УДК 336.74:141.72 **DOI: 10.34670/AR.2025.72.95.002**

Безопасность финансово-валютной сферы в условиях цифровой трансформации: анализ международного опыта и стратегий укрепления экономической безопасности

Чеботарев Владислав Стефанович

Доктор экономических наук, профессор,
главный научный сотрудник,
кафедра экономики и менеджмента,
Волжский государственный университет водного транспорта,
603950, Российская Федерация, Нижний Новгород, ул. Нестерова, 5
e-mail: vschebotarev@rambler.ru

Хмыз Александр Александрович

Старший преподаватель,
кафедра Общеобразовательные и профессиональные дисциплины,
Нижегородский институт путей сообщения
- филиал Приволжский государственный университет путей сообщения,
603011, Российская Федерация, Нижний Новгород, ул. Культуры, 1
Начальник адъюнктуры,
Нижегородская академия МВД России,
603950, Российская Федерация, Нижний Новгород, Анкудиновское шоссе, 3
e-mail: g101@yandex.ru

Аннотация

Сравнительный и системный анализ международных стратегий обеспечения безопасности финансово-валютной сферы в условиях цифровой трансформации позволил выделить три доминирующие модели регулирования: 1) модель, ориентированная на суверенитет и устойчивость Евросоюза; 2) модель, стимулирующая частные инновации США; 3) модель государственно-частного партнерства глобального Юга. Теоретическая новизна представленных в статье результатов исследования заключается в разработке авторской типологии и выявлении ключевых компромиссов между инновациями и стабильностью. Сформулированы практические рекомендации, включая приоритизацию цифровой инфраструктуры, адаптивное регулирование и усиление международной координации.

Для цитирования в научных исследованиях

Чеботарев В.С., Хмыз А.А. Безопасность финансово-валютной сферы в условиях цифровой трансформации: анализ международного опыта и стратегий укрепления экономической безопасности // Экономика: вчера, сегодня, завтра. 2025. Том 15. № 9А. С. 13-22. DOI: 10.34670/AR.2025.72.95.002

Ключевые слова

Экономическая безопасность, киберустойчивость, цифровая трансформация, цифровые валюты центральных банков, регулирование, международный опыт, сравнительный анализ, управление рисками, государственная политика.

Введение

Центральным элементом научной новизны представленного исследования выступает предложенная типология регуляторных моделей, которая, в отличие от распространенных дихотомий, выстроена на основе и в разработке оригинальной аналитической конструкции, преодолевающей фрагментарность существующих подходов к оценке регуляторных моделей киберустойчивости финансовой сферы. В результате идентифицированы и концептуализированы три доминирующие модели: «превентивный суверенитет», где доминирует цель защиты монетарного суверенитета и операционной устойчивости; «инновационный драйв», акцентирующий стимулирование частного сектора; и «инклюзивный прагматизм» глобального Юга, нацеленный на симбиоз финансовой инклюзии и технологического рывка через государственно-частное партнерство.

Основная часть

Важным результатом проведенного анализа стало также выявление ключевого парадокса современного регулирования: усиление национальных рамок кибербезопасности, призванное повысить устойчивость, объективно ведет к фрагментации глобального регуляторного поля. Эта фрагментация создает арбитражные возможности для злоумышленников и повышает транзакционные издержки для легитимных операторов, тем самым потенциально подрывая одну из декларируемых целей - общую стабильность глобальной финансовой системы.

Наконец, практическая значимость и новизна исследования воплощены в комплексе адаптированных рекомендаций, которые являются не калькой западных моделей, а результатом критического осмысления их применимости. Доказывается, что для стран с формирующейся рыночной экономикой приоритетом должна стать последовательная реализация принципа «цифровой пирамиды»: от базовых инвестиций в инфраструктуру и грамотность через создание стимулирующих регуляторных «песочниц» к развертыванию интероперабельных платформ и лишь затем - к реализации сложных проектов вроде цифровых валют центральных банков. Такой подход позволяет аккумулировать преимущества международного опыта, нивелируя присущие ему системные риски и противоречия.

