УДК 336.763

О.М. Рац

Харківський національний економічний університет імені Семена Кузнеця, Харків

ДОСЛІДЖЕННЯ ОСОБЛИВОСТЕЙ ОРГАНІЗАЦІЇ ФРОД-МОНІТОРИНГУ В СИСТЕМІ УПРАВЛІННЯ ЕКОНОМІЧНОЮ БЕЗПЕКОЮ БАНКУ

В статті визначено сутність фрод-моніторингу як інструменту системи управління економічною безпекою банку. Досліджено об'єкти фрод-моніторингу відповідно до видів шахрайства в банківській діяльності та визначено особливості застосування моніторингових систем залежно від об'єкту шахрайства. На основі аналізу особливостей організації фрод-моніторингових систем, запропоновано принципи організації системи фрод-моніторингу для ефективної протидії шахрайству.

Ключові слова: *банк, економічна безпека банку, шахрайство, фрод-моніторинг, ризик-менеджмент банку.*

Постановка проблеми

Вітчизняні банківські установи, як і інші суб'єкти економіки, здійснюють свою діяльність в умовах непередбачуваності, невизначеності, загроз і небезпек. В той же час роль банків постійно підсилюється. Банківська система є важливим елементом економіки і справляє значний, різнобічний вплив на всі аспекти життєдіяльності суспільства. Банки виконують широкий спектр операцій, таких як: акумулювання грошових коштів і заощаджень, здійснення кредитно-розрахункових та інші операції. Крім того, майже всі фінансові потоки фізичних та юридичних осіб проходять через банки.

Сучасні банки функціонують в умовах дестабілізуючого впливу як зовнішніх, так і внутрішніх факторів. Нині гостро постає питання забезпечення економічної безпеки банківської системи держави як основи фінансової системи. Так, з 2013 р. у вітчизняному банківському секторі розпочався масовий процес реорганізації та ліквідації банків, обумовлений кризовими явищами в економіці. Тільки за 2014-2015 рр. кількість банків скоротилась на 46 (з 163 до 117) і станом на 01.02.2016 р. склала 116 установ [1]. Однак, діяльність банків, які залишились на ринку не можна визначити як успішну, що наглядно демонструє показник від'ємного фінансового результату впродовж двох останніх років (станом на 01.01.2016 р. чистий збиток склав 66 600 млн. грн.) [1].

Наявність вищезазначених проблем обумовлюється низкою факторів, серед яких, насамперед, слід відмітити низький рівень економічної безпеки банків, обумовлений недоліками функціонування діючих систем управління безпекою банківського бізнесу, які мають забезпечувати реалізацію основних інтересів, пріоритетних цілей банків, захист від впливу дії негативних факторів.

Однією з основних складових системи економічної безпеки є моніторинг банківських операцій як форма протидії шахрайству за різними функціональними сферами діяльності банку. Постійний моніторинг шахрайських дій як один з обов'язкових елементів системи управління економічною безпекою банку, є, на наш погляд, важливим та актуальним питанням в контексті забезпечення стійкого та ефективного функціонування вітчизняної банківської системи.

Аналіз останніх досліджень і публікацій

В літературі моніторинг несанкціонованих або шахрайських дій при неправомірному використанні банківських ресурсів (фрод-моніторинг) розглядають як частину системи моніторингу банківських процесів.

Різні аспекти проблем, пов'язаних з боротьбою з шахрайськими діями в банку досліджувались в роботах зарубіжних авторів: Т. Брар, М. Маннана, Дж. Сінкі, А. Усман, Х. Фрексіаза, Ю. Хатис [2-7] та ін. Іноземними вченими розглядається вузьке коло питань, спрямованих на вирішення певних практичних аспектів застосування фрод-моніторингових систем, зокрема у сфері електронного банкінгу.

Питанням досягнення стійкого фінансового й економічного стану банків на основі використання підходів, методів та інструментів забезпечення економічної безпеки банку присвячено праці вітчизняних науковців, зокрема Т. М. Болгар, С. І. Мельник, О. М. Колодізєва, І. М. Чмутової, Л. М. Перехрест, Р. Г. Сніщенка, О. М. Штаєр [8-15] та ін.

Аналіз даних робіт засвідчив, що теоретична база з питань з фрод-моніторингу банківської діяльності представлена надзвичайно невеликою

кількістю розробок, що потребує подальших досліджень в цій галузі, зважаючи на специфіку функціонування банківських установ України.

