15. Kuzminov Ya. ... And yet why do Russia need migrants? // Migration XXI century. 2011. № 2 (5). Pp. 2–4. (In Russ.).
16. Sidenko I. K., Sidenko A. G Influence of migration flows on the economic security of the state // Bulletin of St. Petersburg University of the Ministry of Internal Affairs of Russia. 2010. No. 2. Pp. 129–135. (In Russ.).
17. Goryachkina T. V. Organizational and economic mechanism for managing labor diversification: dissertation for candidate of economics' degree. Tyumen, 2002. 142 p. (In Russ.).

Как цитировать статью: Лузина Т. В., Елфимова О. С. Проблемы миграционной безопасности и региональные тенденции миграционных процессов // Бизнес. Образование. Право. 2019. № 1 (46). С. 213–221. DOI: 10.25683/VOLBI.2019.46.103.

For citation: Luzina T. V., Elfimova O. S. Problems of migration security and regional trends of migration processes // Business. Education. Law. 2019. No. 1 (46). Pp. 213–221. DOI: 10.25683/VOLBI.2019.46.103.

УДК 338
ББК 65.26

DOI: 10.25683/VOLBI.2019.46.174

Magomaeva Leyla Rumanovna,
candidate of economics, assistant professor,
head of the department of information systems in economics,
Grozny state technical university
named after Academician M. D. Millionschikov,
doctoral student of the department
«Economics and Entrepreneurship»
of the North Ossetian State
University named after K. L. Khetagurov,
Grozny,
e-mail: rumanovna@gmail.com

Магомаева Лейла Руслановна,
канд. экон. наук, доцент,
зав. кафедрой информационных систем в экономике,
Грозненский государственный технический университет
им. академика М. Д. Миллионщикова;
докторант кафедры
экономики и предпринимательства,
Северо-Осетинский государственный
университет им. К. Л. Хетагурова,
г. Грозный,
e-mail: rumanovna@gmail.com

ВОПРОСЫ СОВЕРШЕНСТВОВАНИЯ НОРМАТИВНО-ЗАКОНОДАТЕЛЬНОЙ ОСНОВЫ КРОСС-КАНАЛЬНЫХ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ КРЕДИТНО-ФИНАНСОВОГО СЕКТОРА

ISSUES OF IMPROVEMENT OF THE LEGAL AND LEGISLATIVE BASIS OF THE CROSS-CHANNEL INFORMATION TECHNOLOGIES OF THE CREDIT-FINANCIAL SECTOR

08.00.10 – Финансы, денежное обращение и кредит
08.00.10 – Finance, monetary circulation and credit

Данное исследование посвящено вопросам нормативно-законодательного регулирования кросс-канальных информационных технологий в кредитно-финансовом секторе. Автором сформирован качественно иной взгляд на применение информационных данных в условиях их интеграции в новые технологические решения. В работе детально рассмотрены направления, которые в большой степени формируют будущее современной кредитно-финансовой сферы с учетом совершенствования нормативно-законодательной основы регулирования кросс-канальных информационных технологий. Автором представлена практическая реализация рекомендаций по совершенствованию нормативно-законодательной основы регулирования кросс-канальных информационных технологий, что в будущем позволит обеспечить развитие инструментальных видов контроля и защиты информации в кредитно-финансовой сфере, повысить степень взаимодействия FinTech-компаний с традиционными финансовыми посредниками при использовании онлайн-моделей и моделей замкнутого взаимодействия, раскрыть требования к финансовым продуктам и сервисам совместного потребления, закрепить понятие «аналитика данных» в действующем законодательстве в рамках определения допустимых границ и форм их использования, формализовать методы прогнозирования и бэк-тестинга при использовании информационных систем и предусмотреть создание единой системы управления и обеспечения информационной кибербезопасности для кредитно-финансовых организаций.

This study focuses on issues of regulatory and legislative regulation of cross-channel information technologies in the credit and financial sector. The author has formed a qualitatively different view on the application of information data in the context of their integration into new technological solutions. The paper examines in detail the directions that, to a greater degree, shape the future of the modern credit and financial sphere, taking into account the improvement of the regulatory framework for the regulation of cross-channel information technologies. The author presents the practical implementation of recommendations to improve the regulatory framework for the regulation of cross-channel information technologies, which in the future will allow to ensure the development of instrumental types of control and protection of information in the credit and financial sector, to increase the degree of interaction between FinTech companies and traditional financial intermediaries using online models and models of closed interaction, to disclose the requirements for fi-

nancial products and services of joint consumption, to consolidate the concept of "data Analytics" in the current legislation in the framework of determining the permissible limits and forms of their use, to formalize methods of forecasting and back-testing when using information systems and to provide for the creation of a unified system of management and information cyber security for credit and financial institutions.

Ключевые слова: кредитно-финансовый сектор, кросс-канальные информационные решения, нормативно-законодательная база, информационные технологии, FinTech-компании, блокчейн, Базель.

Keywords: credit and financial sector, cross-channel information solutions, regulatory framework, information technology, FinTech companies, block-chain, Basel.

