УДК 336.025

ФИНАНСОВОЕ МОШЕННИЧЕСТВО КАК УГРОЗА ЭКОНОМИЧЕСКОЙ БЕЗОПАСНОСТИ: ТЕОРЕТИЧЕСКИЙ ОБЗОР

К.Д. ИЛЛАРИОНОВА, И.О. ЛУТОВА
(Представлено: канд. экон. наук, доц. Н.А. БОРЕЙКО)

Статья представляет теоретический обзор феномена финансового мошенничества как одной из наиболее серьезных угроз экономической безопасности в современных условиях. Проанализированы сущностные характеристики и виды финансового мошенничества, систематизированы подходы к его определению в научной литературе. Выявлены основные угрозы и факторы, способствующие распространению мошеннических схем: технологические, социальные, экономические и правовые. Особое внимание уделено источникам угроз и их классификации. Определены перспективные направления противодействия финансовому мошенничеству на государственном и личностном уровнях.

Ключевые слова: *финансовое мошенничество, экономическая безопасность, кибермошенничество, социальная инженерия, финансовые пирамиды, угрозы, источники угроз, финансовая грамотность, противодействие мошенничеству, цифровизация экономики.*

Современные государства и граждане сталкиваются с растущими финансовыми и правовыми вызовами. Увеличение числа безналичных платежей, рост киберпреступности, высокий уровень ущерба от мошеннических действий негативно влияют на благосостояние населения и доверие к финансовой системе. В условиях глобальной цифровизации и стремления к экономической безопасности традиционные методы защиты финансовых интересов требуют пересмотра. Одним из ключевых инструментов противодействия финансовому мошенничеству становятся правовые механизмы, цифровые технологии и программы повышения финансовой грамотности, способные снизить уязвимость граждан, обеспечить безопасность транзакций и минимизировать экономический ущерб [1, с. 2].

Таким образом, актуальность темы обусловлена стремительной цифровизацией экономики, ростом объемов финансовых операций и повышенным вниманием к вопросам защиты имущественных прав и экономической безопасности.

Целью исследования является анализ сущности и видов финансового мошенничества, оценка ключевых угроз и факторов его распространения, а также выработка рекомендаций по преодолению барьеров в системе противодействия.

Рассмотрим различные аспекты, в которых проявляется финансовое мошенничество, нацеленное на незаконное завладение чужими денежными средствами.

Одним из наиболее распространенных направлений является мошенничество с использованием банковских пластиковых карт. Оно позволяет злоумышленникам получать доступ к реквизитам карты для последующего обналичивания или оплаты товаров, используя поддельные накладки на банкоматах (скимминг) и методы обмана держателя карты для получения CVV-кода и SMS-паролей [5, с. 8].

Далее следует кибермошенничество, один из примеров использования данного метода в финансовой сфере – это фишинговые атаки, при которых создаются поддельные сайты банков и платежных систем для кражи конфиденциальных данных, а также вишинг (звонки от имени сотрудников банка) и фарминг (перенаправление на фальшивые веб-ресурсы) [6].

Финансовые пирамиды играют критическую роль в подрыве доверия к инвестиционной среде. Одним из примеров их функционирования является привлечение денег вкладчиков под видом высокодоходных инвестиционных проектов, где капитал формируется исключительно из взносов новых участников для выплаты прибыли старым вкладчикам, а при прекращении притока средств структура рушится, и большинство участников теряют свои сбережения [9].

Еще одним важным направлением является мошенничество с использованием социальной инженерии. Примером их использования в финансовой сфере может служить метод управления действиями человека, при котором злоумышленники представляются сотрудниками банка или правоохранительных органов с целью вынудить жертву перевести деньги на «безопасный» счет. Техническая инфраструктура здесь служит лишь инструментом для установления психологического контакта и введения в заблуждение, что существенно повышает уязвимость населения [3, с. 48].

Однако, противодействие финансовому мошенничеству сталкивается с комплексом взаимосвязанных проблем, которые можно условно разделить на:

– технологические барьеры – отставание банковских систем защиты от методов кибермошенников, необходимость обработки больших объемов транзакций в реальном времени для выявления подозрительных операций, интеграция с существующей платежной инфраструктурой [2];

– регуляторные барьеры – несовершенство законодательной базы и отсутствие единых стандартов для квалификации новых видов мошенничества (например, с использованием криптовалют и дипфейков). Это создает сложности для правоохранительных органов, вынужденных адаптировать свои подходы под различные юрисдикции, особенно при трансграничных преступлениях [8];

– социальное восприятие – низкий уровень финансовой грамотности населения, доверчивость граждан, психологическая готовность к принятию быстрых необдуманных решений, а также недоверие к новым технологиям защиты;

– экономическая целесообразность – высокие затраты на внедрение современных систем безопасности и необходимость доказательства долгосрочной эффективности инвестиций в противодействие мошенничеству [10];

– правовая неопределенность в вопросах ответственности за решения, принятые автоматизированными системами, представляет собой серьезный барьер для их широкого внедрения. В случае ошибочной блокировки счета или несанкционированного списания сложно определить, кто несет ответственность – разработчик алгоритма, сотрудник банка, платежная система или конечный пользователь [9].

Также возникают дополнительные сложности. Демографические и психологические особенности создают дополнительные сложности для применения мер противодействия. Например, программы повышения финансовой грамотности, разработанные для молодежной аудитории, часто оказываются неэффективными для пожилых граждан, которые являются наиболее уязвимой категорией и подвержены методам социальной инженерии, поскольку их поведенческие паттерны существенно отличаются [10].

