Инженерный вестник Дона, №12 (2025)
ivdon.ru/ru/magazine/archive/n12y2025/10595

Исследование уязвимостей абонента телефонной связи с точки зрения деструктивной социальной инженерии

Н.М. Котиков, Д.С. Горин, Р.Р. Шатовкин

МИРЭА – Российский технологический университет, Москва

Аннотация: Рассмотрены актуальные угрозы и уязвимости абонентов телефонной связи в условиях массовой цифровизации, развития технологий искусственного интеллекта и машинного обучения, а также их использования в мошеннических сценариях. В рамках исследования проведен анализ основных факторов уязвимости, а также рассмотрены статистические данные по инцидентам телефонного мошенничества в России и за рубежом. Отдельное внимание уделено феноменам доверия к авторитету, недостаточной цифровой грамотности и применению технологий синтеза голоса и дипфейков для реализации атак с использованием методов социальной инженерии.
Ключевые слова: социальная инженерия, мошенничество, вишинг, дипфейк, искусственный интеллект, цифровая грамотность, информационная безопасность.

Введение

Телефонная связь была и остается одним из ключевых каналов взаимодействия человека с другими людьми, государственными структурами и бизнесом. Несмотря на активное развитие цифровых сервисов и мессенджеров, традиционные методы связи по-прежнему обладают высоким уровнем популярности со стороны населения, что обусловлено их персональным характером и исторически сложившимся восприятием звонка как наиболее легитимного средства коммуникации. Этим доверием в том числе активно пользуются злоумышленники, используя в атаках с использованием методов социальной инженерии, наиболее распространенной формой которых является вишинг (voice phishing).

В своих атаках злоумышленники используют распределенную технологическую инфраструктуру, а также совокупность методов психологического давления, в результате их жертвы добровольно передают критические данные – банковские реквизиты, коды подтверждения из SMS, персональные данные и конфиденциальную информацию.

По данным Центрального Банка России, только в течение второго квартала 2024 года было зарегистрировано более 20 тысяч случаев мошенничества, связанных с социальной инженерией, что составило порядка 70 % всех инцидентов в сфере неправомерных операций без согласия клиента. Суммарный ущерб от этих действий превысил 9,3 млрд. рублей [1].

Кроме того, подобные тенденции фиксируются и мировым сообществом. Согласно Verizon Data Breach Investigations Report (DBIR) 2023 года, социальная инженерия остается одним из ведущих векторов кибератак, при этом на долю метода «искусственного предлога», который часто реализуется при помощи телефонных звонков, приходится более 50 % всех инцидентов в этом паттерне [2].

Исследование Proofpoint подчеркивает, что атаки с компрометацией деловой электронной почты – Business Email Compromise (BEC), неотъемлемой частью которых зачастую является телефонный звонок для верификации, наносят колоссальный финансовый ущерб, исчисляемый миллиардами долларов [3].

Статистический обзор показал, что число атак с использованием методов социальной инженерии ежегодно увеличивается на 20–30 %, а ущерб от подобных преступлений в мировой практике достигает миллиардов долларов. В российском контексте особую угрозу представляют звонки с подменой номера и мошенничество с использованием технологий синтеза речи, что подтверждается аналитикой компетентных компаний в области информационной безопасности.

Цель проводимого исследования – выявление ключевых аспектов, влияющих на уязвимость абонентов, и обоснование необходимости комплексного подхода к противодействию мошенничеству, включающего технические, организационные и юридические меры. В работе приведены кейсы использования технологий искусственного интеллекта в реализации

атак с использованием методов социальной инженерии, а также даны аналитические выводы в отношении масштабов проблемы.

Феномен доверия к источнику

В качестве ключевого психологического фактора, которым обусловлена эффективность телефонного мошенничества с применением методов социальной инженерии, выступает феномен автоматического доверия к источникам, обладающим признаками авторитетности или официального статуса. Данный когнитивный паттерн, известный как «принцип авторитета» [4], формируется при восприятии абонентом таких социальных институтов, как финансовые организации, государственные институты и силовые ведомства. Это доверие функционирует как когнитивная эвристика (ментальный ярлык), провоцируя снижение уровня критического мышления, пренебрежение процедурами верификации и, как следствие, способствуя успешному раскрытию конфиденциальной информации.