Введение

Интернет, как и большинство технологических нововведений последних десятилетий, уже вызвал и в дальнейшем может повлечь за собой разрушение привычного положения вещей, однако его потенциальные выгоды намного превосходят издержки. Вместо того чтобы защищать существующие рабочие места за счет сопротивления новым технологиям, государственные органы могли бы сосредоточить силы на поддержке тех, кто лишился работы и ищет новые возможности трудоустройства; вместо попыток контролировать информацию «сверху вниз» нужно использовать меры, направленные на извлечение преимуществ из инноваций «снизу вверх», открывающихся благодаря улучшению доступа к Интернету и большим данным, что требует отказа от традиционных компетенций в пользу цифровых.

Некоторые специалисты [1] разделяют вполне обоснованные опасения о возможности «переформатирования» отдельных финансовых отраслей в суверенные корпорации, размещающиеся в наиболее развитых и технологически активных странах мира. Различные научные гипотезы и сценарии дальнейшего развития финансового рынка определенно связывают с новой технологической революцией, задачей которой является имплементация и создание новых цифровых компетенций в условиях совершенствования и транснационализации банковской и расчетной систем.

Нельзя не согласиться с утверждением о том, что развитие высоких технологий на мировом уровне определяет готовность стран к повышению собственной конкурентоспособности и цифровизации экономики. В соответствии с международным индексом сетевой готовности, публикуемом в докладе «Глобальные информационные технологии» [2], Россия в 2016 г. заняла 41-е место, а в 2017 — 45-е место из 127 стран мира по уровню технологического развития, существенно отставая от наиболее развитых стран, таких как Сингапур, США, Великобритания и Скандинавские страны. Среди наиболее существенных проблем нашей страны на пути к развитию цифровых технологий эксперты называют недостаточность нормативной и правовой базы для регулирования сектора, отсутствие благоприятных условий для развития инновационного предпринимательства в сфере высоких технологий и, наконец, недостаточность цифровых компетенций у сотрудников для их применения в практической деятельности.

Сегодня уже сформированы основные направления, которые в будущем определят вектор развития новых кросс-канальных информационных решений и требуют регламентации в действующем законодательстве.

1. FinTech-сегмент формирует новую модель кредитно-финансового сектора, что обуславливает отказ от традиционных сервисов в пользу высокотехнологичных, в связи с чем возникает необходимость регулирования таких компаний наряду с финансовыми посредниками на уровне действующего законодательства.

2. Экономика совместного потребления формирует новый тип клиентоориентированного предложения, оказывающего влияние на кредитно-финансовую деятельность, что определяет возникновение новых продуктов и сервисов, ранее не регламентированных документами регулятора.

3. Применение блокчейн-технологий способствуют реструктуризации финансовой отрасли, формируя новые способы защиты продуктов и сервисов, подлежащих регламентации в законодательстве на уровне новой формы «услуги или сервиса».

4. Повсеместная цифровизация банковской системы и отказ от нетехнологичных сервисов способствуют изменению информационных данных и их наполнению, что требует усиления защиты персональных данных и регламентации в нормативно-законодательной базе.

5. Создание нового финансового сегмента — аналитики данных о клиенте — станет наиболее востребованным цифровым продуктом, использование которого позволит прогнозировать рост выручки и рентабельности. Целесообразно закрепление понятия «аналитика данных» в действующем законодательстве и определение допустимых границ и форм их использования.

6. Развитие робототехники и систем искусственного интеллекта определяет развитие новой эры операционных и информационных систем, реализуемых в различных юрисдикциях и не подлежащих регулированию со стороны стран-реципиентов, что предопределяет изменение в налоговом и валютном законодательстве и законодательстве, регулирующем внешнеэкономическую деятельность при проведении операций и платежей.

7. Облачные технологии приходят на смену традиционной инфраструктуре и вскоре станут ее основой, что формализует необходимость регламентации новых форм информационного риска и способов его идентификации, формируемого внешними факторами.

8. Информационные риски, создающие основные киберугрозы, станут основными рисками, с которыми столкнутся кредитно-финансовые институты в ближайшие годы, что определяет внедрение качественно нового алгоритма их прогнозирования и бэк-тестинга при использовании информационных систем, закрепленного на уровне действующего законодательства.

9. Вектор регулирования кредитно-финансового сектора сместится в сторону нормативной регламентации технологических решений, используемых в практической деятельности, в связи с чем возникает необходимость изменения алгоритма расчета капитала и обязательных нормативов с обязательным включением расширенного информационного риска (далее — РИС), входящего в состав операционного и учитывающего все возникающие IT-инциденты.

Новизна исследования состоит в создании комплексной системы управления и обеспечения информационной кибербезопасности Банка России с целью обеспечения контроля и защиты глобальных информационных данных кредитно-финансового сектора. С этой целью необходимо: формализовать методы прогнозирования и бэк-тестинга при использовании информационных

систем; сформировать единую систему управления и обеспечения информационной кибербезопасности для кредитно-финансовых организаций.

Основная часть

Различные научные гипотезы и сценарии дальнейшего развития финансового рынка определенно связывают с новой технологической революцией, задачей которой является имплементация и создание новых цифровых компетенций в условиях совершенствования и транснационализации банковской и расчетной систем.

