплементація окремих елементів цієї моделі в національну практику України може сприяти підвищенню якості збирання цифрових і фінансових доказів, зменшенню процесуальних ризиків та посиленню ефективності кримінального переслідування у сфері фінансової кіберзлочинності.

Швейцарська Конфедерація є однією з провідних держав Європи у сфері фінансових послуг, що зумовлює високий рівень уваги до протидії кіберзлочинам, спрямованим на банківський сектор, платіжні системи та ринок віртуальних активів. Позитивний досвід Швейцарії полягає у поєднанні розвиненого фінансового контролю, високих стандартів цифрової безпеки та чітко вибудуваної системи доказування у кримінальних провадженнях фінансового характеру.

Ключовою особливістю швейцарської моделі є тісна інтеграція кримінального переслідування з фінансовим наглядом. Провідну роль у цьому процесі відіграє Federal Office of Justice у взаємодії з правоохоронними органами та фінансовими регуляторами. Розслідування фінансових кіберзлочинів ґрунтується на ранньому залученні фінансових аналітичних механізмів, що дозволяє оперативно ідентифікувати підозрілі транзакції та забезпечити їх належне процесуальне закріплення як доказів [2].

Важливим елементом позитивного досвіду Швейцарії є діяльність служби фінансової розвідки — Money Laundering Reporting Office Switzerland, яка відіграє ключову роль у збиранні та аналізі інформації про підозрілі фінансові операції, у тому числі пов’язані з кіберзлочинами. Матеріали фінансової розвідки активно використовуються в кримінальних провадженнях як джерело доказової інфор-

мації щодо походження коштів, механізмів їх переміщення та фактичного контролю над активами.

Швейцарська практика також вирізняється високим рівнем стандартизації цифрової криміналістики. Під час розслідування фінансових кіберзлочинів застосовуються уніфіковані технічні протоколи збирання та збереження цифрових доказів, що відповідають міжнародним стандартам серії ISO/IEC [2]. Це забезпечує автентичність і цілісність електронних даних, а також мінімізує ризики визнання таких доказів недопустимими у судовому провадженні.

Окрему увагу у Швейцарії приділено доказуванню кримінальних правопорушень, пов'язаних із використанням криптоактивів. Завдяки чітко врегульованому правовому статусу віртуальних активів та розвиненій практиці фінансового моніторингу, слідчі органи мають можливість ефективно трасувати операції з цифровими активами, встановлювати кінцевих бенефіціарів і доводити причинно-наслідковий зв'язок між кіберзлочином і заволодінням коштами. Такий підхід відповідає рекомендаціям FATF і забезпечує комплексний характер доказування.

Таким чином, позитивний досвід Швейцарії щодо розслідування фінансових кіберзлочинів характеризується високим рівнем координації між правоохоронними органами та фінансовими інституціями, стандартизованими підходами до цифрової криміналістики та ефективним використанням фінансової розвідки як інструменту доказування. Імплементація окремих елементів швейцарської моделі в національну практику України може сприяти посиленню фінансової складової доказування та підвищенню ефективності протидії кіберзлочинам у фінансовій сфері.

Велика Британія сформувала інтегровану та практикоорієнтовану модель протидії фінансовим кіберзлочинам, у межах якої розслідування поєднує кримінально-правові, фінансово-аналітичні та технологічні інструменти. Особливістю британського підходу є концентрація зусиль не лише на виявленні кіберінцидентів, а й на доказуванні повного фінансового ланцюга злочину, включно з кінцевим вигодонабувачем.

Координаційну роль у розслідуванні фінансових кіберзлочинів відіграє National Crime Agency, у структурі якої функціонує спеціалізований підрозділ National Cyber Crime Unit (NCCU). Цей орган забезпечує централізований аналіз складних кіберсправ, у тому числі пов'язаних з банківським шахрайством, онлайн-платежами, криптоактивами та транснаціональними схемами відмивання коштів [4]. Така модель дозволяє уникнути фрагментарності розслідувань і забезпечує єдність стандартів доказування.

Важливою складовою британського досвіду є тісна взаємодія кримінального переслідування з фінансовою розвідкою. У цьому контексті ключову роль відіграє UK Financial Intelligence Unit, яка акумулює та аналізує звіти про підозрілі фінансові операції (SARs), зокрема пов'язані з кіберзлочинами. Матеріали фінансової розвідки системно використовуються як джерело доказової інформації для встановлення походження коштів, їх руху та контролю над цифровими активами.

