Юрислингвистика

Legal Linguistics, 2026, 40, 94-102, doi: https://doi.org/10.14258/leglin(2026)4016

РЕЧЕВЫЕ ПРАВОНАРУШЕНИЯ *УДК 81-11, ББК 67.408.121.2, ГРНТИ 16.21.55, Код ВАК 5.9.8*

Телефонное мошенничество: лингвопрагматические механизмы речевого воздействия

Г. В. Напреенко[1], В. Д. Солдатова[2]

Кемеровский государственный университет

ул. Красная, 6, 650000, Кемерово, Россия. E-mail: [1]galina_napreenko@mail.ru, [2]soldatvaleria16@gmail.com

Статья посвящена исследованию лингвистических механизмов и речевых стратегий, применяемых злоумышленниками в телефонном мошенничестве. На основе комплексного анализа транскриптов реальных телефонных разговоров, полученных из открытых источников, в работе детально исследуются вербальные и паралингвистические приемы, обеспечивающие эффективное воздействие мошеннических схем на жертву. В качестве методологической основы исследования применяется теория речевых актов Дж. Остина, что позволяет выявить иллокутивные и перлокутивные эффекты в мошенническом дискурсе и проанализировать структуру диалога через призму речевых действий. В результате проведенного исследования систематизированы ключевые манипулятивные стратегии: создание искусственного цейтнота для блокировки критического мышления, симуляция официального статуса для внушения доверия, эксплуатация базовых эмоциональных реакций и использование жаргона для формирования иллюзии достоверности. Особое внимание уделяется анализу характерных речевых актов и идентификации лингвистических маркеров мошенничества, таких как отсылки к авторитету, указание точных цифр для правдоподобия, использование специфических формул («верификация данных», «блокировка счета», «подозрительные операции»). Практическая значимость работы раскрывается в нескольких аспектах: разработка образовательных программ по повышению медиаграмотности населения, создание алгоритмов автоматического распознавания мошеннических звонков на основе выявленных лингвистических паттернов, а также разработка методик лингвистической экспертизы для судебной практики. Полученные результаты позволяют углубить понимание манипулятивных механизмов в коммуникации и расширяют научные представления о роли речи в управлении поведением. Материал адресован специалистам в области прикладной лингвистики, экспертам по информационной безопасности, а также разработчикам систем защиты от социальной инженерии.

Ключевые слова: телефонное мошенничество, социальная инженерия, речевая манипуляция, коммуникативное воздействие, фишинг.

Telephone Fraud: Lingua-Pragmatic Mechanisms of Speech Influence

G. V. Napreenko[1], V. D. Soldatova[2]

Kemerovo State University

6 Krasnaya St.,650000, Kemerovo, Russia. E-mail: [1]galina_napreenko@mail.ru, [2]soldatvaleria16@gmail.com

The article covers the study of linguistic mechanisms and speech strategies used by scammers in telephone fraud for psychological manipulation of victims. Based on a comprehensive analysis of transcripts of real telephone conversations obtained from open sources, the paper examines in detail verbal and paralinguistic techniques that ensure an effective impact on the consciousness of the victim of fraudulent schemes. The theory of speech acts by J. Ostin is used as the methodological basis of the research thus enabling us to analyze illocutionary and perlocutionary effects in the dialog of fraud-related discourse. As a result of the conducted research, key manipulative strategies are systematized, including the creation of artificial time pressure to block critical thinking, the pretense of official authority to inspire trust, the exploitation of basic emotional reactions and the use of specialized jargon to create the illusion of credibility. Special attention is given to representative speech acts and language markers such as impersonation of an official, reference to data and clichés like “verification of personal data”, “account blocking”, “suspicious transaction”. The practical significance of the work is revealed in several aspects: the development of educational programs to improve the media literacy of the population, the creation of algorithms for automatic recognition of fraudulent calls based on identified linguistic patterns, as well as the development of

linguistic expertise techniques for judicial practice. The results obtained make it possible to deepen the understanding of manipulative mechanisms in communication and expand scientific understanding of the role of speech in behavior management. The material is addressed to specialists in the field of applied linguistics, information security experts, as well as developers of protection systems against social engineering.

Key words: telephone fraud, social engineering, speech manipulation, communication influence, phishing.

С момента коммерциализации и приобретения массовой доступности сотовой связи телефонное мошенничество стало социально-экономическим явлением. Распространенность случаев телефонного мошенничества демонстрирует устойчивую динамику, что напрямую коррелирует с уровнем проникновения мобильных телефонов во все возрастные и социальные группы населения. Наиболее уязвимой социальной группой для злоумышленников традиционно становятся лица с низким уровнем цифровой грамотности, в частности, представители старшего поколения. Однако потенциально жертвой телефонного мошенничества может стать любой пользователь мобильной связи, не осведомленный о базовых правилах кибербезопасности. Согласно репрезентативным данным исследования ВЦИОМ за первый и второй квартал 2021 года, с телефонным мошенничеством в форме голосовых звонков сталкивались 57 % респондентов. Еще 19 % опрошенных получали СМС-сообщения. При этом 35 % граждан указали на отсутствие подобного опыта. Финансовые потери в результате действий злоумышленников понесли 9% россиян, из которых 6 % сообщили о значительном материальном ущербе (по данным официального сайта Всероссийского центра изучения общественного мнения).

