

УДК 338.2 DOI: 10.14451/1.221.177

Инновационный подход к деятельности финансовых институтов в условиях цифровизации*

© 2023 Кулакова Людмила Ивановна

кандидат экономических наук, доцент, заведующий кафедрой «Экономика и управление».

Дальневосточный филиал ФГБОУ ВО «Всероссийская академия внешней торговли Министерства экономического развития Российской Федерации». Россия, Петропавловск-Камчатский.

E-mail: milakul2606@rambler.ru

© 2023 Кичигин Олег Эмильевич

Доктор экономических наук, доцент. Профессор Высшей инженерно-экономической школы.

Санкт-Петербургский политехнический университет Петра Великого. Россия, Санкт-Петербург.

E-mail: kichigin_oe@spbstu.ru

Ключевые слова: технология блокчейн, смарт-контракты, безопасность финансовых институтов и банковских операций.

Актуальность выбранной темы обусловлена постоянно возрастающей ролью использования цифровых технологий в финансовых институтах. Сегодня необходимость обеспечения безопасности финансовых операций при осуществлении взаимодействия экономических субъектов не вызывает сомнения, так как они являются гарантами стабильности социально-экономического благополучия общества, а безопасность играет ключевую роль в развитии банковской системы и является её важным элементом. Интенсивность развития информационных технологий способствовала пересмотру действующих процедур обеспечения безопасности в финансово-кредитных организациях и переходу к разработке и/или внедрению новых технологий. Такие решения повлекли за собой необходимость в обеспечении надёжной защиты информации, задействованной в работе коммерческих банков, в особой защите от потери её свойств, а именно конфиденциальности, целостности и доступности, что непосредственно отражается на эффективности деятельности и деловой активности банка. В настоящей статье рассмотрены сущность системы распределенного реестра, его роль в формировании инструментов защиты и снижении затрат на обеспечение безопасности. Даны сравнительные характеристики используемым в настоящее время автоматизированным банковским системам. Предложены рекомендации по внедрению в финансово-кредитные организации системы распределенного реестра для безопасности банковских операций. Предметом исследования является совокупность процедурных приёмов и методов оценки эффективности внедрения цифровых технологий в финансовые институты, с целью обеспечения безопасности банковских операций, способствующих повышению эффективности функционирования финансово-кредитной организации.

*Работы выполнены в рамках реализации проекта «Разработка методологии формирования инструментальной базы анализа и моделирования пространственного социально-экономического развития систем в условиях цифровизации с опорой на внутренние резервы» (FSEG-2023-0008). (₽)

Введение

Актуальность исследования заключается в том, что на сегодняшний день современные финансовые технологии могут заменить все функции традиционной финансовой системы. Благодаря развитию интернет-банкинга экономические агенты могут кредитоваться, приобретать товары и услуги, осуществлять денежные переводы, совершать сделки с активами без услуг сотрудников банка. Интенсивность развития информационных технологий способствовала пересмотру действующих процедур обеспечения безопасности в финансово-кредитных организациях и переходу к разработке и/или внедрению новых технологий. Такие решения повлекли за собой потребность в обеспечении надёжной защиты информации, задействованной в работе коммерческих банков, что непосредственно отразилось на деловой активности и эффективности их деятельности. С этой целью был изучен вопрос необходимости применения современных цифровых технологий, а именно системы распределённого реестра в обеспечении безопасности банковских операций.

Авторский подход к совершенствованию системы обеспечения безопасности операций институтов финансовой системы, способствующих повышению эффективности деятельности финансово-кредитной организации и оценке их эффективности в организационно-управленческом аспекте базировался на теоретико-методологических работах отечественных и зарубежных авторов. В основу исследования легли научные труды отечественных авторов Андреева В. Д. [1], Бабаш А. В. [2], Грязнова Е. С., Панасенко С. А. [11], Громова Ю. Ю. [10], Черемшанов С. В. [1], посвященные информационной безопасности.

Существенный вклад в развитие научного обоснования применения системы распределённого реестра в кибербезопасности внесли зарубежные исследователи Panda Security [9], Вита-

лик Бутерин [20] и др. Теоретические основы внутрифирменного контроля и финансового менеджмента отражены в трудах Вакуленко Т. Г. [6], Фоминой Л. Ф. [6], Галицкой С. В. [7], Круглова М. И. [14] и др.

