

Вестник Евразийской науки / The Eurasian Scientific Journal <https://esj.today>

2025, Том 17, № s6 / 2025, Vol. 17, Iss. s6 <https://esj.today/issue-s6-2025.html>

URL статьи: <https://esj.today/PDF/56FAVN625.pdf>

5.2.3. Региональная и отраслевая экономика (экономические науки)

Ссылка для цитирования этой статьи:

Михайлова, М. А. Цифровая трансформация финансового мониторинга: от истории развития технологии к современным решениям в сфере ПОД/ФТ / М. А. Михайлова, А. М. Муцалханов, П. К. Шубин // Вестник евразийской науки. — 2025. — Т. 17. — № s6. — URL: <https://esj.today/PDF/56FAVN625.pdf>.

For citation:

Mikhailova M.A., Mutsalkhanov A.M., Shubin P.K. Digital transformation of financial monitoring: from the history of technology development to modern AML/CFT solutions. *The Eurasian Scientific Journal*. 2025;17(s6): 56FAVN625. Available at: <https://esj.today/PDF/56FAVN625.pdf>. (In Russ., abstract in Eng.).

УДК 338

Михайлова Мария Андреевна

ФГБОУ ВО «Финансовый университет при Правительстве Российской Федерации», Москва, Россия
E-mail: Mariya.mixajlova.00@inbox.ru

Муцалханов Абдулжаппар Муцалханович

ФГБОУ ВО «Финансовый университет при Правительстве Российской Федерации», Москва, Россия
E-mail: 242537@edu.fa.ru

Шубин Пётр Кириллович

ФГБОУ ВО «Финансовый университет при Правительстве Российской Федерации», Москва, Россия
E-mail: 240430@edu.fa.ru

Научный руководитель: **Тургаева Аксана Альбековна**

ФГБОУ ВО «Финансовый университет при Правительстве Российской Федерации», Москва, Россия
Доцент кафедры «Экономической безопасности и управления рисками»

Кандидат экономических наук, доцент

E-mail: a_turgaeva@mail.ru

ORCID: <https://orcid.org/0000-0002-8374-1706>

РИНЦ: https://elibrary.ru/author_profile.asp?id=455538

Цифровая трансформация финансового мониторинга: от истории развития технологии к современным решениям в сфере ПОД/ФТ

Аннотация. В статье исследуется процесс внедрения передовых цифровых технологий в систему противодействия легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма (ПОД/ФТ). Актуальность темы обусловлена стремительной цифровой трансформацией финансового ландшафта, усложнением методов сокрытия преступных доходов и необходимостью повышения эффективности национальных систем финансовой безопасности для выполнения регуляторных требований. Целью исследования является комплексный анализ возможностей искусственного интеллекта, машинного обучения, технологий больших данных (Big Data) и сетевой аналитики для выявления рисков, схем и типологий преступной деятельности в сфере ПОД/ФТ. В работе проведен ретроспективный анализ генезиса цифровых технологий в России, начиная с создания первых электронно-вычислительных машин в середине XX века и заканчивая современным этапом развития экономики данных. Автором подробно рассмотрены ключевые направления цифровизации:

внедрение регуляторных (RegTech) и надзорных (SupTech) технологий, а также трансформация института идентификации клиентов (включая биометрию и удаленную идентификацию). Особое внимание уделено практическим аспектам применения технологий искусственного интеллекта и анализа больших данных в деятельности российских кредитных организаций и надзорных органов. В результате исследования автором систематизированы преимущества цифровизации (автоматизация процессов, повышение точности анализа, возможность проактивного управления рисками) и основные вызовы (угрозы кибербезопасности, дефицит квалифицированных кадров, высокие финансовые затраты и нормативно-правовая неопределенность). Заключение содержит вывод о необходимости поиска баланса между технологическими инновациями, безопасностью данных и гибкостью регулирования для дальнейшего развития устойчивой экосистемы ПОД/ФТ в условиях цифровой экономики.

Ключевые слова: финансовый мониторинг; цифровизация; искусственный интеллект (ИИ); финансовая безопасность; информационные технологии; управление рисками; большие данные (Big Data); ПОД/ФТ

Введение

Актуальность исследования возможностей технологий для выявления и анализа рисков, схем и типологий преступной деятельности в сфере противодействия легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма (ПОД/ФТ) не вызывает сомнений. Динамичная цифровая трансформация финансового ландшафта, характеризующаяся появлением новых платежных инструментов, ростом объема и скорости транзакций, а также изощренностью методов их сокрытия, создает беспрецедентные вызовы для систем финансовой безопасности.

