



**Руслан Насимович
ШАНГАРАЕВ,**
профессор кафедры
государственного
управления
Дипломатической академии
МГИМО МИД России,
доктор политических наук,
кандидат экономических
наук, доцент
**r.shangaraev@
dipacademy.ru**
119021, Россия, г. Москва,
ул. Остоженка, д. 53/2



**Сергей Витальевич
ГОНЧАРОВ,**
главный советник
отдела протокола
Центра народной
дипломатии, ассистент
главного редактора
научно-аналитического
журнала
«Вестник ученых-
международников»
**goncharov.serg2018@
yandex.ru**
119021, Россия, г. Москва,
ул. Остоженка, д. 53/2

Правовое регулирование финансовой безопасности в глобальном контексте: международные стандарты и механизмы ПОД/ФТ

Аннотация. В статье рассматривается эволюция правового регулирования финансовой безопасности на глобальном уровне с акцентом на противодействие легализации преступных доходов и финансированию терроризма (ПОД/ФТ). Авторы анализируют становление и развитие ключевых международных стандартов, в первую очередь рекомендаций Группы разработки финансовых мер борьбы с отмыванием денег (ФАТФ), а также механизмы их имплементации в национальные правовые системы. Особое внимание уделено новым вызовам, связанным с цифровизацией финансовых услуг, включая использование криптоактивов и технологий искусственного интеллекта (ИИ), которые создают как новые возможности, так и риски для режимов ПОД/ФТ. В рамках разрешения научной проблемы в контексте правового регулирования технологий ИИ исследуется возникающая дилемма между необходимостью его применения для повышения эффективности финансового мониторинга и обязательством обеспечить защиту фундаментальных прав человека, таких как приватность и недискриминация. На основе сравнительного анализа международного опыта делается вывод о необходимости сбалансированного, инновационно-ориентированного, но при этом основанного на правах человека подхода к дальнейшему развитию глобальной системы финансовой безопасности.

Ключевые слова: финансовая безопасность, ПОД/ФТ, ФАТФ, международные стандарты, искусственный интеллект, регулирование ИИ, цифровизация, права человека

DOI: 10.17803/2311-5998.2026.139.3.112-122

Ruslan N. SHANGARAEV,

*Professor of the Department of Public Administration
of the Diplomatic Academy MGIMO of the Ministry of Foreign Affairs of Russia,
Dr. Sci. (Political Sciences), Cand. Sci. (Economics), Associate Professor*
r.shangaraev@dipacademy.ru
53/2, ul. Ostozhenka, Moscow, Russia, 119021

Sergey V. GONCHAROV,

*Chief Adviser of the Protocol Department
of the Center for Public Diplomacy, Assistant to the Editor-in-Chief
of the Scientific and Analytical Journal "Ir Scientists' Herald"*
goncharov.serg2018@yandex.ru
53/2, ul. Ostozhenka, Moscow, Russia, 119021

Legal Regulation of Financial Security in a Global Context: International AML/CFT Standards and Mechanisms

Abstract. *The article examines the evolution of the legal regulation of financial security at the global level with an emphasis on combating money laundering and terrorist financing (AML/CFT). The authors analyze the formation and development of key international standards, primarily the recommendations of the Financial Action Task Force on Money Laundering (FATF), as well as the mechanisms for their implementation in national legal systems. Particular attention is paid to new challenges associated with the digitalization of financial services, including the use of crypto assets and artificial intelligence (AI) technologies, which create both new opportunities and risks for AML/CFT regimes. As part of the solution of the scientific problem in the context of the legal regulation of AI technologies, the emerging dilemma is explored between the need to use it to improve the effectiveness of financial monitoring and the obligation to ensure the protection of fundamental human rights, such as privacy and non-discrimination. Based on a comparative analysis of international experience, the author concludes that there is a need for a balanced, innovation-oriented, but at the same time human rights-based approach to the further development of the global financial security system.*

Keywords: *financial security, AML/CFT, FATF, international standards, artificial intelligence, AI regulation, digitalization, human rights*

Введение

Финансовая безопасность, понимаемая как состояние защищенности финансовой системы от угроз, подрывающих ее стабильность и устойчивость, является неотъемлемым элементом национальной и глобальной безопасности. В условиях глобализации и стремительной цифровизации экономики транснациональный



характер приобрели такие угрозы, как отмывание денег (ОД) и финансирование терроризма (ФТ). Противодействие этим явлениям (ПОД/ФТ) превратилось в одну из приоритетных задач международного сотрудничества, требующую выработки единых стандартов и согласованных правовых механизмов.

