УДК 004.056.5

Левченко Татьяна Александровна,
канд. экон. наук, доцент,
Владивостокский государственный университет,
г. Владивосток

Попова Татьяна Романовна,
студент 2 курса, группа БЭУ-23-ФЭ1
факультет «Экономика»,
Владивостокский государственный университет,
г. Владивосток

Телефонное мошенничество и его этапы. Профилактика и развитие устойчивости, анализ имеющихся методик, предложения по совершенствованию

Аннотация: статья посвящена проблеме телефонного мошенничества. Рассматриваются различные схемы, используемые мошенниками для обмана жертв. Представлены основные этапы мошеннических действий, а также психологические приемы, направленные на манипуляцию людьми. Рассматриваются профилактические меры, которые могут защитить пользователей. Приводятся рекомендации по улучшению существующих методов борьбы с телефонным мошенничеством.

Ключевые слова: телефонное мошенничество, жертва, профилактика мошенничества, методы мошенничества, мошенник.

Телефонное мошенничество стало одной из наиболее распространенных и актуальных проблем в современном обществе, затрагивающей как отдельных граждан, так и целые организации. С развитием технологий и увеличением количества мобильных пользователей, мошенники находят новые способы обмана граждан, что приводит к значительным финансовым потерям. По данным различных исследований, количество случаев телефонного мошенничества неуклонно растет.

Актуальность темы обусловлена не только растущей репутацией телефонного мошенничества как одной из серьезных угроз безопасности граждан, но и необходимостью формирования устойчивости общества к подобным манипуляциям.

Телефонное мошенничество – это распространенный способ обмана, когда мошенники пытаются заработать деньги, обманывая людей по телефону, не встречаясь с ними лицом к лицу. Обычно они выдают себя за родственников жертвы или притворяются сотрудниками банка.

Так, в лаборатории Касперского отметили, что в России в 2024 году зафиксирован рост телефонного мошенничества – 61% пользователей столкнулся с подозрительными звонками [11]. Как заявил замглавы Сбербанка: мошенники похитили у людей в 2024 г. 250-300 млрд. руб., а самой большой похищенной суммой МВД назвало около 180 млн. руб. [8].

По статистическим данным, представленных на сайте Центрального Банка РФ [3] наблюдается рост доли хищения сумм (таблица 1).

Таблица 1

Статистика по похищенным сумма у граждан РФ

Сумма	2023 г., %	2024 г., %	Отклонение, %
До 20 тыс. руб.	64,1	55,3	-8,8
От 20 тыс. до 100 тыс. руб.	17,9	20,3	+2,4
От 100 тыс. до 500 тыс. руб.	9,9	13,0	+3,1
От 500 тыс. до 1 млн. руб.	3,8	5,9	+2,1
Более 1 млн. руб.	4,3	5,5	+1,2

Статистика показывает, что доля хищения сумм до 20 тыс. руб. снизилась на 8,8%. В тоже время наблюдается тенденция роста доли хищений в категориях свыше 20 тыс. руб. Это указывает на то, что мошенники нацеливаются на более крупные суммы.

Чтобы понимать, какими схемами мошенничества мы сталкиваемся, важно рассмотреть способы мошенничества. Так, изучив различные источники, можно выделить распространённые способы телефонного мошенничества:

1) Родственник в беде. На телефон может прийти сообщение или звонок с новостью, что родственник в беде. Чтобы все уладить просят перевести или отнести приличную сумму денег.

2) Обвинение в государственной измене. Мошенники звонят жертве, выдавая себя за сотрудников полиции или ФСБ, и утверждают, что кто-то из банков крадет их деньги для поддержки ВСУ. Они пугают жертву, говоря о государственной измене, за которую могут дать много лет тюрьмы. В панике люди переводят свои деньги на безопасный счет или берут кредит, чтобы остановить мошенника.

3) Мошенничество на «Авито». Например, «Авито» – это площадка, где часто происходят мошенничества. Если вы хотите купить что-то, продавец может сказать, что много желающих, и попросить предоплату, чтобы забронировать товар.

После того как вы отправите деньги, он исчезает. Также, если вы сами продаете что-то, мошенники могут предложить внести предоплату, а затем попросить ваши банковские данные и коды из SMS, чтобы украсть ваши деньги.

4) Сообщение о выигрыше в лотерею. Мошенники могут звонить и говорить, что вы выиграли в лотерее, но для получения приза вам нужно покрыть какие-то расходы.

