Цыцорина Алена Алексеевна
магистрант
Цельникер Григорий Феликсович
канд. юрид. наук, доцент
ФГАОУ ВО «Самарский государственный
экономический университет»
г. Самара, Самарская область

DOI 10.31483/r-115688

БОРЬБА С ФИНАНСОВЫМ МОШЕННИЧЕСТВОМ: ПРАВОВЫЕ АСПЕКТЫ И ЭФФЕКТИВНОСТЬ МЕР ПРОТИВОДЕЙСТВИЯ

Аннотация*: статья представляет собой всесторонний анализ правового регулирования борьбы с финансовым мошенничеством в России. Рассмотрены ключевые аспекты законодательства, устанавливающие ответственность за финансовое мошенничество, а также практические механизмы противодействия, включая превентивные меры, правоохранительные действия, технологические решения и международный опыт. В статье выделены проблемы и недостатки в действующей системе борьбы с финансовым мошенничеством в России. Отмечено, что, несмотря на принимаемые меры, уровень финансового мошенничества остается высоким.*

Ключевые слова*: финансовое мошенничество, финансовая грамотность, борьба с финансовым мошенничеством.*

Финансовым мошенничеством является серьезная проблема, затрагивающая людей, предприятия не только в России, но и во всем мире. Мошенники стараются изобретать новые способы обмана людей, приводя их к финансовым потерям, и, конечно же к эмоциональным страданиям в том числе. В мире уже создано множество способов противодействия, однако мошенничество в сфере финансов все равно процветает.

На сегодняшний день в России также растут финансовые преступления, включая мошенничество с инвестициями, кредитованием, страхованием. Еже-

годно от таких преступлений страдают миллионы граждан, а потери исчисляются миллиардами рублей. Новые технологии и схемы – это то, что помогает мошенникам совершенствовать свои методы обмана людей и компаний.

Если говорить о доверии, что финансовое мошенничество очень сильно подрывает доверие ко всему финансовому институту и рынкам, что отрицательно сказывается на инвестициях и экономическом росте.

Следует понимать, что мошенники используют самые уязвимые слои населения, усугубляют социальное неравенство.

Масштабы финансового мошенничества, к сожалению, не ограничены, ведь чаще всего его используют для отмывания денег, а также финансового терроризма, что в свою очередь угрожает безопасности России.

На основе данных размышлений можно сделать вывод, что борьба с финансовым мошенничеством – это вопрос национальной безопасности и социального благополучия, и требует решения путем использования комплексного подхода и неотложных мер противодействия.

Несмотря на исследования правовых норм, отсутствует достаточный анализ реальной эффективности мер по противодействию финансового мошенничества.

Например, работы Бойко С.Я. («Мошенничество в сфере кредитования» [3]) и Яковлева А.Б. («Противодействие легализации (отмыванию) доходов, полученных преступным путем, финансирование терроризма как вид финансового контроля» [9]) сосредоточены преимущественно на правовом регулировании, не уделяя внимание практике применения норм и ее результатам.

Как мы все понимаем, теория без практики – неполная картина, а бывает, что и вовсе другая. Правовые нормы сами по себе не гарантируют эффективности. Важно изучать, как они работают на практике, какие проблемы возникают при их применении, как можно улучшить механизмы исполнения. Чрезмерное сосредоточение на теоретических аспектах может привести к формальному подходу, с которым сталкиваются граждане.

Финансовое мошенничество – это достаточно сложное преступление, требующее участие сразу нескольких органов. Прокуратура, налоговая инспекция и банки имеют разные компетенции и инструменты для борьбы с мошенничеством. А отсутствие координации между органами приводит к противоречивым действиям, дублированию усилий и, в итоге, к снижению эффективности борьбы с мошенничеством.

К сожалению, исследователи в данной сфере не уделяют достаточного внимания использованию новых технологий в финансовом мошенничестве и разработке новых методов противодействия с опорой на законодательство РФ.

Например, анализируя научную работу Несмеяновой А.В. по теме «Мошенничество с использованием информационно-телекоммуникационных технологий как угроза экономической безопасности России», здесь видим в основном только статистические данные подобных преступлений [6].