С точки зрения технического обоснования, ключевую роль играет спуфинг Caller ID (подмена идентификатора вызывающего абонента). Это позволяет злоумышленникам отображать номер, принадлежащий другой организации, хотя фактический вызов исходит от другой информационной системы. Отмечается, что протоколы защиты широко внедряются преимущественно в Voice over Internet Protocol (VoIP)-сетях, тогда как традиционные сети долгое время остаются слабо защищенными от подмены.

В исследовании The Impact of Call Spoofing on Trust and Communication [5] проанализирована корреляция между фактом возможности подмены, уровнем восприятия угрозы и доверия к коммуникации посредством телефонного звонка. Обнаружено, что по мере повышения уровня знаний об атаках с использованием подмены, доверие к вызовам меняется, однако степень восприятия угрозы играет лишь поведенческую роль.

Кроме того, в исследовании Users Really Do Answer Telephone Scams проанализированы случаи, когда злоумышленниками подвергается смене код региона или комбинации цифр в публичных номерах. Авторы отмечают, что визуальное восприятие, аналогично технологиям тайпсквоттинга в фишинге, существенно влияет на поведение жертв [6].

В аналитике российского сегмента прослеживается аналогичная ситуация: отчеты Group-IB подчеркивают, что звонки от сотрудников банка и службы поддержки цифровых сервисов остаются основными сценариями атак с использованием методов социальной инженерии [7].

Психологический фактор внимания

С точки зрения механизмов социальной инженерии, используемых в телефонном мошенничестве, создание искусственной временной стрессовой ситуации представляет собой высокоэффективный инструмент психологического воздействия на жертвы. Данный метод основан на искусственном создании состояния стресса путем сообщений о необходимости немедленных действий. Популярными предлогами являются: блокировка счета, мошеннические операции, подтверждение переводов, доступ к аккаунтам государственных сервисов. В условиях ограничения времени на оценку ситуации и принятие решения у жертвы наблюдается снижение способности к рациональному анализу информации, что повышает вероятность раскрытия конфиденциальной информации.

Эффективность данного метода подтверждается фундаментальными исследованиями в области когнитивной психологии и поведенческого анализа. Работы Д. Канемана и его последователей демонстрируют преобладание системы быстрого и интуитивного мышления в условиях дефицита времени, что приводит к использованию упрощенных когнитивных эвристик и снижению активности аналитического мышления [8]. Злоумышленники осознанно эксплуатируют данную закономерность, усиливая давление серией повторных

контактов и использованием комбинации методов, о чем свидетельствуют отчеты Kaspersky – 43 % россиян столкнулись с мошенническими звонками посредством мобильной связи или мессенджеров.

Недостаточная осведомленность

Недостаточная цифровая грамотность подтверждается широким спектром эмпирических исследований. Например, авторы Research of Social Engineering Mechanisms and Analysis [9] показали, что подавляющее большинство успешных атак реализуется не за счет технических параметров, а благодаря манипуляциям с восприятием и доверием жертв. Пользователи, наименее осведомленные в вопросах информационной безопасности, значительно чаще становятся жертвами мошенничества.

Аналогичные выводы были произведены в междисциплинарном исследовании Interdisciplinary view of social engineering [10]: низкий уровень цифровой гигиены является системным фактором, определяющим социальную инженерию как серьезный и долгосрочный риск. При этом в обществе с быстрым цифровым переходом, где значительная часть граждан получает доступ к цифровым сервисам без должного обучения, наблюдается наиболее высокий риск подобного воздействия.

В контексте исследования методологии социальной инженерии необходим фокус на эксплуатацию низкого уровня цифровой грамотности абонентов. Ключевым аспектом данной методологии является целевое использование когнитивных моделей, связанных с верификацией источника коммуникации.

