DOI: 10.25629/SMW.2025.04.02
УДК: 336.7

# МОБИЛЬНЫЙ БАНКИНГ ДЛЯ УЯЗВИМЫХ ГРУПП НАСЕЛЕНИЯ: АНАЛИЗ РИСКОВ ФИНАНСОВОГО МОШЕННИЧЕСТВА И ПУТИ ЗАЩИТЫ

**Кузнецова Д.А., Сахибгареева Э.В., Губанова И.Р.**
Финансовый университет при Правительстве РФ

***Аннотация***

*Статья посвящена актуальной проблеме обеспечения безопасности уязвимых категорий населения при использовании мобильного банкинга в условиях стремительного роста финансового мошенничества. Цифровая трансформация финансового сектора значительно повышает удобство и доступность банковских сервисов, однако одновременно формирует новые угрозы для граждан с недостаточным уровнем цифровой и финансовой грамотности. В центре исследования находятся пожилые пользователи, люди с низкими доходами, мигранты, а также граждане, испытывающие трудности в освоении технологий и работе с цифровыми устройствами. Анализируются наиболее распространённые механизмы мошенничества, такие как социальная инженерия, фишинговые схемы, вредоносное программное обеспечение, а также использование технологий искусственного интеллекта, включая генерацию дипфейков для имитации голоса или внешности знакомых людей. Уделено внимание психологическим аспектам уязвимости – повышенной доверчивости, цифровой тревожности и стрессу при взаимодействии с банковскими приложениями. Также рассматриваются технические барьеры, включая сложные интерфейсы, медленные смартфоны и ограниченный доступ к актуальным обновлениям безопасности. Предлагается комплексный подход к повышению безопасности, включающий технологические меры банков (биометрическая аутентификация, поведенческий анализ, упрощённые интерфейсы), государственные инициативы (образовательные программы, стандарты безопасности) и формирование осознанных цифровых привычек у пользователей.*

***Ключевые слова***

*мобильный банкинг, цифровая грамотность, уязвимые группы населения, финансовое мошенничество, социальная инженерия, цифровая безопасность, биометрия, цифровые технологии*

## Введение

Сегодня финансовый сектор активно цифровизируется, и мобильный банкинг перестал быть просто дополнительной функцией – он стал основным способом взаимодействия клиентов с банками. Через мобильные приложения пользователи могут управлять широким спектром услуг – от простых переводов до инвестиций и страховых продуктов – что делает финансовые сервисы максимально доступными и удобными. Вместе с тем, рост популярности мо-

бильного банкинга сопровождается активным развитием финансового мошенничества, которое использует как технические уязвимости приложений, так и психологические особенности пользователей [12].

Проблема кибербезопасности особенно актуальна для уязвимых категорий населения. Пожилые люди, граждане с низким уровнем дохода и образования, мигранты, а также пользователи с ограниченным опытом работы с цифровыми технологиями оказываются наиболее подверженными мошенническим атакам из-за социальных, экономических и когнитивных факторов [3]. Исследования показывают значительный разрыв между поколениями в уровне цифровой грамотности, а также тенденцию снижения восприятия реальных рисков, что усиливает уязвимость этих групп.

Цель исследования – провести системный анализ рисков финансового мошенничества, направленного на уязвимые категории пользователей мобильного банкинга, и на этой основе предложить комплекс практических рекомендаций для банков, государственных органов и самих пользователей с целью повышения уровня финансовой и цифровой

**Уязвимые группы населения в цифровой среде**

К наиболее уязвимым категориям граждан в цифровой финансовой среде относятся те люди, которые по разным социальным, экономическим или когнитивным причинам чаще остальных становятся жертвами мошенничества. Это главным образом пожилые граждане, люди с невысоким уровнем дохода или образования, мигранты, пользователи с ограниченными возможностями, а также те, кто редко сталкивается с современными технологиями и не обладает достаточными навыками их использования.

«Методология исследования цифровой грамотности, данные которого приводятся ниже, основана на всероссийском опросе, проведенном Аналитическим центром НАФИ в октябре 2024 года. Выборка составила 1600 человек в возрасте старше 18 лет. Она построена на данных официальной статистики Росстата и репрезентирует население РФ по полу, возрасту, уровню образования и типу населенного пункта. Статистическая погрешность данных не превышает 3,1%» [18].

Ярко выраженный разрыв между поколениями только подтверждает масштаб проблемы: среди молодых людей от 18 до 30 лет уверенно чувствуют себя в цифровой среде около 75,8% респондентов, а среди граждан старше 60 лет – всего 21,1%. Более того, 51% представителей старшего возраста прямо говорят о том, что им сложно пользоваться цифровыми сервисами, из-за чего они стараются минимизировать взаимодействие с ними. Дополнительный риск создаёт и финансовая нестабильность: люди, у которых нет накоплений, сильнее подвержены влиянию обещаний быстрой финансовой выгоды и легче попадаются на мошеннические схемы [2].

По международной методологии DigComp также хорошо видно, что пользователи старше 55 лет заметно уступают более молодым в разных видах цифровых навыков. Аналитический центр НАФИ в 2025 году подтвердил существенные различия по всем ключевым компетенциям (График 1).

