Психология и право
2026. *16*(1), 240–265.
https://doi.org/10.17759/psylaw.2026160115
ISSN 2222-5196 (online)

Psychology and Law
2026. *16*(1), 240–265.
https://doi.org/10.17759/psylaw.2026160115
ISSN 2222-5196 (online)

МЕЖДИСЦИПЛИНАРНЫЕ ИССЛЕДОВАНИЯ |
INTERDISCIPLINARY STUDIES

Научная статья | Original paper

Разработка и апробация методики диагностики уязвимости к техникам социальной инженерии на основе индивидуально-типологического подхода Л.Н. Собчик

И.Ф. Нурмухаметова[1], **Э.А. Нурмухаметов**[1] ✉
[1] Уфимский университет науки и технологий, Уфа, Российская Федерация
✉ misall@mail.ru

Резюме

Контекст и актуальность. В эпоху цифровизации, когда высок риск утечки персональных данных в сеть Интернет, люди все чаще становятся жертвами кибермошенничества, в основе которого лежат техники социальной инженерии. Предметное понимание того, какие именно индивидуально-типологические свойства личности предрасполагают к уязвимости перед мошенниками, важно для формирования более эффективных стратегий противодействия кибермошенничеству и улучшения кибербезопасности в целом. **Цель.** Разработать, описать и провести первичную апробацию авторской методики диагностики индивидуальной уязвимости к техникам социальной инженерии, основанной на теории ведущих тенденций личности Л.Н. Собчик. **Гипотеза.** Существует статистически значимая связь между ведущими тенденциями личности (по Л.Н. Собчик) и уязвимостью к техникам социальной инженерии. **Методы и материалы.** В исследовании приняли участие 185 респондентов в возрасте от 18 до 30 лет (M = 21,5, SD = 2,8; 68% девушек, 32% юношей). Индивидуально-типологические свойства личности оценивались с помощью методики Л.Н. Собчик, диагностика уязвимости к социальной инженерии осуществлялась на основе разработанной авторской методики «УкСИ». **Результаты.** Эмпирически подтверждено, что различные конфигурации личностных тенденций обусловливают специфическую уязвимость к определенным манипулятивным техникам социальной инженерии. На основе результатов исследования выделены устойчивые профили риска, что подтверждает конструирующую валидность и диагностическую ценность разработанной методики для выявления «слабых мест» в психологической защите личности. **Выводы.** Разработанная методика показала свою диагностическую состоятельность и открывает возможности для перехода к персонализированным программам повышения осведомленности в области информационной безопасности. Подтверждены принципиальная возможность

и эффективность использования индивидуально-типологического подхода Л.Н. Собчик (теории ведущих тенденций) для диагностики уязвимости к социальной инженерии: глубинные личностные характеристики являются значимым предиктором поведения в ситуациях манипулятивного воздействия, что расширяет существующие представления о природе уязвимости в кибербезопасности.

Ключевые слова: социальная инженерия, кибермошенничество, индивидуально-типологические свойства, когнитивные ошибки, личность, теория ведущих тенденций

Для цитирования: Нурмухаметова, И.Ф., Нурмухаметов, Э.А. (2026). Разработка и апробация методики диагностики уязвимости к техникам социальной инженерии на основе индивидуально-типологического подхода Л.Н. Собчик. *Психология и право, 16*(1), 240—265. https://doi.org/10.17759/psylaw.2026160115

Development and testing of a methodology for diagnosing vulnerability to social engineering techniques based on L.N. Sobchik's individual-typological approach

I.F. Nurmukhametova[1], **E.A. Nurmukhametov**[1] ✉
[1] Ufa University of Science and Technology, Ufa, Russian Federation
✉ misall@mail.ru

Abstract

Context and relevance. In the era of digitalization, with its high risk of personal data breaches on the Internet, people are increasingly becoming victims of cyber fraud based on social engineering techniques. Understanding which individual-typological personality traits predispose individuals to vulnerability to fraudsters is crucial for developing more effective counter-fraud strategies and improving cybersecurity overall. **Objective.** To develop, describe, and conduct initial testing of an original methodology for diagnosing individual vulnerability to social engineering techniques, based on L.N. Sobchik's theory of leading personality tendencies. **Hypothesis.** There is a statistically significant relationship between an individual's profile of leading personality tendencies (according to L.N. Sobchik) and their level of vulnerability to social engineering techniques. **Methods and materials.** The study involved 185 respondents aged 18 to 30 (M = 21.5, SD = 2.8; 68% female). Individual-typological personality traits were assessed using the L.N. Sobchik methodology, while vulnerability to social engineering was diagnosed using the developed author's methodology. **Results.** It was empirically confirmed that various configurations of personality tendencies lead to a specific vulnerability to certain manipulative techniques. Based on the research results, stable risk profiles were identified, confirming the construct validity and diagnostic value of the developed methodology for revealing “weak spots” in an individual's psychological defense.

Conclusions. The developed methodology has demonstrated its diagnostic validity and opens up opportunities for transitioning to personalized information security awareness programs. The fundamental possibility and effectiveness of using L.N. Sobchik's individual-typological approach (theory of leading tendencies) for diagnosing vulnerability to social engineering has been confirmed: deep-seated personality characteristics are a significant predictor of behavior in situations of manipulative influence, which expands existing understanding of the nature of vulnerability in cybersecurity.

