DOI: https://doi.org/10.32782/2524-0072/2021-32-55

УДК 336.713:343.72

ФІНАНСОВЕ ШАХРАЙСТВО З БАНКІВСЬКИМИ РАХУНКАМИ В УКРАЇНІ

FINANCIAL FRAUD WITH BANK ACCOUNTS IN UKRAINE

Маршук Ліна Миколаївна
кандидат економічних наук, доцент,
Вінницький торговельно-економічний інститут
Київського національного торговельно-економічного університету
ORCID: https://orcid.org/0000-0003-4333-7458

Складанюк Марина Сергіївна
студентка,
Вінницький торговельно-економічний інститут
Київського національного торговельно-економічного університету
ORCID: https://orcid.org/0000-0001-7082-373X

Marshuk Lina, Skladaniuk Maryna
Vinnytsia Institute of Trade and Economics of
Kyiv National University of Trade and Economics

У статті проведено дослідження найпопулярніших схем фінансового шахрайства та методів боротьби з ними. Дослідження показує, якими способами шахраї можуть оволодіти фінансовими ресурсами фізичних та юридичних осіб з банківських карт. Проаналізовано кількість випадків фінансового шахрайства та збитки понесених витрат, встановлено чітку тенденцію щодо їх постійного зростання. Описано теоретико-методологічні засади формування механізму протидії фінансовому шахрайству в Інтернеті та шахрайським схемам з банківськими картками фізичних осіб Запропоновано шляхи та способи захисту фізичних та юридичних осіб від злочинів такого роду. У дослідженні, зокрема, розроблено рекомендації та пропозиції щодо механізму протидії фінансовому шахрайству з фінансовими ресурсами фізичних та юридичних осіб в Інтернеті та шахрайським схемам з банківськими картками.

Ключові слова: фінансове шахрайство, банківська карта, шахрай, фінансові ресурси, платіжна безпека.

В статье проведены исследования популярнейших схем финансового мошенничества и методов борьбы с ними. Исследование показывает, какими способами мошенники могут овладеть финансовыми ресурсами физических и юридических лиц с банковских карт. Проанализировано количество случаев финансового мошенничества и убытки понесенных расходов, установлена четкая тенденция их постоянного роста. Описаны теоретико-методологические основы формирования механизма противодействия финансовому мошенничеству в Интернете и мошенническим схемам с банковскими карточками физических лиц. Предложены пути и способы защиты физических и юридических лиц от преступлений такого рода. В исследовании разработаны рекомендации и предложения по механизму противодействия финансовому мошенничеству с финансовыми ресурсами физических и юридических лиц в Интернете и мошенническим схемам с банковскими карточками.

Ключевые слова: финансовое мошенничество, банковская карта, мошенник, финансовые ресурсы, платежная безопасность.

The article examines the most popular schemes of financial fraud and methods of combating them. The main ways of committing fraudulent actions with the financial resources of individuals and legal entities that use bank cards are described. The study shows what schemes fraudsters use to seize financial resources. The most popular of them are theft of a financial phone number, extortion of confidential information through calls and deceptive SMS messages, fraud of individuals on the Internet, theft of card data by installing fraudulent devices in ATMs. The number of cases of financial fraud and losses was analyzed, monitored and the dynamics of their constant growth was determined. Theoretical and methodological bases of formation of the mechanism of counteraction to financial fraud on the Internet and fraudulent schemes with bank cards of individuals are described. The necessity and importance of studying this topic are highlighted. The main reason and the need to detail financial fraud are to protect individuals and legal entities by raising their awareness of the safe storage and use of their financial resources. Ways and

means of protection of individuals and legal entities from crimes of this kind are offered. The study, in particular, developed recommendations and proposals for a mechanism to combat financial fraud with the financial resources of individuals and legal entities on the Internet and fraudulent schemes with bank cards. The main tips for protecting the financial resources of individuals and legal entities are to increase the level of financial literacy of individuals, keeping confidential data secret, caution in communicating with strangers, caution when using ATMs to withdraw cash, regularity and frequency in changing passwords, responsibility and creativity time to create passwords for e-banking, etc. The study is important for households because it helps protect their financial resources, reduce the number of misled individuals and the number of stolen financial resources. The application of the research results will increase the efficiency of detection and investigation of schemes of Internet fraud, telephone and SMS fraud, fraud with bank cards, ATMs.