Самые заметные различия – в коммуникационных навыках (разрыв 5 п.п.) и в способности решать возникшие цифровые проблемы (разрыв 3,8 п.п.). Именно эти умения наиболее важны для безопасной работы с мобильным банкингом. Анализ конкретных тем показывает, какие области вызывают наибольшие трудности у людей старшего возраста и какие риски это может создавать с точки зрения финансовой безопасности (Таблица 1).


График 1 – Значения компонент цифровой грамотности россиян младше и старше 55 лет (2025 г.), в п.п. от 0 (цифровая грамотность отсутствует) до 100 (абсолютное владение цифровыми компетенциями) [18].

Таблица 1 – Наименее усвоенные темы цифровой грамотности у россиян старше 55 лет (2025 г.)

| **Компоненты ЦГ** | **Темы теста** | **Среднее значение** |
|---|---|---|
| **Информационная грамотность** | Поиск информации на компьютере | 63,0 |
| | Поиск информации в Интернете | 73,0 |
| | Работа с информацией онлайн | 76,9 |
| | Оценка достоверности информации | 64,5 |
| | Виды информации и соответствующие им типы файлов | 80,9 |
| | Работа с информацией и данными | 74,6 |
| **Коммуникативная грамотность** | Использование мобильных устройств (smartphone, tablet) в целях коммуникации | 76,1 |
| | Использование стационарных устройств (PC, laptop) в целях коммуникации | 70,9 |
| | Традиционные форматы документов и совместная работа над ними | 56,8 |
| | Облачные документы и сервисы | 65,6 |
| | Государственные сервисы | 64,7 |
| | Финансовые и платежные услуги, электронная коммерция | 68,1 |
| | Социально-сетевые инструменты групповой работы | 71,6 |
| | Нормы общения и поведения в сети | 71,3 |
| **Создание цифрового контента** | Создание текстовых документов и электронных таблиц | 71,6 |
| | Создание изображений | 76,7 |
| | Создание аудио / видео и мультимедиа-контента | 66,2 |
| | Редактирование текстовых документов и электронных таблиц | 65,8 |
| | Редактирование изображений | 68,2 |
| | Редактирование аудио и видео | 71,1 |
| | Авторские права и лицензии | 70,5 |
| | Настройка ПО | 60,3 |
| **Цифровая безопасность** | Антивирусная защита | 81,2 |
| | Риски социальной инженерии и мошенничества с использованием высоких технологий | 68,9 |

| | | |
|---|---|---|
| | Безопасность персональных данных | 63,5 |
| | Влияние на физическое и психическое здоровье | 61,9 |
| | Влияние использования цифровых устройств на окружающую среду | 68,4 |
| **Навыки решения проблем в цифровой среде** | Решение аппаратных (hardware) проблем | 71,5 |
| | Решение программных (software) проблем | 68,4 |
| | Мобильные приложения и программы для повседневной жизни, работы и учебы | 68,5 |
| | Источники информации о новых технологиях и их использование | 76,7 |
| | Оценка и расширение знаний в сфере цифровых технологий | 60,0 |

Особенно низкий балл – 60 – получен по теме, связанной с оценкой и расширением цифровых знаний. Это говорит о том, что людям старше 55 сложнее осваивать новые цифровые навыки, понимать обновления в технологиях и своевременно замечать появление новых мошеннических схем. Гендерные различия также играют свою роль: мужчины и женщины старшего возраста показывают разные результаты по отдельным компонентам цифровой грамотности, что видно на следующей таблице (График 2).