Keywords: social engineering, cyber fraud, individual-typological traits, cognitive errors, personality, theory of leading tendencies

For citation: Nurmukhametova, I.F., Nurmukhametov, E.A. (2026). Development and testing of a methodology for diagnosing vulnerability to social engineering techniques based on L.N. Sobchik's individual-typological approach. *Psychology and Law, 16*(1), 240—265. (In Russ.). https://doi.org/10.17759/psylaw.2026160115

Введение

Растущие сложность и изощренность кибератак закономерно сместили фокус научных исследований с сугубо технических уязвимостей на человеческий фактор, остающийся наиболее слабым звеном в системе информационной безопасности. Методы социальной инженерии, основанные на психологических механизмах манипуляции, позволяют злоумышленникам эффективно обходить самые совершенные технические средства защиты. Данные ведущих компаний в области кибербезопасности, например таких, как IBM Security, подтверждают, что от 70 до 90% успешных атак инициируются с использованием методов социальной инженерии. Несмотря на осознание масштаба данной угрозы, доминирующие в настоящее время подходы к оценке и снижению рисков — такие как разовые тренинги по осведомленности и ситуативное тестирование на фишинг — носят реактивный и фрагментарный характер. Они позволяют оценить знание правил в конкретный момент времени, однако не затрагивают глубинных психологических механизмов уязвимости, что делает невозможным проактивный прогноз индивидуальной подверженности социальной инженерии, в основе которой лежит манипуляция сознанием личности. Сложившаяся ситуация указывает на значительный пробел, связанный с отсутствием в диагностическом арсенале современной психологии валидных инструментов для проактивной оценки личностных детерминант уязвимости перед техниками социальной инженерии. Таким образом, возникает необходимость разработки соответствующего инструментария, направленного не на оценку ситуативных знаний, а на выявление глубинных психологических паттернов, обусловливающих устойчивую уязвимость личности к манипуляции.

Анализ предыдущих исследований выявил несколько ключевых направлений в изучении психологических детерминант уязвимости к социальной инженерии. Некоторые исследователи справедливо связывают подверженность манипуляции с такими чертами личности, как низкая добросовестность и высокий невротизм, например, в рамках модели «Big five» (Sleep, Lynam, Miller, 2021), а также с поиском острых ощущений (Розова и др.,

2021). Другие авторы акцентируют внимание на роли таких когнитивных факторов, как склонность к доверию (Монахова и др., 2024), сниженная критичность мышления и когнитивные искажения, такие как, например, влияние авторитета и дефицит рационального анализа в условиях стресса или неопределенности (Milgram, 1963; Stanovich, West, 2000; Starcke, Brand, 2012), сниженный самоконтроль одновременно с повышенным уровнем эмоциональной лабильности, низкий порог фрустрации, неуверенность в себе, добавляя к этому также доверчивость и наивность в ходе общения, отсутствие навыков дипломатично выстраивать коммуникацию (Власова, Буслаева, 2022). Некоторые исследователи определяют фактором, обуславливающим киберпреступное поведение и условием стать жертвой мошенников, кроме отдельно взятых черт личности, также и недостаточную цифровую грамотность (Вознесенская, 2025). Тем самым оценка психологических детерминант уязвимости, по большому счету, базируется на основе анализа изолированных черт личности или когнитивных искажений. Однако такой редукционистский подход, на наш взгляд, не учитывает целостность личности, где уязвимость к манипуляции является следствием сложного взаимодействия устойчивых индивидуально-типологических свойств.

В качестве методологической основы, позволяющей преодолеть такой разрыв, резонно использовать личностно-ориентированный подход в рамках научной школы Л.Н. Собчик. В отличие от моделей, описывающих «статичные» черты личности, в теории ведущих тенденций, разработанной Л.Н. Собчик, личность рассматривается как целостная система, где индивидуальный стиль восприятия, переживания и поведения детерминирован базовыми врожденными свойствами нервной системы, такими как ригидность, лабильность, интроверсия, экстраверсия, спонтанность, сензитивность (Собчик, 2022). И именно ригидность, с нашей точки зрения, как одна из ведущих тенденций личности, характеризующаяся инертностью нервных процессов, трудностью переключения с одной программы поведения на другую и приверженностью стереотипам, представляет собой ключевой системообразующий фактор уязвимости к определенным типам манипулятивного воздействия.

В контексте анализа техник социальной инженерии роль ригидности, на наш взгляд, является амбивалентной. С одной стороны, она может обусловливать устойчивое следование правилам безопасности, создавая «иммунитет» к атакам мошенников, рассчитанным на спонтанность. С другой стороны, в ситуации нестандартного манипулятивного давления, требующего гибкого отклонения от шаблона, именно личность с выраженной ригидностью оказывается наиболее уязвимой, демонстрируя неспособность критически переоценить ситуацию и выйти за рамки навязанного злоумышленником сценария. Это согласуется с данными о том, что универсальной схемой манипулятивного влияния является комплексное воздействие, приводящее жертву в состояние растерянности, беспомощности и болезненного ощущения «утраты контроля», выход из которого человек ищет через принятие быстрого решения, предлагаемого самим манипулятором (Розенова, Огнев, Лихачева, 2025).

Настоящим исследованием предлагается ввести и эмпирически проверить модель психографических профилей риска, где центральным связующим конструктом является ригидность, а каждый тип уязвимости к техникам социальной инженерии перекликается с ведущими тенденциями, выделенными Л.Н. Собчик. Концепция ведущих тенденций предоставляет единый объяснительный механизм: уязвимость трактуется не как случайная

ошибка, а как закономерное следствие индивидуального стиля взаимодействия с миром. Например, тенденция к доверчивости (обусловленная сензитивностью) или конформности (связанная с интровертированностью и тревожностью) напрямую определяет мишени для манипуляции. Такой подход напрямую диктует структуру методики, где каждый диагностируемый параметр уязвимости имеет четкое обоснование в теоретическом плане, что обеспечивает высокую конструктную валидность предлагаемого нами методического инструментария.

Методический инструментарий исследования

Участники исследования

В исследовании приняли участие 185 респондентов. Выборка была сформирована целевым методом и преимущественно состояла из студентов вузов, что является репрезентативным показателем для первичной апробации авторской методики диагностики уязвимости к техникам социальной инженерии (УкСИ), так как данная социальная группа активно использует цифровые сервисы и регулярно сталкивается с угрозами социальной инженерии в виртуальной среде. Социально-демографические характеристики выборки приведены в табл. 1.