Важное место в массиве исследований, связанных с совершенствованием теоретико-методологических основ качества информационных систем занимают работы Исаева Г. А. [13], Багишева И. [3], Маньшина Г. Г., Артамонова В. А., Артамоновой Е. В. [15] и др.

Целью исследования является совершенствование системы обеспечения безопасности банковских операций на основе блокчейн технологий.

Для достижения поставленной цели решен ряд задач, направленных на приращение знаний о внедрении технологии распределённого реестра в систему безопасности и навыков его применения в финансово-кредитных организациях.

Материалы и методы.

Методология исследования включает теоретические и эмпирические методы, позволившие провести оценку безопасности банковских операций, влияющих на эффективность деятельности финансово-кредитной организации. На основе методов группировок и классификации проведен SWOT-анализ автоматизированной банковской системы FIS Profile. Методы моделирования позволили рассмотреть положительные аспекты от внедрения технологии распределённого реестра финансово-кредитной организацией в целях повышения эффективности её функционирования и выработать рекомендации по внедрению современных цифровых технологий для обеспечения безопасности банковских операций.

Результаты и обсуждение

Выделив операции, которые подпадают под понятие банковских, и при применении к которым посредством технологии распределённого ре-

естра в теории можно достигнуть повышения уровня безопасности, мы разделили их на внутренние и внешние:

Внутренние банковские операции

- Оформление документации с клиентом и внесение его в реестр; Внутренний документооборот, содержащий коммерческую тайну. Межбанковские переводы, выдача наличных денег.

Внешние банковские операции

- Взаимодействие с клиентом посредством мобильного (интернет) банка.
- Оплата клиентом товаров, работ, услуг картой системы VISA, MasterCard, Мир.

Внутренние и внешние банковские операции условно можно разделить на две основные категории, требующие особого внимания: это обеспечение безопасности персональных данных и обеспечение безопасности документооборота

Опираясь на существующие практики Центрального Банка ранжирования информации, требующей надежной защиты по ценности и уровню защиты выявлены основные информационные активы:

- Сведения делового характера;
- Сведения о клиентах банка;
- Сведения о предоставленных услугах;
- Сведения по вопросам обеспечения безопасности;
- Сведения о финансовой отчетности;
- Сведения о сотрудниках банка.

В результате предлагается шкала оценки для определения приоритетов и шкала для определения угроз, которые варьируются от 0 до 10:

Шкала оценки для определения приоритетов

1. Информация от 0–3 обладает низким приоритетом;
2. Информация от 3–5 обладает средним приоритетом;
3. Информация от 5–8 обладает высоким приоритетом;

4. Информация от 8–10 обладает наивысшим приоритетом.

Шкала оценки для определения угроз

1. Информация от 0–4 обладает низкой защитой;
2. Информация от 4–7 обладает средней защитой;
3. Информация от 7–10 обладает высокой защитой.

Начиная с 1992 года в Российской Федерации финансово-кредитные организации используют автоматизированные банковские системы (АБС), представляющие собой аппаратно-программный комплекс, который состоит из множества компьютеров, объединенных в единый защищенный контур, где обрабатываются платежные поручения и формируются реестры платежей [5]. Сформированные в АБС реестры поступают в автоматизированное рабочее место клиента Банка России – специальный компьютер в банке в отдельном защищенном контуре, с которого уходят платежи в ЦБ РФ [18].

Большинство российских банков использует иностранную систему АБС-FIS Profile, производителем которой являются Соединённые Штаты Америки. Чтобы сформировать представление о надёжности модели АБС-FIS Profile, проведен SWOT-анализ системы (табл. 1).

Таким образом, автоматизированная банковская система не способна обеспечить надлежащий уровень безопасности данных, вдобавок риск, при котором произойдёт сбой системы, достаточно велик.

Для хранения внутренней документации банк использует внутренний сервис – информационную инфраструктуру, которая построена на топ-моделях оборудования (сервера Oracle M6 и HP Blade System, системы хранения Hitachi HUS VM, телекоммуникационное оборудование CISCO), обеспечивающего необходимую производительность и обладающего большими возможностями по масштабированию ресурсов, что позволяет увеличить количество клиентов и операций

Таблица 1. SWOT-анализ АБС FIS Profile.

