УДК 159:004:343.9.018
https://doi.org/10.17072/2078-7898/2024-3-374-390
EDN: UIDSUM

Поступила: 01.08.2024
Принята: 16.09.2024
Опубликована: 03.10.2024

МАНИПУЛЯЦИЯ ЭМОЦИОНАЛЬНОЙ БЕЗОПАСНОСТЬЮ КИБЕРМОШЕННИКАМИ С ПРИМЕНЕНИЕМ ТЕХНОЛОГИЙ СОЦИАЛЬНОЙ ИНЖЕНЕРИИ: CASE-STUDY

Игнатова Екатерина Сергеевна

Пермский государственный национальный исследовательский университет (Пермь)

В психологии распространяющееся социальное мошенничество только становится предметом интереса. Мошенничество рассматривается с точки зрения манипулятивного воздействия на психическое состояние потенциальной жертвы, «добровольно» нарушающей информационную безопасность. Поставлена и обоснована проблема необходимости распознавания механизма мошеннического воздействия на личность и ее поведение. Рассмотрены теоретические основы указанной проблемы. Показан исторический аспект применения технологий социальной инженерии для получения персональной информации и регуляции человеческого поведения. Описаны виды социального мошенничества. Обозначена неоднородность мошеннических схем. Представлены факторы мошеннического воздействия, выступающие мишенями, в т.ч. приведены эмпирически подтвержденные личностные особенности потенциальных и реальных жертв, их системы мышления и базальной эмоциональной регуляции. Показана роль когнитивных искажений, снижающих эффективность критического мышления в эмоционально небезопасном состоянии. Выявлены этапы оказания манипулятивного воздействия мошенниками. Описан психологический анализ случая манипулятивного воздействия на эмоциональную безопасность кибермошенниками с применением технологий социальной инженерии. Представлены результаты исследования личности жертвы кибермошенников. Обнаружено соответствие личностных особенностей испытуемого эмпирическому портрету жертвы мошенников в выраженных показателях доброжелательности, добросовестности, тревожности, ориентации на ценность безопасности, убежденности в морально-нравственных качествах Другого. Анализ нарратива жертвы кибермошенников позволил описать сценарий злоумышленников в диапазоне «ситуационная напряженность – снятие психологического» напряжения, когда жертву последовательно лишают ключевых составляющих эмоциональной безопасности: спокойствия, уверенности в управляемости происходящим и возможности прогноза последствий; установить соответствующую динамику эмоционального переживания жертвы и ее влияния на восприятие реальности, систему психического и, в конечном счете, на иррациональное поведение. Сформулированы рекомендации по профилактике виктимного поведения жертвы мошенников. Полученные данные могут быть использованы в психологическом консультировании, в сфере управления и прогнозирования рисков различных отраслей, в которых так или иначе представлено социальное мошенничество.

Ключевые слова: информационная безопасность, эмоциональная безопасность, социальная инженерия, манипуляция, манипулятивное воздействие, мошенники, кибермошенники, критическое мышление, когнитивные искажения, эмоциональная уязвимость, виктимность, жертва, доверчивость, доверие, институты власти.

Для цитирования:

Игнатова Е.С. Манипуляция эмоциональной безопасностью кибермошенниками с применением технологий социальной инженерии: case-study // Вестник Пермского университета. Философия. Психология. Социология. 2024. Вып. 3. С. 374–390. https://doi.org/10.17072/2078-7898/2024-3-374-390. EDN: UIDSUM

https://doi.org/10.17072/2078-7898/2024-3-374-390

Received: 01.08.2024
Accepted: 16.09.2024
Published: 03.10.2024

MANIPULATION OF EMOTIONAL SECURITY BY CYBERCRIMINALS USING SOCIAL ENGINEERING TECHNOLOGIES: A CASE STUDY

Ekaterina S. Ignatova

Perm State University (Perm)

In psychology, the pervasive social fraud is only becoming a matter of interest. The article looks at fraud from the perspective of manipulative influence on the mental state of a potential victim who «voluntarily» violates information security. The study raises the problem of the need to recognize the mechanism of fraudulent influence on a person and their behavior. The theoretical foundations of this problem are considered. The historical aspect of the application of social engineering technologies to obtain personal information and regulate human behavior is shown. The types of social fraud are described. The heterogeneity of fraudulent schemes is indicated. The factors of fraudulent influence that act as targets are presented, including empirically confirmed personal characteristics of potential and real victims, their thinking systems and basal emotional regulation. The role of cognitive distortions that reduce the effectiveness of critical thinking in an emotionally insecure state is shown. The stages of manipulative influence by fraudsters have been identified. A psychological analysis of a case of manipulative influence on emotional security by cybercriminals using social engineering technologies is described, with the results of a study into the victim's identity presented. The study has found correspondence between the personal characteristics of the subject and the empirical portrait of a fraudsters' victim in expressed indicators of benevolence, conscientiousness, anxiety, orientation to the value of security, conviction in the moral qualities of Another. The analysis of the victim's narrative made it possible: to describe the criminals' scenario within the range «situational tension – removal of psychological tension», when the victim is consistently deprived of key components of emotional security: calmness, confidence in the controllability of what is happening and the possibility of predicting the consequences; to establish the dynamics of the victim's emotional experience and its influence on the perception of reality, on the mental system and, ultimately, on irrational behavior. Recommendations for the prevention of victimized behavior of a victim of fraud are formulated. The data obtained can be used in psychological counseling, in the field of risk management and forecasting in various industries where social fraud is represented in one way or another.

Keywords: information security, emotional security, social engineering, manipulation, manipulative influence, scammers, cyber fraudsters, critical thinking, cognitive distortions, emotional vulnerability, victimization, victim, credulity, trust, institutions of power.

To cite:

Ignatova E.S. [Manipulation of emotional security by cybercriminals using social engineering technologies: a case study]. *Vestnik Permskogo universiteta. Filosofia. Psihologia. Sociologia* [Perm University Herald. Philosophy. Psychology. Sociology], 2024, issue 3, pp. 374–390 (in Russian), https://doi.org/10.17072/2078-7898/2024-3-374-390, EDN: UIDSUM

Постановка проблемы

В условиях цифрового общества пугающе увеличивается масштаб индустрии социального мошенничества за счет информационно-коммуникативных технологий [Рачева Н.В. и др., 2021; Романов В.Г., Романова И.В., 2020; Bidgoli M., Grossklags J., 2017; Богданов А.В. и др., 2020; Старостенко Н.И., 2020; Мешкова Н.В. и др., 2022; Зотина Е.В., 2023; Lu H.Y. et al., 2020; Габалова Е.Б., Тегетаева О.Р., 2021; Ананьина К.П., Изофатова Д.А., 2022], особенно в кредитно-финансовой сфере [Ананьина К.П., Изофатова Д.А., 2022; Asri F.M., Ма-

hamad T.E.T., 2023; Богданов А.В. и др., 2020; DeLiema M. et al., 2023; Шипулин Г.Ф., 2022].

Традиционно мошеннические схемы и результат их негативного влияния входят в область интересов представителей правовой сферы, которые изучают подготовительные действия (поиск потенциальной жертвы, создание условий совершения преступления), организацию провокации, обусловленную выбранным способом воздействия, сокрытие преступных действий [Кузьмин Ю.А., 2022; Романов В.Г., Романова И.В., 2020]. Вместе с тем этот негативный тренд имеет последствия не только в правовой, но в социально-психологической сфере. Эмпирически подтверждено отрицательное воздействие мошенничества на психологическое здоровье личности [Мешкова Н.В. и др., 2022; Eze O.J. et al., 2023; Ghani N.M. et al., 2023] независимо от пола, возраста образования [Романов В.Г., Романова И.В., 2020; Первушина О.Н., Федоров А.А., 2022; Богданов А.В. и др., 2020; Трахов А.И., Бешукова З.М., 2022; Шипулин Г.Ф., 2022], хотя выборка многих исследований состоит преимущественно из лиц пожилого возраста [Мешкова Н.В. и др., 2022; Ананьина К.П., Изофатова Д.А., 2022; Зотина Е.В., 2023; Asri F.M., Mahamad T.E.T., 2023].