Метою цієї статті є аналіз сутності фрод-моніторингу в системі управління економічною безпекою банківського бізнесу та визначення особливостей його впровадження та організації в вітчизняному банківському секторі.

Виклад основного матеріалу

Економічна безпека банку є складною економічною категорією, яка визначається науковцями як певний стан, за якого при найбільш ефективному використанні матеріальних, інтелектуальних та фінансових ресурсів реалізуються його основні інтереси, забезпечується стабільність функціонування, фінансово-комерційний успіх, прогресивний розвиток, гарантується захист фінансового та кадрового потенціалу від усіх видів загроз та дестабілізуючих факторів, а також здатність миттєво реагувати на зміни внутрішнього та зовнішнього середовища, що забезпечить конкурентну перевагу на ринку банківських послуг, зумовлену відповідністю потенціалу й організаційної структури банку його стратегічним цілям і завданням [15, с. 101].

Залежно від поставлених керівництвом банку стратегічних завдань щодо забезпечення економічної безпеки банку, можна виділити основні цілі управління безпекою банківського бізнесу:

досягнення високих (запланованих) показників фінансових результатів функціонування банку;

забезпечення конкурентоспроможності банківських продуктів;

удосконалення організаційної структури банку та наявність ефективних менеджерів;

високий рівень кваліфікації персоналу;

ефективно організована система безпеки банку;

досконала система прогнозування, діагностування та попередження внутрішніх та зовнішніх загроз та ін.

Для ідентифікації й уникнення загроз, пов'язаних із несанкціонованими діями суб'єктів банківських операцій, використовується фрод-моніторинг окремих видів діяльності банку.

Фрод-моніторинг є важливим інструментом управління економічною безпекою банку. Його сутність полягає у моніторингу як внутрішньої, так і зовнішньої інформації на предмет виявлення зловмисних дій [8, с. 39]. Фрод-моніторинг базується на визначенні поведінкової моделі користувача і формальних правилах проведення банківських операцій [].

Загалом, під терміном «фрод» розуміють будь-який вид шахрайства в IT-сфері [2, с. 128]. Поширення електронної комерції сприяло значному збільшенню незаконних операцій з банківськими платіжними картками (кардінг або картковий фрод). Картковий фрод може значно загальмувати он-лайн бізнес, тому що власник карти може ініціювати процедуру повернення коштів. В ряді випадків міжнародні платіжні системи, які обслуговують цю картку, можуть застосувати штрафні санкції щодо власника он-лайн бізнесу.

Для вирішення даної проблеми існує спеціальний сервіс – «антифрод», який не дозволяє шахраям зняти гроші або купити товари з чужої банківської картки [7, с. 11].

Проте, на нашу думку, проблема карткового фрода повинна вирішуватись банком-емітетном картки, а власником бізнесу за рахунок власних коштів.

Після фінансово-економічної кризи 2008 р. питання захисту власних та залучених коштів від зовнішніх та внутрішніх загроз почали розглядатись банками на іншому, більш високому рівні. Якщо раніше такими заходами займалась служба безпеки банку майже тільки рівні фізичної охорони, то зараз вітчизняні банківські установи використовують комплексний підхід до організації моніторингу шахрайських дій. Розширюється впровадження систем фрод-моніторингу на основі різних програмних платформ.

Поява різних систем фрод-моніторингу пов'язано, насамперед з різноманіттям об'єктів фрод-моніторингу шахрайства банківської діяльності:

- шахрайство при наданні кредитів;
- шахрайство при здійсненні депозитних операцій;
- шахрайство в сфері дистанційного банківського обслуговування (ДБО);
- шахрайство з банківськими платіжними картками;
- шахрайство при здійсненні розрахункових операцій;
- шахрайство, пов'язане з неправомірними діями персоналу та ін.

З метою мінімізації проблемної заборгованості за кредитними операціями банки запроваджують різноманітні заходи, спрямовані на організацію на місцях моніторингу кредитного процесу. Його метою є виявлення проблем у стані якості кредитного портфеля, який останнім часом суттєво знизився під впливом як економічної, так і політичної нестабільності [12, 13].

