

УДК 336.62**Современные автоматизированные банковские системы и их роль в обеспечении информационной безопасности кредитных организаций****Горшков Арсений Алексеевич**

Экономист,
ООО «Гелио-Пакс-Агро-6»,
403912, Российская Федерация, п. Хоперский, ул. Мира, 2;
e-mail: arseney849@gmail.com

Горшкова Наталья Валерьевна

Доктор экономических наук, профессор,
заведующий кафедрой финансов, учета и экономической безопасности,
Волгоградский государственный университет,
400062, Российская Федерация, Волгоград, просп. Университетский, 100;
e-mail: gorshkovanv@volsu.ru

Аннотация

В контексте усиления санкционного давления, цифровой трансформации и ужесточения регуляторных требований, включая изменения в 58-ФЗ и поправки в 115-ФЗ, обеспечение информационной и экономической безопасности становится ключевым фактором устойчивости российских банков. Статья на примере ПАО «ВТБ» исследует роль современных автоматизированных банковских систем (АБС) как основного инструментария управления рисками, обеспечения комплаенса и защиты данных. Детально анализируется текущая трансформация ИТ-инфраструктуры банка – переход от универсальной зарубежной АБС «ЦФТ main 2.0» к модульным отечественным решениям (ФРКК для корпоративных клиентов и ПРО для розницы), направленный на повышение суверенитета и соответствия новым нормам. Особое внимание уделяется выявлению и оценке сопутствующих технологических, финансовых и операционных рисков данного перехода с использованием авторской методики расчета интегрального показателя риска (ИПР). Анализ выявил приоритетность технологических рисков (ИПР 6.0-6.7), связанных со сбоями и интеграцией.

Для цитирования в научных исследованиях

Горшков А.А., Горшкова Н.В. Современные автоматизированные банковские системы и их роль в информационной безопасности кредитных организаций // Экономика: вчера, сегодня, завтра. 2025. Том 15. № 4А. С. 332-341.

Ключевые слова

Автоматизированная банковская система; учетно-аналитическое обеспечение, система внутреннего контроля; комплаенс-риски; кредитные организации; информационная трансформация; финансовый мониторинг.

Введение

Учетно-аналитическое обеспечение коммерческого банка напрямую определяет эффективность функционирования системы внутреннего контроля путем формирования объективной, достоверной и оперативной информации. Современные автоматизированные банковские системы (АБС) плотно интегрированы в процесс бухгалтерского, статического, управленческого и иных видов учета, упрощая и расширяя их ведение в интересах нивелирования угроз несоблюдения банковского законодательства и в целом повышения экономической безопасности субъекта.

Однако в современных условиях, характеризующихся беспрецедентным санкционным давлением, ужесточением регуляторных требований и экспоненциальным ростом киберугроз, роль АБС кардинально трансформируется. Она выходит далеко за рамки инструмента автоматизации учета, становясь ключевым элементом системы информационной безопасности и основным барьером на пути комплаенс-рисков. Особую актуальность приобретает анализ этой роли в контексте масштабной импортозамещающей трансформации ИТ-инфраструктуры крупнейших кредитных организаций.

АБС как инструментальный системы внутреннего контроля кредитной организации

Система бухгалтерского учета и система внутреннего контроля, как и в любой организации, играют ключевую роль в обеспечении надежности и эффективности финансовых операций. Бухгалтерский учет обеспечивает точное отражение всех финансовых операций банка, позволяя формировать отчетность, необходимую для анализа и принятия управленческих решений. Внутренний контроль, в свою очередь, обеспечивает соблюдение законодательства и внутренних регламентов, минимизируя риски финансовых потерь и мошенничества.

Эти две системы работают в тесной взаимосвязи, создавая надежный механизм управления и контроля, который способствует повышению прозрачности и доверия со стороны клиентов и инвесторов.

В сущности, наибольшим отличием ведения учета в кредитной организации от иной помимо очевидной специфики является практически полная автоматизация процесса учета банковских операций и бизнес-процессов. Безусловно, сотрудники бухгалтерии или кассиры-операционисты не фиксируют каждый банковский перевод, оплату по дебетовой или кредитной карте, или поступление процентов по вкладу. Это происходит автоматически и фиксируется в разрезе каждого лицевого или расчетного счета в разрезе физических и юридических лиц.