Мошенничество являет собой преступную деятельность для достижения личной корыстной выгоды с использованием неблаговидных жульнических действий, в основе которых лежит обман/искажение истины. Данную форму хищения характеризует внешняя добровольность жертвы/потерпевшего, уверенного в правомерности действий мошенников. Кибермошенники выстраивают манипуляцию таким образом, чтобы потенциальная жертва, находясь в состоянии заблуждения или будучи обманутой, сама «добровольно» нарушила требования информационной безопасности: предоставила персональные данные, платежную информацию, данные для доступа и т.д. [Менщиков А.А., Федосенко М.Ю., 2021]. Поэтому сегодня потребность в безопасности можно рассматривать не только как личную безопасность, но и как безопасность данных о личности в условиях риска оказания психологического давления мошенниками [Заболоцкая А.В., Ткачева Е.Г., 2022].

В цифровом обществе такие преступления, как правило, имеют дистанционную форму и носят латентный характер, что осложняет их расследование и раскрываемость. Затруднения связаны, с одной стороны, с сокрытием факта мошенничества по разным причинам: не все потерпевшие социокультурно (репутационные риски, значительность ущерба), психологически (общественное мнение, чувство стыда и вины) готовы официально идентифицировать себя с жертвой, встретиться с последствиями произведенного обмана и, соответственно, заявить о факте мошенничества в правоохранительные органы. С другой стороны, не всегда есть возможность завести уголовное дело, т.к. определение места нахождения мошенников и проверка информации на достоверность проблематичны, следы преступления отсутствуют, пострадавший как будто по своей воле все выполнял, выступая одновременно потерпевшим и гражданский ответственным. Условное согласие жертвы действовать определенным образом, выполняя ошибочные поведенческие паттерны, и, как следствие, встречаться с негативными последствиями такого поведения могут усложнить правоохранительным органам возможность доказательства мошеннических действий и обеспечить безопасность личности, например, в финансовой среде.

Для профилактики обозначенных рисков используются следующие меры:

– повышение информационной и экономической безопасности организаций;

– просвещение населения по вопросам: финансовой грамотности [Габалова Е.Б., Тегетаева О.Р., 2021], информационной безопасности [Богданов и др., 2020] за счет социальной рекламы, создания рекомендаций [Lu H.Y. et al., 2020; Психологические аспекты противодействия…, 2024];

– развитие нормативно-правовой сферы профилактики виктимного поведения граждан в рамках предотвращения правонарушений, расширения судебно-следственной практики по делам о мошенничестве [Ананьина К.П., Изофатова Д.А., 2022; Богданов А.В. и др., 2020];

– создание центра борьбы с телефонным мошенничеством и киберпреступлениями [Шипулин Г.Ф., 2022].

Несмотря на социально-экономическую значимость, перечисленные мероприятия обладают рядом методологических ограничений:

– имеют односторонний характер воздействия: например, поднимается вопрос об экономической безопасности среды [Габалова Е.Б., Тегетаева О.Р., 2021], но не личности как участника коммуникации с такой средой;

– содержат системные институциональные противоречия: обнаруживается необходимость коллаборации различных институтов для борьбы с мошенничеством, что само по себе затруднительно ввиду слабой коллегиальности институциональных коммуникаций и отсутствия комплексного подхода к профилактике и коррекции последствий мошенничества [Старостенко Н.И., 2020];

– не учитывают кризисное состояние, в котором находится жертва мошенников, оставляя ее в одиночестве при разрешении сложившихся эмоциональных и финансовых проблем. При этом факт заблуждения жертвы часто не предопределяет юридическую ничтожность кредитно-финансовой сделки [Богданов А.В. и др., 2020]. Предложенные рекомендации, как правило, обращены к рациональному, когнитивно-ориентированному восприятию [Lu H.Y. et al., 2020]. Для закрепления правильного поведения взаимодействия с мошенниками данные рекомендации следует регулярно использовать в работе с разными категориями населения. Например, знакомить с ними школьников уже на уроках «Основы безопасности жизнедеятельности». Это связано с тем, что следовать инструкциям в состоянии эмоциональной уязвимости, испытывая сильные эмоции, практически невозможно, если только правила поведения с потенциальными мошенниками не «записаны на подкорку». При этом остается риск нарушения алгоритма действия в ситуации угрозы потери, наказания, привлечения к ответственности.

Для повышения осведомленности и обеспечения безопасности зарубежные исследователи апробировали алгоритм обучения поведению в ситуациях, имитирующих взаимодействие с мошенниками. В тренинговом формате отрабатываются навыки распознавания мошеннических звонков, анализа поступающей информации, выстраивания диалога [Yoshioka T. et al., 2024]. Однако для эффективного виктимологического предупреждения [Зотина Е.В., 2023], по нашему мнению, необходимо начинать работу не с когнитивной сферы, а с эмоциональной, т.к. эволюционно лимбическая система определяет работу префронтальной коры, где находится блок мозга, ответственный за принятие решений.

Итак, проблема распознавания кибермошенничества базируется на понимании механизма манипулятивного воздействия на личность, возможности его предвосхищения и пресечения на этапе принятия решения об удовлетворении требований злоумышленников.

Анализ литературы

Одним из условий воплощения мошеннических посягательств выступает формирование доверительных отношений между преступником(ами) и жертвой, которое невозможно без психологического манипулирования. Такая противоправная деятельность реализуется за счет технологий социальной инженерии.

Исторически социальная инженерия рассматривалась как целенаправленная профессиональная деятельность специалистов по общественному переустройству. К. Поппер научно обосновал социальную инженерию как молодую науку, отмечая применение социологических технологий для разрешения проблемы рационального изменения общества с целью прогноза последствий выполненных преобразований [Ламинина О.Г., 2017]. Контекстом использования обозначенных технологий традиционно (как в Древней Греции и Риме, так и в послевоенный период в США и Великобритании) выступала сфера управления государством, требующая реализации в т.ч. дипломатических задач, проектов спецслужб, когда возникала необходимость манипулировать человеческим сознанием. Данные коммуникативные технологии нацелены на получение определенной, как правило, персональной информации, регуляцию поведения личности. К сожалению, сегодня социальная инженерия представляет собой также современную форму мошенничества, предполагающую нарушение информационной безопасности [Старостенко Н.И., 2020; Pimentel A., Steinmetz K.F., 2022].

Анализ литературы позволяет выделить следующие виды социального мошенничества [Кузьмин Ю.А., 2022; Менщиков А.А., Фед-

осенко М.Ю., 2021; Шипулин Г.Ф., 2022; Button M. et al., 2024]:

– вишинг и спуфинг, когда в ходе телефонной коммуникации злоумышленники играют определенную роль, запуская ряд сценариев («ошибочный платеж», «реклама», «родственник в беде»; «звонок из службы безопасности организации» / «интерес со стороны представителя власти»), при этом нарушая ст. 159 УК РФ «Мошенничество» (злоупотреблении доверием), ст. 288 УК РФ «Присвоение полномочий должностного лица»;

– БМБ-фишинг, когда мошенники проигрывают сценарий, отправляя жертве текстовые сообщения через различные мессенджеры [Шипулин Г.Ф., 2022].

Мошеннические схемы различаются по степени сложности. Многие из них предполагают многоуровневую индивидуально-ориентированную обработку потенциальной жертвы с задействованием нескольких персоналий (сотрудники полиции, правоохранительных органов, банков, ФСБ и т.д.). Такой процесс невозможен без тщательной проработки, а также привлечения профессиональных психологов.

Местами реализации мошеннических действий, согласно судебно-следственной практики, выступают: исправительные учреждения, call-центры, которые могут находиться в т.ч. на территории указанных учреждений [Грязева Н.В., Некрасов А.П., 2020; Богданов А.В. и др., 2020].

Организация мошеннических схем требует помещения, материально-технического обеспечения и персонала, которому представляются скрипты для коммуникации с потенциальными жертвами [Менщиков А.А., Федосенко М.Ю., 2021].

Социальная инженерия в аспекте информационной и эмоциональной безопасности предполагает побуждение человека к определенным действиям вопреки его собственным интересам за счет обращения к базовым и эмоциональным потребностям [Wang J. et al., 2024]. Задействуется личностная система ценностей, для чего достаточно подробно составляется профайлинг жертвы [Менщиков А.А., Федосенко М.Ю., 2021]. «Уязвимыми мишенями» воздействия на систему мышления с последующим выполнением указаний выступают: возраст [Мешкова Н.В. и др., 2022], личностные особенности (выраженный нейротизм и, соответственно, сниженная эмоциональная устойчивость, доброжелательность, добросовестность, доверчивость и наивный оптимизм, преобладание ценности безопасности) [Сафуанов Ф.С., Докучаева Н.В., 2015; Первушина О.Н., Федоров А.А., 2022; Мешкова Н.В. и др., 2022; Maharjan A., 2023]. При этом важно обратить внимание на то, что уровень восприимчивости по-разному влияет на склонность личности участвовать в мошеннических схемах. По данным отечественных исследований, внушаемость предопределяет подверженность человека воздействию злоумышленников [Первушина О.Н., Федоров А.А., 2022]; по данным зарубежных исследований — не всегда [Button M. et al., 2024]. Дополнительную виктимогенную роль в стимулировании небезопасного стиля реагирования на провокации мошенников играют: низкая информационная и финансовая грамотность населения [Maharjan A., 2023], отсутствие у людей опыта противодействия дезадаптивному влиянию мошенников.

