ДОСЛІДЖЕННЯ ОСОБЛИВОСТЕЙ НЕЗАЛЕЖНОГО АУДИТУ ДЛЯ ПОПЕРЕДЖЕННЯ ШАХРАЙСТВА БАНКІВСЬКОГО ПЕРСОНАЛУ[1]

RESEARCH ON THE FEATURES OF INDEPENDENT AUDIT TO PREVENT FRAUD OF BANKING PERSONNEL

УДК 657.631:336.7
https://doi.org/10.32843/infrastruct37-102

Гриценко К.Г.
к.т.н., доцент,
доцент кафедри економічної кібернетики
Сумський державний університет

Попередити шахрайство банківського персоналу на рівні технологічних засобів або регламентів практично неможливо, тому актуальною є проблема організації системи незалежного аудиту. У разі шахрайства персоналу службі внутрішнього аудиту банку важко забезпечити повну незалежність у діях і неупередженість у судженнях. Особливого значення набуває зовнішній аудит банку, основними характеристиками якого є незалежність і об'єктивність, можливість оцінити ризики шахрайства персоналу та виявити слабкі сторони у функціонуванні системи кібербезпеки банку. Система незалежного аудиту повинна використовувати базу даних шахрайств, заповнену системою фрод-моніторингу банку, а також перевіряти реакцію банку на випадки шахрайства банківського персоналу. Її складовою частиною має бути оцінка ризику шахрайства банківського персоналу. Це створює умови для використання ризик-орієнтованого підходу під час побудови плану аудиту.
Ключові слова: *банківський персонал, попередження шахрайства, фрод-моніторинг, оцінка ризику, незалежний аудит.*

Предупредить мошенничество банковского персонала на уровне технологических средств или регламентов практически невозможно, поэтому актуальной является проблема организации системы независимого аудита. В случае мошенничества персонала службе внутреннего аудита трудно обеспечить полную независимость в действиях и беспристрастность в суждениях. Особое значение приобретает внешний аудит банка, основными характеристиками которого являются независимость и объективность, возможность оценить риски мошенничества персонала и выявить слабые стороны системы кибербезопасности банка. Система независимого аудита должна использовать базу данных, заполненную системой фрод-мониторинга банка, а также проверять реакцию банка на случаи мошенничества персонала. Ее частью должна быть оценка риска мошенничества персонала, что создает условия для применения риск-ориентированного подхода при построении плана аудита.
Ключевые слова: *банковский персонал, предупреждение мошенничества, фрод-мониторинг, оценка риска, независимый аудит.*

Banking frauds are global and causes the most financial losses in the world. It is almost impossible to warn them at the level of intra-bank technological means or regulations. In this regard, the problem of organizing an independent audit system is urgent. Independent audit is an important element of counteracting fraud carried out by bank personnel. In the case of personnel fraud, it is extremely difficult for the internal audit service of the bank to ensure full independence in actions and impartiality in judgment, so external audit of the bank by independent experts is of importance. The main characteristics of an external audit are independence and objectivity, the ability to assess the risks of fraud by banking personnel, weaknesses in the functioning of the bank's cybersecurity system. In the course of an external audit, it is advisable to evaluate the effectiveness of the bank's cybersecurity system towards reducing the risk of bank personnel fraud. The system of independent audit should use the fraud database, filled in by the bank's fraud-monitoring system, as well as check the response of the relevant units of the bank to cases of fraud by banking personnel. The purpose of the bank's fraud-monitoring system is to prevent credit fraud, deposit fraud, remote banking fraud, bank card fraud, payment fraud, fraud related to fraudulent personnel activity. An integral part of an independent audit system should be the assessment of risk of fraud by banking personnel. This creates the conditions for using a risk-oriented approach when building an audit plan. Typical fraudulent actions of management and bank employees include misappropriation of assets and fraudulent financial statements. To detect fraudulent financial statements in the banking sector, neural networks are widely used that can handle tasks without an algorithmic solution; Bayesian networks used to detect anomalies; genetic algorithms used for binary classification; text mining, which is used for clustering and anomaly detection. The current trend of detecting and preventing fraud is to use hybrid methods that use the strengths of different methods.
Key words: *banking personnel, fraud prevention, fraud monitoring, risk assessment, independent audit.*