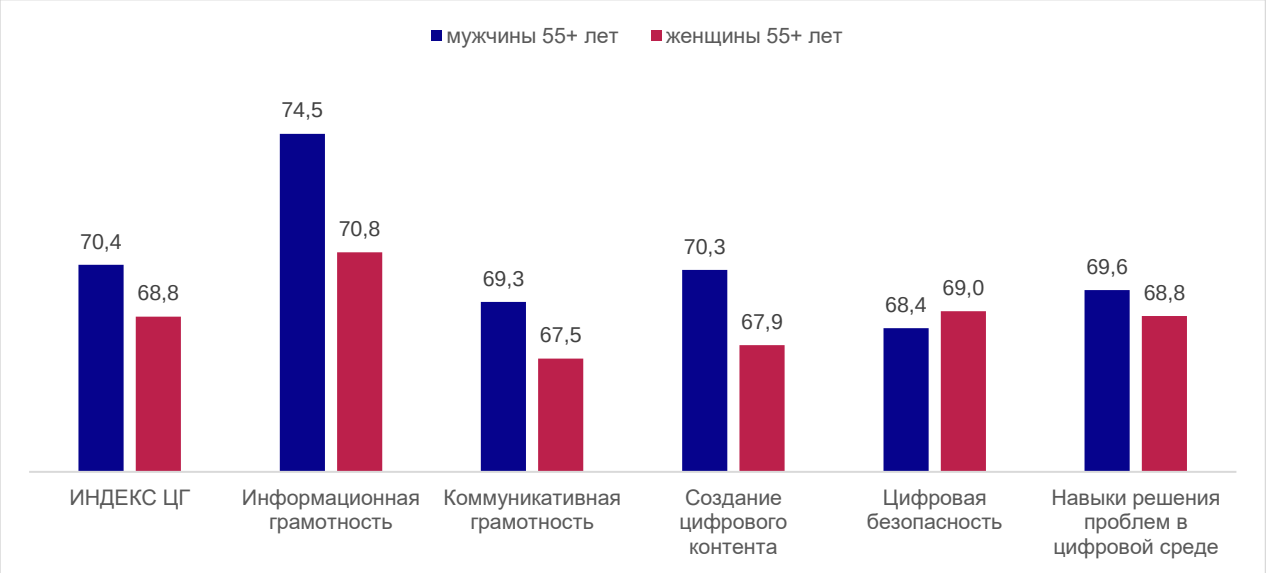


График 2 – Значения компонент цифровой грамотности мужчин и женщин старше 55 лет (данные 2025 г.), в п.п. от 0 (цифровая грамотность отсутствует) до 100 (абсолютное владение цифровыми компетенциями)

Женщины в этой возрастной группе немного лучше ориентируются в вопросах цифровой безопасности, но при этом сталкиваются с трудностями при создании цифрового контента и работе с информацией.

Дополнительные риски создаются и из-за поведенческих особенностей: многие пожилые пользователи испытывают цифровую тревожность, поэтому меньше концентрируются на деталях при использовании банковских приложений, пренебрегают базовыми правилами безопасности, слишком доверяют сообщениям, которые выглядят официально, особенно если они касаются социальных выплат или угрозы блокировки счёта.

Ещё одним признаком уязвимости является то, что представители старшего поколения ограничиваются минимальным набором операций в цифровой среде. Например, сравнительно часто пользуются онлайн-покупками (56,1%) и базовыми банковскими услугами (21,5%), но

крайне редко – сложными финансовыми сервисами, такими как страхование (1,9%) или инвестиции и НПФ (1,4%). Такая диспропорция показывает, что люди не чувствуют уверенности в работе со сложными цифровыми инструментами и поэтому более уязвимы к мошенникам, которые предлагают «выгодные вложения» или «быструю помощь» [9].

Кроме того, многие пожилые пользователи сталкиваются с социальными и психологическими трудностями – одиночеством, недостатком поддержки, страхом ошибиться. Это делает их более восприимчивыми к манипуляциям, особенно если мошенники создают видимость срочности, угрожают блокировкой счета или маскируются под официальные структуры. Возрастные когнитивные особенности, такие как более медленная обработка информации или трудности в понимании сложных интерфейсов, также повышают риски.

Дополнительным фактором является то, что старшее поколение чаще перекладывает ответственность за цифровое обучение на государство. По данным исследований, 36% граждан старше 55 лет считают, что именно государство должно обеспечивать их цифровую грамотность (для сравнения: среди молодежи так считают 29%). При этом только 30% готовы самостоятельно развивать свои цифровые навыки, тогда как среди молодых – 42%. Это создаёт потребность в продуманной системе поддержки, где важную роль будут играть социальные службы и государственные программы [14].

В итоге можно сказать, что уязвимость формируется из-за сочетания объективных причин – недостатка цифровых и финансовых знаний, слабой материальной базы – и субъективных факторов, таких как тревожность, страх ошибиться и когнитивные возрастные изменения. Все эти обстоятельства вместе делают перечисленные группы особенно привлекательной целью для мошенников, работающих через мобильный банкинг. Поэтому необходим комплекс мер защиты и обучения, который будет адаптирован под особенности каждой уязвимой категории пользователей.

**Мобильный банкинг как среда повышенных мошеннических рисков**

Мобильный банкинг сегодня стал обычной частью жизни, превратив смартфон в универсальное средство для управления личными финансами. Данные Аналитического центра НАФИ показывают: за последние шесть лет использование мобильного банка в России выросло более чем вдвое (Таблица 2). Этот формат обслуживания постепенно выходит на первое место, вытесняя интернет-банкинг, рост которого за те же годы оказался значительно слабее, а местами даже снизился (Таблица 3).

Таблица 2 – Динамика использования мобильного банкинга, в % от всех опрошенных

| | **2018** | **2020** | **2023** | **2024** |
|---|---|---|---|---|
| Да, пользовался | 34 | 51 | 70 | 74 |
| Нет, не пользовался | 66 | 49 | 30 | 26 |

Таблица 3 – Динамика использования интернет-банкинга, в % от всех опрошенных

| | **2018** | **2020** | **2023** | **2024** |
|---|---|---|---|---|
| Да, пользовался | 14 | 39 | 43 | 41 |
| Нет, не пользовался | 86 | 61 | 57 | 59 |

Сосредоточение финансовых инструментов в одном устройстве делает управление деньгами проще, но параллельно создаёт почву для увеличения мошенничества. Мобильные банковские приложения остаются одной из главных целей злоумышленников: здесь сочетаются и технические слабые места, и ошибки, которые пользователи допускают по невнимательности [17].

