УДК 004.056:336:351
DOI: 10.34020/1993-4386-2025-2-124-135

О МОДЕРНИЗАЦИИ МЕХАНИЗМА ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В КРЕДИТНО-ФИНАНСОВОЙ СФЕРЕ В ЦЕЛЯХ ДОСТИЖЕНИЯ ЭКОНОМИЧЕСКОЙ БЕЗОПАСНОСТИ ГОСУДАРСТВА

Н. В. Фадейкина
Новосибирский государственный университета экономики и управления «НИНХ»,
Новосибирск, Россия

Г. А. Фадейкин
ООО «Аудиторская фирма «Финансовая экспертиза»,
Новосибирск, Россия

О. В. Морозова
Новосибирский государственный университета экономики и управления «НИНХ»,
Новосибирск, Россия

В статье на основе множества определений понятий «информационная безопасность», «информационная безопасность кредитно-финансовой сферы» и «экономическая безопасность», сформулированных разными исследователями с учетом различных точек зрения, определена сущность информационной безопасности кредитно-финансовой сферы (КФС) как существенной составляющей экономической безопасности государства. Особое внимание уделено новым нормативным документам, регулирующим вопросы безопасности критической информационной инфраструктуры Российской Федерации, обеспечения информационной безопасности КФС, совершенствования системы управления операционным риском и комплексной модернизации корпоративных систем риск-менеджмента в организациях КФС, учитывающих новые условия обеспечения информационной безопасности КФС, существенно влияющей на обеспечение экономической безопасности государства.

Ключевые слова: информационная безопасность, кредитно-финансовая сфера, модернизация системы риск-менеджмент организаций кредитно-финансовой сферы, экономическая безопасность Российской Федерации.

Если рассматривать все сферы национальной экономики любой страны, то можно признать, что кредитно-финансовая сфера (КФС), регулируемая центральными (национальными) банками (в РФ – Банком России), наиболее подвержена риску. У отечественных организаций КФС (впрочем, как и у зарубежных) может возникнуть высокая вероятность или угроза, способная привести к возникновению незапланированных расходов (как по основной (финансовой), так и по административно-хозяйственной деятельности), в результате чего может снизиться уровень доходов и размер капитала, что, как правило, приводит не только к потери собственных ресурсов организации, но и к нарушению установленных Банком России (согласно положений главы X «Банковское регулирование и банковский надзор» Федерального закона «О Центральном банке Российской Федерации (Банке России)»[1] обязательных нормативов [1].

По мнению В. А. Гамзы и его партнеров, имеющих богатый опыт в области теории и практики обеспечения безопасности организаций КФС, термин «опасность» следует трактовать как «действия или обстоятельства, способные нанести ущерб установленному порядку функционирования организации, ее имуществу и инфраструктуре, воспрепятствовать достижению организацией уставных целей и привести в своих крайних формах к прекращению существования организации... С учетом сказанного выше, безопасность организации следует рассматривать как совокупные условия, при которых потенциально опасные для нее действия или обстоятельства предупреждены либо сведены к такому уровню, при котором они не способны нанести ущерб установленному порядку функционирования организации, сохранению и воспроизводству ее имущества и инфраструктуры, а также достижению организацией уставных целей» [2].

[1] Федеральный закон от 10 июля 2002 г. № 86-ФЗ (ред. от 24.07.2023) «О Центральном банке Российской Федерации».

В. О. Одинцов утверждает, что обеспечение экономической безопасности (ЭБ) – приоритетная задача подразделений, ответственных за безопасность в организации КФС. «В условиях повсеместного распространения новых технологий, которые закрепились, в том числе и в кредитно-финансовой сфере, первоочередной целью обеспечения экономической безопасности становится безопасность информационная» [3].

С 2014 г. в связи с изменением геополитической обстановки в РФ активизировалась деятельность Банка России в области подготовки (на основе международных и национальных стандартов[2]) и выпуска стандартов по обеспечению информационной безопасности (ИБ) организаций КФС, в том числе кредитных, составляющих в КФС самый большой сегмент. Одним из первых стандартов, значимых для темы данного исследования, был Стандарт Банка России «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Общие положения» СТО БР ИББС-1.0-2014. В нем присутствуют нормативные ссылки на Стандарт Банка России 2008 г., именуемый «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Общие положения» СТО БР ИББС-1.0-2008. Стандарт 2008 г. содержит *следующие сущностные характеристики ИБ* (применительно к субъектам КФС – организациям банковского сектора РФ), которые используются и в настоящее время; приведем основные из них.

Система ИБ (СИБ) представляет собой «совокупность защитных мер, защитных средств и процессов их эксплуатации, включая ресурсное и административное (организационное) обеспечение»;

система менеджмента ИБ (СМИБ) – это часть менеджмента организации КФС, предназначенная для создания, реализации, эксплуатации, мониторинга, анализа, поддержки и совершенствования системы обеспечения ИБ;

система обеспечения ИБ (СОИБ) – совокупность СИБ и СМИБ организации КФС;

область действия СОИБ – совокупность информационных активов и элементов информационной инфраструктуры организации КФС;

осознание необходимости обеспечения ИБ (осознание ИБ) – понимание руководством организации КФС необходимости самостоятельно на основе принятых в этой организации ценностей и накопленных знаний формировать и учитывать в рамках основной деятельности (бизнеса) прогноз результатов от деятельности по обеспечению ИБ, а также поддерживать эту деятельность адекватно прогнозу;

защитная мера – сложившаяся практика, процедура или механизм, которые используются для уменьшения риска нарушения ИБ в организации КФС;

угроза ИБ – угроза нарушения таких свойств ИБ, как доступность, целостность или конфиденциальность информационных активов организации КФС;

уязвимость ИБ – слабое место в инфраструктуре организации КФС, включая СОИБ, которое может быть использовано для реализации или способствовать реализации угрозы ИБ;

ущерб – утрата активов, повреждение (утрата свойств) активов и (или) инфраструктуры организации или другой вред активам и (или) инфраструктуре организации КФС, наступивший в результате реализации угроз ИБ через уязвимости ИБ;

инцидент ИБ – событие, указывающее на свершившуюся, предпринимаемую или вероятную реализацию угрозы ИБ, то есть реализацию нарушения свойств ИБ информационных активов организации КФС;

нарушитель ИБ – субъект, реализующий угрозы ИБ организации КФС, нарушая предоставленные ему полномочия по доступу к активам организации КФС или по распоряжению ими;

риск нарушения ИБ – риск, связанный с угрозой ИБ;

оценка риска нарушения ИБ – систематический и документированный процесс выявления, сбора, использования и анализа информации, позволяющей провести оценивание рисков нарушения ИБ, связанных с использованием информационных активов организации КФС на всех стадиях их жизненного цикла;

аудит ИБ – систематический, независимый и документируемый процесс получения свидетельств деятельности организации КФС по обеспечению ИБ, установления степени выполнения в организации КФС критериев ИБ, а также допускающий возможность формирования профессионального аудиторского суждения о состоянии ИБ организации КФС.