По оперативным данным, на территории Кемеровской области с начала 2024 года было зафиксировано 764 случая мобильного мошенничества. Совокупный финансовый ущерб от действий киберпреступников оценивается в 250 млн рублей. В качестве основных каналов для совершения противоправных действий злоумышленники активно используют социальные сети и площадки с размещением товарных объявлений. Наиболее распространенными схемами являются: имитация звонков от сотрудников банковских учреждений, правоохранительных органов и служб безопасности, а также инсценировка обращений от лица родственников или знакомых потерпевших. В рамках социального инжиниринга преступники информируют жертв о блокировке расчетных счетов, компрометации учетных записей, оформлении кредитов и иных фиктивных инцидентах, требующих передачи денежных средств или конфиденциальности данных (по данным регионального информационного агентства «Кузбасс»).

В отечественной криминологической науке феномен социальной инженерии остается недостаточно изученным, что актуализирует необходимость его комплексного исследования именно в криминологическом ключе с учетом методологического аппарата цифровой криминологии. Социальная инженерия приобрела выраженное криминогенное звучание в условиях интенсивного развития информационно-телекоммуникационных технологий и стала активно использоваться для совершения противоправных посягательств против собственности и безопасности информационных систем. В российском научном дискурсе концепт социальной инженерии фрагментарен. Так, В. С. Овчинский вводит категорию «психологической атаки», по содержанию эквивалентную криминальной социальной инженерии, определяя ее как нетехнический метод получения конфиденциальных данных, основанный на специфике коммуникативных взаимодействий [Овчинский 2018: 76]. Более развернутую формулировку предлагают авторы монографии «Социальная инженерия и информационная безопасность», трактуя ее как систему методов контроля и воздействия на индивидов с целью побуждения к определенным действиям, направленную на получение персональных данных для достижения преступного результата. Авторы относят социальную инженерию к сфере разработки и применения методик целенаправленного манипулирования людьми, а ее методы определяют как совокупность техник манипуляции, нацеленных на нарушение информационной безопасности [Сиротин 2023: 5].

Манипуляция человеческим сознанием способна реализовываться посредством различных инструментов, включая языковые средства. Исследование лингвистических механизмов манипулирования составляет один из ключевых объектов изучения когнитивной лингвистики. Становление речевой манипуляции в качестве самостоятельного направления лингвистических исследований произошло относительно недавно. Несмотря на актуальность данной проблематики, ее методологический аппарат остается в процессе формирования. В широком смысле О. С. Иссерс отождествляет речевое воздействие с речевым общением, поскольку даже нейтральный разговор способен структурировать и изменять картину мира собеседника. Именуя речевое воздействие убеждением в широком смысле, исследователь высказывает мысль о том, что убеждение – это «совместная идентификация, которая происходит при использовании языковых знаков, причем в процессе участвуют оба – говорящий и слушающий. У коммуникантов происходит взаимная «пристройка», взаимовлияние, поскольку в процессе общения осуществляется коррекция модели мира обоих» [Иссерс 2009: 43].

Согласно мнению В. Е. Чернявской, речевая манипуляция представляет собой форму речевого воздействия, ориентированную на имплицитное и скрытое побуждение реципиента к совершению определенных действий [Чернявская 2006: 19]. Данный процесс предполагает латентное внедрение в сознание адресата желаний, установок и поведенческих моделей, служащих реализации интересов отправителя сообщения, которые могут не совпадать с интересами самого адресата. Ключевой целью речевой манипуляции выступает склонение объекта воздействия к некритическому восприятию определенных утверждений в качестве истинных без всестороннего анализа аргументации. Речевое манипулирование вводится через отбор и применение таких языковых средств, которые позволяют оказывать целевое влияние на адресата [Чернявская 2009: 139]. Характерной особенностью является то,

что такое воздействие остается неосознанным для реципиента и воспринимается им как часть объективно передаваемой информации.

Отдельные манипулятивные уловки, распространенные языковые клише, которые используют преступники в телефонном мошенничестве, психологические предпосылки поведения потерпевших рассматриваются в работе [Кирюшина 2025]. Автор подчеркивает, что мишенями манипулятивного воздействия «практически всегда выступают устойчивые, шаблонные, стереотипные навыки и привычки восприятия, мышления, поведения» [Кирюшина 2025: 104], потерпевшими «становятся лица с прочными социальными, психологическими, нравственными и поведенческими установками» [Кирюшина 2025: 104]. В случае если реакция потерпевших не соответствует выбранному мошенниками шаблону или стереотипному поведению, общение может завершиться.

Е. И. Галяшина приводит примеры типичных речевых зачинов телефонного фишинга, в которых мошенники используют те или иные ключевые слова, воздействующие на адресата и побуждающие совершить действия, выгодные для него, например: «ваш аккаунт был взломан», «нужна твоя помощь», «данные вашей банковской карты», «перевести ваши средства на безопасный счет» и пр. [Галяшина 2025: 25].

Таким образом, речевое манипулирование предполагает не объективную репрезентацию действительности, а ее субъективную интерпретацию. При изучении данного феномена в современной лингвистике ключевое значение приобретают два термина: персуазивность и суггестивность.