Отдельного внимания заслуживает ещё одна тенденция. Несмотря на рост цифровизации и увеличение числа мошеннических попыток, уровень осознанности рисков среди россиян снизился на 4 п.п. по сравнению с предыдущим годом (Таблица 4). Это может говорить о снижении осторожности, что, естественно, выгодно преступникам. Получается парадокс: чем больше людей активно пользуются цифровыми сервисами, тем менее опасными они им кажутся – при том что мошенническая активность растёт.

Таблица 4 – Восприятие рисков использования цифровых финансовых услуг, в % от всех опрошенных [18].

| | **2023** | **2024** |
|---|---|---|
| Рисков много | 59 | 55 |
| Рисков мало или их нет | 34 | 34 |
| Затрудняюсь ответить | 7 | 11 |

Современные банковские приложения – это уже не просто сервисы для переводов и проверки баланса. Они включают оформление кредитов, страховых продуктов, инвестиции, подписки и другие функции. Для продвинутых пользователей это удобство, но для людей с низким уровнем цифровой грамотности такой функционал может стать источником ошибок. Сложные интерфейсы, навязчивые всплывающие окна и многочисленные уведомления легко приводят к тому, что человек не замечает подозрительное сообщение или ошибочно нажимает на нужную кнопку [11].

Не стоит забывать и о технических рисках. Смартфоны без актуальных системных обновлений содержат дырки в защите, которые могут использоваться злоумышленниками. К этому добавляются слабые пароли, отсутствие блокировки экрана, передача телефона третьим лицам – всё это серьёзно повышает вероятность доступа к банковским данным.

Большая часть мошеннических схем строится на манипуляции и психологическом давлении. Преступники активно используют социальную инженерию: звонки или сообщения о «подозрительных списаниях», «попытке входа в приложение», «оформленном кредите». В стрессовой ситуации люди склонны действовать быстро и доверять тому, кто представляется сотрудником банка. Дополнительную угрозу создают поддельные приложения, которые внешне ничем не отличаются от настоящих банковских программ. Скачивание таких приложений из неофициальных источников фактически ведёт к полной компрометации данных пользователя [16].

За последние годы методы мошенников стали заметно технологичнее. Использование ИИ позволяет им подделывать голоса сотрудников банка, имитировать видеосвязь и создавать реалистичные сообщения. Активно применяются и технические атаки: SIM-свапинг, перехват push-уведомлений, внедрение вредоносных клавиатур, скрытые вредоносные обновления – особенно на старых устройствах и у пользователей, которые плохо разбираются в цифровых технологиях [13].

В итоге мобильный банкинг объединяет в себе и значительные преимущества, и большие риски. Уязвимее всего оказываются те пользователи, которые недостаточно хорошо понимают принципы цифровой безопасности. Быстрое расширение аудитории мобильного банкинга (Таблицы 1 и 2) на фоне снижения осознания рисков (Таблица 3) лишь повышает вероятность атак. Поэтому понимание распространённых мошеннических схем и особенностей поведения пользователей – ключевой шаг к разработке эффективной защиты и повышению уровня цифровой грамотности.

**Причины успешных мошеннических операций в отношении уязвимых пользователей**

Основные причины, по которым мошенники столь легко обманывают уязвимых пользователей мобильного банкинга, связаны с одновременным воздействием технических, организационных и психологических факторов. В результате создаётся ситуация, при которой человек не успевает оценить происходящее и совершает действия, выгодные злоумышленникам. Масштабы проблемы наглядно демонстрирует статистика последних лет, показывающая, через какие каналы атаки достигают цели чаще всего.

Таблица 5 – Основные каналы мошеннических атак против уязвимых пользователей (по данным за 2024-2025 гг.) [16].

| Канал мошенничества | Масштаб и статистика | Наиболее уязвимая группа | Финансовые потери / особенности |
|---|---|---|---|
| Социальная инженерия (звонок) | Более 353 тыс. преступлений за 9 мес. 2024 г. До 61% россиян сталкивались с подозрительными звонками. | Пользователи 65+, люди с низким уровнем цифровой грамотности. | Общий ущерб от ИКТ-преступлений – 150 млрд руб. за 9 мес. 2024 г. |
| Фишинг (SMS / Email / Мессенджеры) | Резкий рост в Telegram: 20 тыс. мошеннических ресурсов за первое полугодие 2025 г. | Пользователи 45-60 лет, ищущие альтернативные инвестиции. | Схемы с образами инфлюенсеров принесли злоумышленникам около 300 млн руб. |
| Вредоносное ПО | 68% инцидентов с частными лицами в I кв. 2024 г. Рост атак на Android в 2024 г. – в 5,2 раза. | Пользователи с устаревшими ОС, скачивающие приложения с пиратских площадок. | Ущерб всей экономике от мошеннических схем в 2024 г. оценивается до 1 трлн руб. |
| Мошенничество с использованием ИИ | Активное использование дипфейков (поддельные аудио и видео) в 2024-2025 гг. | Любая группа, подверженная доверию к визуальным и аудиодоказательствам. | Одна из самых быстроразвивающихся и опасных угроз, несмотря на отсутствие точных данных по среднему чеку. |

Одной из ключевых проблем становится то, что многие мобильные приложения банков недостаточно адаптированы под реальные возможности и опыт различных категорий населения. Интерфейсы зачастую оказываются перегруженными функциями, всплывающими подсказками и избыточными уведомлениями. Для молодых пользователей подобная насыщенность не вызывает значительных затруднений, но для пожилых людей или граждан с низким уровнем цифровой грамотности она становится серьёзным барьером. Они путаются в структуре меню, не всегда понимают смысл уведомлений и из-за этого рискуют принять фишинговое сообщение за настоящее. В таких условиях вероятность случайного подтверждения подозрительной операции существенно возрастает [1].