Таблица 1 / Table 1

Социально-демографическая характеристика выборки (N = 185)
Socio-demographic characteristics of the sample (N = 185)

Параметры / Parameters	**Значение / Value**
Средний возраст / Mean Age (M ± SD)	21,5 ± 2,8
Гендерный состав / Gender	68% девушек / female, 32% юношей / male
Основной статус / Primary Status	Студенты /students — 85%, работающие / employed — 15%

Методики исследования

Для сбора эмпирических данных был использован малый диагностический комплекс, включающий две методики: собственно, авторская методика диагностики уязвимости к техникам социальной инженерии (УкСИ[1]) для оценки уровня ригидности и индивидуальной подверженности основному спектру манипулятивных техник социальной инженерии; индивидуально-типологический опросник (ИТО[2]) Л.Н. Собчик для диагностики структуры индивидуально-типологических свойств личности в рамках теории ведущих тенденций и согласованности.

Методика «ИТО» Л.Н. Собчик была выбрана как соответствующая методологической основе исследования, поскольку позволяет оценить целостный личностный профиль, а также

[1] *Методика УкСИ*. [б.г.]. Online Test Pad. URL: https://onlinetestpad.com/nrd6yyevykvme (дата обращения: 25.09.2025).

[2] *Индивидуально-типологический опросник, ИТО*. [б.г.]. Психологические тесты онлайн. https://psytests.org/accent/ito-run.html (дата обращения: 25.09.2025).

помочь осуществить анализ конвергентной и дискриминантной валидности предлагаемой авторской методики «УкСИ». В рамках данного исследования анализировались все базовые шкалы методики «ИТО»: «Ригидность», «Лабильность», «Экстраверсия», «Спонтанность», «Сензитивность», «Тревожность», «Интроверсия», «Агрессивность». Профиль ведущих тенденций строился на основе стандартных ключей и процедур, предусмотренных методикой. Для дальнейшего анализа использовались стандартные сырые баллы по каждой из шкал.

Авторская методика «УкСИ» представляет собой единый опросник, состоящий из 80 утверждений. Из них 64 утверждения направлены на диагностику уязвимостей к 8 ключевым техникам социальной инженерии (по 8 утверждений на каждую шкалу), а 16 утверждений направлены на измерение инертности нервных процессов, трудности переключения с одной деятельности на другую и приверженности стереотипам (шкала «Ригидность»).

Диагностируемые шкалы (уязвимости к техникам социальной инженерии).

Шкала 1. Уязвимость к технике «Imposture» («Самозванец»). Когда мошенники прибегают к методу социальной инженерии, избрав технику «Самозванец», они создают образ авторитетной и сильной фигуры, зачастую изображая сотрудников полиции, спецслужб, налоговых служб или крупных коммерческих предприятий. Имитация высокопоставленной роли сама по себе формирует впечатление надежности и солидности, что апеллирует к внутреннему желанию большинства людей признавать превосходство сильных и влиятельных личностей. Однако ключевым фактором успеха становится не только позиционирование силы, но и активное воздействие на внутренние импульсы жертвы, инициируемые тенденцией агрессивности. Что перекликается сущностно с ведущей тенденцией личности «Агрессивность», выделяемой Л.Н. Собчик. На наш взгляд, человек, испытывающий внутренний импульс доказать собственную значимость, силу воли или покорность власти, воспринимает давление со стороны псевдоавторитетного субъекта как приглашение продемонстрировать собственное достоинство и лояльность. Это означает, что такая форма социальной атаки прекрасно «работает» благодаря активизации подсознательного желания казаться сильным, достойным и заслуживающим внимания в глазах значимой инстанции. Принимая во внимание, что агрессивность, по теории Л.Н. Собчик, символизирует потребность в самореализации и упорство в достижении целей, резонно говорить о том, что люди с такими чертами характера обладают своими непоколебимыми принципами и интересами, которые они активно продвигают. Вопросы в методике, которые характеризуют уязвимость к технике «Imposture»: № 1, № 2, № 7, № 14, № 50, № 57, № 60, № 71.

Шкала 2. Уязвимость к технике «Offer» (Предлог) кроется в игре на любопытстве и жадности. В данном случае создается сфабрикованный сценарий для манипулирования эмоциями или любопытством жертвы, например, предложения о крупном выигрыше, неожиданном наследстве или выгодных сделках могут привлечь внимание и заставить людей раскрывать свою личную информацию. С позиции теории Л.Н. Собчик, данная уязвимость, на наш взгляд, хорошо согласуется с ведущей тенденцией «Эмоциональная лабильность», так как эмоционально лабильные личности характеризуются повышенной впечатлительностью, импульсивностью и склонностью легко поддаваться сиюминутным настроениям и соблазнам. Их неустойчивый эмоциональный фон делает их особенно

восприимчивыми к заманчивым, но сфабрикованным предложениям, которые сулят быструю выгоду или яркие переживания, минуя критическую оценку рисков. Вопросы в методике, которые характеризуют уязвимость к этой технике: № 15, № 24, № 28, № 30, № 31, № 36, № 45, № 68. Этот блок вопросов направлен на определение чувствительности к эмоциональным факторам и восприимчивости к искусственно создаваемым сценариям.

