УДК 343.98

М.А. Костина

Коммуникативные стратегии телефонных мошенников: технологические и методологические особенности

Аннотация:

Исследуются технологические и методологические особенности коммуникативных стратегий телефонных мошенников, рассматриваются ключевые технологии, используемые злоумышленниками: IP-телефония, подмена Caller ID, синтез голоса с помощью нейросетей (deepfake), автоматизированные системы массовых звонков и инструменты обеспечения анонимности. Особое внимание уделяется методологии социальной инженерии, включающей создание искусственной срочности, эксплуатацию авторитетов, эмоциональный шантаж и манипуляцию когнитивными искажениями жертв. Анализируется синтез технических и психологических приемов, повышающих эффективность мошеннических схем. Подчеркивается необходимость комплексного противодействия, сочетающего технологические решения (системы идентификации подозрительных звонков), правовое регулирование VoIP-сервисов и повышение цифровой грамотности населения. Предлагаются перспективные направления борьбы с телефонным мошенничеством, включая разработку ИИ-систем для детекции мошеннических коммуникативных паттернов.

Ключевые слова: телефонное мошенничество, социальная инженерия, IP-телефония, Caller ID spoofing, deepfake, кибербезопасность, психология мошенничества.

Об авторе: Костина Маргарита Андреевна, МГТУ им. Н.Э. Баумана, магистрант кафедры «Безопасность в цифровом мире»; эл. почта: kostinama@student.bmstu.ru

Научный руководитель: Багдасарьян Надежда Гегамовна, МГТУ им. Н.Э. Баумана, доктор философских наук, профессор, профессор кафедры социологии и культурологии; эл. почта: ngbagda@mail.ru

Проблема телефонного мошенничества в России приобрела критический масштаб: финансовые потери граждан продолжают расти: по данным Центробанка, в 2024 г. мошенники похитили 27,5 млрд рублей – на 74,4% больше, чем в 2023 г. При этом основной ущерб нанесен через банковские приложения (9,76 млрд руб.) [7]. Это подтверждается обращением жертв телефонного мошенничества к главе государства во время «Прямой линии с Владимиром Путиным» с просьбой оказать содействие и принять меры по защите граждан от мошеннических действий, что свидетельствует о высокой социальной напряженности вокруг этой проблемы.

В этой связи встает вопрос изучения коммуникативных и иных стратегий злоумышленников с точки зрения научной проблематики. Так, в январе 2025 г. вышел специальный выпуск журнала «Правовой альманах», посвященный борьбе с кибермошенничеством [6]. Авторы публикаций акцентировали внимание на специфике преступлений, разнообразии используемых мошенниками схем телефонного мошенничества. Особое внимание уделено социальной инженерии, как ключевому инструменту манипулирования потенциальными жертвами.

В ответ на растущую угрозу был принят новый закон, усиливающий защиту граждан от финансовых афер. Среди ключевых мер – реальный мониторинг подозрительных операций, ограничение на снятие крупных сумм, блокировка нежелательных звонков и ужесточение контроля за SIM-картами [7].

Статья направлена на анализ современных тактик телефонных аферистов, что может стать основой для разработки эффективных профилактических мер в сфере деловой и личной коммуникации. Глубокие трансформации в сфере коммуникации, происходящие в последние десятилетия, оказывают значительное влияние на все аспекты человеческой жизни, включая социальное поведение и когнитивные процессы. Современные информационно-коммуникационные технологии (ИКТ) формируют принципиально новые модели взаимодействия. Как подчеркивает М. Кастельс, стремительное развитие интернета с 1990-х гг. стало возможным благодаря трем ключевым факторам:

1. созданию Всемирной паутины как технологического прорыва;
2. децентрализованному управлению интернетом, допускающему как коммерческое, так и общественное использование;
3. глобальным изменениям в культуре и социальных практиках, включая рост индивидуализации и сетевых форм общения [4].

Важнейшим культурным сдвигом стал переход от массовых коммуникаций (через СМИ) к массовой самокоммуникации (через интернет) [4, с. 17.]. Сегодня люди проводят значительную часть времени в цифровом пространстве, оставляя множество персональных данных, которые нередко становятся инструментом в руках мошенников. Особую опасность представляет телефонное мошенничество, которое эволюционировало параллельно с развитием телекоммуникационных технологий, адаптировав стратегии к новым цифровым реалиям.

Телефонные мошенники комбинируют технологии VoIP, AI, автоматизацию и методы социальной инженерии, чтобы повысить эффективность атак. Борьба с ними требует не только технических решений (блокировка подменных номеров, анализ голосовых паттернов), но и повышения цифровой грамотности пользователей. Особую проблему представляет отсутствие визуального контакта между преступником и жертвой, что существенно сокращает объем идентификационной информации, доступной для следствия. При этом технические возможности для маскировки продолжают развиваться, опережая методы противодействия со стороны правоохранительных органов. Рассмотрим основные технологические инструменты телефонных мошенников.

