УДК 336.71
DOI 10.52575/2687-0932-2024-51-2-393-401

Внутренний аудит в системе обеспечения кибербезопасности коммерческого банка

Мусацкая Я.С.
Донецкий национальный университет экономики и торговли имени Михаила Туган-Барановского
Россия, 283015, Донецкая Народная Республика, г. Донецк, ул. 50-летия СССР, д. 157
E-mail: yana.musatskaya@mail.ru

Аннотация. В статье исследован механизм внутреннего аудита в системе обеспечения кибербезопасности коммерческого банка. Рассмотрены способы реализации угроз кибербезопасности банка на различных уровнях. Обоснована взаимосвязь субъектов кибербезопасности и службы внутреннего аудита банка. Обосновано, что механизм внутреннего аудита в системе обеспечения кибербезопасности коммерческого банка должен функционировать на основе системы принципов: основополагающих, методологических и специфических. Проведен сравнительный анализ экономико-математических методов выявления мошенничеств в банках, осуществляемых персоналом банка.

Ключевые слова: киберугроза, мошенничество, киберэкосистема, мониторинг, операционные процессы, уровень кибербезопасности

Для цитирования: Мусацкая Я.С. 2024. Внутренний аудит в системе обеспечения кибербезопасности коммерческого банка. Экономика. Информатика, 51(2): 393–401. DOI 10.52575/2687-0932-2024-51-2-393-401

Internal Audit in the Cybersecurity System of a Commercial Bank

Yana S. Musatskaya
Donetsk National University of Economics and Trade named after Mikhail Tugan-Baranovsky
157 50 years of the USSR St., Donetsk, Donetsk People's Republic, 283015, Russia
E-mail: yana.musatskaya@mail.ru

Abstract. The article examines the mechanism of internal audit in the cybersecurity system of a commercial bank. Ways to implement threats to the bank's cybersecurity at various levels are considered. The relationship between cybersecurity entities and the bank's internal audit service is substantiated. The article also proves that the internal audit mechanism in the cybersecurity system of a commercial bank should function on the basis of a system of principles: fundamental, methodological and specific. A comparative analysis of economic and mathematical methods for detecting fraud in banks carried out by the bank's staff is carried out.

Keywords: cyber threat, fraud, cyber ecosystem, monitoring, operational processes, cybersecurity level

For citation: Musatskaya Ya.S. 2024. Internal Audit in the Cybersecurity System of a Commercial Bank. Economics. Information technologies, 51(2): 393–401 (in Russian). DOI 10.52575/2687-0932-2024-51-2-393-401

Введение

Сектор банковских и финансовых услуг является наиболее привлекательным для кибератак и кибермошенничества из-за возможности получения злоумышленниками значительных финансовых и нефинансовых выгод.

Проблема усугубляется тем, что банковские информационные системы становятся все более взаимосвязанными, операционные процессы – более автоматизированными, при этом уже имеющаяся инфраструктура информационных и коммуникационных технологий не была разработана с приоритетом кибербезопасности, что требует ее адаптации к новым условиям деятельности.

Имея это в виду, формирование мер по предотвращению возникновения ситуаций, классифицируемых как киберугроза или мошенничество, является важной научной и прикладной задачей. При этом актуальным для банков является создание превентивной системы обеспечения кибербезопасности, одним из важных элементов которой является внутренний аудит.

Следует отметить, что подавляющее большинство исследований учитывают специфику банковских систем и угроз кибербезопасности, присущих конкретным странам и регионам. Поэтому полученные научные результаты могут лишь частично быть учтены при формировании системы внутреннего аудита для предотвращения угроз потери кибербезопасности в отечественных банках.

Комплексные теоретические разработки, обосновывающие систему внутреннего аудита кибербезопасности как превентивную составляющую в системе кибербезопасности банка, в научной литературе практически отсутствуют.

