

Колесникова Елизавета Олеговна

студент специалитета
Российская академия народного хозяйства и
государственной службы при Президенте
Российской Федерации
Сибирский институт управления
Новосибирск, Россия

Товстокоп Софья Александровна

студент специалитета
Российская академия народного хозяйства и
государственной службы при Президенте
Российской Федерации
Сибирский институт управления
Новосибирск, Россия

**МОШЕННИЧЕСТВО В ТЕНЕВОМ СЕКТОРЕ КАК УГРОЗА ЭКОНОМИЧЕСКОЙ
БЕЗОПАСНОСТИ РОССИИ: МАСШТАБЫ И МЕХАНИЗМЫ ПРОТИВОДЕЙСТВИЯ****Аннотация**

Рассматривается проблема мошенничества в теневом секторе экономики как одной из ключевых угроз экономической безопасности России. Проанализированы сущность теневого мошенничества, его современные формы и масштабы распространения в условиях цифровизации финансовой сферы. Особое внимание уделено телефонному и интернет-мошенничеству, незаконному обналичиванию денежных средств, фиктивными инвестиционным платформам и использованию компаний-однодневок. Рассмотрены основные механизмы противодействия теневого мошенничеству со стороны Центрального банка РФ, МВД России, Росфинмониторинга и банковского сектора. Сделан вывод о необходимости комплексного подхода к обеспечению экономической безопасности, включающего развитие финансового мониторинга, совершенствование законодательства и повышение уровня цифровой грамотности населения.

Ключевые слова: мошенничество, теневой сектор, экономической безопасности

Мошенничество в теневом секторе экономики представляет собой одну из наиболее опасных форм экономической преступности, поскольку подобная деятельность сочетает незаконное извлечение прибыли, скрытый характер финансовых операций и высокий уровень адаптации к изменениям экономической среды [1, 3]. В российской практике теневой сектор охватывает широкий круг неформальных и противоправных операций, начиная от уклонения от налогообложения и фиктивного предпринимательства и заканчивая масштабными схемами обналичивания денежных средств, финансовыми пирамидами и цифровым мошенничеством. Опасность подобных процессов связана не только с прямыми материальными потерями государства и граждан, но и с постепенным разрушением доверия к финансовым институтам и механизмам государственного регулирования [7].

Содержание теневого сектора традиционно связывается с деятельностью, скрываемой от официального учёта и контроля [5]. При этом мошенничество внутри

такой системы отличается особой сложностью выявления. Причина заключается в том, что значительная часть операций формально маскируется под законную предпринимательскую активность. Используются фиктивные договоры, подставные фирмы, электронные переводы через цепочки посредников, счета физических лиц и анонимные цифровые инструменты. На практике граница между нелегальной экономикой и внешне легальными финансовыми процессами становится всё менее заметной.

Существенный вклад в развитие современных мошеннических схем внесла цифровизация экономики. Распространение дистанционного банковского обслуживания, онлайн-платежей и электронных платформ заметно упростило проведение финансовых операций, однако одновременно создало новые возможности для преступных групп. Особенно активно используются методы социальной инженерии, при которых граждан вводят в заблуждение через телефонные звонки, мессенджеры и поддельные сайты банковских организаций. По данным Центрального банка РФ, объём операций без добровольного согласия клиентов ежегодно исчисляется миллиардами рублей, а количество подобных преступлений продолжает увеличиваться [12].

А также по данным Центрального банка РФ можно рассмотреть динамику подозрительных операций в России за 2020-2025 гг., представленную на рисунке 1 [13].

