DOI: <https://doi.org/10.32353/khrife.2.2020.37>

УДК 343.98:33

К. І. Говорова,

науковий співробітник лабораторії економічних досліджень
Національного наукового центру «Інститут судових експертиз

ім. Засл. проф. М. С. Бокаріуса», м. Харків, Україна,

ORCID: <https://orcid.org/0000-0002-0893-8605>,

e-mail: kg0667241734@gmail.com

МІСЦЕ СУДОВО-ЕКОНОМІЧНОЇ ЕКСПЕРТИЗИ У ПРОТИДІЇ ШАХРАЙСТВАМ З НАДАННЯ ПОСЛУГ У БАНКІВСЬКІЙ СФЕРІ ЧЕРЕЗ ІНТЕРНЕТ

У статті окреслено місце судово-економічної експертизи у протидії шахрайствам з надання послуг у банківській сфері через інтернет. Окремо слід звернути увагу на високотехнологічні злочини з використанням новітньої техніки та програмного забезпечення, тому подальших досліджень потребує питання: чи можливо попередити кіберзлочинність у банківській сфері. Розглянуто питання проведення судово-економічних досліджень щодо надання послуг у банківській сфері через інтернет. На основі аналізу наслідків кібершахрайств, які відбуваються у сфері використання клієнтами банків платіжних засобів, виявлено, що найбільш вразливим місцем є сам клієнт, який під дією різних методів соціальної інженерії стає об'єктом шахрайства.

Ключові слова: інтернет-банкінг, фінансово-кредитні операції, фінансові махінації, онлайн-сервіс, злочини у банківській сфері, банківські послуги, кредитні операції, комп'ютерні технології у сфері платежів, розрахунки через інтернет.

Постановка наукової проблеми. В умовах стрімкого розвитку ринкової економіки дедалі більших обертів набирає сфера банківських послуг. Банківська система є однією з головних ланок фінансово-кредитної системи країни. Найчастіше вона є одним з об'єктів, які приваблюють шахраїв і злочинців, що підриває авторитет банків як гарантів збереження та накопичення коштів населення, держави й суб'єктів господарювання.

Останнім часом у сфері фінансово-кредитних відносин дедалі частіше фіксують махінації, що стосуються незаконних кредитних операцій. Це один із найпоширеніших способів фінансового шахрайства, до якого вдаються як кредитори (банки, фонди, асоціації), так і позичальники (суб'єкти господарювання, фізичні особи). При цьому економічні збитки названих суб'єктів і, передусім, фінансово-кредитних установ, можуть сягати значних сум у національній або іноземній валюті.

Аналіз основних досліджень і публікацій. Питання виявлення правопорушень у банківській сфері розкрито в роботах О. М. Бандурки,

Г. А. Матусовського, М. І. Камлика, М. Т. Білухи, Ф. Ф. Бутинця, В. Д. Понікарова та інших¹. Окрему увагу О. В. Аніщенко й О. В. Хомутенко приділили цьому питанню, висвітлюючи класифікацію судових економічних експертиз на сучасному етапі розвитку судової експертизи². Вони дали визначення основним видам правопорушень та акцентували увагу на основних характеристиках подібних правопорушень; загальних підходах до їх виявлення; засадах експертних досліджень, під час яких фахівці вивчають різноманітні документи про банківські операції; особах, причетних до проведення банківських операцій. Однак, більшість аспектів, пов'язаних із проведенням судових економічних експертиз із надання послуг у банківській сфері через інтернет, залишились поза увагою провідних науковців.

Мета статті. Метою статті є визначення місця проведення судових економічних експертиз у протидії шахрайствам з надання послуг у банківській сфері через інтернет.

Викладення основного матеріалу дослідження. Нормативно-правова база, яка стосується цієї сфери, містить основні документи: Закони України «Про споживче кредитування» та «Про банки і банківську діяльність», постанови Правління НБУ «Про затвердження Положення про здійснення банками фінансового моніторингу» та «Про затвердження Інструкції про порядок відкриття, використання і закриття рахунків у національній та іноземних валютах» та ін.

Усі численні незаконні фінансово-кредитні операції умовно можна розподілити на кілька груп залежно від суб'єкта (позичальник чи кредитор), що їх здійснює.