Персуазивность обозначает целенаправленное языковое воздействие на сознание адресата с целью убеждения или побуждения к определенным действиям. Персуазивная коммуникация характеризуется сознательным продуцированием сообщений, направленных на изменение поведения или точки зрения реципиента [Чернявская 2012: 24].

Суггестивность подразумевает скрытое, замаскированное включение внушения в передаваемую информацию. Отличительными чертами суггестивного воздействия являются неосознанность, непроизвольность и незаметность усвоения внушаемых установок [Чернявская 2012: 25].

В соответствии с теорией речевых актов, разработанной Дж. Остином, язык рассматривается как инструмент прямого воздействия на коммуниканта. В данной парадигме каждое высказывание выполняет не только функцию передачи информации, но и обладает иллокутивной силой – способностью осуществлять определенные действия и вызывать конкретные поведенческие реакции у адресата.

Дж. Остин выделяет три структурные компонента речевого акта:

1. Локутивный акт – физическое произнесение или написание высказывания (например, фраза «Вы должны передать мне деньги» как факт артикуляции);

2. Иллокутивный акт – коммуникативное намерение говорящего, подразумеваемое действие (та же фраза воспринимается как требование или команда);

3. Перлокутивный акт – фактический результат речевого воздействия (например, передача денег адресатом) [Остин 1999: 332].

Таким образом, применение данной теории позволяет проанализировать, как языковые высказывания становятся инструментом социального воздействия. В контексте мошеннических схем перлокутивный акт выражается в том, что адресат, подчиняясь иллокутивной силе высказывания, совершает конкретные действия: передает деньги, сообщает конфиденциальные данные или иным образом выполняет указания говорящего. Совершение адресатом требуемых действий представляет собой перлокутивный эффект, который выходит за рамки простой коммуникации и переходит в практические, правовые последствия.

Данная модель применяется для анализа коммуникативных стратегий мошенников. В телефонных переговорах преобладают *директивные* (требования действий под видом официальных распоряжений), *комиссивные* (обещания решения проблем) и *эмотивные* акты (моделирование экстренных ситуаций). Стратегический отбор речевых конструкций формирует у адресата когнитивные искажения, провоцируя дальнейшие действия.

Теория Дж. Остина объясняет эффективность мошеннических схем через способность злоумышленников корректно формировать иллокутивные акты с учетом когнитивных ожиданий и социальных стереотипов жертв. Моделирование диалога и воспроизведение социальных ролей, соответствующих ожиданиям адресата, провоцируют перлокутивный эффект в форме доверия к ложному нарративу.

Эмпирической базой исследования явились 58 аудиозаписей, опубликованных на видеохостинге YouTube. В аудиозаписях зафиксирована целенаправленная деятельность блогеров по взаимодействию со злоумышленниками с целью разоблачения схем их противоправной деятельности. Длительность проанализированных записей варьируется от 1 до 30 минут. Отбор материала проводился по критериям достаточного хронометража и тематического разнообразия мошеннических сценариев, что позволило включить в анализ такие направления, как банковское мошенничество, псевдомедицинские услуги и симуляция работы органов правопорядка. Далее на примере расшифровок телефонных разговоров из видеоматериалов произведена идентификация ключевых манипулятивных приемов с цитированием речевых стратегий, эксплицирующих мошеннические намерения.

1. Создание ложного авторитета и легитимности

Мошенники часто представляются сотрудниками государственных органов, банков или известных компаний, чтобы вызвать доверие:

- *«С вами связывается главное управление МВД России, отдел экономической безопасности. С вами говорит Евгеив Андрей Андреевич».*

- *«Финансовый отдел Сбербанка вас беспокоит. Меня зовут Михаил».*
- *«Звоню Вам по теме инвестирования с коротким вопросом. Возможно, какой-то опыт у вас был уже в этом направлении?»*
- *«Здравствуйте! Меня зовут Руслан. Я представляю Тинькофф Банк. Как могу к вам обращаться?»*
- *«Главное управление МВД России вас беспокоит. Капитан полиции Звягин Сергей Андреевич. Сразу информирую о вашей записи диалога. Дальнейшая запись диалога будет подкрепляться к общим материалам дела в единый реестр».*
- *«Объясняю ситуацию. Меня зовут Сергей Иванович, фамилия Соболев, инспектор ДПС».*
- *«Я с регистратуры вам звоню… Вам нужно будет пересдать».*
- *«Полиция беспокоит вас, главного управления МВД. Лейтенант полиции Козлов Роман Сергеевич. Хотел бы обратить ваше внимание, в первую очередь, что диалог наш с вами ведется под запись телебезопасности».*

В данных примерах использование названий реальных структур («МВД России», «Сбербанк»), званий («капитан полиции») и полных ФИО выступает в качестве сигналов легитимности и выполняет перформативную функцию присвоения статуса официального институционального общения, что вызывает доверие и снижает бдительность адресата. Упоминание «материалов дела», предупреждение о «записи разговоров» и использование глаголов долженствования («Вам нужно») формирует в высказывании модальность долженствования. Эта лингвистическая стратегия направлена на конструирование фрейма «юридически неизбежного процесса», что может подавлять критическое мышление из-за страха перед системой. В коммерческих сценариях мошенники используют вежливый тон и формулы речевого этикета («короткий вопрос», «как мне к Вам обращаться?»), реализуя речевую стратегию установления контакта и вовлечения в диалог.