Следовательно, внедрение и развитие передовых технологий — таких как искусственный интеллект (ИИ), машинное обучение (МО), анализ больших данных (Big Data) и сетевая (графовая) аналитика — становится не просто конкурентным преимуществом, а критической необходимостью для обеспечения устойчивости финансовой системы и выполнения регуляторных требований.

Целью данного исследования является комплексный анализ и систематизация возможностей современных и перспективных технологий (ИИ, МО, Big Data, сетевая аналитика) для повышения эффективности процессов выявления, оценки и анализа рисков, а также для противодействия конкретным схемам и типологиям преступной деятельности в сфере ПОД/ФТ.

1. Методы и материалы

Методологическую основу настоящего исследования составляет комплекс взаимодополняющих научных методов, применение которых обеспечивает системный и всесторонний охват изучаемой проблематики.

Нормативно-документальную базу исследования образуют материалы Банка России, включая доклады об институте идентификации клиентов и платформе «Знай своего клиента» (KYC Service), аналитические публикации Росфинмониторинга, национальные программные документы Российской Федерации в сфере цифровой экономики, а также данные опросов ФАТФ относительно применяемых юрисдикциями технологических решений.

2. Результаты и обсуждение

Цифровая трансформация системы ПОД/ФТ

В современную эпоху цифровая трансформация перестала быть лишь технологическим трендом, превратившись в ключевой фактор национального развития государства в

долгосрочной перспективе и сохранения им технологического суверенитета, что находит выражение в национальных проектах Российской Федерации. Находясь на этапе перехода от индустриального типа хозяйствования к постиндустриальному типу, российское государство активно инвестирует в экономику знаний.

Развитие цифровых технологий имеет стратегическое значение как для отдельных компаний, так и для всего государства в целом. Активная цифровизация затрагивает все сферы — от здравоохранения и образования до оборонного комплекса, определяя конкурентоспособность страны на мировой арене. Особую роль цифровые технологии играют в развитии экономики страны. Таким образом, анализ развития цифрового ландшафта в России позволяет оценить не только технологический прогресс, но и траекторию её будущего, балансирующую между вызовами импортозамещения в условиях обострившегося санкционного давления со стороны недружественных стран и возможностями для глобального лидерства в новых условиях.

Согласно Осмоловской С.М., цифровизация представляет собой «процесс внедрения цифровых технологий во все сферы жизнедеятельности, который влечёт за собой изменения в экономике, управлении, социальной сфере и культуре».¹ В свою очередь, под цифровыми технологиями понимаются инновационные средства, основанные на использовании цифровой информации и ее обработке с помощью компьютерных устройств и высокотехнологичных аппаратных комплексов. Цель цифровизации заключается в повышении эффективности и адаптивности различных систем, что в итоге приводит к повышению качества их работы.

Цифровые технологии тесно связаны с цифровой экономикой — деятельностью по созданию, распространению и использованию цифровых технологий и связанных с ними продуктов и услуг [1]. Перечень типов инновационных технологий обширен и включает в себя нейротехнологии и искусственный интеллект, системы распределенного реестра, квантовые технологии и новые производственные технологии. Технологии виртуальной и дополненной реальности, технологии беспроводной связи и компоненты роботехники — теперь не фантастическая картина далекого будущего, а новая реальность, к которой вынуждены приспосабливаться люди, компании и государства. В условиях быстро изменяющегося мира гибкость и адаптивность — ключевые качества, помогающие бороться с устареванием и «быть в тренде».

Российские цифровые технологии прошли долгий путь становления и развития. История Российской Федерации ведет отсчет с декабря 1991 г., однако ретроспективный анализ целесообразно проводить с более раннего периода, так как Россию традиционно принято считать правопреемницей СССР. Согласно Воронько М.С. [2], точкой отсчета можно теоретически принять создание проекта одной из первых электронно-вычислительных машин — малой электронной счётной машины (МЭСМ) лабораторией Лебедева С.А. в 1948 г. Хотя это была не первая модель такого рода, но переоценить вклад ее создателей в становление российского государства на путь цифровизации невозможно.