Одним из методов является механизм доверия к визуальным маркерам и параметрам абонента. Злоумышленники манипулируют эвристикой доверия, при которой абонент подсознательно выстраивает ассоциативный ряд в отношении номера телефона, официальных реквизитов известных ему институтов и легитимностью самого звонка. Жертва, будучи убежденной в отсутствии предпосылок к подмене идентификатора, интерпретирует

параметр положительно, что позволяет злоумышленникам успешно мимикрировать под доверенный институт. Эффективность метода обусловлена в первую очередь когнитивной моделью восприятия абонента.

Другая группа методов направлена на понимание абонентом базовых норм цифровой гигиены и принципов информационной безопасности. Требование оператора раскрыть конфиденциальную информацию, такую как номера счетов, пароли, персональные данные и одноразовые коды не идентифицируется как угроза при условии первоначального доверия источнику. Таким образом, злоумышленники используют дефицит знаний и навыков, маскируя неправомерный запрос под обычную процедуру верификации пользователей.

Не менее значимым остается и недостаток навыков использования альтернативных каналов связи – абоненты редко инициируют повторное соединение с официальными контактами банка или государственного института для подтверждения полученной информации. Отсутствие привычки к верификации усугубляется использованием упрощенных когнитивных эвристик и снижением возможности критически мыслить.

Системный анализ показывает, что недостаток осведомленности абонентов фактически является основополагающим фактором, который предоставляет злоумышленникам возможность обхода современных технических средств защиты. В случае, если телеком-оператор внедрил механизмы отслеживания и фильтрации спам-вызовов или спуфинга номеров, абонент, не обладающий необходимым знаниями и навыками о природе атаки, с высокой долей вероятности раскроет конфиденциальную информацию нарушителю. А в случае отсутствия встроенных инструментов проверки подлинности абонента и оценки уровня угрозы исходящего соединения в реальном времени пользователь остается один на один с атакующим. Это подтверждают и данные Verizon Data Breach Investigations

Report (DBIR) за 2023 год: около 74 % инцидентов кибербезопасности связаны с человеческим фактором, при этом преобладающее большинство приходится именно на социальную инженерию [2].

В контексте российского сегмента мобильной связи проблема приобретает дополнительный уровень угрозы. Цифровизация правовых и государственных процессов за последние десятилетия не сопровождалась системной программой обучения и специальных мер защиты преимущественно для старших возрастных групп пользователей. Особенно уязвимы люди в возрасте 65 лет и старше, а также пользователи из группы 45–64 лет, – по данным Центрального Банка России, совокупная доля этих групп жертв кибермошенничества составляет около 44 %, при этом возрастная группа 65+ имеет долю 16,6 % от общего числа пострадавших [1].

Современные технологии и дипфейки

За последние годы генеративные модели на основе глубокого обучения достигли уровня, при котором синтезируемые изображения, видеофайлы и звукозаписи становится все сложнее отличить от реальных объективных данных. С развитием архитектур для синтеза речи, генерации речи в реальном времени (text-to-speech), а также генеративных нейронных сетей для изображений и видео появилась технологическая основа для создания дипфейк-материалов, которые активно используются в мошеннических сценариях. Одновременно появились инструменты и датасеты для создания инструментов обнаружения сгенерированного контента на базе машинного обучения, однако новые поколения генеративных моделей зачастую опережают скорость совершенствования методов детектирования.

Современные системы синтеза и клонирования речи представляют собой комплексные системы, функционирующие на основе двух взаимосвязанных модулей: акустической модели, преобразующей текст в спектральные характеристики, и голосового кодера, генерирующего звуковую

волну. Развитие этих технологий стартовало от технически сложных архитектур и достигло реализации в виде компактных решений, обеспечивающим синтез качественной и «живой» речи в реальном времени. Также стоит обратить внимание на инновационные методы клонирования голоса, позволяющие на основе короткого фрагмента речи в качестве образца создавать персонифицированные речевые модели. Такой скачок в развитии генеративных моделей обусловлен прогрессом в области алгоритмов векторного представления речи и использования эффективных голосовых кодеров. Актуальный анализ методов и их классификация представлены в обзорной работе «Voice Cloning: Comprehensive Survey», посвященной влиянию искусственного интеллекта на синтез речи [11].