2. Имитация срочности и давление угрозами

Мошенники создают ситуацию повышенной эмоциональной напряженности, вынуждая адресата действовать незамедлительно, лишая его возможности рационально осмыслить происходящее:

- *«Дело в том, что 7 минут назад в реестр нашего банка поступила анкета на кредитование от ваших паспортных данных… Вы данные действия подтверждаете?»*
- *«Без пятого номера ваше письмо останется на платном хранении в сортировочном центре… 340 рублей в сутки, срок хранения 5 лет».*
- *«Две минуты назад в систему банка поступила заявка на изменение вашего финансового номера телефона. Скажите, пожалуйста, данное заявление вы подавали самостоятельно?»*
- *«Финансовая безопасность всей страны под угрозой! А вы сейчас, в данный момент, пренебрегаете предупреждениями сотрудников правоохранительных органов!»*
- *«Данную связь разрывать нельзя, мне необходимо либо же провести с Вами процедуру верификации».*
- *«Соответственно, за данным протоколом ваше финансовое обслуживание будет приостановлено на 30 минут для проведения технических работ в целях безопасности. Также обращаю ваше внимание, что диалог записывается и будет передан в правоохранительные органы по факту мошенничества».*
- *«Риски действительно присутствуют, потому что Центральный банк в заявлении указывает на ряд операций на суммы свыше 100 тысяч рублей, которые были приостановлены…».*

Упоминание точных временных рамок («7 минут назад», «2 минуты назад», «340 рублей в сутки», «30 минут») делает историю правдоподобной, создает ощущение срочности и достоверности происходящего. Адресат не успевает проверить информацию, так как вымышленная ситуация якобы развивается в реальном времени. Фразы вроде «ваше обслуживание будет приостановлено», «финансовая безопасность под угрозой» или «вы пренебрегаете предупреждениями» переводят диалог в плоскость немедленной опасности. Жертву ставят перед выбором: немедленно подчиниться или столкнуться с необратимыми последствиями. Слова «верификация», «протокол», «реестр», «приостановлено по факту мошенничества» имитируют официальную процедуру. Это лишает человека инициативы, создавая иллюзию, что все действия предопределены правилами, которые нельзя оспаривать.

3. Апелляция к страху через юридическую ответственность

Злоумышленники запугивают адресата уголовной ответственностью, блокировкой счетов или другими правовыми последствиями:

- *«Пожизненное заключение за госизмену. И это все распространяется непосредственно на родственников, друзей, коллег, детей».*
- *«Если с вашими счетами ведутся мошеннические действия, будет открыто расследование по статье 159, часть 2 по факту мошенничества».*
- *«Сегодняшним днем нам поступило заявление у Центрального банка по факту мошенничества. Это статья 159, часть 3… сотрудники полиции… массово похитили персональные данные порядка 120 тысяч граждан. И… к сожалению, вы также попали в данный список граждан, которые могут пострадать».*
- *«Вы нарушаете статью 183. Это политика конфиденциальности. Штраф в размере 1 миллиона. Либо лишение условно на 2 года».*
- *«Сегодняшним днем нам поступило заявление от Центрального банка по факту мошенничества. Это статья 159, часть 3. Гласит она о том, что это мошенничество, совершенное должностным лицом с использованием своего служебного положения».*
- *«Ой, тут авария случилась… Тут приехали родители, заявление на меня написали… Если я оплачу операцию и*

лечение их дочери, заберут заявление… запросили 30 тысяч долларов…».

- *«Если сейчас ваша карта заблокируется, или спишутся с ваших счетов деньги, мы не виноваты будем. Потому что вы прервали куплю-продажу договора».*

Упоминание конкретных статей УК РФ («статья 159, часть 2», «статья 183») и процедур («расследование», «заявление от Центрального банка») создает иллюзию легитимности. Жертва, не разбираясь в профессиональной лексике, не может сразу оценить уместность этих норм, что вызывает ощущение непререкаемости обвинений. Фразы вроде «пожизненное заключение», «штраф 1 миллион», «блокировка счетов» выполняют иллокутивную функцию прямой угрозы. Угроза намеренно масштабируется («распространяется на родственников, друзей, детей»), что реализует стратегию гиперболизации последствий, направленную на интенсификацию психологического давления и индукцию генерализированного чувства вины. Сценарий с «аварией и родителями» использует манипуляцию на личных страхах, имитируя бытовой кризис. Лексика маркирована эмоционально, также содержит прагматические маркеры срочности («ой», «заберут заявление»), что служит реализации речевой тактики провокации паники и призвано вызвать у адресата иллокутивный эффект – потребность в немедленных действиях по разрешению искусственно созданного кризиса.