Традиционно эффективная манипуляция строится на обнаружении и последующем использовании человеческой слабости [Сидоренко Е.В., 2004], которая кроется в эмоциональной уязвимости личности. Для проведения атак злоумышленники, применяющие технологии социальной инженерии, зачастую эксплуатируют доверчивость, любезность, испытание страха и вины для повышения стрессогенности внешнего контекста за счет угроз. Отсутствие или малая представленность в жизненном опыте регламентации предлагаемых мошенниками сценарных взаимодействий предопределяет усиление ощущения незащищенности личности. «Выбивание почвы из-под ног» происходит за счет утраты ею контроля вследствие переживания растерянности и беспомощности.

В стрессовой виктимогенной ситуации, когда нарастает эмоциональное возбуждение, происходит снижение базальной эмоциональной саморегуляции. Данная динамика проявляется как на аффективном, так и на поведенческом уровнях, что негативно влияет в т.ч. на функциональность когнитивной сферы [Lu H.Y. et al., 2020]. Активизируются когнитивные ис-

кажения, которые способствуют понижению концентрации внимания и эффективности критического мышления [Ярославцева И.В., Дорохина С.А., 2016], усиливая размытость восприятия и нелогичность рассуждений. Такое состояние в условиях целенаправленного создания иллюзии принятия быстрого решения, выступающего дополнительным стресс-фактором, и оперативных действий снижает осознанность и произвольность, провоцируя иррациональные изменения в поведении, приводящие к драматическим последствиям.

Представим этапы мошеннической схемы, в структуру которой входит манипулятивное воздействие:

– поиск и получение информации о жертве (от номера телефона до биографических данных в зависимости от степени сложности схемы). Данный этап с одной стороны, показывает факт нарушения злоумышленниками 152-ФЗ «О персональных данных»; с другой стороны, подсвечивает необходимость формирования и развития информационной и финансовой грамотности в цифровой среде;

– психологическая атака с целью введения в заблуждение с помощью угроз, последующим переживанием страха, тревоги и даже паники [Старостенко Н.И., 2020]. Когда мошенники применяют манипулятивные скрипты, активизирующие эмоциональную уязвимость [Asri F.M., Mahamad T.E.T., 2023] снижается эмоциональная безопасность с сопутствующими потерями уверенности, стабильности, управляемости происходящим. Традиционно они «играют» на: страхе утраты («Ваш родственник попал в беду…»), финансовых страхах («У вас просроченный долг…»), страхе перед властью, законом и судом [Богданов А.В. и др., 2020; Зотина Е.В., 2023];

– формирование доверительных отношений с одновременным снижением бдительности за счет: эксплуатации «статуса», предоставления реальных персональных сведений, заверения в собственной социально-психологической компетентности обращения со сложными жизненными ситуациями, а также с помощью скорого оперирования сценарной информацией. Например, мошенники могут обращаться к алгоритмам, которыми потенциальная жертва может и не обладать ввиду отсутствия опыта. Привлечению жертвы к сотрудничеству способствуют такие манипулятивные скрипты, как: «Я могу помочь вам … решить эту проблему гораздо более простым способом. Все, что вам нужно сделать, это успокоиться и просто следовать моим инструкциям», «Давайте действовать вместе» [Parti K. et al., 2023];

– убеждение выполнить определенные действия за счет удержания человека в состоянии веры в реальность угрозы и достоверность разыгрываемого сценария. Посредством блокировки возможности проверки информации с использованием психологического давления происходит формирование чувства реальности происходящего [Старостенко Н.И., 2020];

– организация и контроль мошенниками иррационального поведения жертвы с сохранением у нее иллюзии важности совершающегося, эмоциональной зависимости от «добродетелей», когда жертва выполняет требуемые действия, находясь в состоянии даже какой-то степени безопасности, для благоволения (получения внимания и поддержки) «представителей власти» и их положительной реакции в проблемной ситуации [Психологические аспекты противодействия…, 2024];

– окончание взаимодействия с жертвой в связи с изъятием информации, финансовых средств [Богданов А.В. и др., 2020] и, возможно, участия в противоправном мероприятии.

Как мы видим, дестабилизирующими факторами манипулятивного воздействия выступают:

– информационно-психологические риски, являющиеся индикатором социального напряжения в следующих сферах: социально-экономической, политической, технологической, духовной [Белоусова Е.А., 2024];

– формирование у потенциальной жертвы заданной оценки воспринимаемой ситуации;

– снижение субъектности жертвы в ходе управления собой и ситуацией [Pimentel A., Steinmetz K.F., 2022].

Соответственно, у жертвы формируется эмоциональное переживание в диапазоне: ситуационная напряженность – разрешение ситуационной напряженности с последующим управлением [Pimentel A., Steinmetz K.F., 2022]. «Игра» мошенников начинается с побуждения потенциальной жертвы к переживанию страха за счет угроз и одновременного ее убеждения в законности коммуникации

[Asri F.M., Mahamad T.E.T., 2023]. Обращение к «законности» обусловлено сущностью авторитета побуждать с помощью различных технологий подражания, внушения, заражения за счет обращения к системе ценностей аудитории и ее самооценке. Одним из приемов обеспечения «законности» выступает демонстрация мошенниками информированности и влиятельности в ходе коммуникации с жертвой: оперирование точными биографическими данными самой жертвы и, возможно, членов ее семьи с последующим предложением алгоритма разрешения проблемы.

Методология исследования

Для изучения эмоционального опыта потерпевших от мошенников обычно используются качественные методы исследования (нарративы, глубинные интервью), т.к. применение личностных опросников затрудняет ретроспективные исследования [Bidgoli M., Grossklags J., 2017; Asri F.M., Mahamad T.E.T., 2023]. Традиционно case-study ассоциируется также с качественной методологией. Вместе с тем в современной социальной науке его методологический статус не однозначен. Case-study рассматривается и как комплексный исследовательский подход, и как технология сбора уникальных данных о социально-психологическом явлении, в т.ч. из приватной сферы [Михайлов А.С., 2014; Козина И.М., Сережкина Е.В., 2015]. Достоинства case-study одновременно выступают его ограничениями, т.к. данный метод позволяет подробно и глубоко изучить феномен на основе анализа небольшого числа, как правило, неслучайных данных. Использование аналитической стратегии интерпретации таких данных позволяет сделать некоторые обобщения о природе исследуемого феномена в определенном контексте [Aberdeen T., 2013].

Случай представляет собой специфическую единицу наблюдения за фрагментом социальной реальности. Является примером проявления определенного социального феномена [Козина И.М., Сережкина Е.В., 2015].

Целью настоящего исследования является анализ случая манипулятивного воздействия на эмоциональную безопасность кибермошенниками с применением технологий социальной инженерии.

Тип случая: развернутый. Акцент сделан на процессуальном аспекте, когда отслеживаются и описываются события, происходящие с определенным кругом лиц, участвующих в происходящем в течение длительного времени [Козина И.М., Сережкина Е.В., 2015].

Стратегия анализа случая: описательная с элементами объяснения [Aberdeen T., 2013].

Методологическими принципами анализа случая выступают: системный принцип, принцип личностного подхода и принцип развития.

Методы исследования: диагностика личностных особенностей; нарратив; анализ истории взаимодействия с мошенниками.

Результаты исследования

Анализ случая:

Лицо Н. женского пола, 38 лет. Является гражданином РФ. Имеет высшее социально-гуманитарное образование. Не замужем. Детей нет. Не зарегистрирована в качестве индивидуального предпринимателя. Работает в сфере образования.

Соматический статус: без явно выраженных патологий.

Медикаментозное лечение: не проводится.

Психическое состояние: переживание кризисного состояния. В беседе откровенна. Фон настроения: тревожный.

Согласие на участие в исследовании: предоставлено.