Среди наиболее существенных проблем нашей страны на пути к развитию цифровых технологий эксперты называют недостаточность нормативной и правовой базы для регулирования сектора, отсутствия благоприятных условий для развития инновационного предпринимательства в сфере высоких технологий и, наконец, недостаточность цифровых компетенций у сотрудников для их применения в практической деятельности.

Сегодня уже сформированы основные направления, которые в будущем определяют вектор развития новых кросс-канальных информационных решений и требуют регламентации в действующем законодательстве.

Однако, с нашей точки зрения, не все направления нуждаются в детальной регламентации, поскольку фокус современной проблематики и перспектив на фоне происходящих технологических сдвигов сместился на системную оценку глобальных и национальных трендов, оказывающих влияние на кредитно-финансовую сферу и технологии, порождаемые современными вызовами и потребностями научно-технологического развития, с учетом стоящих перед Россией социально-экономических целей, имеющихся ресурсов и накопленных задач. Рассмотрим более подробно те направления, которые в большей степени формируют будущее современной кредитно-финансовой сферы с учетом совершенствования нормативно-законодательной основы регулирования кросс-канальных информационных технологий.

1. Регулирование FinTech-сегмента как новой формы финансового посредничества. На сегодняшний день существует не одна тысяча компаний, деятельность которых связана с предоставлением информационно-технологических услуг компаниям кредитно-финансового сектора. Специалисты обращают внимание на статистику по глобальным инвестициям в FinTech-сегмент, которые за последние пять лет выросли более чем в три раза, превысив 12 млрд долл. США. Для сравнения, согласно оценкам, банки по всему миру потратили на развитие информационных технологий около 215 млрд долл. США, в том числе на приобретение компьютерного оборудования, программного обеспечения, внутренние и внешние услуги [3]. Указанная статистика в полной мере объясняет угрозы от экспансии на рынок FinTech-компаний, главным образом сосредоточенных на развитии высокотехнологичных финансовых продуктов и сервисов.

Со стороны традиционных финансовых посредников наблюдается устойчивый спрос на данные услуги и сервисы, что позволяет говорить о зарождении нового «финансового сегмента», имеющего собственную финансовую платформу и консультантов, ориентированного на снижение операционных затрат и приобретение дорогостоящих информационно-технологических систем. Однако как показывает практика, в ст. 4 закона о банках и банковской деятельности [4] определен ограниченный перечень финансовых посредников, подлежащих обязательному регулированию.

Например, в европейском законодательстве регламентирован более широкий перечень организаций, реализующих функции платежных и финансовых посредников. Так, согласно ст. 1 Директивы 2015/2366 [5], в перечень субъектов, подлежащих обязательному регулированию, входит деятельность института электронных денег и некредитных организаций, реализующих функции финансовых посредников.

Кроме того, некоторые специалисты [6] обращают внимание на то, что в европейском законодательстве регламентирован ряд платежных и финансовых институтов, деятельность которых подлежит регулированию, к числу которых можно отнести:

— сервисы по инициации платежей;

— сервисы по агрегации платежной и расчетной информации;

— сервисы по переводу средств между физическими лицами.

Поскольку деятельность FinTech-компаний связана с реализацией функций по агрегации платежной и расчетной информации, а также инициацией расчетов, считаем, что наряду с банками и банковскими группами в законе о банках и банковской деятельности необходимо закрепить понятие «финансово-технологической компании».

Деятельность FinTech-компаний ориентирована на использование онлайн-моделей и моделей замкнутого взаимодействия, что определяет различные способы обмена информацией с кредитно-финансовыми организациями и их клиентами. Наиболее уязвимыми с точки зрения регулирования являются компании замкнутого типа, поскольку их деятельность сопряжена с двухсторонним обменом сообщениями без использования внешних информационных источников. В качестве положительной стороны их деятельности выступает качественное операционное обслуживание традиционных финансовых посредников по низким ценам, что позволяет существенно снизить затраты на обслуживание клиентов. Как правило, в качестве таких компаний выступают небольшие стартапы, активно внедряющиеся в сегмент международных расчетов. С другой стороны, такая форма предоставления услуг должна носить идентичный с банковской деятельностью порядок лицензирования и предоставляться через Банк России, что требует определения в действующем законе перечня услуг, оказываемых данными компаниями, подпадающими под контроль финансового регулятора.

2. Регламентация в законодательстве финансовых продуктов и сервисов совместного потребления и защиты от информационных рисков. Некоторые специалисты отмечают [2], что уже к 2020 г. потребители кредитно-финансовых услуг будут использовать сервисы не только традиционных банков, но и других организаций, предоставляющих аналогичные услуги на открытой платформе. Главной угрозой для традиционных банков выступает возможность отказа от традиционного владения активами и переход на децентрализованное владение, а также открывающиеся возможности для клиентов по оперативному выбору банка или поставщика финансовых услуг с использованием общего интерфейса. В научной и деловой литературе [7] подобная система получила название «Открытый банк» — Open Banking, в основе которой лежит объединение различных финансовых услуг с использованием общего интерфейса для повышения качества клиентского обслуживания.