До *першої групи* належать шляхи, за допомогою яких позичальник посягає на фінансові ресурси фінансово-кредитних установ:

- фізична-особа підприємець або юридична особа, які мають право на здійснення підприємницької діяльності,— отримують кредит за підробленими документами. Наприклад, фальсифікують дані балансу, документи на майно під заставу з метою техніко-економічного обґрунтування потреби в ньому. Після отримання кредиту та

¹ Див., наприклад: Бандурка О. М., Литвинов О. М. Протидія злочинності та профілактика злочинів: монографія. Харків, 2011 ; Матусовский Г. А. Экономические преступления: криминалистический анализ. Харьков, 1999. 480 с. ; Понікаров В. Д., Кравченко С. С., Теленик С. С. Роль правоохоронних органів у здійсненні економічного контролю//*Економіка. Фінанси. Право*. 2004. № 3. С. 31—36 ; Камлик М. І. Особливості обліку і використання обліково-бухгалтерських документів при виявленні та розслідуванні корисливих злочинів у галузях економіки. Судова бухгалтерія. Київ, 1995. 256 с. ; Петрук О. М. Банківська справа: навч. посіб./за ред. Ф. Ф. Бутинця. Київ, 2007. 461 с. ; Білуха М. Т. Курс аудиту. Київ, 1998. 573 с.

² Аніщенко О. В., Хомутенко О. В. Класифікація судових економічних експертиз на сучасному етапі розвитку судової експертизи//*Теорія та практика судової експертизи і криміналістики*: зб. наук. пр. Харків, 2018. Вип. 18. С. 476—480. URL: <https://doi.org/10.32353/khriife.2018.54> (дата звернення: 12.06.2020).

його привласнення такий суб'єкт господарювання банкрутує, ліквідується або в інший спосіб припиняє свою діяльність;

- позичальник, який є офіційно зареєстрованим, використовує свідомо помилкову інформацію для укладення кредитного договору. Отримані кошти він використовує в підприємницькій діяльності для закупівлі, наприклад, товарно-матеріальних цінностей, основних засобів;
- посадова особа (переважно державне підприємство) отримує пільговий кредит на законних підставах з наступним його передаванням певній комерційній структурі під відсотки або комерційна структура за усною домовленістю розраховується з посадовою особою, яка привласнює кошти;
- фізична особа оформляє споживчий кредит за підробленими документами або на підставних осіб.

Друга група махінацій містить способи, до яких вдаються працівники банків. Останні, використовуючи конфіденційну інформацію про клієнта, що є банківською таємницею, знімають з його розрахункового рахунку кредитні кошти й використовують їх на власні потреби або в інший незаконний спосіб. Також до цієї групи махінацій належить оформлення кредитного договору на ім'я клієнта з наступним привласненням отриманих кредитних коштів. Найчастіше такі незаконні оборудки трапляються у віддалених відокремлених підрозділах банку — філіях, відділеннях, за якими контроль центрального відділення слабший.

Третя група операцій кредитного шахрайства пов'язана із взаємною домовленістю представників кредитора і позичальника про отримання незаконного кредиту, тобто це органічне поєднання двох попередніх груп. Схема реалізації кожного зі способів цієї групи орієнтовно може бути такою:

- кредитор разом із позичальником створюють підприємство для отримання кредиту. Після його отримання затягують термін повернення, на підприємстві цілком імовірна зміна засновників, власника, посадових осіб позичальника;
- працівник банківської установи, який має відповідні повноваження, надає незаконний кредит позичальникові. З метою відстрочення повернення кредиту надають підроблені документи, неправдиву інформацію тощо;
- надання працівниками фінансово-кредитних установ пільгового кредиту позичальникові, наприклад, за низькою відсотковою ставкою, на основі сфальсифікованих документів. Після його отримання позичальник перераховує на розрахунковий рахунок позичодавця обумовлену суму — різницю між відсотковими ставками звичайного і пільгового кредиту ¹.

¹ Горлачук О. А. Новини (станом на 12.06.2019 р.)/Офіційний сайт Тернопільського НДЕКЦ МВС України. URL: <http://www.ndekc.te.ua/news/kreditn-mahnats-v-sfer-fnansovokreditnih-vdnosin-ta-zahist-nteresv-h-subktv> (дата звернення: 12.06.2019).

На наше переконання, з метою захисту інтересів суб'єктів фінансово-кредитних відносин і, відповідно, уникнення ними економічних збитків, рекомендується: з боку кредитора (це стосується передусім банків) — забезпечити відповідний рівень фінансового контролю, що полягає в належному документальному оформленні кредитних операцій (організації документообігу, що містить банківську таємницю), обґрунтованості надання кредиту клієнтові шляхом подвійної перевірки відповідними службами банків, а з боку клієнтів — постійно підвищувати фінансову грамотність, що стосується зазначених вище відносин.