Заместитель директора Департамента по вопросам новых вызовов и угроз МИД России А. Л. Лыженков и третий секретарь Департамента Я. А. Алешкина в статье «Международная «антиотмывочная» система: структура, актуальные тенденции и вызовы» рассматривают историю понятия «отмывание денег», создания и развития ФАТФ, а также стратегию ее регионализации. Целью стратегии является вовлечение все большего количества стран в единую глобальную сеть ПОД/ФТ/ФРОМУ. Авторы приходят к выводу, что «сформировавшаяся к началу 2010-х годов международная система ПОД/ФТ/ФРОМУ продолжает развиваться под влиянием финансовых инноваций, включая виртуальные активы, и социально-экономических изменений, что отражается в периодическом обновлении стандартов и методологии взаимных оценок. Однако в последние годы ее технический мандат сталкивается с нарастающей политизацией и проблемой геополитического диктата со стороны коллективного Запада, что представляет серьезную угрозу самим основам международного сотрудничества в этой сфере и будущему авторитету ФАТФ»¹.

Таким образом, имплементация стандартов ФАТФ предусматривает создание на национальном уровне комплексных правовых и институциональных рамок, включающих криминализацию ОД/ФТ, внедрение превентивных мер для финансовых институтов и нефинансовых бизнесов и профессий, учреждение финансовых разведок и обеспечение международного сотрудничества.

Однако динамичное развитие финансовых технологий (FinTech), появление децентрализованных финансов (DeFi), распространение криптоактивов и активное внедрение ИИ ставят перед традиционными системами ПОД/ФТ новые сложные вызовы. Эти технологии, с одной стороны, предлагают мощные инструменты для анализа больших данных, выявления сложных схем и автоматизации мониторинга, а с другой — создают новые уязвимости и каналы для незаконных финансовых потоков. Более того, использование ИИ в сфере безопасности, в том числе финансовой, придает практическую значимость вопросам защиты прав человека, поскольку алгоритмические системы могут приводить к нарушениям права на приватность, усилению дискриминации и ущемлению процедурных гарантий.

Современное правовое регулирование финансовой безопасности формируется в точке пересечения двух ключевых векторов развития: необходимости адаптации к технологическим инновациям для сохранения эффективности и обязательства обеспечивать верховенство права и защиту основных свобод. В статье авторы ставят цель проанализировать, как в глобальном контексте происходит поиск баланса между этими императивами через призму международных стандартов ПОД/ФТ и формирующихся подходов к регулированию ИИ.

¹ Лыженков А. Л., Алешкина Я. А. Международная «антиотмывочная» система: структура, актуальные тенденции и вызовы // Международная жизнь. 2025. № 9.

Международные стандарты ПОД/ФТ: эволюция и основные механизмы

Глобальная система ПОД/ФТ включает в себя 40 Рекомендаций ФАТФ, впервые опубликованных в 1990 г. и с тех пор неоднократно пересматривавшихся для отражения новых рисков. В 2012 г. была принята их очередная версия, структурированная вокруг нескольких ключевых блоков:

- 1) правовые основы, предусматривающие, что странам рекомендуется криминализировать отмывание денег на основе **всех** серьезных преступлений (подход заключается в указании «всех преступлений»), а также прямо криминализировать финансирование терроризма, террористических организаций и отдельных террористов. Конфискация инструментов и доходов от преступной деятельности определяется как основная цель;
- 2) превентивные меры для частного сектора. На финансовые институты и ряд нефинансовых организаций (например, юристов, риелторов, бухгалтеров) возлагаются обязательства по проведению политики «знай своего клиента» (KYC), постоянному мониторингу транзакций, выявлению и сообщению в уполномоченные органы о подозрительных операциях (STR/SAR)². Центральное место занимает оценка рисков, которая должна быть основой для построения риск-ориентированного подхода;
- 3) национальные институты и сотрудничество: страны должны создавать специализированные органы — подразделения финансовых разведок (ПФР), наделенные полномочиями по сбору, анализу и распространению информации о подозрительных операциях. Важную роль играют надзорные органы, обеспечивающие соблюдение требований частным сектором. ФАТФ подчеркивает необходимость как внутренней координации между правоохранительными, судебными и регуляторными органами, так и активного международного сотрудничества, включая правовую помощь и обмен информацией;
- 4) мониторинг и обеспечение соблюдения (комплаенс). Для оценки эффективности национальных систем ПОД/ФТ ФАТФ совместно с региональными группами по типу ФАТФ (например, МАНИВЭЛ, ЕАГ) проводит взаимные оценки. Процесс включает анализ технического соответствия законодательства Рекомендациям и оценку эффективности его применения. Страны, демонстрирующие системные недостатки, могут быть включены в «серый» список ФАТФ (повышенного мониторинга), что влечет за собой рекомендации по применению мер предосторожности со стороны других юрисдикций, а в случае отказа от сотрудничества — в «черный» список (стран с высоким уровнем риска), что может привести к серьезным экономическим и репутационным издержкам.