Сильные стороны (Strengths)	Слабые стороны (Weaknesses)
Система автоматизирует работу в организации, исключая возможность ошибки человека при составлении отчётности Система зарекомендовала себя на рынке АБС систем как надёжную, многие банки используют её	Система исключает возможность резервного копирования информации в «облако» цифровое пространство По факту ЦБ не контролирует деятельность АТБ, отсутствие возможности отслеживать процессы в режиме реального времени
Возможности (Opportunities)	Угрозы (Threats)
Проработать процесс создания резервной копии	Сбой системы хотя бы на несколько минут может привести к потере огромных денежных средств и репутации банка Реальная угроза потери данных, возникает от осуществления хакерских атак

Источник: составлено автором.

в несколько раз без модернизации оборудования. Системы построены с использованием виртуализации, которая позволяет эффективно использовать оборудование: гибко распределять нагрузку и легко наращивать мощности, без остановки работы систем и обеспечить непрерывность бизнеса. Инженерная инфраструктура построена на оборудовании мировых лидеров (STULZ, APC, AMP NetConnect, Schneider Electric).

Для осуществления внешних банковских операций коммерческие банки используют систему SWIFT-Society of Worldwide Interbank Financial Telecommunications (в переводе «Общество всемирных межбанковских финансовых каналов связи»).

С технической точки зрения система представляет собой международную корпоративную сеть, к которой подключены участники (банки и другие пользователи) и которая управляется системными ресурсами (региональными процессорами и операционными центрами).

На рисунке 1 представлены пути движения платежей и сообщений при использовании системы SWIFT.

На рисунке 1 можно наблюдать, что при взаимодействии с системой SWIFT в процессе осуществления банковской операции участвуют несколько субъектов финансовых отношений.

Несмотря на выстроенную систему безопасности и цифровой электронной подписи система остаётся крайне уязвимой к хакерским атакам, поскольку информация проходит, как минимум, через два финансовых института, вдобавок ко всему, использование системы SWIFT влечёт за собой большие затраты, в частности только для поддержания работоспособности системы банки тратят порядка 6 млн рублей в год.

В России постепенно осуществляется подключение к системам «PayPal». Подобный вид платежных систем призван обеспечивать потребителю высокий уровень безопасности, т.к. данные находятся в распоряжении авторитетной платежной системы, а не у случайного пользователя-поставщика товаров, работ, услуг. Несомненным преимуществом системы «PayPal» является единовременное фиксирование данных клиента с дальнейшей аутентификацией в процессе совершения финансовых операций в независимости от расположения точки доступа.

Однако настоящую угрозу безопасности данным и денежным средствам для клиента несёт само приложение банка, об этом свидетельствует официальная статистика попыток взлома (более 14,6 тыс. в день), представленная компанией «Fortinet», которая изучает попытки информационных атак на Российском финансовом рынке [3]. При этом удельная себестоимость для защиты от одной атаки составляет 290 рублей, что, безусловно, является дополнительной финансовой

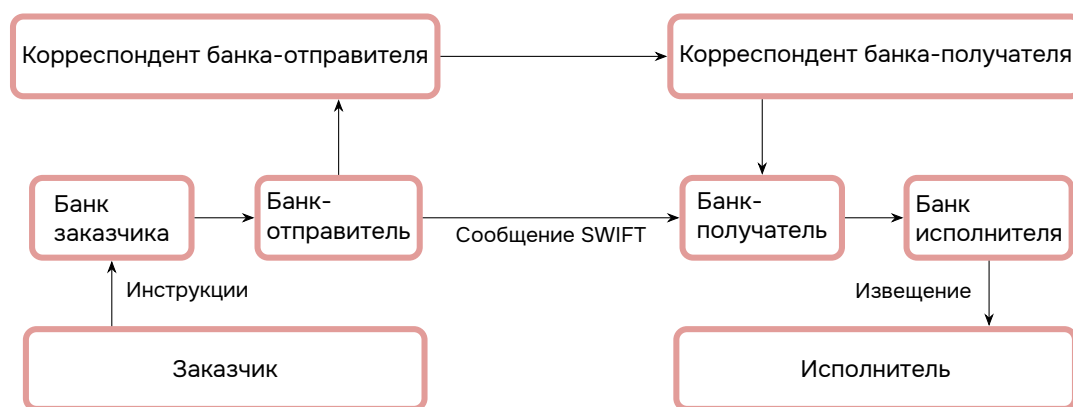


Рис. 1. Движение платежей и сообщений в системе SWIFT.