В дальнейшем были созданы и другие проекты электронно-вычислительных машин, в том числе БЭСМ-1 и ЭВМ «Стрела». В начале 1950-ых гг. началась работа над постройкой М-1, одной из двух первых в союзном государстве цифровых вычислительных машин. В дальнейшем в истории СССР к реализации предлагались передовые инновационные идеи, в том числе система электронного правительства, функционирующая на базе АСПР (автоматизированной системы плановых расчетов). Ее реализация не соответствовала задумке в полной мере, так как

¹ Осмоловская, С.М., Цифровизация, сетевизация и виртуализация общества: учебник / С.М. Осмоловская. — Москва: Русайнс, 2025. — 110 с. — ISBN 978-5-466-09126-7. — URL: <https://book.ru/book/958277> (дата обращения: 11.12.2025). — Текст: электронный.

уровень развития компьютерной техники в СССР в 1970-ые гг. не отвечал поставленным задачам.

Таким образом, формирование цифровой экономики российского пространства берет начало в период с 1960 по 1990 гг. Этот этап отмечен не только эволюцией ключевых информационных технологий, но и выработкой первых правовых норм, призванных поддержать развитие технологической инфраструктуры. Отправной точкой стал 1948 г., ознаменовавшийся созданием проекта одной из первых электронно-вычислительных машин. В дальнейшем были разработаны базовые компоненты будущей цифровой эпохи: транзисторные компьютеры, специализированное программное обеспечение и системы автоматизации [3]. ЭВМ перестали быть лабораторными образцами и начали использоваться в промышленности и научных организациях для решения практических задач по обработке данных и сложным вычислениям.

С конца 1990-ых гг. информационные технологии активно включаются в социально-экономическую жизнь как мирового, так и российского сообществ [4]. Наступает этап ранней цифровизации, продлившийся с 1990 г. по 2000 г. и характеризующийся массовым распространением интернета и цифровых технологий и активным внедрением их в различные сферы жизни. Технологии становятся более доступными для населения. Идет активное совершенствование не только технологической стороны цифровизации, но и инфраструктурной, проявляющееся в создании нормативно-правовой базы, направленной на регулирование использования цифровых технологий и обеспечение защиты данных.

В 2000–2010 гг., на этапе массовой цифровизации, интернет, мобильная связь и облачные технологии проникли во все сферы жизни, дав мощный толчок электронной коммерции. Этот технологический скачок потребовал адекватной правовой реакции: страны начали активно разрабатывать законодательство в области защиты данных, кибербезопасности и поддержки ИТ-инноваций. Принятые законы стали отправной точкой для развития современных цифровых платформ и технологий.

Период с 2010 по 2020 гг, озаглавленный становлением умной экономики и платформенной трансформацией, стал эпохой, когда цифровая среда обрела «интеллект». Доминирующими драйверами изменений выступили повсеместное внедрение искусственного интеллекта (AI), аналитика больших данных (Big Data) и распределенные реестры (блокчейн). Эти технологии не просто совершенствовали процессы, а кардинально перестраивали традиционные бизнес-модели. В ответ на формирование новой цифровой реальности государства активизировали законодательскую деятельность, направленную на регулирование возникающих отношений, обеспечение безопасности данных и стимулирование дальнейших технологических инноваций.

Начиная с 2020 г. экономика вступает в фазу, где данные становятся ключевым активом, а цифровая трансформация — условием выживания. Прорывные технологии более не являются экспериментальными, а массово внедряются, перестраивая промышленность, транспорт, города и социальную сферу. В этой новой реальности AI управляет критически важными процессами, автономные системы действуют рядом с человеком, а IoT и 5G обеспечивают их мгновенное взаимодействие. Перед законодателями всего мира стоит сложнейшая задача: создать адаптивные правовые нормы, которые одновременно стимулируют технологический прогресс, гарантируют кибербезопасность и защищают права граждан.

Развитие цифровизации в РФ является приоритетной целью правительства, так как информационные технологии играют важную роль в различных отраслях экономики, науки, образования и других сферах общества [5].

Этапы развития цифровых технологий в России отражены на рисунке 1.



Рисунок 1. Этапы развития цифровых технологий в России (составлено авторами)

Таким образом, Россия последовательно прошла ключевые этапы становления цифровых технологий — от зарождения вычислительной техники до современной экономики данных. Сегодня государство и бизнес активно развивают такие передовые направления, как искусственный интеллект, квантовые вычисления и телекоммуникационные сети нового поколения.