Для оценки личностной предрасположенности Н. к манипулятивному воздействию использовались психодиагностические методики, отобранные в ходе анализа литературы:

– Шкала удовлетворенности жизнью, SWLS — по E. Diener et al. (1985), в адаптации: Е.Н. Осина, Д.А. Леонтьева (2004);

– Короткий портретный опросник Большой пятерки, Б5-10 — М.С. Егорова, О.В. Паршикова (2016);

– Шкала межличностного доверия, ШСД — по J. Rotter (1967), в адаптации: И.Ю. Леоновой, И.Н. Леонова (2016);

– Тест «Внушаемость–конформность» — С.В. Клаучек, В.В. Деларю (1997);

– Портретный ценностный опросник, PVQ-RR — по S. Schwartz (2011), в адаптации: Т.П. Бутенко, Д.С. Седовой, А.С. Липатовой, (2012).

По результатам диагностики можно говорить о том, что Н. в целом удовлетворена жизнью; доброжелательна, сознательна, невротична; имеет средние показатели социального и институционального доверия, высокий уровень конформности. В ее системе ценностей преобладают: репутация, межличностная безопасность, традиции, ориентация на надежность и преданность при взаимодействии, понимание и принятие при построении отношений с Другими и миром. Как мы видим, полученный портрет в целом согласуется с имеющимися данными о личностных особенностях жертв мошенников [Сафуанов Ф.С., Докучаева Н.В., 2015; Первушина О.Н., Федоров А.А., 2022; Мешкова Н.В. и др., 2022; Maharjan A., 2023]. Виктимность Н. может быть предопределена ее общей просоциальностью, которая выражается в доброжелательности, лояльности к Другим, ориентации на сотрудничество, а также тревожностью.

Н. стала жертвой мошенников в рамках финансовой суггестии [Психологические аспекты противодействия…, 2024] в 2023 г. Предъявлены банковские требования о возврате денежных средств на сумму более 1 млн. руб. Все кредиты брала, пребывая в уверенности, что помогает полиции в ведении расследования и будет нести уголовную ответственность в случае отказа от этих действий. Другими словами, данная ситуация сложилась в результате действий мошенников, оказавших моральное давление на личность Н., создав иллюзию необходимости. Добровольного намерения брать кредиты не было; крупные покупки или деятельность, требующие инвестиций, не планировались.

Рассмотрим кейс реализации сложной многопозиционной мошеннической схемы, которая развернута во времени, имеет фейковую иерархическую ролевую структуру с задействованием вишинга, спуфинга и фишинга.

Мошенники позвонили на служебный стационарный телефон в рабочее время — осуществили вишинг. Звонок приняли на кафедре; после чего сразу методист забежал на учебное занятие и взволнованно сообщил, что звонят из полиции и просят немедленно подойти к телефону. Услышав это, Н. испытала беспокойство, подумав, что звонок может быть связан с кем-то из студентов или коллег, что кто-то из них попал в беду. Сила беспокойства обусловлена высоким уровнем нейротизма личности Н. Как следует из данных, еще до разговора сформирована иллюзия важности за счет эффекта обращения к авторитетам [Психологические аспекты противодействия…, 2024].

Телефонный звонок запустил «игру». Н. проследовала к телефону. Звонивший представился сотрудником МВД г. Москвы (спуфинг), уточнил фамилию, имя и отчество Н. Далее он спросил, знает ли Н. некоего человека, имеющего сходные фамилию и отчество. Н. впервые слышала это имя и, соответственно, ответила, что нет. Звонивший сообщил, что указанный человек в настоящее время обращается в разные кредитные учреждения г. Москвы с поддельной доверенностью и берет кредиты на ее имя. Данная информация повергла Н. в шок: другой город, нарушение закона, уголовная ответственность, жуткие последствия — перед глазами проносились страшные картинки социального отвержения. Стала резонансной ценность репутации. Итак, на лицо построение ландшафтного дизайна сценария и создания иллюзии эмоциональной небезопасности за счет отсутствия контроля за происходящим [Психологические аспекты противодействия…, 2024]. Н. ощущает страх и отчаяние; думает, что теперь должна деньги, и поскольку доверенность оформлена на ее имя, у нее нет никаких доказательств непричастности. Созданы условия для идентификации Н. с фигурантом уголовного дела, риском нести финансовую и уголовную ответственность за действия Другого [Мешкова Н.В. и др., 2022] и ожиданием последующего предъявления обвинения, процедурным знанием которого Н. не владеет. Последовательная манипуляция эмоциональным возбуждением Н. делает ее эмоционально уязвимой и готовой к коммуникации. На первое место выходит страх оказаться правонарушителем.

На следующем этапе, продолжая поддерживать все уже созданные иллюзии и обращаясь к указанным выше эффектам, «сотрудник правоохранительных органов» манипулирует гражданской ответственностью Н. следующим сообщением: по данному факту проводится предварительное расследование, и, если она, действительно, не является сообщником описанного лица, должна помочь его поймать и

призвать к ответу, наказать. Будучи сознательной и имеющей ценности репутации, межличностной безопасности и ориентации на надежность, в этот момент Н. испытала огромную благодарность за то, что он ей доверяет и не обвиняет, не разобравшись. На фоне иллюзии единства Н. выражает полную готовность помочь следствию и тем самым снять с себя все подозрения. Мошенники приступили к созданию доверительных отношений. Соответственно, возникает необходимость изолировать Н. и минимизировать саму возможность противостояния влиянию со стороны жертвы [Button M. et al., 2024; Parti K. et al., 2023].

Со ссылкой на режим секретности и апеллированием к государственной власти поступает приказ удалить посторонних из помещения для продолжения разговора. В течение следующих 40 минут в ходе продолжения разговора наедине происходит когнитивная обработка эмоционально уязвленной Н. Имея высокий уровень сознательности и на фоне повышенной невротичности, жертва «добровольно» искренне дает ответы на заданные вопросы о:

– состоянии здоровья (ведь «родственник», беря кредиты по поддельной доверенности в банках г. Москвы, объяснял отсутствие Н. недомоганием);

– причинах того, каким образом подпись Н. могла оказаться у «родственника» (подпись могла оказаться в Интернете в открытом доступе в период пандемии, когда с применением ИКТ-технологий происходило подписание документов через вставку фото подписи).

Н. «послушно» выполняет требования привести прямые доказательства непричастности к данной доверенности, пытаясь найти аргументы. Следует обратить внимание на то, что во время разговора «сотрудник правоохранительных органов» искусно балансирует между акцентированием на угрозе безопасности Н. и демонстрацией понимания, оказания поддержки. Наконец, он «приходит к выводу», что Н. не является соучастницей описанного преступления. Становится резонансной ее ценность межличностной безопасности. У жертвы складывается портрет немногословного, логичного, радеющего за дело специалиста, производящего впечатление профессионального и неравнодушного человека. На этом коммуникация с ним заканчивается. Напоследок для закрепления эффекта авторитета используется эффект подтверждения: мошенник диктует номер мнимого служебного удостоверения. Н., будучи незнакомой с действительной номенклатурой, пребывает в уверенности важности и реальности происходящего.

Далее на фоне достигнутого «сотрудничества» формулируется задача совместными усилиями разоблачить мошенническую группировку («родственник» – нотариус – сотрудник банка), без организованной деятельности которой взятие кредитов по поддельной доверенности «невозможно». Изначально представленная легенда преобразуется. Перед Н. ставится задача следовать указаниям мошенника. Это связано с тем, что на этапе манипуляции поведением Н. важно, удерживая жертву в эмоциональной зависимости, заставить ее выполнять инструкции для достижения цели.

Происходит смена ролей — в коммуникацию (без прерывания телефонного разговора) вступает «представитель Центрального банка РФ (ЦБ РФ)». При этом Н. не сомневалась в том, что в современных условиях цифрового общества возможно такое оперативное подключение работника из другой сферы — кредитно-финансовой. Для закрепления сложившегося впечатления сотрудник повторил уже сказанное «коллегой» из правоохранительных органов и назначил ведущего специалиста для оказания персональной помощи и постоянного сопровождения через чат в Telegram — фишинг. Далее «представитель» сказал, что Н. нужно взять паспорт и следовать дальнейшим инструкциям. Н. ответила, что паспорта у нее с собой нет. Тогда, ссылаясь на срочность и важность дела, он велел ей сходить домой за паспортом, особо отметив, что она не имеет права сообщать кому бы то ни было о «деле», поскольку оно имеет общественно-государственную значимость и подпадает под статью 310 УК РФ о конфиденциальности. В качестве подтверждения высылается мнимый документ «о неразглашении», оформленный якобы в ЦБ РФ. Итак, искаженная реальность сформирована, жертва изолирована и готова действовать.

