

УДК 336.71:343.359 ББК 65.262.1+67.408

Хантаев Алан Халгаевич
ОУП ВО «Академия труда и социальных отношений»
Khantaev Alan Khalgaevich
Academy of Labor and Social Relations

**ПРОТИВОДЕЙСТВИЕ ОТМЫВАНИЮ ДЕНЕГ В БАНКОВСКОМ СЕКТОРЕ:
ПРАВОВЫЕ И ТЕХНОЛОГИЧЕСКИЕ АСПЕКТЫ
COUNTERING MONEY LAUNDERING IN THE BANKING SECTOR:
LEGAL AND TECHNOLOGICAL ASPECTS**

Аннотация. В статье рассматривается современная система противодействия легализации доходов, полученных преступным путем, в банковском секторе. Автор анализирует правовую природу ПОД/ФТ как элемента финансовой безопасности, раскрывает роль риск-ориентированного подхода, идентификации клиентов, внутреннего контроля и надзора Банка России. Особое внимание уделяется соотношению национального законодательства с рекомендациями FATF, актуальным требованиям к правилам внутреннего контроля кредитных организаций, цифровой идентификации, автоматизированному мониторингу операций и рискам, связанным с виртуальными активами. Подчеркивается, что эффективность антиотмывочного регулирования определяется не количеством формальных процедур, а способностью банков выявлять экономический смысл операций, оценивать клиентский риск и своевременно взаимодействовать с уполномоченными органами. Сделан вывод о необходимости развития комплаенс-систем на основе технологической надежности, профессионального суждения, защиты прав добросовестных клиентов и межведомственного обмена информацией.

Abstract. The article examines the modern system for countering the legalization of proceeds of crime in the banking sector. The author analyzes the legal nature of AML/CFT as an element of financial security and reveals the role of the risk-based approach, customer identification, internal control and supervision by the Bank of Russia. Particular attention is paid to the correlation between national legislation and FATF Recommendations, current requirements for internal control rules of credit institutions, digital identification, automated transaction monitoring and risks associated with virtual assets. The article emphasizes that the effectiveness of anti-money laundering regulation is determined not by the number of formal procedures, but by banks' ability to identify the economic substance of transactions, assess customer risk and interact with authorized bodies in a timely manner. The conclusion is made that compliance systems should develop on the basis of technological reliability, professional judgment, protection of bona fide customers' rights and interagency information exchange.

Ключевые слова: Отмывание денег, банковский сектор, ПОД/ФТ, внутренний контроль, Банк России, FATF, комплаенс, цифровая идентификация.

Keywords: Money laundering, banking sector, AML/CFT, internal control, Bank of Russia, FATF, compliance, digital identification.

Для цитирования: Хантаев А. Х. Противодействие отмыванию денег в банковском секторе: правовые и технологические аспекты //

© Хантаев А. Х., 2026

For citation: Khantaev A. Kh. Countering money laundering in the banking sector: legal and technological aspects //

Введение

Легализация доходов, полученных преступным путем, представляет угрозу не только для отдельных банков, но и для устойчивости финансовой системы в целом. Через банковский сектор преступные доходы могут вводиться в законный оборот, маскироваться под обычные



коммерческие операции, использоваться для вывода капитала, финансирования терроризма и иных противоправных целей. Поэтому противодействие отмыванию денег является одной из ключевых задач банковского регулирования и финансового надзора [1].

Банк в системе ПОД/ФТ выполняет двойственную функцию. С одной стороны, он оказывает клиентам финансовые услуги и обязан обеспечивать доступность законных операций. С другой стороны, банк является субъектом первичного финансового мониторинга, который должен выявлять подозрительные операции, оценивать риски клиентов и передавать предусмотренную законом информацию в уполномоченные органы. Это требует от кредитной организации сочетания клиентского сервиса, правовой дисциплины и развитой комплаенс-инфраструктуры.

Международные стандарты в данной сфере формируются прежде всего FATF. Рекомендации FATF закрепляют риск-ориентированный подход, требования к надлежащей проверке клиентов, прозрачности бенефициарной собственности, обмену информацией и контролю за новыми технологиями [2]. Российское законодательство развивает эти подходы в Федеральном законе № 115-ФЗ, а также в нормативных актах Банка России, устанавливающих требования к внутреннему контролю и идентификации клиентов [1; 3; 4].