Источник: составлено автором.

нагрузкой и представляет собой дополнительный барьер к улучшению конкурентной составляющей на финансовом рынке.

Рассмотрим структуру объёма затрат на обеспечение безопасности банковских операций за 2018 год (рис. 2).

Исходя из данных рисунка 2, можно сделать вывод, что большая часть затрат – 73%, приходится на обеспечение безопасности мобильного банка. Удельный показатель находится в пределах нормы, однако, как показывают исследования, внедрение технологии распределённого реестра позволит сократить данный показатель на 32%, следовательно, ещё одной актуальной проблемой является минимизация затрат на обеспечение безопасности банковских операций.

Проведённый анализ безопасности банковских операций в коммерческих банках свидетельствует о недостаточно надёжной системе безопасности, помимо угрозы потери данных существует также и угроза использования персональных данных клиента банка недобросовестными сотрудниками в корыстных целях. Помимо этого, активное развитие современных технологий, следовательно, и вредоносного программного обеспечения является серьёзной угрозой для существующих систем безопасности, делая их работу неэффективной. Внедрение системы распределённого реестра могло бы решить эти проблемы.

Распределённый реестр представляет собой базу данных активов, которая может быть распределена по сети разнообразных сайтов, в разных географических зонах или организациях (рис. 3).

Базой системы распределённого реестра является технология «Blockchain» (Блокчейн), развитие которой позволит осуществить переход деятельности государственных и частных компаний в совершенно иное качество.

Благодаря двум основополагающими элементам системы распределённого реестра, обеспечивающим его безопасность, хеш-функции и электронной подписи можно гарантировать целостность блоков транзакций, т. е. исключение возможности внесения изменений в отдельно взятый блок без внесения изменений во всю цепочку [4]. Данная система предусматривает такой алгоритм действий, при котором, совершая каждую последующую операцию, создающую новый блок, она обязательно ссылается на «хеш» предшествующий в реестре. При этом индивидуальный «хеш» каждого блока зависит от всех его транзакций, но вместо того, чтобы последовательно передавать транзакции хеш-функции, они собираются воедино.

Особенностью данной технологии является то, что в цифровых подписях используются два ключа – закрытый и открытый [17]. Открытый ключ применяется при создании цифровой подписи и является секретным. Закрытый ключ выступает инструментом проверки подлинности

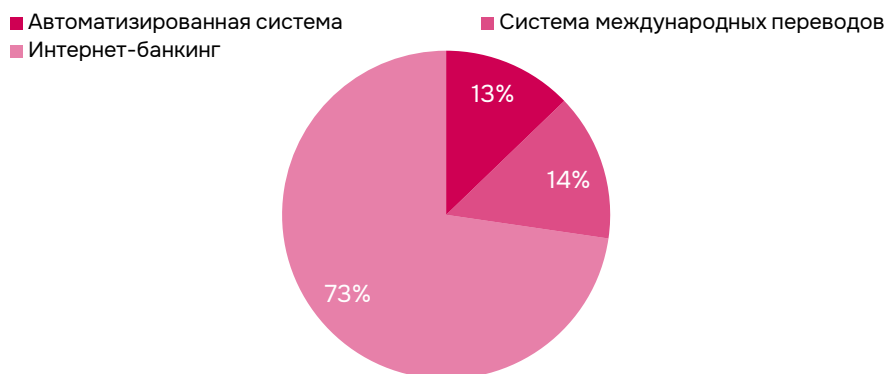


Рис. 2. Структура затрат на обеспечение безопасности банковских операций.

Источник: составлено автором.

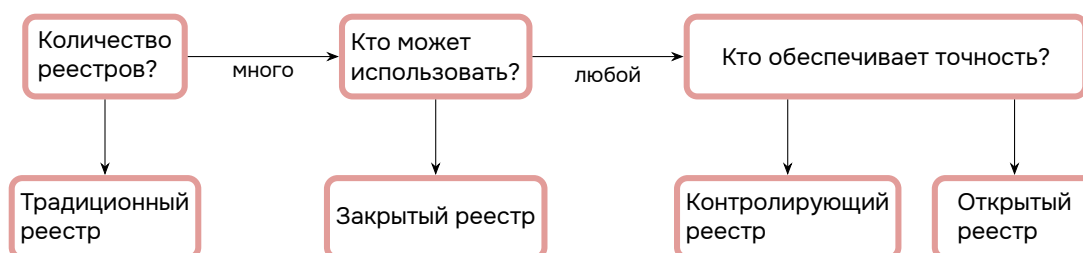


Рис. 3. Сущность системы распределённого реестра.

