

## ШАХРАЙСТВО ЯК ЗАГРОЗА ЕКОНОМІЧНІЙ БЕЗПЕЦІ БАНКУ

**Анотація.** У статті основна увага приділяється шахрайству в банках та заходам щодо мінімізації цієї проблеми. Банківське шахрайство на сьогоднішній день є проблемою глобального характеру для банків та їх клієнтів. За останні роки збитки від фінансових шахрайств зросли кардинально. Це має негативні наслідки для клієнтів фінансово-економічних агентів, які стають основним об'єктом шахрайств та втрачають кошти. В умовах зародження і становлення ринкових відносин шахрайство є досить поширеним явищем, оскільки і звичайні, і нестандартні форми бізнесу можуть здійснюватися в межах чинного законодавства. Інколи неможливо визначити, що здійснюється: нова форма бізнесу, афера чи незловмисно допущена помилка. Небезпечність шахрайства завжди була і є досить актуальною, особливо, коли банк може непомітно втратити значний капітал.

**Ключові слова:** безпека банків, банківська система, шахрайство, фінансова безпека, крадіжка, вішинг, смішинг, мобільний банк, банківська картка.

Yanchuk Tetiana, Selivanova Kateryna, Nesterchuk Kateryna  
University of State Fiscal Service of Ukraine

## FRAUD AS A THREAT TO ECONOMIC SECURITY OF BANK

**Summary.** The article focuses on bank fraud and measures to minimize this problem. Today, electronic financial transactions are getting popular, card transactions and digital money are growing rapidly. Modern innovative technologies have made it possible to make payments through special software applications installed on mobile devices. Information technologies made payment and financial transactions easy and fast, regardless of the location of the payer or payee, the availability of funds on the account, the type of payment transaction, etc. However, along with the mentioned trends, banking fraud is also growing and today it is a global problem for banks, their customers and those entities that are eligible to conduct financial transactions. In recent years, losses from financial fraud have increased dramatically. This has negative consequences for clients of financial and economic agents who become a major fraud target and lose money. Fraud is also causing significant damage to banks, resulting in the loss of customers, the need to recoup stolen funds, increasing the cost of cybersecurity upgrade. In the context of the emergence and formation of market relations, fraud is quite common because both ordinary and non-standard forms of business can be carried out within the current legislation. Sometimes it is simply impossible to determine what is happening: a new form of business, a scam, or a mistake. Fraud danger is always relevant, especially in the banking sector, when the bank may lose significant capital in seconds. It can be argued that banking activities are quite risky, since every moment is exposed to a large number of threats, the implementation of which can cause significant losses to the bank. Today, scammers can chat with their victims on job search sites, dating sites, and more. Under these conditions, banks should constantly monitor for such threats and take all measures to counteract and counteract them. To combat fraud, banking institutions need to be approached comprehensively, constantly improving the bank's economic security system. Obviously, the more efficient this system will operate, the less fraud will occur.

**Keywords:** bank security, banking system, fraud, financial security, theft, voice phishing, SMS phishing, mobile bank, bank card.

**Постановка проблеми.** Безпека банків є частиною фінансової безпеки країни. Необхідно зазначити, що банківська система – важливий елемент фінансово-кредитної системи країни, адже через неї відбувається велика кількість фінансових операцій, які обслуговують усі сфери діяльності держави. В умовах зростаючої відкритості економіки України та послідовної її інтеграції у світове господарство забезпечення безпеки банківської системи є актуальним завданням. Актуальність даного питання зумовлена необхідністю реалізації національних інтересів щодо створення конкурентоспроможної, соціально орієнтованої ринкової економіки та забезпечення постійного зростання рівня життя і добробуту населення [1].

На жаль, сучасний стан української банківської системи залежить від низки чинників, які роблять її вразливою та мінливою, що, своєю чергою, поглиблює недовіру з боку клієнтів.