Залишається незрозумілим, як бути з новим видом банківського шахрайства, що стосується інтернет-банків? В умовах стрімкого розвитку ринкової економіки та нестримного збільшення кількості нових технологій завдяки інтернет, у банківському секторі з'явився новий вид послуг — інтернет-банк.

Інтернет-банкінг (англ. *Online Banking*), або веб-банкінг — один із видів дистанційного банківського обслуговування, засобами якого доступ до рахунків та операцій за рахунками забезпечується в будь-який час і з будь-якого комп'ютера через інтернет¹.

Особливістю такого банку є те, що банк не має відділень, усі послуги надаються за допомогою мобільного додатку. Клієнтами можуть стати власники пристроїв *Apple* на *iOS 10* і *Android* версії 4.4 і новіших. Відповіді на запитання клієнтів надаються у месенджері (*вайбери*, *фейсбуці* або *телеграмі*).

Для банківського сектору України — це дійсно щось свіже й оригінальне. Але в інших країнах банками без відділень уже нікого не здивуєш. Однією з перших віртуальних фінустанов є американський *Security First Network Bank*, який почав свою діяльність іще 1995 р. Причому буквально за півтора року його активи сягнули \$40 млн, а кількість відкритих рахунків — \$10 000. У Європі першим банком без офісної мережі 1996 р. став німецький *Advance Bank*. Щоправда, він проіснував лише 7 років і 2003 р. був ліквідований.

Утім, у Німеччині є інший успішний проєкт — *Fidor Bank*, заснований 2009 р. Він є, по суті, IT-системою, яка забезпечує проведення різноманітних операцій: перекази, обмін валют, купівлю дорогоцінних металів, видачу кредитів, відкриття депозитів і навіть вкладення у криптовалюти. 2015 р. *Fidor Bank* вийшов на ринок Великої Британії, а в липні 2016 р. його поглинув *France's Groupe BPCE*, але *Fidor Bank* продовжив працювати під своїм брендом.

Одним з перших на території України представником інтернет-банку є *Monobank*. Проте, *Monobank* не зовсім банк у звичному розумінні цього слова. У проєкті немає банківської ліцензії, яку видає НБУ та яка надає

¹ Інтернет-банкінг. Вікіпедія. URL: <https://uk.wikipedia.org/wiki/Інтернет-банкінг> (дата звернення: 12.06.2019).

право здійснювати розрахункові операції, приймати гроші на депозити або видавати кредити. *Monobank* — це лише онлайн-сервіс, який забезпечує доступ до банківських послуг. При цьому безпосередньо операції здійснює *Universal Bank*. Він є фінансовим партнером *Monobank*'у, і саме він оперує грошима клієнтів. Іншими словами, підключаючись до онлайн-сервісу, людина, по суті, стає клієнтом *Universal Bank*. Доступ до його послуг клієнт отримує не безпосередньо у відділеннях *Universal Bank*, а дистанційно через *Monobank*. Таку модель, до речі, використовує російський «Рокетбанк». На початку його банком-партнером був «Інтеркоммерц».

Стати клієнтом *Monobank*'у дуже просто. Необхідно встановити додаток з *Play Market* (для *Android*) або *Apple Store (iOS)* і замовити платіжну карту. Для цього, пройшовши коротку реєстрацію в додатку, слід сфотографувати паспорт і ідентифікаційний код, зазначити інформацію про місце роботи й доходи. Після оброблення даних майбутній (точніше — уже справжній) клієнт *Monobank*'у зможе забрати готову карту в одній з точок видачі або отримати її кур'єром. До речі, сама карта платіжної системи *MasterCard*, а на ній нанесено не тільки назву *Monobank*, а й *Universal Bank*, що додатково підтверджує, хто саме відповідає за збереження грошей¹.

Подібні впровадження і використання комп'ютерних технологій у сфері платежів є характерною ознакою сучасного життя. Банківські послуги, які надають клієнтові дистанційно, а також платежі, що здійснюються без участі готівки, прискорюють обіговість, скорочують кількість грошових коштів, необхідних в обігу. Це, як результат, знижує витрати обігу, збільшує прозорість розрахунків. Завдяки своїй простоті, масовості, доступності технологій, подібні банківські операції все більше приваблюють шахраїв.

У зв'язку із цим суттєво зростає кількість злочинів у банківській сфері з використанням інтернету. У сучасній юридичній літературі для відокремлення цієї категорії злочинів найчастіше вживають термін «кіберзлочинність у банківській сфері».