Как уже упоминалось выше, мошенники используют новые технологии для совершенствования преступлений. Это может быть и использование интернета, мобильных приложений, искусственного интеллекта и других важных инноваций. Старые методы борьбы уже выглядят не так эффективно, как хотелось бы. Да, статистика важна, но она также не дает полной картины проблемы, необходимо изучать правовые механизмы пресечения мошенничества с использованием новых технологий и разрабатывать новые стратегии борьбы.

Необходимо проводить более глубокое исследование эффективности мер по противодействию финансовому мошенничеству в России, опираясь на законодательство, уделив внимание взаимодействию разных государственных структур, использованию новых технологий и анализу социально-экономических последствий, применения эффективности мер борьбы с мошенничеством в сфере финансов.

Получается, что финансовое мошенничество действительно становится все более распространенным и опасным. Это связано с развитием технологий, которые открывают новые возможности для мошенников. Финансовое мошенни-

чество представляет собой большой спектр схем, и важно понимать, что мошенники постоянно изобретают новые схемы обмана.

Стоит обратить внимание и проанализировать примеры распространенных форм финансового мошенничества.

Начнем с фишинга, основная цель которого – это получение доступа к аккаунтам жертвы или кража личной информации, которая может быть использована для мошеннических действий. Мошенники создают поддельные веб-сайты или отправляют электронные письма, которые выглядят как официальные сообщения от банков, платежных систем или других доверенных организаций. Защита от данного вида мошенничества проста – не стоит переходить по ссылкам, не вводить личную информацию, проверять адреса сайтов и использовать надежные антивирусные программы.

Следующим примером является так называемая социальная инженерия. Она основана на психологических манипуляциях и использовании человеческих слабостей, например, доверия, жадности и страха. Среди методов социальной инженерии можно привести следующие – притвориться сотрудником банка, полиции, технической поддержки, предлагать выгодные инвестиции или обещать крупные призы. Важно быть бдительным, не доверять незнакомцам и никогда не предоставлять информацию по телефону или сообщениями.

Еще одним «интересным» примером является скимминг. Скиммер – это небольшое устройство, которое мошенники устанавливают на карт-ридер банкомата. Когда жертва вставляет карту в банкомат, скиммер считывает данные с магнитной полоски карты. Мошенники также могут установить на банкомат фальшивую клавиатуру, которая записывает введенный PIN-код. Части скиммеры трудно обнаружимы невооруженным взглядом, так как они маскируются. Способ защиты – проверять банкомат перед использованием на наличие подозрительных устройств.

Ну и еще одним примером финансового мошенничества, на который хочется обратить внимание, является взлом. Он может осуществляться разными способами, например, через атаки на веб-сайты, программы, серверы банков,

использование вирусов. Как следствие, взлом приводит к краже денежных средств, потери доступа к банковским счетам, утери личной информации. Как способ защиты можно использовать антивирусные программы и надежные пароли.

В России стараются примерять комплексный подход к борьбе с финансовым мошенничеством.

Во-первых, это предупреждение, то есть профилактика мероприятий по информированию населения о видах мошенничества, способах защиты от него и развитию финансовой грамотности. Это ключевой аспект борьбы с преступностью, поскольку предупреждение мошеннических действий гораздо эффективнее, чем их позднее расследование и наказание.

Во-вторых, правоохранительные меры, то есть расследование преступлений и привлечение виновных к ответственности. То есть это те действия органов полиции и прокуратуры, которые направлены на выявление, пресечение и наказание за мошеннические действия.

В-третьих, нормативно-правовое регулирование, то есть совершенствование законодательства, усиление ответственности за мошеннические действия. Правовое регулирование – это не просто создание законов, а постоянно совершенствование законодательства с целью усиления ответственности за мошеннические законодательства с целью усиления ответственности за мошеннические действия и повышения эффективности мер противодействия преступлениям. Важно отметить, что это не «разовая акция», а постоянный процесс, который требует мониторинга практики применения норм и своевременного внесения изменений с учетом новых вызовов.

В-четвертых, использование технологических мер, то есть внедрение новых технологий для защиты финансовых систем (системы мониторинга транзакций, биометрическая идентификация). А такие разработки позволяют укрепить защиту финансовых систем от мошеннических действий. Это не только покупка специального оборудования и программ, но и перестройка системы безопасности с учетом новых рисков. Важно учитывать риски, связанные с ис-

пользованием новых технологий, например, риск кибератак на финансовые системы.