Источник: составлено автором.

созданной подписи. Обычная система совершения финансовых (или иных) операций является наиболее трудоемкой и менее защищенной. Тогда как технология блокчейн обеспечивает высокую скорость транзакций, гарантирует прозрачность, точность, надежность и безопасность данных. Сравнительная характеристика обычной и Блокчейн системы представлена на рисунке 4.

Ныне существующая система хранения данных и совершения операций не в полной мере способна защитить от такого вида мошенничества как вирусные атаки, посредством которых происходят хищения паролей от счетов. Система распределенного реестра призвана обеспечить безопасность тройной защитой: электронной подписью, токеном и ключом. Но следует отметить, что в финансовой сфере существует и такой вид угрозы безопасности данных, как мошенничество работников финансово-кредитных организаций, проявляющееся в махинациях со счетами клиентов и кредитными линиями [8]. Технология распределенного реестра направлена на искоренение таких фактов, оказывающих

влияние не только на эффективность работы банка, но и на его репутацию.

Ключевое отличие «блокчейна» от обычных баз заключается в децентрализации при формировании блоков, которые практически невозможно взломать или изменить в одностороннем порядке. Применение системы распределенного реестра позволит исключить возможность мошенничества, т.к. исчезнет вероятность внесения изменений в состояние счета клиента без его электронной подписи, которая находится лично у него; изменить процентные ставки по кредитам или вкладам, а также иные мошеннические действия, скрытые от регуляторов и клиентов. Условия, прописанные в кредитном или ином договоре, будут зафиксированы в блоке, который изменить невозможно. Фиксирование каждой следующей записи, изменяющей состояние предыдущей, гарантирует прозрачность и синхронизацию на всех электронных ресурсах. При этом не исключается, а предусматривается возможность доступа клиента к текущей информации по счету, кредиту, переводу и т. д.

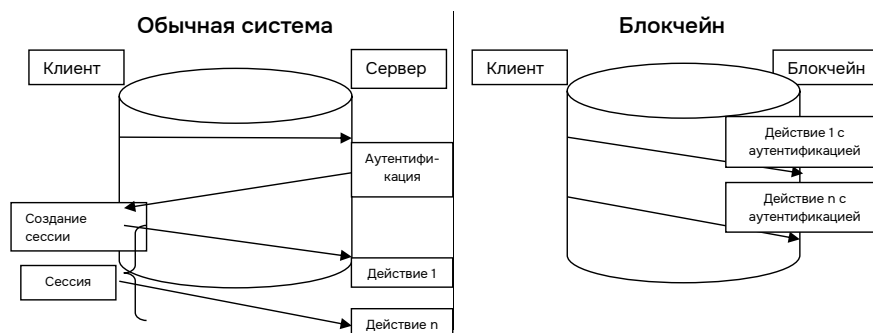


Рис. 4. Сравнительная характеристика обычной и Блокчейн систем.

Источник: составлено автором по данным [13].

Взаимодействие между банками по взаиморасчетам, переводам между различными банками клиентов, расчетам по клирингу и эквайринг требуют частного (приватного) блокчейна, с расширенным доступом к чтению информации пользователями.

Основное преимущество безопасности в данном случае по сравнению с тем, что обеспечивает сейчас SWIFT, возможность совершить откат блокчейна к состоянию «предатаки» (поскольку были украдены только цифровые активы), если более 50% участников сети согласятся. В данном случае присутствует определенная конфронтация с самой философией блокчейна, что уже завершенные блоки не удаляются.

Технология распределённого реестра позволяет повысить эффективность и качество управленческой работы, усилить режим экономии финансовых ресурсов на обеспечение безопасности банковских операций. За счёт внедрения единой системы (цепочки блоков) появится возможность сократить излишние затраты организации. Проведенные исследования показали, что они могут сократиться на 28%.