Keywords: financial fraud, bank card, fraud, financial resources, payment security.

Постановка проблеми. У наш час широко розповсюджене фінансове шахрайство і розвивається воно швидкими темпами. Якщо ще нещодавно шахраї просто телефонували людям і намагалися змусити їх різними маніпуляціями та вигаданими історіями про родичів віддати свої кошти, то зараз людина навіть може й не одразу дізнатися, що стала жертвою таких злочинців.

Усі не одноразово чули про різноманітні схеми фінансового шахрайства. Проте переконані, що їх шахраї точно не зможуть обманути. Проте все одно в той чи інший період часу фізичні особи можуть стати жертвами фінансових злочинців.

Сьогодні існують багато різноманітних схем фінансового шахрайства: від найпростіших – якимось чином дізнатися пін-код від карти і викрасти карту, і до складних маніпуляцій через телефон та мережу Інтернет, зокрема інтернет-банкінгу.

Аналіз основних досліджень і публікацій. Необхідно закцентувати увагу, що в Україні дослідження проблем фінансового шахрайства переважно перебуває у полі зору представників юридичної науки, а саме наступних науковців: Абрамейцевої Є.А., Атаманова Р., Каратаєва М., Кізими Т., Хамиги Ю., Франка С., Пола В. та інших. А ось вітчизняна економічна наука, і фінансова зокрема, ці питання, на жаль, практично не досліджує. Саме тому дана проблематика залишається відкритою.

Виділення невирішених раніше частин загальної проблеми. Актуальною проблемою сьогодення є вирішення питань щодо обізнаності населення щодо існуючих схем фінансового шахрайства з банківськими рахунками та способів убезпечення фізичних та юридичних осіб від шахраїв.

Формулювання цілей статті (постановка завдання). Завданням статті є проведення дослідження найпоширеніших шахрайських схем, аналізу обсягів збитків від шахрайських маніпуляцій та шляхів захисту фізичних та юридичних осіб від злочинців такого роду.

Виклад основного матеріалу дослідження. В умовах розвитку науково-технічного прогресу людство все менше виконує в повсякденному житті платежі готівкою, що підсилює роль банківських карток у фінансових розрахунках. Це в свою чергу зумовлює розвиток фінансового шахрайства з банківськими рахунками фізичних та юридичних осіб [2].

Найпростіша схема фінансового шахрайства – встановлення шахрайських пристроїв на банкоматах для зняття готівки. Шахрайськими пастками є приховані камери, накладні клавіатури та пристрої (скіммери), які викрадають персональну інформацію фізичних осіб з банківських карт. Скіммер встановлюється на картоприймач, або всередину нього. За допомогою нього зчитуються данні банківської карти. Частіше це стається з картками, що мають лише магнітну стрічку, оскільки безконтактні картки та картки з чіпом захищені краще. Проте за даними НБУ таких карток у 2019 році було лише близько 15%, а саме 6 млн. У 2020 році їх кількість зросла на 73% – безконтактних платіжних карток було емітовано 13,2 млн. штук. Це означає, що переважна більшість фізичних осіб володіють банківськими картками з меншим рівнем захисту [1].

Наступний крок – фінансові шахраї роблять копію карти фізичної особи, щоб зняти готівку. Для цього їм ще необхідний пін-код. Його вони дізнаються за допомогою прихованої камери, або накладки на клавіатуру, яка фіксує, які цифри було натиснено.