Кроме того, важным элементом риска выступает доверие к стандартным инструментам безопасности. Пользователи слишком часто относятся к SMS-кодам и push-уведомлениям как к формальной части процесса, не анализируя текст сообщений. За годы привычки многие нажимают кнопку подтверждения автоматически, а мошенники активно используют эту особенность. Они подделывают уведомления, перехватывают коды, используют методы социальной инженерии. На фоне того, что действующее законодательство и нормативные стандарты иногда не успевают адаптироваться к новым схемам атак, появляются уязвимости, которые злоумышленники успешно используют. Правовые механизмы не всегда оперативно реагируют на технологические изменения, что создаёт дополнительные риски [4].

Однако даже современные технические средства защиты оказываются малоэффективными, если пользователь действует под воздействием эмоций. Психологический компонент играет огромную роль: злоумышленники намеренно создают у человека состояние тревоги, сообщая о «блокировке счёта», «подозрительной операции» или «угрозе списания средств». Люди старшего возраста чаще всего испытывают сильное эмоциональное напряжение в подобных ситуациях, что снижает их способность критически оценивать информацию. Дополнительным фактором выступает доверие к авторитетным источникам – если звонящий представляется сотрудником банка, многие считают необходимым выполнить его инструкции. Мошенники искусно имитируют манеру общения специалистов, используют профессиональную терминологию и даже воспроизводят характерный звук колл-центров.

Не менее значимой проблемой остаются и технические ограничения, характерные для конкретных категорий пользователей. У многих представителей уязвимых групп установлены устаревшие смартфоны, которые давно не получают обновления безопасности. Такие устройства легче заражаются вредоносным ПО, на них проще подменить системные уведомления и перехватить данные. Кроме того, пользователи часто игнорируют базовые правила кибербезопасности: не устанавливают антивирусы, используют незащищённые Wi-Fi-сети, записывают пароли в заметки или на бумажки, передают доступ к телефону знакомым. Всё это создаёт дополнительные точки входа для злоумышленников

Отдельного внимания заслуживает низкий уровень финансовой грамотности. Многие пользователи просто не знают, что настоящий банк никогда не запрашивает коды подтверждения по телефону, не понимают, как выглядят официальные уведомления, не умеют отличать подозрительные операции и не осознают, какие действия необходимо предпринять при утечке данных. Отсутствие базовых знаний делает их лёгкой целью даже для простейших мошеннических схем [10].

Социальные обстоятельства также усиливают риск – одиночество, недостаточная поддержка со стороны родственников, стремление не «беспокоить» окружающих и желание быстро решить проблему. Особенно часто такая ситуация встречается у пожилых людей, которые по привычке доверяют «официальному голосу» и не подозревают, что реальные банки уже давно не используют практику звонков с предложением «обезопасить счёт».

В совокупности все эти факторы делают мобильный банкинг зоной повышенного риска для уязвимых категорий граждан. Ошибки пользователей обусловлены не отсутствием компетентности, а сочетанием эмоционального давления, недостатка цифровых навыков и несовершенства цифровой среды. Высокая успешность мошеннических схем объясняется не только профессионализмом злоумышленников, но и тем, что системы защиты, интерфейсы и механизмы информирования пока недостаточно адаптированы под реальные возможности и потребности различных групп населения. Понимание таких причин необходимо для разработки мер, которые действительно смогут повысить уровень цифровой и финансовой безопасности граждан.

**Механизмы повышения безопасности мобильного банкинга**

Повышение безопасности мобильного банкинга сегодня требует комплексного подхода, потому что рост цифровых мошеннических схем и активное вовлечение в них всё более уязвимых категорий населения создают дополнительные риски. По данным Банка России, только в 2024 году количество дистанционных мошеннических операций увеличилось на 22%, а суммарный ущерб граждан превысил 15,8 млрд рублей. Причём около 78% всех таких преступлений происходят именно через мобильный банкинг, который стал основным инструментом для повседневных финансовых операций. Одновременно с этим технологическая составляющая атак тоже усложняется: по данным отчёта Kaspersky за 2025 год, число вредоносных программ, нацеленных на банковские приложения, выросло в 36 раз, а количество фишинговых попыток

в сфере цифровых финансов увеличилось на 83% [7]. Всё это показывает, что повышение безопасности невозможно без сочетания технических решений, правового регулирования, а также формирования у пользователей правильных привычек цифрового поведения [5].