Аналізуючи зарубіжний досвід боротьби з кіберзлочинністю, стає чітко видно, що вона (кіберзлочинність) має тенденцію до зростання. Однією з причин її зростання є постійне вдосконалення технічних систем глобального зв'язку та прямий доступу користувачів до комп'ютерних технологій через персональні комп'ютери.

За даними Інтерполу, щорічні збитки, яких зазнає Європа через кіберзлочинців, складають понад 300 млрд євро, також щодня жертвами кіберзлочинців стає майже мільйон громадян Європи. Інтернет-злочинці незаконним шляхом отримують номери банківських карт та пін-коди до них, виводять грошові кошти на свої рахунки.

¹ Банк в кишені: що таке Monobank/Uteka. URL: <https://uteka.ua/ua/publication/news-14-delovye-novosti-36-bank-v-karmane-chto-takoe-monobank> (дата звернення: 12.06.2019).

При цьому багато інтернет-видань вважає, що ці проблеми — тільки початок того, що в майбутньому може чекати на суспільство. Із метою боротьби зі злочинними проявами в інтернеті 23.11.2001 р. в Будапешті Рада Європи прийняла Конвенцію про кіберзлочинність¹. Відтоді конференції з проблем інтернет-безпеки у Будапешті стали регулярними і щоразу все більше країн не тільки Європи, а й усього світу беруть у них участь.

У січні 2013 р. за ініціативою Єврокомісії розпочав роботу новостворений Європейський центр з боротьби з кіберзлочинністю. Серед пріоритетів цієї організації, яка здійснює свою діяльність під протекцією Європолу, виокремлено розслідування випадків шахрайства через електронні мережі, окремо — у сфері інтернет-банкінгу.

Сьогодні питання протидії кібершахрайству в банківській сфері є актуальним і в Україні. На основі проведеного аналізу наслідків кібершахрайств, які відбуваються у сфері використання клієнтами банків платіжних засобів, найбільш вразливим місцем є сам клієнт, який під дією різних методів соціальної інженерії стає об'єктом шахрайства. Для боротьби із цим способом шахрайства українські банки не мають доволі дієвих інструментів. Як наслідок — призначення економічних експертиз документів фінансово-кредитних операцій, які проходять саме через інтернет-банкінг, і розширення змісту експертних завдань².

Слід зазначити, що поряд з основними завданнями експертизи фінансово-кредитних операцій, визначеними Науково-методичними рекомендаціями з питань підготовки та призначення судових експертиз та експертних досліджень³, на вирішення експертів усе частіше ставляться питання, викликані змінами й удосконаленням законодавства у сфері комп'ютеризації банківської сфери.

Як зазначає Є. Зозуля, ефективна протидія транснаціональній банківській кіберзлочинності вимагає тісного, швидкого, ефективного та функціонального міжнародного співробітництва всіх державних структур (щонайперше — правоохоронних органів) у розслідуванні такого роду злочинів⁴.

¹ Конвенція про кіберзлочинність (зі змін. та допов.): ухв. Радою Європи 23.11.2001 р., ратиф. Законом України від 07.09.2005 р. № 2824-IV. URL: https://zakon.rada.gov.ua/laws/show/994_575 ; <https://zakon.rada.gov.ua/laws/show/2824-15> (дата звернення: 12.06.2019).

² Яровенко Г. М., Бояджян М. М. Аналіз наслідків кібершахрайств в банківській системі України//*Економіка і суспільство*. 2018. Вип. 18. С. 836—837.

³ Про затвердження Інструкції про призначення та проведення судових експертиз та експертних досліджень та Науково-методичних рекомендацій з питань підготовки та призначення судових експертиз та експертних досліджень: наказ Мін'юсту України від 08.10.1998 р. № 53/5 (зі змін. та допов.). URL: <http://zakon4.rada.gov.ua/laws/show/z0705-98> (дата звернення: 12.06.2019).

⁴ Зозуля Є. В. Діяльність МВС України щодо протидії транснаціональній злочинності у сфері високих технологій//*Наукові записки. Серія: Історія*. 2011. Вип. 1. С. 205—211.