Злоумышленники комбинируют возможности синтеза речи с классическими сценариями социальной инженерии, создавая новые векторы атак.

Voice-deepfake vishing: классический вишинг с использованием имитации речи близкого человека или коллеги с целью раскрытия конфиденциальной информации или осуществления мошеннических финансовых операций.

Масштаб проблемы

Атаки с использованием методов социальной инженерии остаются одним из ключевых векторов реализации экономических и социальных рисков [12]. Анализ публичных отчетов Центрального Банка Российской Федерации демонстрирует высокую частоту и экономическую значимость операций, реализуемых посредством мошеннических манипуляций и социальной инженерии. По данным обзора, в 2024 году кредитные организации предотвратили порядка 72,17 млн. попыток несанкционированных операций, при этом предотвращенная сумма составила ~13,5 трлн. рублей. Количество заблокированных мошеннических телефонных номеров – почти 172 тысячи. Эти показатели как отражают реальный объем попыток мошенничества, так и не исключают значительной части незафиксированных инцидентов.

В статистических сводках также прослеживается преобладающий характер методов в общей структуре мошенничества: социальная инженерия сохраняет ведущие позиции среди инструментов реализации неправомерных операций. Так, отчеты Банка России фиксируют десятки тысяч попыток атак в квартал: один из обзоров за II квартал 2025 г. зафиксировал ~13,7 тыс. попыток воздействия с использованием методов социальной инженерии, что на 30 % меньше среднего за предыдущий год [1].

Международные отчеты также подтверждают, что социальная инженерия представляет собой значимую долю успешных инцидентов: согласно Verizon DBIR, на методы социальной инженерии приходится нескольких десятков процентов в структуре причин утечек/компрометаций [2], а FBI/IC3 оценивает потери от интернет-мошенничества в течение 2024 года в 16,6 млрд. долларов США [13].

Заключение

Таким образом, статистические данные Банка России, а также международных регуляторов и аналитических компаний однозначно подтверждают: телефонное мошенничество и методы социальной инженерии приобрели системный характер и наносят ущерб, сопоставимый с крупными экономическими потерями. Масштаб атак измеряется миллионами попыток ежегодно, а финансовый эффект – триллионами рублей в предотвращенных транзакциях и миллиардами долларов в мировом масштабе.

Повышенный уровень риска представляет собой совмещение традиционных сценариев социальной инженерии с современными технологиями искусственного интеллекта и машинного обучения, что позволяет существенно повысить достоверность атак и усложнить их выявление. Публичные кейсы с использованием имитации голоса и регулярные спам-звонки подчеркивают актуальность и массовость проблемы.

В совокупности формируется устойчивая тенденция, при которой успешное противодействие возможно только посредством использования комплекса из технических, организационных и юридических мер. В целом, масштаб проблемы подтверждает необходимость исследований и разработки инновационных методов и средств защиты, ориентированных не только на технические, но и на поведенческие параметры атак.

Литература

1. ЦБ: использование социнженерии сократилось почти на 30 % в III квартале // URL: tass.ru/ekonomika/22618801.

2. Verizon, Data Breach Investigations Report (DBIR) 2023 // URL: inquest.net/wp-content/uploads/2023-data-breach-investigations-report-dbir.pdf.

3. Takeaways from the 2023 Verizon Data Breach Investigations Report // URL: proofpoint.com/us/blog/takeaways-from-2023-verizon-data-breach-investigations-report.

4. Афанасьева Н.С., Елизаров Д.А., Мызникова Т.А. Классификация фишинговых атак и меры противодействия им // Инженерный вестник Дона, 2022, № 5 URL: ivdon.ru/ru/magazine/ archive/n5y2022/7641.

5. A Social Engineering Attack Modeling Approach // Journal of Theoretical and Applied Information Technology, 2023. URL: iieta.org/download/file/fid/127266.