Автоматизированная банковская система (сокр. АБС, от англ. Core banking system) – это аппаратно-программный комплекс для обработки, накопления, анализа и передачи информации о денежных платежах, расчётах и других финансово-кредитных операциях.

Как видно из названия, ключевым преимуществом АБС в сравнении с классическим программным обеспечением (ПО) для коммерческих предприятий является своеобразный автопилот наиболее важных бизнес-процессов банка.

Модуль автоматизированной банковской системы (АБС) — это подпрограмма, предназначенная для расчёта различных банковских продуктов.

Как правило, системообразующие банки создают, отлаживают и развивают АБС самостоятельно с помощью собственного штата специалистов, не привлекая сторонних разработчиков.

Важно подчеркнуть, что АБС – это не модель искусственного интеллекта или нейросеть, способная принимать автономные решения вне группы лиц, ответственных за конкретный модуль или отдел. Это лишь программируемая иерархия множества алгоритмов, призванных оптимизировать и упростить ведение бизнес процессов.

Традиционно, автоматизированная банковская система выполняет несколько ключевых функций:

- Автоматизация операций клиентов: АБС обеспечивает автоматическое проведение клиентских операций, включая платежи, переводы, начисления и списания без ручного вмешательства.
- Аккумуляция данных: система собирает статистическую, бухгалтерскую и операционную информацию, формируя сводные данные для управленческой и финансовой отчетности.
- Контроль и мониторинг: встроенные механизмы контроля позволяют выявлять аномалии и ошибки в операциях, что способствует повышению качества обслуживания и снижению рисков.

Важно отметить, что при возникновении нестандартных ситуаций (например, задержка платежа, необходимость изменения статуса операции вручную) вмешательство осуществляется сотрудниками фронт-офиса. Если же обнаруживается техническая ошибка, ее решают специалисты бэк-офиса. Таким образом, вопросы, связанные с проведением операций, не входят в прямые трудовые функции бухгалтерии [Положение Банка России № 809-П, 2022, 2024].

В таблице 1 представлено взаимодействие уровней и модулей типовой АБС. На практике система значительно сложнее, автоматизированная система является лишь инструментарием экосистемы банка.

Таблица 1 – Взаимодействие уровней и модулей типовой АБС

Уровень АБС	Модули АБС	Описание взаимодействия
Фронт-офис	Модуль управления клиентами	Обрабатывает запросы клиентов и передает данные в бэк-офис.
	Интерфейс пользователя	Предоставляет доступ клиентам к услугам банка (веб, мобильные приложения, чат-боты).
	Модуль расчетов	Обрабатывает платежи и переводы, взаимодействует с бухгалтерией.
Бэк-офис	Модуль кредитования	Получает заявки от фронт-офиса, обрабатывает и передает данные в бухгалтерию.
	Модуль депозитов	Управляет депозитами, взаимодействует с фронт-офисом для обработки запросов клиентов.
	Модуль бухгалтерии	Ведет учет всех операций, получает данные от модулей кредитования и депозитов.
	Модуль отчетности и аналитики	Формирует отчеты на основе данных из бухгалтерии и других модулей.
	Модуль бухгалтерии	Ведет учет, формирует отчетность, получает данные из бэк-офиса.
	Модуль отчетности и аналитики	Формирует отчеты на основе данных из бухгалтерии и других модулей.
Модуль безопасности	Аутентификация пользователей	Обеспечивает безопасность всех уровней, взаимодействует как с фронт-, так и с бэк-офисом.
	Мониторинг подозрительной активности	Следит за действиями в системе, взаимодействует со всеми модулями.
	Защита данных клиентов	Обеспечивает защиту данных на всех уровнях системы.

Источник: составлено авторами

В контексте типовой АБС, бесперебойном взаимодействии с ее функциональными составляющими, активно вызывает интерес модуль безопасности, ориентированный на информационную и финансовую безопасность банка. Кроме защиты персональных данных клиентов и защиты от утечки данных, предназначенных для внутренних пользователей, следует акцентировать на службе финансового мониторинга, входящего в систему внутреннего контроля [Кидяева, 2017].