За допомогою фрод-моніторингу кредитних операцій, банк може виявляти відхилення від встановленого алгоритму процесу кредитування клієнтів банку. При відхиленні від заданих параметрів кредитування, наприклад, таких як, недотримання графіку погашення заборгованості,

погіршення фінансового стану позичальника, нецільового використання кредиту й ін., система фрод-моніторингу визначає напрямок змін встановлених процесів та сповіщає про це відповідного спеціаліста. Впровадження фрод-моніторингу кредитних операцій дозволяє виявляти причини виникнення кредитного ризику та своєчасно застосовувати превентивні заходи з формування якісного кредитного портфелю.

Іншим видом шахрайства у банківській сфері є шахрайство з грошовими вкладами. Банки стикаються з постійними проблемами з попередження використання несанкціонованого використання банківських рахунків та, відповідно, захисту клієнтів від збитків з причини шахрайства [5, с. 3].

Застосування моніторингових систем боротьби із фродом з банківськими рахунками припускає налаштування сповіщень, які розкривають всі аспекти ризику, пов'язані з депозитними операціями і незаконним вилученням коштів. Дана система систематизує випадки шахрайства та дозволяє провести не тільки ретроспективний аналіз шахрайський дій, а й надавати інформацію щодо географічного розташування випадків шахрайства та виявляти стратегії шахрайства із банківськими рахунками.

Схожими за принципом організації є системи фрод-моніторингу шахрайства в сфері ДБО, при здійсненні розрахункових операцій та використанні банківських платіжних карток. На базі існуючої платформи фрод-моніторингу банківської діяльності впроваджуються додаткові рішення у вигляді модулів щодо боротьби з шахрайством з електронними платежами, ДБО, дебетовими та АТМ картками, для повного захисту рахунків клієнтів від шахрайства за будь-якими каналами зв'язку [14].

Робота з протидії шахрайству в цій сфері передбачає моніторинг підозрілих операцій з емісії та еквайрингу (аналіз операцій, робота з власниками карт, торговими точками) модернізацію і редагування правил відбору транзакцій в моніторингу залежно від зростання тенденцій ризиків шахрайства на ринку платіжних карт та в системі ДБО, блокування карт при підозрі на шахрайство, передача їх до відділення банку для подальшої консультації та перевипуску співробітниками фронт-офісу.

Окремим видом шахрайства, яке представляє суттєву загрозу діяльності банку є неправомірні та несанкціоновані дії його персоналу. Цей вид шахрайства пов'язаний із розкраданням коштів банку, неправомірним наданням кредитів (шахраям, заздалегідь неплатоспроможним клієнтам), крадіжкою внутрішньобанківської інформації, порушенням правил та інструкцій.

Моніторинг шахрайства персоналу поєднує алгоритми для виявлення видів шахрайства, які найбільш часто зустрічаються, а також комплексну аналітику з поведінковим профілюванням для виявлення дуже складних і серйозних випадків шахрайства [1, с. 126].

Аналіз розпізнавання шахрайства, як правило, проводитися за блоками: розкрадання активів клієнта, даних про клієнта, активів банку, порушення нормативних правил. Здійснення моніторингу шахрайства персоналу за блоками передбачає застосування аналітичних процедур для визначення кореляції шахрайства, аналізу поведінки клієнтів та пов'язаних з ними співробітників, аналіз прихованих зв'язків між співробітниками і рахунками, аналіз ефективності боротьби із шахрайством.

В цілому застосування систем фрод-моніторингу дозволяє відповідно до заданих правил автоматично виявляти і блокувати підозрілі операції.

Основними індикаторами, за якими проводиться відстеження шахрайських дій в банках є такі [2, 5]:

- суми платежів;
- одержувачі платежів (фізичні та юридичні особи) та їх призначення;
- середня або загальна кількість операцій за встановлений інтервал часу;
- IP/MAC-адреси і їх географія;
- ідентифікаційний номер пристрою;
- ресурси, які використовуються (тип операційної системи, браузер);
- «чорні» та «білі» списки одержувачів.

Всі системи фрод-моніторингу можна розділити на online і offline системи. Перші системи дозволяють проводити здійснення аналізу транзакцій в режимі реального часу. Offline системи виконують аналіз транзакцій тільки після їх завершення.

На думку деяких спеціалістів [4] на ринку статичні offline системи фрод-моніторингу втратили свою актуальність: при виявленні шахрайських транзакцій «постфактум», вони не здатні запобігти розкраданню грошових коштів. Однак, побудова комплексним систем, які б включали і оперативний аналіз транзакцій і систему обробки даних в режимі offline дозволила би нівелювати недоліки останньої та забезпечити міцну та гнучку систему запобігання шахрайству.