Постановка проблеми. Згідно зі звітом Асоціації сертифікованих фахівців із розслідування шахрайства [1], у 2018 році шахрайства нанесли організаціям у всьому світі фінансових збитків на загальну суму понад 7 млрд. доларів США. Згідно з цим звітом найбільша кількість випадків шахрайства у фінансовому секторі фіксується в банках, причому кількість виявлених випадків шахрайства за участі банківського персоналу набагато перевищує кількість випадків зовнішнього шахрайства. На жаль, попередити шахрайство банківського персоналу на рівні внутрішньобанківських технологічних засобів або регламентів сьогодні практично неможливо [2]. У зв'язку з цим надзвичайно актуальною та практично значущою є проблема організації системи незалежного аудиту для попередження шахрайства банківського персоналу.

Аналіз останніх досліджень і публікацій. Проблемі виявлення та попередження шахрайств, що здійснюються персоналом банку, присвячено багато праць вітчизняних і зарубіжних науковців та практиків. Окремим аспектам цієї проблеми приділяють увагу у своїх працях Б.Ф. Усач, М.А. Маркевич [3], Т.М. Болгар [4], О.М. Рац [5], Г.М. Яровенко [6], О. Мовчан, М. Вольська [7], К. Сомунале, Р. Роснер, Т. Сехтон (*Comunale C., Rosner R., Sexton T.*) [8], М. Крамбіа-Капардіс (*Krambia-Kapardis M.*) [9] та інші. Проте аналіз наукових праць показав недо-

[1] Робота виконана в рамках держбюджетної науково-дослідної роботи № 0118U003574 «Кібербезпека в боротьбі з банківськими шахрайствами: захист споживачів фінансових послуг та зростання фінансово-економічної безпеки України»

статність вивчення цієї проблематики стосовно особливостей проведення незалежного аудиту для попередження шахрайства банківського персоналу. Це зумовлює необхідність подальших досліджень у цьому напрямі.

Постановка завдання. Мета статті полягає в дослідженні особливостей незалежного аудиту для попередження шахрайства банківського персоналу. Основними завданнями, що сприяють досягненню поставленої мети, є: розгляд методів оцінювання стану кібербезпеки банку, розгляд особливостей виявлення шахрайства персоналу в банках, обґрунтування необхідності застосування зовнішнього аудиту для попередження шахрайства банківського персоналу.

Виклад основного матеріалу дослідження. У роботі [10] внутрішній аудит кібербезпеки банку розглядається як система збору та аналізу інформації для визначення рівня захищеності об'єктів внутрішнього аудиту – інформаційних активів та інформаційної інфраструктури, а також збереження властивостей інформаційних активів (доступності, цілісності та конфіденційності). Його метою є визначення відповідності системи кібербезпеки банку стратегії та цілям діяльності банку, а завданнями – надання доказів відповідності системи кібербезпеки політиці банку, вивчення гарантій системи кібербезпеки та операційного середовища тощо.

Ми вважаємо, що система кібербезпеки банку повинна відповідати міжнародному стандарту ISO/IEC 27001 «Управління інформаційною безпекою» [11], який містить специфікації щодо обов'язкових політик безпеки, яких слід дотримуватися банку, а також документацію щодо процесів та процедур, які повинні застосовуватися в банку на постійній основі. Внутрішній аудит кібербезпеки банку повинен визначити ступінь відповідності банку вимогам стандарту ISO/IEC 27001 «Управління інформаційною безпекою», а також базовий рівень кібербезпеки для подальшого вдосконалення системи кібербезпеки банку. Для цього внутрішній аудит кібербезпеки банку повинен використовувати відповідні методи оцінювання поточної ситуації в сфері кібербезпеки банку, необхідні для прийняття обґрунтованих управлінських рішень [12].