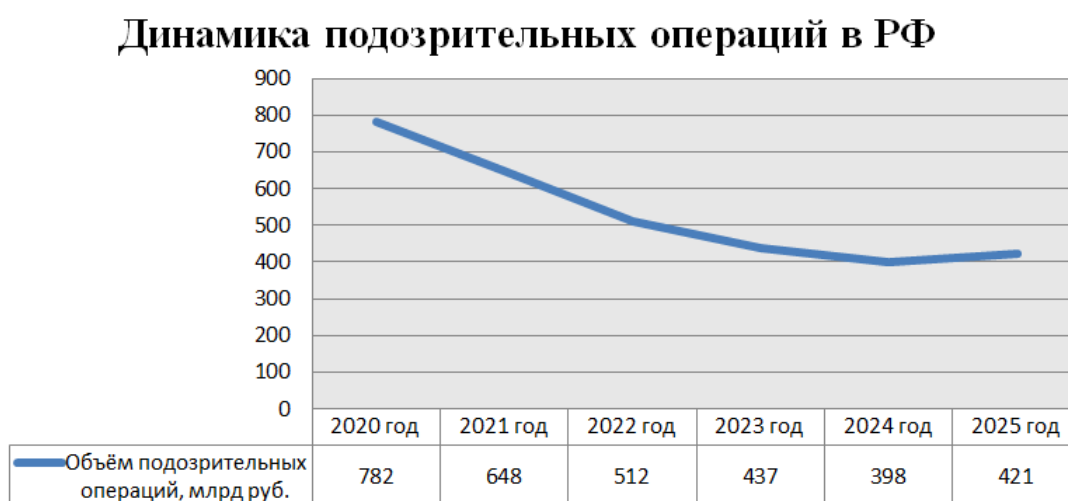


Рисунок 1 – Динамика объёма подозрительных операций, выявленных Банком России в 2020-2025 гг.

Анализ динамики показывает постепенное снижение объёма подозрительных операций в период с 2020 по 2024 год. Подобная тенденция связана с усилением

финансового мониторинга, внедрением цифровых механизмов контроля и ужесточением требований к банковским операциям. Существенное влияние оказало развитие автоматизированных систем выявления сомнительных транзакций, применяемых Банком России и коммерческими банками [13].

Небольшой рост показателя в 2025 году может быть связан с адаптацией теневого сектора к новым условиям контроля, а также с активным использованием криптовалютных инструментов и трансграничных цифровых сервисов. Дополнительную роль сыграло расширение схем дистанционного мошенничества и увеличение числа операций через электронные платформы. Несмотря на общее снижение объёмов подозрительных операций по сравнению с 2020 годом, проблема сохраняет высокий уровень актуальности для системы экономической безопасности России.

Отдельного внимания заслуживает проблема фиктивного предпринимательства. В теневом секторе активно применяются компании-однодневки, через которые осуществляются незаконное обналичивание денежных средств, вывод капитала и сокрытие налоговой базы. Подобные схемы позволяют участникам теневой экономики минимизировать контроль со стороны государства и затрудняют расследование финансовых преступлений. Нередко в подобных операциях участвуют сразу несколько организаций, зарегистрированных в разных регионах, что дополнительно осложняет выявление реальных выгодоприобретателей.

Значительное влияние на развитие мошенничества оказывает и высокая скорость трансформации финансовых технологий. Появление криптовалют, электронных кошельков и анонимных способов перевода средств создало условия для формирования новых моделей теневого оборота [11]. Часть операций фактически выходит за пределы традиционного банковского контроля. В результате государственным структурам становится сложнее отслеживать движение денежных потоков и устанавливать источники происхождения средств. Особенно опасным подобный процесс становится в условиях международных ограничений и нестабильной экономической ситуации, когда теневой сектор начинает использовать альтернативные каналы расчётов.

Экономическая безопасность государства напрямую зависит от способности ограничивать масштабы подобных преступлений. Массовое распространение

мошеннических схем приводит к снижению налоговых поступлений, росту нелегального денежного оборота и усилению коррупционных рисков. Помимо финансовых потерь возникает и более глубокая проблема. Население постепенно теряет доверие к банковской системе, цифровым сервисам и государственным институтам защиты прав потребителей. Подобное недоверие способно негативно влиять на инвестиционную активность и общую стабильность экономической среды.

Серьёзную угрозу представляет взаимосвязь теневого мошенничества с организованной преступностью. Финансовые схемы нередко используются для легализации незаконных доходов, финансирования нелегального бизнеса и вывода капитала за рубеж. В результате теневой сектор начинает выполнять функцию параллельной экономической системы, существующей вне полноценного государственного контроля. Подобная ситуация усиливает нагрузку на правоохранительные органы и требует постоянного совершенствования механизмов финансового мониторинга.