Цель настоящей статьи заключается в анализе современных правовых и организационных механизмов противодействия отмыванию денежных средств в банковском секторе. Для достижения цели рассматриваются правовые основы ПОД/ФТ, риск-ориентированный подход, процедуры KYC и CDD, автоматизированный мониторинг, цифровая идентификация, виртуальные активы и проблемы защиты прав добросовестных клиентов.

Правовые основы ПОД/ФТ в банковском секторе

Российская система противодействия отмыванию денег строится на Федеральном законе № 115-ФЗ. Данный закон определяет обязанности организаций, осуществляющих операции с денежными средствами или иным имуществом, включая кредитные организации. Для банков особенно важны требования об идентификации клиентов, представителей клиента, выгодоприобретателей и бенефициарных владельцев, выявлении операций, подлежащих обязательному контролю, и направлении информации в Росфинмониторинг [1, ст. 7].

Правовая модель ПОД/ФТ не предполагает механического отказа от любых нетипичных операций. Ее смысл состоит в оценке риска и выявлении экономически необъяснимого поведения. Поэтому банк должен анализировать не только формальные реквизиты операции, но и ее хозяйственную цель, профиль клиента, деловую репутацию, источник происхождения средств, связь операции с обычной деятельностью клиента и наличие признаков искусственного дробления платежей.

В 2025 году требования к правилам внутреннего контроля кредитных организаций были актуализированы новым Положением Банка России № 860-П. Этот акт заменил прежнее регулирование и закрепил современные подходы к организации ПВК по ПОД/ФТ/ЭД, включая управление риском, роль специального должностного лица, участие различных подразделений банка и учет информации Банка России о рисках клиентов [3]. Такая актуализация отражает усложнение банковских операций и необходимость более гибкого контроля.

Идентификация клиентов регулируется отдельными нормативными требованиями. Положение Банка России № 499-П устанавливает порядок идентификации кредитными организациями клиентов, представителей клиента, выгодоприобретателей и бенефициарных владельцев [4]. На практике это означает сбор и проверку сведений о клиенте, выяснение структуры владения, оценку полномочий представителей и обновление информации в процессе обслуживания.

В научной литературе подчеркивается, что противодействие отмыванию денег нельзя рассматривать только как вопрос уголовно-правовой репрессии. Значительная часть работы переносится на уровень финансовых посредников, которые должны заранее выявлять подозрительные модели поведения и предотвращать использование легального банковского



оборота в преступных целях [5, с. 44–46]. Такой подход повышает значение внутреннего контроля и профессиональной подготовки банковских сотрудников.

Институциональные основы ПОД/ФТ включают взаимодействие национальных регуляторов, банков, правоохранительных органов, финансовой разведки и международных организаций. Исследователи отмечают, что эффективность системы зависит от согласованности этих элементов и от способности участников обмениваться информацией без нарушения прав добросовестных клиентов [6, с. 223–228].

Риск-ориентированный подход и банковский комплаенс

Современная антиотмывочная система основывается на риск-ориентированном подходе. Его преимущество заключается в том, что ресурсы банка направляются прежде всего на тех клиентов и операции, которые действительно несут повышенную угрозу. Такой подход отличается от формального контроля, при котором одинаковые процедуры применяются ко всем клиентам независимо от их профиля, вида деятельности и характера операций.

Оценка риска клиента должна учитывать организационно-правовую форму, сферу деятельности, страновую и региональную составляющую, структуру собственности, наличие политически значимых лиц, частоту и объем операций, использование наличных денежных средств, дистанционных каналов и трансграничных переводов. Чем сложнее и непрозрачнее структура клиента, тем выше требования к документальному подтверждению экономического смысла операций.

Процедуры KYC и CDD составляют ядро банковского комплаенса. Они позволяют банку понять, кто является клиентом, в чьих интересах он действует, какие операции для него обычны и какие источники средств являются экономически объяснимыми. Усиленная проверка применяется в ситуациях повышенного риска: при обслуживании политически значимых лиц, сложных корпоративных структур, клиентов из высокорисковых юрисдикций или операций, не соответствующих заявленному профилю.

Особое значение имеет обновление сведений о клиентах. Первичная идентификация не может быть достаточной на протяжении всего периода обслуживания, поскольку бизнес-модель клиента, состав участников, бенефициары и характер операций могут изменяться. Если банк не поддерживает сведения в актуальном состоянии, его риск-модель становится формальной и перестает отражать реальное положение дел.