В европейских странах использование продуктов и сервисов совместного потребления стандартизировано, и данный процесс находится в стадии дальнейшего развития. Например,

инициатива открытого банка поддерживается регуляторами в связи с вступлением в силу новой Европейской платежной директивы (PSD2) [5], а с января 2016 г. банки уже обеспечили доступ третьих сторон к транзакционной информации. Директива позволила клиентам использовать информационные онлайн-сервисы, получающие консолидированную информацию об их платежных счетах, вне зависимости от того, есть ли договор между информационным и финансовым провайдерами. В российском законодательстве отсутствует подобная стандартизация, в связи с чем считаем, что необходимо на уровне действующего законодательства закрепить определение «продукта и сервиса совместного потребления» [8], а также определить перечень провайдеров для их предоставления, порядок их лицензирования и стандартизации в рамках Европейской платежной директивы (PSD2) [9].

Кроме того, необходимо учитывать то обстоятельство, что обмен информационными данными в кредитно-финансовых услугах, как правило, связан с высокими рисками, что предопределяет необходимость применения политики информационной безопасности в части регулирования и управления рисками. Дополнительным звеном, нейтрализующим риски, может стать использование внутреннего стандарта «Знай своего клиента» для цели дополнительной проверки личности и превентивных мер по выявлению мошеннических действий.

Таким образом, сформированная экосистема в рамках реализации Open Banking Standard должна предусматривать внедрение алгоритма развития информационной инфраструктуры нового поколения, обеспечивающей защиту от информационных рисков и идентификацию пользователей с точки зрения антилегализационного законодательства для последующей интеграции нематериальных активов в монетизированные продукты с учетом разработки готовых технологий и бизнес-решений для управления и развития интеллектуальных систем в компаниях кредитно-финансового сектора. В связи с этим необходимо внести изменения в ст. 5 действующего Федерального закона № 115-ФЗ [10] для определения типа организации, подпадающей под специальное регулирование, и закрепления нормы по идентификации клиента [11] при использовании продуктов и сервисов совместного потребления с использованием открытых информационных платформ.

3. Регламентация в банковском законодательстве определения «блокчейн-продукта и блокчейн-сервиса».

На сегодняшний день использование блокчейна сравнимо с технологической революцией на рынке капитала, которая позволит отказаться от традиционной инфраструктуры банков и перейти на новую форму платежей и расчетов. Достаточно сказать, что проведенное в 2015 г. исследование позволило выявить 13 блокчейн-компаний, которые получили финансирование в размере свыше 365 млн долл. США [12], а к началу 2016 г. блокчейн-компании привлекли инвестиции на сумму более 1 млрд долл. для финансирования своего развития и операций [13].

В рамках проводимого исследования мы не раз упоминали об основных преимуществах использования данной технологии, как минимум выделив два ключевых аспекта. Первый заключается в возможности значительного удешевления инфраструктуры отрасли финансовых услуг. Второй заключается в том, что возможности применения блокчейн-технологий практически безграничны и охватывают широкий спектр операций — от финансирования сделок до сопровождения договоров.

С нашей точки зрения, в поле высокой неопределенности и рисков находится деятельность финансовых посредников, реализующих блокчейн-технологии во внерегуляционном режиме. В российском законодательстве уже определено понятие криптовалюты, эмиссия которой осуществляется с помощью блокчейна, однако не определен порядок регулирования деятельности самих посредников и более широкий перечень производимых ими продуктов и услуг с использованием данной технологии.

Необходимо отметить, что на сегодняшний день на официальном сайте Министерства финансов Российской Федерации размещен проект Федерального закона «О цифровых финансовых активах» [14], определяющий понятие цифрового финансового актива, цифровой транзакции и порядка обмена цифровых финансовых активов. Разделяя позицию некоторых авторов [15], полагаем, что существенным недостатком закона является его фрагментарность, что при его практическом использовании создаст ряд очевидных трудностей с учетом используемого понятийного аппарата. В законопроекте отсутствует определение блокчейн-технологии, блокчейн-сервиса и продукта, что создает пробелы в его практическом применении.

В связи с этим предлагаем на уровне данного законопроекта закрепить определение «блокчейн-продукт» и «блокчейн-сервис», порядок регулирования деятельности компаний, формализуемых как финансовые посредники, при предоставлении блокчейн-технологий в рамках децентрализованного реестра или перечня операций в одноуровневой сети для перевода активов с помощью Интернета без привлечения централизованной третьей стороны.

Дополнительно предлагаем закрепить определение «эмиссия с использованием блокчейн-технологии», порядок ее регулирования и возможности использования для цели развития российской банковской системы.

Не менее существенным недостатком в существующем законопроекте нам видится описание порядка обмена цифровых активов на рублевую единицу или иностранную валюту, тогда как в законе о валютном регулировании и валютном контроле не определен порядок расчета с цифровыми активами и условия для их возникновения, что определяет необходимость дополнения существующего валютного законодательства и приведения в соответствие с законопроектом.

4. Закрепление понятия «аналитика данных» в действующем законодательстве и определение допустимых границ и форм их использования. На сегодняшний день глобализация финансовых сервисов и их гиперподключенность создают высокое поле для индивидуализации финансовых продуктов и сервисов, делая их эксклюзивными. Определяющим условием для их создания является аналитика данных о клиенте, что формализует ее с точки зрения нового типа актива, не регламентированного в действующем законодательстве.