Внимание ученых, в основном, сосредотачивается на отдельных объектах системы обеспечения кибербезопасности банка. Так, одни исследователи [Скареднова, Скареднов, 2022; Султанов, 2020; Knezevic, Živković, Milojević, 2021; Patricia, 2022] рассматривают аудит информационной безопасности банка при работе с электронными деньгами. Основное внимание акцентируется на ключевых направлениях проверки, в частности, организационно-технической и правовой обеспеченности банков для предотвращения угроз стабильного функционирования систем электронных денег. Кроме того, исследуются методы социальной инженерии и способы предупреждения этого типа угроз кибербезопасности. Другие исследователи [Власова, Шишлянников, 2020; Курныкина, 2020; Alharbi M, 2017] сформировали методологию аудита электронных денег в банках как составляющей системы контроля информационной безопасности. При этом следует отметить необходимость дальнейшего углубления этих теоретических исследований с учетом специфики деятельности российских банков.

Исходя из вышеуказанного, есть необходимость в разработке теоретико-методических основ системы внутреннего аудита кибербезопасности банка, с детализацией ее составляющих и научном обосновании принципов функционирования, на основе чего можно было бы решать задачи обеспечения эффективного контроля кибербезопасности.

Учитывая рост внешних и внутренних угроз, влияющих на уровень кибербезопасности банков России, есть необходимость развития системы внутреннего аудита как превентивной составляющей в системе кибербезопасности. Парадигма превентивности реализуется на основе независимой и объективной оценки текущего уровня защищенности банка от внешних и внутренних киберугроз, разработки рекомендаций по устранению выявленных недостатков в системе обеспечения кибербезопасности и мониторинга их своевременного внедрения.

Объекты и методы исследования

Внутренний аудит кибербезопасности банка можно рассматривать как систему сбора и оценки информации для определения того, обеспечивают ли все системы банка надлежащее состояние защищенности информационных активов и информационной инфраструктуры, сохранение свойств информационных активов (доступности, целостности или конфиденциальности) на целевом уровне в соответствии с установленными критериями.

Перечень способов реализации угроз кибербезопасности банка, на которых должен концентрироваться аудит, приведен в табл. 1.

Ввиду увеличения количества операционных процессов, в том числе ключевых, передаваемых сторонним организациям (например, интернет-провайдеры, подрядчики, осуществляющие монтаж оборудования), растет зависимость банков от кибербезопасности этих сторон. В ответ на это в банке должна быть предусмотрена возможность аудита кибербезопасности сторонних организаций для обеспечения того, чтобы их деятельность соответствовала установленным стандартам и не создавала угрозы потери кибербезопасности.

Таблица 1
Table 1

Перечень способов реализации угроз кибербезопасности банка
List of ways to implement threats to the bank's cybersecurity

Уровень кибербезопасности	Способы реализации угроз
Физический уровень	- утечка информации; - уничтожение / разрушение / диверсии; - несанкционированный физический доступ; - хищение / кража.
Сетевой уровень	- атаки «отказ в обслуживании»; - внедрение аппаратных угроз; - подмена доверенного объекта сети и передача по каналам связи; сообщений от его имени с присвоением его прав доступа; - нарушение штатных режимов работы сетевого оборудования.
Уровень сетевых приложений и сервисов	- анализ трафика; - использование специализированных программ; - внедрение вредоносного ПО; - нарушение штатных режимов работы сетевых приложений; - сканирование сети, направленное на обнаружение открытых портов и служб, открытых соединений.
Уровень операционных систем и систем управления базами данных	- копирование; - кража / потеря паролей; - модификация / удаление данных; - неправильная (неполная) конфигурация систем защиты информации; - несанкционированный логический доступ к операционным системам / системам управления базами данных с использованием специализированного программного обеспечения; - подмена идентификаторов пользователя; - распространение вредоносных программ.
Уровень банковских технологических процессов и программ	- модификация / удаление данных; - распространение / передача данных; - печать документов; - кража документов и карточек; - кража паролей.
Уровень бизнес-процессов	- саботаж; - халатность и ошибки; - вредительство.

Источник: составлено автором на основе [Битов, Жуков, 2022; Михайлова, 2020; Сипратов, 2022]
Source: compiled by the author on the basis of [Битов, Жуков, 2022; Михайлова, 2020; Сипратов, 2022]

Результаты и их обсуждение

К реализации задач внутреннего аудита кибербезопасности приобщается служба внутреннего аудита банка. Аудит также может быть проведен путем привлечения юридических/физических лиц с надлежащим уровнем компетенции и опыта (аутсорсинг).

На рис. 1 схематически представлена взаимосвязь субъектов кибербезопасности и службы внутреннего аудита банка.