Актуальные проблемы службы финансового мониторинга банка в условиях бесперебойного нивелирования комплаенс-рисков

Служба финансового мониторинга (СФМ), или, как кратко выражаются на сленге сотрудники, «финмон», является качественным примером оценки рисков банковской организации, в которой угроза информационной безопасности линейно влияет на финансовый ущерб.

Цель и задачи службы, в сущности, идентичны службе финансового мониторинга и валютного контроля Банка России, поскольку именно его политику и реализуют коммерческие банки, а именно осуществляет меры по противодействию отмыывания преступных доходов, финансированию терроризма и финансированию распространения оружия массового уничтожения (ПОД/ФТ/ФРОМУ), а также в сфере валютного контроля [Федеральный закон № 115-ФЗ, 2001].

Согласно внесенным с 01 июля 2025 года изменениям в 115-ФЗ банки обязаны расширить регулирование по операциям с цифровым рублем, активное развитие которых прогнозируется на сентябрь 2026 года, а также усилить контроль над счетами, используемыми для дропперства.

Примечательность деятельности СФМ заключается в работе поискового модуля АБС, способного распознавать нетипичные паттерны поведения хозяйствующего субъекта, действия которого потенциально несут в себе, в первую очередь, комплаенс-риски для кредитной организации [Березина, 2023].

Согласно Положению Банка России № 242-П «Об организации внутреннего контроля в кредитных организациях и банковских группах», комплаенс-риск – это риск возникновения у кредитной организации убытков из-за несоблюдения законодательства Российской Федерации, внутренних документов кредитной организации, стандартов саморегулируемых организаций (если такие стандарты или правила являются обязательными для кредитной организации), а также в результате применения санкций и (или) иных мер воздействия со стороны надзорных органов.

В таблице 2 представлен перечень основных нормативно-правовых актов, на принципах которых прямо или косвенно строится распознающий механизм поискового модуля АБС.

Несмотря на многочисленные рекомендации и установки Банка России по распознаванию клиентов, осуществляющих противозаконные (отмывочные) операции, каждая кредитная организация самостоятельно определяет маркеры, фильтрующие финансовое поведение конкретного субъекта. Разумеется, эти маркеры являются коммерческой тайной и они неизвестны никому кроме узкого круга лиц, занимающихся отладкой соответствующего поискового модуля АБС.

В общем порядке маркерами могут служить следующие ситуации:

- 1) Необоснованные обороты денежных средств на счёте, особенно если они поступают со счетов других юридических лиц или физических лиц, не связанных с клиентом.

- 2) Проведение операций, которые не соответствуют предоставленной информации о цели и природе бизнеса клиента. Иначе говоря, не совпадают с кодами ОКВЭД, выбранными организацией.
- 3) Отсутствие или недостаточность информации о клиенте или сделке, особенно в случае непрозрачной структуры собственности или сложных финансовых операций.
- 4) Низкий кредитный рейтинг, характеризующий качество пользования лицом финансовыми продуктами, полученный из Национального бюро кредитной истории (НБКИ).

Важно подчеркнуть, что в случае выявления подозрений или потенциальной ненадежности клиента вне зависимости от причин, Банк не сообщает эти сведения третьим лицам, в том числе государственным органам, поскольку эта информация является банковской тайной. Тем не менее, в случае с дропперством работа данного механизма становится менее ясной.

Таблица 2 – Основные нормативно-правовые акты, акцентирующие комплаенс-риски как часть системы внутреннего контроля банка

Характер регламентации действий	Нормативно-правовой акт	Рекомендации и обязательства кредитной организации
Обязательства к выполнению банком	Положение Банка России от 16.12.2003 № 242-П «Об организации внутреннего контроля в кредитных организациях и банковских группах»	обязывает все кредитные учреждения организовывать службы внутреннего контроля
	Федеральный закон «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма»	обязывает банки отслеживать и препятствовать совершению операций, связанных с отмыванием нелегальных доходов и финансированием терроризма
	Положение Банка России от 02.03.2012 № 375-П «О требованиях к правилам внутреннего контроля кредитной организации в целях противодействия легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма»	устанавливает требования к правилам внутреннего контроля банка в целях противодействия легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма, по которым должны работать банковские службы;
	Федеральный закон от 10.12.2003 № 173-ФЗ	требует от банков проведения валютного контроля по международным переводам клиентов
Методические рекомендации Банка России	№ 18-МР от 21.07.2017	регламентирует порядок мониторинга клиентов и программирования АБС
	№ 19-МР от 26.06.2019	регламентирует отражение операций нерезидентов Российской Федерации