С нашей точки зрения, наряду с цифровыми активами, регламентированными в рамках проекта Федерального закона «О цифровых финансовых активах» [14], необходимо формализовать новый тип сенсорной технологии и коммуникационной сети как аналитику данных с учетом определения порядка его использования, стоимости, порядка обмена, покупки и реализации среди участников финансового рынка. Такая формализация позволит не только привести расчеты с данным типом активов к более точному ценообразованию и ориентированности на клиента, но и изменить модель формирования стоимости кредитно-финансовых продуктов и сервисов, исходя из существующих рисков и конкурентной стратегии на рынке.

5. Формализация методов прогнозирования и бэк-тестинга при использовании информационных систем. На сегодняшний день информационные риски, создающие основные киберугрозы, остаются основными рисками, с которыми в ближайшие годы столкнутся кредитно-финансовые институты и другие участники финансового рынка, что определяет необходимость внедрения качественно нового алгоритма его прогнозирования и бэк-тестинга при использовании информационных систем.

В отечественной практике регулирования внедрены стандарты [16] информационной безопасности, разработаны рекомендации в области стандартизации обеспечительных мер. Необходимо также отметить, что на официальном сайте регулятора опубликован проект положения «О требованиях к системе управления операционным риском в кредитной организации и банковской группе», устанавливающий требования к сфере информационных технологий и управлению операционными рисками. Банк России раскрывает лишь общие требования к управлению информационным риском (включая киберриск), а также риском информационных систем, дополнительно определяя требования к оценке достаточности капитала для покрытия потерь по операционному риску. Целью данного документа является регламентация требований к содержанию и ведению базы по событиям операционного риска для цели перспективы использования стандартизированного подхода к расчету капитала Базель III [17].

Вместе с тем документ содержит лишь общие требования и рекомендации, оставляя без внимания прикладные и методические вопросы для практической реализации. С нашей точки зрения, документ не раскрывает общие подходы к прогнозированию и бэк-тестингу при использовании информационных систем в условиях существующего операционного риска, что является необходимым условием для полноценной оценки качества системы управления операционными рисками начиная с 2020 г.

В научно-методологическом плане регламентации подлежит определение системы управления существенных рисков, обусловленных безопасностью информации, что предполагает описание следующих ключевых функций:

— выявление и идентификация рисков, связанных и обусловленных операционными рисками;

— процедура оценки рисков с использованием качественных или количественных методов, а также бэк-тестинга и прогнозирования ошибок ИС;

— определение лимитов и иных целевых показателей допустимого уровня риска ИС (с учетом оценки достаточности имеющегося капитала на покрытие принятого объема риска);

— установление контрольных значений лимитов и иных целевых показателей, по достижению которых необходима реализация мероприятий по минимизации риска ИС;

— контроль объемов принимаемых рисков ИС. Формирование отчетности об уровне принятого риска и результатах оценки эффективности применяемых методов управления рисками;

— совершенствование системы управления рисками ИС в случае выявления новых факторов операционного риска и отражения этих изменений в нормативных документах Банка России.

Отдельной регламентации подлежит процедура проверки выявления рисков ИС. К раскрытию разновидности риска ИС необходимо включить все направления его возникновения, а именно:

— риск внешнего и внутреннего мошенничества;

— риск нарушения управления доступом;

— риск утечки конфиденциальной информации;

— риск недоступности активов.

В то же время идентификация рисков ИС предполагает регламентацию подходов и методов управления рисками, целевых показателей допустимого уровня рисков, процедур выявления рисков.

Необходимо также учитывать, что обеспечение информационной кибербезопасности достигается путем применения различных организационных и технических мер, сгруппированных в сервисы (подсистемы) организации на основе методов управления доступом к информации, криптографической защиты, регистрации и анализа событий, обнаружения вторжений, мониторинга активностей, физической защиты информации [18].

Подобную точку зрения мы можем встретить и в работе М. А. Биганової [19], где автор обращает внимание на особенности институционального развития корпоративных структур инновационно ориентированного типа, включая кредитные организации, ориентированные на использование инновационных технологий в условиях обеспечения их комплексной безопасности.

Реализация функций прогнозирования и бэк-тестинга при использовании информационных систем в условиях существующего операционного риска предполагает дополнительную оценку и анализ:

— качества и ценности бизнес-продукта или сервиса для предотвращения потерь и повышения качества, поскольку в цифровом банковском бизнесе ни один продукт не может быть качественным, если он является небезопасным;

— взаимосвязанных, взаимодействующих и изменяющихся во времени элементов, условий и факторов, значимых с точки зрения сохранения и защиты информации. При создании системы обеспечения информационной кибербезопаности должны учитываться все слабые и наиболее уязвимые места, а также характер и возможные направления кибератак;

— используемых средств защиты при обычной работе пользователей информационных сетей;

— обязательности контроля для обеспечения своевременности выявления и пресечения попыток нарушения установленных правил и процедур безопасности, применения средств оперативного мониторинга и регистрации событий, охватывающих как санкционированные, так и несанкционированные действия;

— реагирования на угрозы с учетом перехода от «датацентричной» к «человекоцентричной» модели информационной безопасности, включая мониторинг инцидентов и событий на основе анализа поведения пользователей и учетных записей;

— обеспечения норм и требований международных стандартов защиты информации и банковской безопасности.