Трансформация финансово-валютной сферы создает беспрецедентные вызовы для глобальной экономической безопасности [Чеботарев и др., 2016; Голубев, Чеботарев, 2017; Чеботарев, 2006]. По мере того как цифровые услуги становятся неотъемлемой частью повседневной жизни - от коммуникаций и онлайн-платежей до международной торговли - возрастает и уязвимость финансовых систем перед киберугрозами. Финансовые услуги остаются наиболее целевой отраслью для кибератак, количество которых за последнее десятилетие утроилось [Евдокимова, 2024]. Успешная атака на крупное финансовое учреждение или критически важный сервис может быстро распространиться по всей финансовой системе, вызывая широкомасштабные сбои и потерю доверия, что ставит под угрозу финансовую стабильность в целом.

Эти вызовы требуют принципиально нового подхода к обеспечению экономической безопасности, понимаемой как состояние защищенности национальной экономики от внутренних и внешних угроз. Гипотеза исследования состоит в том, что эффективное противодействие цифровым угрозам в финансово-валютной сфере требует комплексного подхода, сочетающего технологические инновации, адаптивное регулирование и усиление международной координации. Целью статьи является анализ международного опыта и выработка на его основе рекомендаций для укрепления экономической безопасности.

Современный ландшафт киберугроз характеризуется быстрой эволюцией тактик и методов злоумышленников. Наблюдается переход от массовых атак к целевым и высокоспециализированным операциям. Инструменты для взлома становятся дешевле, проще и мощнее, позволяя хакерам с меньшей квалификацией наносить значительный ущерб различного характера, особенно - финансовый. Расширение мобильных финансовых услуг, являющихся единственной технологической платформой для многих слоев населения, увеличивает возможности для злоумышленников [Восканян, 2020].

Ключевые векторы атак включают: фишинговые атаки, на которые приходится значительный процент инцидентов в финансовом секторе; программы-вымогатели, способные парализовать работу крупных финансовых институтов; эксплуатацию уязвимостей в цепочках поставок и стороннем программном обеспечении, что демонстрирует системный характер современных угроз.

Особую категорию рисков представляют угрозы для новых цифровых активов и инфраструктур. Более 100 центральных банков (ЦБ) по всему миру изучают возможность выпуска цифровых валют (цифровые валюты центральных банков (ЦВЦБ)), что создает новую, масштабную и сложную экосистему, которая усиливает существующие риски и порождает новые [IMF, 2024]. Экосистема ЦВЦБ, включающая центральные банки, коммерческие банки, поставщиков платежных услуг и технологических вендоров, сталкивается с множеством проблем кибербезопасности, усугубляемых социальными уязвимостями и использованием новых технологий, не испытанных в крупных масштабах. Учитывая последствия выпуска ЦВЦБ, его следует рассматривать как фундаментальное изменение способа функционирования центрального банка, требующее переосмысления устоявшихся подходов к безопасности.

Ответом на растущие киберугрозы стало формирование комплексных регуляторных мер, направленных на повышение операционной устойчивости финансового сектора (табл. 1).

Европейский союз принял закон о цифровых услугах (Digital Services Act, DSA [7]) и закон о цифровых рынках (Digital Markets Act, DMA [Регламент (ЕС) 2022/1925, 2022]), назначение которых создать более безопасное цифровое пространство для защиты основных прав пользователей, и создание равных условий ведения бизнеса. Эти нормативные акты вводят строгие обязательства для крупных онлайн-платформ и поисковых систем, имеющих более 45 миллионов пользователей в месяц в ЕС. Отдельного внимания заслуживает регламент о цифровой операционной устойчивости (Digital Operational Resilience Act, DORA [Регламент (ЕС) 2022/2554, 2022]), который вступил в силу с 15 января 2025 года и делает акцент на операционной устойчивости и управлении рисками третьих сторон.

США демонстрируют стратегический сдвиг в сторону инноваций в области финансовых технологий, управляемых частным сектором. Указ 2025 года о цифровых финансовых технологиях и о национальных инновациях для стейблкоинов (Guiding and Establishing National Innovation for U.S. Stablecoins Act, GENIUS [GENIUS Act, 2025]) устанавливают федеральные рамки для стейблкоинов, обеспеченных фиатом, и предусматривает их нормативный надзор, а

закон (Cyber Incident Reporting for Critical Infrastructure, CIRCIA [CIRCIA, 2022]) обязывает сообщать об инцидентах в течение 72 часов.