Технические меры сегодня играют ключевую роль в защите мобильного банкинга. Банки постепенно отказываются от классических SMS-кодов, которые легко перехватываются через SIM-свапинг или вредоносные приложения, и переходят к многофакторной аутентификации, основанной на биометрии, push-уведомлениях и динамических ключах. Распространение получает поведенческая биометрия – технология, анализирующая характерные движения пользователя, скорость ввода, силу нажатия и другие индивидуальные параметры. По оценкам компании BI.ZONE, внедрение таких решений позволяет снижать успешность мошеннических входов на 40–60%. Важным направлением стала и защита самих мобильных приложений: современные банковские программы блокируют работу на устройствах с рут-правами, проверяют наличие вредоносных компонент, а критичная финансовая информация хранится в защищённых аппаратных модулях смартфона, таких как Secure Enclave или TrustZone. Согласно Positive Technologies, почти половина атак на мобильные банки связана с подменой системных окон и интерфейсов, поэтому проверка окружения и защита от поддельных экранов становятся обязательным механизмом обеспечения безопасности.

При этом безопасность зависит не только от того, насколько защищено приложение, но и от того, насколько понятен его интерфейс. Исследования НАФИ (2025) показывают, что около 27% пользователей старшего возраста совершают ошибочные действия в мобильном приложении именно из-за непонятного или перегруженного интерфейса. Банки учитывают эту особенность и внедряют упрощённые режимы, крупные элементы управления, предупреждения о рисковых действиях, а также визуальные подсказки. Такой подход помогает снизить вероятность ошибок и делает фишинговые подделки заметнее, поскольку мошенники редко могут воспроизвести сложные анимации и визуальные элементы оригинального приложения.

Не менее существенную роль играют организационно-правовые механизмы. Банк России постепенно ужесточает требования к банковским сервисам: обязательная двухфакторная аутентификация, автоматическое применение антифрод-проверок, ограничения на сомнительные операции и информирование клиентов о новых рисках стали частью нормативных стандартов. Благодаря этому доля заблокированных подозрительных транзакций по банковской системе увеличилась с 10% до 18% всего за год. Параллельно развивается государственная система противодействия телефонному мошенничеству. Минцифры и операторы связи создают базы вредоносных номеров, блокируют подмену Caller ID и внедряют автоматические предупреждения о возможном мошенническом звонке. По данным Минцифры РФ, количество таких звонков уменьшилось на 35% за 2024 год, что показывает эффективность системных мер [6].

Однако техническая и правовая защита была бы недостаточной, если бы не сопровождалась образовательными инициативами. Проблема состоит в том, что, по данным ЦБ, 73% мошеннических операций происходят при активном участии пользователя: люди сами сообщают коды, переходят по ссылкам или следуют инструкциям злоумышленников. Поэтому важным направлением становится повышение цифровой и финансовой грамотности. В 2024 году государственные образовательные программы прошли более 1,2 млн человек, и исследования показывают, что даже краткие курсы снижают успешность атак на граждан старше 60 лет на 25–30%. Банки также активно включаются в обучение клиентов – добавляют обучающие баннеры в приложение, отправляют предупреждения, внедряют всплывающие подсказки и создают «режимы безопасности» для уязвимых пользователей [8].

Дополнительный эффект дают поведенческие механизмы защиты. Многие банки начали применять персонализированные лимиты, задержки на выполнение крупных операций, запрет переводов ночью без биометрии, а также специальные предупреждения при попытке отправить деньги незнакомому человеку. Отдельные кредитные организации используют анализ по-

ведения во время операции: если клиент получает подозрительный звонок, проявляет нервозность, делает несколько попыток подтвердить перевод или резко меняет своё поведение в приложении, антифрод-система может автоматически заблокировать операцию. По данным «Сбера», внедрение таких «анти-социально-инженерных» механизмов позволило предотвратить более 5 млн мошеннических транзакций в 2024 году.

В целом можно сделать вывод, что повышение безопасности мобильного банкинга возможно только при одновременном использовании технологических, правовых и образовательных мер. Новые механизмы делают защиту более гибкой и интеллектуальной, адаптируя её под растущие риски и особенности поведения пользователей. Комбинация биометрии, антифрода, аналитики поведения, стандартов регулятора и программ повышения цифровой грамотности позволяет значительно снижать вероятность успешных мошеннических атак и делает мобильный банкинг более безопасным даже для тех категорий населения, которые традиционно считаются наиболее уязвимыми.

## Стратегии противодействия: комплексные меры для повышения устойчивости к мошенничеству

Для обеспечения эффективной защиты пользователей мобильного банкинга от финансового мошенничества необходим комплексный подход, включающий взаимодействие финансовых организаций, государственных органов и самих пользователей. Согласно исследованию BI.ZONE, внедрение базовых элементов поведенческого анализа позволяет предотвратить до 40% попыток несанкционированного доступа, что свидетельствует о высокой результативности превентивных мер.