6. Создание единой системы управления и обеспечения информационной кибербезопасности для кредитно-финансовых организаций.

На сегодняшний день нормативно-законодательная база не предусматривает создание единой системы управления и обеспечения информационной кибербезопасности. В то же время Правительством РФ в 2018 г. утвержден план мероприятий по направлению «Информационная безопасность» в рамках Федеральной программы «Цифровая экономика РФ» [20], внесение изменений в Федеральные законы «О национальной платежной

системе», «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма» в целях обеспечения доступности финансовых услуг, а также снижения информационных рисков.

Анализ утвержденного плана мероприятий показал отсутствие комплексных мер по обеспечению мониторинга и защиты информации и единой платформы по противодействию киберпреступлений в кредитно-финансовой сфере. В данной связи считаем необходимым рекомендовать расширить и дополнить действующий план мероприятий по направлению «Информационная безопасность» в рамках Федеральной программы «Цифровая экономика РФ» созданием комплексной системы управления и обеспечения информационной кибербезопасности Банка России с целью обеспечения контроля и защиты глобальных информационных данных в части:

— идентификации угроз и рисков информационной кибербезопасности на основе систематического мониторинга деятельности по идентификации и оценке рисков внешней и внутренней среды. Такая оценка должна использоваться при принятии организационных и технических решений относительно методов, средств и механизмов защиты информации в системе обеспечения информационной кибербезопасности, а также при осуществлении деятельности по управлению рисками;

— управления доступом к информационным активам, определяющим ограничения круга лиц и технологических процессов, имеющих доступ к информационным активам, на основе обеспечения прав пользователей на уровне сети. Процедура управления доступом к информации должна осуществляться на уровне прав пользователей с учетом определенной персональной ответственности и прав. На практике необходимо разделять привилегированный или защищенный удаленный доступ к информации, определяемый для каждого вида информационного ресурса. С нашей точки зрения, ключевыми мерами по управлению доступом на сетевом уровне является защита периметра банковской сети и зонирование (сегментирование) информации внутри сети. Аналогичным образом должен определяться принцип хранения информации во внутренней или внешней сети с учетом степени ее критичности. Разграничение доступа на уровне сети целесообразно выполнять средствами межсетевого экранирования (включая соответствующие встроенные механизмы сетевых маршрутизаторов);

— безопасной разработки и тиражирования банковских продуктов. Осуществление обязательного анализа информационных рисков на всех стадиях разработки и внедрения банковских продуктов и услуг начиная с самых ранних этапов (подготовка концепции), а также принятие адекватных идентифицированным угрозам и рискам мер противодействия. При создании банковских продуктов необходимо предусматривать возможность перехода в красную тактику[1], заранее согласованную владельцем бизнес-продукта, и дополнительные меры по управлению риском (временное ограничение функциональности продукта, изменение уровня предоставляемого сервиса) как ответ на повышение уровня операционного риска свыше установленного порога;

— обеспечения непрерывности банковского бизнеса. Непрерывность бизнеса заключается в выполнении кредитно-финансовой организацией в условиях чрезвычайных ситуаций (экономических и политических кризисов, природных и техногенных катастроф, террористических угроз) на минимально необходимом уровне функций, без которых ее деятельность становится невозможна. Важно учитывать, что мероприятия по обеспечению непрерывности могут включать в себя создание процедур резервирования и восстановления информационных функций организации, в том числе для предотвращения чрезвычайных ситуаций в условиях вероятности их возникновения. Необходимость резервирования и восстановления функций определяется оценкой ущерба от их прерывания. Непрерывность бизнеса подразумевает также обеспечение непрерывности и надежности средств информационной защиты, которая не должна быть ниже надежности защищаемой системы;

— управления инцидентами информационной кибербезопасности для минимизации ущерба, вызванного реализованной угрозой, статистики по инцидентам, выявления причин возникновения инцидентов и принятия упреждающих мер по исключению подобных ситуаций в будущем;

— использования дополнительных средств защиты при использовании облачных технологий и личных мобильных устройств для повышения эффективности основной деятельности;

— выявления и предотвращения кибермошенничества недобросовестных сотрудников, а также злоумышленников, не являющихся клиентами кредитно-финансовой организации, в рамках системы фрод-мониторинга, нацеленной на снижение уровня убытков от мошенничества и безопасное развитие систем дистанционного банковского обслуживания в условиях роста рисков информационного кибермошенничества;

— регулярного мониторинга, контроля и ответственности системы обеспечения кибербезопасности информации. В рамках реализации принципов защиты информации на регулярной основе должен осуществляться мониторинг существующей системы кибербезопасности. Для этих целей целесообразно разработать и внедрить перечень индикаторов с целью выявления наиболее существенных рисков в существующей системе.

Выводы

Практическая реализация рекомендаций по совершенствованию нормативно-законодательной основы регулирования кросс-канальных информационных технологий позволит обеспечить развитие инструментальных видов контроля и защиты информации в кредитно-финансовой сфере, повысить степень взаимодействия FinTech-компаний с традиционными финансовыми посредниками при использовании онлайн-моделей и моделей замкнутого взаимодействия, раскрыть требования к финансовым продуктам и сервисам совместного потребления, закрепить понятие аналитики данных в действующем законодательстве в рамках определения допустимых границ и форм их использования, формализовать методы прогнозирования и бэк-тестинга при использовании информационных систем и предусмотреть создание единой системы управления и обеспечения информационной кибербезопасности для кредитно-финансовых организаций.