Ведущий специалист «вел» Н. в течение трех дней с 08.00 до 20.00 посредством постоянного нахождения на связи: звонков и пере-

писки в Telegram. Каждый раз он сообщал о том, что обнаружена очередная заявка на кредит, в которой Н. фигурирует как заемщик, а «родственник» — как получатель (его мнимая фотография, якобы обнаруженная с помощью камеры одного из банкомата, была отправлена Н. для подтверждения реальности ведущейся оперативно-розыскной деятельности). В качестве подтверждения Н. высылалась копия каждой кредитной заявки. Далее ведущий специалист давал Н. инструкцию: идти в банк и подавать «дублетную» заявку с целью аннулирования уже оформленной мнимым родственником. При этом Н. должна была внимательно следить за действиями сотрудников банка и незамедлительно сообщать ведущему специалисту о фактах отказа в кредитах, поскольку это якобы являлось признаком сговора банка с преступной группировкой, которую необходимо разоблачить. Признаки такого «сговора» обнаружились в ряде банков, которые отказали Н. в выдаче денежных средств.

Н., находясь в полном одиночестве, уже автоматически выполняла действия согласно предложенному мошенниками алгоритму. Во всех банках Н. общалась с операционистами. По указанию ведущего специалиста деньги просила выдавать наличными, сохраняя расходный кассовый ордер. Затем Н. шла в строго определенный банкомат и переводила деньги по указанным реквизитам — якобы в ЦБ РФ на «безопасный счет», сохраняя чеки и отправляя «куратору» копии. Мошенникам удалось убедить Н. в том, что перевод денег является гарантией ее безопасности. Каждый раз после такого перевода Н. получала копию справки с печатью ЦБ РФ, подтверждающей, что кредит погашен, и банку она ничего не должна. Стараясь все сделать правильно, Н. четко следовала всем инструкциям и искренне пыталась помочь следствию и самой себе. Напирая на безотлагательность и срочность, мошенник говорил, что действовать надо максимально быстро, и что ЦБ РФ гарантирует Н. безопасность только при условии соблюдения полной секретности и четкого следования его указаниям. Во время визитов в банки он требовал все время держать телефон включенным, слушал, давал инструкции, демонстрируя знания в области финансов.

Спустя некоторое время ситуацию стал параллельно контролировать еще один человек, представившийся майором юстиции, следователем. Разговоры с ним отличались обилием правоохранительной лексики.

На третий день в силу объективного психофизиологического истощения эмоциональное возбуждение Н. стало спадать. Ставший уже знакомым порядок действий не способствовал разрешению проблемы. На фоне продолжающейся неопределенности естественным образом накапливалась усталость. У Н. стали появляться вопросы. В ситуации опасного вызова активизировались потребности в осмыслении и рефлексии для объяснения происходящего и завершения напряженного кейса. Прежде всего, ей хотелось узнать, когда наступит финальная стадия предварительного расследования и невиновность Н. будет окончательно подтверждена. Ей отвечали, что пока продолжают поступать заявки на кредит, о прекращении оперативных действий не может быть и речи.

Утром четвертого дня подозрения Н. о ненормальности происходящего переросли в уверенность, и она решила обо всем рассказать отцу. Он настоял на подаче заявления в полицию, что Н. и сделала в тот же день. В полиции было заведено уголовное дело по факту мошенничества в особо крупных размерах.

Тем временем, мошенники продолжали звонить и запугивать Н. тем, что лишат ее гарантий безопасности, а также «аннулируют» и «заблокируют» счета. Несмотря на более критическое понимание происходящего, которое сформировалось у Н. к тому моменту, эти угрозы производили на нее сильное впечатление, и она начинала сомневаться в правильности своих действий. Преследование звонками и сообщениями продолжалось еще в течение 10 дней. Возможно, мошенники надеялись, вновь обрушив эмоциональную безопасность Н., завершить сценарий, т.к. она из него незапланированно «вышла».

В настоящее время аккаунт ведущего специалиста в Telegram имеет название «Удаленный аккаунт» (статус — «был давно»), аккаунт его «руководителя» — «АН» (статус — «был недавно»); аккаунт «майора юстиции» существует под тем же именем (статус — «был недавно»).

Следует отметить, что финансовые организации в течение трех дней выдавали кредиты на большие суммы без анализа кредитного потенциала и актуальной кредитной истории Н., которая до этого случая была чиста. По описанному факту мошенничества заведено уголовное дело, в котором Н. присвоен статус потерпевшей.

Обсуждение результатов

Находясь в панике, Н. объясняла происходящее искаженно — единственным представленным мошенниками образом и послушно следовала указаниям третьих лиц, передвигаясь по созданной «потемкинской деревне» (как называет манипуляцию Е.В. Сидоренко [Сидоренко Е.В., 2004]) нарушая собственную информационную и эмоциональную безопасность. Когнитивная обработка информации в тензионном состоянии, особенно у личности с высоким уровнем нейротизма, минимизирована: амигдала работает вне сознания человека, запуская в ситуации опасности эмоциональную реакцию на раздражитель в 10 раз быстрее, нежели происходит обработка информации в кортексе. Сильные нейрофизиологические импульсы, эмоциональная напряженность, поддерживаемые постоянной стрессогенной коммуникацией и принуждению быстро принимать решения, препятствовали осознанности и критичности Н.

Манипулируя выраженными доверчивостью и сознательностью личности Н., мошенники навязали Н. алгоритм действий [Atkins B., Huang W., 2013]: произвели эмоциональную атаку с последующей десубъективизацией и эксплуатацией за счет апеллирования к ценностям репутации, межличностной безопасности, ориентации на надежность. Ее поведение регулировали за счет предоставления дозированной информации, последовательного применения положительных и отрицательных форм подкрепления, авторитетных и настойчивых убеждений [Atkins B., Huang W., 2013]. Как результат — смоделированы перцептивные и когнитивные искажения, обусловленные стереотипами восприятия институтов власти, социальными и эмоциональными причинами, в т.ч. индивидуальными психоэмоциональными факторами личности Н., нанесен информационно-психологический вред качеству ее жизни [Заболоцкая А.В., Ткачева Е.Г., 2022].

Ограничениями данного исследования выступают: 1) представление единственного случая для анализа; 2) отсутствие в жанре case-study общепринятой структуры предъявления данных; 3) малая представленность психологического аспекта в статьях по проблеме социального мошенничества.

Заключение

Таким образом, на основании проведенного исследования можно сделать следующие основные выводы:

1. Современное социальное мошенничество включает в себя проигрывание определенных сценариев (спуфинг) в ходе коммуникаций по телефону (вишинг), а также через отправку текстовых сообщений в различных мессенджерах (БМБ-мобинг). Дифференцируется по степени сложности подготовки и реализации. Негативно влияет на психологическое здоровье личности.

2. Применение технологий социальной инженерии требует составления профайлинга жертвы, который предусматривает учет не только возраста, но и личностных особенностей (выраженные нейротизм, доброжелательность, добросовестность, наивный оптимизм), систему ценностей личности (преобладание ценности безопасности). При этом роль внушаемости личности в ее виктимной склонности не определена.

3. Механизм манипулятивного воздействия состоит в обращении к стрессогенным факторам, которые усиливают эмоциональное возбуждение, формируют ощущение незащищенности и беспомощности, способствуют утрате контроля, снижению критичности и выбору дезадаптивного поведения за счет нахождения в иллюзии принятия быстрого решения. Ключевой мишенью манипулятивного воздействия кибермошенников является информационная безопасность, которая в ситуации психологического давления напрямую связана с личной безопасностью, затрагивает психоэмоциональные факторы, к которым в т.ч. относятся страх утраты, финансовые страхи, страх перед институтами власти.

4. Этапы мошеннической схемы предполагают:

а) информационную подготовку к коммуникации с потенциальной жертвой;

б) психологическую атаку с использованием манипулятивных скриптов для снижения эмоциональной безопасности;

в) формирование доверительных отношений путем эксплуатации «статуса», предоставления гарантий поддержки и помощи;

г) убеждение выполнить определенные действия и последующий контроль требуемых действий;

д) достижение цели и завершение коммуникаций с жертвой.

5. Феноменология поведения жертвы мошенников, злоупотребивших ее доверием, может быть описана с помощью case-study. Выявлена личностная предрасположенность жертвы к виктимному поведению. Повышенная невротичность и страх оказаться правонарушителем способствуют включению в «игру»: создаются условия для формирования иллюзии важности и действенности эффекта авторитета. Трехдневная коммуникация с мошенниками становится возможной из-за сознательности и добросовестности личности жертвы, ее ориентации на ценности репутации и межличностной безопасности, которые даже в ходе сильного эмоционального переживания, обусловленного высоким уровнем нейротизма, предопределяют виктимное поведение.