В рамках деятельности финансовых организаций ключевым является разработка сервисов, сочетающих высокий уровень безопасности и удобство использования. Помимо внедрения многофакторной аутентификации (включая биометрические методы и динамические коды) и систем антифрода, существенное значение имеет эргономика интерфейсов. Например, «режим безопасности», предусматривающий увеличенные шрифты, упрощённую навигацию и блокировку операций повышенного риска, таких как мгновенные переводы на новые счета, может существенно снизить вероятность ошибок у пользователей старших возрастных категорий. Современный тренд в цифровой безопасности заключается также в превентивном информировании: вместо сложных технических уведомлений используются понятные формулировки, способствующие осознанному принятию решений пользователями. Исследования НАФИ демонстрируют, что прозрачность операций и возможность их быстрой отмены повышают уровень доверия клиентов на 15–20%.

Со стороны государства и регулирующих органов значимой является разработка единых стандартов кибербезопасности и проведение образовательных мероприятий. Помимо обязательного внедрения банками сквозного шифрования и поведенческой биометрии, масштабные программы обучения пользователей оказывают существенное влияние на снижение рисков. Опыт Европейского центрального банка показывает, что даже краткосрочные целевые образовательные программы для пенсионеров снижают вероятность успешного мошенничества почти на треть. Государство может способствовать созданию национальной платформы цифровой гигиены, включающей интерактивные курсы, симуляторы атак и актуальную информацию о новых схемах мошенничества. Эффективным инструментом также является внедрение «социального лимита» – добровольного ограничения на сумму или количество операций в день, что особенно востребовано среди уязвимых категорий пользователей.

Для самих пользователей фундаментальными являются формирование и соблюдение цифровых привычек. К числу ключевых мероприятий относятся:

- Критическое восприятие информации, включающее осознание того, что сотрудники банка никогда не запрашивают полный номер карты, CVV-код или пароли из SMS;

- Техническая гигиена, предполагающая регулярное обновление операционной системы и приложений, использование исключительно официальных магазинов приложений и установку антивирусного программного обеспечения;

- Контроль доступа, включающий применение биометрии для входа в приложение и телефон, а также установку лимитов на онлайн-платежи.

Для пользователей пожилого возраста эффективной практикой является «правило двух ключей», заключающееся в обязательной консультации с технически компетентным родственником или доверенным лицом при совершении крупных или незнакомых операций.

Комплексное взаимодействие банков, государства и пользователей формирует многоуровневую систему защиты, что позволяет адаптировать меры безопасности к динамично изменяющимся угрозам. Эмпирические данные свидетельствуют, что в кредитных организациях, внедривших комплексные программы, сочетающие технологические решения и обучение клиентов, количество успешных мошеннических операций сокращается в 1,5–2 раза, что подтверждает высокую эффективность комплексного подхода [15].

## Заключение

Проведённое исследование позволило достичь поставленной цели – системно изучить риски финансового мошенничества для уязвимых групп пользователей мобильного банкинга и предложить комплекс мер по их защите. В ходе работы были решены ключевые задачи: определены основные уязвимые категории, проанализированы наиболее распространённые и эффективные схемы мошенничества, а также оценены существующие механизмы защиты. Подтверждена гипотеза о том, что уязвимость пользователей формируется комплексно, под влиянием цифрового неравенства, психологических особенностей, технических ограничений и недостаточной адаптации финансовых сервисов.

Результаты имеют практическую ценность для разных участников финансовой экосистемы. Банки могут использовать выводы для разработки инклюзивных интерфейсов, внедрения поведенческой биометрии и систем проактивного антифрода, что повышает безопасность клиентов и снижает операционные риски. Государственные и регуляторные органы получают основания для совершенствования нормативной базы, запуска образовательных программ и создания национальных платформ цифровой гигиены. Пользователи, особенно из уязвимых групп, могут применять практические рекомендации по формированию безопасных цифровых привычек.

Перспективы дальнейших исследований связаны с оценкой эффективности конкретных мер защиты через пилотные проекты, изучением новых угроз, связанных с квантовыми технологиями, а также разработкой стандартов и метрик для оценки киберустойчивости разных категорий пользователей, что позволит более целенаправленно повышать безопасность цифровой финансовой среды.

## Литература

1. Бугаева В. Б. The impact of fintech on the security of the banking sector / В. Б. Бугаева, Д. Ю. Соловьев, Т. В. Люлина // Digital Transformation and Global Society. – 2024. – Vol. 2. – P. 145–158.

2. Deepstrike. Fintech Breach Statistics 2025. – URL: https://deepstrike.io/blog/fintech-breach-statistics-2025 (дата обращения: 20.05.2025).

3. European Central Bank. Financial Literacy and Fraud Prevention: A Study on Elderly Populations. – 2023. – 45 p.

4. FinanceMagnates. Fintech investment slumps to seven-year low of USD 95.6 billion as rate hikes bite. – 2025. – URL: https://www.financemagnates.com/fintech/fintech-investment-slumps-to-seven-year-low-of-956-billion-as-rate-hikes-bite/ (дата обращения: 20.05.2025).