С нашей точки зрения, либерализация законодательной базы, регулирующей сферу информационных технологий в кредитно-финансовой сфере, позволит не только сформировать комплексную систему защиты информации как наиболее ценного актива, но и обеспечить непрерывность и устойчивость развития банковской деятельности, повысив степень информационного и операционного контроля в условиях активного развития технологий и инноваций в мировых финансах.

[1] Красная тактика — намеренное превышение допустимых объемов информации.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. DataFlowDiagramming: особенности построения моделей описания управления потоками данных в организационных системах / В. Е. Петеляк, Т. Б. Новикова, О. Е. Масленникова, М. В. Махмутова, А. М. Агдавлетова // Фундаментальные исследования. 2016. № 8 (часть 2). С. 323–327.

2. Fabunmi M. Management Information Systems in Education // Basic Text in Educational Planning / J. B. Babalola (ed.). Ibadan: Department of Educational Management, Bank of Ibadan, Ibadan. 2013.

3. Всемирный обзор ФинТех-сегмента, подготовленный PwC, 2016 год. URL: https://www.pwc.ru/ru

4. Федеральный закон от 2 декабря 1990 г. № 395-I «О банках и банковской деятельности».

5. Официальный сайт Европейской комиссии. Свод стандартов информационной безопасности. URL: https://www.cbr.ru/credit/Gubzi_docs/

6. Достов В. Л., Мамута М. В., Шуст П. М. Новое в регулировании розничных платежных услуг в европейском союзе // Деньги и кредит. 2016. № 7. С. 25–30.

7. Осипов Д. С. Тенденции развития банковского сектора и модернизация кредитных продуктов // Банковское кредитование. 2013. № 4. С. 87–96.

8. Федеральный закон от 27.06.2011 № 161-ФЗ «О национальной платежной системе».

9. Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No. 1093/2010, and repealing Directive 2007/64/EC // Official Journal of the European Union. L 337. 23.12.2015. Pp. 35–127.

10. Федеральный закон от 7 августа 2001 г. № 115-ФЗ «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма».

11. Положение Банка России от 15 октября 2015 г. № 499-П «Об идентификации кредитными организациями клиентов, представителей клиента, выгодоприобретателей и бенефициарных владельцев в целях противодействия легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма».

12. Инвестиции в биткойн. URL: https://gomedici.com/13-blockchain-bitcoin-companies-that-raised-serious-funding-in-2015/

13. Взгляд в будущее. URL: https://bitcointalk.org/index.php?topic=1235334.0

14. О финансовых активах: проект Федерального закона. URL: https://www. minfin.ru/ru/document/?id_4=121810&order_4=P_ DATE&dir_4=DESC&is_new_4=1&page_4=1&area_id=4&page_id=2104&popup=Y

15. Максуров А. А. Понимание транзакций в криптовалютной сфере в терминах проекта Федерального закона «О цифровых финансовых активах» // Экономика и управление. 2018. № 6. С. 26–30.

16. Свод рекомендаций в области информационной безопасности банковской деятельности. URL: https://www.cbr.ru/credit/Gubzi_docs/met/

17. Basel III: Finalising post-crisis reforms, December 2017.

18. Магомаева Л. Р. Информационно-коммуникативные технологии в мировой финансовой глобализации // Экономические и гуманитарные науки. 2017. № 10(309). С. 72–84.

19. Биганова М. А., Ересько А. В. Основные закономерности институционального развития корпоративных структур инновационно-ориентированного типа // Экономика и предпринимательство. 2015. № 9-1 (62-1). С. 526–529.

20. Ход реализации программы «Цифровая экономика РФ». URL: http://government.ru/rugovclassifier/614/events/

REFERENCES

1. Petelyak V. E., Novikova T. B., Maslennikova O. E., Makhmutova M. V., Agdavletova A. M. Data Flow Diagramming: features of building models for the description of data flow and management in organizational systems // Fundamental research. 2016. No. 8 (part 2). Pp. 323–327.

2. Fabunmi M. Management Information Systems in Education // Basic Text in Educational Planning. Ibadan, Department of Educational Management, Bank of Ibadan, Ibadan, 2013.

3. World FINTECH segment review prepared by PwC, 2016. (In Russ.). URL: https://www.pwc.ru/ru

4. Federal law No. 395-I dated December 2, 1990 “On banks and banking activities”. (In Russ.).

5. Official website of the European Commission Code of information security standards. (In Russ.). URL:https://www.cbr.ru/credit/Gubzi_docs/

6. Dostov V. L, Mamuta M. V., Shust P. M. New in regulation of retail payment services in the European Union // Money and credit. 2016. No. 7. Pp. 25–30. (In Russ.).

7. Osipov D. S. Trends in the development of the banking sector and modernization of credit products // Bank lending. 2013. No. 4. Pp. 87–96. (In Russ.).