Інтеграційні процеси України у світову економіку, слабкий розвиток фінансового ринку

та його інфраструктури, недосконалість чинного законодавства, фінансова криза, зменшення реальних доходів населення і бізнесу, масове скорочення робочих місць та зростання безробіття, корупція та криміналізація економіки ставлять перед системою економічної безпеки банку нові завдання, що призводить до появи нових, раніше не характерних банківській діяльності загроз.

Захист інтересів банків – найважливіша функція його сил безпеки. Одне з провідних місць у сфері інтересів банку посідає збереження своїх ресурсів і ефективне їх використання. Процес забезпечення даного інтересу передбачає активну участь у ньому персоналу банку, від професіоналізму, лояльності, надійності та чесності якого залежить ефективність досягнення мети даного інтересу. На жаль, історія розвитку стосунків банків зі своїм персоналом показує, що вони практично ніколи не були ідеальними.

Причин цьому вельми багато, але природа одна – різниця інтересів. Банки прагнуть отри-

мати від свого персоналу максимальну вигоду, суттєво оптимізуючи його утримання. В цей же час персонал прагне до максимального задоволення своїх потреб, суттєво оптимізуючи свою працю під час роботи в банку.

Відомий фахівець у сфері кадрової безпеки І.Г. Чумарін вказує, що близько 80% збитків матеріальним активам компаній наноситься їх власним персоналом. Опираючись на дані американських компаній, можна побачити наступну динаміку: вартість злочинів, здійснених посадовими особами і працівниками цих компаній склала в 1980 році 50 млрд дол., у 1990 – 250 млрд дол., в 1998 – 400 млрд дол., в 2002 – 600 млрд дол. [2]. Повертаючись до вітчизняних реалій, слід звернути увагу на такі факти: у 2009 р. з українських банків було викрадено 64 млн. грн., з них 62 млн. грн. вкрали співробітники цих фінансових установ [3].

#### **Аналіз останніх досліджень і публікацій.**

Проблема боротьби з шахрайством і не тільки в банках неодноразово розглядалась на різних всеукраїнських та міжнародних форумах, їй досить багато присвячено публікацій, аналітичних оглядів, пропозицій щодо протидії шахрайству. Аналізуючи сучасні публікації з даної тематики, підходи до визначення причин шахрайства персоналу з точки зору вказаних взаємовідносин можна знайти лише в обмеженій кількості авторів. Загальною проблематикою визначення шахрайства в банківській сфері, його суб'єктів, способів займалися такі науковці, як: А. Єпіфанов, М. Зацеркляний, Д. Козлов, О. Кришевич, В. Левін, С. Ніколаюк, С. Поперешняк, І. Сало, О. Саяпін, С. Шапочка, А.М. Шевченко та інші, що знайшло відображення у низці наукових публікацій.

Слід звернути увагу, що посилення на шахрайські дії персоналу суб'єктів підприємницької діяльності, в тому числі і банківського бізнесу як одну із загроз, зустрічаються не рідко, але дослідження цих проблем, особливо з точки зору протидії йому здебільшого авторами обходяться.

Боротьба з фінансовим шахрайством є поширеною проблемою на банківському ринку, тому актуальним є розв'язання завдань із забезпечення фінансової безпеки кожного комерційного банку. Важливим напрямом у вирішенні завдань із забезпечення фінансової безпеки в комерційному банку є застосування механізмів боротьби з фінансовим шахрайством.

**Постановка завдання.** Основними завданнями статті є: формування погляду щодо економічної і морально-соціальної суті шахрайства, особливостей його скоєння персоналом банків; обґрунтування специфіки та основних характеристик умов, за яких скоюються шахрайські дії в банках; аргументування підходів до створення системи комплексного захисту і протидії шахрайству персоналу установ банків.