Например, 21.10.2021 Турция была включена в «серый список» ФАТФ **«из-за нарушений надзора в банковском деле, торговле золотом и драгоценными**

² Suspicious Transaction Report (STR) — Отчет о подозрительной операции; Suspicious Activity Report (SAR) — Отчет о подозрительной деятельности.



камнями, а также в сфере недвижимости»³. Однако уже в 2024 г. Турция «повысила эффективность мер ПОД/ФТ для выполнения обязательств по своему плану действий в отношении стратегических недостатков»⁴.

Последняя версия рекомендаций ФАТФ была принята в июне 2025 г. Она предусматривает **стратегическое усиление основополагающего принципа КУС на этапе инициации платежа (Рекомендация 16)**⁵. ФАТФ системно переводит глобальную борьбу с отмыванием денег в цифровую эпоху, смещая акцент с пассивного наблюдения на активное, технологически подкрепленное **предотвращение рисков в точке входа в финансовую систему**. Это создает более жесткие, но единые правила игры для всех участников рынка и задает вектор развития регуляторных требований на ближайшее десятилетие.

С точки зрения международного права система ФАТФ является развитой моделью «мягкого права». Ее стандарты формально не имеют обязывающей юридической силы, однако их действие обеспечивается мощными механизмами взаимного давления (на взаимной основе) и рыночными стимулами, которые формируют условия для глобального сближения подходов в сфере противодействия отмыванию денег и финансированию терроризма (ПОД/ФТ).

Цифровая трансформация и новые вызовы для режимов ПОД/ФТ

Развитие технологий кардинально меняет финансовый ландшафт, создавая для режимов ПОД/ФТ как возможности, так и серьезные угрозы.

Криптоактивы и DeFi. Анонимность или псевдонимность, децентрализация, скорость и трансграничный характер операций с криптоактивами используются для отмывания денег, схем кибермошенничества и финансирования терроризма. В ответ ФАТФ в 2019 г. распространила свои Рекомендации на поставщиков услуг, связанных с виртуальными активами (VASP), обязав их соблюдать стандарты КУС и сообщать о подозрительных операциях. Однако регулирование DeFi-протоколов, где нет централизованного оператора, остается сложной проблемой.

Искусственный интеллект как инструмент ПОД/ФТ. ИИ, в частности машинное обучение и обработка естественного языка (NLP), предлагает революционные возможности для повышения эффективности ПОД/ФТ:

³ См.: FATF исключила Турцию из «серого списка» // Ведомости. 2024. URL: <https://www.vedomosti.ru/finance/news/2024/06/28/1046844-fatf-isklyuchila> ; Шангараев Р. Н., Гончаров С. В. Роль искусственного интеллекта (ИИ) в противодействии Турции отмыванию денег и финансированию терроризма (ОД/ФТ) // Социально-политические науки. 2025. Т. 15. № 3. С. 100—107.

⁴ FATF исключила Турцию и Ямайку из серого списка и добавила туда Монако // РБК. 2024. URL: <https://www.rbc.ru/rbcfreenews/667e8dbf9a7947389fadaa72>.

⁵ Рекомендации ФАТФ: Международные стандарты по противодействию отмыванию денег, финансированию терроризма и финансированию распространения оружия массового уничтожения // ФАТФ. 2025. URL: https://cbr.ru/content/document/file/185641/3.fatf_rec_062025_rus.pdf.