8. Federal law dated 27.06.2011 No. 161-FL “On the national payment system”. (In Russ.).

9. Directive (EU) 2015/2366 of the European Parliament and Council dated November 25, 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repeating Directive 2007/64/EC // Official Journal of the European Union. L 337. 23.12.2015. Pp. 35–127.

10. Federal law No. 115-FL dated August 7, 2001 “On combating legalization (laundering) of revenues from crime and the financing of terrorism”. (In Russ.).

11. Regulation of the Bank of Russia No. 499-P of 15 October 2015 “On identification by credit institutions of clients, representatives of the client, beneficiaries and beneficial owners in order to counteract the legalization (laundering) of proceeds from crime and the financing of terrorism”. (In Russ.).

12. Investing in bitcoin. (In Russ.). URL: https://gomedici.com/13-blockchain-bitcoin-companies-that-raised-serious-funding-in-2015/

13. A look into the future. (In Russ.). URL: https://bitcointalk.org/index.php?topic=1235334.0

14. On financial assets: draft Federal law. (In Russ.). URL: https://www ahhh! minfin.ru/ru/document/?id_4=121810&order_4=P_DATE&dir_4=DESC&is_new_4=1&page_4=1 & area_id=4&page_id=2104 & popup=Y

15. Understanding of transactions in the field of crypto-currency in terms of the draft Federal Law "on digital financial assets" // Economics and management. 2018. No. 6. Pp. 26–30. (In Russ.).

16. Set of recommendations in the field of information security of banking activities. (In Russ.). URL: https://www.cbr.ru/credit/Gubzi_docs/met/

17. Basel III: Finishing post-crisis reforms, December 2017.

18. Magomaeva L. R. Information and communication technologies in the world financial globalization // Economic and human Sciences. 2017. No. 10(309). Pp. 72–84. (In Russ.).

19. Biganova M. A., Yeresko V. A. Main regularities of the institutional development of corporate structures innovation-oriented type // Economics and entrepreneurship. 2015. No. 9-1 (62-1). Pp. 526–529. (In Russ.).

20. Progress in the implementation of the program "Digital economy". (In Russ.). URL: http://government.ru/rugovclassifier/614/events/

Как цитировать статью: Магомаева Л. Р. Вопросы совершенствования нормативно-законодательной основы кросс-канальных информационных технологий кредитно-финансового сектора // Бизнес. Образование. Право. 2019. № 1 (46). С. 221–228. DOI: 10.25683/VOLBI.2019.46.174.

For citation: Magomaeva L. R. Issues of improvement of the legal and legislative basis of the cross-channel information technologies of the credit-financial sector // Business. Education. Law. 2019. No. 1 (46). Pp. 221–228. DOI: 10.25683/VOLBI.2019.46.174.

УДК 332.133.6
ББК 65.04

DOI: 10.25683/VOLBI.2019.46.140

Mishura Natalia Amirovna,
candidate of economics, researcher
of the Department of scientific and international activities,
Volzhsky branch
of Volgograd State University
Volzhsky
e-mail: mis.nata-volga@yandex.ru

Мишура Наталья Амировна,
канд. экон. наук, научный сотрудник
отдела научной и международной деятельности,
Волжский филиал
Волгоградского государственного университета,
г. Волжский,
e-mail: mis.nata-volga@yandex.ru

Публикация подготовлена в рамках поддержанного РФФИ научного проекта 18-410-340007 р_а «Кластерный подход к развитию сельских территорий региона: механизм реализации и апробация результатов»

The publication was prepared in the framework of the RFBR supported scientific project 18-410-340007 p_a "Cluster approach to the development of rural areas of the region: the mechanism of implementation and testing of results"

ВЫЯВЛЕНИЕ КЛАСТЕРНОГО ПОТЕНЦИАЛА ЭКОНОМИКИ В ОБЕСПЕЧЕНИИ УСТОЙЧИВОГО РАЗВИТИЯ СЕЛЬСКИХ ТЕРРИТОРИЙ РЕГИОНА

DETECTION OF THE CLUSTER POTENTIAL OF ECONOMICS IN PROVIDING SUSTAINABLE OF THE RURAL AREAS DEVELOPMENT

08.00.05 – Экономика и управление народным хозяйством
08.00.05 – Economics and management of national economy

Переход на траекторию устойчивого развития всех регионов РФ, и в частности сельских территорий, является важнейшей теоретической и практической проблемой отечественной экономики современного этапа. В связи с этим, как показано в статье, поиск путей и средств социально-экономического развития сельских территорий посредством реализации кластерного подхода представляется актуальной научной задачей. Представлено методическое обеспечение исследования кластерного потенциала посредством использования ресурсно-факторного подхода к количественной и качественной оценке кластерного потенциала экономики района. Обосновано, что развитие кластерного потенциала зависит от степени освоения ресурсов и возможности превращения их в факторы производства. В условиях регионализации экономической деятельности усиливается значение роли региональных и муниципальных органов власти по продвижению интересов предприятий и организаций на внутренний и внешний рынок. Обострение конкурентной борьбы в современной экономике увеличивает значимость изучения процессов кластерообразования как эффективного способа организации экономики районов и повышения конкурентоспособности сельских территорий. Определено,