5) Звонок от правоохранительных органов. Злоумышленники звонят людям, представившись сотрудниками правоохранительных органов. Они начинают беседу с информирования о том, что по указанию Центрального банка ведется расследование о масштабной утечке банковских данных, в числе которых могут быть и сведения о собеседнике. Они просят жертву подтвердить информацию о банке и предоставить данные карты, включая трехзначный код, под предлогом проверки. Для убедительности могут отправить поддельный документ.

6) Просьбы о помощи. Мошенники взламывают аккаунт вашего друга или родственника, изучают его переписки и создают голосовое сообщение, которое сложно отличить от настоящего. В нем просят одолжить деньги из-за возникшей проблемы, обещая вернуть их в ближайшие дни. Вместо номера знакомого мошенник

предоставляет данные третьего лица, и на вопрос о необходимости отправить деньги туда он предлагает правдоподобное объяснение.

7) Смотри, какая «фотка». Мошенники отправляют сообщения с вопросом и прикрепленным файлом формата APK, который выглядит как фото. Открывать такой файл нельзя, так как он содержит вирус, способный получить доступ к банковским приложениям и украсть деньги. Также, это может быть простая ссылка с просьбой перейти на нее, что тоже влечет за собой внедрение вируса.

Мы рассмотрели самые популярные способы обмана, но мошенники не стоят на месте и придумывают всё новые и новые способы украсть наши деньги. Их так много, что все даже не перечислить. Тем не менее, если есть способы обмана, то также существуют и меры, которые помогут избежать мобильного мошенничества. Но даже самые осторожные люди иногда попадаются на крючок мошенникам. Это происходит из-за того, что мошенники применяют социальную инженерию. Е.В. Димидова-Петрона полагает, что социальная инженерия это -психологическая и речевая манипуляция человеком в целях достижения преступной цели; а приемы социальной инженерии – совокупность не только психологических, но и речевых способов манипуляции жертвой [2]. З. М. Бешукова определяет, мошенничество с использованием методов социальной инженерии происходит в четыре этапа (Рисунок 1) [1].

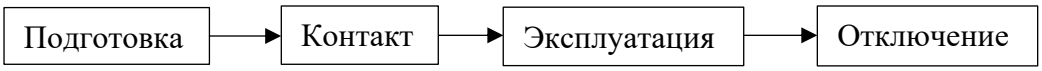

Рис. 1. Четыре этапа телефонного мошенничества

В первом этапе «подготовка» мошенник заранее собирает информацию о жертве различными способами (через социальные сети, открытые данные, размещенные на сайтах различных организаций и учреждений и т.д.). Во втором этапе «контакт» мошенник связывается с жертвой, притворяясь кем-то, кому можно доверять (например, сотрудником банка или полиции). Он использует собранную информацию, чтобы завоевать доверие жертвы. В третьем этапе «эксплуатация» мошенник убеждает жертву раскрыть ему конфиденциальную информацию, которую он использует для достижения своей цели. В четвертом этапе «исчезновение» мошенник получает, то, что ему нужно, прекращает общение с жертвой и скрывается.

Не менее важно отметить, что на каждом этапе мошенники применяют психологические уловки, чтобы убедить жертву действовать в их пользу. Изучив работы К.В. Макарова, В.А. Лукинова, в которых они описывают как мошенники манипулируют жертвами, можно описать самые распространённые [5,4]. Так, в ходе телефонного разговора мошенники используют психологические уловки:

1) Страх потери. Мошенники часто пытаются вызвать у вас чувство тревоги, сообщая о том, что ваша карта заблокирована или ваши данные могут быть украдены. Они создают атмосферу паники, чтобы вы быстрее реагировали на их требования.

2) Давление на жажду наживы. Если собеседник предлагает вам «выгодные» условия, такие как компенсации, выплаты или участие в опросах с обещанием вознаграждения, это может быть признаком мошенничества.

3) Срочность действий. Мошенники часто требуют немедленного принятия решений и могут угрожать потерей денег или возможностью получить какие-либо выгоды, если вы не выполните их инструкции.

На основании данных Центрального Банка РФ [3] за 2024 г. число случаев, когда люди совершили действия под влиянием мошенников, увеличились (Рисунок 2).

Рис. 2. Число людей, совершивших действия под влиянием

В связи с этим возникает вопрос, что необходимо сделать, чтобы люди не велись на уловки мошенников? Существует множество профилактических мер и рекомендаций, чтобы не стать жертвой мошенников. Изучив множество источников, можно выделить основные профилактические меры:

1) Не разглашать личную информацию. Никогда не следует передавать свои паспортные данные или финансовую информацию, включая данные банковской карты, её владельца, трехзначный код с обратной стороны карты и СМС-коды. Сотрудники банков и государственных учреждений не запрашивают такую информацию. Кроме того, не стоит публиковать её в социальных сетях, на форумах или веб-сайтах, а также хранить данные карт и PIN-коды на своих электронных устройствах.