Таким образом, внутренний аудит кибербезопасности направлен на оценку соответствия системы кибербезопасности банка стратегии и целям деятельности банка на рынке в текущих условиях киберэкосистемы. Для достижения поставленной цели следует выполнить значительное количество разнонаправленных задач (рис. 2).

Рис. 1. Организационно-управленческая подсистема обеспечения кибербезопасности коммерческого банка на основе внутреннего аудита
Fig. 1. Organizational and managerial subsystem for ensuring the bank's cybersecurity based on internal audit
Источник: составлено автором
Source: compiled by the author

Рис. 2. Задачи системы внутреннего аудита в системе обеспечения кибербезопасности коммерческого банка
Fig. 2. Tasks of the internal audit system in the cybersecurity system of a commercial bank
Источник: составлено автором на основе [Архангельская, 2019; Карпунин, Ефремова, 2020; Simpson, 2022]
Source: compiled by the author on the basis of [Архангельская, 2019; Карпунин, Ефремова, 2020; Simpson, 2022]

Эффективность достижения этих задач можно обеспечить в результате формирования и регулярной модернизации механизма внутреннего аудита кибербезопасности.

Этот механизм должен функционировать на основе системы принципов внутреннего аудита. При этом общие принципы внутреннего аудита остаются важными. При структуризации принципов считаем целесообразным выделять:

- основополагающие принципы, отражающие сущность внутреннего аудита как общественного явления (теоретическая составляющая): независимость; объективность; системность; комплексность; компетентность; эффективность;

- методологические принципы, являющиеся основой его практики:

1) принципы профессиональной этики: честность; объективность; конфиденциальность; профессиональная компетентность;

2) принципы организации: систематичность; оперативность; планирование; сбалансированность; документация; коммуникация.

Помимо приведенных выше принципов, целесообразно учитывать также более специфические принципы, ориентированные на аудит в системе обеспечения кибербезопасности банка:

- актуальность: соответствие механизма внутреннего аудита действующей нормативно-правовой базе, международным рекомендациям и стандартам и киберэкосистеме;

- полнота: аудит должен охватывать все объекты и сферы аудита кибербезопасности, учитывать все угрозы и факторы, которые могут повлиять на эффективность механизма обеспечения кибербезопасности банка;

- надежность: имеющиеся подсистемы механизма внутреннего аудита позволяют сделать последовательную оценку киберрисков или измерения объекта аудита и обосновать аудиторские выводы;

- периодичность в соответствии с целями внутреннего аудита: эффективная система внутреннего аудита должна предусматривать возможность проведения предварительного, регулярного, случайного и ночного (нерабочего) аудита.

Важную роль в системе внутреннего аудита системы обеспечения кибербезопасности банка играет предупреждение мошенничества со стороны персонала. Для предупреждения мошенничеств банковского персонала составной частью системы независимого аудита должна быть оценка риска мошенничества персонала в направлениях ложного отражения финансовой отчетности и незаконного присвоения активов. Это создает условия для использования риск-ориентированного подхода при построении плана аудита.

По нашему мнению, система независимого аудита для предупреждения мошенничеств банковского персонала должна использовать базу данных, заполненную системой фрод-мониторинга, а также проверять реакцию соответствующих подразделений банка на случаи мошенничеств банковского персонала.

Проанализируем экономико-математические методы, которые могут быть использованы для выявления мошенничеств персонала в банковской сфере. Наиболее распространенными видами мошенничества в банках являются отмывание денег, мошенничества с кредитами и незаконное присвоение активов [Журавлёва, 2023]. Первой причиной совершения мошенничества являются финансовые трудности мошенника. Второй – существование возможности для совершения мошенничества. Третьей – уверенность мошенника в существовании веских причин для совершения им мошеннических действий.

Львиная доля банковских мошенничеств происходит с кредитными картами. Известно, что мошенничество с кредитными картами включает незаконное использование кредитной карты или ее информации без ведома владельца. Сегодня для выявления таких мошенничеств широко применяются: логистическая регрессия, которая способна решать категориальные классификационные задачи; метод опорных векторов (SVM, Support Vector Machine), который способен обрабатывать несбалансированные данные и сложные связи между переменными; удобные в использовании деревья решений; случайный лес (random forest);

самоорганизующиеся карты Кохонена (SOM, Self-Organizing Map), используемые для классификации и кластеризации; нечеткая логика, повышающая эффективность управленческих решений [Лазарева, 2022].