Согласно вышеупомянутому Федеральному закону № 86-ФЗ, деятельность организаций КФС контролируется и регулируется в установленном законом порядке с учетом тех нормативных правовых актов (НПА), которые утверждены Президентом РФ[3], Правительством РФ, а также нормативными

[2] Одним из первых стандартов по информационной безопасности в РФ был «ГОСТ Р ИСО/МЭК 27001-2006. Национальный стандарт Российской Федерации. Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования» (утв. Приказом Ростехрегулирования от 27.12.2006 г. № 375-ст); он был разработан на основе Международного стандарта ИСО/МЭК 27001:2005 «Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования» (ISO/IEC 27001:2005 «Information technology - Security techniques - Information security management systems – Requirements»).

[3] Напомним, что в «Стратегии экономической безопасности Российской Федерации на период до 2030 года», утв. Указом Президента РФ от 13 мая 2017 г. № 208, к основным вызовам и угрозам ЭБ (в отношении КФС) отнесена «подверженность финансовой системы Российской Федерации глобальным рискам (в том числе в результате влияния спекулятивного иностранного капитала), а также уязвимость информационной инфраструктуры финансово-банковской системы». В развитие положений указанной Стратегии был принят Федеральный закон от 26 июля 2017 г. № 187-ФЗ (ред. от 10.07.2023) «О безопасности критической информационной инфраструктуры Российской Федерации», где к ее субъектам были отнесены организации КФС (т.е. организации банковской сферы и иных сфер финансового рынка).

актами Банка России, которые содержат положения, ограничения и рекомендации по обеспечению ИБ, в том числе в организациях КФС.

В контексте темы данного исследования, рассмотрению подлежат НПА, содержащие положения о развитии ИБ КФС. Одним из первых таких документов были *«Основные направления развития информационной безопасности кредитно-финансовой сферы на период 2019-2021 годов»* (утв. Банком России), которые были разработаны с учетом:

– *Доктрины информационной безопасности Российской Федерации*[4], представляющей собой «систему официальных взглядов на обеспечение национальной безопасности Российской Федерации в информационной сфере» и содержащей такие понятия, как «информационная безопасность Российской Федерации», «обеспечение информационной безопасности», «силы обеспечения информационной безопасности», «средства обеспечения информационной безопасности», «система обеспечения информационной безопасности», «информационная инфраструктура Российской Федерации», а также разделы «Национальные интересы в информационной сфере», «Основные информационные угрозы и состояние информационной безопасности», «Стратегические цели и основные направления обеспечения информационной безопасности», «Организационные основы обеспечения информационной безопасности»;

– *Стратегии развития информационного общества в Российской Федерации на 2017-2030 годы*[5] (далее – Стратегия ИО), определившей «цели, задачи и меры по реализации внутренней и внешней политики Российской Федерации в сфере применения информационных и коммуникационных технологий, направленные на развитие информационного общества, формирование национальной цифровой экономики, обеспечение национальных интересов и реализацию стратегических национальных приоритетов».

После утверждения Стратегии ИО (буквально следом) был принят *Федеральный закон от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации»*. Закон был чрезвычайно необходим для реализации рассматриваемых «Основных направлений развития информационной безопасности кредитно-финансовой сферы на период 2019-2021 годов»[6] (далее – Основные направления 2019-2021), в которых были определены и структурированы:

– «ключевые цели и задачи развития ИБ и киберустойчивости», а именно: «обеспечение ИБ и киберустойчивости в целях финансовой стабильности каждой организации финансового рынка (ФР); обеспечение операционной надежности и непрерывности деятельности организаций кредитно-финансовой сферы; противодействие компьютерным атакам (в том числе при использовании инновационных финансовых технологий); защита прав потребителей финансовых услуг»;

– предпосылки и тренды; задачи и основные направления деятельности Банка России в области ИБ; правовое регулирование[7]; обеспечение ИБ и киберустойчивости инфраструктуры; обеспечение ИБ и киберустойчивости прикладного программного обеспечения (ПО); обеспечение ИБ и киберустойчивости технологий обработки данных; обеспечение ИБ и киберустойчивости финансовых технологий;

– подготовка кадров и обеспечение доверия граждан к цифровой среде; международное сотрудничество; Национальная программа «Цифровая экономика Российской Федерации»[8]; деятельность Центра компетенций по обеспечению ИБ и противодействию кибератакам в КФС; надзорная деятельность, осуществляемая Банком России «с учетом лучшего мирового опыта, накопленного ведущими международными организациями, в том числе Советом по финансовой стабильности (FSB)».

Для повышения эффективности функционирования Правительства РФ, ФСБ России, Банка России и других федеральных структур в области обеспечения ИБ *Президентом России 1 мая 2022 г. был принят Указ № 250 «О дополнительных мерах по обеспечению информационной безопасности Российской Федерации», в который четыре раза*

[4] Утв. Указом Президента РФ от 5 декабря 2016 г. № 646.

[5] Утв. Указом Президента РФ от 9 мая 2017 г. № 203.

[6] Указанные Основные направления 2019-2021 соответствовали мировому опыту и лучшим практикам в области обеспечения ИБ КФС и управления риском ИБ (киберриском): при их разработке использовался опыт Национального института стандартов и технологий США, Денежно-кредитного управления Сингапура, Европейской службы банковского надзора, Международной организации комиссий по ценным бумагам, Комитета по платежным и рыночным инфраструктурам Банка международных расчетов, Базельского комитета по банковскому надзору».

[7] В этой части была проиллюстрирована взаимосвязь Основных направлений 2019-2021 с Конституцией РФ, Доктриной информационной безопасности Российской Федерации, статьями 57.4, 76.1, 76.4-1 Федерального закона № 86-ФЗ «О Центральном банке Российской Федерации (Банке России)», статьей 27 Федерального закона от 27 июня 2011 г. № 161-ФЗ «О национальной платежной системе» (в ред. от 19.12.2023), Национальной программой «Цифровая экономика Российской Федерации», которая была утверждена протоколом заседания Президиума Совета при Президенте РФ по стратегическому развитию и национальным проектам от 4 июня 2019 г. № 7.

[8] Речь идет о необходимости согласованности текста Основных направлений 2019-2021 с механизмом реализации НП «Цифровая экономика Российской Федерации».