В современной России борьба с мошенничеством постепенно становится одним из ключевых направлений обеспечения экономической безопасности. Активное участие в этом процессе принимают МВД России, Центральный банк РФ, Росфинмониторинг и налоговые органы [2, 13]. Усиливается контроль за подозрительными финансовыми операциями, вводятся дополнительные механизмы идентификации клиентов банков, развиваются цифровые инструменты мониторинга. Вместе с тем высокая адаптивность теневого сектора показывает, что проблема остаётся системной и требует комплексного подхода, сочетающего правовые, экономические и технологические меры противодействия.

В итоге мошенничество в теневом секторе следует рассматривать не как совокупность отдельных преступлений, а как серьёзный фактор дестабилизации экономической системы государства. Масштаб подобных процессов влияет на финансовую устойчивость, уровень общественного доверия и эффективность государственного управления. По этой причине противодействие теневому мошенничеству становится важным элементом защиты национальной экономической безопасности России.

Современный этап развития российской экономики сопровождается усложнением структуры теневого сектора и расширением мошеннических схем, ориентированных как на граждан, так и на организации. Особую опасность

представляет сочетание традиционных незаконных механизмов с цифровыми технологиями, позволяющими преступным группам быстро адаптироваться к изменениям финансовой среды. В последние годы заметно выросло число преступлений, связанных с дистанционным хищением денежных средств, фиктивными инвестиционными проектами, незаконным обналичиванием и использованием подставных юридических лиц.

Статистика МВД России и Центрального банка РФ показывает устойчивую тенденцию роста преступлений в сфере финансового мошенничества. Наибольшее распространение получили схемы телефонного обмана, при которых злоумышленники выдают себя за сотрудников банков, правоохранительных органов или государственных служб. Граждан убеждают переводить средства на «безопасные счета», оформлять кредиты или передавать конфиденциальные данные банковских карт [12]. Подобные преступления отличаются высокой психологической подготовкой преступников и значительным уровнем организованности.

Наряду с этим активно развиваются схемы фиктивного предпринимательства. Компании-однодневки продолжают использоваться для уклонения от налогов, вывода денежных средств и сокрытия финансовых потоков. Особую роль играет теневой рынок обналичивания, позволяющий легализовать незаконные доходы и минимизировать контроль со стороны государства. Часть операций проводится через цепочки посредников, электронные кошельки и криптовалютные сервисы, что значительно затрудняет отслеживание движения средств [10].

Отдельное место занимают интернет-платформы псевдоинвестиций. В условиях нестабильной экономической ситуации многие граждане стремятся найти способы быстрого увеличения доходов, чем активно пользуются мошеннические структуры. Под видом инвестиционных компаний создаются фиктивные площадки, обещающие высокую доходность от операций с криптовалютами, акциями или иностранной валютой. После получения денежных средств доступ к платформе блокируется, а организаторы прекращают связь с клиентами.

Динамика отдельных видов мошенничества в российской экономике отражена на рисунке 2, данные которой основаны на открытых материалах МВД РФ и аналитических обзорах Банка России.