Источник: составлено авторами

Риски экономической безопасности финансовых организаций в условиях обязательного изменения критической инфраструктуры

В связи с вступлением в силу Федерального закона от 7 апреля 2025 «О внесении изменений в Федеральный закон «О безопасности критической информационной инфраструктуры Российской Федерации» банки как капиталоемкие организации вовлечены в масштабный процесс трансформации информационной структуры, направленный на повышение

устойчивости и безопасности банковских информационных систем [Федеральный закон № 58-ФЗ, 2025].

До 2025 года второй по капитализации банк ПАО «ВТБ» использовал АБС под названием «ЦФТ main 2.0». Эта система представляла собой многофункциональный комплекс, включающий в себя модули для ведения учета по всем видам счетов (расчетные, специальные, лицевые и т.д.), а также обеспечивающий детализированную аналитику по финансовым активам и обязательствам банка. В первом квартале 2025 банк начал интегрировать первичные функции АБС в новые отечественные решения – модуль ФРКК (фронтальное решение корпоративных клиентов) для работы с юридическими лицами и программу ПРО для сотрудников фронт-офиса, обслуживающих физических лиц (табл. 3).

Таблица 3 – Сравнительная характеристика зарубежной и отечественной АБС ПАО «ВТБ»

Параметр	«ЦФТ main 2.0»	ФРКК и ПРО (новая система)
Тип системы	Многофункциональная АБС	Модульные решения для фронт- и бек-офиса
Основные пользователи	Все сотрудники банка	Фронт- и бек-офис, включая бухгалтерию (юридические и физические лица)
Функции	Ведение учета, аналитика, операции	Первичные операции, управление клиентскими счетами
Уровень доступа	Широкий, полный	Ограничен профильными функциями сотрудников
Информационная безопасность	Стандартная	Усиленная, с ограничением доступа
Интеграция с другими сервисами	Да, но с международными ограничениями	Да, с упором на отечественные технологии

Источник: составлено авторами

Основным вектором изменений стал пересмотр использования унифицированной АБС в пользу ответвления отдельных модулей (ПО) для работы каждого отдела фронт - и бек офиса.

Данный переход сопровождается рядом объективных трудностей, среди которых выделены следующие: необходимость обучения сотрудников работе с новым программным обеспечением и АБС; значительные финансовые затраты на разработку, внедрение и сопровождение отечественных программных продуктов; адаптация внутренних бизнес-процессов банка к новым техническим требованиям.

Таким образом, информационная трансформация сопряжена с рядом рисков (рис. 1), которые необходимо учитывать для минимизации потенциальных негативных последствий и обеспечения устойчивости банковской деятельности. Внедрение предложенных мер, направленных на модернизацию информационной инфраструктуры, автоматизацию процессов и повышение компетенций сотрудников, требует комплексного анализа возможных угроз и разработки механизмов их нивелирования.