В свою очередь для выявления искажений финансовой отчетности в банковской сфере широко применяются: нейронные сети, которые способны справиться с задачами без алгоритмического решения; байесовские сети, используемые для выявления аномалий; генетические алгоритмы, используемые для бинарной классификации; текст майнинг (text mining), используемый для кластеризации и обнаружения аномалий. Также современной тенденцией обнаружения мошенничества является использование гибридных методов, которые используют сильные стороны различных методов.

Выявление финансового мошенничества включает мониторинг поведения владельцев карточных счетов с целью выявления их нежелательного поведения.

В табл. 2 представлены результаты сравнительного анализа экономико-математических методов выявления мошенничеств в банках, осуществляемых персоналом банка.

Таблица 2
Table 2

Сравнительный анализ экономико-математических методов выявления мошенничеств в банках, осуществляемых персоналом банка
Comparative analysis of economic and mathematical methods for detecting fraud in banks carried out by the bank's staff

Группа методов выявления мошенничеств в банках	Характеристика	Учет неопределенности
Количественные (закон Бенфорда, ассоциативный анализ, логистическая регрессия, скрытая Марковская модель)	Основан на стандартном математическом аппарате	Неопределенность учитывается с помощью средств статистики и теории вероятностей
Машинное обучение (метод опорных векторов, дерево решений, нейронные сети, самоорганизующиеся карты Кохонена, байесовские сети, генетические алгоритмы, текст-майнинг)	Базируются на технологиях искусственного интеллекта (обучение с учителем и без него)	Неопределенность учитывается с помощью средств статистики и теории вероятностей
Качественные (нечеткая логика)	Базируются на экспертных оценках	Неопределенность учитывается с помощью экспертных оценок
Гибридные (нейронечеткие системы)	Основаны на синергетическом подходе (используются сильные стороны различных методов)	Неопределенность учитывается с помощью количественного и качественного математического аппарата

Источник: составлено автором на основе [Бабаева, Назаров, 2023; Скареднова, Скареднов, 2022; Султанов, 2020; AlSharif, Al-Slehat, 2019; Harahap, Nasrizal, Indrawati, Sandri, 2022]

Source: compiled by the author on the basis of [Бабаева, Назаров, 2023; Скареднова, Скареднов, 2022; Султанов, 2020; AlSharif, Al-Slehat, 2019; Harahap, Nasrizal, Indrawati, Sandri, 2022]

В целом можно сделать вывод, что в системе внутреннего аудита целесообразно использовать гибридные методы для учета неопределенности и выявления мошенничества. Они учитывают неопределенность с помощью средств статистики и теории вероятностей.

Заключение

По результатам исследования выявлено, что ландшафт киберэкосистемы постоянно меняется, создавая новые угрозы потери кибербезопасности банков и приводя к росту уровня киберрисков. В этих условиях банки должны иметь эффективную систему обеспечения кибербезопасности для устранения имеющихся и потенциальных внешних и внутренних угроз. Исходя из этого, важную роль для предупреждения киберугроз играет внутренний аудит, который определен как периодическая система сбора и оценки информации для определения того, обеспечивают ли все системы банка надлежащее состояние защищенности информационных активов и информационной инфраструктуры, сохранение свойств информационных активов (доступности, целостности или конфиденциальности) на целевом уровне.

Своевременное проведение мероприятий банковского аудита с использованием гибридных методов позволяет снизить уровень мошенничества и повысить ответственность банковского персонала. Особенно перспективным является риск-ориентированный подход, на основе которого целесообразно составлять план аудита. Он использует модель оценки риска, построенную на основе индикаторов риска мошенничества персонала, и дает возможность определить области, которые больше всего способствуют мошенничеству банковского персонала.

Список литературы

Архангельская А.И. 2019. Непрерывный дистанционный аудит в банке: расширение возможностей. Банковское дело, 4: 65–69.

Бабаева Г.Я., Назаров С. 2023. Риски, связанных с активными операциями банков и их минимизация. Экономика и социум, 6-1 (109): 642–645.