вносились изменения и дополнения (Указ действует в ред. от 13.06.2024 г. № 500). Выполнение Указа в отношении организаций КФС является достаточно сложным, хотя Банк России своевременно инициировал внесение изменений и дополнений в вышеуказанный Федеральный закон № 86-ФЗ[9] и утвердил множество нормативных актов и стандартов, в том числе:

– Стандарт Банка России «Безопасность финансовых (банковских) операций. Управление инцидентами, связанными с реализацией информационных угроз, и инцидентами операционной надежности. О формах и сроках взаимодействия Банка России с кредитными организациями, некредитными финансовыми организациями и субъектами национальной платежной системы при выявлении инцидентов, связанных с реализацией информационных угроз, и инцидентов операционной надежности»[10];

– Положение Банка России от 17 октября 2022 г. № 808-П «О требованиях к обеспечению защиты информации при осуществлении деятельности в сфере оказания профессиональных услуг на финансовом рынке в целях противодействия осуществлению незаконных финансовых операций, обязательных для лиц, оказывающих профессиональные услуги на финансовом рынке, к обеспечению бюро кредитных историй защиты информации, указанной в статье 4 Федерального закона "О кредитных историях", при ее обработке, хранении и передаче сертифицированными средствами защиты, а также к сохранности информации, полученной в процессе деятельности кредитного рейтингового агентства»;

– «Методические рекомендации (от 26.10.2023 г. № 14-МР) по выполнению кредитными и некредитными финансовыми организациями мероприятий по обеспечению *безопасности критической информационной инфраструктуры Российской Федерации* в части информирования федерального органа исполнительной власти, уполномоченного в области обеспечения функционирования государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации, о компьютерных инцидентах, результатах мероприятий по реагированию на них и принятии мер по ликвидации последствий компьютерных атак»;

– Методические рекомендации (от 26.10.2023 г. № 15-МП) по взаимодействию кредитных организаций с МВД России и ФСБ России в целях принятия процессуальных решений при проведении компьютерных атак в отношении объектов критической информационной инфраструктуры» и др.

К концу 2022 г. Банк России изменил требования к специалистам, работающим в организациях КФС в области ИБ, – они полностью должны отвечать требованиям Профессионального стандарта (ПС) «Специалист по информационной безопасности в кредитно-финансовой сфере»[11] (наименование вида профессиональной деятельности (ПД) данного ПС – «обеспечение ИБ в организациях КФС»; основная цель вида ПД – «управление рисками ИБ, обеспечение защиты информации, операционной надежности (киберустойчивости) в организациях КФС»).

Банк России ужесточил контроль за деятельностью организаций КФС в области обеспечения ИБ в части соблюдения ими не только НПА и нормативных актов Банка России, но и корпоративных документов, регулируемых проведение аудита и деятельность департаментов (служб) обеспечения ИБ и ЭБ в указанных организациях.

По мнению В. В. Ерохина, основной задачей департамента (службы) ИБ организации КФС является «отслеживание, предотвращение и ведение расследований инцидентов нарушения правил работы с информационным и программным обеспечением организации. Также в полномочия работников департамента входит проверка поступающего в организацию аппаратного и ПО на наличие вирусов, программных и аппаратных закладок, подслушивающих устройств и т.д. Департамент ИБ также несет ответственность за поддержку функционирования Автоматизированной системы разграничения доступа к информационному и программному обеспечению (АСРДкИПО), поэтому его работники должны проходить особую проверку (на полиграфе). «Who guards the guardians?» (Кто следит за следящими?) – философский вопрос, который до сих пор не решен, поэтому подбор персонала в департамент ИБ организаций КФС должен осуществлять особо строго» [4, с. 57]. Ответственность за обеспечение функционирования АСРДкИПО ложится именно на работников департамента ИБ, поэтому «данное подразделение можно классифицировать как подразделение высшего уровня доступа. При зачислении в штат департамента ИБ организации КФС специалисты, имеющие соответствующее образование и опыт, должны проходить особую проверку» [4, с. 71], в том числе подтверждающую наличие у кандидатов профессиональных компетенций и необходимого уровня квалификации (УК) в области исполнения следующих обобщенных трудовых функций (ОТФ),

[9] В Законе № 86-ФЗ появились новые статьи (57.5-1, 57.5-2, внесены изменения и дополнения в статью 76.9-6 и другие статьи).

[10] Стандарт СТО БР БФБО-1.5-2023 принят и введен в действие приказом Банка России 8 февраля 2023 г.

[11] Данный стандарт утвержден приказом Минтруда России от 28 ноября 2022 г. № 739н и зарегистрирован в Минюсте России 22 декабря 2022 г.

указанных в ПС «Специалист по информационной безопасности в кредитно-финансовой сфере»:

– *организация процессов обеспечения ИБ в организациях КФС* (УК – 8; в состав данной ОТФ входят такие трудовые функции (ТФ), как «организация управления рисками ИБ на высшем управленческом уровне в организациях КФС; организация обеспечения защиты информации и операционной надежности (ОН), то есть киберустойчивости, на высшем управленческом уровне (ВУУ) в организациях КФС; контроль процедур управления рисками ИБ и обеспечения защиты информации и ОН (киберустойчивости) на ВУУ в организациях КФС; совершенствование системы управления рисками ИБ, обеспечение защиты информации и ОН (киберустойчивости) на ВУУ в организациях КФС»);

– *контроль обеспечения ИБ и обеспечение операционной надежности (киберустойчивости) в организациях КФС* (УК – 7; ТФ – «проведение контрольных проверок работоспособности и оценка эффективности применяемых программно-аппаратных средств защиты информации в организациях КФС; контроль процессов защиты информации и обеспечения ОН (киберустойчивости) в организациях КФС; реализация программ повышения осведомленности организаций КФС по вопросам защиты информации и обеспечения ОН (киберустойчивости) в организациях КФС»);

– *методологическое обеспечение процессов ИБ в организациях КФС* (УК – 7; ТФ – «разработка политики в области обеспечения ИБ по вопросам управления рисками ИБ, обеспечения ОН (киберустойчивости) и защиты информации в организациях КФС; разработка методологии обеспечения защиты информации и ОН (киберустойчивости) в организациях КФС; разработка методологии управления рисками ИБ в организациях КФС; разработка методологии выявления инцидентов ИБ, реагирования на них и восстановления после их реализации в организациях КФС»);

– *аналитическое и организационное сопровождение деятельности по управлению рисками ИБ в организациях КФС* (УК – 7; ТФ – «определение угроз ИБ в организациях КФС; выявление, идентификация и оценка рисков ИБ в организациях КФС; сбор и регистрация информации о выявленных рисках ИБ в организациях КФС; разработка мероприятий, направленных на уменьшение негативного влияния рисков ИБ в организациях КФС; мониторинг рисков ИБ и контроль показателей уровня рисков ИБ в организациях КФС; обеспечение ИБ значимых объектов критической информационной инфраструктуры в организациях КФС»);

– *управление инцидентами ИБ в организациях КФС* (УК – 7; ТФ – «выявление и регистрация инцидентов ИБ, в том числе обнаружение компьютерных атак, в организациях КФС; реагирование на инциденты ИБ в организациях КФС; восстановление функционирования бизнес-процессов и технологических процессов и объектов информатизации после реализации инцидентов ИБ в организациях КФС»);

– *обеспечение функционирования систем и средств защиты информации в организациях КФС* (УК – 6; ТФ – «проведение работ по установке, настройке и техническому обслуживанию систем и средств защиты информации в организациях КФС; администрирование систем и средств защиты информации в организациях КФС; реализация процессов обеспечения ОН (киберустойчивости) в организациях КФС»).

