Колесникова Александра Юрьевна
студентка
ФГБОУ ВО «Санкт-Петербургский государственный
архитектурно-строительный университет»
г. Санкт-Петербург

СОВРЕМЕННЫЕ ПРОБЛЕМЫ ОБЕСПЕЧЕНИЯ КОНТРОЛЯ ЗА ФИНАНСОВЫМИ МАХИНАЦИЯМИ

***Аннотация**: финансовые махинации представляют собой одну из наиболее серьезных угроз современной экономики России. Усложнение финансовых операций, развитие новых технологий и глобализация усугубляют проблемы контроля за финансовыми преступлениями. В статье рассмотрены правовые основы для регулирования финансовых инструментов, таких как криптовалюты и технологии блокчейн, проблема нехватки специалистов, способных эффективно выявлять и анализировать финансовые махинации, особенно в условиях цифровизации экономики.*

***Ключевые слова**: финансовые махинации, мошенничество, криптовалюты, блокчейн, анализ, регулирование, контроль, трансакции.*

В условиях стремительного развития финансовых технологий и глобализации экономики проблемы контроля над финансовыми махинациями становятся всё более актуальными. Проблема финансовых преступлений имеет глубокие корни и затрагивает не только экономическую сферу, но и социальные аспекты, влияя на доверие граждан к финансовым институтам и государственным организациям. В России, как и во всем мире, наблюдается значительное увеличение числа случаев мошенничества, связанных с использованием как традиционных финансовых инструментов, так и новейших технологий, таких как блокчейн и криптовалюты.

В последние годы фиксируется рост случаев мошенничества в финансовом секторе, включая, но не ограничиваясь, схемами отмывания денег, мошенничеством с банковскими картами и киберпреступлениями. Развитие цифровых

финансовых услуг создает новые возможности как для законопослушных пользователей, так и для преступников, что требует адаптации и обновления законодательных норм и методов контроля [1].

Одной из ключевых проблем является недостаточная эффективность существующих систем мониторинга и анализа финансовых транзакций. Большинство институтов, занимающихся контролем, сталкиваются с технологическими и кадровыми ограничениями. Многие граждане не обладают достаточной финансовой грамотностью и часто становятся жертвами мошенников, не понимая характер и риск своих действий на финансовых рынках.

Нехватка квалифицированных специалистов в области финансового мониторинга усугубляет ситуацию, затрудняя выявление и предотвращение финансовых преступлений. Несмотря на существующие законодательные меры, направленные на борьбу с финансовыми махинациями, многие факторы указывают на недостаточную эффективность уровня нормативно-правовой базы. Кроме того, большинство финансовых институтов не успевают адаптироваться к стремительным изменениям в технологии и законодательстве. На сегодняшний день многие банки используют устаревшие системы мониторинга, что делает их уязвимыми перед лицом новых угроз.

Одной из проблем, с которыми сталкиваются регулирующие и контролирующие органы, является нехватка финансовых и технических ресурсов. В условиях глобализации и финансовой интеграции объемы транзакций стремительно растут, что требует от органов контроля значительных затрат на развитие инфраструктуры, программного обеспечения и технологий. Многочисленные бюрократические процедуры и ограниченные бюджетные ассигнования часто приводят к тому, что организации не могут позволить себе обновление технологий, внедрение новых систем мониторинга и анализа данных [3].

Блокчейн и криптовалюты представляют собой особенно заметные возможности для мошенников, так как их анонимность и децентрализованная природа зачастую усложняют идентификацию и пресечение подобных преступлений. Блокчейн представляет собой распределённый реестр, в котором данные

хранятся в виде цепочки блоков, защищённых криптографическими методами. Эта технология обеспечивает прозрачность, безопасность и неизменяемость информации, что теоретически делает её устойчивой к мошенническим действиям. Однако именно эти особенности определяют два ключевых направления мошенничества: анонимность пользователей – участники сетей, использующих криптовалюты, зачастую могут оставаться анонимными, что создает дополнительные сложности для правоохранительных органов в их усилиях по выявлению и задержанию мошенников; необратимость транзакций – системы, работающие на основе блокчейна, не позволяют отменить транзакции. Это означает, что после совершения мошеннической операции, вернуть средства становится весьма проблематично.