1. **IP-телефония и подмена номеров (Caller ID Spoofing):**

- VoIP-сервисы (Skype, SIP-телефония, Viber Out), позволяющие звонить через интернет, маскируя реальный номер;
- подмена Caller ID – изменение номера, который видит жертва (например, имитация номера банка, госоргана или родственника);
- сервисы виртуальных номеров (Google Voice, Twilio, Zadarma), обеспечивающие возможность создания временных номеров в разных странах;
- SIP-телефония и Asterisk-ATC, использующиеся для массовых автоматизированных звонков.

2. **Голосовые технологии и искусственный интеллект:**

- Deepfake-голоса – нейросети (например, Resemble.AI, ElevenLabs), синтезирующие речь, имитируя голос знакомого человека;
- автоматизированные боты (роботы-звонящие) – записывающие или синтезирующие сообщения для массовых атак;
- обработка голоса в реальном времени – изменение тембра, интонации для создания доверия;

3. Анонимизация и обход блокировок:

- VPN и прокси-серверы, скрывающие реальное местоположение злоумышленников;
- браузеры, использующиеся для доступа к запрещенным сервисам подмены номеров;
- SIM-банки и перепродажа номеров – покупка «серых» SIM-карт через дропов (посредников).

4. Социальная инженерия и автоматизация:

- готовые скрипты (сценарии разговоров) – базы данных с проверенными фразами для разных типов жертв;
- Telegram-боты и автоматизированные системы для управления звонками, смены номеров, анализа ответов жертв;
- CRM-системы – запись разговоров, разметка успешных кейсов, ведение статистики.

5. Фишинг и удаленный доступ:

- фишинговые SMS (с поддельными ссылками) для кражи банковских данных;
- удаленный доступ через TeamViewer/AnyDesk, благодаря которым под предлогом помощи мошенники получают контроль над устройством жертвы.
- вредоносные приложения, маскирующиеся под банковские сервисы или Госуслуги [1].

Телефонные мошенники представляют собой особую категорию преступников, которые в своей деятельности искусно сочетают технические возможности с глубоким пониманием психологии человека. Коммуникативные стратегии строятся на тонкой игре человеческими эмоциями и когнитивными искажениями, что делает их методы особенно эффективными. В основе методологии мошенников лежит тщательно разработанная система психологического воздействия, включающая несколько ключевых элементов.

Распространенной для мошенников становится техника нейролингвистического программирования (НЛП). Воздействие, оказывающееся вербальным программированием, не всегда удается распознать, как неподготовленному человеку не удается распознать заблуждение или бессознательное манипулирование. Зачастую после такого общения у пострадавшего остается неприятный осадок, угнетенное и поддавленное состояние. Перечислим три известных приема, которыми пользуются мошенники: активное

использование информационных технологий, связка сообщника с сотрудником банка, предоставление ложных гарантий [5].

Важнейшим инструментом в арсенале мошенников оказывается создание искусственной срочности. Используя фразы типа «Ваш счет будет заблокирован через 10 минут» или «Если не переведете деньги сейчас, вашего родственника арестуют», они намеренно провоцируют состояние стресса у жертвы. Этот прием работает благодаря особенностям человеческой психики – в условиях дефицита времени и эмоционального напряжения критическое мышление существенно ослабевает, и человек становится более внушаемым. Дополнительную результативность придает использование социального доказательства, когда мошенники ссылаются на якобы массовый характер подобных операций («Уже 50 клиентов сегодня подтвердили свои данные»), что создает у жертвы ложное ощущение безопасности и законности происходящего.

Особое место в методологии телефонного мошенничества занимает эксплуатация авторитета. Представляясь сотрудниками банков, правоохранительных органов или государственных учреждений, злоумышленники используют естественную склонность людей доверять официальным структурам. Этот эффект усиливается за счет применения профессионального жаргона и специфической терминологии, что придает разговору видимость достоверности. Примечательно, что мошенники тщательно адаптируют свои сценарии под конкретные социальные группы – пенсионерам они говорят о пенсиях и льготах, бизнесменам – о налоговых проблемах, молодым людям – о проблемах с законом.

Эмоциональный шантаж составляет еще один важный компонент методологии. Сообщения о несчастных случаях с родственниками или угрозах карьере действуют на психику особенно разрушительно, вызывая состояние, близкое к панике. В этой связи жертва часто действует импульсивно, не подвергая информацию критической оценке. Дополнительную эффективность методу придает так называемый «эффект взаимного обмена», когда мошенники сначала якобы оказывают жертве какую-то услугу («Мы уже заблокировали несанкционированное списание») и лишь затем просят о встречной услуге («Теперь нужно подтвердить данные»), используя естественное человеческое стремление к взаимности.

Техника ведения разговора у профессиональных мошенников заслуживает особого внимания. Применяется особая манера речи – уверенная, спокойная, но в то же время настойчивая, что создает эффект «гипноза голоса». Сценарии тщательно проработаны и

включают заранее подготовленные ответы на возможные возражения. Важной частью методологии выступает предотвращение возможности перепроверки информации – мошенники искусственно создают ситуации, когда жертве якобы некогда перезвонить или проконсультироваться («Пока вы будете звонить в банк, деньги успеют списать») [3].