Манипуляция эмоциональной безопасностью жертвы с помощью создания иллюзии разрешения проблемы и поддержки может привести к финансовым потерям и способствовать последующему переживанию кризисного состояния.

Обращаем внимание на то, что задачи осуществлять экономический либо криминологический анализы произошедшего поставлено не было. Фокус внимания сосредоточен на том, каким образом произошла виктимизация Н., когда мошенники использовали в основном иллюзии важности, необходимости, срочности с преобладанием эмоциональной зависимости, эффекты авторитета и подтверждения, играя на потребности в безопасности и артикулируя ее ценностью.

Вышеуказанные выводы позволяют сформулировать следующие рекомендации по профилактике виктимного поведения жертвы мошенников:

1. Сформировать намерение в ходе принятия решения ориентироваться на ценности информационной и личностной безопасности, а также на принципы прагматизма, отвечая на вопрос: «Зачем я это делаю в этих условиях?»

2. В ситуации опасного вызова помнить о необходимости осмысления и рефлексии угрожающей информации, которые требуют стабилизации эмоционального напряжения, паузы и доверительной коммуникации с проверенным Другим.

3. Находясь в состоянии эмоциональной уязвимости, сфокусировать внимание на саморегуляции, а не на предлагаемой помощи посторонними.

4. Важно осваивать технологии психологической самопомощи, развивать осознанность и тренировать толерантность к дистрессу, в т.ч. в ходе манипулятивного воздействия.

5. Осуществить диагностику собственной личностной предрасположенности к виктимному поведению. Это можно сделать самостоятельно, но для более четкой и точной интерпретации психодиагностической информации необходимо обратиться к специалисту, с которым в целях выработки адекватного стиля реагирования на провокации можно составить концептуализацию проблемных аспектов психического, провести прикладной анализ поведения и разработать индивидуальные правила сохранения эмоциональной безопасности.

Полученные результаты способствуют расширению представлений об особенностях управления мошенниками личностью, способах достижения их личной выгоды в условиях формирования иллюзии у жертвы безальтернативной ситуации. С целью противодействия социальному мошенничеству, профилактики виктимного поведения становится значимым, помимо финансового и информационного просвещения, формировать у населения намерение осознавать систему отношений к себе, миру и Другому, ориентироваться на сопротивление деструктивному воздействию, поддерживать безопасные границы, развивать эмоциональную устойчивость и критичность за счет сдерживания рисков. Дальнейшие исследования в данном направлении призваны выделить

эмоциональные и поведенческие маркеры, которые позволят своевременно провести дифференциальную диагностику психического состояния и активности жертвы мошенников, уточнить прогноз социальных последствий для частной и общественной жизни, разработать и апробировать протокол по работе с эмоциональной безопасностью жертв социальных мошенников.

Благодарность

Автор выражает благодарность канд. психол. наук, доценту, доценту кафедры общей и клинической психологии ПГНИУ М.В. Балевой за ценные советы и рекомендации при описании случая.

Gratitude

The author expresses her sincere gratitude to Milena V. Baleva – Candidate of Psychology, Docent, Associate Professor of the Department of General and Clinical Psychology of Perm State University for her valuable advice and guidelines while describing the case.

Список литературы

Ананьина К.П., Изофатова Д.А. Актуальные вопросы профилактики телефонного мошенничества // Закон и общество: история, проблемы, перспективы: материалы XXVI Межвуз. междунар. науч.-практ. конф. студентов и аспирантов, посвящ. 70-летию Красноярского ГАУ (Красноярск, 21–22 апреля 2022 г.) / отв. ред. Е.А. Ерахтина и др. Красноярск: Изд-во Краснояр. гос. аграр. ун-та, 2022. С. 217–219.

Белоусова Е.А. Факторы информационно-психологического воздействия на личность в условиях цифрового развития общества // Вестник науки. 2024. Т. 4, № 5(74). С. 436–441.

Богданов А.В., Ильинский И.И., Хазов Е.Н. Киберпреступность и дистанционное мошенничество как одна из угроз современному обществу // Криминологический журнал. 2020. № 1. С. 15–20.

Габалова Е.Б., Тегетаева О.Р. Телефонные мошенничества: угроза для развития бизнеса // Modern Science. 2021. № 2–1. С. 128–130.

Грязева Н.В., Некрасов А.П. Актуальные способы совершения мошенничеств с использованием средств сотовой связи в учреждениях уголовно-исполнительной системы // Вестник Самарского юридического института. 2020. № 4(40). С. 33–42. DOI: https://doi.org/10.37523/sui.2020.40.4.005

Заболоцкая А.В., Ткачева Е.Г. Психологическая безопасность личности в Интернете // Автономия личности. 2022. № 1(27). С. 91–97.

Зотина Е.В. Предупреждение телефонного мошенничества в отношении граждан пожилого возраста // Ученые записки Казанского юридического института МВД России. 2023. Т. 8, № 2(16). С. 19–25.

Козина И.М., Сережкина Е.В. Концепция кейс-стади в социальных науках и французская традиция монографических исследований трудовых организаций // Социологические исследования. 2015. № 1. С. 64–73.

Кузьмин Ю.А. Предупреждение телефонного мошенничества (криминологический аспект) // Oeconomia et Jus. 2022. № 3. С. 47–54. DOI: https://doi.org/10.47026/2499-9636-2022-3-47-54

Ламинина О.Г. Возможности социальной инженерии в информационных технологиях // Гуманитарные, социально-экономические и общественные науки. 2017. № 2. С. 21–23.

Менщиков А.А., Федосенко М.Ю. Возможности применения методов социальной инженерии в организации телефонного мошенничества // Экономика и качество систем связи. 2021. № 4(22). С. 36–47.

Мешкова Н.В., Кудрявцев В.Т., Ениколопов С.Н. К психологическому портрету жертв телефонного мошенничества // Вестник Московского университета. Серия 14: Психология. 2022. № 1. С. 138–157. DOI: https://doi.org/10.11621/vsp.2022.01.06

Михайлов А.С. Кейс-стади — исследовательская стратегия или мета-метод? // Экономика и социум. 2014. № 3–2(12). С. 543–551.

Первушина О.Н., Федоров А.А. Личностные особенности жертв телефонного мошенничества // Вопросы психологии. 2022. Т. 68, № 3. С. 92–103.

Психологические аспекты противодействия телефонному мошенничеству в финансовой сфере: метод. материалы / авт.-сост.: С.П. Баранцев, О.В. Медяник, Н.А. Низовских, О.А. Николаева / Упр. МВД РФ по Кировской области. Киров, 2024. 60 с.

Рачева Н.В., Балеевских Ф.В., Котов В.В. Современные способы совершения мошенничества в отношении имущества физических лиц с использованием интернет-ресурсов и технологий социальной инженерии // Юридическая наука. 2021. № 2. С. 101–105.

Романов В.Г., Романова И.В. Социальное мошенничество «Covid-19» и манипулятивные технологии социальной инженерии // Вестник

Забайкальского государственного университета. 2020. Т. 26, № 9. С. 57–67. DOI: https://doi.org/10.21209/2227-9245-2020-26-9-57-67

Сафуанов Ф.С., Докучаева Н.В. Особенности личности жертв противоправных посягательств в Интернете // Психология и право. 2015. Т. 5, № 4. С. 80–93. DOI: https://doi.org/10.17759/psylaw.2015050407

Сидоренко Е.В. Тренинг влияния и противостояния влиянию. СПб.: Речь, 2004. 256 с.

Старостенко Н.И. Криминалистический аспект техник социальной инженерии при совершении преступлений // Вестник Краснодарского университета МВД России. 2020. № 1(47). С. 80–83.

Трахов А.И., Бешукова З.М. Предупреждение телефонного мошенничества: российский и зарубежный опыт // Цифровые технологии и право: сб. науч. тр. I Междунар. науч.-практ. конф. (Казань, 23 сентября 2022 г.): в 6 т. / под ред. И.Р. Бегишева и др. Казань: Познание, 2022. Т. 6. С. 357–361.