Согласно рассматриваемого ПС, *главной целью ПД специалиста по ИБ* в организациях КФС, как уже было указано выше, является *управление рисками ИБ, обеспечение защиты информации и операционной надежности (киберустойчивости).* С точки зрения Председателя Ассоциации пользователей стандартов по информационной безопасности (АБИСС) А. Харыбиной, «принципиально новым в данном ПС является факт наделение ИБ-специалистов *обязанностями по управлению рисками*. Тем самым регулятор фиксирует в ПС свою стратегическую линию, ранее уже реализованную в ряде нормативных актов, – *внедрение риск-ориентированного подхода и усиление работы по управлению рисками ИБ в КФС.* Такой подход в качестве ключевого одобряют не все представители банковского сообщества, так как зачастую он противоречит бизнес-потребностям организаций КФС, которые в первую очередь являются коммерческими структурами». Описывая содержание ПС, А. Харыбина отмечает, что в стандарте «выделяется пять типов специалистов: руководитель, аналитик, методолог, специалист по ИБ, специалист по инцидентам. Документ описывает их функции, необходимые знания и умения, а также требования к образованию и практическому опыту. Так, руководитель ИБ-подразделения в организации КФС должен иметь высшее образование в области ИБ или непрофильное высшее плюс допобразование по ИБ (512 часов). При этом он должен обладать не менее чем пятилетним опытом работы в сфере ИБ, из них не менее трех лет – на позиции руководителя. Профильное образование по ИБ должны также иметь все остальные перечисленные выше специалисты ИБ-подразделения» [5].

В системе ПС группы *06 «Связь, информационные и коммуникационные технологии»* присутствует 55 стандартов, 10 из них, включая вышеупомянутый стандарт «Специалист по информационной безопасности в кредитно-финансовой сфере», имеют непосредственное отношение к обеспечению ИБ в организациях КФС. В состав указанной группы 10-ти входят также: *ПС «Специалист по безопасности компьютерных систем и сетей»*, целью вида профессиональной деятельности (ЦВПД) которого

является обеспечение безопасности информации в компьютерных системах и сетях в условиях существования угроз их ИБ; *ПС «Специалист по защите информации в телекоммуникационных системах и сетях»*, ЦВПД которого – обеспечение защиты средств связи сетей электросвязи от несанкционированного доступа к ним в условиях существования угроз их ИБ; *ПС «Специалист по защите информации в автоматизированных системах»*, ЦВПД которого – повышение защищенности автоматизированных систем, функционирующих в условиях существования угроз в информационной сфере и обладающих информационно-технологическими ресурсами, подлежащими защите; *ПС «Специалист по технической защите информации»*, ЦВПД которого – предотвращение утечки информации ограниченного доступа по техническим каналам в результате несанкционированного доступа к информации и специальных воздействий на информацию в целях ее добывания, уничтожения, искажения и блокирования доступа к ней; *ПС «Специалист по контролю качества информационно-коммуникационных систем и сервисов»*, ЦВПД которого – обеспечение соответствия характеристик инфокоммуникационных систем и предоставляемых на их основе сервисов заданным требованиям; *ПС «Специалист по большим данным»*, ЦВПД которого – создание ИТ нового поколения, обеспечивающих экономически эффективное извлечение полезной информации из больших объемов разнообразных данных путем высокой скорости их сбора, обработки и анализа, и применение этих технологий в информационно-аналитической деятельности, в системах управления и принятия решений, а также для разработки на их основе новых продуктов и услуг.

Следует также подчеркнуть, что в некоторых *ПС 8-ой группы «Финансы и экономика»* указана необходимость наличия у специалиста знаний в области обеспечения ИБ. Это касается следующих стандартов: *ПС «Специалист в области национальной платежной системы»; ПС «Специалист по микрофинансовым операциям», ПС «Специалист по ипотечным кредитам и займам», ПС «Специалист по потребительскому кредитованию», ПС «Специалист по корпоративному кредитованию», «ПС «Специалист по внутреннему контролю (внутренний контролер)».* Что касается ПС «Специалист по управлению рисками», то в нем в отношении ТФ «Координация работ по технико-информационному обеспечению системы стратегического управления рисками» определены знания «положений национальных и международных стандартов и руководств в области управления ИТ и ИБ».

По мнению Н. В. Фадейкиной и ее партнеров, «риском необходимо грамотно управлять, используя все рычаги и методы, позволяющие прогнозировать наступление рискового события. Особенно это важно для организаций КФС, которые сталкиваются с многочисленными рисками: кредитным, операционным, рыночным, стратегическим, репутационным, риском ликвидности и др.

Управление рисками в организациях КФС:

– представляет собой непрерывный процесс, охватывающий всю деятельность указанных организаций;

– используется при разработке и реализации корпоративной стратегии;

– применяется на каждом уровне организации и в каждом ее подразделении, включает анализ портфеля рисков на уровне организации;

– нацелено на выявление событий, способных оказать влияние на организацию КФС и управление рисками таким образом, чтобы они не превышали риск-аппетита акционеров;

– дает руководству и совету директоров (наблюдательному совету) разумную гарантию достижения целей;

– обеспечивает достижение целей по одному или нескольким отдельным, но пересекающимся критериям, в том числе в области обеспечения информационной и экономической безопасности.

Политика банка в области риск-менеджмента представляет собой заявление высшего руководства об общих намерениях, руководящих принципах и направлениях его деятельности в области риск-менеджмента, эффективность которого является одним из факторов обеспечения информационной и экономической безопасности организации КФС [6-7].

Новый этап развития процесса обеспечения информационной безопасности в КФС наступил после одобрения Советом директоров Банка России 22 мая 2023 г. *«Основных направлений развития информационной безопасности кредитно-финансовой сферы на период 2023-2025 годов»* (далее – Основные направления 2023-2025), где были подведены итоги реализации Основных направлений 2019-2021 и определено содержание следующих новых направлений развития ИБ КФС на период 2023-2025 гг.