Психологическая уязвимость жертв усугубляется когнитивными искажениями, которыми умело пользуются преступники. Эвристика доступности заставляет людей верить в правдоподобность сообщений о проблемах с банковскими счетами или законом, поскольку подобные ситуации действительно происходят в реальной жизни. Эффект Даннинга-Крюгера проявляется, когда жертва недостаточно компетентна в вопросах банковских операций или юридических процедур, а потому не может адекватно оценить ситуацию [2].

Обозначенные психологические механизмы работают в комплексе, создавая мощный инструмент манипуляции сознанием. Защита от манипуляций требует осознания психологических механизмов. В этой связи ключевыми правилами безопасности должны стать обязательная перепроверка информации через официальные каналы, сохранение хладнокровия даже в условиях искусственно созданной стрессовой ситуации, категорический отказ от сообщения конфиденциальных данных по телефону, а также развитие привычки подвергать сомнению любые неожиданные звонки, особенно связанные с финансовыми вопросами. Понимание методологии действий мошенников и психологических приемов выступает важнейшим условием защиты от преступлений.

Проведенный анализ коммуникативных стратегий телефонных мошенников выявил их комплексный характер, сочетающий современные технологические возможности с отработанными методами психологического воздействия. На технологическом уровне преступники активно используют IP-телефонию, подмену Caller ID, голосовые нейросети и автоматизированные системы звонков, методология их действий основана на глубоком понимании психологических механизмов, включая создание искусственной срочности, эксплуатацию авторитетов, эмоциональный шантаж и использование когнитивных искажений.

Особую опасность представляет синтез технических и психологических приемов, когда, например, технология deepfake-голосов усиливает качество социальной инженерии. Это приводит к созданию высокореалистичных сценариев обмана, противодействие которым требует комплексного подхода. Примечательно, что мошенники постоянно

адаптируют свои методы, оперативно осваивая новые технологии и учитывая изменения в поведенческих паттернах потенциальных жертв.

Борьба с телефонным мошенничеством должна развиваться по нескольким направлениям: совершенствование технических средств защиты (системы идентификации подозрительных звонков, блокировки спам-активности), ужесточение регулирования VoIP-сервисов, а также повышение цифровой грамотности населения. Особое значение имеет популяризация знаний о психологических приемах мошенников, поскольку осведомленность граждан остается главным инструментом противодействия. Перспективным направлением исследований может стать разработка систем искусственного интеллекта, способных анализировать коммуникативные паттерны телефонных мошенников в реальном времени и предупреждать пользователей о потенциально опасных звонках, что уже постепенно реализуется.

Проблема телефонного мошенничества в цифровую эпоху требует постоянного внимания со стороны правоохранительных органов, телекоммуникационных компаний и общества в целом. Синтез технологических, правовых и просветительских мер сможет обеспечить прочную защиту граждан от киберпреступлений.

Библиографический список:

1. Барагунова А.Т. Проблемы расследования мошенничества, совершаемого с использованием IP-телефонии // Правовой альманах. 2025. №1 (41). С. 67-74.

2. Галяшина Е.И. Языковые приемы телефонного мошенничества и способы его распознавания // Правовой альманах. 2025. №1 (41). С. 19-26.

3. Змазнева О.А. Язык обмана: схема сценария и причины вовлечения жертв в ситуации телефонного мошенничества // Вестник МГПУ. Серия: Философские науки. 2024. №4 (52). С. 81-89.

4. Кастельс М. Власть коммуникации. М.: ВШЭ, 2020. 591 с.

5. Мочалова А.Б. Осторожно – мошенники! Или как распознать финансовых мошенников // Просвещение и познание. 2022. №5 (12). С. 24-32.

6. Правовой альманах. 2025. №1 (41) [Электронный ресурс] // Журнал «Правовой альманах». Режим доступа: https://pravovoyalmanah.ru/jurnal-in-41/ (дата обращения: 14.04.2025).

7. Путин подписал закон о защите россиян от телефонных и кибермошенников [Электронный ресурс] // РБК. Режим доступа: https://www.rbc.ru/rbcfreenews/67ebcc379a79470c4ed3220b (дата обращения: 14.04.2025).

Kostina M.A. **Communication strategies of phone scammers: technological and methodological features**

The article explores the technological and methodological features of phone scammers' communication strategies and examines the key technologies used by attackers, such as IP telephony, Caller ID spoofing, voice synthesis using neural networks (deepfake), automated mass call systems, and anonymity tools. The article also focuses on the methodology of social engineering, including the creation of artificial urgency, the exploitation of authority figures, emotional blackmail, and the manipulation of victims' cognitive biases. The article analyzes the synthesis of technical and psychological techniques that enhance the effectiveness of fraudulent schemes. The article emphasizes the need for comprehensive counteraction that combines technological solutions (suspicious call identification systems), legal regulation of VoIP services, and improving digital literacy among the population. The article also proposes promising approaches to combating phone fraud, including the development of AI systems for detecting fraudulent communications.

Keywords: telephone fraud, social engineering, IP telephony, Caller ID spoofing, deepfake, cybersecurity, psychology of fraud.