2) Осторожно относиться к звонкам от неизвестных. Если поступает звонок от лица, представляющегося сотрудником Центробанка, правоохранительных органов, госучреждения или банка с предложениями, вызывающими сомнения (например, о попытке оформления кредита на имя человека или срочной необходимости перевести деньги на специальный счет), рекомендуется немедленно положить трубку. При наличии сомнений лучше позвонить в банк по номеру, указанному на банковской карте или на официальном сайте.

3) Не выполнять инструкции по переводу денег. Если звонящий требует или предлагает перевести средства на защищенный или специальный счет, необходимо быть на чеку. Банк России не открывает счета и не взаимодействует с гражданами напрямую.

4) Установить антивирусное ПО. Рекомендуется использовать антивирусное программное обеспечение на всех своих устройствах и регулярно обновлять его для обеспечения максимальной защиты.

5) Осуществлять покупки в интернете только на проверенных сайтах. Следует делать покупки исключительно на надежных и проверенных веб-сайтах. Хорошей практикой является открытие отдельной карты для интернет-покупок и пополнение её только на ту сумму, которая необходима для конкретной сделки.

Однако, профилактических мер недостаточно для защиты от мошенников. Существуют и способы защиты, которые разрабатываются Банком России и Правительством России. На основе их можно выделить преимущества и недостатки (таблица 2).

Для минимизации недостатков, важно внедрить ряд рекомендаций, которые помогут устранить выявленные проблемы. Это могут быть следующие рекомендации по совершенствованию методов борьбы с телефонным мошенничеством:

– внедрить упрощенный процесс для надежных клиентов,

– обновлять базы данных о мошеннических номерах,

– упростить процесс подтверждения для пользователей,

– регулярно обновлять и расширять базы данных.

Таблица 2

Преимущества и недостатки методов борьбы с мошенничеством

Название	Описание	Преимущества	Недостатки
Запрет на онлайн-кредитование	С 1 марта 2025 года граждане смогут воспользоваться правом на общий самозапрет на выдачу кредитов в режиме онлайн. Это будет распространяться на все кредитные и микрофинансовые организации [9].	Полностью исключает возможность оформления кредита онлайн без ведома клиента и может быть предложено всем клиентам банка, что поможет снизить количество случаев мошенничества.	Это может усложнить процесс получения кредита для добросовестных клиентов, которые предпочитают онлайн-сервисы.
Защита через оператора связи	Мобильные операторы активно развивают средства от защиты телефонных мошенников. Например, «Защитник МТС».	Предотвращает некоторые распространенные типы мошенничества (с использованием коротких номеров и ссылок).	Не защищает от всех видов мошенничества (например, звонки с подменой номера).
Подключение сервиса «второй руки»	Суть в том, что каждый дистанционный перевод средств должен быть подтвержден не только владельцем счета, но и специально назначенным лицом — так называемым «помощником» [10].	Обеспечивает дополнительную защиту транзакций, что делает мошенничество более сложным.	Для некоторых пользователей это может стать неудобным, так как требует дополнительных действий для завершения перевода.
Единая платформа верификации телефонных вызовов «Антифрод»	Платформа запущена в 2022 году для борьбы с мошенничеством. Она определяет правда ли абонент, с чего номера звонят, совершает этот звонок [7].	Используя данные от операторов связи, банков и других организаций, автоматически выявляет и блокирует подозрительные звонки.	Эффективность зависит от актуальности и полноты данных в системе.

Основным методом борьбы с мошенничеством является блокировка номеров, которые используют злоумышленники. Чтобы не стать жертвой мошенников, никогда не переводите деньги после подозрительных звонков с незнакомых номеров. Также важно проверять информацию, полученную по телефону. Для этого лучше самостоятельно позвонить в банк или родственникам [6].

В заключение, телефонное мошенничество остается серьезной проблемой в современном обществе, нанося значительный ущерб как индивидуальным гражданам, так и организациям. Растущее количество мошеннических схем подчеркивает важность повышения осведомленности и бдительности граждан. Не смотря на усилия Банка России и Правительства России минимизировать количество случаев мошенничества, телефонное мошенничество продолжает эволюционировать, осваивая новые условия и технологии. Для эффективного противодействия телефонному мошенничеству нужны новые меры по совершенствованию.