Наступна розповсюджена схема сьогодення – фінансове SMS-шахрайство. Фінансові шахраї надсилають на мобільний телефон SMS з різноманітним текстом. Таке SMS-повідомлення може інформувати фізичну особу, ніби від імені банку, що карта заблокована і необхідно терміново зателефонувати

за номером вказаним нижче. Або ж у повідомленні йдеться про те, що з платіжної карти даної фізичної особи було переказано фінансові ресурси у певному розмірі, і вказано телефон для довідок. Коли фізична особа зателефонує за цим номером, фінансові шахраї виманять одноразовий пароль, який прийде у іншому SMS-повідомленні. Володіючи такою інформацією фінансові шахраї можуть оволодіти фінансовими ресурсами фізичної особи, які знаходяться на банківському рахунку.

Також повідомлення можуть надходити від імені друга чи родича фізичної особи із проханням позичити певну суму коштів. Фінансові шахраї злочинним шляхом отримують доступ до їх сторінок в соціальних мережах і пишуть фізичній особі.

Третя схема – телефонне фінансове шахрайство. Це найпоширеніший вид фінансового шахрайства. Фінансовий злочинець телефонує і переконує фізичну особу повідомити особисту, фінансову чи конфіденційну інформацію або переказати фінансові ресурси. Метою фінансових шахраїв є дізнатися реквізити карти, паролі та SMS-коди від банків та мобільних операторів. Найпоширенішими ознаками телефонної розмови із фінансовим шахраєм є тривожна ситуація для фізичної особи, психологічний тиск з боку співрозмовника та поспіх.

Сценарії телефонного фінансового шахрайства можуть бути різноманітними. Наприклад, фізичній особі повідомляють, що воно виграла велику суму коштів, але, щоб їх отримати потрібно переказати на інший банківський рахунок плату за комісію, тощо. Або ж фінансовий шахрай представляється представником служби безпеки банку. Він повідомляє про кібератаку на ІТ-систему банку, запевняє, що вони намагаються все виправити і взяти ситуацію під контроль, але щоб фінансові ресурси фізичної особи були в безпеці, то їх потрібно перерахувати на тимчасовий резервний рахунок. Жертвою фінансових телефонних шахраїв може стати особа, яка хоче продати певне майно через мережу Інтернет. Фінансові шахраї запевняють продавця, що проведуть безготівковий розрахунок на банківську карту, дізнаються від фізичної особи необхідну інформацію (номер карти та одноразовий пароль). Зазвичай, такі телефонні дзвінки здійснюють вранці, в кінці робочого дня чи робочого тижня, коли фізична особа виснажена, втомлена та не така сконцентрована, чуття притуплені, не така хороша пам'ять, увага та сприйняття інформації. Розмова тримається у нервовому напружені, що збиває з пантелику [6].

Четверта схема – крадіжка фінансового номеру телефону. Фінансовий номер телефону – це номер, який прив'язаний до банківських рахунків. На нього приходять усі коди для підтвердження операцій, паролі від банків, інформація про баланс коштів на рахунках.

Фінансові шахраї поповнюють фінансовий номер телефону фізичної особи двічі на незначну суму, роблять дзвінок фізичній особі і кидають слухавку. Володіючи інформацією про останні суми поповнення фінансового номеру телефону та номер останнього вхідного дзвінка, фінансові шахраї відновлюють SIM-карту як втрачену, і стають власниками фінансового номеру телефону фізичної особи. Таким чином фінансовий шахрай має доступ до інтернет-банкінгу та до одноразових паролів. За допомогою даної схеми фінансового шахрайства за три роки було збільшено середню суму викрадених фінансових ресурсів з банківських рахунків фізичних осіб в 5 разів, а саме з 2400 грн. до 12500 грн.

П'ята схема – фінансове шахрайство у сфері онлайн-покупок. Фізична особа переказує фінансові ресурси фінансовим шахраям, але не отримує товар. Є певні ознаки псевдо-продавців, які мають насторожити фізичну особу перед здійсненням покупки. Це занижена вартість товару, короткі терміни для оплати, мало інформації про товар, необізнаність продавця щодо технічних характеристик товару, перенаправлення з сайту на месенджер для листування [4].