В-пятых, совместные усилия с другими странами по обмену информации и пресечению трансграничных финансовых мошенничеств. Ведь в сегодняшней политической обстановке, в большинстве случаев используются международные каналы для отмывания денег, перемещения активов и уклонения от налогообложения, что делает необходимым объединение усилий разных стран, то есть это не просто обмен информацией, а совместное пресечение преступной деятельности и обеспечение безопасности в мировом масштабе.

Хочется отметить, что оценка эффективности мер по борьбе с финансовым мошенничеством – это сложная и многогранная задача. Несмотря на все принятые меры, проблема остается актуальной, а ее масштабы не уменьшаются.

Основная часть дел о мошенничествах относится к уголовной специфике, однако, в гражданском сфере такие дела тоже рассматриваются.

Однако Гражданский кодекс РФ (далее – ГК РФ) регулирует мошенничество в рамках гражданско-правовой ответственности, как деликт, то есть неправомерное действие, приводящее к ущербу [5]. ГК РФ устанавливает меры ответственности за вред, причиненный мошенническими действиями, например, возмещение ущерба и компенсации морального вреда.

Мошеннические действия могут одновременно попадать под действия норм УК РФ [8] и ГК РФ, тогда может быть возбуждено уголовное дело, и потерпевший может подать гражданский иск о возмещении ущерба.

Мошенничество (ст. 159 УК РФ) тесно переплетено с гражданско-правовыми отношениями. Это особенно актуально в сфере предпринимательской деятельности, где граница между данными видами правоотношений размыта.

Предприниматель, сознательно не исполняющий свои обязанности по договору поставке товара или оказании услуги, может быть признан виновным в мошенничестве, если его действия были направлены на присвоение имущества или уклонение от уплаты денежных средств. В то же время, его действия могут

быть оценены как нарушение договора (ст. 393 ГК РФ), что повлечет гражданско-правовую ответственность (взыскания, штрафы).

Предприниматель, получивший кредит на основе ложных сведений о своем финансовом положении, может быть привлечен по ст. 159.5 УК РФ. Но одновременно, банк может подать иск о взыскании задолженности по кредитному договору (ст. 819 ГК РФ).

Предприниматель, использующий фиктивные сделки для уклонения от уплаты налогов, может быть признан виновным в мошенничестве по УК РФ, а также привлечен к налоговой ответственности по Налоговому кодексу РФ.

Уровень развития страны сильно влияет на эффективность борьбы с финансовым мошенничеством.

Слабая правовая база в развивающихся странах приводит к более высокому уровню финансового мошенничества. Отсутствие четких норм и механизма контроля делает финансовые системы более уязвимыми для мошенников. В связи с этим, низкий уровень осведомленности о мошеннических схемах делает людей более уязвимыми к обману. В развитых же странах широко распространено правовое просвещение и профилактические меры компаний, направленные на повышение финансовой грамотности населения.

Экономические трудности и жажда быстрого обогащения делают людей опять же уязвимыми.

Если опираться на статистику, то Россия – на втором месте по количеству по количеству кибератак.

В первом квартале 2024 года количество мошеннических операций в России увеличилось на 17%, а атаки через систему быстрых платежей и электронные кошельки стали более частыми. Банки отразили в 5 раз больше атак, чем в прошлом году. Несмотря на рост числа атак, мошенникам удалось похитить на 6,3% меньше денег. Средний перевод мошенникам снизился с 18 000 рублей до 14 000 рублей. Мошенники реже звонили по телефону, но перешли на мессенджеры. Доля возврата похищенных денег клиентам увеличилась вдвое, но остается все также незначительной (7,7% от общей суммы потерь). Числа мошенни-

ческих операций выросло почти на 17% по сравнению с прошлым годом. Общая сумма похищения 1,13 миллиардов рублей, что вдвое больше, чем в первом квартале 2023 года [7].

Для сравнения возьмем проблемы с финансовым мошенничеством в некоторых зарубежных странах.

В Соединенных Штатах Америки наблюдается рост финансового мошенничества, связанного с кражей личных данных и использованием поддельных документов личности (то есть называются известными людьми). Было зафиксировано более 160 миллиардов спам-сообщений, что привело к росту телефонного мошенничества [1].