Шкала 3. Уязвимость к технике «Phishing» («Выуживание»), в основе которой лежит массовая рассылка сообщений (чаще всего электронных писем или смс), замаскированных под официальные уведомления от банков, сервисов доставки или государственных органов, кроется в низкой степени критичности оценивания ситуации. С точки зрения психологии, здесь заложен механизм создания чувства срочности — сообщение о том, что необходимо немедленно предпринять действия «здесь и сейчас». Такой подход заставляет людей действовать без достаточного обдумывания. При задействовании данной техники злоумышленники, чаще всего, апеллируют к авторитету (ведь, фишинговые атаки часто мимикрируют под официальные сообщения от известных организаций, чтобы создать впечатление легитимности). Однако наравне с авторитетом мошенники также прибегают и к запугиванию, созданию ситуации страха и тревоги. Используя страх жертвы, они заставляют подчиняться своей воле, например, угрожая утратой доступа к аккаунту или финансовыми потерями. Конечная цель сводится к тому, чтобы побудить жертву перейти по фальшивой ссылке и ввести свои конфиденциальные данные (логины, пароли, данные карт). Сущностно, данная уязвимость, в контексте теории Л.Н. Собчик, связана с такими ведущими тенденциями, как «Тревожность», «Экстраверсия» и «Сенситивность». На наш взгляд, ключевым психологическим механизмом данной уязвимости является не столько страх, сколько **повышенная откликаемость на внешние социально-коммуникативные стимулы**, характерная для экстравертированного и сензитивного типа личности. Легкая отвлекаемость, выраженная ранимость и впечатлительность, склонность к вовлечению в интерактивные сценарии и привычка к широкому, но поверхностному кругу контактов делают личность более восприимчивой к фишинговым атакам, которые мимикрируют под легитимные сообщения из их социального окружения. Вопросы в методике, диагностирующие уязвимость к выделенной технике: № 40, № 43, № 49, № 54, № 55, № 56, № 63, № 70.

Шкала 4. Уязвимость к технике «Scareware» («Устрашение»), архитектура которой, как и у техники «Phishing», сводится к тенденции играть на страхах и формировать тревожность у личности, кроется в том, что личность действует инстинктивно, руководствуясь своим внутренним состоянием, а не фактическими обстоятельствами. Техника устрашения основана на запугивании жертвы несуществующей угрозой (например, заражением компьютера вирусом, блокировкой банковского счета, возбуждением уголовного дела). Мошенники создают ситуацию угрозы, говоря, например, о вирусе, взломе аккаунта или потере денег, чтобы вызвать быстрый отклик и принудить жертву действовать незамедлительно. По нашим расчетам, люди с выраженной тревожностью находятся в постоянной готовности отреагировать на воображаемые угрозы, не пытаясь глубоко проанализировать ситуацию. Соответственно, данная уязвимость напрямую должна быть связана с ведущей тенденцией «Тревожность» (по Л.Н. Собчик), а также с некоторыми психастеническими чертами личности. Полагаем, что люди с высоким уровнем тревожности

и мнительности наиболее подвержены панике и готовы на все, чтобы немедленно устранить мнимую угрозу. Именно это делает их уязвимыми перед данной техникой социальной инженерии. Вопросы в методике, диагностирующие уязвимость к выделенной технике: № 5, № 6, № 18, № 21, № 23, № 51, № 66, № 76.

Шкала 5. Уязвимость к технике «Vishing» («Вишинг»), схожей в некотором смысле по своей природе с техникой «Scareware», кроется в том, что здесь так же, как и в предыдущем случае, имеет место быть игра на тревожности и низком уровне коммуникативных навыков личности. Например, используя убедительный голос и четкую аргументацию, мошенники способны заставить жертву почувствовать давление, уговаривая ее незамедлительно принять решение или предоставить конфиденциальную информацию. Человек, обладающий интровертированным характером, с нашей точки зрения, менее подготовлен к противостоянию подобным манипуляциям, так как его привычки и ограничения делают его менее стойким к внешнему влиянию (ведущая тенденция личности, по Л.Н. Собчик, — «Интроверсия»). Людям с преобладанием интроверсии характерны, чаще всего, низкая коммуникабельность, замкнутость, осторожность в принятии решений и трудность в налаживании контактов. Интроверсия «ограничивает» круг знакомств и опыт личного общения, снижая социальную адаптивность и увеличивая шанс попасться на удочку злоумышленников, особенно в новых ситуациях. Если интроверт получит звонок от лжепредставителя банка, например, попросившего продиктовать данные карты, он может воспринять такую просьбу буквально и согласиться, потому что старается, по своей природе, избегать конфликтных ситуаций, общаясь скорее формально, не желая разбираться в нюансах. Интровертированный человек, на наш взгляд, меньше сомневается в правильности своих поступков, что упрощает задачу злоумышленникам. Вопросы в методике, диагностирующие уязвимость к выделенной технике: № 8, № 17, № 32, № 41, № 47, № 72, № 75, № 80.

Шкала 6. Уязвимость к технике «Bait» («Приманка»). В случае, когда социальная инженерия направлена на то, чтобы акцентировать внимание человека на внешних объектах, избирается техника так называемой приманки. Мошенники оставляют в свободном доступе зараженные носители информации (например, флеш-карты) или создают фиктивные точки доступа Wi-Fi с привлекательными названиями («Free_Wi-Fi»). Расчет делается на любопытство и беспечность жертвы. С нашей точки зрения, учитывая подход Л.Н. Собчик, эта уязвимость хорошо коррелирует как с экстраверсией, так и с интроверсией в сочетании с впечатлительностью. Вопросы в методике, диагностирующие уязвимость к выделенной технике: № 4, № 20, № 25, № 26, № 37, № 48, № 69, № 78. Данный блок вопросов фокусируется на оценке отношения личности к выгоде и стимулам, связанным с бесплатными услугами и подарками. Вопросы построены относительно внешних впечатлений, стремления к новым возможностям и положительным эмоциям извне.

Шкала 7. Уязвимость к технике «Quid Pro Quo» («Услуга за услугу»). В данном случае происходит игра на чувстве вежливости, долга и социальной норме взаимности. Нередко, прибегая к социальной инженерии, мошенники играют на человеческой склонности обмениваться благами и ощущением благодарности за предоставленное содействие. Мошенник предлагает жертве какую-либо услугу или помощь (например, техническую поддержку, помощь в оформлении документа) в обмен на конфиденциальные данные или

доступ к системе. На наш взгляд, в группу риска чаще попадают впечатлительные люди, так как, по теории Л.Н. Собчик, люди с такими чертами личности уютнее чувствуют себя под прикрытием более сильной личности, чаще всего любят помогать другим и получают удовольствие от взаимодействия, причем ответственны и исполнительны, сверхтревожно реагируют на стресс-ситуацию, сверхболезненно относятся к низким оценкам по отношению к себе. Вопросы в методике, диагностирующие уязвимость к выделенной технике: № 3, № 16, № 34, № 42, № 58, № 61, № 62, № 67.