У 2020 році 32 банки звернулися до НБУ із скаргами щодо платіжного шахрайства по відношенню до їх клієнтів. Загальна кількість незаконних дій з платіжними картками та фінансові збитки фізичних осіб понесені від фінансового шахрайства наведені у таблиці 1.

Кількість незаконних дій з платіжними картками коливається від 71,9 до 105,5 випадків. Середня сума однієї шахрайської операції має стійку тенденцію до спадання – від 2500 грн. зменшилася до 1900 грн.

Дані про розподіл збитків від шахрайських дій за різновидами представлено на рисунку 2.

Встановлено чітку тенденцію до зростання збитків понесених фізичними особами у 2020 році порівняно з 2019 у всіх напрямах фінансового шахрайства. Сума викрадених фінансових ресурсів від скіммінгу збільшилася на 46,67%, від фінансового шахрайства в мережі Інтернет – на 27,63%, від фінансового шахрайства у торговельних мережах – на 8,82% та від інших фінансових шахрайських дій – на 33,33%.

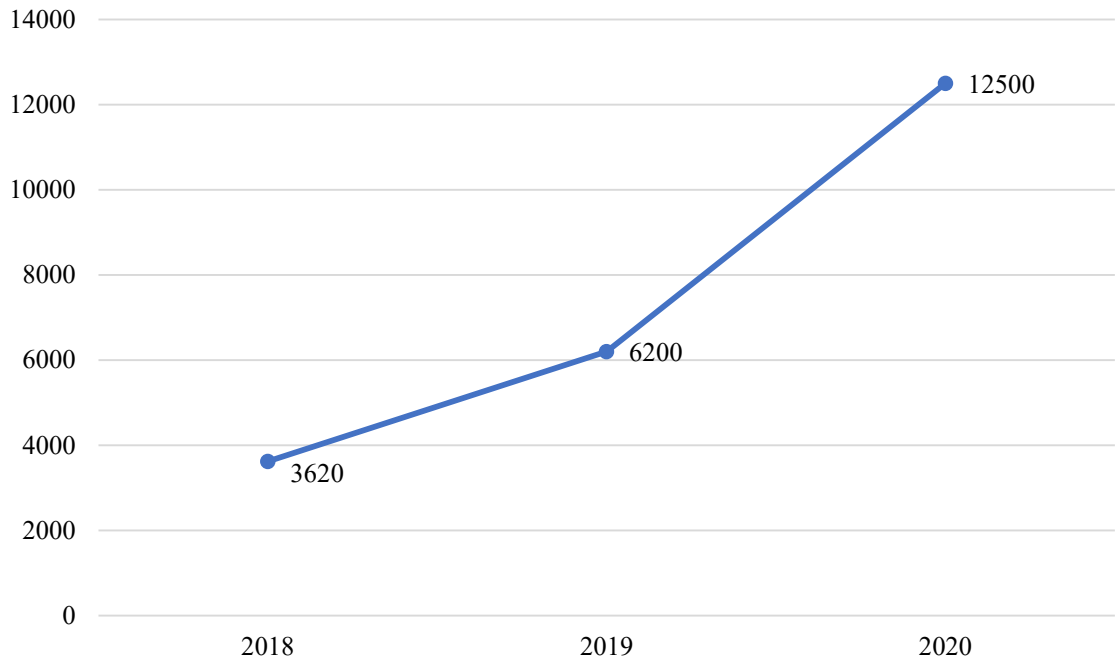

Рис. 1. Середня сума збитку від викрадення фінансового номеру телефона у 2018–2020 рр.

Джерело: дані систематизовано авторами на основі [3]

Дані про кількість здійснених шахрайських фінансових операцій з платіжними картками фізичних осіб представлено на рисунку 3.