Метод аналізу розривів може бути використаний аудитором у сфері кібербезпеки для оцінки того, наскільки банк дотримується вимог кібербезпеки. Отриманий у результаті аналізу розривів аудиторський звіт містить сфери діяльності банку, в яких вимоги кібербезпеки успішно виконуються, а також рекомендації щодо задоволення вимог кібербезпеки, що не виконуються.

Метод оцінки ризику може бути використаний для оцінювання рівня потенційного ризику кібершахрайства в розрізі персоналу, банківських процесів і технологій, а також впливу, який він може мати на функціонування банку. Цей метод дає змогу отримати відповідь на питання, наскільки ефективно система кібербезпеки банку зменшує ризики кібершахрайства, а також наскільки захищеними є інформаційні активи та інформаційна інфраструктура банку.

Як зазначено в роботі [3], у разі шахрайства персоналу службі внутрішнього аудиту банку важко забезпечити повну незалежність у діях і неупередженість у судженнях, тому особливого значення набуває зовнішній аудит банку незалежними експертами, що є поширеною практикою в іноземних банках. До того ж у Міжнародному стандарті професійної практики внутрішнього аудиту 1200 «Професійна компетентність та належна ретельність» зазначено, що «внутрішні аудитори повинні мати достатні знання для того, щоб оцінити ризик шахрайства та спосіб управління таким ризиком в організації, але не передбачається, що внутрішній аудитор повинен володіти такою ж компетенцією, що й особа, основним обов'язком якої є виявлення та розслідування фактів шахрайства» [13]. Основними характеристиками зовнішнього аудиту є:

1) незалежність і об'єктивність (незаангажованість у судженнях);

2) вдосконалення системи кібербезпеки банку, що передбачає можливість оцінити ризики шахрайства банківського персоналу, слабкі сторони системи кібербезпеки банку та дати рекомендації, спрямовані на підвищення ефективності системи кібербезпеки банку.

Залучені незалежні експерти, що спеціалізуються на виявленні шахрайства в банку, часто використовують системи фрод-моніторингу інформації, отриманої банком під час ведення бізнесу [4]. Метою фрод-моніторингу в банку згідно з [5] є попередження шахрайства під час надання кредитів, шахрайства під час здійснення депозитних операцій, шахрайства у сфері дистанційного банківського обслуговування, шахрайства з банківськими платіжними картками, шахрайства під час здійснення розрахункових операцій, шахрайства, пов'язаного з неправомірними діями персоналу тощо. У роботі [6] наведено перелік об'єктів, які, на думку автора, доцільно перевіряти системою фрод-моніторингу:

– активність рахунку, коли персонал у власних цілях використовує «сплячі рахунки»;

– власники рахунків, якщо власник присутній у «чорному списку» або є іноземцем, померлим тощо;

– ліміти за операціями, що здійснюються згідно з вимогами Національного банку України, політикою банку, посадовими інструкціями тощо, в результаті чого виявляються надлишки за лімітами;

– активність банківських співробітників на предмет дотримання банківських нормативів,

які співробітник може перевищувати чи недовиконувати;

– операції працівників на відповідність належним їм правам доступу;

– операції працівників на відповідність політиці безпеки банку.

Результати роботи системи фрод-моніторингу накопичуються в базі даних шахрайств, обробляються та надсилаються відповідним підрозділам банку. Це дає змогу більш ніж на 50% знизити фінансові збитки від шахрайства персоналу [1]. Як зазначено в роботі [4], виявлення аномалій поведінки співробітників банку є приводом для додаткової перевірки діяльності цих співробітників. Ми вважаємо, що у процесі зовнішнього аудиту доцільно оцінювати ефективність системи кібербезпеки банку в напрямі зменшення ризику шахрайства персоналу банку.