- автоматизированный мониторинг транзакций (алгоритмы могут анализировать огромные объемы данных в реальном времени, выявляя сложные, неочевидные паттерны и аномалии, которые ускользают от традиционных систем, основанных на правилах);
- улучшение процедур КYC (биометрическая идентификация (распознавание лиц, отпечатки пальцев) и анализ цифровых следов повышают точность верификации клиентов);
- снижение «ложных срабатываний» (самообучающиеся системы способны минимизировать объем ложных подозрительных отчетов, что снижает операционную нагрузку на финансовые институты и правоохранительные органы);
- прогнозная аналитика (модели могут прогнозировать новые схемы ОД и ФТ, адаптируясь к меняющейся тактике преступников).

Международные организации, такие как **Ассоциация глобальной системы мобильной связи (GSMA)**, активно выступают за более глубокую интеграцию ИИ в системы ПОД/ФТ, подчеркивая, что в условиях роста объема незаконных финансовых потоков традиционные методы мониторинга теряют эффективность.

В свою очередь, новые технологии могут использоваться и для обхода систем контроля. Террористические организации могут применять ИИ для анализа уязвимостей в системах мониторинга, создания сложных цепочек транзакций, маскировки финансовых потоков и генерации фиктивных документов. Как отмечал Генеральный секретарь Парламентской ассамблеи Азии Мохаммад Реза Маджиди, «необходимы совместный поиск баланса в сфере международной безопасности и разработка четких мер по снижению рисков использования ИИ в террористических целях»⁶.

Российская позиция в отношении защиты прав в эпоху искусственного интеллекта

Российская Федерация формирует свою позицию в области международно-правового регулирования искусственного интеллекта на стыке двух стратегических императивов: стремления к технологическому лидерству в условиях глобальной конкуренции и безусловной защиты государственного суверенитета и безопасности в цифровой сфере. Данная позиция носит комплексный характер, укоренена в развитой системе национальной стратегической документации и проецируется на международную арену через призму специфического понимания угроз и возможностей, создаваемых новыми технологиями. Концептуальной основой выступают утвержденная Указом Президента РФ от 12.04.2021 № 213 «Основа государственной политики Российской Федерации в области международной информационной безопасности»⁷, а также обновленная в 2024 г. Национальная

⁶ Генсек АПА: противодействовать использованию ИИ для терроризма нужно сообща // EvrazesNews.com. 2025. URL: <http://evrazesnews.ru/index.php/news/article/view/14/47865/>.

⁷ Официальный интернет-сайт Президента России. 2021. URL: <http://www.kremlin.ru/acts/bank/46614>.



стратегия развития искусственного интеллекта на период до 2030 года⁸. В совокупности эти документы задают рамки, в которых технологическое развитие подчинено задачам обеспечения национальной безопасности, правопорядка и технологической независимости.

Фундаментальным принципом, пронизывающим российский подход как на национальном, так и на международном уровне, является принцип технологического суверенитета. Он трактуется как обеспечение необходимого уровня самостоятельности в критически важных технологических областях, включая разработку и использование отечественных решений в области ИИ, программно-аппаратных комплексов и инфраструктуры. Этот принцип является прямой реакцией на фиксируемую в официальных документах тенденцию, когда «некоторые государства вводят ограничения в отношении доступа стран к передовым и инновационным технологиям с целью усиления их технологической зависимости»⁹.

Таким образом, на международной арене Россия выступает не только за сотрудничество, но и за предотвращение создания правовых барьеров, которые могли бы консервировать технологическое доминирование узкой группы государств и усугублять цифровое неравенство.

Краеугольным камнем стал примат безопасности и суверенитета. Российская концепция международной информационной безопасности (МИБ) определяет ее как состояние глобального информационного пространства, при котором на основе норм международного права обеспечиваются мир, безопасность и стабильность. Ключевыми угрозами, актуальными и в контексте ИИ, признаются использование информационно-коммуникационных технологий (ИКТ) для подрыва суверенитета, нарушения территориальной целостности, вмешательства во внутренние дела, а также в террористических, экстремистских и преступных целях.

Следовательно, любое международно-правовое регулирование ИИ, с российской точки зрения, должно прежде всего создавать механизмы предотвращения и урегулирования межгосударственных конфликтов в киберпространстве и нейтрализовать именно эти виды угроз. Российская дипломатия последовательно продвигает идею разработки под эгидой ООН юридически обязывающего международного договора, который бы прямо запрещал использование ИКТ (в расширительной трактовке включающего и инструменты ИИ) в указанных враждебных целях.