Окремою перевагою британської моделі є високий рівень стандартизації цифрової криміналістики. Під час розслідування фінансових кіберзлочинів застосовуються чітко регламентовані протоколи збирання, збереження та аналізу електронних доказів, які відповідають міжнародним стандартам ISO/IEC і забезпечують безперервність chain of custody [5]. Судова практика Великої Британії приділяє особливу увагу процесуальній якості цифрових доказів і прозорості методів їх отримання.

Значна увага у Великій Британії приділяється доказуванню кримінальних правопорушень, пов'язаних із криптоактивами та фінансовими технологіями. Слідчі органи активно використовують блокчейн-аналітику, фінансово-економічні експертизи та дані від криптобірж і платіжних провайдерів для доведення фактичного контролю особи над цифровими активами. Такий підхід узгоджується з рекомендаціями FATF і дозволяє ефективно поєднувати цифрові та фінансові докази в єдину доказову систему.

Таким чином, позитивний досвід Великої Британії характеризується високим рівнем інституційної координації, активною роллю фінансової розвідки, жорсткими стандартами цифрової криміналістики та орієнтацією на доказування повного фінансового механізму кіберзлочину. Імплементація окремих елементів британської моделі в Україні може суттєво посилити спроможність правоохоронних органів у протидії фінансовій кіберзлочинності та підвищити якість доказування у таких кримінальних провадженнях.

Висновки. Удосконалення національної системи розслідування кіберзлочинів у фінансовій сфері доцільно здійснювати з урахуванням позитивного зарубіжного досвіду держав Європейського Союзу та інших країн із розвиненою фінансово-цифровою інфраструктурою. Аналіз відповідних моделей свідчить, що ефективність кримінального переслідування у цій сфері забезпечується комплексним поєднанням інституційної спеціалізації, стандартизації доказування, інтеграції фінансового аналізу та активного міжнародного співробітництва.

По-перше, доцільним є подальший розвиток інституційної спеціалізації органів досудового розслідування шляхом формування міжвідомчих спеціалізованих підрозділів або робочих груп, орієнтованих на розслідування фінансових кіберзлочинів. Такий підхід дозволяє поєднати кримінально-правову, технічну та фінансово-аналітичну складові доказування, усунути фрагментарність розслідувань і забезпечити належну координацію дій усіх залучених суб'єктів.

По-друге, необхідним є впровадження уніфікованих процесуальних і технічних стандартів роботи з цифровими доказами, зокрема на основі міжнародних стандартів серії ISO/IEC. Стандартизація процедур ідентифікації, збирання, копіювання та збереження електронних даних із фіксацією ланцюга їх збереження сприятиме підвищенню автентичності й цілісності доказової інформації та зменшенню ризиків визнання цифрових доказів недопустимими у судовому провадженні.

По-третє, з урахуванням динамічного характеру цифрових і фінансових даних доцільно інституціоналізувати механізми термінового (раннього) збереження електронної інформації на початкових стадіях кримінального провадження. Обов'язкове застосування таких механізмів щодо банківських установ, платіжних сервісів, провайдерів електронних комунікацій і хмарних послуг забезпечить збереження доказової інформації та створить передумови для її подальшого процесуального використання.

По-четверте, потребує посилення інтеграція фінансової розвідки та фінансового моніторингу в систему доказування у справах про фінансові кіберзлочини. Використання аналітичних матеріалів фінансової розвідки для встановлення походження коштів, трасування фінансових потоків і доведення фактичного контролю над активами дозволяє сформувати цілісну доказову модель злочинного механізму, що відповідає рекомендаціям міжнародних організацій у сфері протидії відмиванню коштів.

По-п'яте, доцільним є розроблення методичних підходів до доказування фактичного контролю особи над цифровими фінансовими інструментами, зокрема банківськими рахунками, платіжними засобами та віртуальними активами. Такий підхід має ґрунтуватися на сукупності цифрових, фінансових і поведінкових доказів та враховувати сучасну міжнародну судову практику щодо персоніфікації відповідальності у фінансових кіберпровадженнях.