4. Имитация официальных процедур

Создавая иллюзию законности своих действий, мошенники вводят адресата в заблуждение, вынуждая его пройти фиктивные технические процедуры:

- *«Нам с Вами необходимо будет составить технический дубликат анкеты… Банковская система не может одновременно рассматривать две одинаковые заявки».*
- *«Ваш номер талона 13-52-14… А теперь мне нужен ваш СНИЛС».*
- *«По регламенту банка я не могу совместить разговор, поскольку я могу вести либо же самим клиентом, либо же заверенным лицом».*

Профессиональный жаргон («технический дубликат анкеты», «регламент банка», «заверенное лицо») имитирует реальные банковские или бюрократические процедуры, что создает иллюзию официальности и заставляет адресата поверить в существование правил, с которыми он не знаком, но должен выполнить. Злоумышленники подкрепляют свои требования вымышленными, но звучащими правдоподобно обоснованиями: «система не может рассматривать две заявки» или «не могу совместить разговор». Это лишает возможности оспорить действия, так как они представлены как часть строгого технологического или юридического процесса.

5. Использование социальной инженерии и личных данных

Мошенники используют информацию об адресате (имя, место работы, семейное положение и т. п.) для того, чтобы усилить его доверие:

- *«Ваша мама родилась непосредственно в Донецкой Республике… Она говорит, на Украине у нее, ну, много то ли знакомых, то ли товарищей есть».*
- *«Вы являетесь пенсионером, верно? Вы обычный пенсионер, либо же ребенок войны, либо ветеран труда?»*
- *«Антон Олегович, в данный момент Вам нужно предоставить либо же банковский договор, номер банковского договора, либо же номер Вашей дебетовой карты…».*

Упоминание конкретных данных («Ваша мама родилась в Донецкой Республике», «Антон Олегович», статус пенсионера) создает иллюзию звонка уполномоченного сотрудника, у которого есть доступ к закрытым базам данных, что автоматически легитимизирует звонок в глазах человека. Кроме того, вопросы о статусе («пенсионер, ветеран труда») и использование имени и отчества создают видимость индивидуального подхода и заботы. Это смещает фокус с проверки личности звонящего на обсуждение проблемы, что позволяет мошеннику эффективно использовать мошенническую схему.

6. Имитация заботы и помощи

Мошенники часто выступают в роли помощников, стремящихся избавить адресата от возможных проблем:

- *«Моя задача передавать заявление на Центральный банк Российской Федерации, который займется полной проверкой, а также отменой всех неправомерных действий».*
- *«Это в ваших интересах получить полис, поймите».*
- *— И я ваши, соответственно, ваши финансы разморожу, чтобы вы спокойны были.*

— Ой, Вы знаете, а мне кажется, я не буду спокойна, пока вы не разморозите…

— Моя хорошая, вы не переживайте…

- *«Сейчас нам необходимо произвести возврат денежных средств обратно на карту, а также установить вам двухфакторную защиту для вашей безопасности».*
- *«Но вы не переживайте, на текущий момент система банка отобразила данную заявку как подозрительной, поэтому мы приостановили данную транзакцию до выяснения обстоятельств».*

Фразы «моя задача – передать заявление», «я ваши финансы разморожу» и «нам необходимо произвести возврат» создают образ сотрудника, который действует в интересах жертвы для решения некой проблемы. Эмоциональные обращения («моя хорошая», «вы не переживайте») и заверения в безопасности («для вашей безопасности») используются для снижения тревоги и блокировки сопротивления. Жертву убеждают, что ее благополучие – главная

забота звонящего. Процедуры, которые на самом деле ведут к переводу денег, подаются как защитные меры. Такой прием вынуждает человека воспринимать действия как помощь.

7. Требование конфиденциальной информации

Ключевой целью мошенников часто является получение данных для доступа к счетами или оформления кредитов:

- *«Назовите, пожалуйста, ИНН. Давайте сейчас зайдем с вами перепроверим, если не против».*
- *«Уточните, как вам будет комфортно пройти этапы идентификации. По десяти цифрам вашего финансового договора или по нумерации вашей любой активной карты?»*
- *«Уточните, пожалуйста, полный серийный номер вашего физического пластика, который с лицевой стороны. 16 цифр, сразу вас предупреждаю, это не является конфиденциальной информацией».*
- *«Карта при вас находится? Никто не мог из сторонних лиц воспользоваться?»*
- *«…предъявите проверочный код карты…это на обратной стороне карты у вас указан под магнитной полосой после вашей подписи трехзначные числа…».*
- *«Для этого мне необходимо будет указать или страховое свидетельство, или ИНН».*

Запросы данных подаются как обычные операционные действия, создавая у адресатов ощущение, что это стандартная банковская практика, не требующая повышенной бдительности. Прямые утверждения «это не является конфиденциальной информацией» или вопросы о том, «комфортно» ли предоставить данные, призваны снять естественные защитные реакции. Одновременно демонстративная забота о безопасности усиливает доверие к говорящему. Предложение выбрать способ идентификации («по договору или по карте») ставит адресата перед ложным выбором, смещая фокус внимания с вопроса «зачем это делать?» на вопрос «как это сделать?».