Таблица 1 - Сравнительный анализ международных регуляторных подходов

Регион/Организация	Ключевые инициативы	Основные акценты
Европейский союз	DSA/DMA, DORA	Защита прав пользователей, операционная устойчивость, управление рисками третьих сторон
США	GENIUS Act, CIRCIA, Исполнительный указ 2025	Частный сектор, стейблкоины, отчетность об инцидентах
МВФ	Руководство по ЦВЦБ, принципы киберустойчивости	Макрофинансовая стабильность, безопасность цифровых платежей, международная координация

Международные организации играют ключевую роль в разработке основ политики для цифровых платежей и ЦВЦБ. МВФ предлагает центральным банкам динамические рамки, которые являются итеративными, гибкими и реагирующими на новую информацию по мере ее появления. Исследования МВФ подчеркивают, что, если ЦВЦБ будет подвержена киберрискам, это может подорвать доверие потребителей и доверие к финансовой системе в целом [IMF, 2024].

Как следует из данных табл. 1, формирующаяся глобальная архитектура финансовой киберустойчивости демонстрирует принципиально разные философии регулирования. Европейский подход, ориентирован на превентивное выстраивание операционной устойчивости, в то время как американская модель делает ставку на стимулирование частных инноваций. При этом наднациональные институты, такие как МВФ, выступают в роли мета-регулятора, задающего общие рамки. Это сопоставление наглядно иллюстрирует гипотезу о комплексном характере противодействия угрозам

Путем сравнительного метода исследование выявляет и наглядно демонстрирует принципиально разные философии регулирования: европейскую, ориентированную на превентивное выстраивание операционной устойчивости и жесткие стандарты, и американскую, направленную на стимулирование частных инноваций при усилении экстренного реагирования. Одновременно данные приведенные в таблице 1 подчеркивают растущую роль международных организаций в качестве мета-регулятора, задающего общие рамки. Таким образом, форма матричной взаимосвязи данных таблицы 1 сама по себе становится аналитическим инструментом, визуализирующим авторскую гипотезу о комплексном характере противодействия угрозам, где технологические, регуляторные и международно-координационные аспекты неразрывно связаны.

Повышение киберустойчивости финансового сектора требует сочетания передовых технологий и эффективных организационных практик.

Технологические меры защиты включают внедрение многофакторной аутентификации, шифрования данных, систем мониторинга, а также использование искусственного интеллекта и машинного обучения для проактивного обнаружения угроз и анализа паттернов мошенничества. Для экосистемы ЦВЦБ предлагается оценивать технологические и дизайнерские решения для обеспечения безопасности, опираясь на четыре основополагающих принципа, а именно конфиденциальность, целостность, доступность, и управление рисками, вытекающих из фундаментальных требований и лучших практик [ГОСТ Р 50922-2006, 2008].

Особое внимание уделяется обучению пользователей и сотрудничеству заинтересованных сторон для снижения киберрисков.

Управление рисками становится все более важным в контексте растущей зависимости финансовых организаций от сторонних поставщиков. Проактивное управление рисками третьих сторон, включая строгий аудит и соблюдение требований, является критически важным элементом стратегии безопасности.

Организационная культура безопасности играет ключевую роль в противодействии угрозам. Непрерывное обучение сотрудников необходимо для противодействия социальной инженерии и формирования «первой линии обороны». Как подчеркивается в исследованиях, индивидуальные стимулы фирм к инвестированию в защиту недостаточны; необходимо регулирование и вмешательство государственной политики для защиты от недоинвестирования и защиты более широкой финансовой системы от последствий атаки [Предпринимательское право, 2023].

Разные регионы демонстрируют различные подходы к цифровизации финансов и обеспечению безопасности, отражающие их уникальные экономические, институциональные и социальные контексты (табл. 2).

Таблица 2 - Сравнительный анализ региональных стратегий цифровизации финансов

Регион	Ключевые особенности	Влияние на экономическую безопасность
США	Ориентация на частный сектор, стейблкоины, регулирование инноваций	Риски олигопольной власти, снижение финансовой стабильности, потеря дохода
ЕС	Разработка цифрового евро, акцент на приватности и суверенитете	Защита монетарного суверенитета, снижение зависимости от иностранных платформ
Индия, Бразилия	Государственно-частные модели (UPI, Pix), финансовая инклюзия	Снижение неформальности, повышение прозрачности, улучшение доступа к кредиту
Африка к югу от Сахары	Мобильные деньги, проблемы инфраструктуры, региональная координация	Повышение финансовой инклюзии, снижение стоимости переводов, сохраняющиеся уязвимости

США и Европейский союз представляют две контрастные модели. США делают ставку на частный сектор и стейблкоины, в то время как ЕС развивает цифровой евро, частично для защиты приватности и монетарного суверенитета. Европейские эксперты рассматривают центральные банковские электронные наличные как необходимые для сохранения монетарного суверенитета, поскольку они помогают противостоять возникающим угрозам в пяти измерениях: они защищают макрофинансовую стабильность, предотвращая долларизацию; обеспечивают доступ к платежным системам без злоупотребления рыночной властью; сохраняют доход и финансовую независимость центральных банков; сокращают стратегическую зависимость от иностранных субъектов; и защищают информационный суверенитет, позволяя избежать чрезмерной зависимости от иностранных платформ.