Что касается регулирования прав человека и этических аспектов ИИ, то российская позиция носит более сдержанный и избирательный характер. Национальная стратегия развития ИИ провозглашает «принципы защиты прав и свобод человека, безопасности, прозрачности (объяснимости) и недискриминационного доступа к информации об алгоритмах»¹⁰. Однако эти принципы реализуются преимущественно в рамках национальной правовой системы и не являются доминирующим вектором внешнеполитической активности. В отличие от подхода,

⁸ Указ Президента РФ от 10 октября 2019 г. № 490 «О развитии искусственного интеллекта в Российской Федерации» // Официальный интернет-сайт Президента России. 2021. URL: <http://www.kremlin.ru/acts/bank/44731>.

⁹ Указ Президента РФ «О развитии искусственного интеллекта в Российской Федерации».

¹⁰ Указ Президента РФ «О развитии искусственного интеллекта в Российской Федерации».

закрепленного, например, в Конвенции Совета Европы об искусственном интеллекте (май 2024 г.)¹¹, который ставит во главу угла права человека, демократию и верховенство права, российская модель регулирования рассматривает ИИ, скорее, как инструмент обеспечения государственной и общественной безопасности, правопорядка и технологического развития. Поэтому участие России в глобальных этических дискуссиях об ИИ часто мотивировано не столько идеалистическими соображениями, сколько прагматичной целью защиты своих регуляторных моделей и недопущения навязывания извне стандартов, которые могли бы ограничить оперативные возможности государства в цифровой сфере.

На национальном уровне происходит активное формирование правового поля для ИИ, что служит материальной основой для международной позиции. После периода экспериментов (например, федерального эксперимента по внедрению ИИ в Москве¹²) идет работа над созданием комплексного рамочного законодательства. Предполагаемый базовый закон призван унифицировать терминологию, установить градацию рисков для различных сфер применения ИИ (с особым вниманием к «чувствительным» областям: здравоохранению, правосудию, образованию, общественной безопасности) и закрепить гибкую модель разграничения ответственности между разработчиками и пользователями. Эта внутренняя работа позволяет России вести международный диалог, опираясь на собственный практический опыт регулирования, и отстаивать право на специфический, контекстно зависимый подход, отличный от европейской модели жесткого горизонтального регулирования.

Стоит отметить, что в рамках своего выступления на X Международной конференции по искусственному интеллекту и машинному обучению AI Journey в ноябре 2025 г. Президент России дал поручение о формировании национального плана по внедрению генеративного искусственного интеллекта на уровне всей страны, в разрезе отраслей и регионов. Целью данного плана является обеспечение фронтального внедрения технологий ИИ в промышленность, транспорт, здравоохранение, госуправление и другие сектора для достижения целевого показателя Национальной стратегии — вклада ИИ в ВВП страны более 11 трлн руб. к 2030 г. Для практической координации этой масштабной работы В. В. Путин указал «на необходимость создания реального штаба руководства, обладающего административным ресурсом для постановки задач и контроля их исполнения»¹³.

¹¹ Искусственный интеллект с европейским акцентом // HSEdaily. 2025. URL: <https://daily.hse.ru/post/iskusstvennyi-intellekt-s-evropeiskim-akcentom>.

¹² Федеральный закон от 24.04.2020 № 123-ФЗ «О проведении эксперимента по установлению специального регулирования в целях создания необходимых условий для разработки и внедрения технологий искусственного интеллекта в субъекте Российской Федерации — городе федерального значения Москве и внесении изменений в статьи 6 и 10 Федерального закона “О персональных данных”» // СПС «КонсультантПлюс».

¹³ Путин поручил создать национальный план внедрения искусственного интеллекта // Российская газета. 19.11.2025.



Защита прав человека в эпоху ИИ: новый контекст для финансовой безопасности

Активное внедрение ИИ в сферу безопасности, включая финансовый мониторинг, выдвигает на первый план этико-правовые дилеммы. Международная практика последних лет демонстрирует растущее число судебных прецедентов, связанных с нарушением фундаментальных прав системами на основе ИИ.

К рискам, связанным с применением ИИ в ПОД/ФТ и смежных областях, относится, например, нарушение приватности и защиты данных. Такой риск предусматривает массовый сбор и анализ финансовых и иных данных, создание детальных профилей. Отслеживание связей и перемещений лиц представляют угрозу «праву на частную жизнь»¹⁴, гарантированному, в частности, ст. 17 Международного пакта о гражданских и политических правах.