Комплаенс в банке должен быть организационно самостоятельным и одновременно связанным с другими подразделениями: юридической службой, риск-менеджментом, внутренним аудитом, информационной безопасностью и операционными подразделениями. Изолированная комплаенс-служба не способна эффективно выявлять сложные схемы, поскольку признаки риска часто проявляются на стыке правовых, технологических и экономических данных.

Банк России на своем официальном сайте указывает, что основные положения, регулирующие вопросы ПОД/ФТ/ФРОМУ, содержатся в Федеральном законе № 115-ФЗ [7]. Однако практическое значение имеют не только нормы закона, но и способность кредитной организации встроить их в повседневные процессы: открытие счета, проведение платежей, обслуживание корпоративных клиентов, анализ операций и принятие решений о мерах реагирования.

Цифровые технологии, виртуальные активы и новые риски

Развитие цифровых технологий существенно изменило инструменты противодействия отмыванию денег. Банки используют автоматизированный мониторинг операций, сценарные правила, поведенческую аналитику и модели выявления аномалий. Такие системы помогают обнаруживать дробление платежей, транзитные операции, необычные цепочки переводов, повторяющиеся операции между связанными лицами и резкое изменение клиентского поведения.



Однако автоматизация не должна превращаться в безусловную замену профессионального суждения. Алгоритм может указать на нетипичность операции, но окончательная оценка должна учитывать документы клиента, экономический смысл сделки, отраслевую специфику и добросовестные объяснения. Чрезмерная автоматизация без человеческой проверки создает риск необоснованных отказов, блокировок и нарушения прав клиентов.

Цифровая идентификация также имеет двойственный характер. С одной стороны, она ускоряет клиентские процедуры, снижает затраты и расширяет доступ к банковским услугам. С другой стороны, цифровая идентичность требует надежной защиты персональных данных, устойчивости информационных систем и ясных правил оспаривания ошибочных решений. Для ПОД/ФТ это особенно важно, поскольку ошибка в идентификации может привести как к пропуску подозрительного клиента, так и к необоснованному ограничению прав добросовестного лица.

Отдельную группу рисков образуют виртуальные активы. FATF указывает, что виртуальные активы и провайдеры услуг, связанных с ними, требуют применения специальных мер контроля, поскольку трансграничность операций, технологическая сложность и возможность использования анонимизирующих инструментов осложняют выявление конечных участников платежа [8, р. 9–13]. Для банков это означает необходимость учитывать связь клиентов с виртуальными активами при оценке общего уровня риска.

Блокчейн-технологии не являются ни абсолютной угрозой, ни универсальным решением. Прозрачность распределенного реестра может помочь последующему анализу цепочек операций, однако использование смешивающих сервисов, децентрализованных платформ и сложных трансграничных маршрутов снижает эффективность традиционного контроля. Поэтому банк должен оценивать не только сам факт использования цифровых инструментов, но и экономический контекст операций.

Новые технологии усиливают значение межведомственного обмена информацией. Банковская комплаенс-система не может самостоятельно видеть весь финансовый маршрут клиента, особенно если операции проходят через разные юрисдикции и сервисы. Поэтому развитие ПОД/ФТ требует надежных каналов взаимодействия между банками, Банком России, Росфинмониторингом, правоохранительными органами и, в необходимых случаях, иностранными компетентными органами.

Проблемы правоприменения

Одной из основных проблем ПОД/ФТ остается риск формализации. Банк может иметь правила внутреннего контроля, назначенное ответственное лицо и автоматизированные системы, но при этом фактически не выявлять экономический смысл подозрительных операций. Формальное соблюдение процедур создает видимость контроля, однако не обеспечивает реального предотвращения легализации преступных доходов.

Вторая проблема связана с конфликтом между антиотмывочными мерами и правами клиентов. Отказ в проведении операции, расторжение договора банковского счета или ограничение дистанционного обслуживания могут серьезно затронуть хозяйственную деятельность клиента. Поэтому решения банка должны быть документально обоснованы, соразмерны выявленному риску и подлежать эффективному обжалованию. Иначе ПОД/ФТ может восприниматься бизнесом как источник неопределенности, а не как механизм финансовой безопасности.

Третья проблема – внутренняя недобросовестность. Даже развитая система контроля может быть ослаблена, если сотрудники банка сознательно игнорируют признаки подозрительности, помогают клиентам обходить процедуры или участвуют в подделке документов. Следовательно, ПОД/ФТ должно включать не только внешний мониторинг клиентов, но и внутренний контроль за действиями работников, обучение, разделение полномочий и независимый аудит.