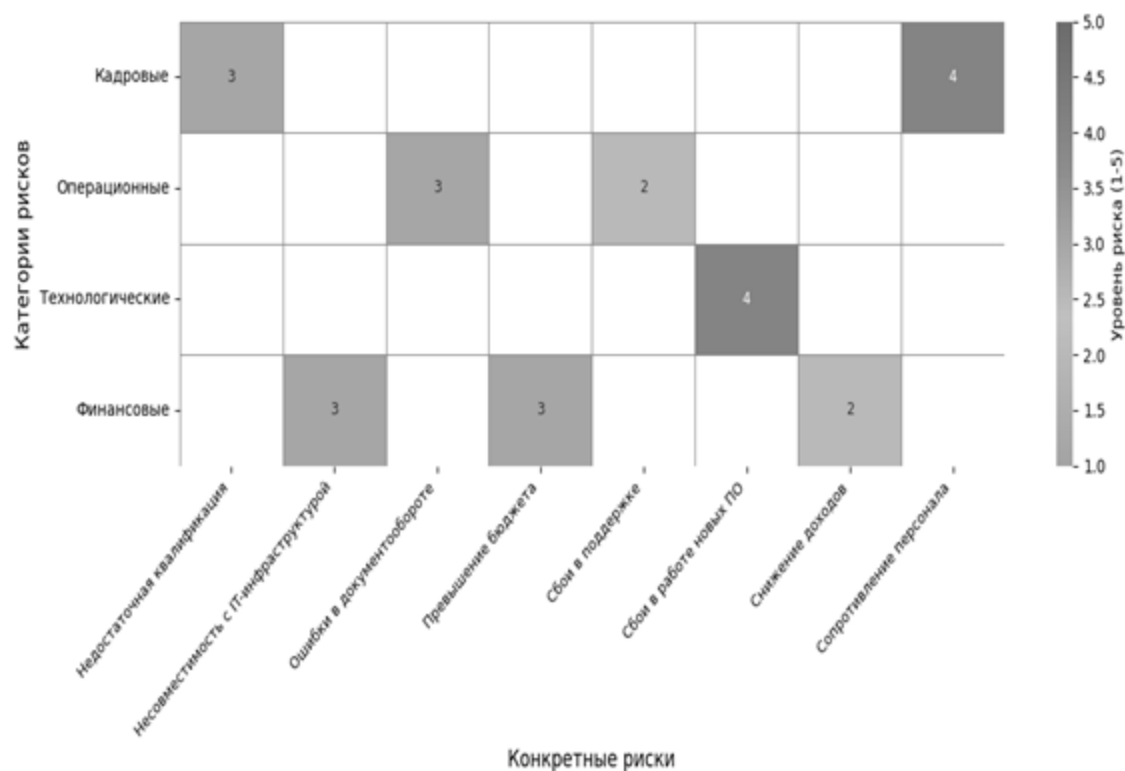
Для экспресс-оценки предлагается использовать взвешенный интегральный показатель риска (ИПР) по следующей формуле:

$$\text{ИПР} = ((P \cdot I)) / M, \text{ где}$$

P – вероятность наступления события (1–5);

I – степень влияния (1–5);

M – коэффициент эффективности



Источник: составлено авторами

Рисунок 1 – Тепловая карта рисков, возникающих вследствие обязательной трансформации инфраструктуры кредитных организаций в 3–4 квартале 2025 года

В табл. 4 приведен расчет ИПР исходя из тепловой карты рисков.

Таблица 4 – Расчет ИПР для ключевых рисков кредитной организации на примере ПАО «ВТБ»

Конкретный риск	Р	І	М	ИПР	Приоритет
Сбой в работе новых программных решений	4	5	3	6,7	Средний
Несовместимость с IT-инфраструктурой	3	4	2	6,0	Средний
Превышение бюджета	3	4	2	6,0	Средний
Сопротивление персонала	4	3	2	6,0	Средний
Недостаточная квалификация сотрудников	3	4	3	4,0	Низкий

Источник: составлено авторами

Наибольший приоритет имеют технологические риски (ИПР ~6–7), особенно сбой ПО. Кадровые и финансовые риски требуют контроля, но менее критичны. В целом риски имеют усредненный характер по банковскому сектору и ИПР может быть применен для экспресс-анализа любого системообразующего банка, сходного по капитализации.

Заключение

В условиях давления на российскую финансовую систему – санкций, ужесточения регуляторных норм и стремительного роста динамически меняющихся киберугроз – вопрос

обеспечения экономической и информационной безопасности кредитных организаций выходит на первый план. Проведенное исследование однозначно подтверждает, что современная автоматизированная банковская система (АБС) перестала быть просто удобным инструментом автоматизации рутинных операций. Она трансформировалась в центральный нервный узел и фундаментальный элемент всей системы внутреннего контроля и экономической безопасности банка. На примере масштабной трансформации ИТ-инфраструктуры ПАО «ВТБ» – перехода с универсальной системы «ЦФТ main 2.0» на специализированные отечественные решения ФРКК (для корпоративного сегмента) и ПРО (для розничного) – наглядно видно, как АБС решает комплекс критических задач.