**Виклад основного матеріалу.** Згідно ст. 190 ККУ, під шахрайськими діями розуміється заволодіння чужим майном або придбання права на майно шляхом обману або зловживання довірою. Шкода шахрайства для банків проявляється у втраті клієнтів, необхідності відшкодувати вкрадені кошти, збільшенні коштів на модернізацію служби кібербезпеки та посилення захисних заходів. Поширеними є: шахрайства з банківськими картками, як найбільш простий, доступний

та масовий спосіб платежу, Інтернет-шахрайства, коли Інтернет, який є платформою для клієнтів банку, використовується шахраями як інструмент для крадіжки особистих фінансових даних клієнтів; соціальна інженерія, коли шахрай від імені банку дізнається у клієнта всю його інформацію та викрадає кошти з його рахунку.

За своїм походженням банківське шахрайство може бути як внутрішнім, так і зовнішнім. Лише незначна частина шахрайських дій відноситься безпосередньо до клієнтів банківських установ або зовнішніх злодіїв.

Основними видами шахрайства з їхнього боку є надання неправдивих відомостей про себе і свою діяльність, приховування обставин і фактів, організація фіктивного підприємництва, фальсифікація товарів і послуг з метою створення в банку уявлення про перспективне підприємство та ефективну його діяльність.

Суттєва частка шахрайств здійснюється за згодою і за участю співробітників банку, оскільки привласнити певну суму грошей без залучення співробітників банку практично неможливо.

Для забезпечення високого рівня регулювання дій і поведінки працівників банку необхідно розробити відповідні норми, яким повинна відповідати та або інша робота за якістю, кількістю, часом і т. д. Подібні параметри (вимоги) мають бути також розроблені для поведінки і професійних дій працівників як на своєму робочому місці, так і на весь період їх робочого часу.

Законність дій і поведінки персоналу досягається розробкою нормативних документів, що визначають порядок, правила, технології проведення операцій, виконання посадових функцій, встановленням режимів безпеки, високими і об'єктивними вимогами до персоналу і невідворотним покаранням працівників, що порушили трудову або виробничу дисципліну.

Банківська система безпеки часто не встигає за швидкими темпами модернізації способів та інструментів шахраїв. Відповідно рівень протидії загрозам поступаєть рівню зростаючих загроз. За оцінками експертів серед галузей, які найбільше потерпають від шахраїв, перше місце займає банківський сектор, друге – енергетичний та добувний сектор, третє – телекомунікаційний. Так, у 2018 році від фішингових атак найбільшої шкоди зазнали 51,7% банків у порівнянні з електронною комерцією та платіжними системами – представниками фінансового сектору [4].

За статистичними даними ЕМА (Української міжбанківської асоціації членів платіжних систем), сума збитків громадян внаслідок дій шахраїв із платіжними картками у 2018 році досягла 670 млн грн, що значно перевищує збитки за попередні роки – 339,13 млн грн (2017 р.), 181,00 млн грн (2016 р.), 90,00 млн грн (2015 р.). Збільшилася також і середня сума втрат від шахрайства із використанням методів соціальної інженерії. Так, у 2017 році ця сума склала 2543,00 грн проти 1403,00 грн у 2016 році та 834,00 грн у 2015 році [5].

Боротьба із шахрайством – це глобальна проблема. Для її вирішення створюються спеціальні підрозділи, її намагаються регулювати на законодавчому рівні. На боротьбу із шахрайством впливають:

- розвиток нових способів шахрайства;
- збільшення обсягу інформації, обробка якої потребує нових методів, наприклад, Data Mining;
- обмеження в інформаційних системах, які не дозволяють своєчасно адаптувати їх до ефективною протидії новим за формою і рівнем новизни загрозам;
- проблеми, пов'язані з управлінням даними на фізичному та організаційному рівнях; – банківські ризики;
- психологія взаємовідносин «клієнт – шахрай – банк», яка дозволяє клієнту у випадках спілкування із шахраєм надавати конфіденційну інформацію [6].

