

УДК 622

**ТЕЛЕФОННОЕ МОШЕННИЧЕСТВО В РОССИИ:
МАШСТАБЫ, ПОРТРЕТ ЖЕРТВЫ, ПОИСК РЕШЕНИЙ**

Эндерт К.А., Пономарев К.С., Кассин М.Г.

студенты гр. БЭс-241, II курс

Научный руководитель: Слесаренко Е.В., к.н., доцент
Кузбасский государственный технический университет
имени Т.Ф. Горбачева, г. Кемерово

За последние несколько лет телефонное мошенничество превратилось из одиночных разрозненных случаев обмана в одну из главных угроз экономической безопасности страны. Так, согласно актуальным данным, ВЦИОМ, с попытками обмана по телефону сталкиваются уже 2/3 россиян, а по некоторым оценкам, этот показатель приближается к 100% [1]. При этом государственные структуры, банки и правоохранительные органы ведут непрерывную борьбу с киберпреступностью, пытаясь переломить негативный тренд.

В данной статье рассматривается текущая ситуация на основе мониторинга ВЦИОМ, данных Банка России, а также аналитики «Лаборатории Касперского» и прогнозов крупнейших финансовых институтов таких, как Сбер.

Мониторинг Всероссийского центра изучения общественного мнения (ВЦИОМ), проведенный в феврале 2024 года, фиксирует устойчивый рост количества нежелательных контактов с мошенниками. Так, если в 2021 г. о получении подозрительных звонков заявляли 57% опрошенных, то к началу 2024 г. эта цифра достигла 67%. То есть за последние полгода-год как минимум каждый третий россиянин вступал в прямой контакт с мошенниками.

При этом география преступной активности неравномерна. Наиболее уязвимыми группами оказались жители двух столиц: 85% москвичей и петербуржцев сообщили о попытках обмана. Данный факт объясняется как высокой концентрацией денежных средств в мегаполисах, так и более активно используемой цифровой средой граждан. В сельской местности этот показатель значительно ниже – 57%, что, однако, не делает сельских жителей застрахованными от атак [1].

Интересным является и тот факт, что уровень образования также коррелирует с вероятностью столкновения с мошенничеством. Среди людей с высшим и неполным высшим образованием доля получавших фейковые звонки составляет не более 77%. Эксперты ВЦИОМ полагают, что это связано не с большей привлекательностью образованных граждан как объектов мошенников, а с их способностью быстрее распознать попытку обмана и идентифицировать звонок как мошеннический. Люди с более низким уровнем образования могут просто не осознавать, что общались именно с преступником, списывая разговор на обычную рекламу или путаницу [1].

Молодежь в возрасте 18-24 лет, которая считается «цифровыми аборигенами», демонстрирует наименьшую подверженность звонковому спаму (57%), но при этом чаще других сталкивается с СМС-мошенничеством (25%). Вероятно, это связано с тем, что молодые люди активнее используют мессенджеры и реже поднимают трубку на незнакомые номера, предпочитая текстовую коммуникацию, однако именно в текстовых каналах они оказываются более уязвимы.

Несмотря на пугающую статистику звонков, данные ВЦИОМ содержат и обнадеживающие выводы. Абсолютное большинство россиян, столкнувшихся с телефонными мошенниками, не поддаются на уловки и не теряют свои средства. Так, доля финансово пострадавших среди тех, кому звонили, остается стабильно низкой: в 2024 г. – 7% (из них лишь 4% оценили ущерб как значительный). Для сравнения: в 2021 и 2022 гг. этот показатель был на уровне 9%. Таким образом, рост количества звонков не приводит к пропорциональному росту числа обманутых граждан.

Данная тенденция во многом является результатом масштабной информационно-просветительской работы и повышения финансовой грамотности среди различных групп населения. Опросы фиксируют рост уверенности граждан в своей способности противостоять злоумышленникам. В 2021 г. только 18% респондентов были уверены, что смогут распознать мошенничество, к 2024 г. этот показатель вырос до 27%. Одновременно с этим снизилась и доля пессимистически настроенных граждан (с 34% до 23%), уверенных, что обман вполне вероятен.