Битов А.А., Жуков А.З. 2022. Обеспечение информационной безопасности в финансовом секторе Российской Федерации: проблемы и стратегия противодействия. Евразийский юридический журнал, 6 (169): 394–395.

Власова Н.В., Шишлянников А.В. 2020. Экспертная оценка учетной политики для целей бухгалтерского учета кредитной организации. М., КноРус, 150 с.

Журавлёва Т.А. 2023. Нормативное правовое регулирование и информационное обеспечение выявления и документирования рисков хозяйственной деятельности коммерческого банка. Управленческий учет,10: 71–76.

Карпунин В.И., Ефремова Ю.С. 2020. Системная парадигма риск-ориентированного внутреннего контроля кредитной организации. Вестник Российского экономического университета имени Г.В. Плеханова, 2 (110): 13–31. DOI: 10.21686/2413-2829-2020-2-13-31

Курныкина О.В. 2020. Учетно-аналитическое обеспечение управления и контроля в коммерческом банке в условиях цифровизации и МСФО. М., ООО «РУСАЙНС», 222 с.

Лазарева И.Е. 2022. Финансовые технологии в структуре финансовой системы. Сборник научных работ серии «Финансы, учет, аудит», 4 (28): 117–125.

Михайлова О.Д. 2020. Кибербезопасность: влияние на банковскую цифровизацию в Российской Федерации. Человеческий капитал и профессиональное образование, 2 (32): 23–28.

Сипратов Р.О. 2022. Страхование киберрисков в условиях функционирования банковских экосистем. Финансовая экономика, 8: 134–139.

Скареднова О.Л., Скареднов И.С. 2022. Особенности практической реализации внутреннего аудита коммерческого банка. Журнал прикладных исследований, 11: 229–237.

Скареднова О.Л., Скареднов И.С. 2022. Российский и зарубежный опыт оценки механизма управления рисками коммерческого банка в процессе проведения внутреннего аудита. Финансовый бизнес, 9 (231): 98–102.

Султанов Г.С. 2020. Международная практика аудита деятельности финансово-кредитных учреждений. Экономика и предпринимательство, 12 (125): 1483–1486.

Султанов Г.С. 2020. Роль и значение аудита финансово-кредитных учреждений. Научная матрица, 4: 29–32.

Alharbi, M. S. A. 2017. The effectiveness of the implementation of internal control in kuwaiti shareholding companies. International Journal of Academic Research in Accounting, Finance and Management Sciences, 7: 232–241.

AlSharif M.B., Al-Slehat, F.Z. 2019. The effect of internal control on the competitive advan-tage of the bank. International Journal of Business And Management, 14(9), 91 p. DOI: 10.5539/ijbm.v14n9p91

Harahap D.S.P., Nasrizal N., Indrawati N., Sandri S.H. 2022. The pengaruh internal audit dan whistleblowing system terhadap pencegahan fraud dengan moralitas individu sebagai variabel moderator (studi empiris pada bank perkreditan rakyat di provinsi RIAU). Jurnal Akuntansi dan Ekonomika, 12: 82–91.

Knezevic S., Živković A., Milojević S. 2021. The role and importance of internal control and internal audit in the prevention and identification of fraudulent actions in banks. Bankarstvo, 50 (1): 66–89. DOI:10.5937/bankarstvo2101066K

Patricia V.L.T. 2022. The role of internal auditors in supporting the implementation of the principles of transparency and accountability (study at pt. Bank mega syariah kc. Medan). Journal of Indonesian Management (JIM), 1: 28–45.

Simpson B. 2022. An Introduction to Internal Auditing in Banking. London, Barclay Simpson Associates Limited, 23 p.

References

Arkhangelskaya A.I. 2019. Continuous remote audit in the bank: expanding opportunities. Banking, 4: 65–69. (in Russian)

Babaeva G.Ya., Nazarov S. 2023. Risks associated with active operations of banks and their minimization. Economy and society, 6-1 (109): 642–645. (in Russian)

Bitov A.A., Zhukov A.Z. 2022. Ensuring information security in the financial sector of the Russian Federation: problems and counteraction strategy. Eurasian Law Journal, 6 (169): 394–395. (in Russian)

Vlasova N.V., Shishlyannikov A.V. 2020. Expert assessment of accounting policy for the purposes of accounting of a credit institution. Moscow, Publ. KnoRus, 150 p. (in Russian)