В Австралии, власти государства критикуют крупные банки за недостаточную защиту клиентов от мошенничества. У клиентов крадутся сотни миллионов долларов [4].

Если взять на разбор Китай, то ситуация, к сожалению, там аналогичная. В Китае финансовое мошенничество распространено из-за слабого регулирования онлайн-финансовых структур [2].

Эффективность борьбы с мошенничеством в России увеличилась благодаря совместным усилиям, но мошенники перешли на мессенджеры. Многие жертвы не сообщают о преступлениях, что затрудняет оценку масштабов проблемы.

Для эффективной борьбы с финансовым мошенничеством предлагается усилить контроль и прозрачность финансовых операций, а также ввести более строгие наказания для мошенников. Борьба с этой проблемой требует совместных усилий государства, бизнеса и гражданского общества. И, конечно же, борьба должна быть постоянной.

Правовая база России предусматривает широкий спектр норм, регулирующих финансовое мошенничество. Однако законодательство не всегда успевает за изменениями в методах совершения преступлений, что приводит к неэффективности борьбы с мошенничеством. Необходимо постоянно совершенствовать

законодательство, уточнять термины, усиливать ответственность и расширять полномочия правоохранительных органов.

Меры противодействия включает в себя предупреждение, правоохранительные меры, технологические решения и международный опыт. А внедрение новых технологий играет ключевую роль в борьбе с финансовым мошенничеством.

Существуют проблемы с недостатком ресурсов для правоохранительных органов, отсутствуем координации между разными ведомствами и слабой информированностью населения.

Борьба с финансовым мошенничеством – это динамический процесс, который требует постоянного внедрения новых подходов.

Среди перспектив развития противодействия, можно отметить следующие:

– создание эффективной системы обмена информацией и координация действий между странами, что позволит более эффективно бороться с транснациональными мошенническими схемами;

– внедрение искусственного интеллекта и машинного обучения в системы мониторинга транзакций;

– создание более эффективных законов и норм с учетом развития технологий и мошеннических схем;

– информирование компаний и образовательные программы для повышения уровня финансовой грамотности;

– развитие систем кибербезопасности;

– усиление контроля за финансовыми организациями;

– создание единой платформы обмена информацией.

Список литературы

1. Петросян А. Объем финансовых потерь в результате кражи личных данных в США в 2023 и 2024 годах / Ани Петросян [Электронный ресурс]. – Режим доступа: https://translated.tubopages.org (дата обращения: 07.12.2024).

2. Аносов Б.А. Регулирование сомнительных валютных операций и развитие цифрового юаня к КНР / Б.А. Аносов // Экономика и управление. – 2022. – №7 (89).

3. Бойко С.Я. Мошенничество в сфере кредитования (статья 159.1 Уголовного кодекса Российской Федерации): вопросы квалификации / С.Я. Бойко // Вестник Краснодарского университета МВД России. – 2026. – №2 (34).

4. Власти Австралии обвинили один из крупнейших банков страны в отмывании денег [Электронный ресурс]. – Режим доступа: https://finance.rambler.ru (дата обращения: 07.12.2024).

5. Гражданский кодекс Российской Федерации (часть 1) от 30.11.1994 №51-ФЗ (ред. от 08.08.2024 г.) // Собрание законодательства Российской Федерации.

6. Несмеянова А.В. Мошенничество с использованием информационно-телекоммуникационных технологий как угроза экономической безопасности России / А.В. Несмеянова // Международный журнал гуманитарных и естественных наук. – 2023 – №6–1 (81).

7. Обзор отчетности об инцидентах информационной безопасности при переводе денежных средств Банка России (1 квартал 2023 г. / 1 квартал 2024 г.).

8. Уголовный кодекс Российской Федерации (часть 1) от 13.06.1996 №63-ФЗ (ред. от 23.11.2024 г.) // Собрание законодательства Российской Федерации.

9. Яковлев А.Б. Противодействие легализации (отмыванию) доходов, полученных преступным путем, финансирование терроризма как вид финансового контроля / А.Б. Яковлев // Актуальные проблемы российского права. – 2019. – №5 (102).