Сложность технологий неуклонно растет, что знаменует наступление эпохи глубокой интеграции интеллектуальных систем во все сферы жизни. Это требует от России постоянной адаптации правовой базы и инвестиций в инновации для сохранения конкурентоспособности в глобальном цифровом пространстве.

Ключевым вектором этой трансформации выступает активное внедрение регуляторных (RegTech) и надзорных (SupTech) технологий. RegTech-решения направлены на помощь субъектам финансового рынка в соблюдении постоянно усложняющихся нормативных требований [6]. Их преимущества, согласно анализу, включают повышение эффективности и точности за счет обработки больших массивов данных, устранение пробелов в комплаенс-процессах, вызванных человеческим фактором, и улучшение управления рисками [7]. В России ярким примером такой инициативы является платформа «Знай своего клиента» (KYC Service) Банка России, которая в режиме реального времени генерирует оценки уровня риска ПОД/ФТ для клиентов финансовых организаций, автоматически относя их к категориям высокого, среднего или низкого риска. В свою очередь, SupTech подразумевает использование цифровых инструментов самими надзорными и регуляторными органами. Эти технологии позволяют автоматизировать сбор, валидацию, консолидацию и визуализацию данных из разнородных источников, включая открытые, что улучшает качество анализа и позволяет выявлять нетипичные модели поведения. Практическим воплощением SupTech в России является, например, подсистема «Административное производство» Минэкономразвития, которая обеспечивает полный электронный цикл ведения дел об административных правонарушениях и интегрирована с ключевыми государственными информационными системами [8].

Параллельно с развитием RegTech и SupTech происходит стремительная цифровизация процессов идентификации клиентов, что напрямую связано с общим трендом на перевод финансовых услуг в дистанционный формат. Как подробно описывается в докладе Банка России², институт идентификации прошел значительный путь трансформации: от обязательного

² Банк России. Консультационный доклад «Становление и развитие механизмов удаленной идентификации в российской системе противодействия легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма». — Москва, 2024. Режим доступа — URL: https://www.cbr.ru/Content/Document/File/166305/Consultation_Paper_09102024.pdf.

личного присутствия до возможностей делегированной идентификации, использования электронных документов с квалифицированной подписью, данных государственных систем (ЕГРЮЛ, ЕГРИП) и биометрических платформ (ЕСИА).³ Международные стандарты ФАТФ не требуют обязательного личного присутствия, делая акцент на надежных и независимых способах верификации, что стимулирует поиск новых решений.⁴ В настоящее время Банк России совместно с Росфинмониторингом исследует возможность внедрения видеоидентификации в рамках экспериментального правового режима, признавая при этом сопутствующие риски, такие как атаки с использованием дипфейков. Международный опыт показывает широкое распространение подобных практик: от биометрической идентификации по лицу и отпечаткам пальцев в Казахстане, Беларуси и Бангладеш до использования цифровых идентификаторов (BankID в Швеции) и специализированных приложений (Itsme в Бельгии).

Зарубежный опыт цифровизации в сфере ПОД/ФТ демонстрирует разнообразие высокотехнологичных подходов. Согласно имеющимся данным, около 40 % участвующих в опросе ФАТФ юрисдикций используют передовые решения для передачи и углубленного анализа данных, причем более чем в 70 % случаев инициативы реализуются в партнерстве государства и частного сектора.

Основными целями такого цифрового взаимодействия являются мониторинг операций, управление рисками и выявление типологий противоправной деятельности. Так, в Сингапуре надзорные органы применяют методы сетевого анализа для выявления связей между юридическими и физическими лицами через множество сообщений о подозрительной деятельности, поданных в разное время, что позволяет определять области повышенного риска. В Великобритании пилотный проект TriBank был нацелен на создание единой информационной базы от нескольких банков с использованием специальных меток, обеспечивающих конфиденциальность персональных данных, что позволило повысить эффективность мониторинга межбанковских операций. В Австрии успешно функционирует централизованная система сбора и анализа отчетности (AuRep), а в США Комиссия по ценным бумагам и биржам (SEC) использует инструменты машинного обучения для анализа тональности текстов в неструктурированных отчетных формах. Эти примеры иллюстрируют применение таких технологий, как машинное и глубокое обучение, обработка естественного языка, гомоморфное шифрование и безопасные многосторонние вычисления, которые способствуют оптимизации анализа и защиты данных.