Динамика видов финансового мошенничества в РФ

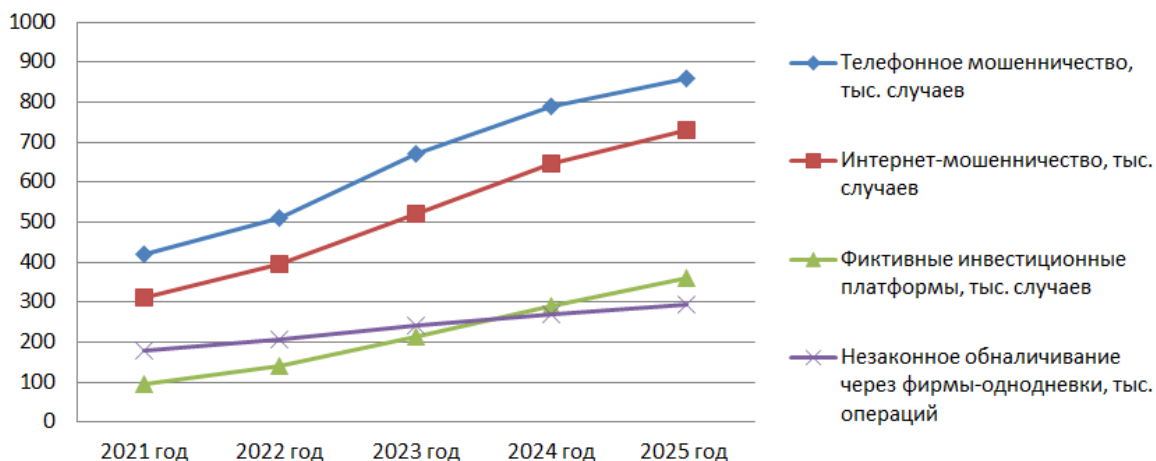


Рисунок 2 - Динамика распространения отдельных видов финансового мошенничества в России за 2021–2025 гг.

Анализ представленных данных позволяет сделать вывод о стабильном росте практически всех ключевых форм теневого мошенничества. Особенно быстро увеличивается количество интернет-преступлений и операций, связанных с цифровыми финансовыми инструментами. Причина подобной тенденции заключается не только в распространении онлайн-сервисов, но и в недостаточном уровне финансовой грамотности части населения. Преступные схемы становятся более технологичными, а механизмы психологического воздействия приобретают всё более сложный характер.

Дополнительным фактором роста теневого мошенничества выступает развитие трансграничных цифровых платформ. Многие незаконные операции организуются через иностранные сервисы, что усложняет взаимодействие между государственными структурами разных стран [9]. Финансовые потоки распределяются между несколькими юрисдикциями, а часть средств переводится в криптовалюту. В подобных условиях расследование преступлений требует серьёзных технологических ресурсов и межведомственного взаимодействия.

Немаловажную роль играет и проблема вовлечения граждан в незаконные схемы в качестве посредников. Распространённой практикой стало использование так называемых дропперов, через банковские карты которых проходят похищенные денежные средства. Часть таких участников осознаёт противоправный характер действий, однако нередко граждане становятся участниками схем из-за финансовых

трудностей или недостаточного понимания последствий. Подобная модель существенно усложняет выявление организаторов преступлений.

Экономические последствия распространения теневого мошенничества носят системный характер. Государство сталкивается с потерями налоговых поступлений, ростом нагрузки на правоохранительные органы и увеличением расходов на развитие систем кибербезопасности. Бизнес вынужден усиливать защиту цифровой инфраструктуры и инвестировать дополнительные средства в системы финансового контроля. Для населения проблема выражается в росте финансовых потерь и снижении доверия к банковскому сектору и электронным сервисам.

В результате современное теневое мошенничество постепенно превращается в сложную многокомпонентную систему, объединяющую цифровые технологии, незаконные финансовые операции и элементы организованной преступности. Масштаб распространения подобных схем подтверждает необходимость дальнейшего усиления механизмов государственного контроля, совершенствования финансового мониторинга и повышения уровня цифровой грамотности населения.

Рост масштабов теневого мошенничества в России привёл к необходимости активного усиления системы экономической безопасности на государственном уровне. Современные механизмы противодействия уже не ограничиваются только уголовным преследованием отдельных преступников. Основной акцент постепенно смещается в сторону комплексного финансового мониторинга, цифрового контроля операций, межведомственного взаимодействия и профилактики мошеннической активности. Подобный подход связан с тем, что современные теневые схемы обладают высокой гибкостью и быстро меняются под воздействием экономических и технологических факторов.

Ключевую роль в системе противодействия играет Центральный банк Российской Федерации. Именно Банк России координирует значительную часть мер, связанных с выявлением подозрительных финансовых операций, защитой клиентов банков и ограничением незаконного вывода денежных средств. В последние годы активно внедряются автоматизированные системы мониторинга транзакций, позволяющие выявлять атипичные переводы, подозрительные цепочки операций и признаки использования подставных счетов [13, 14]. Существенное значение имеет и развитие платформ обмена информацией между банками и государственными структурами.

Отдельным направлением стала борьба с телефонным и интернет-мошенничеством. Банковские организации начали применять технологии искусственного интеллекта для анализа подозрительных действий клиентов и автоматического выявления потенциально опасных операций. При обнаружении нетипичной активности система способна временно блокировать перевод средств или направлять дополнительное подтверждение операции. Подобные меры позволяют сократить количество успешных хищений, хотя полностью устранить проблему пока не удаётся.