Индия и Бразилия демонстрируют успешные модели государственно-частного партнерства. Индийская система, запущенная в 2016 году, повысила эффективность платежных систем на основе счетов, устраняя основные проблемы обмена информацией, аутентификации и окончательного расчета. В Бразилии Центральный банк Бразилии внедрил всеобъемлющую стратегию инноваций [Яковлев, 2023] способствуя токенизации и интеграции для обеспечения более быстрых, прозрачных и программируемых переводов активов. Эта экосистема включает

Pix (систему мгновенных платежей), Open Finance (открытые финансы), Drex (цифровую валюту центрального банка Бразилии) и интернационализацию бразильского реала.

Страны Африки к югу от Сахары сталкиваются с уникальными проблемами, включая слабость цифровой инфраструктуры, ограниченные институциональные возможности, низкий уровень финансовой и цифровой грамотности и высокие затраты на развертывание систем. Чтобы решить эти проблемы, эксперты определяют четыре политических приоритета:

– инвестиции в инфраструктуру и навыки;
– поддержка частных инноваций в рамках безопасных и конкурентных нормативных рамок, обеспечивающих взаимодействие и укрепляющих управление;
– позиционирование государственных цифровых инструментов как дополнения, а не конкуренции частным решениям;
– содействие региональной и международной координации.

Таблица «Сравнительный анализ региональных стратегий цифровизации финансов» имеет фундаментальный базис и обладает существенной научной новизной, которые заключаются в следующем. Функциональный смысл табл. 2 состоит в преодолении фрагментарности при рассмотрении международного опыта. Без такого сравнительного инструментария анализ цифровизации финансов в разных странах и регионах остается набором разрозненных кейсов. Матричная цифровизация финансов как функционально связанная информация табл.2 позволяет синтезировать эти данные в единую аналитическую модель, где каждый регион занимает определенное место в многомерном пространстве критериев: «ключевые особенности» и «влияние на экономическую безопасность». Это превращает «сырую» информацию о конкретных инициативах цифровых валют в разных регионах в систематизированное знание, выявляя неочевидные причинно-следственные связи. Такой подход позволяет увидеть не просто перечень стратегий, а целостную картину глобальной конкуренции различных парадигм финансовой цифровизации и их последствий для национального суверенитета. Такой формат таблицы 2 является результатом концептуального обобщения, в котором заложена оригинальная типологизация региональных подходов. Через прямое сопоставление данных таблицы 2 наглядно демонстрирует ключевой научный тезис: не существует универсальной модели цифровизации, а выбор конкретной стратегии является следствием компромисса между технологическими возможностями, экономическими целями и рисками для экономической безопасности. В частности, она визуализирует фундаментальный конфликт между американской моделью, ориентированной на частные инновации с сопутствующими рисками олигополии и снижения финансовой стабильности, и европейской, где во главу угла поставлены защита монетарного суверенитета и приватности. Одновременно табл. 2 выделяет уникальную «прыгающую через этапы» модель лидеров глобального Юга (Индия, Бразилия), которая доказывает, что государственно-частное партнерство может одновременно решать задачи финансовой инклюзии и снижения неформальности экономики. Таким образом, приведенной формат таблицы 2 становится компактным аналитическим выводом, который эмпирически обосновывает центральную гипотезу исследования о комплексном характере противодействия цифровым угрозам, где технологический выбор неразрывно связан с задачами обеспечения экономической безопасности в глобальном контексте.

Проведенный анализ позволяет констатировать, что в современных условиях обеспечение кибербезопасности финансового сектора трансформировалось в неотъемлемый элемент поддержания общей финансовой стабильности. Каскадный характер потенциальных последствий успешной кибератаки на системно значимый финансовый институт или критически важный сервис способен спровоцировать нарушения функционирования всей

финансовой системы. При этом эффективность любых регуляторных мер напрямую зависит от степени международной координации, поскольку фрагментарность и противоречивость национальных требований не только повышает издержки соблюдения, но и создает регуляторные арбитжи, используемые злоумышленниками.