Організація фрод-моніторингу в вітчизняних та зарубіжних банках має суттєві відмінності. Якщо поширеною практикою іноземних банків є залучення сторонніх компаній, які спеціалізуються на виявленні шахрайства, то вітчизняні фінансові установи надають перевагу застосуванню власних

фрод-моніторингових систем.

Сьогодні на вітчизняному ринку існують пропозиції щодо продажу діючих фрод-моніторингових систем та модулей, таких як RSA Transaction Monitoring, Oracle Adaptive Access Manager, ArcSight FraudView [16] та ін.

Великі вітчизняні банки, як правило, використовують власні фрод-моніторингові системи та впроваджують в систему управління ризик-менеджменту банку спеціальні структурні підрозділи до функцій яких входить [17]:

- формування правил і алгоритмів для розпізнавання і превентивного виявлення шахрайських операцій;
- взаємозв'язків, що описують підозрілі операції;
- аналіз можливого шахрайства на основі першого неплатежу по кредиту;
- розрахунки рівня проблемності кредитних карт;
- централізоване блокування операцій співробітників і точок продажу на основі перевищення заданого прийнятного рівня ризику та ін.

В цілому, фрод-моніторинг в Україні є безсистемним і не являє собою певної комплексної системи. Як правило, функції фрод-моніторингу покладаються на підрозділи IT та служби безпеки або на кваліфікованих фахівців [8, с. 39].

В Україні у 2002 р. введена в експлуатацію міжбанківська система обміну інформацією про шахрайство з платіжними картами в режимі реального часу «Exchange-OnLine» [16]. Нині до системи підключено 84 українських банків і компаній, найбільший банк Молдови — Victoriabank, казахський Цеснабанк й ін.

Таким чином, єдиного методу або засобу захисту від фроду не існує. Банки використовують системи фрод-моніторингу, які основані на різному ступені централізації, комплексності та системності організації таких систем.

На нашу думку, для ефективної протидії шахрайства, організація системи фрод-моніторингу в банку має ґрунтуватись на системі певних принципів:

1. Системності та комплексності. Оцінка шахрайських дій має проводитись із врахуванням можливостей впливу на неї не тільки зовнішніх, а й внутрішніх факторів на основі online і offline протоколів моніторингу.

2. Організованості й безперервності. Фрод-моніторинг повинен здійснюватись спеціальними підрозділами банку на постійній основі.

3. Цілеспрямованості. Завдання фрод-моніторингу мають знаходитись в площині цілей економічної безпеки банку.

4. Легітимності. Процесс моніторингу повинен здійснюватись на основі нормативно-законодавчих документів.

5. Дотримання банківської таємниці. Цей принцип передбачає нерозголошення даних для внутрішньобанківського користування та інформації про клієнтів банку.

6. Об'єктивності. Оцінка несанкціонованих дій інсайдерів та аутсайдерів має проводитись на основі використання затверджених керівництвом методів, методик та протоколів без суб'єктивних суджень.

7. Економічності. Витрати на фрод-моніторинг повинні бути економічно доцільними та відповідати адекватності заходів на досягнення результатів підсилення економічної безпеки банку.

Дотримання наведених принципів необхідно здійснювати в комплексі з організаційно-технічними заходами попередження шахрайства:

- використовувати технологію смс-інформування клієнтів банку;
- застосовувати не формальні, а фактичні стандарти забезпечення безпеки даних;
- впроваджувати спеціальні програмні системи фрод-транзакцій.

Висновки

Отже, дослідивши в статті особливості організації систем фрод-моніторингу в банках, можна зробити висновок, що надійних систем моніторингу, які б надавали гарантований захист від шахрайства сьогодні не існує.

Сфера електронної комерції, електронний банкінг, операції з платіжними картками й інші банківські операції нерозривно пов'язані з різними видами шахрайства. Боротьба з шахрайством здійснюється банківськими установами в різній мірі. Впровадження в діяльність банків систем фрод-моніторингу, їх прогресивність та професіоналізм організації залежить від пріоритетів банку залежно від актуальності фрод-моніторингу в системі управління економічною безпекою. Критеріями прийняття рішень при цьому є обсяги існуючого бізнесу та поточних втрат від шахрайських операцій.

Таким чином, ефективний захист від шахрайства, який дозволить мінімізувати пов'язані з ним ризики можливий лише на основі дотримання ряду принципів організації системи фрод-моніторингу та застосування комплексу організаційно-технічних заходів, основаних на інноваційних методиках та рішеннях дотримання безпеки банківських операцій.