Способы защиты, применяемые сотовыми операторами против несанкционированного вмешательства, постоянно обновляются. Клиенты, пережившие негативный опыт, становятся более осторожными и недоверчивыми к информации, связанной с мобильной связью. Это дает надежду на то, что в будущем удастся полностью искоренить телефонное мошенничество или хотя бы значительно уменьшить его последствия. Можно сделать вывод, что большинство случаев обмана можно предотвратить, если подходить к информации критически, не спешить и не следовать указаниям незнакомцев, даже если они представляются сотрудниками банка или специалистами в какой-либо области.

Библиографический список

1. Бешукова З. М. Мошенничество с использованием методов социальной инженерии: механизм совершения и основные способы защиты // Цифровые технологии и право : сб. науч. тр. II Междунар. науч.-практ. конф., Казань, 22 сент. 2023 г. Казань : Познание, 2023. С. 61-64.

2. Демидова-Петрова Е. В., Зотина Е. В. Телефонное мошенничество: современные угрозы и вызовы // Всероссийский криминологический журнал. 2024. Т. 18, № 4. С. 341-348. DOI 10.17150/2500-4255.2024.18(4).341-348.

3. Кибермошенничество: портрет пострадавшего. URL: https://cbr.ru/statistics/information_security/cyber_portrait/2024/ (дата обращения: 15.02.2025).

4. Лукинова В. А. О мерах противодействия телефонному мошенничеству / В. А. Лукинова // Молодежь XXI века: образование, наука, инновации : материалы X Междунар. конф. аспирантов и молодых ученых, Витебск, 8 дек. 2023 г. Витебск : Витебский гос. ун-т им. П. М. Машерова, 2023. С. 258-259.

5. Макаров К. В., Шумилина В. Г. Речевые манипуляции в телефонном мошенничестве // Трибуна ученого. 2021. № 5. С. 397-405.

6. Мошенники звонят под видом Центробанка (ЦБ), действия финансовых мошенников. URL: https://cbr.ru/information_security/pmp/ (дата обращения: 13.02.2025).

7. Роскомнадзор запустил платформу для борьбы с телефонным мошенничеством. URL: https://digital.gov.ru/ru/events/42390/ (дата обращения: 13.02.2025).

8. Сбербанк оценил сумму похищенных мошенниками у россиян в 2024 году денег. URL: https://rbcru.turbopages.org/turbo/rbc.ru/s/society/11/01/2025/6781f-36a9a79478d4e5c2708 (дата обращения: 05.02.2025).

9. Самозапрет на заключение договоров потребительских кредитов (займов). URL: https://cbr.ru/ckki/self-prohibition_credit/ (дата обращения: 10.02.2025).

10. ЦБ поддержал механизм «второй руки» для переводов пенсионеров. URL: https://rbcru.turbopages.org/turbo/rbc.ru/s/finances/10/04/2024/661666379a79478d1-43dd36c (дата обращения: 10.02.2025).

11. Число случаев телефонного мошенничества в России за год выросло в 1,5. URL: разahttps://mkam.businessgazeta.ru/news/661639?ysclid=m6rsu3ue4q358011-824 (дата обращения: 05.02.2025).

УДК 004.056:336.11

Волков Константин Александрович,
канд. юрид. наук, доцент,
Дальневосточный филиал Университет правосудия им. В.М. Лебедева,
г. Хабаровск

Алешина Анна Альбертовна,
студент 3 курса, группа 231,
факультет подготовки специалистов для судебной системы
(юридический факультет)
Дальневосточный филиал Университет правосудия им. В.М. Лебедева,
г. Хабаровск

Роль киберграмотности в обеспечении экономической безопасности общества в контексте растущих угроз кибермошенничества на финансовом рынке Российской Федерации

Аннотация: данная работа исследует роль киберграмотности в обеспечении экономической безопасности общества в контексте растущих угроз кибермошенничества на финансовом рынке Российской Федерации. Анализируются текущее состояние киберграмотности населения, ее влияние на экономическую безопасность и предлагаются меры по повышению уровня цифровой компетентности граждан. Внимание уделяется правовым аспектам и роли Центрального банка России в противодействии кибермошенничеству.

Ключевые слова: киберграмотность, экономическая безопасность, кибермошенничество, социальная инженерия, финансовый рынок, цифровая компетентность, Центральный банк России.

В эпоху стремительной цифровизации экономики и финансового сектора проблема кибербезопасности приобретает значение для экономической безопасности общества. Актуальность тема получила в связи с ростом числа кибермошенничеств, совершаемых с применением методов социальной инженерии на финансовом рынке Российской Федерации.