Шкала 8. Уязвимость к технике «The Apple of the Road» («Дорожное яблоко»). Название этой техники происходит от исторической тактики, когда на пути кавалерии противника разбрасывали острые шипы. В современном контексте — это размещение в общедоступных местах зараженных носителей информации, как и в случае с техникой «Bait», но с расчетом на конкретную, целевую жертву. Уязвимость здесь связана, на наш взгляд, не только с любопытством, но и с профессиональной деформацией и гиперболизированной тенденцией «Агрессивность» в виде сверхнастойчивости и целеустремленности, а также стремлением к независимости и самоутверждению, выраженное в совершении импульсивных и необдуманных поступков (тенденция «Спонтанность»). Сотрудник, чрезмерно увлеченный своей работой и стремящийся любой ценой добиться результата, может подобрать и использовать такую «приманку», игнорируя правила безопасности. Вопросы в методике, диагностирующие уязвимость к выделенной технике: № 9, № 27, № 44, № 53, № 59, № 65, № 73, № 77.

Шкала «Ригидность» представляет собой интегративный показатель, измеряющий инертность нервных процессов, трудность переключения с одной деятельности на другую и приверженность стереотипам. Высокие показатели по этой шкале указывают на то, что человек с трудом адаптируется к новым ситуациям, склонен действовать по шаблону и может быть уязвим для техник социальной инженерии, которые эксплуатируют его неготовность к нестандартным ситуациям и критическому переосмыслению происходящего. Низкие показатели, наоборот, свидетельствуют о высокой психической подвижности, быстрой переключаемости и гибкости поведения. Такой человек легко адаптируется к изменениям, однако в крайних проявлениях это может приводить к излишней импульсивности, непоследовательности и недостаточной критической оценке ситуации в условиях цейтнота, когда быстрое решение подменяет собой верное. Оптимальным вариантом является средний показатель данной переменной: умеренная устойчивость взглядов и поведения, проявляющаяся в способности менять позицию при наличии достаточно весомых оснований, одновременно сохраняя определенную долю консерватизма и устойчивости в действиях. Человек со средним уровнем ригидности обладает балансом между гибкостью и стабильностью. Эта шкала является характерной «лакмусовой бумажкой» для всех остальных шкал, так как ригидность усиливает проявление любой из уязвимостей, мешая гибко отреагировать на манипуляцию. Вопросы в методике, диагностирующие уязвимость к выделенной технике: № 10, № 11, № 12, № 13, № 19, № 22, № 29, № 33, № 35, № 38, № 39, № 46, № 52, № 64, № 74, № 79.

Далее, на основе эмпирических данных по уязвимостям к техникам социальной инженерии, строятся профили риска. Профиль риска — это не просто высокий показатель по

одной шкале, а уникальная комбинация, которая являет собой так называемую «ахиллесову пяту» в восприятии и анализе информации.

Мы выделили *5 профилей риска* с учетом уровня ригидности.

1. Ригидно-импульсивный профиль (когда стресс «отключает» разум).

Ключевая уязвимость: склонность к сбросу когнитивной нагрузки под давлением; мозг в стрессе отключает критическое мышление и переходит на автоматические, шаблонные реакции.

Проявляется: внезапными, необдуманными действиями в условиях цейтнота или кризиса; вспышками раздражения; поспешным нажатием на кнопку «отправить» или «подтвердить».

Сценарий атаки строится на создании искусственного, высокоинтенсивного кризиса, который вынуждает жертву действовать немедленно, чтобы избежать негативных последствий (убытка, сбоя, срыва сроков), подавляя тем самым возможность критической оценки ситуации.

2. Ригидно-отзывчивый профиль (конфликт между долгом и безопасностью).

Ключевая уязвимость: гипертрофированная потребность в социальном одобрении и эмоциональном контакте; «жесткие» убеждения о долге, вежливости и взаимопомощи.

Проявляется: неспособностью отказать авторитетной фигуре или симпатичному коллеге; готовностью нарушить правила, чтобы «помочь» или «не обидеть».

Сценарий атаки основан на техниках социальной инженерии, строящихся на доверии (имперсонация начальника, коллеги из другого отдела) или на создании чувства вины/обязательства.

3. Ригидно-осторожный профиль (иллюзия контроля над ситуацией).

Ключевая уязвимость: избирательная бдительность и «когнитивная слепота» (неспособность заметить что-либо из-за концентрации на другой задаче), порожденная самой структурой защитного поведения. Человек часто переоценивает свою защищенность из-за успешного сопротивления одним конкретным видам атак.

Проявляется: уверенностью в своей неуязвимости после успешного отражения простых атак. Субъект пропускает сложные, многоходовые атаки, так как ожидает очевидных признаков обмана (опечатки, грубые подделки).

Сценарий атаки основан на качественном фишинге с безупречной орфографией и личными данными, собранными из открытых источников (таргетированный фишинг). Атака чаще всего идет через доверенный, но скомпрометированный канал связи.

4. Адаптивно-устойчивый профиль (гибкость мышления как главная защита).

Ключевая характеристика: когнитивная гибкость и развитое мета мышление (понимание особенностей своего мышления, эффективное распределение когнитивных ресурсов, развитое «чувство ошибки»), эмоциональная стабильность. Способность быстро адаптироваться к новым угрозам и эффективно противостоять манипуляциям.

Когнитивная гибкость обращается против жертвы. Мозг жертвы занят решением рабочей головоломки, а не поиском угроз. Угроза маскируется под рутинное препятствие.