Встановлено чітку тенденцію до зростання кількості здійснених шахрайських фінансових операцій з банківськими картками фізичних осіб у 2020 році порівняно з 2019 у всіх напрямах фінансового шахрайства. Кількість випадків скіммінгу збільшилася на 9,09%, фінансового шахрайства в мережі Інтернет – на 46,34%, фінансового шахрайства у торговельних мережах – на 36,36% та інших фінансових шахрайських дій – на 37,5%.

У випадку з скіммінгом сума збитків зросла майже вдвічі, а от кількість шахрайств лише на 9%. Це означає, що фінансові шахраї почали викрадати фінансові ресурси фізичних осіб у більшому обсязі за одну здійснену операцію. Щодо фінансового шахрайства у мережі Інтернет та торговельних мережах – більше зросла кількість збитків, аніж сума викрадених фінансових ресурсів. Це означає, що фінансові шахраї оволоділи фінансовими ресурсами більшої кількості фізичних осіб, але на одну операцію припадала менша кількість фінансових ресурсів.

Таблиця 1

Основні показники здійснення незаконних операцій з платіжними картками у 2018–2020 рр.

Показник	2018	2019	Відхилення		2020	Відхилення	
			Абсолютне 2019–2018	Відносне 2019/2018, %		Абсолютне 2020–2019	Відносне, 2020/2019, %
Кількість незаконних дій з платіжними картками, тис. шт.	105,5	71,9	-33,6	68,15	101	29,1	140,47
Середня сума однієї шахрайської операції, грн.	2500	2100	-400	84	1900	-200	90,48
Сума збитків від шахрайських дій від загального обсягу всіх операцій, %	0,0092	0,0042	-0,005	45,65	0,0048	0,0006	114,29

Джерело: дані систематизовано авторами на основі [3]

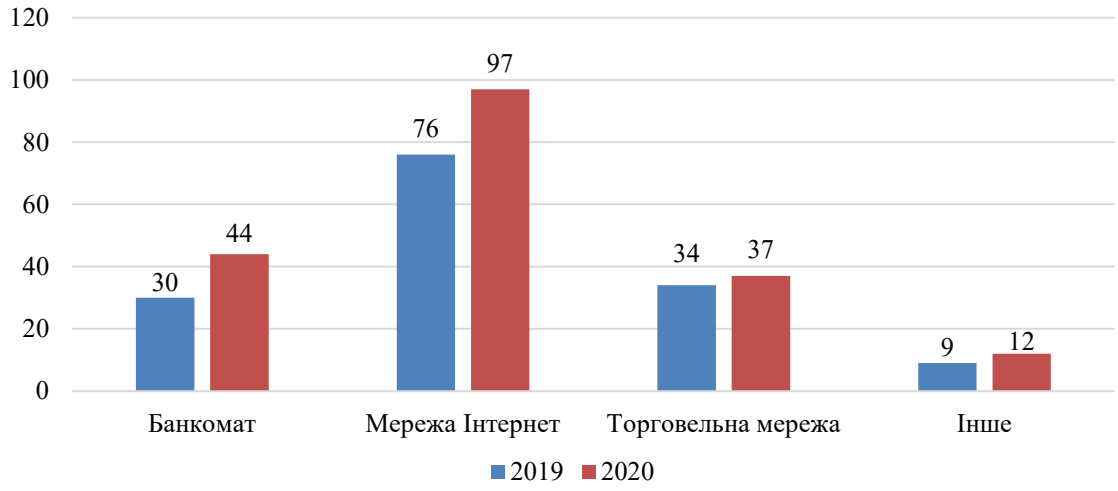

Рис. 2. Сума збитків від шахрайських дій з платіжними картками

Джерело: дані систематизовано авторами на основі [3]