Згідно з Положенням з міжнародної практики аудиту 1006 «Аудит фінансових звітів банку» типові шахрайські дії управлінського персоналу та працівників банку включають у себе [3]:

1) незаконне привласнення активів:

– депозитні операції: маскування вкладів; невідображення депозитів у обліку; крадіжка депозитів клієнтів; неправильне визначення відсотків за вкладами;

– кредитні операції: надання кредиту на підроблені чи незаконно отримані документи; позики фіктивним позичальникам; продаж заставного майна за ціною, що нижча за ринкову; підкупи для отримання звільнення від застави чи для зменшення суми позову; не подання інформації про заставне майно для внесення її у державні реєстри обтяжень; завищення вартості активів, що оцінюються з метою передачі у заставу для отримання кредиту; помилки у визначенні фінансового стану та класу позичальника;

– поточні рахунки: незаконне привласнення коштів із рахунків, за якими часто проводяться транзакції;

2) неправдиве відображення фінансової звітності:

– навмисні викривлення;

– пропуск загальних сум;

– виправлення облікових записів;

– некоректне відображення позик на рахунках простроченої чи строкової заборгованості.

Як показано на рис. 1, найбільше збитків у світі в 2018 році було заподіяно через такі типи шахрайства персоналу, як [1]: неправдиве відображення фінансової звітності (10% випадків), корупція (38% випадків), незаконне привласнення активів (89% випадків).

Таким чином, для попередження шахрайств банківського персоналу складовою частиною системи незалежного аудиту має бути оцінювання ризику шахрайства персоналу в напрямах неправдивого відображення фінансової звітності та незаконного привласнення активів. Це створює умови для використання ризик-орієнтованого підходу під час побудови плану аудиту. У роботі [14] наведена нечітко-множинна модель, побудована на основі індикаторів ризику шахрайства персоналу, наведених, наприклад, у [7], яка надає системі незалежного аудиту можливість оцінити ризик шахрайства банківського персоналу та визначити основні сфери, що найбільше сприяють шахрайству. На нашу думку, система незалежного аудиту для попередження шахрайств банківського персоналу повинна використовувати базу даних, заповнену системою фрод-моніторингу, а також перевіряти реакцію відповідних підрозділів банку на випадки шахрайств банківського персоналу.

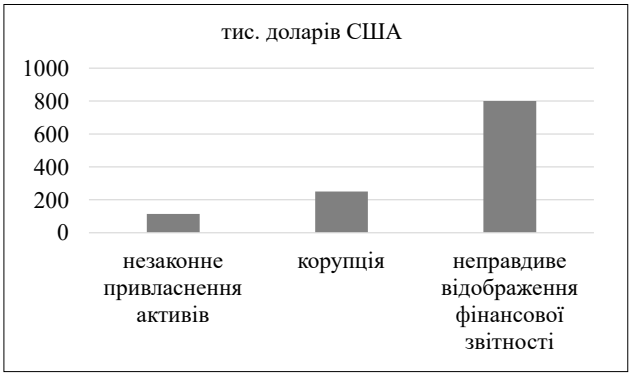

Рис. 1. Медіана фінансових збитків за типами шахрайства персоналу

У роботі [15] зазначається, що для виявлення викривлень фінансової звітності в банківській сфері широко застосовуються нейронні мережі, які здатні впоратися із задачами без алгоритмічного рішення; байєсові мережі, що використовуються для виявлення аномалій; генетичні алгоритми, які використовуються для бінарної класифікації; текст майнінг (text mining), який використовується для кластеризації та виявлення аномалій. Сучасною тенденцією виявлення та попередження шахрайства є використання гібридних методів, які використовують сильні сторони різних методів.

На нашу думку, для виявлення шахрайства персоналу у процесі незалежного аудиту доцільно також використовувати так звані «золоті правила» аудитора, що вимагають від нього [16]:

– намагатися з'ясувати причину відхилень;

– не розглядати питання довіри до людей тільки залежно від їхнього становища в суспільстві;

– не припускатися думки, що шахрайство неможливе на цьому підприємстві;

– відчувати особисту відповідальність за виявлення шахрайства;

– у разі виявлення потенційних проблем посилити контроль з метою зниження ризику;

– знати ситуації, що супроводжуються значним ризиком шахрайства, та їх ознаки.