Цифровая трансформация оказывает амбивалентное воздействие на состояние экономической безопасности. С одной стороны, она способствует повышению прозрачности операций и сокращению транзакционных издержек, а с другой - порождает принципиально новые уязвимости, выражающиеся в росте киберпреступности, рисках масштабных утечек данных и сбоев в работе ключевой финансовой инфраструктуры. Сравнительный анализ региональных стратегий указывает на существенные различия в их результативности. Успешные кейсы, демонстрируемые такими странами, как Индия и Бразилия, подтверждают критическую важность эффективного государственно-частного партнерства. В то же время опыт регионов с формирующейся рыночной экономикой, в частности стран Африки, актуализирует задачу первоочередных инвестиций в развитие базовой инфраструктуры и укрепление институционального потенциала.

Проведенный компаративный анализ позволяет сформулировать ключевые практические рекомендации, сгруппированные вокруг трех системообразующих направлений.

Первое направление концентрируется на стратегических и инфраструктурных приоритетах. Его реализация предполагает осуществление стратегических инвестиций в модернизацию критической финансовой и телекоммуникационной инфраструктуры, что составляет основу долгосрочной операционной устойчивости. Смежным императивом является развитие человеческого капитала через реализацию программ системного повышения цифровой грамотности и целенаправленной подготовки высококвалифицированных специалистов в области кибербезопасности для финансового сектора.

Второе направление охватывает совершенствование регуляторной среды. Ключевая задача здесь – развитие гибкой, технологически нейтральной нормативной базы, сфокусированной на управлении рисками. Такой адаптивный регуляторный подход призван стимулировать инновации, в том числе через использование регуляторных «песочниц», а не ограничивать их исключительно запретительными мерами. На институциональном уровне это дополняется внедрением комплексных систем управления киберрисками, интегрирующих передовые технологии защиты, регламентированные организационные процедуры и регулярное тестирование на проникновение.

Третье, межуровневое, направление актуализирует необходимость усиления международной координации. Трансграничный характер современных киберугроз детерминирует обязательность активного участия национальных регуляторов и центральных банков в работе профильных международных форумов по выработке согласованных стандартов безопасности для цифровых валют и трансграничных платежей. Важнейшей практической задачей в этой связи становится содействие гармонизации национальных регуляторных требований к кибербезопасности финансового сектора, что позволяет минимизировать регуляторные арбитражи и повысить общую эффективность противодействия общим вызовам.

В контексте реализации данного комплекса мер особое внимание должно быть уделено сбалансированному процессу разработки и внедрения цифровых валют центральных банков, который требует проведения скрупулезной оценки сопутствующих киберрисков и создания многоуровневых механизмов защиты, охватывающих всю экосистему ЦВЦБ.

Перспективные направления для дальнейших научных изысканий включают углубленный анализ киберрисков, связанных с токенизацией активов, изучение вызовов, которые квантовые вычисления бросают современной криптографии, оценку действенности моделей защиты приватности в рамках систем ЦВЦБ, а также разработку надежных методологий для квантификации киберрисков с точки зрения их влияния на финансовую стабильность.

Заключение

Таким образом, обеспечение экономической безопасности в контексте цифровой трансформации финансово-валютной сферы диктует необходимость проактивного, системного и скоординированного на международном уровне подхода, способного адаптироваться к эволюционирующему ландшафту угроз. Накопленный международный опыт недвусмысленно свидетельствует о том, что ни одно государство не в состоянии в одиночку противостоять этим вызовам, что делает укрепление глобального сотрудничества императивом сохранения стабильности мировой финансовой системы.