Значительная нагрузка в сфере противодействия теневому мошенничеству ложится на МВД России. Подразделения экономической безопасности и киберпреступности занимаются выявлением преступных групп, расследованием схем обналичивания и пресечением деятельности фиктивных организаций. В последние годы заметно увеличилось количество уголовных дел, связанных с цифровыми финансовыми преступлениями. Особое внимание уделяется организованным схемам, использующим электронные платформы, криптовалюты и поддельные инвестиционные сервисы.

Серьёзную роль играет и деятельность Росфинмониторинга. Федеральная служба финансового мониторинга осуществляет анализ подозрительных операций и контролирует процессы легализации незаконных доходов [6]. Одним из наиболее эффективных инструментов стал риск-ориентированный подход, при котором финансовые операции оцениваются по вероятности связи с теневой деятельностью. При выявлении признаков незаконного происхождения средств информация передаётся правоохранительным органам и банковским организациям.

Правовая база противодействия экономическому мошенничеству также продолжает расширяться. В российском законодательстве регулярно обновляются нормы, связанные с цифровыми финансовыми активами, банковской идентификацией клиентов и противодействием легализации преступных доходов. Усиливается контроль за деятельностью финансовых посредников и электронных платёжных сервисов. Дополнительное значение приобретают механизмы обязательной идентификации пользователей при проведении отдельных видов операций.

Наряду с государственными структурами активное участие в борьбе с теневым мошенничеством принимает банковский сектор. Крупные российские банки создают

собственные подразделения кибербезопасности и инвестируют значительные средства в развитие систем защиты клиентов. Используются биометрические технологии, анализ поведенческих моделей пользователей и алгоритмы раннего выявления мошеннической активности. Подобные меры особенно важны в условиях постоянного роста количества дистанционных финансовых операций.

Несмотря на активное развитие механизмов противодействия, сохраняется ряд серьёзных проблем. Преступные схемы адаптируются значительно быстрее, чем обновляется законодательство и технические инструменты контроля. Дополнительные сложности возникают из-за использования зарубежных цифровых платформ и криптовалютных сервисов, деятельность которых частично выходит за пределы российского регулирования. Сохраняется и проблема недостаточной финансовой грамотности населения, позволяющая мошенникам эффективно использовать методы психологического воздействия.

Отдельное значение приобретает профилактическое направление. Государственные органы, банки и образовательные организации всё активнее участвуют в информировании граждан о распространённых схемах мошенничества. В средствах массовой информации регулярно публикуются рекомендации по защите персональных данных и безопасному использованию банковских сервисов [12]. Практика показывает, что повышение уровня цифровой грамотности населения способно существенно сократить количество успешных мошеннических операций.

В современных условиях противодействие теневому мошенничеству требует постоянного технологического обновления и координации действий между государством, финансовыми организациями и обществом. Только сочетание правовых, цифровых и профилактических механизмов позволяет снижать уровень экономических угроз и ограничивать развитие незаконного финансового оборота. Эффективность подобной системы напрямую влияет на устойчивость российской экономики, уровень доверия к финансовым институтам и общее состояние экономической безопасности страны.

Проблема мошенничества в теневом секторе экономики России в последние годы приобрела масштабный и системный характер. Развитие цифровых технологий, рост объёма дистанционных финансовых операций и расширение нелегальных каналов движения денежных средств создали благоприятную среду для появления новых мошеннических схем. Подобные процессы оказывают влияние не только на

отдельных граждан и организации, но и на устойчивость всей экономической системы государства. Финансовые потери, снижение уровня доверия к банковскому сектору, рост коррупционных рисков и усиление теневого оборота формируют серьёзную угрозу экономической безопасности страны.

В ходе рассмотрения теоретических аспектов темы было установлено, что мошенничество в теневом секторе представляет собой сложное многоуровневое явление, сочетающее незаконные финансовые операции, скрытый характер деятельности и использование современных цифровых инструментов. Особое значение имело выявление взаимосвязи между теневой экономикой и финансовой преступностью. Наиболее опасным фактором стало постепенное стирание границы между формально легальными операциями и скрытыми механизмами незаконного извлечения прибыли. Существенную роль в развитии подобных схем сыграли цифровизация экономики и расширение электронных финансовых сервисов.