Висновки з проведеного дослідження. Отже, за результатами проведеного дослідження можна зробити такі висновки та рекомендації. Підтверджено, що незалежний аудит є важливим елементом протидії шахрайству, яке здійснюється персоналом банку. Він оцінює ефективність системи кібербезпеки банку з погляду зменшення ризику шахрайства персоналу банку. Встановлено, що в системі незалежного аудиту доцільно використовувати сучасні методи виявлення та попередження шахрайства персоналу. До них належить стандарт ISO/IEC 27001 «Управління інформаційною безпекою», метод аналізу розривів, метод оцінки ризиків, система фрод-моніторингу тощо. Своєчасне проведення заходів зовнішнього аудиту з використанням цих методів дає змогу знизити рівень шахрайства та підвищити відповідальність банківського персоналу. Особливо перспективним є ризик-орієнтований підхід, на основі якого доцільно складати план аудиту. Він використовує модель оцінки ризику, побудовану на основі індикаторів ризику шахрайства персоналу, та дає можливість визначити сфери, які найбільше сприяють шахрайству банківського персоналу.

БІБЛІОГРАФІЧНИЙ СПИСОК:

1. 2018 Report to the nations on occupational fraud and abuse, Association of Certified Fraud Examiners (ACFE). URL: https://s3-us-west-2.amazonaws.com/acfepublic/2018-report-to-the-nations.pdf (дата звернення: 29.11.2019).

2. Спритність рук: топ-схеми шахрайства в банках. *Financial club*. URL: https://finclub.net/ua/priama-mova/sprytnist-ruk-topskhemy-shakhraistva-v-bankakh.html (дата звернення: 29.11.2019).

3. Усач Б.Ф., Маркевич М.А. Виявлення фактів шахрайства у контексті аудиту фінансових звітів банків. *Вісник Житомирського державного технологічного університету. Серія «Економічні науки»*. 2010. № 3 (53). С. 253–255.

4. Болгар Т.М. Удосконалення моніторингу банківського кредитного процесу. *Академічний огляд*. 2013. № 2 (39). С. 36–42.

5. Рац О.М. Дослідження особливостей організації фрод-моніторингу в системі управління економічною безпекою банку. *Комунальне господарство міст*. 2016. Випуск 127. С. 33–38.

6. Яровенко Г.М. Розробка інформаційної моделі виявлення ознак шахрайства у банках. *Інвестиції: практика та досвід*. 2018. № 14. С. 23–28.

7. Мовчан О., Вольська М. Шахрайство, як один з найбільших ризиків, або як не проґавити головну проблему під час проведення внутрішнього аудиту. URL: https://www.iia.org.ua/wp-content/uploads/2017/04/Fraud-as-one-of-biggest-rist.pdf (дата звернення: 29.11.2019).

8. Christie L. Comunale, Rebecca L. Rosner, Thomas R. Sexton. The Auditor's Assessment of Fraud Risk: A Fuzzy Logic Approach. *Journal of Forensic & Investigative Accounting*. 2010. Vol. 2, Issue 3, Special Issue. P. 95–140.

9. Krambia-Kapardis M. A fraud detection model: a must for auditors. *Journal of Financial Regulation and Compliance*. 2002. Vol. 10, no. 3. P. 266–278. DOI: 10.1108/13581980210810256.

10. Криклій О.А., Павленко Л.Д. Внутрішній аудит як превентивна складова в системі кібербезпеки банку. *Облік і фінанси*. 2019. № 2 (84). С. 124–133.

11. Стандарт ISO/IEC 27001:2013. URL: https://intercert.com.ua/articles/posts/292-standart-iso-iec-27001-2013 (дата звернення: 29.11.2019).

12. Monique Magalhaes. Cybersecurity assessments and audits: everything you need to know. URL: http://techgenix.com/cybersecurity-assessments-and-audits/ (дата звернення: 29.11.2019).

13. Міжнародні стандарти професійної практики внутрішнього аудиту. URL: https://na.theiia.org/translations/PublicDocuments/IPPF-Standards-2017-Ukrainian.pdf (дата звернення: 29.11.2019).