Анализ международного опыта позволяет выделить несколько сквозных принципов успешной цифровизации в сфере ПОД/ФТ. Во-первых, это приоритет безопасности и конфиденциальности данных на всех этапах, что достигается использованием передовых криптографических методов и четким нормативным регулированием. Во-вторых, эффективность напрямую зависит от качества и стандартизации данных, что требует от регуляторов разработки машиночитаемых форматов отчетности. В-третьих, очевидна тенденция к переходу от ретроспективного контроля к проактивному, предиктивному анализу рисков на основе искусственного интеллекта [9]. Наконец, наиболее устойчивые экосистемы формируются на основе государственно-частного партнерства, где регулятор выступает не только надзорным органом, но и создателем технологической инфраструктуры (например, тестовых песочниц и API) для рынка.

³ КонсультантПлюс. Положение Банка России от 15.10.2015 № 499-П (ред. от 20.07.2016) «Об идентификации кредитными организациями клиентов, представителей клиента, выгодоприобретателей и бенефициарных владельцев в целях противодействия легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма. Режим доступа — URL: https://www.consultant.ru/document/cons_doc_LAW_190354/.

⁴ ФАТФ (FATF). Критическая оценка объединения данных, совместного анализа и защиты данных. — Июль 2021. — URL: https://eurasiangroup.org/files/uploads/files/05.Stocktake-Datapooling-Collaborative-Analytics_RUS.pdf (дата обращения: 03.12.2025).

В Российской Федерации формирование цифровой экосистемы ПОД/ФТ также идет активно. Росфинмониторинг развивает автоматизированные системы оценки рисков и онлайн-сервисы, ключевым из которых является «Личный кабинет», объединяющий более 60 тысяч подотчетных организаций.⁵ Этот портал превратился в multifunctional инструмент не только для обмена сообщениями, но и для дистанционной корректировки поведения субъектов через доведение риск-оценок, проведения дистанционного обучения и предоставления обратной связи. Внедрение «Индекса качества информационного потока», визуализированного в виде дашборда в Личном кабинете, позволило увеличить оперативность выявления сомнительных операций и повысить фокус сообщений о подозрительных операциях на риски.

Со стороны кредитных организаций, в частности крупнейших банков, наблюдается активное внедрение искусственного интеллекта и машинного обучения в комплаенс-контроль. Например, ПАО «Сбербанк» использует нейросетевые модели для поиска аномалий в поведении клиентов, прогнозирования сомнительных оборотов и оценки рисков новых клиентов, что формирует целостную концепцию управления комплаенс-риском [10].

Однако масштабная цифровизация сопряжена со значительными вызовами и уязвимостями. К основным проблемам, относятся: необходимость обеспечения неприкосновенности и защиты данных (что отмечается как главная уязвимость), высокие финансовые затраты на внедрение и поддержку решений, дефицит квалифицированных IT-специалистов, нормативно-правовая неопределенность и быстрое устаревание технологий [11]. Дороговизна современных автоматизированных систем ПОД/ФТ, как подчеркивается в исследовании, ставит небольшие кредитные организации в уязвимое положение, повышая роль субъективизма в оценках и потенциально делая их более привлекательными для криминальных структур. Кроме того, технологии создают новые риски, такие как кибератаки, использование дипфейков для обмана систем биометрической верификации, а также появление более изощренных способов отмывания денег через цифровые каналы и криптоактивы [12].

Помимо технических и экономических барьеров, серьезным вызовом является поиск баланса в нормативном регулировании. С одной стороны, регламенты должны быть достаточно гибкими, чтобы не тормозить инновации и позволять внедрять перспективные технологии, такие как экспериментальные правовые режимы для видеоидентификации. С другой стороны, они обязаны обеспечивать надежный уровень безопасности и единообразие подходов для всех участников рынка. Отсутствие международно согласованных стандартов для новых технологий (например, для проверки подлинности цифровых идентификаторов или использования данных распределенных реестров) создает регуляторный арбитраж и усложняет трансграничное взаимодействие в расследованиях.