Сценарий атаки основан на том, что жертва действует в рамках стандартной рабочей процедуры: получила задачу от начальства → столкнулась с проблемой → вызвала

техподдержку → выполняет инструкции для решения проблемы. Ее добросовестность и ориентация на результат заставляют ее пройти этот путь до конца. Иначе говоря, это тонкая, многоуровневая инсценировка рабочей ситуации, где жертва, используя все свои сильные стороны, самостоятельно приходит к нужному злоумышленнику действию, будучи уверенной, что просто выполняет свою работу.

5. Смешанный профиль (комбинация уязвимостей, не вписывающаяся в чистые типы). Может иметь любой уровень ригидности с уникальным набором чувствительных точек. Требует индивидуального анализа паттернов уязвимости. Варианты сочетаний могут быть следующие, например: SPB — уязвимость к устрашению, фишингу и приманке; IOV — чувствительность к тактике самозванства, различным «соблазнительным» предложениям и вишингу; QA — риск при оказании взаимной помощи и при использовании мошенниками техники «Дорожные яблоки». Любые другие комбинации.

Процедура исследования и обработка данных по методике «УкСИ»

Сбор данных осуществлялся дистанционно с использованием следующих онлайн-платформ: «Onlinetestpad» и «Psytests». Процедура исследования уязвимости к техникам социальной инженерии проходила поэтапно. Участникам направлялись ссылки на опросники с подробной инструкцией, разъясняющей цели исследования, гарантирующей анонимность и конфиденциальность данных. Комплекс методик предъявлялся в фиксированной последовательности: сначала авторская методика «УкСИ», затем опросник «ИТО». Средняя продолжительность прохождения общего опроса по двум методикам составляет 30—35 минут.

При прохождении авторской методики «УкСИ» респонденту предлагается оценить утверждения относительно себя лично по 5-балльной шкале Лайкерта (где 1 — «полностью не согласен», а 5 — «полностью согласен»), т. е. насколько эти утверждения соответствуют его личностным особенностям и вероятной реакции на что-либо. Степень выраженности каждой уязвимости определялась посредством сложения набранных в ходе опроса баллов: чем выше бал, тем ярче выражена уязвимость к той или иной технике социальной инженерии.

На основании показателей уязвимостей к техникам социальной инженерии можно высчитать профиль риска (интегральный показатель, который связывает конкретную конфигурацию ведущих тенденций с повышенной вероятностью поддаться определенным техникам социальной инженерии). По сути, это ответ на вопрос: «Каков психологический портрет человека, который с наибольшей вероятностью станет жертвой мошенника, использующего, например, техники “Imposture” или “Phishing”?». Из-за некоторых технических ограничений на платформе «Onlinetestpad», возможный профиль риска определяется посредством автоматического расчета в программе Excel для работы с электронными таблицами (при необходимости авторы методики готовы предоставить данный файл). Обработка эмпирических данных проводилась с использованием программного пакета Statistica v.12.0. Применялись следующие методы статистического анализа данных.

1. Для проверки внутренней согласованности авторской методики «УкСИ» был задействован расчет с применением коэффициента α Кронбаха и скорректированный корреляционный анализ: оценивалась корреляция между баллом за вопрос и суммой всех баллов без учета данного вопроса.

2. С целью описания выборки использовалась дескриптивная статистика: расчет средних значений (M) и стандартных отклонений (SD) для всех шкал методик.

3. Для выделения устойчивых профилей риска («мишеней для манипуляции») использовался кластерный анализ.

4. Для верификации статистической значимости различий между выделенными кластерами использовался многомерный дисперсионный анализ (MANOVA).

5. Для пост-хок сравнения применялся тест Тьюки / Tukey HSD для множественных сравнений.

Результаты

Надежность и внутренняя согласованность методики «УкСИ» оценивались с помощью ряда статистических критериев. Значение α Кронбаха относительно всей методики составило 0,902, а показатель стандартизированной α составил 0,899, что свидетельствует не только о высокой внутренней согласованности опросника, но и о том, что высокая согласованность не является артефактом разного масштаба или дисперсии отдельных пунктов. При этом значение средней межпунктовой корреляции (Average Inter-Item Correlation) находится на нижней границе допустимого диапазона (0,103). Такая картина является типичной и ожидаемой для многомерных опросников, измеряющих сложные конструкты. Вместе с тем средний балл (Mean) по методике составил 26,74. Стандартное отклонение указывает на умеренный разброс результатов вокруг среднего значения (Std. Deviation: 28,20), что свидетельствует о том, что респонденты демонстрируют разнообразие в ответах, а это является хорошим признаком для методики. Также можно утверждать и о том, что методика охватывает широкий диапазон проявлений измеряемого свойства (Minimum-Maximum: от 147 до 332). Распределение показателей является положительно асимметричным, что означает небольшое смещение в сторону более низких баллов (асимметрия/skewness: 0.49). Однако это значение находится в пределах нормы, что указывает на отсутствие серьезных нарушений нормальности распределения. Распределение является островершинным (лептокуртическим) (эксцесс/ kurtosis: 1,08), т. е. данные несколько более сконцентрированы вокруг среднего и имеют более тяжелые «хвосты» по сравнению с нормальным распределением. Как и асимметрия, это значение является допустимым. Следовательно, распределение общего балла по методике близко к нормальному без критических нарушений, что позволяет использовать параметрические методы статистики для дальнейшего анализа. Методика успешно дифференцирует респондентов с разным уровнем выраженности измеряемого свойства. Полученные данные для удобства представлены в табличной форме (табл. 2).