Указанные ограничения представляют собой важные факторы, которые необходимо учитывать при моделировании систем защиты от финансового мошенничества и разработке профилактических мер.

Однако несмотря на различные ограничения по противодействию финансовому мошенничеству, важным результатом эффективной защиты является повышение уровня доверия к финансовой системе. Современные банковские системы для выявления подозрительных операций позволяют сократить количество успешных мошеннических транзакций. Алгоритмы поведенческого анализа способны выявлять аномалии в действиях держателей карт, что позволяет блокировать подозрительные операции до момента списания средств [4, с. 162].

Значительный эффект достигается за счет повышения финансовой грамотности населения. Программы просвещения и информационные кампании, анализирующие типичные мошеннические схемы, позволяют сократить количество обманутых граждан. По оценкам экспертов, это приводит к снижению совокупного ущерба от мошенничества [5].

На макроэкономическом уровне эффективное противодействие финансовому мошенничеству способствует росту ВВП за счет сохранения сбережений граждан и повышения устойчивости финансовой системы.

Особого внимания заслуживает социально-экономический эффект. Снижение числа успешных мошеннических атак с помощью систем поведенческого анализа позволяет сократить общий объем похищенных средств. В пересчете на экономические показатели, это означает существенную экономию на мероприятиях по компенсации ущерба и правоохранительной деятельности [1, с. 10].

Следует также отметить и косвенный экономический эффект от противодействия финансовому мошенничеству. Повышение надежности и безопасности финансовых услуг положительно влияет на смежные отрасли – розничную торговлю, электронную коммерцию, инвестиционную деятельность, туризм и строительство.

Таким образом, важность противодействия финансовому мошенничеству на государственном уровне подтверждается постоянным совершенствованием законодательства, внедрением систем мониторинга подозрительных операций и активной просветительской работой с населением, что способствует повышению уровня защищенности финансовых интересов граждан и организаций.

Таким образом, системное противодействие финансовому мошенничеству – это ключевой драйвер обеспечения экономической безопасности, предлагающий решения для защиты имущественных прав, повышения финансовой стабильности и доверия к банковской системе. Как показал анализ, современные подходы – от правового регулирования до цифровых систем мониторинга – уже демонстрируют значительные результаты в снижении ущерба от мошеннических действий.

Однако для реализации полного потенциала систем противодействия финансовому мошенничеству необходимо преодолеть ряд барьеров, включая проблемы кибербезопасности, интеграцию с устаревшими системами, регуляторные и социальные вопросы. Важными шагами станут разработка международных стандартов, инвестиции в цифровую инфраструктуру, адаптация законодательства и подготовка квалифицированных кадров в сфере финансовой безопасности.

Современные методы противодействия не только революционизируют защиту финансовых интересов граждан, но и становятся катализатором экономического роста, повышая устойчивость банковской системы. При условии комплексного подхода и международного сотрудничества, меры противодействия способны обеспечить устойчивое развитие финансового сектора и значительный вклад в экономику. Для

успешной реализации потенциала в сфере противодействия финансовому мошенничеству необходима координация усилий технологических организаций, банковских учреждений и регуляторов для разработки отраслевых стандартов и нормативной базы [4].

ЛИТЕРАТУРА

1. Ганич, А.П. Экономические преступления. Виды и пути мошенничества / А.П. Ганич. – Витебск: ВГУ им. П.М. Машерова, 2003. – С. 55-58.
2. Исаков, В.А. Возникновение и развитие предпринимательской деятельности [Электронный ресурс] / В.А. Исаков. – Режим доступа: https://cyberleninka.ru/article/n/vozniknovenie-i-razvitie-predprinimatelskoy-deyatelnosti. – Дата доступа: 20.04.2026.
3. Рутковский, И.И. Финансовое мошенничество в современном мире [Электронный ресурс] / И.И. Рутковский. – Режим доступа: https://elib.utmn.ru/jspui/bitstream/ru-tsu/28525/1/SibSoc202326797.pdf. – Дата доступа: 20.04.2026.
4. Корнеева, С.Г. Финансовое мошенничество / С.Г. Корнеева. – 2020. – С. 24.
5. Дедюхина, И.Ф. Финансовое мошенничество в современном мире / И.Ф. Дедюхина. – Ставрополь: СГАУ, 2008. – 2 с.
6. Финансовые махинации [Электронный ресурс] // Provtech. – Режим доступа: https://provtech.ru/about/finansovaya-gramotnost/Tema-4.3.pdf. – Дата доступа: 20.04.2026.
7. Воспякова, О.Ф. Понятие мошенничества в белорусском и европейском законодательстве [Электронный ресурс] / О.Ф. Воспякова. – Режим доступа: https://elib.institutemvd.by/bitstream/MVD_NAM/2916/1/Vospjakova.pdf. – Дата доступа: 20.04.2026.
8. Информационная безопасность. Мошенничество [Электронный ресурс] // Rep.bntu. – Режим доступа: https://rep.bntu.by/bitstream/handle/data/150224/10-12.pdf?sequence=1&isAllowed=y. – Дата доступа: 20.04.2026.
9. Гузова, Л.А. Уголовно-правовая оценка мошенничества [Электронный ресурс] / Л.А. Гузова. – Режим доступа: https://pdf.vlib.by/BS-2020/dajdjest-moshennichestvo.pdf. – Дата доступа: 20.04.2026.
10. Романова, А.А. Финансовое мошенничество в сети: схема обмана и уголовная ответственность / А.А. Романова. – 2002. – С. 158-164.