Кроме того, риском может быть алгоритмическая дискриминация, а именно системы машинного обучения могут воспроизводить и усиливать системные предубеждения, заложенные в обучающих данных. Это может приводить к несправедливому профилированию клиентов по расовому, этническому, социальному или иному признаку, что нарушает принцип недискриминации. Примером служат системы оценки рецидивизма в США, которые показали предвзятость в отношении афроамериканцев.

Следующим риском может служить отсутствие прозрачности и подотчетности. Сложность алгоритмов связана с тем, что проблема «черного ящика» (Black Box Problem) затрудняет понимание логики принятия решений, что подрывает право на справедливое судебное разбирательство и эффективные средства правовой защиты. Голландский суд, отменяя систему SyRI для выявления мошенничества с пособиями, особо указал на непрозрачность и дискриминационный характер ее работы.

Наряду с вышеперечисленными рисками к последним может также относиться автоматизация предубеждений, т.е. слепая вера в «объективность» алгоритмов. Она может привести к делегированию критически важных решений, влияющих на права и свободы человека (например, о блокировке счетов, включении в «черные списки»), непроверенным системам, лишенным человеческого сочувствия и контекстуального понимания.

Перспективы и выводы: поиск баланса в глобальном регулировании

Будущее правового регулирования финансовой безопасности будет определяться способностью международного сообщества найти сбалансированные ответы на двойственный вызов технологий.

В этой связи можно обозначить следующие перспективы развития:

- 1) углубление международного сотрудничества (транснациональный характер как финансовых преступлений, так и технологических платформ требует

¹⁴ Международный пакт о гражданских и политических правах // URL: https://www.un.org/ru/documents/decl_conv/conventions/pactpol.shtml.

усиления координации между странами, регуляторами и международными организациями. Необходимы общие стандарты для регулирования крипто-активов и обмена информацией о киберугрозах);

- 2) интеграция инноваций в правовые рамки (регуляторам необходимо развивать компетенции (RegTech, SupTech) для понимания новых технологий и создания регулятивного механизма, позволяющего безопасно тестировать инновационные решения в области ПОД/ФТ);
- 3) развитие «ответственного ИИ» в сфере безопасности (ключевым станет внедрение принципов «прозрачность по замыслу» и «справедливость по замыслу» при разработке ИИ для финансового мониторинга. Это включает обеспечение объяснимости решений алгоритмов, регулярный аудит на предмет смещений, обязательный человеческий надзор для критически важных решений);
- 4) обновление международных стандартов (ожидается, что ФАТФ и другие органы будут далее развивать свои рекомендации, более детально охватывая риски, связанные с цифровыми активами, и формулировать ориентиры для этичного и эффективного использования ИИ в целях ПОД/ФТ).

Заключение

Правовое регулирование финансовой безопасности в глобальном контексте переживает период глубокой трансформации. Сформировавшийся вокруг стандартов ФАТФ режим доказал свою жизнеспособность, обеспечивая основу для международного сотрудничества. Однако цифровая революция требует его существенной адаптации.

Главный вызов современности заключается не в выборе между безопасностью и инновациями или между безопасностью и правами человека, а в их гармоничном совмещении. Искусственный интеллект как наиболее амбивалентная технология нашего времени является ярким примером этого. Его потенциал для повышения эффективности борьбы с отмыванием денег и финансированием терроризма огромен, но его применение должно быть жестко встроено в правовые рамки, гарантирующие уважение человеческого достоинства, приватности, равенства и справедливости.

Таким образом, формирование устойчивой и легитимной глобальной системы финансовой безопасности в XXI в. будет зависеть от способности международного сообщества разработать и внедрить инклюзивные, технологически грамотные и ориентированные на права человека стандарты и механизмы регулирования. Это сложная задача, требующая диалога между государствами, регуляторами, технологическими компаниями, финансовыми институтами и гражданским обществом, но ее решение необходимо для построения безопасного и справедливого цифрового будущего.



БИБЛИОГРАФИЯ

1. *Лыженков А. Л., Алешкина Я. А.* Международная «антиотмывочная» система: структура, актуальные тенденции и вызовы // *Международная жизнь*. — 2025. — № 9.
2. *Шангараев Р. Н., Гончаров С. В.* Роль искусственного интеллекта (ИИ) в противодействии Турции отмыванию денег и финансированию терроризма (ОД/ФТ) // *Социально-политические науки*. — 2025. — Т. 15. — № 3. — С. 100—107.