1. «*Защита прав потребителей финансовых услуг и повышение уровня доверия к цифровым технологиям*» (в том числе в области: противодействия компьютерным атакам; противодействия совершению операций без согласия клиентов, социальной инженерии; обеспечения финансовой киберграмотности).

Предварительные результаты реализации Основных направлений 2023-2025 подтверждают тот факт, что в целях *противодействия компьютерным атакам* совершенствуется информационный обмен между Банком России и организациями КФС по тактике, технике совершения компьютерных атак. Для повышения эффективности реагирования на компьютерные атаки, цепочки компьютерных

атак и качество расследования киберинцидентов осуществляется дальнейшее развитие информационного взаимодействия ФинЦЕРТ[12] с организациями КФС.

В целях *противодействия совершению операций без согласия клиентов, социальной инженерии* совершенствуются механизмы сохранения и возврата денежных средств; а в рамках мероприятий по *обеспечению финансовой киберграмотности* «реализуются *Программы по повышению финансовой киберграмотности и пропаганде кибергигиены* для различных категорий населения, в том числе для лиц с низким уровнем дохода и социально незащищенных категорий населения. Для этого реализуются как информационно-просветительские, так и образовательные мероприятия с применением современных педагогических технологий и форматов продуктивного, дифференцированного обучения, а также с реализацией компетентностного подхода и развивающего обучения». Осуществляется применение Единой рамки компетенций по финансовой грамотности (ЕРКФГ) в вопросах повышения финансовой киберграмотности и кибергигиены. ЕРКФГ «содержит базовые компетенции по финансовой грамотности для учащихся школьного возраста (от 15 лет), взрослого населения и является основой для развития различных инструментов повышения финансовой грамотности (включая вопросы финансовой киберграмотности и кибергигиены): образовательные программы, программы дополнительного образования, олимпиады и т.д. ЕРКФГ описывает общие разделы и образовательные результаты по темам на двух уровнях: базовом и продвинутом».

2. «*Создание условий для безопасного внедрения цифровых, платежных технологий и достижения технологического суверенитета*» (в том числе развитие регулирования и последующего надзора, национальной платежной инфраструктуры и цифрового рубля (ЦР), экспериментальных правовых режимов и регулятивной «песочницы», а также обеспечение технологического суверенитета).

Банк России «создает условия для обеспечения ИБ и киберустойчивости цифровых и платежных технологий через *регулирование и последующий надзор* по следующим приоритетным направлениям: цифровой профиль; маркетплейс; открытые интерфейсы на ФР (Open API), открытые банковские интерфейсы в национальной платежной системе (НПС), а также интерфейсы небанковских поставщиков платежных услуг; электронное хранение документов; экосистемы; Единая информационная система проверки сведений об абоненте (ЕИС ПСА); обеспечение ИБ для новых способов инициирования платежей и переводов (смарт-устройства и др.); Единая биометрическая система и коммерческие биометрические системы; новые субъекты НПС (небанковские поставщики платежных услуг и другие); оборот данных организаций КФС в части их ИБ, включая целостность; среда доверия при удаленном предоставлении финансовых услуг и программ для реализации протоколов ИБ. В рамках дальнейшего совершенствования регулирования будут реализованы инициативы, связанные с формированием правовых механизмов обеспечения ИБ и киберустойчивости в области цифровых и платежных технологий. В целях проведения единой государственной политики в сфере ИБ и киберустойчивости указанные подходы будут согласованы с ФСБ России и ФСТЭК России».

В качестве приоритетных направлений в *области развития национальной платежной инфраструктуры и ЦР* Банком России заявлены: «развитие стандартов ИБ, обеспечивающих расширение доступа к платежной системе Банка России, в том числе нерезидентов; развитие Системы быстрых платежей (СБП) в части: внедрения механизмов ИБ для интероперабельности СБП; расширения доступа к СБП, в том числе нерезидентов; развития системы управления рисками ИБ; обеспечения ИБ и надежности мобильного приложения СБПэй; развитие Системы передачи финансовых сообщений».

Банк России планирует «расширить набор надзорных инструментов и практик, учитывающих

[12] ФинЦЕРТ (Financial Computer Emergency Response Team), Центр мониторинга и реагирования на компьютерные атаки в КФС с 1 июля 2015 г. функционировал в статусе структурного подразделения Главного управления безопасности и защиты информации Банка России. В настоящее время ФинЦЕРТ является Центром взаимодействия и реагирования Департамента информационной безопасности Банка России, в информационном обмене с ним участвуют более 1200 организаций, в том числе все организации КФС. По данным Банка России, «на базе ФинЦЕРТ создана система информационного обмена (ИО) между участниками ФР, правоохранительными органами, провайдерами и операторами связи, системными интеграторами, разработчиками антивирусного ПО и другими организациями, работающими в сфере ИБ. Участники ИО сообщают о выявленных ими угрозах и совершенных на них атаках, ФинЦЕРТ дает рекомендации по противодействию этим рискам. Это помогает оперативно реагировать на возникающие угрозы в финансовой сфере, не допускать их распространения, минимизировать потери организаций КФС и их клиентов. Подключиться к системе ИО может любой участник ФР или организация, работающая в сфере защиты информации в финансовой сфере. Автоматизированная система обработки инцидентов (АСОИ ФинЦЕРТ) – основной канал передачи информации об инцидентах в Банк России. Резервные способы передачи информации используются только в случаях отсутствия телекоммуникационной доступности личного кабинета участника ИО и (или) отсутствия технической возможности передачи информации». / Официальный сайт Банка России. URL: https://cbr.ru/information_security/fincert/ (дата обращения: 11.04.2025).

принцип соразмерности и разумности для надлежащего выполнения поднадзорными организациями КФС требований по защите информации и операционной надежности», подчеркивая при этом необходимость развития «практических навыков работников подразделений ИБ по реагированию на компьютерные атаки и расследованию киберинцидентов в отношении цифровых и платежных технологий», получаемых в рамках программы практико-ориентированного обучения.

Для реализации *экспериментальных правовых режимов и регулятивной «песочницы»* Банк России проводит исследование инновационных финансовых продуктов, предложенных участниками рынка, на предмет ИБ и киберустойчивости в рамках регулятивной "песочницы", с учетом комплексного анализа риска ИБ (киберриска). Аналогичный подход будет применяться к новым бизнес-моделям и решениям в рамках экспериментальных правовых режимов. По результатам экспериментов Банк России продолжит работу по совершенствованию правового регулирования в области ИБ и киберустойчивости.