Библиография

1. Восканян, Р. О. (2020). Кибератаки как угроза мировой экономики. В Система ПОД/ФТ в глобальном мире: риски и угрозы мировой экономики (с. 118-120). Российский экономический университет имени Г.В. Плеханова.
2. Голубев, С. С., & Чеботарев, С. С. (2017). Эффективная стратегия управления рисками как основа экономической безопасности банка. Экономические стратегии, 19(3 (145)), 186-195.
3. ГОСТ Р 50922-2006. (2008). Защита информации. Основные термины и определения. Стандартинформ.
4. Евдокимова, А. А. (2024). Основные тенденции в области кибербезопасности. В Экономические и правовые аспекты реализации государственных программ и проектов (с. 37-39). Русайнс.
5. О Регламенте Европейского парламента и Совета Европейского Союза от 14 декабря 2022 года о цифровой операционной устойчивости в финансовом секторе и о внесении изменений в Регламенты (ЕС) № 1060/2009, (ЕС) № 648/2012, (ЕС) № 600/2014 и (ЕС) № 909/2014 (Регламент о цифровой операционной устойчивости — DORA): Регламент (ЕС) 2022/2554* (2022). Официальный журнал Европейского Союза, L 333, 1-79. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32022R2554
6. О Регламенте Европейского парламента и Совета Европейского Союза от 14 сентября 2022 года о состязательных и справедливых рынках в цифровом секторе и о внесении изменений в Директивы (ЕС) 2019/1937 и (ЕС) 2020/1828 (Закон о цифровых рынках): Регламент (ЕС) 2022/1925* (2022). Официальный журнал Европейского Союза, L 265, 1-66. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32022R1925
7. О Регламенте Европейского парламента и Совета Европейского Союза от 19 октября 2022 года о едином рынке цифровых услуг и о внесении изменений в Директиву 2000/31/ЕС (Закон о цифровых услугах): Регламент (ЕС) 2022/2065* (2022). Официальный журнал Европейского Союза, L 277, 1-102. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32022R2065
8. О Законе, направляющем и устанавливающем национальные инновации для стейблкоинов США: Закон GENIUS (2025). Конгресс США. https://www.congress.gov/
9. О сообщении о киберинцидентах на объектах критической инфраструктуры: Закон CIRCIA от 2022 г. (2022). Агентство по кибербезопасности и безопасности инфраструктуры США (CISA). https://www.cisa.gov/topics/cyber-threats-and-advisories/information-sharing/cyber-incident-reporting-critical-infrastructure-act-2022-circia
10. Государственные гарантии прав субъектов инвестиционной деятельности и защита капитальных вложений (2023). В Предпринимательское право: Учебное пособие (с. 203-205). Индивидуальный предприниматель Коняхин Александр Викторович.
11. Чеботарев, В. С., Елфимов, О. М., Тимченко, А. В., & Киселева, Л. В. (2016). Технологии финансового контроля. Нижний Новгород.
12. Чеботарев, С. С. (2006). В поисках алгоритмов безопасного развития общества. Гражданская защита, 5, 7.
13. Яковлев, П. П. (2023). Страны Глобального Юга и проблемы глобального управления в интересах устойчивого развития. Постколониализм и современность, 1(1), 79-102. https://doi.org/10.31249/j.2949-1711.2023.01.04
14. International Monetary Fund (IMF). (2024). Cyber resilience of the central bank digital currency ecosystem (IMF Fintech Notes No. 2024/003). https://www.imf.org/en/Publications/fintech-notes/Issues/2024/08/27/Cyber-Resilience-of-the-Central-Bank-Digital-Currency-Ecosystem-554090

Financial and Currency Sector Security in the Context of Digital Transformation: Analysis of International Experience and Strategies for Strengthening Economic Security

Vladislav S. Chebotarev

Doctor of Economics, Professor,
Chief Researcher at the Department of Economics and Management,
Volga State University of Water Transport,
603950, 5 Nesterova str., Nizhny Novgorod, Russian Federation;
e-mail: vschebotarev@rambler.ru

Aleksandr A. Khmyz

Senior Lecturer,
Department of General Education and Professional Disciplines,
Nizhny Novgorod Institute of Transport Engineering
– Branch of the Volga State University of Transport,
603011, 1 Kultury str., Nizhny Novgorod, Russian Federation;
Head of the Postgraduate Department,
Nizhny Novgorod Academy of the Ministry of Internal Affairs of Russia,
603950, 3 Ankudinovskoye highway, Nizhny Novgorod, Russian Federation;
e-mail: g101@yandex.ru

Abstract

A comparative and systematic analysis of international strategies for ensuring the security of the financial and currency sector in the context of digital transformation has revealed three dominant regulatory models: 1) a model focused on the sovereignty and sustainability of the European Union; 2) a model that stimulates private innovation in the United States; and 3) a model of public-private partnerships in the global south. The theoretical novelty of the research presented in this article lies in the development of an author's typology and the identification of key trade-offs between innovation and stability. The article provides practical recommendations, including the prioritization of digital infrastructure, adaptive regulation, and increased international coordination.