Таблица 2 / Table 2

Информация о надежности и внутренней согласованности методики «УкСИ» (N = 185)
Reliability and internal consistency information for the "UkSI" method (N = 185)

Количество пунктов / Number of items in scale	80
Количество валидных случаев / Number of valid cases	185

Количество случаев с пропущенными данными / Number of cases with missing data	2
Пропущенные данные удалялись / Missing data were deleted	построчно / casewise
Сводная статистика / Summary statistics for scale	
Средняя / Mean: 26,74054054	Сумма / Sum: 41947,000000
Стандартное отклонение / Standard Deviation: 28,195700600	Дисперсия / Variance: 794,99753231
Ассиметрия / Skewness: 0,495552126	Эксцесс / Kurtosis: 1,088903286
Миниммум / Minimum: 147,00000000	Максимум / Maximum: 332,00000000
Показатель α Кронбаха / Cronbach's alpha: 0,902045092	Показатель стандартизированной α Кронбаха / Standardized alpha: 0,899629691
Средняя межпунктовая корреляция / Average Inter-Item Correlation: 0,10345644	

Для подтверждения целесообразности сохранения всех вопросов методики «УкСИ» была проведена оценка внутренней согласованности при исключении каждого из вопросов по одному. Было обнаружено, что удаление некоторых из вопросов методики «УкСИ» по отдельности (№ 1, 28, 39, 64) незначительно повышает и без того высокое значение альфы Кронбаха (при 0,902 до 0,904). Следовательно, ни один из вопросов методики существенно не ухудшает общей внутренней согласованности.

Для проверки конвергентной и дискриминантной валидностей были проанализированы корреляции между шкалами предлагаемой методики «УкСИ» и методики Л.Н. Собчик «ИТО» (табл. 3). Как и предполагалось, обнаружены статистически значимые положительные связи между следующими шкалами: «Уязвимость к технике “Imposture”» и «Агрессивность» (0,92), «Уязвимость к технике “Scareware”» и «Тревожность» (0,76), «Уязвимость к технике “Vishing”» и «Интроверсия» (0,84), «Уязвимость к технике “Phishing”» и «Экстраверсия» (0,81), шкалы ригидности (0,91), «Уязвимость к технике “Bait”» и «Экстраверсия» (0,74), «Интроверсия» (–0,71), «Уязвимость к технике “Offer”» и «Лабильность» (0,63), «Уязвимость к технике “Quid Pro Quo”» и «Сензитивность» (0,62), «Уязвимость к технике “Apple of the Road”» и «Спонтанность» (0,52). При этом анализ дискриминантной валидности методики «УкСИ» показал, что, например, шкала «Уязвимость к технике “Imposture”» имеет слабую связь практически со всеми шкалами методики «ИТО» за исключением шкалы «Агрессивность»; шкала «Уязвимость к технике “Scareware”», будучи имея крепкую связь с тревожностью (0,76), имеет низкие корреляции со шкалой «Спонтанность» (0,34), «Экстраверсия» (0,57); с экстраверсией крепко связана и шкала «Уязвимость к технике “Phishing”», при этом с остальными шкалами методики «ИТО» она имеет незначительные связи, включая тревожность (0,582). Шкала ригидности методики «УкСИ» демонстрирует уникальную дискриминантность, коррелируя лишь со шкалой ригидности и лабильности методики «ИТО», с остальными показателями данного опросника у нее отсутствуют какие-либо значимые связи. Профили корреляций шкал «Уязвимость к технике “Quid Pro Quo”» и «Уязвимость к технике “Apple of the Road”» более размыты: первая шкала связана и с сензитивностью, и с экстраверсией, вторая шкала — со

спонтанностью, но также с экстраверсией и с интроверсией (отрицательно). Это указывает на то, что эти техники могут апеллировать к более общим моделям социального поведения, что свидетельствует о том, что методика «УкСИ» измеряет именно специфические уязвимости, а не общие личностные черты.

Таким образом, подавляющее большинство шкал методики «УкСИ» демонстрирует сильные и статистически значимые связи с концептуально близкими шкалами опросника «ИТО» Л.Н. Собчик. Полученные результаты эмпирически обосновывают предложенную уточненную теоретическую модель уязвимостей. При этом анализ матрицы интеркорреляций показал, что шкалы методики «УкСИ» обладают хорошей избирательностью. Наибольшая специфичность наблюдается у шкал, измеряющих уязвимости к техникам прямого давления («Imposture», «Scareware») и коммуникативного воздействия («Vishing», «Phishing»). Это свидетельствует о том, что данные шкалы измеряют именно специфические конструкты, а не общую личностную тревожность или социальность. Также некоторые из шкал методики «УкСИ», например, шкала «Уязвимость к технике “Bait”», показали устойчивые связи с несколькими базовыми тенденциями одновременно (экстраверсия, интроверсия, сензитивность), что отражает сложную, многомерную природу этих уязвимостей, когда одна и та же техника социальной инженерии может эксплуатировать разные психологические механизмы.

Таблица 3 / Table 3

Результаты корреляционного анализа данных с применением критерия Пирсона для проверки конвергентной и дискриминантной валидностей методики «УкСИ» (N = 185)
Results of Pearson correlation analysis for assessing the convergent and discriminant validity of the “UkSI” methodology (N = 185)

Переменные / Variables	Корреляции (попарное удаление пропущенных данных) / Correlations (casewise deletion of missing data)								
	Устрашение / Scareware	Самозванец / Imposture	Предлог / Offer	Выуживание / Phishing	Примanка / Bait	Вишинг / Vishing	Услуга за услугу / Quid Pro Quo	Дорожное яблоко / Apple of the Road	Ригидность / Rigidity
Шкала тревожности / Anxiety scale	**0,76**	0,20	0,07	**0,58**	**0,43**	**–0,52**	**0,37**	0,16	0,05
Шкала стеничности (агрессивности) / Stenic (aggressiveness) scale	0,22	**0,92**	**0,32**	0,23	**0,31**	**–0,32**	0,23	0,03	0,24
Шкала интроверсии / Introversion scale	**–0,66**	**–0,28**	0,22	**–0,66**	**–0,71**	**0,84**	**–0,58**	**–0,44**	0,21
Шкала экстраверсии /	**0,57**	**0,27**	–0,12	**0,81**	**0,74**	**–0,82**	**0,54**	**0,44**	0,01

Extraversion scale									
Шкала сензитивности / Sensitivity scale	**0,74**	**0,56**	0,16	**0,68**	**0,71**	**–0,77**	**0,62**	**0,37**	0,18
Шкала спонтанности / Spontaneity scale	**0,38**	**0,33**	–0,15	**0,46**	**0,54**	**–0,64**	**0,48**	**0,52**	–0,03
Шкала ригидности / Rigidity scale	–0,07	0,13	**0,32**	–0,04	–0,12	0,11	–0,02	0,03	**0,91**
Шкала лабильности / Lability scale	–0,05	0,09	**0,63**	0,00	–0,06	0,11	0,09	–0,20	**0,44**

Примечание: выделенные полужирным шрифтом корреляции значимы при $p < 0,001$.
Note: bold marked correlations are significant at $p < 0,001$.