Література

1. Офіційний сайт НБУ [Електронний ресурс]. – Режим доступу: http://www.bank.gov.ua.

2. Brar, T. Vulnerabilities in e-banking: A study of various security aspects in e-banking / International Journal of Computing & Business Research // T. Brar, D. Sharma, S. Khurmi. – 2012. – №6. – P. 127-132.
3. Freixas, X. D. Microeconomics of banking / X. D. Freixas, D. C. Rochet. – Cambridge: The MIT Press, 2008. – 348 p.
4. Hatice, U. Board Composition and Corporate Fraud / U. Hatice, S. Szewczyk, R. Varma // Financial Analysts Journal. – 2004. – №5l. – P. 60-65.
5. Mannan, M. Security and usability: the gap in real-world online banking / M. Mannan // New Security Paradigms and Workshop. – 2008. – №4. – P. 1 – 14.
6. Sinkey, Joseph F. Commercial Bank Financial Management / Joseph F. Sinkey. – New Jersey: Prentice-Hall, Inc. A Pearson Education Company Upper Saddle Rive, 2001. – 696 p.
7. Usman, A. Critical Success Factors for Preventing e-Banking Fraud / A. Usman, M. Shah / Journal of Internet Banking and Commerce. – 2013. – № 18(2). – P. 1 –13.
8. Болгар, Т. М. Удосконалення моніторингу банківського кредитного процесу / Т. М. Болгар. – Академічний огляд. - 2013. – №2(39). – С. 36–42.
9. Мельник, С. І. Організаційно-правове забезпечення системи економічної безпеки банку / С. І. Мельник // Науковий вісник АДУБС. Серія економічна. – 2011. – №1. – С. 199–206.
10. Колодізєв, О. М. Контролінг як технологія управління фінансовими та нефінансовими структурами: монографія / О. М. Колодізєв, І. М. Чмутова, К. М. Азізова, М. В. Максімова. – Х. : Вид. ХНЕУ ім. С. Кузнеця, 2014. – 352 с.
11. Перехрест, Л. М. Забезпечення фінансової безпеки банків в умовах нестабільного економічного середовища : автореф. дис. на здобуття наук, ступеня канд. екон. наук: спец. 08.00.08 «Гроші, фінанси і кредит» / Л. М. Перехрест. - Ірпінь, 2011. - 24 с.
12. Рац, О.М. Дослідження впливу якості кредитного портфелю на ефективність кредитної діяльності банку як складова моніторингу кредитного ризику / О.М. Рац // Технологічний аудит та резерви виробництва. – 2015. – №1/5(21). – С. 41–45.
13. Рац, О. М. Організаційні засади кредитного моніторингу позичальників в системі управління кредитними ризиками банку / О. М. Рац // Науковий вісник Херсонського державного університету. – 2014. – № 5. – С. 117–120.
14. Сніщенко, Р. Г. Фінансова безпека банку: автореферат дис. на здобуття наук, ступеня канд. екон. наук: спец. 08.00.08 «Гроші, фінанси і кредит» / Р. Г. Сніщенко. – Дніпропетровськ, 2011. - 20 с.
15. Штаєр, О. М. Обгрунтування пріоритетності загроз економічної безпеки банку // О. М. Штаєр / Вісник економіки транспорту і промисловості: збірник науково-практичний статей. – Харків: УДАЗТ, 2012. – №39. – С. 99–103.
16. Сайт Української міжбанківської Асоціації членів платіжних систем [Електронний ресурс]. – Режим доступу: http://ema.com.ua.
17. Сайт ПАТ КБ «Приватбанк» [Електронний ресурс]. – Режим доступу: http://www.privatbank.ua.