Шипулин Г.Ф. Способы совершения мошенничества, связанные с использованием мобильной связи // Международный журнал гуманитарных и естественных наук. 2022. № 2–2(65). С. 186–189. DOI: https://doi.org/10.24412/2500-1000-2022-2-2-186-189

Ярославцева И.В., Дорохина С.А. Критическое мышление пожилых людей — жертв мошеннических действий: теоретический и прикладной аспекты исследования // Известия Иркутского государственного университета. Серия: Психология. 2016. Т. 15. С. 60–71.

Aberdeen T. Yin, R.K. (2009). Case study research: Design and methods (4th ed.). Thousand Oaks, CA: Sage // The Canadian Journal of Action Research. 2013. Vol. 14, no. 1. P. 69–71. DOI: https://doi.org/10.33524/cjar.v14i1.73

Asri F.M., Mahamad T.E.T. Anatomy of Phone Scams: Victims' Recall on the Communication Phrases used by Phone Scammers // Proceedings of the International Conference on Communication and Media 2022 (i-COME 2022). Paris: Atlantis Press, 2023. P. 498–509. DOI: https://doi.org/10.2991/978-2-38476-098-5_43

Atkins B., Huang W. A study of social engineering in online frauds // Open Journal of Social Sciences. 2013. Vol. 1, no. 3. P. 23–32. DOI: https://doi.org/10.4236/jss.2013.13004

Bidgoli M., Grossklags J. «Hello. This is the IRS calling»: A case study on scams, extortion, impersonation, and phone spoofing // 2017 APWG Symposium on Electronic Crime Research (eCrime) (Phoenix, AZ, Apr. 25–27, 2017). Phoenix, AZ: IEEE, 2017. P. 57–69. DOI: https://doi.org/10.1109/ecrime.2017.7945055

Button M., Shepherd D., Hawkins C., Tapley J. Fear and phoning: Telephones, fraud, and older adults in the UK // International Review of Victimology. 2024. URL: https://journals.sagepub.com/doi/epub/10.1177/02697580241254399 (accessed: 21.07.2024). DOI: https://doi.org/10.1177/02697580241254399

DeLiema M., Li Y., Mottola G. Correlates of responding to and becoming victimized by fraud: Examining risk factors by scam type // International Journal of Consumer Studies. 2023. Vol. 47, iss. 3. P. 1042–1059. DOI: https://doi.org/10.1111/ijcs.12886

Eze O.J., Okpa J.T., Onyejegbu Ch.D., Ajah B.O. Cybercrime: victims' shock absorption mechanisms // Malware: Detection and Defense / ed. by E. Babulak. London: IntechOpen, 2023. P. 3–14. DOI: https://doi.org/10.5772/intechopen.106818

Ghani N.M., Bakar M.A.A., Rosli H. Cybercrime experience's impact on women's emotions: a case study in Penang // Malaysian Journal of Tropical Geography (MJTG). 2023. Vol. 49, no. 2. P. 48–67.

Lu H.Y., Chan S., Chai Wh., Lau S.M., Khader M. Examining the influence of emotional arousal and scam preventive messaging on susceptibility to scams // Crime Prevention and Community Safety. 2020. Vol. 22, iss. 4. P. 313–330. DOI: https://doi.org/10.1057/s41300-020-00098-3

Maharjan A.A. Study of Scams and Frauds using Social Engineering in «The Kathmandu Valley» of Nepal: Master of Science in Technology Thesis / University of Turku. 2023, 69 p.

Parti K., Tahir F. «If We Don't Listen to Them, We Make Them Lose More than Money»: Exploring Reasons for Underreporting and the Needs of Older Scam Victims // Social Sciences. 2023. Vol. 12, iss. 5. URL: https://www.mdpi.com/2076-0760/12/5/264/pdf?version=1683172510 (accessed: 21.07.2024). DOI: https://doi.org/10.3390/socsci12050264

Pimentel A., Steinmetz K.F. Enacting social engineering: the emotional experience of information security deception // Crime, Law and Social Change. 2022. Vol. 77, iss. 3. P. 341–361. DOI: https://doi.org/10.1007/s10611-021-09993-8

Wang J., Zhang L., Xu L., Qian X. The dynamic emotional experience of online fraud victims during the process of being defrauded: A text-based analysis // Journal of Criminal Justice. 2024. Vol. 94.

URL: https://www.sciencedirect.com/science/article/abs/pii/S0047235224000801 (accessed: 21.07.2024). DOI: https://doi.org/10.1016/j.jcrimjus.2024.102231

Yoshioka T., Awai S., Ide K., Chikano M., Iwasaki S., Yoshino K., Konno T. Demo: Preventing Phone Fraud by Victim Training Using Personalized Feedback for Behavioral Change // MOBISYS '24: Proceedings of the 22nd Annual International Conference on Mobile Systems, Applications and Services. N.Y.: Association for Computing Machinery, 2024. P. 588–589. DOI: https://doi.org/10.1145/3643832.3661833

References

Aberdeen, T. (2013). Yin, R.K. (2009). Case study research: Design and methods (4th ed.). Thousand Oaks, CA: Sage. *The Canadian Journal of Action Research*. Vol. 14, no. 1, pp. 69–71. DOI: https://doi.org/10.33524/cjar.v14i1.73

Anan'ina, K.P. and Izofatova, D.A. (2022). [Topical issues of telephone fraud prevention]. *Zakon i obschestvo: istoriya, problemy, perspektivy: materialy XXVI Mezhvuzovskoy mezhdunarodnoy nauchno-prakticheskoy konferentsii studentov i aspirantov, posvyaschennoy 70-letiyu Krasnoyarskogo GAU (Krasnoyarsk, 21–22 aprelya 2022 g.)* [Law and Society: History, Problems, Prospects: Proceedings of the 26th Interuniversity International Scientific and Practical Conference of students and postgraduates dedicated to the 70th anniversary of the Krasnoyarsk State Agrarian University (Krasnoyarsk, Apr. 21–22, 2022)]. Krasnoyarsk: KGAU Publ., pp. 217–219.

Asri, F.M. and Mahamad, T.E.T. (2023). Anatomy of phone scams: Victims' recall on the communication phrases used by Phone Scammers. *Proceedings of the International Conference on Communication and Media 2022 (i-COME 2022)*. Paris: Atlantis Press, pp. 498–509. DOI: https://doi.org/10.2991/978-2-38476-098-5_43

Atkins, B. and Huang, W. (2013). A study of social engineering in online frauds. *Open Journal of Social Sciences*. Vol. 1, no. 3, p. 23–32. DOI: https://doi.org/10.4236/jss.2013.13004

Barantsev, S.P., Medyanik, O.V., Nizovskikh, N.A. abd Nikolaeva, O.A. (eds.) (2024). *Psikhologicheskie aspekty protivodeystviya telefonnomu moshennichestvu v finansovoy sfere: metodicheskie materialy* [Psychological aspects of countering telephone fraud in the financial sphere: methodological materials]. Dep. of the Ministry of Internal Affairs of the RF for the Kirov Region. Kirov, 60 p.

Belousova, E.A. (2024). [Factors of information and psychological impact on personality in the context of digital development of society]. *Vestnik nauki* [Bulletin of Science]. Vol. 4, no. 5(74), pp. 436–441.

Bidgoli, M. and Grossklags, J. (2017). «Hello. This is the IRS calling»: A case study on scams, extortion, impersonation, and phone spoofing. *2017 APWG Symposium on Electronic Crime Research (eCrime) (Phoenix, AZ, Apr. 25–27, 2017).* Phoenix, AZ: IEEE Publ., pp. 57–69. DOI: https://doi.org/10.1109/ecrime.2017.7945055

Bogdanov, A.V., Il'inskiy, I.I. and Khazov, E.N. (2020). [Cybercrime and remote fraud as one of the threats to modern society]. *Kriminologicheskiy zhurnal* [Criminological Journal]. No. 1, pp. 15–20.

Button, M., Shepherd, D., Hawkins, C. and Tapley, J. (2024). Fear and phoning: Telephones, fraud, and older adults in the UK. *International Review of Victimology*. Available at: https://journals.sagepub.com/doi/epub/10.1177/02697580241254399 (accessed 21.07.2024). DOI: https://doi.org/10.1177/02697580241254399

DeLiema, M., Li, Y. and Mottola, G. (2023). Correlates of responding to and becoming victimized by fraud: Examining risk factors by scam type. *International Journal of Consumer Studies*. Vol. 47, iss. 3, pp. 1042–1059. DOI: https://doi.org/10.1111/ijcs.12886

Eze, O.J., Okpa, J.T., Onyejegbu, Ch.D. and Ajah, B.O. (2023). *Cybercrime: victims' shock absorption mechanisms*. *E. Babulak (ed.) Malware: Detection and Defense*. London: IntechOpen Publ., pp. 3–14. DOI: https://doi.org/10.5772/intechopen.106818

Gabalova, E.B. and Tegetaeva, O.R. (2021). [Telephone fraud: a threat to business development]. *Modern Science.* No. 2–1, pp. 128–130.