Нормативно-правовими актами, що регулюють суспільні відносини у сфері інформаційної безпеки в Україні, слід вважати: Закони України «Про інформацію» від 02.10.1992 р. № 2657-XII ¹, «Про захист інформації в інформаційно-телекомунікаційних системах» від 05.07.1994 р. № 80/94-ВР ², «Про державну таємницю» від 21.01.1994 р. № 3855-XII ³, «Про основи національної безпеки України» від 19.06.2003 р. № 964-IV ⁴; Укази Президента України «Про деякі заходи щодо захисту державних інформаційних ресурсів у мережах передачі даних» від 24.09.2001 р. № 891/2001 ⁵, «Про Положення про технічний захист інформації в Україні» від 27.09.1999 р. № 1229/99 ⁶, «Про заходи щодо зміцнення банківської системи України та підвищення її ролі у процесах економічних перетворень» від 14.07.2000 р. № 891/2000 ⁷ та ін.

Як свідчить практика протидії кіберзлочинності, зазначеним нормативно-правовим актам необхідна систематизації, одним із варіантів якої є прийняття Кодексу про інформацію, що слугуватиме основою правового забезпечення протидії кіберзлочинам. Верховна Рада України створювала спеціальні структури з питань організаційно-правового забезпечення протидії кіберзлочинності, які функціонували в різний час, а саме: Міжвідомчий комітет з проблем захисту прав на об'єкти інтелектуальної власності, Урядову комісію з питань інформаційно-аналітичного забезпечення діяльності органів виконавчої влади, Міжвідомчу робочу групу з розроблення та узгодження Концепції легалізації програмних продуктів та боротьби з нелегальним їх використанням.

¹ Про інформацію: Закон України від 02.10.1992 р. № 2657-XII (зі змін. та допов.). URL: <https://zakon.rada.gov.ua/laws/show/2657-12> (дата звернення: 12.06.2019).

² Про захист інформації в інформаційно-телекомунікаційних системах: Закон України від 05.07.1994 р. № 80/94-ВР (зі змін. та допов.). URL: <https://zakon.rada.gov.ua/laws/show/80/94-вр> (дата звернення: 12.06.2019).

³ Про державну таємницю: Закон України від 21.01.1994 р. № 3855-XII (зі змін. та допов.). URL: <https://zakon.rada.gov.ua/laws/show/3855-12> (дата звернення: 12.06.2019).

⁴ Про основи національної безпеки України: Закон України від 19.06.2003 р. № 964-IV (утратив чинність). URL: <https://zakon.rada.gov.ua/laws/show/964-15> (дата звернення: 12.06.2019).

⁵ Про деякі заходи щодо захисту державних інформаційних ресурсів у мережах передачі даних: Указ Президента України від 24.09.2001 р. № 891/2001. URL: <https://zakon.rada.gov.ua/laws/show/891/2001> (дата звернення: 12.06.2019).

⁶ Про Положення про технічний захист інформації в Україні: Указ Президента України від 27.09.1999 р. № 1229/99 (зі змін. та допов.). URL: <https://zakon.rada.gov.ua/laws/show/1229/99> (дата звернення: 12.06.2019).

⁷ Про заходи щодо зміцнення банківської системи України та підвищення її ролі у процесах економічних перетворень: Указ Президента України від 14.07.2000 р. № 891/2000. URL: <https://zakon.rada.gov.ua/laws/show/891/2000> (дата звернення: 12.06.2019).

Як зазначає С. Г. Каланча, проблема можливостей глобальних інформаційних мереж, зокрема інтернету, та використання їх для протидії злочинам, причому не тільки зі специфічними комп'ютерними, а й іншими видами злочинів, особливо транснаціональними й організованими, до сьогодні майже не досліджена кримінологією¹.

Отже, сучасні проблеми протидії кіберзлочинності набувають дедалі більшої актуальності, оскільки щороку зростають збитки вітчизняних банків і їх клієнтів від цього виду злочинів. При цьому на особливу увагу заслуговують високотехнологічні злочини з використанням новітньої техніки та програмного забезпечення. Тому подальших досліджень потребує питання: чи можливо попередити кіберзлочинність у банківській сфері.

У цьому разі в пригоді може стати криміналістичне прогнозування. *Криміналістична прогностика* — це самостійне вчення, система наукових положень про загальні закономірності побудови та перевірки прогнозів, які відображають перспективи та напрями розвитку криміналістики й об'єктів її пізнання в майбутньому.