References

1. Official website of the NBU [Electronic resource]. - Access: http://www.bank.gov.ua.
2. Brar, T. (2012). Vulnerabilities in e-banking: A study of various security aspects in e-banking. International Journal of Computing & Business Research, 6, 127-132.
3. Freixas, X. D., Rochet, D. C.(2008). Microeconomics of banking. Cambridge: The MIT Press, 348.
4. Hatice, U., Szewczyk, S., Varma, R. (2004). Board Composition and Corporate Fraud. Financial Analysts Journal, 5l, 60-65.
5. Mannan, M. (2008). Security and usability: the gap in real-world online banking. New Security Paradigms and Workshop, 4, 1-14.
6. Sinkey, Joseph F. (2001). Commercial Bank Financial Management. New Jersey: Prentice-Hall, Inc. A Pearson Education Company Upper Saddle Rive, 696.
7. Usman, A., Shah, M. (2013). Critical Success Factors for Preventing e-Banking Fraud. Journal of Internet Banking and Commerce, 18(2), 1 –13.
8. Bolhar, T. M. (2013). Improving monitoring of bank credit process. Akademichnyi ohliad, 2 (39), 36–42.
9. Melnik, S. I. (2011). Organizational and legal support systems Economic Security Bank. Naukoviy visnik ADUBS. Economic series, 1, 199-206.
10. Kolodizyev, O. M., Chmutova, I. M., Azizova, K. M., Maksimova M. V. (2010). Controlling the technology of financial and non-financial institutions: monograph, 352.
11. Perehrest, L.M. (2011). Ensuring financial security of banks in an unstable economic environment. Author. dis. on competition sciences degree candidate. econ. sciences specials. 08.00.08 "Money, Finance and Credit", 24.
12. Rats, O. M. (2015). The influence of the quality of the loan portfolio on the effectiveness of bank lending as part of monitoring credit risk. Technology audits and reserves production, 1/5(21), 41-45.
13. Rats, O. M. (2014). Organizational principles of credit monitoring borrowers in the management of credit risk of the bank. Scientific Bulletin of Kherson State University, 5, 117-120.
14. Snischenko, R. G. (2011). Financial Security Bank. Author. dis. on competition sciences degree candidate. econ. sciences specials. 08.00.08 "Money, Finance and Credit, 20.
15. Shtayer, O. M. (2012). Rationale priority threats to the economic security of the bank. Bulletin of Economics and Transport industry: a collection of scientific and practical articles. Kharkov: UDAZT, 39, 99-103.
16. The site of the Ukrainian Interbank Payment Systems Member Association [Electronic resource]. - Access: http://ema.com.ua.
17. Site of PJSC CB "PrivatBank" [Electronic resource]. - Access: http://www.privatbank.ua.

Рецензент: д-р екон. наук, проф. О.М. Колодізєв, Харківський національний економічний університет ім. С. Кузнеця, Харків.

Автор: РАЦ Ольга Миколаївна
Харківський національний економічний університет ім. С. Кузнеця, Харків, кандидат економічних наук, доцент.
E-mail – olrats@ukr.net

ИССЛЕДОВАНИЕ ОСОБЕННОСТЕЙ ОРГАНИЗАЦИИ ФРОД-МОНИТОРИНГА В СИСТЕМЕ УПРАВЛЕНИЯ ЭКОНОМИЧЕСКОЙ БЕЗОПАСНОСТЬЮ БАНКА

О.Н. Рац
Харьковский национальный экономический университет имени Семена Кузнеца

В статье определена сущность фрод-мониторинга как инструмента системы управления экономической безопасностью банка. Исследованы объекты фрод-мониторинга в соответствии с видами мошенничества в банковской деятельности и определены особенности применения мониторинговых систем в зависимости от объекта мошенничества. На основе анализа особенностей организации фрод-мониторинговых систем, предложены принципы организации системы фрод-мониторинга для эффективного противодействия мошенничеству.

***Ключевые слова**: банк, экономическая безопасность банка, мошенничество, фрод-мониторинг, риск-менеджмент банка.*

STUDY OF FEATURES FRAUD-MONITORING IN THE MANAGEMENT OF ECONOMIC SAFETY OF THE BANK

O.M. Rats
Simon Kuznets Kharkiv National University of Economics

The article is devoted to the essence of the fraud-monitoring as a tool of economic security system of the bank. Investigated fraud-monitoring facilities under the fraud in banking. The features of the use of monitoring systems based on the object of fraud: fraud in the provision of loans and the implementation of deposit operations; fraud in the area of remote banking services; fraud in the implementation of payment transactions and banking payment cards. The main indicators, which conducted monitoring of fraud in banks considered in the article. The features of online and offline fraud-monitoring systems. Determined that despite the introduction in Ukraine interbank system of exchanging information on fraud, fraud-monitoring in Ukraine remains systemless. Formulated principles of system fraud-monitoring system. Compliance these principles provide effective fraud prevention in the banking sector.

***Keywords:** bank, economic safety of the bank, fraud, fraud-monitoring, risk management of the bank.*