Наибольшую уверенность в своей неуязвимости демонстрируют мужчины (30% против 25% у женщин), молодежь до 24 лет (42%) и люди с хорошим материальным положением (40%). Активные пользователи интернета также чаще считают, что смогут распознать угрозу.

Однако, как отмечает генеральный директор Фонда ВЦИОМ Константин Абрамов [1], уверенность граждан часто противоречит реальной статистике. Методы выманивания данных совершенствуются, преступники активно используют социальную инженерию, дифференцируя жертв по возрасту, региону и даже уровню образования.

Данные Банка России, публикуемые в рамках мониторинга «Кибермошенничество: портрет пострадавшего» [2], позволяют лучше понять, кто чаще всего сталкивается с угрозой телефонного мошенничества. Как правило, в зоне риска находятся люди старшего возраста (45-59 лет). Среди этой возрастной группы 31% допускают возможность стать жертвой, и они же чаще других несут реальные финансовые потери. Люди старшего возраста часто психологически более доверчивы, менее критично относятся к звонкам от якобы «служб безопасности банков» или «правоохранительных органов».

Данные «Лаборатории Касперского» [3] за первый квартал 2025 г. подтверждают, что проблема продолжает оставаться достаточно острой. Так, почти каждый второй россиянин в этот период столкнулся с «традиционным» телефонным мошенничеством – то есть с прямыми звонками от злоумышленников.

Специалисты компании фиксируют не только количественный рост, но и эволюцию сценариев мошенничества.

Классические схемы («ваш родственник попал в ДТП», «подозрительная операция по карте») дополняются более сложными комбинациями, вовлекающими жертву в длительные диалоги и даже принуждающими к оформлению кредитов. Примечательным является тот факт, что согласно опросам, только 17% россиян сталкиваются с СМС-мошенничеством [3]. Это связано с тем, что голосовой звонок остается наиболее эффективным инструментом социальной инженерии, в ходе которого злоумышленнику проще расположить к себе собеседника, создать стрессовую ситуацию и заставить его совершить необходимые действия.

На фоне неоднозначной статистики телефонного мошенничества правоохранительные органы демонстрируют определенные успехи в сдерживании преступности. Согласно данным Генеральной прокуратуры РФ [4], в 2024 г. рост общего числа мошенничеств составил лишь 3,6%, тогда как годом ранее он достигал 27,6%. За 11 месяцев 2024 г. было зарегистрировано 411,6 тыс. мошенничеств, их доля в общей структуре преступности за пять лет возросла почти вдвое – с 12,6% до 23,3%, что свидетельствует о мошенническом перекосе в сторону киберсферы.

Ключевым фактором сдерживания стало внедрение государственной системы «Антифрод» – межоператорская система, запущенная для борьбы с подменой номеров, показала устойчивые положительные результаты. Так, доля звонков с подменных номеров снизилась с 30% до 2% от общего числа соединений. Система заблокировала более 620 млн подозрительных звонков [4].

Также функционирует система «Антифишинг», которая занимается выявлением и блокировкой мошеннических сайтов. Только за первое полугодие 2024 г. по требованиям Генпрокуратуры был ограничен доступ к более чем 60 тыс. интернет-ресурсов [4].

Тем не менее, представители финансового сектора оценивают ситуацию более осторожно. Заместитель председателя правления Сбербанка Станислав Кузнецов [5], выступая на SOC-форуме в ноябре 2025 г., признал, что коренным образом переломить тренд пока не удастся. По его словам, в 2024 г. у россиян было похищено не менее 300 млрд рублей. Более того, прогноз на 2025 г. неутешителен и рост объема похищенных средств ожидается на 15-20%.