6. What is Typosquatting? // Kaspersky. URL: kaspersky.ru/resource-center/definitions/what-is-typosquatting.

7. High-Tech Crime Trends 2025 // Group-IB, 2025. URL: group-ib.com/ru/landing/high-tech-crime-trends-2025.

8. Kahneman D., Thinking, Fast and Slow. New York: Farrar, Straus and Giroux, 2011. 592 p.

9. Evglevsky V. Yu., Putyato M. M., Makaryan A. S. Research of Social Engineering Mechanisms and Analysis of Counteraction Methods // Proceedings of the International Scientific and Practical Conference on Computer and Information

Security (INFSEC 2021), 2022. URL: pdfs.semanticscholar.org/7145/c73259dbe3f5f79a426ce85cd2a2de38f631.pdf.

10. Smith J. The Psychology of Phishing: Why Users Click // Computers & Security, vol. 105, 2021. URL: sciencedirect.com/science/article/pii/S2451958821000749.

11. Azzuni H., El Saddik A. Voice Cloning: Comprehensive Survey // arXiv preprint, 2025. URL: arxiv.org/html/2505.00579v.

12. Селиверстов В.В., Корчагин С.А. Анализ актуальности и состояния современных фишинг-атак на объекты критической информационной инфраструктуры // Инженерный вестник Дона, 2024, № 6. URL: ivdon.ru/ru/magazine/archive/n6y2024/9277.

13. FBI: Internet Crime Loss Hit Record High in 2024 // Axios, 2025. URL: axios.com/2025/04/23/fbi-internet-crime-loss-record-high-2024.

References

1. TsB: ispolzovanie sotsinzhenerii sokratilos pochti na 30 % v III kvartale [Central Bank: Use of social engineering fell by almost 30% in the third quarter] URL: tass.ru/ekonomika/22618801.

2. Verizon, Data Breach Investigations Report (DBIR) 2023. URL: inquest.net/wp-content/uploads/2023-data-breach-investigations-report-dbir.pdf.

3. Takeaways from the 2023 Verizon Data Breach Investigations Report. URL: proofpoint.com/us/blog/takeaways-from-2023-verizon-data-breach-investigations- report.

4. Afanaseva N.S., Yelizarov D.A., Miznikova T.A. Inzhenernyj vestnik Dona, 2022, № 5. URL: ivdon.ru/ru/magazine/ archive/n5y2022/7641.

5. A Social Engineering Attack Modeling Approach. Journal of Theoretical and Applied Information Technology, 2023. URL: iieta.org/download/file/fid/127266.

6. What is Typosquatting? Kaspersky. URL: kaspersky.ru/resource-center/definitions/what-is-typosquatting.

7. High-Tech Crime Trends 2025 Group-IB, 2025. URL: group-ib.com/ru/landing/high-tech-crime-trends-2025.

8. Kahneman D., Thinking, Fast and Slow. New York: Farrar, Straus and Giroux, 2011. 592 p.

9. Evglevsky V. Yu., Putyato M. M, Makaryan A. S. Research of Social Engineering Mechanisms and Analysis of Counteraction Methods. Proceedings of the International Scientific and Practical Conference on Computer and Information Security (INFSEC 2021), 2022. URL: pdfs.semanticscholar.org/7145/c73259dbe3f5f79a426ce85cd2a2de38f631.pdf.

10. Smith J. The Psychology of Phishing: Why Users Click. Computers & Security, vol. 105, 2021. URL: sciencedirect.com/science/article/pii/S2451958821000749.

11. Azzuni H., El Saddik A. Voice Cloning: Comprehensive Survey. arXiv preprint, 2025. URL: arxiv.org/html/2505.00579v.

12. Seliverstov V.V., Korchagin S.A. Inzhenernyj vestnik Dona, 2024, № 6 URL: ivdon.ru/ru/magazine/archive/ n6y2024/9277.

13. FBI: Internet Crime Loss Hit Record High in 2024. Axios, 2025. URL: axios.com/2025/04/23/fbi-internet-crime-loss-record-high-2024.

Авторы согласны на обработку и хранение персональных данных.

Дата поступления: 23.10.2025

Дата публикации: 27.11.2025