Варто зазначити, що для повноцінного функціонування криміналістичного прогнозування кіберзлочинності в банківській сфері необхідно підготувати різноманітні рекомендації, зміст яких може змінюватися залежно від мети прогнозів і спрямованості прогностичних досліджень. Якщо метою такого прогнозування є розроблення нових методик, прийомів і засобів, які в подальшому забезпечать розслідування злочинної діяльності, що видозмінюється, то запропоновані рекомендації матимуть творчий характер. Передбачувані висновки для криміналістичної науки та судово-слідчої практики можуть стати орієнтирами, спрямованість яких з найбільшою вірогідністю розвиватиме об'єкти криміналістичного пізнання. При цьому прогнозування не тільки орієнтує, а й забезпечує динамічний, поступальний розвиток криміналістичних об'єктів згідно з обраною спрямованістю, передбачаючи настання негативних, безвихідних ситуацій, коли судово-слідчі органи нашкоджуються на злочинні прояви, що не знайшли належного правового врегулювання, і не мають належних криміналістичних рекомендацій щодо їх розслідування й попередження.

Для слідчої та судової практики (органів, які призначають експертизу) питання банківської кіберзлочинності є доволі новим. Крім того, слід зазначити, що дослідження документів фінансово-кредитних операцій через інтернет необхідно розглядати як комплексне. Інакше кажучи, необхідно залучати кількох фахівців, застосовувати спеціальні знання з різних галузей науки й техніки для розв'язання одного спільного (інтеграційного) завдання (питання).

Експертиза (дослідження) документів фінансово-кредитних операцій, проведених через інтернет-банкінг, спрямована на дослідження операцій

¹ Каланча С. Г. Кіберзлочинність: шляхи попередження та протидії//*Наше право*. 2012. № 3. Ч. 2. С. 213—217.

з перерахування та зарахування коштів на поточний рахунок, розрахунків за участь в онлайн-аукціонах, використання сервісів з переказування або обміну валюти, розрахунків в інтернет-магазинах, внесення коштів на депозит або кредитування.

Завдання, які експерти розв'язують під час подібних експертних досліджень, спрямовані на визначення документальної обґрунтованості:

- банківських операцій з відкриття рахунків та руху грошових коштів на рахунках;
- операцій з видачі, використання й погашення кредитів і депозитів, а саме — їх оформлення та відображення в обліку.

Водночас для експертизи документів фінансово-кредитних операцій Науково-методичні рекомендації з питань підготовки та призначення судових експертиз та експертних досліджень не містять подібних завдань і не наводять орієнтовного переліку питань, які має вирішити експерт. Унаслідок цього, призначаючи судову економічну експертизу або експертне економічне дослідження, дуже часто на вирішення експерта виносять питання, які передбачають проведення ревізійних дій або потребують надання правової оцінки, що не належить до компетенції експертів-економістів.

Висновки. Отже (з метою більш повного задоволення потреб слідчої та судової практики), внесення відповідних змін потребують Науково-методичні рекомендації з питань підготовки та призначення судових експертиз та експертних досліджень — у частині судово-економічної експертизи в протидії шахрайствам з надання послуг у банківській сфері через інтернет, оскільки кількість експертиз, пов'язаних із дослідженням документів фінансово-кредитних операцій, постійно збільшується, а предмет дослідження розширюється.

References

- Anishchenko, O. V., Khomutenko, O. V. (2018). Klasyfikatsiia sudovykh ekonomichnykh ekspertyz na suchasnomu etapi rozvytku sudovoi ekspertyzy. *Teoriia ta praktyka sudovoi ekspertyzy i kryminalistyky*. Kharkiv. № 18. URL: <https://doi.org/10.32353/khrife.2018.54> (data zvernennia: 12.06.2020) [in Ukrainian].
- Bank v kysheni: shcho take Monobank. Uteka. URL: <https://uteka.ua/ua/publication/news-14-delovye-novosti-36-bank-v-karmane-chto-takoe-monobank> (data zvernennia: 12.06.2019) [in Ukrainian].
- Horlachuk, O. A. Ofitsiinyi sait Ternopilskoho NDEKts MVS Ukrainy. URL: <http://www.ndekc.te.ua/news/kreditn-mahnats-v-sfer-fnansovokreditnih-vdnosin-ta-zahist-nteresv-h-subktv> (data zvernennia: 12.06.2019) [in Ukrainian].
- Internet-bankinh. Vikipediia. URL: <https://uk.wikipedia.org/wiki/Internet-bankinh> (data zvernennia: 12.06.2019) [in Ukrainian].
- Kalancha, S. H. (2012). Kiberzlochynnist: shliakhy poperedzhennia ta protydii. *Nashe pravo*. № 3. Ch. 2 [in Ukrainian].
- Konventsiiia pro kiberzlochynnist (zi zmin. ta dopov.): ukhv. Radoiu Yevropy 23.11.2001 r., ratyf. Zakonom Ukrainy vid 07.09.2005 r. № 2824-IV. URL: https://zakon.rada.gov.ua/laws/show/994_575 ; <https://zakon.rada.gov.ua/laws/show/2824-15> (data zvernennia: 12.06.2019) [in Ukrainian].