5. FFNews. Global fintech investment falls to seven-year low of USD 95.6 billion in 2024, but uptick in Q4'24 is a sign of cautious optimism, says KPMG's Pulse of Fintech H2'24. – 2025. – URL: https://ffnews.com/blog/2025/02/18/global-fintech-investment-falls-to-seven-year-low-of-95-6-billion-in-2024-but-uptick-in-q424-is-a-sign-of-cautious-optimism-says-kpmgs-pulse-of-fintech-h224/ (дата обращения: 20.05.2025).

6. IPP Media. Global fintech investment slips in 2024 as optimism builds for 2025. – 5 марта 2025. – URL: https://www.ippmedia.com/the-guardian/business/read/global-fintech-investment-slips-in-2024-as-optimism-builds-for-2025-2025-03-05-152834 (дата обращения: 20.05.2025).

7. Kaspersky. 36-times surge in mobile banking malware and 83% crypto-phishing spike: new financial cyber-threats report by Kaspersky. – 2025. – URL: https://www.kaspersky.com/about/press-releases/36-times-surge-in-mobile-banking-malware-and-83-crypto-phishing-spike-new-financial-cyberthreats-report-by-kaspersky (дата обращения: 20.05.2025).

8. KPMG. Pulse of Fintech H2 2024. – 2025. – URL: https://assets.kpmg.com/content/dam/kpmgsites/uk/pdf/2025/02/pulse-of-fintech-h2-2024.pdf (дата обращения: 20.05.2025).

9. Матвеевский С. С. FinTech в банковской системе России: проблемы и перспективы / С. С. Матвеевский, А. В. Иванов, П. К. Сидоров. – М. : Издательский дом «Экономика», 2019. – 256 с.

10. Наркевич С. С. Подходы к классификации инновационных финансовых технологий (FinTech) / С. С. Наркевич // Инновации. – 2019. – № 5 (247). – С. 45–52.

11. Павлов А. А. Влияние технологий FinTech на развитие банковского сектора / А. А. Павлов // Экономика и социум. – 2023. – № 2. – С. 112–118.

12. Романов В. А. Индустрия финтех: основные технологии и направления развития финансовой цифровизации / В. А. Романов, В. В. Хубулова // Вестник РУДН. Серия: Экономика. – 2020. – Т. 28, № 4. – С. 700–712.

13. Спильниченко В. К. Новые финансовые технологии (FinTech) в банковской системе: экосистемы, трансформация / В. К. Спильниченко // Индустриальная экономика. – 2021. – Т. 6, № 5–6. – С. 88–95.

14. Сулименко О. В. Развитие цифрового банкинга и компаний FinTech / О. В. Сулименко, К. А. Рябова // Финансовые исследования. – 2019. – № 4 (65). – С. 34–42.

15. Влияние технологий финтех на трансформацию финансово-экономической деятельности реального сектора экономики : коллективная монография / под ред. С. И. Петрова. – Красноярск : Сибирский федеральный ун-т, 2024. – 180 с.

16. BI.ZONE. Отчет о киберугрозах в финансовом секторе за 2024 год. – 2025. URL: https://bi.zone/ru/resources/reports/2024_financial_cyberthreats.pdf (дата обращения: 20.05.2025).

17. Positive Technologies. Анализ угроз безопасности для мобильных банковских приложений. – 2024. – URL: https://www.ptsecurity.com/ru-ru/research/analytics/mobile-banking-threats-2024/ (дата обращения: 20.05.2025).

18. Аналитический центр НАФИ. Цифровая грамотность россиян: поколенческий разрыв и профили компетенций. – 2025. – URL: https://nafi.ru/analytics/tsifrovaya-gramotnost-rossiyan-2025/ (дата обращения: 20.05.2025).

Поступила в редакцию: 19.11.25 Принята к публикации: 04.12.25

# MOBILE BANKING FOR VULNERABLE POPULATION GROUPS: ANALYSIS OF FINANCIAL FRAUD RISKS AND PROTECTION MEASURES

**Kuznetsova D.A., Sakhibgareeva E.V., Gubanova I.R.**
Financial University under the Government of the Russian Federation

***Abstract***

*The article addresses the pressing issue of ensuring the security of vulnerable population groups when using mobile banking, amidst a rapid surge in financial fraud. The digital transformation of the financial sector has significantly enhanced the convenience and accessibility of banking services; however, it has simultaneously created new threats for citizens with insufficient levels of digital and financial literacy. The research focuses on elderly users, people with low incomes, migrants, and individuals who struggle with mastering technology and operating digital devices. The analysis covers the most common fraud mechanisms, such as social engineering, phishing schemes, malicious software (malware), and the use of artificial intelligence technologies, including the generation of deepfakes to imitate the voices or appearances of acquaintances. Attention is paid to the psychological aspects of vulnerability–increased trust, digital anxiety, and stress when interacting with banking applications. Technical barriers are also examined, including complex interfaces, slow smartphones, and limited access to critical security updates. A comprehensive approach to enhancing security is proposed. This includes technological measures from banks (biometric authentication, behavioral analysis, simplified interfaces), government initiatives (educational programs, security standards), and the cultivation of conscious digital habits among users.*

***Keywords***

*mobile banking; digital literacy; vulnerable population groups; financial fraud; social engineering; cybersecurity; biometrics; digital technologies*