8. Использование терминологии, профессионального жаргона

Злоумышленники используют сложные термины, чтобы жертва почувствовала себя неуверенно и согласилась на предлагаемую помощь в вопросе:

- *«Николай, видимо, Вы стали жертвой мошеннических действий, поскольку в Ваш мобильный банк был выполнен вход из города Санкт-Петербург в мобильное устройство iPhone 6. Вам пытались изменить Ваш финансовый номер».*
- *«Система нашего банка зафиксировала несанкционированный вход в Ваш личный кабинет с города Владивосток… Также была попытка списания денежный средств на сумму 3000 рублей».*
- *«Далее будет проведен ряд оперативно-разыскных мероприятий, а также следственных действий».*
- *«Информацию запрашивал не я, а работная система. По регламенту банка я не имею права знать какой информации и запрашивать ее. Запрашивает все. Работирует система фиксации нашего банка. Это отдельный анонимный сервер между клиентом и роботом».*
- *«У Вас блокировка по карте вызвана тем, что кто-то пытался осуществить покупку через интернет-магазин…».*
- *«Для того, чтобы отменить перевод, сейчас необходимо Вас верифицировать… Говорите, активация защиты, после чего код подразделения банка…».*
- *«Поступила к нам в обработку заявка, чтобы выполнить вход в Ваш личный кабинет… Также была зафиксирована подвязка стороннего номера телефона… Вам данная личность известна?»*
- *«Приложение ВТБ Лайта в последней версии Вы не обновили. Это как раз причина взлома Вашего личного кабинета, так как во второй версии низкий уровень безопасности».*
- *«Но регламент банка вышел в 2018 году, то, что даже сотрудники не имеют права запрашивать никакой конфиденциальной информации у клиента».*
- *«В данный момент в нашей системе зафиксирована заявка на пополнение электронного кошелька с Вашей карты за банк».*
- *«…произошла утечка персональных данных, то есть их кража. Полный пакет документов был скомпрометирован, в том числе внутрибанковская информация».*

Употреблением терминов («несанкционированный вход», «оперативно-разыскные мероприятия», «верификация», «подвязка номера»), ссылкой на сложные системы («работирует система фиксации», «анонимный сервер») мошенник создает иллюзию своей экспертизы. Адресат, не разбираясь в деталях, теряется и соглашается с требованием.

9. Дискредитация реальных служб поддержки

Мошенники убеждают адресата в том, что только они способны разрешить возникшую ситуацию, в то время компетентность официальных служб ставится под сомнение:

- *«С вами уже связался квалифицированный специалист Департамента контроля финансовых операций… Сбербанк некомпетентен в решениях таких вопросов, поскольку там работают обычные менеджеры».*

10. Постановка наводящих вопросов для сбора информации

Под предлогом помощи в расследовании мошенник задает вопросы, цель которых – выяснить информацию для того, чтобы в дальнейшем ее использовать:

- *«Скажите, в каких банковских структурах могут фигурировать ваши паспортные данные?»*
- *«Вадим Павлович, вы не пользуетесь ни одним банком на территории Российской Федерации?»*
- *«Картой какой пользуетесь? Зарплатная, кредитная, пенсионная?»*
- *«Скажите, пожалуйста, а вот именно последнюю операцию, которую вы совершали, помните?»*

- *«Скажите, пожалуйста, сколько активных пластиковых продуктов вы в данный момент используете от Сбербанка?»*

Каждый вопрос направлен на выяснение конкретных параметров финансового профиля: какие банки используются адресатом, тип карты, количество продуктов, детали последних операций. Вопросы формулируются в рамках мнимой легитимности процедуры («помощь в расследовании»), что создает впечатление их законности. Адресат ошибочно воспринимает предоставление запрашиваемой информации не как раскрытие персональных данных, а как участие в процедуре их верификации.

11. Давление и обвинение

При возникновении попыток отрицания со стороны адресата в ходе коммуникативного взаимодействия злоумышленник прибегает к тактике агрессивного воздействия, выдвигая обвинения в недостоверности предоставляемых сведений, во лжи. Данный прием провоцирует эмоциональный дискомфорт и стимулирует адресата к раскрытию фактической информации вследствие испытываемого чувства вины.

- *«Зачем мне ложную информацию сейчас предоставлять?»*
- *«Ну, а чего Вы молчали, Вадим?»*

12. Создание иллюзии безопасности

Мошенник специально подчеркивает, что не запрашивает личную информацию, чтобы успокоить бдительность адресата и представить свои вопросы как рутинную и безопасную процедуру:

- *«Я понимаю, но я у вас никакой секретной информации не запрашиваю, это во-первых».*

13. Имитация системы поддержки

Для правдоподобности мошенники могут имитировать передачу звонка между отделами или банками:

- *«Ожидайте, пожалуйста, на линии в течение 30 секунд. С вами свяжется специалист банка».*
- *«Павел, здравствуйте. Старший специалист банка передает заявку от Сбербанка о факте мошенничества».*

Фразы «передает заявку от Сбербанка» и «ожидайте на линии» точно копируют реальные процессы взаимодействия между банковскими службами. Это создает впечатление сложной внутренней системы, работающей по установленным протоколам.

14. Эксплуатация дополнительных каналов для подтверждения надежности звонка

Мошенники предлагают проверить их номер через сервис Google или Яндекс, чтобы убедить в своей легитимности:

- *«Проверьте номер сейчас. Откройте либо Яндекс, либо Google. У вас номер отображается, с которого я вам звоню. Введите этот номер сейчас».*
- *«Мы вам сейчас отправляем рассылку от нашей компании «Авито» на номер твоего телефона… Проверьте самую верхнюю СМС-рассылку».*

Предложение проверить номер через поисковые системы эксплуатирует доверие людей к этим платформам. Адресат думает, что «если номер отображается в поиске, значит, он настоящий». При этом мошенник может использовать поддельный номер, зарегистрированный в спам-базах, или номер, который действительно принадлежит банку. Фразы «проверьте самую верхнюю СМС-рассылку» и «введите номер сейчас» заставляют выполнять конкретные инструкции.