Одним із головних напрямків боротьби із шахрайством, зазначеним у Постанові НБУ №95 «Про затвердження Положення про організацію заходів із забезпечення інформаційної безпеки в банківській системі України» від 28 вересня 2017 року, є впровадження банками основних технічних систем [6]: виявлення атак; моніторингу події управління інцидентами; контролю доступу до мережі; захисту електронної пошти; запобігання атак, спрямованих на відмову в обслуговуванні; антивірусного захисту; двофакторної автентифікації.

Фінансове шахрайство в комерційному банку поширене явище в банківській сфері, особливо серед українських комерційних банків. Слід також урахувати особливі конструкції фінансового шахрайства в комерційних банках, які набирають масштабів поширення. Шахрайською новацією є маскування залучення фінансових ресурсів від вкладників із задіянням небанківської фінансової установи з наступним заволодінням фінансовими ресурсами і позбавлення вкладників грошових коштів та законних прав на державне відшкодування їхніх вкладів.

Представники Національного банку України зазначають, що в Україні сформувалась культура шахрайства і без підвищення рівня захищеності комерційних банків не відбудеться відновлення кредитування [7]. Це, в свою чергу, дозволяє відмітити, що за відсутності кредитування неможливе й відновлення економіки країни в цілому. Такий стан справ вимагає прискіпливої уваги до фінансового шахрайства в комерційних банках, до виявлення його чітких характеристик та їх систематизації, тобто класифікації фінансового шахрайства в комерційному банку. Фінансове шахрайство – типовий спосіб недобросовісного заволодіння фінансовими ресурсами комерційного банку. Цей вид шахрайства призводить до втрати грошових коштів комерційним банком унаслідок їх розміщення на кореспондентських рахунках в іноземних комерційних банках із сумнівною репутацією. Фігурування у кримінальних провадженнях чи підозра у вчиненні злочинів вищих керівників комерційного банку чи його власники, мотивує їх до заволодіння грошовими коштами. Це роблять для того, щоб, по-перше, захистити фінансові ресурси від їх втрати на території держави, по-друге – у разі виїзду за кордон ці ресурси будуть використовуватись для життєзабезпечення, нового бізнесу, по-третє – їх складно виявити слідчим органам і, відповідно, заарештувати, конфіскувати тощо.

Протягом останніх років в українських банках не так часто трапляються гучні крадіжки за до-

помогою технічних ноу-хау. Нещодавно історія, коли шахраї вивели з одної з найбільших фінустанов близько 170 тис. кредитних коштів через поповнення двох десятків мобільних номерів, стала справжньою сенсацією. Ринком ходили плітки, що в справі «працювали» хакери, які виявили уразливість в системі захисту мобільного додатка банку.

Насправді в цій історії не було нічого незвичайного. Але вона нагадала: паралельно з розвитком банківських технологій, еволюціонують і шахраї.

Вище згадана афера сталася в ПУМБі ще на початку 2019 року. Як виявилось, реальний клієнт банку знайшов спосіб обійти обмеження з використання кредитного ліміту (овердрафт). Він просто поповнював свій мобільний, а потім пересилав гроші на 23 різних номерів – всі з системи оператора Київстар.

Ця історія могла б стати черговим прикладом навіть не шахрайства, а звичайної спроби «грубої» крадіжки, якби не одна деталь – у зловмисників навряд чи вийшло б домогтися результату, якби їм не допомагав сам клієнт банку.

За даними Асоціації членів платіжних систем ЕМА, у 2018 році на соцінженерію припадало 68% всіх випадків «роботи» зловмисників. На даний момент сама «галузь» переживає явний регрес: якщо в 2017 році на соцінженерії шахраї заробили 510 млн грн, то в минулому їх доходи склали 241 млн грн. «Середній чек» однієї шахрайської операції залишився на колишньому рівні – близько 2,4 тис. грн. Все це означає, що шахраям стало складніше виманювати дані банківських карт за допомогою примітивного обману. Їх підходи весь час ускладнюються.