Четвертая проблема состоит в высокой динамике преступных схем. После усиления контроля в одной области злоумышленники быстро переходят к новым инструментам: номинальным компаниям, сложным платежным цепочкам, электронным средствам платежа, виртуальным активам, подставным лицам или операциям с фиктивным экономическим основанием. Поэтому банковский комплаенс должен быть адаптивным и регулярно обновлять типологии подозрительных операций.

Наконец, существенным вызовом является подготовка специалистов. Качественный финансовый мониторинг требует знания права, банковских операций, бухгалтерского учета, информационных технологий и криминальных типологий. Недостаточная квалификация сотрудников приводит либо к пропуску подозрительных операций, либо к чрезмерному ограничению добросовестных клиентов.

Заключение

Противодействие отмыванию денежных средств в банковском секторе представляет собой комплексный правовой и организационный механизм. Его основу составляют Федеральный закон № 115-ФЗ, стандарты FATF, нормативные акты Банка России, правила внутреннего контроля кредитных организаций и практические процедуры идентификации, мониторинга и оценки риска [1; 2; 3; 4].

Эффективность ПОД/ФТ определяется не количеством документов, а реальной способностью банка понимать клиента, анализировать экономический смысл операций и своевременно реагировать на признаки подозрительности. Риск-ориентированный подход позволяет сосредоточить внимание на наиболее опасных направлениях, но требует качественных данных, профессионального суждения и постоянного обновления внутренних процедур.

Цифровизация банковских услуг открывает новые возможности для мониторинга, но одновременно создает новые риски: ошибки автоматизированных систем, угрозы персональным данным, сложности контроля виртуальных активов и трансграничных операций. Поэтому дальнейшее развитие ПОД/ФТ должно строиться на балансе финансовой безопасности, технологической надежности и защиты прав добросовестных клиентов. Только такая модель способна обеспечить устойчивость банковского сектора и доверие к финансовой системе

Список литературы:

1. Федеральный закон от 07.08.2001 № 115-ФЗ «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма» [Электронный ресурс]. URL: https://www.consultant.ru/document/cons_doc_LAW_32834/ (дата обращения: 12.06.2026).
2. Financial Action Task Force (FATF). International Standards on Combating Money Laundering and the Financing of Terrorism and Proliferation. The FATF Recommendations. As amended October 2025 [Electronic resource]. URL: <https://www.fatf-gafi.org/en/publications/Fatfrecommendations/Fatf-recommendations.html> (date of access: 12.06.2026).
3. Положение Банка России от 18.06.2025 № 860-П «О требованиях к правилам внутреннего контроля кредитной организации, филиала иностранного банка, через который иностранный банк осуществляет деятельность на территории Российской Федерации, в целях противодействия легализации (отмыванию) доходов, полученных преступным путем, финансированию терроризма и экстремистской деятельности» [Электронный ресурс]. URL: https://www.consultant.ru/document/cons_doc_LAW_512202/ (дата обращения: 12.06.2026).
4. Положение Банка России от 15.10.2015 № 499-П «Об идентификации кредитными организациями клиентов, представителей клиента, выгодоприобретателей и бенефициарных владельцев в целях противодействия легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма» [Электронный ресурс]. URL: https://www.consultant.ru/document/cons_doc_LAW_190354/ (дата обращения: 12.06.2026).



5. Нугуманов А. Р. Отмывание денег: оценка состояния и мер противодействия // Современная наука. 2022. № 1. С. 44–46.
6. Сюпова М. С., Шапилова Д. Е. Институциональные основы международной системы ПОД/ФТ // Ученые заметки ТОГУ. 2025. Т. 16. № 1. С. 223–228.
7. Банк России. Противодействие отмыванию денег и валютный контроль [Электронный ресурс]. URL: https://www.cbr.ru/counteraction_m_ter/ (дата обращения: 12.06.2026).
8. Financial Action Task Force (FATF). Targeted Update on Implementation of the FATF Standards on Virtual Assets and Virtual Asset Service Providers. 2025 [Electronic resource]. URL: <https://www.fatf-gafi.org/content/dam/fatf-gafi/recommendations/2025-Targeted-Update-VA-VASPs.pdf.coredownload.pdf> (date of access: 12.06.2026)