Существует проблема применения системы распределенного реестра во взаимоотношениях между фирмами. Если в розничных сделках участниками являются один покупатель, который переводит деньги за благо, и один продавец, то в секторе корпоративных сделок цепь расчетов длиннее: например, одна из компаний представляет обязательства другой заплатить, следующая предоставляет товар (работу, услугу),

и первая затем осуществляет платеж. Проблема заключается в том, что в настоящее время нет ни одной платформы, способной обеспечить такой функционал. Взаимную выгодность отношений внутри корпоративного сектора банки сейчас интересуют смарт-контракты, которые можно запрограммировать под каждый из возможных сценариев развития событий. Еще одной проблемой подобной управленческой линии является отсутствие регулятивных мер в отношении смарт-контрактов. В случае появления сбоя в контракте, либо неисполнения клиентом своих обязательств апеллировать не представляется возможность ни к одной инстанции. На данном этапе развития цифровой экономики разумно внедрять смарт-контракты именно для сокращения издержек, но не как средство повышения безопасности, поскольку в их кодировании до сих пор еще остаются серьезные проблемы [12].

Внедрение системы распределенного реестра для безопасности банковских операций требует:

1. Обучение специалистов, обладающих определенными компетенциями в области технологий распределённого реестра;
2. Формирование правовой основы, регламентирующей деятельность в области smart-contract и Blockchain;
3. Формирование технических требований со стороны ЦБ, а также практики государства или финансовых институтов использования технологии распределённого реестра.

Следует учитывать и ряд существующих рисков

при использовании системы распределенных реестров, связанных с децентрализованным доступом к данным и управлением криптографическими ключами. Ведь в случае потери ключей пользователи мгновенно могут понести невосполнимые финансовые и репутационные потери, а также потери, связанные с мошенничеством и захватом учетной записи. Компрометация ключей может сделать данные недоступными или нечитаемыми, что непременно приведет к потере средств, защищенных криптографией. Возможность связать открытые ключи с физическим или юридическим лицом тоже является важным аспектом в области цифровой подписи, связанным с соблюдением конфиденциальности, где к пользователям предъявляются юридические требования, такие как соблюдение требований борьбы с отмыванием денежных средств.

Отвечая на современные вызовы в сфере безопасности, многочисленные органы по стандартизации и регулирующие органы разработали подробные рекомендации и минимальные требования к использованию криптографических ключей на предприятиях и дизайну систем управления криптографическими ключами.

Исполнение директивных документов (регламентов, инструкций и т.д.) по формированию и использованию децентрализованных систем станет важным шагом для того, чтобы технология распределенного реестра стала жизнеспособной.

С целью совершенствования системы обеспечения безопасности банковских операций, снижения данного вида затрат, способствующих повышению эффективности деятельности банка, выработан ряд рекомендаций.

1. В целях внедрения технологии распределённого реестра для обеспечения безопасности банковских операций банку необходимо:

- Создать инициативную группу по применения технологии распределённого реестра;
- Акцентировать внимание на использовании, в рамках пилотного проекта, «умных контрактов»;

- Разработать стратегическую политику банка, с целью его полного перехода в Интернет-банкинг.

2. Поскольку успешная деятельность банка и его дальнейшая прибыль, которая может быть направлена на совершенствование систем безопасности банковских операций, зависит от количества клиентов, в целях увеличения объема реализации необходимо проанализировать:

- Возможности увеличения спроса на услуги;
- Потенциал расширения рынка сбыта (исключительно в Интернет-банкинге);
- Деятельность конкурентов;
- Конкурентоспособность предлагаемых услуг.

3. Для обеспечения безопасности банковских операций банкам необходимо регулярно проводить следующую работу:

- Наладить обратную связь с клиентами банка о проблемах при использовании мобильного приложения;
- Осуществлять регулярный мониторинг существующего сервиса и проверку скорости его действия;
- Осуществлять регулярный анализ существующих угроз и выработку мер для их устранения.

Заключение

Автоматизированная банковская система не способна обеспечить надлежащий уровень безопасности данных, вдобавок риск, при котором может произойти сбой системы, достаточно велик. Не стоит забывать и о неэффективном взаимодействии между коммерческими банками и Центральным Банком, ведь последний может контролировать деятельность банка лишь на основании предоставленной отчетности, что, с развитием современных технологий, является неэффективным методом управления, поскольку уровень контроля должен осуществляться в режиме реального времени. Только при таком уровне контроля существует реальная возможность вовремя выявить угрозы как экономического, так и информационного характера. Однако в целом суммарный показатель безопасности банковских операций находится в пределах

допустимой нормы, но стремительное развитие современных технологий, следовательно, и вредоносного программного обеспечения является серьезной угрозой для существующих систем безопасности, делая их работу неэффективной.