В целях *обеспечения технологического суверенитета*, то есть снижения уровня риска технологической зависимости организаций КФС и инфраструктуры от внешних поставщиков Банк России осуществляет координацию деятельности указанных организаций, в том числе применяет следующие подходы: «определение приоритетов импортозамещения по номенклатуре программного и аппаратного обеспечения; реализация механизма оценки зрелости решений российских производителей и поставщиков ИТ; определение вариантов обработки рисков использования иностранных ИТ; распределение задач по техническому тестированию среди организаций КФС, а также обобщение и раскрытие полученных результатов тестирования; осуществление взаимодействия с ответственными федеральными органами исполнительной власти, российскими производителями и поставщиками ИТ; обмен опытом по данной тематике, в том числе с организациями из иных отраслей экономики; осуществление контроля за реализацией вопросов импортозамещения в рамках действующих полномочий Банка России по обеспечению ОН» и др.

3. «*Обеспечение контроля рисков ИБ, ОН для непрерывности оказания банковских и финансовых услуг*» (в том числе: а) развитие RegTech-проектов (технологий, используемых регуляторами для повышения эффективности контроля и надзора за деятельностью организаций КФС и других участников ФР) и SupTech-проектов (технологий, используемые организациями КФС для повышения эффективности выполнения требований регулятора)[13]; б) проведение киберучений; в) реализация практики риск-профилирования; г) развитие аутсорсинга информационных технологий и использование облачных сервисов.

В ходе мероприятий по *развитию RegTech- и SupTech-проектов* осуществляется совершенствование системы внешнего аудита ИБ, внедрение системы мониторинга и анализа операционных рисков организаций КФС, создание правовых условий для аутсорсинга ИТ и использования организациями КФС облачных услуг финансовыми организациями.

В рамках *проведения киберучений* предусмотрено: проведение киберучений (стресс-тестирований) деятельности организаций КФС; оценка киберриска для целей интеграции в надзорную оценку операционного риска в части: риска ИБ, связанного с возможным совершением операций без согласия клиентов, и риска ИБ, связанного с возможным нарушением ОН. Результаты киберучений используются Банком России в системе мониторинга и анализа операционных рисков организаций КФС.

Для *реализации практики риск-профилирования* Банк России внедряет механизмы формирования риск-профиля поднадзорных организаций для оценки фактических рисков ИБ и ОН. Для этого запланировано проведение следующих мероприятий: «разработка метрик оценки киберриска, включая метрики оценки рисков поставщиков услуг аутсорсинга, в части рисков ИБ и ОН» (в том числе риска ИБ; риска ИБ, связанного с возможным совершением операций без согласия клиентов; риска ИБ, связанного с возможным нарушением операционной надежности); «развитие механизма риск-профилирования финансовых организаций по киберриску»; «мониторинг и выявление киберрисков, влияющих на финансовую устойчивость и ОН крупных организаций КФС, финансовых объединений, финансовых экосистем». Результаты риск-профилирования в дальнейшем будут использоваться в системе мониторинга и анализа операционных рисков организаций КФС.

В целях *развития аутсорсинга информационных технологий и использования облачных сервисов* осуществляются следующие мероприятия: совершенствуется институт аутсорсинга ИТ и облачных сервисов для организаций КФС с учетом киберрисков; осуществляется мониторинг рисков аутсорсинга ИТ и облачных сервисов; совершенствуется механизм применения облачных сервисов в КФС (в том числе в части его правового обеспечения).

[13] Подробнее см. «Основные направления развития технологий SupTech и RegTech на период 2021–2023 годов», разработанные и утвержденные Банком России в 2021 г., содержащие три раздела: 1) Международный опыт внедрения SupTech- и RegTech-решений; 2) Цели и задачи внедрения SupTech и RegTech на российском финансовом рынке; 3) План мероприятий («дорожная карта») в сфере SupTech и RegTech в Банке России до 2023 года. URL: https://cbr.ru/Content/Document/File/120709/SupTech_RegTech_2021-2023.pdf.

Многие механизмы в области обеспечения ИБ КФС, указанные в *Основных направлениях 2023-2025, получили развитие в Основных направлениях развития национальной платежной системы на период 2025-2027 годов* (далее – ОНРНПС 2025-2027) и в *Основных направления развития финансовых технологий на период 2025-2027 годов* (далее – ОНРФТ 2025-2027).

Как указано в ОНРНПС 2025-2027, в целях обеспечения ИБ, ОН и киберустойчивости платформы цифрового рубля «Банком России совместно с ФСБ России и Роскомнадзором разработаны необходимые технологические решения для обеспечения безопасного доступа пользователей к платформе. Пользователям платформы цифрового рубля с сентября 2024 г. стали доступны не только открытие, закрытие и пополнение счетов, переводы между гражданами, оплата товаров и услуг, совершение автоплатежей с использованием смарт-контрактов, но и оплата по динамическому QR-коду, а также переводы цифровых рублей между юридическими лицами»[14].

В СБП «реализована возможность осуществления трансграничных переводов физических лиц в другие страны, для чего создано несколько форм подключения иностранных банков и межсистемное взаимодействие с аналогичной системой одной из дружественных стран. Большое внимание уделяется вопросам ИБ, как внутри страны, так и при трансграничном взаимодействии»[15].

В *части ИБ и киберустойчивости цифровых и платежных технологий* Банк России ориентирован на проведение мониторинга фактического уровня защищенности реализуемых проектов с учетом актуальных киберугроз и рисков. Требования, методология и практические инструменты ИБ и киберустойчивости цифровых и платежных технологий дорабатываются Банком России «во взаимодействии с федеральными органами исполнительной власти, организациями КФС с учетом принципов разумной централизации и максимальной автоматизации процессов обмена информацией»[16].

Положения ОНРФТ 2025-2027 свидетельствуют об утверждении *Концепции системы внешнего аудита ИБ*. «Использование разработанных подходов позволит обеспечить качество и достоверность оценки соответствия защиты информации в организациях КФС»[17].

В сфере ИБ реализован «комплекс мероприятий, направленных на развитие механизмов противодействия мошенничеству в финансовой сфере и установление требований к защите информации и ОН при применении финансовых технологий. Банк России продолжает работу по мониторингу, выявлению и анализу системных рисков ИБ и киберугроз, обеспечивает обмен информацией с заинтересованными органами федеральной исполнительной власти и участниками рынка по этим вопросам. В частности, развернута система ФинЦЕРТ, обеспечивающая обмен сведениями между участниками рынка и Банком России о выявленных угрозах и инцидентах»[18].