15. Фишинг под видом возврата средств

Мошенник звонит под видом «аналитического отдела Сбербанка» и предлагает вернуть средства с брокерского счета:

- *«У вас одобрена заявка на ИМИС. Общая сумма 34800 долларов… В течение суток сумма поступает вам на карту».*

Фразы «у Вас одобрена заявка» и «сумма поступает» формирует восприятие процесса как свершившегося события без вмешательства клиента.

Упоминание ИМИС как настоящего финансового продукта, указание конкретной суммы и временных рамок усиливает реалистичность ситуации, отвлекает от возможных рисков путем предоставления детализированной информации.

16. Блокировка счета как метод давления

Мошенник угрожает заблокировать счета, если адресат отказывает сотрудничать:

- *«Я на данный момент блокирую ваши счета на срок от 30 до 90 банковских дней на время разбирательства».*
- *«У вас была перерегистрация мобильного банка… Ваша карта будет заблокирована сроком на 90 дней до выяснения обстоятельств».*
- *«Мне нужно вас идентифицировать как клиента нашего банка по номеру договора… Если вы мне не доверяете, я заблокирую ваши все счета».*

Категоричные формулировки («если вы мне не доверяете, я заблокирую») превращают нежелание адресата сообщать данные в причину для применения санкций. Это ставит жертву перед выбором: немедленное сотрудничество или полная блокировка счетов. Также упоминание конкретных сроков («от 30 до 90 банковских дней»)

и процедурных формулировок («до выяснения обстоятельств», «на время разбирательства») имитирует юридически корректный процесс, что заставляет жертву поверить в законность угрозы и необходимость соблюсти инструкции, чтобы избежать блокировки финансов.

17. Фишинг под видом технической поддержки

Мошенник под предлогом «защиты от вирусов» заставляет установить программу удаленного доступа:

- *«Установите программу поддержки клиентов… TeamWeaver QuickSupport… Это для очистки вашего телефона от вирусных и вредоносных исчитывающих программ».*

Указанная программа удаленного доступа представляется как программа поддержки клиентов и инструмент для очистки от вирусов. Упоминание «вирусных и вредоносных исчитывающих программ», где «исчитывающих» – псевдопрофессиональный неологизм, имитирует техническую экспертизу и запугивает адресата несуществующей опасностью, требуя немедленных действий.

18. Запрос подтверждения действий

Мошенники пытаются заставить адресата санкционировать транзакции, чтобы затем использовать согласие в собственных корыстных целях:

- *«Подскажите, вы совершали вход в ваш личный кабинет 7 минут назад… Дело в том, что у вас транзакция, которая ожидает вашего дополнительного подтверждения, перевод на сумму 4200 рублей, насчет получателя Сидоренко Алексея Владимировича. Вы подтверждаете данный перевод?»*

Указание точного времени, суммы и ФИО получателя создает иллюзию реально существующей транзакции. Вопрос «Вы подтверждаете данный перевод?» маскируется под стандартную банковскую проверку. Человек, опасаясь несанкционированного списания денег, подтверждает операцию, не понимая, что этим дает согласие на противоправные действия в свой адрес.

К сожалению, в настоящее время не существует эффективной защиты от телефонного мошенничества посредством использования готового списка телефонных номеров мошенников для их блокировки в функции «черный список». Единственным доступным способом фильтрации остается ручное внесение незнакомых номеров в базу данных абонентского устройства с последующей их идентификацией и блокировкой.

Согласно исследованиям, телефонные мошенники обычно осуществляют предварительно подготовленный телефонный звонок [Кудрявцева 2014: 335]. Злоумышленники могут располагать информацией о размере денежных средств на счетах потенциальной жертвы, а также о последних финансовых операциях.

Ключевым элементом системы противодействия остается своевременная передача информации о фактах телефонного мошенничества в правоохранительные органы для проведения процессуальных и оперативно-разыскных проверок.

Проведенное исследование позволяет констатировать, что телефонное мошенничество представляет собой многоаспектный феномен, эффективность которого в значительной степени обусловлена умелым применением злоумышленниками речевых приемов манипуляции.

В качестве методологической основы исследования использована теория речевых актов Дж. Остина, что позволило проанализировать мошеннический дискурс через призму иллокутивных намерений (директивы, комиссивы, эмотивы) и достигаемых перлокутивных эффектов (доверие, совершение целевых действий). Систематизированы ключевые манипулятивные приемы, к которым относятся: создание искусственного цейтнота для подавления критического мышления жертвы, симуляция официального статуса для внушения доверия, эксплуатация базовых эмоций (страха, жадности, желания помочь) и использование специализированного жаргона для формирования иллюзии достоверности.