Ghani, N.M., Bakar, M.A.A. and Rosli, H. (2023). Cybercrime experience's impact on women's emotions: a case study in Penang. *Malaysian Journal of Tropical Geography (MJTG)*. Vol. 49, no. 2, pp. 48–67.

Gryazeva, N.V. and Nekrasov, A.P. (2020). [Actual ways to improve fraud using cellular communications in institutions of the penal system]. *Vestnik Samarskogo yuridicheskogo instituta* [Bulletin of the Samara Law Institute]. No. 4(40), pp. 33–42. DOI: https://doi.org/10.37523/sui.2020.40.4.005

Kozina, I.M. and Tserezhkina, E.V. (2015). [The concept of a case study in the social sciences and the French tradition of monographic research of labor organizations]. *Sotsiologicheskie issledovaniya* [Sociological Research]. No. 1, pp. 64–73.

Kuz'min, Yu.A. (2022). [Prevention of telephone fraud (criminological aspect)]. *Oeconomia et Jus* [Economics and Law]. No. 3, pp. 47–54. DOI: https://doi.org/10.47026/2499-9636-2022-3-47-54

Laminina, O.G. (2017). [Possibilities of social engineering in information technologies]. *Gumanitarnye, sotsial'no-ekonomicheskie i obschestvennye nauki* [Humanities, Socio-Economic and Social Sciences]. No. 2, pp. 21–23.

Lu, H.Y., Chan, S., Chai, Wh., Lau, S.M. and Khader, M. (2020). Examining the influence of emotional arousal and scam preventive messaging on susceptibility to scams. *Crime Prevention and Community Safety*. Vol. 22, iss. 4, pp. 313–330. DOI: https://doi.org/10.1057/s41300-020-00098-3

Maharjan, A. (2023). *A study of scams and frauds using social engineering in «The Kathmandu valley» of Nepal: Master of Science in Technology Thesis*. University of Turku, 69 p.

Menschikov, A.A. and Fedosenko, M.Yu. (2021). [The possibilities of using social engineering methods in the organization of telephone fraud]. *Ekonomika i kachestvo sistem svyazi* [Economics and Quality of Communication Systems]. No. 4(22), pp. 36–47.

Meshkova, N.V., Kudryavtsev, V.T. and Enikolopov, S.N. (2022). [On the psychological portrait of a telephone fraud character]. *Vestnik Moskovskogo universiteta. Seriya 14: Psikhologiya* [Moscow University Psychology Bulletin]. No. 1, pp. 138–157. DOI: https://doi.org/10.11621/vsp.2022.01.06

Mikhaylov, A.S. (2014). [Is the case study a research strategy or a meta-method?]. *Ekonomika i sotsium* [Economy and Society]. No. 3–2(12), pp. 543–551.

Parti, K. and Tahir, F. (2023). «If we don't listen to them, we make them lose more than money»: Exploring reasons for underreporting and the needs of older scam victims. *Social Sciences*. Vol. 12, iss. 5. Available at: https://www.mdpi.com/2076-0760/12/5/264/pdf?version=1683172510 (accessed 21.07.2024). DOI: https://doi.org/10.3390/socsci12050264

Pervushina, O.N. and Fedorov, A.A. (2022). [Personal characteristics of a telephone fraud person]. *Voprosy psikhologii.* Vol. 68, no. 3, pp. 92–103.

Pimentel, A. and Steinmetz, K.F. (2022). Enacting social engineering: the emotional experience of information security deception. *Crime, Law and Social Change*. Vol. 77, iss. 3, pp. 341–361. DOI: https://doi.org/10.1007/s10611-021-09993-8

Racheva, N.V., Baleevskikh, F.V. and Kotov, V.V. (2021). [Modern possibilities of improving fraud against the property of individuals using Internet resources and social engineering technologies]. *Yuridicheskaya nauka* [Legal Science]. No. 2, pp. 101–105.

Romanov, V.G. and Romanova, I.V. (2020). [Social fraud «Covid-19» and manipulative technologies of social engineering]. *Vestnik Zabaykal'skogo gosudarstvennogo universiteta* [Transbaikal State University Journal]. Vol. 26, no. 9, pp. 57–67. DOI: https://doi.org/10.21209/2227-9245-2020-26-9-57-67

Safuanov, F.S. and Dokuchaeva, N.V. (2015). [Personality characteristics of victims of unlawful attacks on the Internet]. *Psikhologiya i pravo* [Psychology and Law]. Vol. 5, no. 4, pp. 80–93. DOI: https://doi.org/10.17759/psylaw.2015050407

Shipulin, G.F. (2022). [Ways to improve fraud related to the use of mobile communications]. *Mezhdunarodnyy zhurnal gumanitarnykh i estestvennykh nauk* [International Journal of Humanities and Natural Sciences]. No. 2–2(65), pp. 186–189. DOI: https://doi.org/10.24412/2500-1000-2022-2-2-186-189

Sidorenko, E.V. (2004). *Trening vliyaniya i protivostoyaniya vliyaniyu* [Training influences and counteraction to influence]. St. Petersburg: Rech' Publ., 256 p.

Starostenko, N.I. (2020). [The criminalistic aspect of social engineering techniques in the commission of crimes]. *Vestnik Krasnodarskogo universiteta MVD Rossii* [Bulletin of Krasnodar University of Russian MIA]. No. 1(47), pp. 80–83.

Trakhov, A.I. and Beshukova, Z.M. (2022). [Prevention of telephone fraud: Russian and foreign experience]. *Tsifrovye tekhnologii i pravo: sbornik nauchnykh trudov I Mezhdunarodnoy nauchno-prakticheskoy konferentsii (Kazan', 23 sentyabrya 2022 g.): v 6 t.* [Digital Technologies and Law: a Collection of Scientific Papers and an International Scientific and Practical Conference (Kazan, Sep. 23, 2022): in 6 vols]. Kazan: Poznanie Publ., vol. 6, pp. 357–361.

Wang, J., Zhang, L., Xu, L. and Qian, X. (2024). The dynamic emotional experience of online fraud victims during the process of being defrauded: A text-based analysis. *Journal of Criminal Justice*. Vol. 94. Available at: https://www.sciencedirect.com/science/article/abs/pii/S0047235224000801 (accessed: 21.07.2024). DOI: https://doi.org/10.1016/j.jcrimjus.2024.102231

Yaroslavtseva, I.V. and Dorokhina, S.A. (2016). [Critical thinking of poor people — a victim of fraudulent actions: theoretical and applied aspects of the study]. *Izvestiya Irkutskogo gosudarstvennogo universiteta. Seriya: Psikhologiya* [Proceedings of

Irkutsk State University. Series: Psychology]. Vol. 15, pp. 60–71.

Yoshioka, T., Awai, S., Ide, K., Chikano, M., Iwasaki, S., Yoshino, K. and Konno, T. (2024). Demo: Preventing phone fraud by victim training using personalized feedback for behavioral change. *MOBISYS '24: Proceedings of the 22nd Annual International Conference on Mobile Systems, Applications and Services*. New York: Association for Computing Machinery Publ., pp. 588–589. DOI: https://doi.org/10.1145/3643832.3661833

Zabolotskaya, A.V. and Tkacheva, E.G. (2022). [Psychological security of personality on the Internet]. *Avtonomiya lichnosti* [The Autonomy of Personality]. No. 1(27), pp. 91–97.

Zotina, E.V. (2023). [Telephone fraud against elderly citizens]. *Uchenyye zapiski Kazanskogo yuridicheskogo instituta MVD Rossii* [Scientific Notes of the Kazan Law Institute of MIA Russia]. Vol. 8, no. 2(16), pp. 19–25.

Об авторе

Игнатова Екатерина Сергеевна
кандидат психологических наук, доцент, заведующая кафедрой общей и клинической психологии

Пермский государственный национальный исследовательский университет,
614990, Пермь, ул. Букирева, 15;
e-mail: 131013@mail.ru
ResearcherID: O-1306-2016

About the author

Ekaterina S. Ignatova
Candidate of Psychology, Docent, Head of the Department of General and Clinical Psychology

Perm State University,
15, Bukirev st., Perm, 614990, Russia;
e-mail: 131013@mail.ru
ResearcherID: O-1306-2016