В сфере RegTech реализуются мероприятия, направленные на «совершенствование процедур допуска на ФР, информационного взаимодействия с организациями КФС и иными лицами, обеспечение ИБ. Для этого используются технологии сбора, обработки и хранения данных, технологии ИИ, обработка естественного языка, технологии визуализации данных и другие. В целях дальнейшего развития существующих надзорных процессов и регуляторной деятельности Банк России продолжит изучение, разработку и внедрение SupTech- и RegTech-решений, направленных на совершенствование информационного взаимодействия с организациями КФС, внедрение элементов датацентричного подхода, анализ и управление рисками и обеспечение ИБ, выявление неправомерных действий на ФР»[19] и т.д. «В рамках дальнейшего совершенствования надзорных процессов и регуляторной деятельности Банк России продолжит изучение, разработку и внедрение SupTech- и RegTech-решений в рамках таких направлений, как оптимизация работы с обращениями в Банке России, анализ и управление рисками, совершенствование информационного взаимодействия с организациями КФС, внедрение элементов датацентричного подхода, обеспечение ИБ, выявление неправомерных действий на ФР, совершенствование процедур допуска на ФР»[20].

В части киберустойчивости, в ОНРФТ 2025-2027 подчеркивается тот факт, что «на фоне роста уровня цифровизации и расширения использования дистанционных каналов обслуживания ключевым вызовом для организаций КФС в области ИБ остаются кибератаки на информационную инфраструктуру участников ФР. Участники мирового ФР наиболее подвержены кибератакам: по статистике, почти каждая пятая кибератака затрагивает организации

[14] Основные направления развития национальной платежной системы на период 2025-2027 годов. URL: https://cbr.ru/Content/Document/File/170680/onrnps_2025-27.pdf, с. 12.

[15] Там же, с. 13.

[16] Там же, с. 37.

[17] Основные направления развития финансовых технологий на период 2025-2027 годов. URL: https://cbr.ru/Content/Document/File/166399/onfintech_2025-27.pdf, с. 16.

[18] Там же, с. 19.

[19] Там же, с. 38.

[20] Там же, с. 54.

КФС. По оценке экспертов, с 2004 г. по 2023 год в мире было зафиксировано более 20 тыс. кибератак (правонарушений), которые привели к убыткам организаций КФС в размере 12 млрд долларов США»[21].

С учетом актуальных киберугроз и рисков в КФС, «Банк России совместно с федеральными органами исполнительной власти и участниками рынка проводит комплексную политику по обеспечению ИБ на ФР, в том числе в соответствии с задачами и приоритетами, определенными Основными направлениями развития информационной безопасности кредитно-финансовой сферы на период 2023–2025 годов»[22].

Таким образом «правонарушения[23], совершаемые при осуществлении деятельности организаций КФС, значительно влияют на стабильное функционирование государства, формируют негативное представление о КФС России и государстве в целом. С каждым годом расширяется состав преступлений в КФС, они становятся изощренней и масштабней. Поэтому выработка и эффективная реализация мер по их противодействию и повышению уровня информационной и экономической безопасности организаций КФС является актуальной и значимой не только для развити КФЧ, но и для национальной экономики в целом» [8].

В ОНРФТ 2025-2027 подчеркнуто, что «создание условий для безопасного внедрения платежных и цифровых технологий и обеспечения технологической независимости (технологического суверенитета) является одной из приоритетных задач в области повышения устойчивости экономики к воздействию внешних и внутренних вызовов и угроз, а также защиты национальных интересов России в финансовой сфере»[24]. *Устойчивое развитие страны напрямую зависит от модернизации процессов обеспечения ИБ в КФС, существенно влияющих на экономическую безопасность государства*.

В ОНРФТ 2025-2027 отмечено, что «создание условий для безопасного внедрения платежных и цифровых технологий и обеспечения технологической независимости (технологического суверенитета) является одной из приоритетных задач в области повышения устойчивости экономики к воздействию внешних и внутренних вызовов и угроз, а также защиты национальных интересов России в финансовой сфере». Там же подчеркнуто, что *устойчивое развитие страны напрямую зависит от модернизации процессов обеспечения информационной безопасности в кредитно-финансовой сфере, существенно влияющих на экономическую безопасность государства*.

Все вышесказанное доказывает, что развитие механизма информационной безопасности в кредитно-финансовой сфере существенно влияет не только на экономическую безопасность и устойчивое развитие ее субъектов, но и на обеспечение экономической безопасности государства.

Литература

1. *Фадейкина Н. В., Зырянов В. С.* Информационная и экономическая безопасность кредитной организации как факторы обеспечения ее устойчивого развития // Сибирская финансовая школа. 2024. № 2 (154). С. 50-60. DOI: 10.34020/1993-4386-2024-2-50-60.

2. *Гамза В. А., Ткачук И. Б., Жилкин И. М.* Безопасность банковской деятельности: учебник для вузов / 5-е изд., перераб. и доп. – М.: Юрайт, 2021. – 455 с.

3. *Одинцов В. О.* Современные инструменты обеспечения экономической безопасности коммерческого банка / В сборнике: Теоретические и прикладные вопросы экономики, управления и образования // Сборник статей IV Международной научно-практической конференции (Пенза, 13–14 июня 2023 г.). Под научной редакцией Б. Н. Герасимова. – Пенза: Пензенский государственный аграрный университет, 2023. С. 267–271.

4. *Ерохин В. В.* Верификация информации и защита программного обеспечения в информационно-телекоммуникационных системах банка: монография. – 2-е изд., перераб. и доп. – М.: Издательство «Спутник+», 2025. – 183 с.

5. *Харыбина А.* Нужные люди // Банковское обозрение. 2022. № 3. С. 61-63.

[21] Там же, с. 39, а также сведения из Отчета Международного валютного фонда «Global financial stability report». IMF, 2024.

[22] Там же, с. 40.

[23] Согласно Федеральному закону от 23 июня 2016 г. № 182-ФЗ «Об основах системы профилактики правонарушений в Российской Федерации», правонарушение представляет собой «преступление или административное правонарушение, представляющие собой противоправное деяние (действие, бездействие), влекущее уголовную или административную ответственность; профилактика правонарушений – совокупность мер социального, правового, организационного, информационного и иного характера, направленных на выявление и устранение причин и условий, способствующих совершению правонарушений, а также на оказание воспитательного воздействия на лиц в целях недопущения совершения правонарушений или антиобщественного поведения (действия физического лица, не влекущие за собой административную или уголовную ответственность, нарушающие общепринятые нормы поведения и морали, права и законные интересы других лиц»).

[24] Основные направления развития финансовых технологий на период 2025-2027 годов (URL: https://cbr.ru/Content/Document/File/166399/onfintech_2025-27.pdf), с. 54.

6. *Фадейкина Н. В., Клепиков Н. С., Морозова О. В.* Обеспечение экономической безопасности кредитной организации / В сборнике: Актуальные проблемы экономической безопасности государства и бизнеса: условия новой реальности // Материалы II Международной научно-практической конференции (Новосибирск, 27–28 апреля 2023 г.). – Новосибирск: Новосибирский государственный университет экономики и управления «НИНХ», 2023. С. 345–351.