Zhuravleva T.A. 2023. Regulatory legal regulation and information support for identifying and documenting the risks of a commercial bank's business activities. Management accounting, 10: 71–76. (in Russian)

Karpunin V.I., Efremova Yu.S. 2020. The systemic paradigm of risk-based internal control of a credit institution. Bulletin of the Plekhanov Russian University of Economics, 2 (110): 13–31. DOI: 10.21686/2413-2829-2020-2-13-31 (in Russian)

Kurnykina O.V. 2020. Accounting and analytical support for management and control in a commercial bank in the context of digitalization and IFRS. Moscow, Publ. RUSAINS, 222 p. (in Russian)

Lazareva I.E. 2022. Financial technologies in the structure of the financial system. Collection of scientific papers in the series «Finance, accounting, audit», 4 (28): 117–125. (in Russian)

Mikhailova O.D. 2020. Cybersecurity: the impact on banking digitalization in the Russian Federation. Human capital and vocational education, 2 (32): 23–28. (in Russian)

Sipratov R.O. 2022. Insurance of cyber risks in the context of the functioning of banking ecosystems. Financial economics, 8: 134–139. (in Russian)

Skarednova O.L., Skarednov I.S. 2022. Features of the practical implementation of the internal audit of a commercial bank. Journal of Applied Research, 11: 229–237. (in Russian)

Skarednova O.L., Skarednov I.S. 2022. Russian and foreign experience in assessing the risk management mechanism of a commercial bank in the process of conducting an internal audit. Financial business, 9 (231): 98–102. (in Russian)

Sultanov G.S. 2020. International practice of auditing the activities of financial and credit institutions. Economics and entrepreneurship, 12 (125): 1483–1486. (in Russian)

Sultanov G.S. 2020. The role and importance of auditing financial and credit institutions. The Scientific Matrix, 4: 29–32. (in Russian)

Alharbi, M. S. A. 2017. The effectiveness of the implementation of internal control in ku-waiti shareholding companies. International Journal of Academic Research in Accounting, Finance and Management Sciences, 7: 232–241.

AlSharif M.B., Al-Slehat, F.Z. 2019. The effect of internal control on the competitive ad-van-tage of the bank. International Journal of Business And Management, 14(9), 91 p. DOI: 10.5539/ijbm.v14n9p91

Harahap D.S.P., Nasrizal N., Indrawati N., Sandri S.H. 2022. The pengaruh internal audit dan whistleblowing system terhadap pencegahan fraud dengan moralitas individu sebagai variabel mod-erator (studi empiris pada bank perkreditan rakyat di provinsi RIAU). Jurnal Akuntansi dan Ekonomika, 12: 82–91.

Knezevic S., Živković A., Milojević S. 2021. The role and importance of internal control and internal audit in the prevention and identification of fraudulent actions in banks. Bankarstvo, 50 (1): 66–89. DOI:10.5937/bankarstvo2101066K

Patricia V.L.T. 2022. The role of internal auditors in supporting the implementation of the principles of transparency and accountability (study at pt. Bank mega syariah kc. Medan). Journal of Indonesian Management (JIM), 1: 28–45.

Simpson B. 2022. An Introduction to Internal Auditing in Banking. London, Barclay Simp-son Associates Limited, 23 p.

Конфликт интересов: о потенциальном конфликте интересов не сообщалось.
Conflict of interest: no potential conflict of interest related to this article was reported.

Поступила в редакцию 26.12.2023
Поступила после рецензирования 25.03.2024
Принята к публикации 29.03.2024

Received December 26, 2023
Revised March 25, 2024
Accepted March 29, 2024

ИНФОРМАЦИЯ ОБ АВТОРЕ

Мусацкая Яна Сергеевна, кандидат экономических наук, доцент кафедры цифровой аналитики и контроля Института учета и финансов, Донецкий национальный университет экономики и торговли имени Михаила Туган-Барановского, г. Донецк, Россия

INFORMATION ABOUT THE AUTHOR

Yana S. Musatskaya, PhD in Economics, Associate Professor of the Department of Digital Analytics and Control, Institute of Accounting and Finance, Donetsk National University of Economics and Trade named after Mikhail Tugan-Baranovsky, Donetsk, Russia