- Pro deiaki zakhody shchodo zakhystu derzhavnykh informatsiinykh resursiv u merezhakh peredachi danykh:* Ukaz Prezydenta Ukrainy vid 24.09.2001 r. № 891/2001. URL: <https://zakon.rada.gov.ua/laws/show/891/2001> (data zvernennia: 12.06.2019) [in Ukrainian].
- Pro derzhavnu taiemnytsiu:* Zakon Ukrainy vid 21.01.1994 r. № 3855-XII (zi zmin. ta dopov.). URL: <https://zakon.rada.gov.ua/laws/show/3855-12> (data zvernennia: 12.06.2019) [in Ukrainian].
- Pro informatsiiu:* Zakon Ukrainy vid 02.10.1992 r. № 2657-XII (zi zmin. ta dopov.). URL: <https://zakon.rada.gov.ua/laws/show/2657-12> (data zvernennia: 12.06.2019) [in Ukrainian].
- Pro osnovy natsionalnoi bezpeky Ukrainy:* Zakon Ukrainy vid 19.06.2003 r. № 964-IV (utratyv chynnist). URL: <https://zakon.rada.gov.ua/laws/show/964-15> (data zvernennia: 12.06.2019) [in Ukrainian].
- Pro Polozhennia pro tekhnichniy zakhyst informatsii v Ukraini:* Ukaz Prezydenta Ukrainy vid 27.09.1999 r. № 1229/99 (zi zmin. ta dopov.) URL: <https://zakon.rada.gov.ua/laws/show/1229/99> (data zvernennia: 12.06.2019) [in Ukrainian].
- Pro zakhody shchodo zmitsnennia bankivskoi systemy Ukrainy ta pidvyshchennia yii roli u protsesakh ekonomichnykh peretvoren:* Ukaz Prezydenta Ukrainy vid 14.07.2000 r. № 891/2000. URL: <https://zakon.rada.gov.ua/laws/show/891/2000> (data zvernennia: 12.06.2019) [in Ukrainian].
- Pro zakhyst informatsii v informatsiino-telekomunikatsiinykh systemakh:* Zakon Ukrainy vid 05.07.1994 r. № 80/94-VR (zi zmin. ta dopov.). URL: <https://zakon.rada.gov.ua/laws/show/80/94-vr> (data zvernennia: 12.06.2019) [in Ukrainian].
- Pro zatverdzhennia Instruksii pro pryznachennia ta provedennia sudovykh ekspertyz ta ekspertnykh doslidzhen ta Naukovo-metodychnykh rekomendatsii z pytan pidhotovky ta pryznachennia sudovykh ekspertyz ta ekspertnykh doslidzhen:* nakaz Miniustu Ukrainy vid 08.10.1998 r. № 53/5 (zi zmin. ta dopov.). URL: <http://zakon4.rada.gov.ua/laws/show/z0705-98> (data zvernennia: 12.06.2019) [in Ukrainian].
- Yarovenko, H. M., Boiadzhian, M. M. (2018). Analiz naslidkiv kibershakhraistv v bankivskii systemi Ukrainy. *Ekonomika i suspilstvo*. № 18 [in Ukrainian].
- Zozulia, Ye. V. (2011). Diialnist MVS Ukrainy shchodo protydii transnatsionalnii zlochynnosti u sferi vysokykh tekhnolohii. *Naukovi zapysky. Serii: Istorii*. № 1 [in Ukrainian].

Е. И. Говорова

МЕСТО СУДЕБНО-ЭКОНОМИЧЕСКОЙ ЭКСПЕРТИЗЫ В ПРОТИВОДЕЙСТВИИ МОШЕННИЧЕСТВАМ ПО ПРЕДОСТАВЛЕНИЮ УСЛУГ В БАНКОВСКОЙ СФЕРЕ ЧЕРЕЗ ИНТЕРНЕТ

В статье обозначено место судебно-экономической экспертизы в противодействии мошенничеству по предоставлению услуг в банковской сфере через интернет, поскольку в последнее время в сфере финансово-кредитных отношений всё чаще фиксируются махинации, касающиеся незаконных кредитных операций. Отмечено, что это один из самых распространённых способов финансового мошенничества, к которому прибегают как кредиторы (банки, фонды, ассоциации), так и заёмщики (субъекты хозяйствования, физические лица), а экономический ущерб указанных субъектов