Внедрение технологии распределённого реестра позволит избежать этих проблем, однако на первоначальных этапах потребуется большой объём инвестиций.

Библиографический список

1. Андреев В. Д., Черемшанов С. В. Система внутрихозяйственного контроля: основные понятия // Аудиторские ведомости. — 2011. — № 2.
2. Бабаш А. В., Баранова Е. К., Мельников Ю. Н. Информационная безопасность : Учебное пособие. — М. : КноРус, 2013. — 136 с.
3. Багишев И. Некоторые аспекты информационной безопасности технологии блокчейн. — URL: <http://www.itsec.ru/articles/nekotoryye-aspekty-informatsionnoy-bezopasnosti-tehnologii-blokcheyn> (дата обр. 08.08.2019).
4. Блокчейн: атаки, безопасность и криптография. — URL: https://ipiskunov.blogspot.com/2017/12/blog-post_1.html (дата обр. 08.08.2019).
5. Бутерин В. О «нефинансовых» случаях использования блокчейна. — URL: <https://coinspot.io/technology/vitalik-buterin-o-nefinansovyh-sluchayah-ispolzovaniya-blokcheyna> (дата обр. 08.08.2022).
6. Вакуленко Т. Г., Фомина Л. Ф. Анализ бухгалтерской (финансовой) отчетности для принятия управленческих решений. — Герда, 2009. — 288 с.
7. Галицкая С. В. Финансовый менеджмент. Финансовый анализ. Финансы предприятий : Учебное пособие. — М. : Финансы и статистика, 2009. — 652 с.
8. Головина Т. А., Полянин А. В., Авдеева И. Л. Развитие цифровых платформ как фактор конкурентоспособности современных экономических систем // Вестник Пермского университета. Серия: Экономика. — 2019. — Т. 14, № 4. — С. 551–564.
9. Гретчин В. В., Полянин А. В. Концептуальные положения использования электронного администрирования в менеджменте // Экономические и гуманитарные науки. — 2014. — 11 (274). — С. 112–118.
10. Громов Ю. Ю., Драчев В. О., Иванова О. Г. Информационная безопасность и защита информации : Учебное пособие. — Ст. Оскол : ТНТ, 2010. — 384 с.
11. Грязнов Е. С., Панасенко С. А. Безопасность локальных сетей. — М. : ПиК, 2006. — 525 с.
12. Докукина И. А., Полянин А. В. Организация децентрализованного управления на основе цифровых платформ распределенного реестра // Естественно-гуманитарные исследования. — 2020. — 27 (1). — С. 76–80.
13. Исаев Г. А. Теоретико-методологические основы качества информационных систем. — М. : Инфра-М, 2018. — 258 с.
14. Круглов М. И. Стратегическое управление компаний : учебник для вузов. — М. : Русская деловая литература, 2016. — 456 с.
15. Маньшин Г. Г., Артамонов В. А., Артамонова Е. В. Безопасность информационной технологии Блокчейн. — URL: <http://itzashita.ru/kriptoalyutyi/bezopasnost-informatsionnoy-tehnologii-blokcheyn.html> (дата обр. 08.08.2022).
16. О борьбе с хакерами в банковской сфере / РБК. — URL: <https://www.rbc.ru/finances/30/01/2017/588e93ec9a7947efb32da5f9?from=t> (дата обр. 08.08.2022).
17. О влиянии блокчейн на информационную безопасность. — URL: <https://www.securitylab.ru/blog/company/PandaSecurityRus/342639.php> (дата обр. 08.08.2022).
18. О внедрении технологии распределённого реестра в финансовый сектор. — URL: <https://sberbankonline.ru> (дата обр. 08.08.2022).
19. Об анализе применения технологии блокчейн в целях обеспечения безопасности банковских операций / Allbest. — URL: https://otherreferats.allbest.ru/programming/00820040_0.html (дата обр. 08.08.2022).
20. Panda Security, Blockchain's Profound Effect on Cybersecurity. — URL: <https://www.pandasecurity.com/mediacenter/security/blockchain-profound-effect-cybersecurity> (visited on 08/08/2022).