7. *Фадейкина Н. В., Демчук И. Н., Татаринова Л. Ю.* Менеджмент риска в кредитных организациях // Сибирская финансовая школа. 2013. № 3 (98). С. 105–113.

8. *Фадейкина Н. В., Тагаков Н. Е., Морозова О. В.* О мерах по предупреждению и пресечению правонарушений и преступлений, совершаемых при осуществлении деятельности банков в целях повышения уровня их экономической безопасности / В сборнике: Актуальные проблемы экономической безопасности государства и бизнеса: условия новой реальности // Материалы II Международной научно-практической конференции (Новосибирск, 27–28 апреля 2023 г.). – Новосибирск: Новосибирский государственный университет экономики и управления «НИНХ», 2023. С. 419-426.

Сведения об авторах

Фадейкина Наталья Васильевна – доктор экономических наук, профессор, Заслуженный деятель науки и Заслуженный экономист Новосибирской области, профессор кафедры общественных финансов ФГБОУ ВО «Новосибирский государственный университет экономики и управления «НИНХ», главный редактор научного журнала «Сибирская финансовая школа», Новосибирск, Россия.
ORCID: 0000-0002-5864-9668
E-mail: fadeikinanv@yandex.ru

Фадейкин Георгий Алексеевич – кандидат экономических наук, доцент, член Редакционной коллегии научного журнала «Сибирская финансовая школа», финансовый консультант ООО «Аудиторская фирма «Финансовая экспертиза», Новосибирск, Россия.
E-mail: gfadejkin@yandex.ru

Морозова Оксана Викторовна – кандидат философских наук, доцент (по финансам), доцент кафедры общественных финансов ФГБОУ ВО «Новосибирский государственный университет экономики и управления «НИНХ», Новосибирск, Россия.
E-mail: mov-777@mail.ru

ON THE MODERNIZATION OF THE INFORMATION SECURITY MECHANISM IN THE CREDIT AND FINANCIAL SPHERE IN ORDER TO ACHIEVE THE ECONOMIC SECURITY OF THE STATE

N. Fadeikina
Novosibirsk State University of Economics and Management "NINH", Novosibirsk, Russia
G. Fadeikin
FINEX LLC, Novosibirsk, Russia
O. Morozova
Novosibirsk State University of Economics and Management "NINH", Novosibirsk, Russia

The article defines the essence of information security in the credit and financial sector as an essential component of the economic security of the state based on a variety of definitions of the concepts of "information security", "information security of the credit and financial sector" and "economic security", formulated by different researchers taking into account different points of view. Special attention is paid to new regulatory documents regulating the security of the critical information infrastructure of the Russian Federation, ensuring the information security of the KFS, improving the operational risk management system and comprehensive modernization of corporate risk management systems in KFS organizations, taking into account the new conditions for ensuring the information security of the KFS, which significantly affects the economic security of the state.

Keywords: information security, credit and financial sphere, modernization of the risk management system of organizations.

References

1. Fadeikina N. V., Zyryanov V. S. Information and economic security of a credit institution as factors of ensuring its sustainable development, *Sibirskaya finansovaya shkola*, 2024, No. 2 (154), pp. 50-60. (In Russ.).

2. Gamza V. A., Tkachuk I. B., Zhilkin I. M. *Bezopasnost' bankovskoi deyatel'nosti: uchebnik dlya vuzov* [Banking security: a textbook for universities], Moscow: Yurait, 2021, 455 p. (In Russ.).

3. Odintsov V. O. Modern tools for ensuring the economic security of a commercial bank, *Teoreticheskie i prikladnye voprosy ekonomiki, upravleniya i obrazovaniya* [Theoretical and applied issues of economics, management and education], Collection of articles of the IV International Scientific and Practical Conference (Penza, June 13-14, 2023), Penza: Penzenskii gosudarstvennyi agrarnyi universitet, 2023. S. 267–271. (In Russ.).

4. Erokhin V. V. *Verifikatsiya informatsii i zashchita programmnogo obespecheniya v informatsionno-telekommunikatsionnykh sistemakh banka: monografiya* [Information verification and software protection in the Bank's information and telecommunication systems: monograph], Moscow: Izdatel'stvo «Sputnik+», 2025, 183 p. (In Russ.).

5. Kharybina A. The right people, Bankovskoe obozrenie, 2022, No. 3, pp. 61-63. (In Russ.).

6. Fadeikina N. V., Klepikov N. S., Morozova O. V. Ensuring the economic security of a credit institution, *Aktual'nye problemy ekonomicheskoi bezopasnosti gosudarstva i biznesa: usloviya novoi real'nosti* [Actual problems of economic security of the state and business: conditions of the new reality], Proceedings of the II International Scientific and Practical Conference (Novosibirsk, April 27-28, 2023). – Novosibirsk: Novosibirskii gosudarstvennyi universitet ekonomiki i upravleniya «NINKh», 2023, pp. 345–351. (In Russ.).

7. Fadeikina N. V., Demchuk I. N., Tatarinova L. Yu. Risk management in credit institutions, *Sibirskaya finansovaya shkola*, 2013, No. 3 (98), pp. 105-113. (In Russ.).

8. Fadeikina N. V., Tagakov N. E., Morozova O. V. On measures to prevent and suppress offenses and crimes committed in the course of banks' activities in order to increase their economic security, *Aktual'nye problemy ekonomicheskoi bezopasnosti gosudarstva i biznesa: usloviya novoi real'nosti* [Actual problems of economic security of the state and business: conditions of the new reality], Proceedings of the II International Scientific and Practical Conference (Novosibirsk, April 27-28, 2023). – Novosibirsk: Novosibirskii gosudarstvennyi universitet ekonomiki i upravleniya «NINKh», 2023, pp. 419-426. (In Russ.).

About the authors

Natalia V. Fadeikina – Doctor of Economics, Professor, Honored Scientist and Honored Economist of the Novosibirsk Region, Professor of the Department of Public Finance at the Novosibirsk State University of Economics and Management, Institute of Economics, Editor-in-Chief of the scientific journal Siberian Financial School, Novosibirsk, Russia.
ORCID: 0000-0002-5864-9668
E-mail: fadeikinanv@yandex.ru

Georgy A. Fadeikin is a Candidate of Economics, Associate Professor, financial consultant at the FINEX LLC auditing company, Novosibirsk, Russia.
E-mail: gfadejkin@yandex.ru

Oksana V. Morozova – PhD in Philosophy, Associate Professor (in Finance), Associate Professor of the Department of Public Finance, Novosibirsk State University of Economics and Management, Novosibirsk, Russia.
E-mail: mov-777@mail.ru