и, в первую очередь, финансово-кредитных учреждений может достигать значительных сумм в национальной или иностранной валюте. Подчёркнуто, что все многочисленные незаконные финансово-кредитные операции условно можно разделить на несколько групп в зависимости от субъекта (заёмщик или кредитор). В статье с целью защиты интересов субъектов финансово-кредитных отношений и, соответственно, избегания ими экономического ущерба, рекомендуется: со стороны кредитора (это касается, в первую очередь, банков) — обеспечить соответствующий уровень финансового контроля, который заключается в надлежащем документальном оформлении кредитных операций (организации специального делопроизводства с документами, содержащими банковскую тайну), обоснованности предоставления кредита клиенту путём двойной проверки соответствующими службами банков, а со стороны клиентов — постоянно повышать финансовую грамотность вышеуказанных отношений.

Установлено, что особого внимания заслуживают высокотехнологичные преступления с использованием новейшей техники и программного обеспечения, поэтому дальнейшие исследования нуждаются в предупреждении киберпреступности в банковской сфере. Рассмотрены вопросы проведения судебно-экономических исследований по предоставлению услуг в банковской сфере через интернет. На основе анализа последствий кибермошенничества в сфере использования клиентами банков платёжных средств выявлено, что наиболее уязвимым местом является сам клиент, который под действием различных методов социальной инженерии становится объектом мошенничества. Для борьбы с этим способом мошенничества украинские банки не имеют достаточно действенных инструментов. Постоянно растущее число назначенных экспертиз, связанных с исследованием документов финансово-кредитных операций, и расширение предмета исследования указанного сегмента экспертизы требуют внесения соответствующих изменений в законодательство с целью более полного удовлетворения потребностей следственной и судебной практики.

Ключевые слова: интернет-банкинг, финансово-кредитные операции, финансовые махинации, онлайн-сервис, преступления в банковской сфере, банковские услуги, кредитные операции, компьютерные технологии в сфере платежей, расчёты через интернет.

К. Hovorova

PLACE OF FORENSIC ECONOMIC EXAMINATION IN COMBATING FRAUD ON THE PROVISION OF SERVICES IN BANKING VIA THE INTERNET

The article determines the place of forensic economic examination while combating fraud on provision of services in banking via the Internet, since lately frauds concerning illegal credit operations have been registered more frequently according to research in the field of financial and credit relations. It is noted

that this is one of the most common methods of financial fraud, which is resorted to both by creditors (banks, funds, associations) and by borrowers (business entities, natural persons), and economic damage for these entities and, first of all, for financial and credit institutions, may result in substantial amounts in national or foreign currency. It was emphasized that all numerous illegal financial and credit operations can be divided into several groups, depending on the entity (a borrower or a lender). In order to protect the interests of entities of financial and credit relations and, accordingly, to avoid their economic damage, it is recommended: on the part of a lender (it refers, first of all, to banks) to ensure an appropriate level of financial control which is to properly document credit operations (organization of special office administration by working with documents containing bank secrecy), to ensure reasonableness of granting a loan to a client having him double checked by corresponding bank services, and on the part of clients to constantly improve financial literacy with regard to the above relations.

It has been established that high-tech crimes with the use of the latest technology and software warrant special attention, therefore further research needs to be aimed at acquiring the right to prevent cybercrime in banking. The issues of conducting forensic economic research on the provision of services in banking via the Internet are considered. Based on the analysis of the consequences of cyber fraud that occur while the use of bank funds by customers of banks, it has been revealed that the client himself is the most vulnerable point and he becomes subject to fraud under the influence of various social engineering methods. To combat this method of fraud, Ukrainian banks do not have sufficiently effective tools. The constantly growing number of forensic examinations related to the study of documents of financial and credit operations and expansion of the subject of study of the specified segment of forensic examination requires amending legislation in order to better meet the needs of investigative and judicial practice.

Keywords: Internet banking, financial and credit operations, financial fraud, online service, crimes in banking, banking services, credit operations, computer technologies in the field of payments, payments via the Internet.

Надійшла до редколегії 04.08.2020

Говорова К. І. Місце судово-економічної експертизи у протидії шахрайствам з надання послуг у банківській сфері через інтернет. *Теорія та практика судової експертизи і криміналістики* : зб. наук. пр. / редкол.: О. М. Клюєв, В. Ю. Шенітько та ін. Харків : Право, 2020. Вип. 22. С. 461—472. DOI: <https://doi.org/10.32353/khrife.2.2020.37>.