В качестве перспективных направлений развития цифровой экосистемы ПОД/ФТ можно выделить несколько трендов. Это углубленная концепция «цифрового регулятора», где надзор будет осуществляться в режиме, близком к реальному времени, на основе непрерывного потока данных, а не периодической отчетности. Активно будет развиваться направление «комплаенс как услуга» (Compliance-as-a-Service) на базе облачных платформ, что позволит малым и средним организациям эффективно выполнять требования. Также ожидается рост использования технологий синтетических данных и продвинутых симуляций для обучения алгоритмов ИИ и моделирования сложных мошеннических схем без рисков для реальных данных. Наконец, усилия будут сосредоточены на создании международных безопасных каналов обмена данными для оперативного совместного расследования транснациональных финансовых преступлений.

⁵ Росфинмониторинг. Обзор результатов обобщения и анализа правоприменительной практики контрольной (надзорной) деятельности за 2022 год. — 2023. — URL: <https://www.fedsfm.ru/results> (дата обращения: 03.12.2025).

Заключение

Проведенное исследование позволяет сделать вывод, что цифровая трансформация является неотъемлемым условием эффективного функционирования национальной системы ПОД/ФТ в современных реалиях. Интеграция таких технологий, как искусственный интеллект, анализ больших данных и сетевая аналитика, кардинально меняет подходы к мониторингу, оценке рисков и идентификации клиентов. Успешная реализация этих процессов, подтвержденная как российским опытом (платформа «Знай своего клиента», «Личный кабинет» Росфинмониторинга), так и зарубежными практиками, демонстрирует переход от реактивных мер к проактивному управлению рисками. Однако дальнейшее развитие цифровой экосистемы ПОД/ФТ невозможно без решения комплекса проблем: обеспечения кибербезопасности, унификации нормативной базы, подготовки квалифицированных кадров и укрепления механизмов государственно-частного партнерства. Только комплексный подход, сочетающий технологические инновации с продуманным регулированием, способен обеспечить надежную защиту финансовой системы от новых поколений угроз.

ЛИТЕРАТУРА

1. Цифровые технологии в российской экономике: аналитический доклад / К.О. Вишневский, Л.М. Гохберг, В.В. Дементьев [и др.]; Нац. исслед. ун-т «Высшая школа экономики». — Москва: НИУ ВШЭ, 2021. — 116 с. — ISBN 978-5-7598-2199-1. — DOI 10.17323/978-5-7598-2199-1. — EDN ZJQWHB.
2. Воронько, М.С. Генезис цифровизации и цифровой экономики в России / М.С. Воронько // Известия Санкт-Петербургского государственного экономического университета. — 2022. — № 3(135). — С. 164–168. — EDN AZDZVM.
3. Ужегов, А.О. Цифровая экономика: этапы развития и законодательное регулирование / А.О. Ужегов, О.К. Тихонова. — DOI 10.21684/2411-7897-2025-11-1-174-197 // Вестник Тюменского государственного университета. Социально-экономические и правовые исследования. — 2025. — Т. 11, № 1(41). — С. 174–197. — EDN LECXSN.
4. Romanyuk, M. Trends of the digital economy development in Russia / M. Romanyuk, M. Sukharnikova, N. Chekmareva — DOI 10.1088/1755-1315/650/1/012017. // IOP Conference Series: Earth and Environmental Science. — 2021. — Т. 650. — С. 012017. — EDN SYOCYM.
5. Цифровизация на современном этапе развития РФ / О.Ф. Ермишина, Е.А. Кочергина, А.Д. Халитова [и др.]. — DOI 10.26118/2782-4586.2024.34.57.025 // Журнал монетарной экономики и менеджмента. — 2024. — № 6. — С. 8–17. — EDN NVEQBХ.
6. Карпова, Е.Н. Современные тенденции в области цифровизации внутреннего контроля в целях противодействия отмыванию преступных доходов и финансированию терроризма в кредитных организациях / Е.Н. Карпова, И.А. Колесник, А.А. Коновалов. — DOI 10.17513/fr.42723 // Фундаментальные исследования. — 2020. — № 4. — С. 52–56. — EDN EHSVVR.
7. Кухарчик, А.С. Модель реализации механизма автоматизированного контроля в целях ПОД/ФТ в кредитных организациях / А.С. Кухарчик, Г.С. Азизов // Эпоха криптоэкономики: новые вызовы и Регтех в сфере ПОД/ФТ: материалы IV Междунар. науч.-практ. конф. междунар. сетевого ин-та в сфере ПОД/ФТ, Москва, 12–14 ноября 2018 г. — Москва: НИЯУ МИФИ, 2019. — С. 375–381. — EDN YEGZCL.