14. Гриценко К.Г. Нечітко-множинний метод оцінки рівня ризику шахрайства банківського персоналу. *Приазовський економічний вісник*. 2019. № 3 (14). С. 451–456. URL: http://pev.kpu.zp.ua/vypusk-14 (дата звернення: 29.11.2019).

15. Гриценко К.Г. Аналіз методів виявлення шахрайств у банках, що здійснюються персоналом банку. *Інфраструктура ринку*. 2019. Випуск 34. С. 333–337. URL: http://www.market-infr.od.ua/uk/34-2019 (дата звернення: 29.11.2019).

16. Гутцайт Е.М. Аудит: концепция, проблемы, эффективность, стандарты. Москва: ЭЛИТ 2000; ЮНИТИ ДАНА. 2002.

REFERENCES:

1. 2018 Report to the nations on occupational fraud and abuse, Association of Certified Fraud Examiners (ACFE). Available at: https://s3-us-west-2.amazonaws.com/acfepublic/2018-report-to-the-nations.pdf (accessed 29 November 2019).

2. Sprytnist ruk: top-skhemy shakhraistva v bankakh [Dexterity of the hands: top schemes of bank fraud]. *Financial club*. Available at: https://finclub.net/ua/priama-mova/sprytnist-ruk-topskhemy-shakhraistva-v-bankakh.html (accessed 29 November 2019).

3. Usach B. F., Markevych M. A. (2010) Vyiavlennia faktiv shakhraistva u konteksti audytu finansovykh zvitiv bankiv [Detecting fraud in the context of auditing banks' financial statements]. *Visnyk Zhytomyrskoho derzhavnoho tekhnolohichnoho universytetu. Seriia "Ekonomichni nauky"*, no. 3 (53), pp. 253-255.

4. Bolhar T. M. (2013) Udoskonalennia monitorynhu bankivskoho kredytnoho protsesu [Improvment the monitoring of the banking credit process]. *Akademichnyi ohliad*, no. 2 (39), pp. 36–42.

5. Rats O. M. (2016) Doslidzhennia osoblyvostei orhanizatsii frod-monitorynhu v systemi upravlinnia ekonomichnoiu bezpekoiu banku [Investigation of peculiarities of organization of fraud-monitoring in the system of management of economic security of the bank]. *Komunalne hospodarstvo mist*, issue 127. pp. 33-37.

6. Yarovenko H. M. (2018) Rozrobka informatsiinoi modeli vyiavlennia oznak shakhraistva u bankakh [Development of the information model for detection

fraud signs in the banks]. *Investytsii: praktyka ta dosvid*, no. 14, pp. 23–28.

7. Movchan O., Volska M. Shakhraistvo, yak odyn z naibilshykh ryzykiv, abo yak ne progavyty holovnu problemu pid chas provedennia vnutrishnoho audytu [Fraud as one of the biggest risks, or how not to miss the main issue during an internal audit]. Available at: https://www.iia.org.ua/wp-content/uploads/2017/04/Fraud-as-one-of-biggest-rist.pdf (accessed 29 November 2019).

8. Christie L. Comunale, Rebecca L. Rosner, Thomas R. Sexton (2010) The auditor's assessment of fraud risk: a fuzzy logic approach. *Journal of forensic & investigative accounting*, vol. 2, issue 3, special issue. P. 95–140.

9. Krambia-Kapardis M. (2002) A fraud detection model: a must for auditors. *Journal of financial regulation and compliance*, vol. 10, no. 3, pp. 266–278. DOI: 10.1108/13581980210810256.

10. Kryklii O. A., Pavlenko L. D. (2019) Vnutrishnii audyt yak preventyvna skladova v systemi kiberbezpeky banku [Internal audit as a preventive component in the bank's cybersecurity system]. *Accounting and finance*, no. 2 (84), pp. 124-133.

11. Standard ISO/IEC 27001:2013. Available at: https://intercert.com.ua/articles/posts/292-standart-iso-iec-27001-2013 (accessed 29 November 2019).