Є декілька найбільш поширених способів шахрайства, за допомогою яких злочинці виводять гроші з рахунків фізосіб.

Вішинг – телефонне шахрайство. Злочинці телефонують власнику платіжної картки від імені співробітника банку і розповідають, що його рахунок заблокований або з нього зняли гроші. Щоб вирішити цю проблему, їм потрібно отримати дані карти.

Смішинг – це схожа афера, але за допомогою SMS. Часто аферисти використовують його як підготовку до вішингу. Поширений прийом – повідомлення про те, що користувач виграв грошовий приз і йому потрібно надати додаткову інформацію, тобто дані карти.

Фіктивні покупці і продавці. Покупці зазвичай працюють в парі: перший «переводить» гроші за товар, другий – інформує продавця від імені банку, що гроші зараховані на рахунок, але для підтвердження операції потрібні дані карти. Фіктивні продавці маскуються під реальних, виманюючи передоплати за неіснуючий товар.

Перевипуск SIM-карти і крадіжка фінансового номера, який прив'язаний до платіжної картки. Таким чином шахраї отримують доступ до кодів і паролів, які банк відправляє клієнту для підтвердження платіжних операцій [8].

У 2018 в Україні з'явився новий спосіб отримати персональні банківські дані користувачів. Для цього шахраї створили додаток для Android Універсальний Мобільний банкінг, Шахрайський додаток об'єднує зручний банкінг відразу для всіх банків. Для цього при реєстрації корис-

тувачів просять вказати дані з карт, включаючи CVV-код. Цей додаток з'явився в Google Play 14 лютого і за три дні набрав 5 тис. завантажень. На таку ситуацію у «ПриватБанку» заявили, що єдиним додатком, що дозволяє користуватися послугами банку з мобільних пристроїв, є «Приват24». У банку повідомили, що будь-які сторонні «мобільні банки» створені для крадіжки особистих даних клієнтів і крадіжки грошей [9].

**Висновок.** Отже, протидія шахрайству є досить складною, багатосторонньою і важкою ділян-

кою роботи не лише для підрозділу безпеки, але і всього колективу банку. Складність полягає насамперед у тому, що боротьбі з шахрайством необхідно надати системний і комплексний характер, залучити до неї весь персонал, забезпечити інформаційно і організувати ефективне управління нею. В той же час практика показує, що вартість створення і впровадження в практику діяльності банків комплексної системи протидії шахрайству у декілька разів поступатиметься збиткам, понесеним від шахрайських дій персоналу.

## Список літератури:

1. Про основи національної безпеки України : Закон України від 19 червня 2003 року № 964-IV. *Відомості Верховної Ради України*. 2003. № 39. Ст. 351.
2. Чумарин И.Г. Что такое кадровая безопасность компании? *Кадры предприятия*. 2003. № 2. С. 34.
3. В Черновцах работники банка незаконно выдавали кредиты безработным. URL: [www.analitika.kiev.ua](http://www.analitika.kiev.ua) (дата звернення: 28.11.2019).
4. Козлов Д.Н. Система предотвращения мошенничества как составляющая кредитного конвейера. Д.Н. Козлов, В.В. Левин. *Банковское кредитование*. 2013. № 2(48). С. 15–25.
5. Подосенков Н.С. Риски мошенничества в торговом финансировании. *Управление финансовыми рисками*. 2015. № 4(44). С. 270–277.
6. Шевченко А.М. Зловживання та махінації на ринку фінансових послуг: методи боротьби, засоби протидії. *Глобальні та національні проблеми економіки*. 2015. № 7. С. 767–771.
7. Офіційний сайт Української міжбанківської Асоціації членів платіжних систем ЕМА Fraud Digest. URL: <https://ema.com.ua/fraud-digest-25-05-2017> (дата звернення: 27.11.2019).
8. Соцінженерія 2.0. Як шахраї обманюють банки та їх клієнтів. URL: <http://www.uekka.org.ua/novina/soc%D1%96nzhen%D1%96ya-20-yak-shahrayi-obmanyuyuty-banki-ta-yih-kl%D1%96yent%D1%96v.html> (дата звернення: 26.11.2019).
9. «ПриватБанк» повідомив про нове банківське шахрайство в Україні. URL: [https://zaxid.net/u\\_privatbanku\\_povidomili\\_pro\\_nove\\_bankivske\\_shahraystvo\\_v\\_ukrayini\\_n1449514](https://zaxid.net/u_privatbanku_povidomili_pro_nove_bankivske_shahraystvo_v_ukrayini_n1449514) (дата звернення: 27.11.2019).