Выявлены характерные лингвистические маркеры мошеннического дискурса, такие как отсылки к авторитету («МВД России», «Сбербанк», «Центральный банк», «капитан полиции», «инспектор ДПС»), указание точных цифр и временных рамок («7 минут назад», «в течение суток», «340 рублей в сутки»), использование специфических формул, создающих иллюзию официальности и срочности («верификация данных», «блокировка счета», «подозрительные операции», «протокол», «реестр», «срочно требуется», «иначе будут последствия»). Ключевыми также являются термины, эксплуатирующие эмоции страха и доверия («мошенничество», «уголовная ответственность», «штраф»), и жаргон, имитирующий профессиональные процедуры («технический дубликат анкеты», «регламент банка», «двухфакторная защита», «несанкционированный вход», «анонимный сервер»). Эта лексика выполняет перлокутивную функцию, направленную на подавление критического мышления, формирование доверия и побуждение к немедленным действиям. Ее распознавание позволяет идентифицировать манипулятивную коммуникацию на ранних этапах взаимодействия.

Практическая значимость работы заключается в возможности применения ее результатов в нескольких сферах: разработка программ и материалов для повышения медиаграмотности и цифровой грамотности населения; создание алгоритмов и систем автоматического распознавания мошеннических звонков на основе выявленных лингвистических и паралингвистических паттернов; разработка методик лингвистической экспертизы для анализа коммуникации в целях установления фактов манипуляции.

Таким образом, лексика в телефонном мошенничестве – это не просто набор слов, а инструмент. Мошенники виртуозно комбинируют приемы легитимизации, давления и манипулятивной неопределенности, чтобы

последовательно лишить человека бдительности, вызвать нужную эмоцию (страх, доверие) и в конечном итоге добиться своей преступной цели. Понимание лингвистических уловок позволяет распознать манипуляцию на раннем этапе и прервать диалог. Дальнейшие исследования в данном направлении могут быть сосредоточены на детальном анализе вариативности речевых стратегий в зависимости от целевой аудитории, а также на разработке и внедрении образовательных технологий.

Список источников

Региональное информационное агентство «Кузбасс». URL: https://kuzbass.media/2024/05/04/49754.html
Официальный сайт Всероссийского центра изучения общественного мнения. URL: https://wciom.ru/analytical-reviews/analiticheskii-obzor/telefonnoe-moshennichestvo-masshtaby-i-poteri

Литература

Галяшина Е. И. Языковые приемы телефонного мошенничества и способы его распознавания / Правовой альманах. - 2025. - №1 (41). URL: https://cyberleninka.ru/article/n/yazykovye-priemy-telefonnogo-moshennichestva-i-sposoby-ego-raspoznavaniya
Иссерс О. С. Речевое воздействие: Учебное пособие для студентов, обучающихся по специальности «Связи с общественностью». М., 2009.
Криминология / под ред. В. Н. Кудрявцева и В. Е. Эминова. 5-е изд., перераб. и доп. М., 2014.
Овчинский В. С. Криминология цифрового мира. М., 2018.
Остин Дж. Избранное; перевод с англ. Л. Б. Макеевой и В. П. Руднева. М., 1999.
Социальная инженерия и информационная безопасность: монография. М., 2023.
Чернявская В. Е. Дискурс власти и власть дискурса: проблемы речевого воздействия. М., 2006.
Чернявская В. Е. Дискурс власти и власть дискурса: проблемы речевого воздействия. М., 2012.
Чернявская В. Е. Лингвистика текста. Поликодовость, интертекстуальность, интердискурсивность. М., 2009.

References

Austin, J. L. (1999). Favorites. Translated from English by L. B. Makeeva and V. P. Rudnev. Moscow (in Russian).
Chernyavskaya, V. E. (2006). The discourse of power and the power of discourse: problems of speech impact. Moscow (in Russian).
Chernyavskaya, V. E. (2009). Linguistics of the text. Polycode, intertextuality, interdiscursivity. Moscow (in Russian).
Chernyavskaya, V. E. (2012). The discourse of power and the power of discourse: problems of speech impact. Moscow (in Russian).
Criminology / edited by V. N. Kudryavtsev and V. E. Eminov. (2014). 5th ed., revised and additional. Moscow (in Russian).
Galyashina, E. I. (2025). Linguistic techniques of telephone fraud and ways of its recognition. Legal Almanac, 1 (41). Available from: https://cyberleninka.ru/article/n/yazykovye-priemy-telefonnogo-moshennichestva-i-sposoby-ego-raspoznavaniya (in Russian).
Issers, O. S. (2009). Speech impact: A textbook for students studying in the specialty "Public Relations". Moscow (in Russian).
Kiryushina, L. (2025). Manipulative Form of Communication as One Way of Committing Telephone Fraud. Jurilinguistics, 37, 103–107 (in Russian).
Ovchinsky, V. S. (2018). Criminology of the digital world. Moscow (in Russian).
Social engineering and information security (2023). Monograph. Moscow (in Russian).

Citation:
Напреенко Г. В., Солдатова В. Д. Телефонное мошенничество: лингвопрагматические механизмы речевого воздействия // Юрислингвистика. – 2026 – 40. – С. 94-102.
Napreenko G. V., Soldatova V. D. (2026) Telephone Fraud: Lingua-Pragmatic Mechanisms of Speech Influence. Legal Linguistics, 40, 94-102.