Не менее важна роль АБС в сфере комплаенса. Она является технологической основой работы Службы финансового мониторинга (СФМ), реализующей требования Банка России по противодействию отмыванию доходов (ПОД/ФТ/ФРОМУ) и валютному контролю. Автоматизированные поисковые алгоритмы АБС, запрограммированные на выявление рискованных «маркеров», позволяют банку эффективно выявлять и блокировать потенциально опасные операции, минимизируя риск применения санкций со стороны регулятора и репутационные потери. Кроме того, АБС обеспечивает бесперебойность, точность и прозрачность ключевых учетно-аналитических процессов. Автоматизация подавляющего большинства финансовых операций (платежи, переводы, начисления) не только резко снижает количество ручных ошибок, но и формирует надежную, достоверную базу данных для управленческой отчетности и принятия стратегических решений, что напрямую влияет на финансовую устойчивость.

Однако, как показал пример ВТБ, стратегическая необходимость импортозамещения и адаптации АБС к новым регуляторным вызовам (особенно в свете изменений в 58-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации») сопряжена со значительными вызовами и рисками. Переход на новые, зачастую менее универсальные и еще не отлаженные отечественные платформы – это сложный и ресурсоемкий процесс. Наибольшую угрозу представляют технологические риски: сбои в работе новых программных модулей, проблемы их интеграции с существующей сложной ИТ-инфраструктурой банка и внешними системами. Экспресс-оценка с использованием предложенного интегрального показателя риска (ИПР) подтвердила высокий приоритет именно этих рисков (ИПР ~6.0-6.7).

Библиография

1. Березина Е.Д. Роль денежно-кредитной политики в обеспечении экономической безопасности страны // Экономическая безопасность: финансовые, правовые и ИТ аспекты: Материалы четвертой Всероссийской научно-практической конференции; г. Иркутск-Томск, 10 ноября 2022 г. / Под наус. ред. И.В. Цвигун, А.А. Шелупанова. Иркутск: Байкальский государственный университет, 2023. С. 24-29.
2. Кидяева А.Ю. Система внутреннего контроля в коммерческих банках // Экономика и бизнес: теория и практика. 2017. № 12. С. 95-99.
3. Положение Банка России «О Платежных счетах бухгалтерского учета для кредитных организаций и порядке его применения» от 24.11.2022г. № 809-П (ред. от 02.11.2024) // СПС Консультант Плюс. URL: https://www.consultant.ru/document/cons_doc_LAW_436264/
4. Федеральный закон «О бухгалтерском учете» от 06.12.2011г. № 402-ФЗ // СПС Консультант Плюс. URL: http://www.consultant.ru/document/cons_doc_LAW_339305/
5. Федеральный закон «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма» от 07.08.2001г. №115-ФЗ // СПС Консультант Плюс. URL:

https://www.consultant.ru/document/cons_doc_LAW_32834/

6. Федеральный закон «О банках и банковской деятельности» от 02.12.1990г. № 395-1 (ред. от 29.12.2022, с изм. и доп., вступ. в силу с 18.05.2023) // Собрание законодательства РФ. 1996. № 6. Ст. 492.
7. Федеральный закон «О внесении изменений в Федеральный закон «О безопасности критической информационной инфраструктуры Российской Федерации» от 07.04.2025г. № 58-ФЗ/ URL: <http://publication.pravo.gov.ru/document/0001202504070004>.

Modern Automated Banking Systems and Their Role in the Information Security of Credit Institutions

Arsenii A. Gorshkov

Economist,
LLC “Helio-Paks-Agro-6”,
403912, 2 Mira str., Khopyorsky Settlement, Russian Federation;
e-mail: arseney849@gmail.com

Natal'ya V. Gorshkova

Doctor of Economic Sciences, Professor,
Head of the Department of Finance, Accounting, and Economic Security,
Volograd State University,
100 Universitetsky ave., Volograd, 400062, Russian Federation,
e-mail: gorshkovanv@volsu.ru

Abstract

In the context of increasing sanctions pressure, digital transformation and tightening regulatory requirements, including changes to Federal Law No. 58 and amendments to Federal Law No. 115, ensuring information and economic security is becoming a key factor in the sustainability of Russian banks. The article, using VTB PJSC as an example, examines the role of modern automated banking systems (ABS) as the main tool for risk management, compliance and data protection. The current transformation of the bank's IT infrastructure is analyzed in detail - the transition from the universal foreign ABS CFT main 2.0 to modular domestic solutions (FRKK for corporate clients and PRO for retail), aimed at increasing sovereignty and compliance with new standards. Particular attention is paid to identifying and assessing the associated technological, financial and operational risks of this transition using the author's methodology for calculating the integral risk indicator (IRI). The analysis revealed the priority of technological risks (IRI 6.0-6.7) associated with failures and integration.