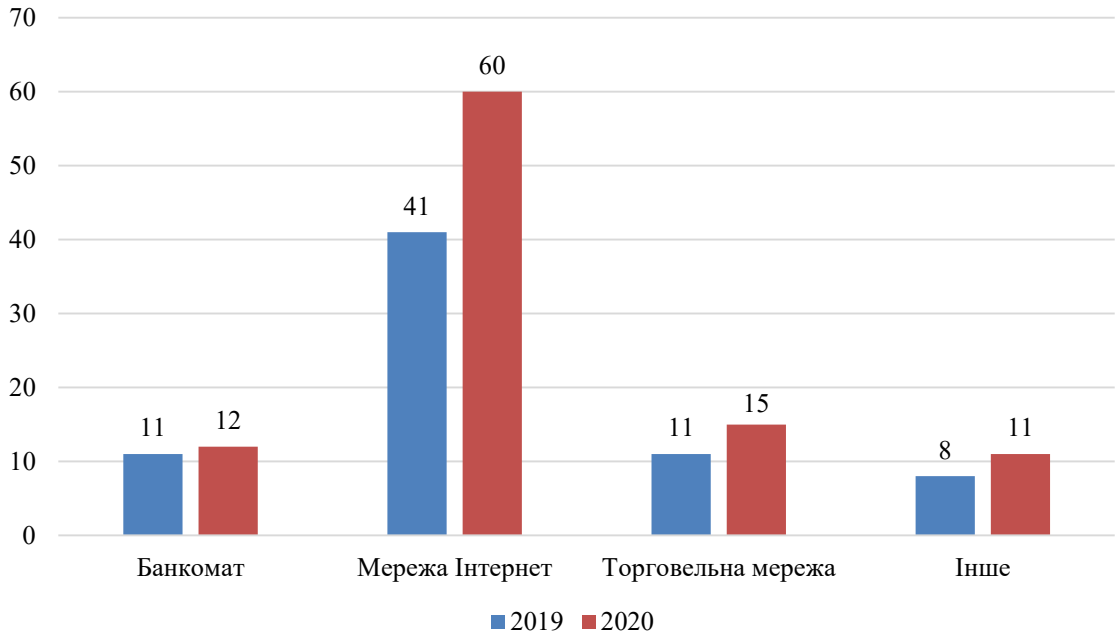

Рис. 3. Кількість здійснених шахрайських фінансових операцій за різновидами

Джерело: дані систематизовано авторами на основі [3]

За середньою сумою збитків банківських установ від фінансових шахрайських дій у 2020 році перше місце зайняло викрадення фінансового номеру телефону – 12500 грн., друге місце посів скіммінг – 3646 грн., а третє місце – фінансове шахрайство у торгових мережах, а саме 1984 грн. Збитки від фінансового шахрайства в мережі Інтернет в середньому становлять 1622 грн.

Збільшення з кожним роком кількості фінансових шахрайських маніпуляцій та обсягів викрадених фінансових ресурсів пояснюється тим, що фінансові шахраї систематично вдосконалюють свої техніки та вигадують нові схеми фінансового шахрайства.

Для того, щоб захистити фінансові ресурси на банківських рахунках від фінансових шахраїв, фізичним особам варто:

– бути обізнаними про відомі схеми фінансового шахрайства та спосіб їх роботи;

– покращувати знання щодо платіжної безпеки;

– знати, які дані безпечно розголошувати третім особам (16-значний номер картки), а які потрібно зберігати в таємниці (CVV/CVC код, термін дії картки, кодові слова та коди з SMS-повідомлень);

– підключити функцію банку SMS-інформування стосовно операцій з платіжною карткою, щоб моніторити здійснені фінансові операції;

– встановити індивідуальні ліміти на операції з платіжною карткою;

– знімати готівку в банкоматах, що розташовані в приміщеннях банків, оскільки ймовірність наявності шахрайських пристроїв значно менша;

– ретельно перевіряти банкомати для зняття готівки на наявність шахрайських пристроїв. У разі виникнення підозр щодо банкомату краще використати інший. Обов'язково необхідно повідомити банківську установу про це;