Разрыв между успехами правоохранителей в блокировке звонков и растущими финансовыми потерями граждан объясняется несколькими факторами:

- *во-первых*, высокая адаптация мошенников, которые переходят от использования подменных номеров к мессенджерам (Telegram, WhatsApp) и звонкам через интернет (VoIP);
- *во-вторых*, реакция системы защиты зачастую запаздывает за появлением новых схем.

В ответ на новые вызовы летом 2024 г. вступил в силу закон о дополнительной защите граждан от финансовых мошенников. Данный закон [6]

обязывает банки возвращать клиентам украденные средства при определенных условиях (например, если перевод был совершен на мошеннический счет из базы Банка России, или если клиент не подтверждал операцию добровольно, став жертвой обмана без использования платежных инструментов).

Общественное мнение, зафиксированное ВЦИОМ, полностью поддерживает ужесточение ответственности финансовых организаций, предусмотренных данным ФЗ. Так, 44% россиян считают, что возвратом денег должны заниматься правоохранительные органы, 31% возлагают ответственность непосредственно на банк, услугами которого пользовался пострадавший. Лишь 13% опрошенных придерживаются консервативной позиции, полагая, что жертва сама виновата в случившемся, и возмещать ущерб не нужно.

Представленные данные показывают высокий запрос общества на защиту со стороны государства и бизнеса. Однако на практике исполнение закона сталкивается с организационными сложностями. Банки опасаются роста издержек и злоупотреблений, а правоохранительная система перегружена делами о киберпреступлениях, значительная часть которых остается нераскрытой из-за сложности идентификации преступников, часто находящихся за рубежом.

Динамика состава и структуры киберпреступлений довольно противоречива. Так, с одной стороны, очевидны институциональные и законодательные государства в виде систем защиты «Антифрод» и «Антифишинг», а также очевиден рост кибер и финансовой грамотности населения. С другой стороны, финансовая статистика говорит о росте объемов похищенных средств и усложнении схем вымогательства денег.

Прогноз Сбера на 2025 г. (рост потерь на 15-20%) указывает на то, что пик проблемы еще не пройден. Основными драйверами борьбы с киберпреступностью должно стать:

- совершенствование законодательства;
- более тесное взаимодействие банков и правоохранительных органов;
- продолжение масштабной работы по повышению финансовой грамотности.

Кроме того, гарантированным способом защиты для гражданина остается правило «нулевого доверия», то есть прекращать любой разговор, если собеседник требует сообщить коды из СМС, перевести деньги на «безопасный счет» или совершить иные финансовые операции по телефону.

Список литературы:

1. Телефонное мошенничество: мониторинг [Электронный ресурс]. URL: <https://wciom.ru/analytical-reviews/analiticheskii-obzor/telefonnoe-moshennichestvo-monitoring> (дата обращения: 30.03.2026).
2. Кибермошенничество: портрет пострадавшего [Электронный ресурс]. URL: https://cbr.ru/statistics/information_security/cyber_portrait/2024/ (дата обращения: 30.03.2026).
3. В первом квартале 2025 года почти каждый второй россиянин столкнулся с «традиционным телефонным мошенничеством»

- [Электронный ресурс]. URL: <https://www.kaspersky.ru/about/press-releases/v-pervom-kvartale-2025-goda-pochti-kazhdyj-vtoroj-rossiyanin-stolknulsya-s-tradicionnym-telefonnym-moshennichestvom> (дата обращения: 30.03.2026).
4. Почти 100% россиян сталкивались с мошенничеством за последний год [Электронный ресурс]. URL: <https://www.rbc.ru/life/news/6851731e9a79476e5b1de2d9> (дата обращения: 30.03.2026).
5. Сбербанк спрогнозировал рост потерь россиян от телефонных мошенников [Электронный ресурс]. URL: <https://1prime.ru/20251118/moshenniki-864656130.html> (дата обращения: 30.03.2026).
6. Федеральный закон от 13.02.2025 № 9-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации» // Консультант Плюс [Электронный ресурс]. URL: <https://www.consultant.ru/law/hotdocs/88316.html> (дата обращения: 30.03.2026).