Анализ современных масштабов теневого мошенничества показал устойчивую тенденцию роста преступлений в сфере дистанционного хищения денежных средств, интернет-мошенничества и фиктивных инвестиционных проектов. Показательной стала таблица, в которой были отражены изменения количества отдельных видов финансовых преступлений за последние годы. Наиболее быстрый рост наблюдается в сфере интернет-мошенничества и цифровых схем незаконного вывода средств. Подобная динамика свидетельствует о высокой адаптивности преступных групп и активном использовании технологий социальной инженерии. Дополнительную опасность создаёт вовлечение граждан в мошеннические схемы через использование банковских карт и электронных сервисов в качестве промежуточных инструментов перевода денежных средств.

Особое внимание было уделено действующим механизмам противодействия теневому мошенничеству. Значительная роль в обеспечении экономической безопасности принадлежит Центральному банку РФ, МВД России, Росфинмониторингу и банковскому сектору. Развитие систем автоматического мониторинга операций, применение технологий искусственного интеллекта, усиление финансового контроля и совершенствование законодательства постепенно повышают эффективность борьбы с незаконными финансовыми схемами. Вместе с тем сохраняется проблема быстрого обновления преступных механизмов, особенно в сфере криптовалютных операций и трансграничных цифровых сервисов.

Практическое значение рассмотренной темы связано с необходимостью дальнейшего укрепления системы финансовой безопасности России. Особую важность приобретают повышение уровня цифровой грамотности населения, развитие механизмов межведомственного взаимодействия и совершенствование технологий финансового мониторинга. Ограничение масштабов теневого мошенничества напрямую влияет на устойчивость национальной экономики, доверие граждан к государственным институтам и эффективность функционирования финансовой системы.

Список использованных источников

1. Абалкин Л. И. Экономическая безопасность России: угрозы и их отражение / Л.И. Абалкин // М. Издательство «Дело» – 2019 – С. 512;
2. Батурина Е. В. Оценка эффективности правоохранительной деятельности во взаимосвязи с созданием благоприятной экономической среды // Экономическая безопасность. 2021. № 3. С. 623–638. (1ECONOMIC.RU);
3. Богомолов В. А. Экономическая безопасность. М. ЮНИТИ-ДАНА – 2020 – С. 295;
4. Глазьев С. Ю. Основы обеспечения экономической безопасности страны. М. Проспект – 2021 – С. 432;
5. Кузнецов В. П. Теневая экономика и экономическая безопасность государства // Вестник экономической безопасности. 2022. № 4. С. 45–53.
6. Кучеров И. И. Противодействие легализации преступных доходов в Российской Федерации. М. Юрлитинформ – 2020 – С. 368;
7. Сенчагов В. К. Экономическая безопасность России. Общий курс. М. БИНОМ – 2021 – С. 815;
8. Федотова М. А. Финансовое мошенничество и механизмы противодействия в цифровой экономике // Финансы и кредит. 2023. № 7. С. 112–126.
9. Экономическая безопасность России в условиях цифровизации / под ред. А. Г. Аганбегяна. М. Инфра-М – 2022 – С. 401;
10. Информация Банка России от 10 сентября 2021 г. «Банк России выделил признаки карт и электронных кошельков, вовлеченных в теневой бизнес» // ГАРАНТ. URL: ГАРАНТ (дата обращения: 22.05.2026). (Гарант)

11. Информация Банка России от 11 июня 2025 г. «Банк России предупреждает граждан о риске вовлечения в преступные схемы при расчетах с криптообменниками и онлайн-казино» // ГАРАНТ. URL: ГАРАНТ (дата обращения: 22.05.2026). (Гарант)

12. Осторожно: мошенники! // Банк России (дата обращения: 22.05.2026). (Центральный банк России)

13. Противодействие нелегальной деятельности на финансовом рынке // Банк России (дата обращения: 22.05.2026). (Центральный банк России)

14. Противодействие недобросовестным практикам // Банк России (дата обращения: 22.05.2026). (Центральный банк России)

15. ЦБ оценил число потребителей услуг теневого бизнеса в 10 млн человек // Российская газета (дата обращения: 22.05.2026).