12. Monique Magalhaes. Cybersecurity assessments and audits: everything you need to know. Available at: http://techgenix.com/cybersecurity-assessments-and-audits (accessed 29 November 2019).

13. Mizhnarodni standarty profesiinoi praktyky vnutrishnoho audytu [International standards for the professional practice of internal auditing]. Available at: https://na.theiia.org/translations/PublicDocuments/IPPF-Standards-2017-Ukrainian.pdf (accessed 29 November 2019).

14. Gritsenko K. H. (2019) Nechitko-mnozhynnyi metod otsinky rivnia ryzyku shakhraistva bankivskoho personalu [Fuzzy method of fraud assessment of bank personnel]. *Pryazovskyi ekonomichnyi visnyk*, no. 3 (14), pp. 451–456. Available at: http://pev.kpu.zp.ua/vypusk-14 (accessed 29 November 2019).

15. Gritsenko K. H. (2019) Analiz metodiv vyiavlennia shakhraistv u bankakh, shcho zdiisniuiutsia personalom banku [Analysis of methods of fraud detection of bank personnel]. *Infrastruktura rynku*, issue 34. pp. 333–337. Available at: http://www.market-infr.od.ua/uk/34-2019 (accessed 29 November 2019).

16. Guttsayt E.M. (2002) *Audit: kontseptsiya, problemy, effektivnost', standarty* [Audit: concept, problems, efficiency, standards]. Moscow: ELIT; UNITY DANA. (in Russian)

Gritsenko Konstantin
Candidate of Technical Sciences, Associate Professor,
Senior Lecturer at Department of Economic Cybernetics
Sumy State University

RESEARCH ON THE FEATURES OF INDEPENDENT AUDIT TO PREVENT FRAUD OF BANKING PERSONNEL

The purpose of the article. The purpose of the article is to investigate the features of an independent audit to prevent fraud of banking personnel. The main tasks that should contribute to the achievement of this goal are: consideration of modern methods of assessing the state of cyber security of the bank, consideration of the features of detection of fraud personnel in banks, justification of the need for external audit to prevent fraud of banking personnel.

Methodology. In this study, we have used systematization and comparative analysis. Gap analysis and risk assessment are used to assess the state of bank's cybersecurity. This creates conditions for using a risk-oriented approach when building an audit plan. The mathematical apparatus (neural networks, Bayesian networks, genetic algorithms, text mining) used in the economic-mathematical methods to identify fraudulent financial statements in the banking sector also was considered.

Results. It is shown that the internal cybersecurity audit of the bank should reveal the degree of compliance of the bank with the requirements of ISO/IEC 27001 "Information Security Management", as well as the basic level of cybersecurity for further improvement of the bank's cybersecurity system. It is shown that it is extremely difficult for the internal audit service of the bank to ensure full independence in actions and impartiality in judgments therefore external audit of the bank by independent experts is of importance. In the course of external audit, it is advisable to evaluate the effectiveness of the bank's cybersecurity system, in particular in the direction of reducing the risk of bank personnel fraud. It is revealed that an integral part of the system of independent auditing for the prevention of bank fraud is to assess the risk of fraud of banking personnel in the areas of misappropriation of assets and fraudulent financial statements. It is shown that, based on personnel' fraud risk indicators, an independent audit system can assess the risk of fraud by banking personnel and identify the main areas that are most conductive to fraud. Hybrid methods that use the strengths of different economic-mathematical approaches are best for identifying bank personnel fraud.

Practical implications. The author believes that timely conduct of external audit activities using the proposed approaches (gap analysis, risk assessment, fraud monitoring system and risk-oriented approach when building an audit plan) will reduce fraud and increase the responsibility of bank personnel.

Value/originality. The world's largest financial losses have been caused by fraud of personnel: fraudulent financial statements, corruption and misappropriation of assets. In our work, we considered a very significant issue of prevention of bank personnel' frauds. Independent audit is an important element of counteracting fraud of bank personnel. Unfortunately, there is currently no researches on the features of independent audit to prevent fraud of banking personnel. We have analyzed main features of independent audit to prevent fraud of banking personnel and have proposed ways to improve it.