For citation

Chebotarev V.S., Khmyz A.A. (2025) Bezopasnost finansovo-valyutnoi sfery v usloviyakh tsifrovoi transformatsii: analiz mezhdunarodnogo opyta i strategii ukrepleniya ekonomicheskoi bezopasnosti [Financial and Currency Sector Security in the Context of Digital Transformation: Analysis of International Experience and Strategies for Strengthening Economic Security]. *Ekonomika: vchera, segodnya, zavtra* [Economics: Yesterday, Today and Tomorrow], 15 (9A), pp. 13-22. DOI: 10.34670/AR.2025.72.95.002

Keywords

Economic security, cyber resilience, digital transformation, central bank digital currencies, regulation, international experience, comparative analysis.

References

1. Chebotarev, S. S. (2006). V poiskakh algoritmov bezopasnogo razvitiya obshchestva [In search of algorithms for the safe development of society]. Grazhdanskaya Zashchita, 5, 7.
2. Chebotarev, V. S., Elfimov, O. M., Timchenko, A. V., & Kiseleva, L. V. (2016). Tekhnologii finansovogo kontrolya [Technologies of financial control]. Nizhny Novgorod.
3. Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA), Pub. L. No. 117-103, 136 Stat. 49 (2022). Cybersecurity and Infrastructure Security Agency (CISA). Retrieved October 18, 2025, from https://www.cisa.gov/topics/cyber-threats-and-advisories/information-sharing/cyber-incident-reporting-critical-infrastructure-act-2022-circia
4. Evdokimova, A. A. (2024). Osnovnye tendentsii v oblasti kiberbezopasnosti [Main trends in cybersecurity]. In Ekonomicheskie i pravovye aspekty realizatsii gosudarstvennykh program i proektov (pp. 37-39). Rusains.
5. Gosudarstvennye garantii prav subektov investitsionnoi deyatelnosti i zashchita kapitalnykh vlozhenii [State guarantees of the rights of subjects of investment activity and protection of capital investments]. (2023). In Predprinimatelskoe pravo: Uchebnoe posobie (pp. 203-205). Individualnyi predprinimatel Konyakhin Aleksandr Viktorovich.
6. Golubev, S. S., & Chebotarev, S. S. (2017). Effektivnaya strategiya upravleniya riskami kak osnova ekonomicheskoi bezopasnosti banka [Effective risk management strategy as the basis of bank economic security]. Ekonomicheskie Strategii, 19(3 (145)), 186–195.
7. Guiding and Establishing National Innovation for U.S. Stablecoins Act (GENIUS Act), (2025). U.S. Congress. Retrieved September 24, 2025, from https://www.congress.gov/
8. International Monetary Fund (IMF). (2024). Cyber resilience of the central bank digital currency ecosystem (IMF Fintech Notes No. 2024/003). Retrieved December 15, 2024, from https://www.imf.org/en/Publications/fintech-notes/Issues/2024/08/27/Cyber-Resilience-of-the-Central-Bank-Digital-Currency-Ecosystem-554090
9. Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act)*, (2022). Official Journal of the European Union, L 265, 1–66. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32022R1925
10. Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act)*, (2022). Official Journal of the European Union, L 277, 1–102. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32022R2065
11. Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014 and (EU) No 909/2014 (Digital Operational Resilience Act – DORA)*, (2022). Official Journal of the European Union, L 333, 1–79. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32022R2554
12. State Standard GOST R 50922-2006. (2008). Zashchita informatsii. Osnovnye terminy i opredeleniya* [Information protection. Basic terms and definitions]. Standartinform.
13. Voskanyan, R. O. (2020). Kiberataki kak ugroza mirovoi ekonomiki [Cyberattacks as a threat to the world economy]. In Sistema POD/FT v globalnom mire: riski i ugrozy mirovoi ekonomiki (pp. 118-120). Rossiiskii ekonomicheskii universitet imeni G.V. Plekhanova.
14. Yakovlev, P. P. (2023). Strany Globalnogo Yuga i problemy globalnogo upravleniya v interesakh ustoychivogo razvitiya [Global South countries and problems of global governance in the interests of sustainable development]. Postkolonializm i Sovremennost, 1(1), 79–102. https://doi.org/10.31249/j.2949-1711.2023.01.04