8. Курьянов, А.М. Цифровизация надзорной деятельности в сфере ПОД/ФТ / А.М. Курьянов. — DOI 10.52210/2224669X_2023_4_37 // Вестник Московского финансово-юридического университета МФЮА. — 2023. — № 4. — С. 37–49. — EDN FUOXLX.
9. Чурилова, Э.Ю. Статистический анализ направлений оптимизации работы банков по противодействию легализации преступных доходов / Э.Ю. Чурилова, В.Н. Салин // Экономика: вчера, сегодня, завтра. — 2018. — Т. 8, № 2А. — С. 147–154. — EDN OVBMMLP.
10. Ионина, Т.Р. Актуальные риски легализации преступных доходов в банковском секторе и программы по их минимизации / Т.Р. Ионина // Вестник экспертного совета. — 2019. — № 3(18). — С. 42–47. — EDN GEEKBC.
11. Чекунова, В.А. Управление бизнес-процессами в организации в рамках цифровой трансформации / В.А. Чекунова, В.А. Рычков, В. Давыденко // Цифровая экономика в контексте национальной безопасности: материалы IV Междунар. науч.-практ. конф., Москва, 14 декабря 2021 г. — Москва: НИЯУ МИФИ, 2022. — С. 114–120. — EDN OGUNUP.
12. Исроилов, Б.И. Теневая экономика и экономическая безопасность в условиях цифровизации / Б.И. Исроилов // Цифровая экономика в контексте национальной безопасности: материалы IV Междунар. науч.-практ. конф., Москва, 14 декабря 2021 г. — Москва: НИЯУ МИФИ, 2022. — С. 106–113. — EDN AXEBBX.

Mikhailova Maria Andreevna

Financial University under the Government of the Russian Federation, Moscow, Russia
E-mail: Mariya.mixajlova.00@inbox.ru

Mutsalkhanov Abduldzhappar Mutsalkhanovich

Financial University under the Government of the Russian Federation, Moscow, Russia
E-mail: 242537@edu.fa.ru

Shubin Pyotr Kirillovich

Financial University under the Government of the Russian Federation, Moscow, Russia
E-mail: 240430@edu.fa.ru

Academic adviser: **Turgaeva Aksana Albekovna**

Financial University under the Government of the Russian Federation, Moscow, Russia
E-mail: a_turgaeva@mail.ru

ORCID: <https://orcid.org/0000-0002-8374-1706>

RSCI: https://elibrary.ru/author_profile.asp?id=455538

Digital transformation of financial monitoring: from the history of technology development to modern AML/CFT solutions

Abstract. This article examines the implementation of advanced digital technologies in anti-money laundering and counter-terrorism financing (AML/CFT) systems. The relevance of this topic is driven by the rapid digital transformation of the financial landscape, the increasing sophistication of methods for concealing criminal proceeds, and the need to improve the effectiveness of national financial security systems to meet regulatory requirements. The aim of the study is to comprehensively analyze the capabilities of artificial intelligence, machine learning, big data technologies, and network analytics to identify risks, patterns, and typologies of criminal activity in the AML/CFT sphere. This paper provides a retrospective analysis of the genesis of digital technologies in Russia, beginning with the creation of the first electronic computers in the mid-20th century and ending with the current stage of development of the data economy. The author examines in detail key areas of digitalization: the implementation of regulatory (RegTech) and supervisory (SupTech) technologies, as well as the transformation of the customer identification system (including biometrics and remote identification). Particular attention is paid to the practical aspects of applying artificial intelligence technologies and big data analysis in the activities of Russian credit institutions and supervisory authorities. As a result of the study, the author systematizes the advantages of digitalization (process automation, increased analytical accuracy, the possibility of proactive risk management) and the main challenges (cybersecurity threats, shortages of qualified personnel, high financial costs, and regulatory uncertainty). The conclusion highlights the need to find a balance between technological innovation, data security, and regulatory flexibility for the further development of a sustainable AML/CFT ecosystem in the digital economy.

Keywords: digitalization; artificial intelligence (AI); financial security; risk management; big data; AML/CFT