– відповідально підходити до створення паролів до банківської карти та інтернет-банкінгу. Складний пароль має містити більше 7 символів. Краще застосовувати і малі, і великі літери, а також символи та цифри. Не потрібно пов'язувати паролі з датою народження, чи вашим ім'ям та прізвищем. Також не слід користуватися загальновідомими комбінаціями (qwerty12, password123456, тощо) чи послідовним написанням цифр ти літер. Основним правилом є те, що всі паролі мають бути унікальними. Не можна використовувати один пароль для всіх сторінок, електронної пошти, інтернет-банкінку тощо, навіть якщо він складний.

– раз на три місяці змінювати пін-код до карти, або якщо виникла підозра, що його хтось дізнався;

– ігнорувати незрозумілих SMS-повідомлень;

– не розмовляти з фінансовими шахраями по телефону

– зареєструвати фінансовий номер телефону на паспорт, щоб відновити втрачену SIM-карту можна було лише з паспортом власника;

– здійснювати онлайн-покупки на захищених та перевірених сайтах;

– заблокувати карту та повідомити банківську установу про випадок шахрайства у разі підозрілої ситуації – зняття готівки з ненадійного банкомату, виявлення фінансових операцій, що здійснені третіми особами;

Висновки. Варто зазначити, що фінансові шахраї постійно вдосконалюють свої навички по викраденню фінансових ресурсів фізичних осіб з банківських рахунків. Кількість фінансових злочинів та суми понесених збитків мають чітку тенденцію до зростання. На жаль, не існує ідеального способу протидії фінансовим шахраям, який буде працювати на 100%. Проте вже багато схем відомо та є багато порад, як правильно й ефективно протидіяти фінансовим шахраям. Тобто потрібно завжди цікавитися актуальної інформацією, щоб знати як діяти у тій чи іншій ситуації. Необхідно з особливою обережністю підходити до збереження конфіденційної інформації в таємниці. З відповідальністю підходити до створення паролів та не використовувати надто легкі паролі чи однакові для усіх аккаунтів.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. Абрамейцева Є.А. Види фінансового шахрайства. *Фінансове право*. 2020. № 3. С. 45–52.

2. Атаманов Р. Основи методики розслідування шахрайства в Інтернеті. Москва, 2018. 182 с.

3. Дані з сайту НБУ. URL: https://bank.gov.ua/ua/news/all/zbitki-vid-nezakonnih-diy-iz-platijnimi-kartkami-zmenshilisya-bilshe-nij-udvichi

4. Каратаєв М. Фінансове шахрайство в Інтернеті. Москва, 2016. 20 с.

5. Кізима Т., Хамига Ю. Фінансове шахрайство: теоретична концептуалізація та економічне підгрунтя. *Світ фінансів*. 2019. № 2. С. 109–123.

6. Франк С., Пол В. Розуміння жертв шахраїв: сім принципів безпеки систем. *Комунікації ACM*. 2017. № 54(3). С. 70–75.

REFERENCES:

1. Abrameytseva E.A. (2020) Types of financial fraud. *Finance law*, no. 3, pp. 45–52.

2. Atamanov R. (2018) Fundamentals of methods of investigating fraud on the Internet. Moscow.

3. Electronic resource. Data from the NBU website. Available at: https://bank.gov.ua/en/news/all/zbitki-vid-nezakonnih-diy-iz-platijnimi-kartkami-zmenshilisya-bilshe-nij-udvichi

4. Karatayev M. (2016) Financial fraud on the Interne. Moscow.

5. Kizima T., Khamiga Y. (2019) Finansove shakhraistvo: teoretychna kontseptualizatsiia ta ekonomichne pidhruntia [Financial fraud: theoretical conceptualization and economic basis]. *Svit finansiv – The world of finance*, no. 2, pp. 109–123.

6. Frank S., Paul W. (2017) Understanding the victims of fraud: seven principles of system security. *ACM communications,* no. 54(3), pp. 70–75.