## References:

1. Pro Osnovy Natsionalnoi Bezpeky Ukrainy (2003). [On the basics of Ukraine's national security]. Zakon Ukrainy vid 19 chervnia 2003 roku № 964-IV. Vidomosti Verkhovnoi Rady Ukrainy [Law of Ukraine of June 19, 2003 No. 964-IV. Information of the Verkhovna Rada of Ukraine]. № 39, p. 351.
2. Chumaryn, Y.H. (2003) Chto Takoe Kadrovaia Bezopasnost Kompanyy? [What is company personnel security?]. *Kadry Predpriyatiya* [Company personnel]. № 2, p. 34.
3. V Chernovtsakh rabotnyky banka nezakonno vydavaly kredyty bezrabytnym [In Chernivtsi, bank employees illegally issued loans to unprotected]. Available at: [www.analitika.kiev.ua](http://www.analitika.kiev.ua) (accessed 28 November 2019)
4. Kozlov, D.N., & Levyn, V.V. (2013). Systema predotvrashcheniya moshennychestva kak sostavliaiushchaia kredytnoho konveiera [Fraud Prevention System as a Part of the Credit Conveyor]. *Bankovskoe kredytovanye* [Bank lending]. № 2(48), pp. 15–25.
5. Podosenkov, N.S. (2015). Rysky moshennychestva v torhovom fynansyrovanny [Risks of fraud in trade finance]. *Upravlenye fynansovymy ryskamy* [Financial risk management]. № 4(44), pp. 270–277.
6. Shevchenko, A.M. (2015). Zlovzhyvannia ta makhinatsii na rynku finansovykh posluh: metody borotby, zasoby protydi [Abuse and fraud in the financial services market: methods of struggle, countermeasures]. *Hlobalni ta natsionalni problemy ekonomiky* [Global and national problems of economy]. № 7, pp. 767–771.
7. Ofitsiynyi sait Ukrainskoi mizhbankivskoi Asotsiatsii chleniv platizhnykh system EMA Fraud Digest [Official site of the Ukrainian Interbank Association of Payment System Members EMA Fraud Digest]. Available at: <https://ema.com.ua/fraud-digest-25-05-2017> (accessed 27 November 2019)
8. Sotsinzheneriia 2.0. Yak shakhray obmaniuiut banky ta yikh kliientiv [Co-engineering 2.0. How fraudsters cheat banks and their customers]. Available at: <http://www.uekka.org.ua/novina/soc%D1%96nzhen%D1%96ya-20-yak-shahrayi-obmanyuyuty-banki-ta-yih-kl%D1%96yent%D1%96v.html> (accessed 26 November 2019)
9. «PryvatBank» povidomyv pro nove bankivske shakhraistvo v Ukraini [PrivatBank has announced a new banking fraud in Ukraine]. Available at: [https://zaxid.net/u\\_privatbanku\\_povidomili\\_pro\\_nove\\_bankivske\\_shahraystvo\\_v\\_ukrukray\\_n1449514](https://zaxid.net/u_privatbanku_povidomili_pro_nove_bankivske_shahraystvo_v_ukrukray_n1449514) (accessed 27 November 2019).