For citation

Gorshkov A.A., Gorshkova N.V. (2025) *Sovremennye avtomatizirovannye bankovskie sistemy i ih rol' v obespechenii informacionnoj bezopasnosti kreditnyh organizacij* [Modern Automated Banking Systems and Their Role in the Information Security of Credit Institutions]. *Ekonomika: vchera, segodnya, zavtra* [Economics: Yesterday, Today and Tomorrow], 15 (4A), pp. 332-341.

Keywords

Automated Banking System (ABS); accounting and analytical framework; internal control system; compliance risks; credit institutions; information transformation; financial monitoring.

References

1. Berezina E.D. (2023) Rol' denezhno-kreditnoy politiki v obespechenii ekonomicheskoy bezopasnosti strany [The role of monetary policy in ensuring the country's economic security]. *Ekonomicheskaya bezopasnost': finansovyye, pravovyye i IT aspekty: Materialy chetvertoy Vserossiyskoy nauchno-prakticheskoy konferentsii; g. Irkutsk-Tomsk, 10 noyabrya 2022 g.* [Economic security: financial, legal and IT aspects: Proceedings of the Fourth All-Russian scientific and practical conference; Irkutsk-Tomsk, November 10, 2022]. Under the ed. of I.V. Tsvigun, A.A. Shelupanova. Irkutsk, "Baikal State University" Publ., pp. 24-29.
2. Kidyayeva A.Yu. (2017) Sistema vnutrennego kontrolya v kommercheskikh bankakh [Internal control system in commercial banks]. *Ekonomika i biznes: teoriya i praktika* [Economy and business: theory and practice], 12, pp. 95-99.
3. (2022, 2024) Polozheniye Banka Rossii «O Plane schetov bukhgalterskogo ucheta dlya kreditnykh organizatsiy i poryadke yego primeneniya» ot 24.11.2022g. № 809-P (red. ot 02.11.2024) [Regulation of the Bank of Russia "On the Chart of Accounts for Credit Institutions and the Procedure for its Application" dated November 24, 2022. No. 809-P (as amended on 02.11.2024)]. SPS Consultant Plus. URL: https://www.consultant.ru/document/cons_doc_LAW_436264/
4. (2011) Federal'nyy zakon «O bukhgalterskom uchete» ot 06.12.2011g. № 402-FZ [Federal Law "On Accounting" dated 06.12.2011 No. 402-FZ]. SPS Consultant Plus. URL: http://www.consultant.ru/document/cons_doc_LAW_339305/
5. (2001) Federal'nyy zakon «O protivodeystvii legalizatsii (otmyvaniyu) dokhodov, poluchennykh prestupnym putem, i finansirovaniyu terrorizma» ot 07.08.2001g. № 115-FZ [Federal Law "On Combating the Legalization (Laundering) of Criminally Obtained Incomes and the Financing of Terrorism" dated 07.08.2001 No. 115-FZ]. SPS Consultant Plus. URL: https://www.consultant.ru/document/cons_doc_LAW_32834/
6. (1996) Federal'nyy zakon «O bankakh i bankovskoy deyatel'nosti» ot 02.12.1990g. № 395-1 (red. ot 29.12.2022, s izm. i dop., vstup. v silu s 18.05.2023) [Federal Law "On Banks and Banking Activities" dated 02.12.1990 No. 395-1 (as amended on 29.12.2022, as amended and supplemented, entered into force on 18.05.2023)]. *Sobraniye zakonodatel'stva RF* [Collected Legislation of the Russian Federation], 6, Art. 492.
7. (2025) Federal'nyy zakon «O vnesenii izmeneniy v Federal'nyy zakon «O bezopasnosti kriticheskoy informatsionnoy infrastruktury Rossiyskoy Federatsii» ot 07.04.2025g. № 58-FZ [Federal Law "On Amendments to the Federal Law "On the Security of Critical Information Infrastructure of the Russian Federation" dated 07.04.2025 No. 58-FZ]. URL: <http://publication.pravo.gov.ru/document/0001202504070004>.