Финансовые пирамиды и схемы Ponzi – эти схемы продолжают существовать даже в окружении новейших технологий. Мошенники создают видимость прибыльных инвестиционных проектов, обещая высокие доходы, но фактически выплачивают деньги за счет новых вкладчиков [4].

При применении фишинг-взломов злоумышленники используют различные методы, чтобы получить доступ к частным ключам или учетным данным пользователей. Это может происходить через поддельные сайты или рассылки, создающие видимость законных сервисов [1].

На данный момент остаются открытыми вопросы эффективного регулирования и контроля за трансакциями в блокчейне. Разработка правовых норм и стандартов, направленных на борьбу с мошенничеством в этой сфере, становится необходимым в условиях постоянно меняющегося технологического ландшафта.

Технологические решения, такие как использование систем мониторинга и анализа транзакций, также могут способствовать выявлению аномальных действий. Платформы, работающие в области противодействия отмыванию денег, могут использовать алгоритмы машинного обучения для анализа данных и выявления потенциально мошеннических транзакций [2].

Существующая законодательная база также требует пересмотра и адаптации к новым рыночным реальностям. В России отсутствуют полноценные

механизмы, позволяющие эффективно регулировать новые финансовые инструменты и технологии, что создает правовые пробелы. Это требует совместных усилий государственных органов, научных исследователей и представителей бизнеса для разработки эффективных стратегий контроля и профилактики финансовых махинаций.

Растущая анонимность финансовых операций, особенно в контексте использования децентрализованных финансовых платформ, создает дополнительные трудности для мониторинга и предотвращения мошеннических схем. Важным шагом вперед является внедрение технологий анализа больших данных и машинного обучения, которые способны выявлять аномальные транзакции и в реальном времени информировать о подозрительных действиях [3].

Контроль над финансовыми махинациями в России представляет собой комплексную задачу, требующую интеграции усилий различных секторов. Устранение существующих пробелов в законодательстве, повышение уровня финансовой грамотности и подготовка квалифицированных кадров должны стать приоритетными направлениями в борьбе с финансовыми преступлениями. Это позволит не только улучшить безопасность финансовой системы, но и способствовать её устойчивому развитию.

Список литературы

1. Ершова С.А. Цифровизация и экономическая безопасность до и после пандемии коронавирусной инфекции / С.А. Ершова, Т.Н. Орловская // Экономическая безопасность строительной отрасли: опыт, проблемы, перспективы: материалы региональной научно-практической конференции с международным участием (Санкт-Петербург, 27–28 апреля 2021 года). – СПб.: Санкт-Петербургский государственный архитектурно-строительный университет, 2021. – С. 75–86. – EDN GLYUXO.

2. Моденов А.К. Методологические аспекты формирования информационно-аналитической деятельности в системе экономической безопасности / А.К. Моденов // Проблемы экономической безопасности в условиях цифровизации экономики: материалы Межрегиональной научно-практической

конференции с международным участием (Санкт-Петербург, 23 марта 2022 года). – СПб.: Санкт-Петербургский государственный архитектурно-строительный университет, 2022. – С. 77–95. – EDN STWPZD.

3. Моденов А.К. Экономика и преступность в постковидный период: угрозы экономической безопасности / А.К. Моденов, А.И. Васильченко // Russian Economic Bulletin. – 2022. – Т. 5. №2. – С. 241–247. – EDN KIBQXE.

4. Харланов А.С. Киберпреступность в период пандемии коронавируса COVID-19 / А.С. Харланов, А.А. Бобошко, А.В. Гросу // Закон и власть. – 2021. – №3. – С. 48–52. – EDN HUGGBI.