По-шосте, важливим напрямом удосконалення доказування є розвиток практики комплексних експертних досліджень, що поєднують комп'ютерно-технічні, фінансово-економічні та, за потреби, блокчейн-аналітичні експертизи. Комплексний підхід дозволяє відтворити повний механізм злочину та встановити причинно-наслідковий зв'язок між використанням цифрових технологій і заволодінням коштами.

По-сьоме, ефективна імплементація позитивного зарубіжного досвіду неможлива без підвищення рівня професійної підготовки та спеціалізації слідчих, прокурорів і суддів у сфері цифрових доказів і фінансових технологій. Системне навчання та формування сталої практики спеціалізації сприятимуть правильній оцінці доказів і підвищенню якості кримінального переслідування.

По-восьме, у контексті євроінтеграційних процесів доцільно адаптувати національні процедури до регіональних механізмів доступу до електронних доказів, зокрема підходів, закладених у правовому режимі e-evidence Європейського Союзу. Це дозволить скоротити строки отримання доказової інформації з-за кордону та підвищити ефективність розслідування транснаціональних фінансових кіберзлочинів.

Таким чином, впровадження позитивного зарубіжного досвіду має здійснюватися системно та комплексно, із поєднанням організаційних, процесуальних і технічних заходів. Реалізація запропонованих підходів сприятиме підвищенню ефективності доказування, забезпеченню допустимості цифрових доказів і формуванню сучасної моделі кримінально-правового захисту фінансових відносин у цифровому середовищі.

Список використаної літератури:

1. Національне агентство з безпеки інформаційних систем Франції (ANSSI). Кібербезпека та реагування на фінансові кіберінциденти. URL: https://www.ssi.gouv.fr
2. Money Laundering Reporting Office Switzerland (MROS). Роль фінансової розвідки у протидії кіберзлочинам. URL: https://www.fedpol.admin.ch/fedpol/en/home/kriminalitaet/geldwaescherei.html.
3. Федеральне відомство юстиції Швейцарії. Кримінальне переслідування фінансових злочинів та міжнародне співробітництво. URL: https://www.bj.admin.ch.
4. Національне агентство з боротьби зі злочинністю Великої Британії (National Crime Agency). Фінансова кіберзлочинність та роль National Cyber Crime Unit. URL: https://www.nationalcrimeagency.gov.uk.
5. Фінансова розвідка Великої Британії (UK Financial Intelligence Unit). Використання фінансової аналітики у кримінальних провадженнях. URL: https://www.nationalcrimeagency.gov.uk/what-we-do/crime-threats/money-laundering-and-economic-crime.

Suslikova I. S. Implementation of positive foreign experience in the investigation of cybercrimes committed in the financial sphere

The article is devoted to the study of the possibilities of implementing positive foreign experience in investigating cybercrimes committed in the financial sector into the national law enforcement practice of Ukraine. The relevance of the topic is due to the rapid digitalization of financial relations, the growth of the number of transnational financial cybercrimes, as well as the complication of the evidence process in criminal proceedings of this category, especially in conditions of martial law and limited resources of law enforcement agencies. The article analyzes the key elements of foreign models of combating financial cybercrimes using the example of France, Switzerland, Germany and the United Kingdom. It is established that the common features of effective models are the institutional specialization of law enforcement agencies, the active integration of financial intelligence into criminal prosecution, the standardization of procedures for working with digital evidence, the use of comprehensive expert research and the widespread use of international cooperation mechanisms. Special attention is paid to the role of the Budapest Convention on Cybercrime, FATF recommendations and regional mechanisms of the European Union in the field of access to electronic evidence (e-evidence) as a normative and methodological basis for proof in financial cyber proceedings. Based on the generalization of foreign experience, scientifically substantiated proposals for its adaptation to the conditions of Ukraine are formulated. The feasibility of developing institutional coordination, unification of digital forensics standards, implementation of mechanisms for early preservation of electronic and financial data, strengthening the role of financial monitoring and the formation of methodological approaches to proving actual control over digital financial instruments is substantiated. It is concluded that the systematic implementation of positive foreign experience will contribute to increasing the efficiency of pre-trial investigation, admissibility of digital evidence and ensuring the proper balance between the interests of criminal prosecution and the protection of human rights in the field of financial cyber crimes.

Key words: *cybercrimes in the financial sector; financial cyber fraud; digital evidence; evidence in criminal proceedings; cybercrime investigation; international standards of evidence; foreign experience; financial intelligence; digital forensics; e-evidence; FATF; Budapest Convention.*