Многомерный дисперсионный анализ (MANOVA) показал наличие статистически значимых различий между кластерами по всем исследуемым параметрам ($p < 0,001$). Наибольшие различия между группами обнаружены по уязвимости к таким техникам, как «Scareware» ($F = 60,93$, $p < 0,001$) и «Vishing» ($F = 54,61$, $p < 0,001$). Также были обнаружены значимые различия по уровню ригидности ($F = 42,84$, $p < 0,001$). Более подробнее информация приведена в табл. 4.

Таблица 4 / Table 4

Результаты дисперсионного анализа (MANOVA) по результатам опроса с помощью методики «УкСИ»
Results of the Analysis of Variance (MANOVA) based on the survey data obtained using the "UkSI" method

В отношении уязвимости к технике «Самозванец» / Concerning vulnerability to the Imposture technique					
Effect	Степени свободы / Degr. of Freedom	Сумма квадратов / Sum of Squares	Дисперсия / Mean Squares	F	p-value
Intercept	1	**88254,56**	**88254,56**	**4948,7**	**0,00**
Cluster	4	**2383,29**	**595,82**	**33,4**	**0,00**
Error	180	3210,10	17,83		
Total	184	5593,38			
В отношении уязвимости к технике «Предлог» / Concerning vulnerability to the Offer technique					
Intercept	1	**100616,2**	**100616,2**	**5938,9**	**0,0000**
Cluster	4	**1645,0**	**411,2**	**24,2**	**0,0000**
Error	180	3049,5	16,9		
Total	184				
В отношении уязвимости к технике «Выуживание» /					

Concerning vulnerability to the Phishing technique					
Intercept	1	**137692,4**	**137692,4**	**8753,9**	**0,0000**
Cluster	4	**1141,6**	**285,4**	**18,145**	**0,0000**
Error	180	2831,3	15,7		
Total	184	3972,9			
В отношении уязвимости к технике «Приманка» / Concerning vulnerability to the Bait technique					
Intercept	1	**65888,29**	**65888,29**	**3963,0**	**0,00**
Cluster	4	**2447,13**	**611,78**	**36,797**	**0,00**
Error	180	2992,62	16,63		
Total	184	5439,75			
В отношении уязвимости к технике «Вишинг» / Concerning vulnerability to the Vishing technique					
Intercept	1	**68727,34**	**68727,34**	**6102,0**	**0,00**
Cluster	4	**2460,10**	**615,02**	**54,606**	**0,00**
Error	180	2027,34	11,26		
Total	184	4487,44			
В отношении уязвимости к технике «Устрашение» / Concerning vulnerability to the Scareware technique					
Intercept	1	**60777,56**	**60777,56**	**3796,5**	**0,00**
Cluster	4	**3901,47**	**975,37**	**60,927**	**0,00**
Error	180	2881,59	16,01		
Total	184	6783,06			
В отношении уязвимости к технике «Услуга за услугу» / Concerning vulnerability to the Quid Pro Quo technique					
Intercept	1	**83603,35**	**83603,35**	**4909,4**	**0,00**
Cluster	4	**2369,73**	**592,43**	**34,790**	**0,00**
Error	180	3065,22	17,03		
Total	184	5434,95			
В отношении уязвимости к технике «Дорожное яблоко» / Concerning vulnerability to the The Apple of the Road technique					
Intercept	1	**59973,01**	**59973,01**	**3439,2**	**0,0000**
Cluster	4	**1429,13**	**357,28**	**20,489**	**0,0000**
Error	180	3138,85	17,44		
Total	184	4567,98			
В отношении ригидности / For rigidity					
Intercept	1	**467743,5**	**467743,5**	**23428**	**0,00**
Cluster	4	**3421,0**	**855,2**	**42,84**	**0,00**
Error	180	3593,6	20,0		
Total	184	7014,6			

Примечание: полужирным шрифтом в таблице выделены статистически значимые эффекты (уровень значимости $p < 0,001$).
Note: boldface in the table indicates statistically significant effects (significance level $p < 0.001$).

Для конкретизации профилей риска («мишеней для манипуляции») был применен кластерный анализ в два этапа: на первом этапе использовался иерархический кластерный анализ (метод Уорда) для определения оптимального числа кластеров, на втором этапе для точного распределения респондентов по кластерам использовался метод k-средних. В качестве переменных для кластеризации использовались показатели уязвимости по 8 техникам социальной инженерии и шкала ригидности. На основании кластерного анализа были выделены 5 профилей риска (табл. 5).

В контексте дальнейшей интерпретации и описания результатов, полученным профилям условно были присвоены следующие номера: профиль 1 — ригидно-отзывчивый, профиль 2 — ригидно-импульсивный, профиль 3 — адаптивно-устойчивый, профиль 4 — смешанный, профиль 5 — ригидно-осторожный.

Таблица 5 / Table 5

Результаты кластерного анализа на основе опроса с применением методики «УкСИ»
Findings from cluster analysis of "UkSI" questionnaire data

Кластер / Cluster	n	%	Профиль риска / Vulnerability Profile
1	48	30,2	Адаптивно-устойчивый
2	29	18,2	Ригидно-импульсивный
3	37	23,3	Ригидно-осторожный
4	57	35,8	Ригидно-отзывчивый
5	31	19,5	Смешанный профиль

Для выявления статистически значимых попарных различий между выделенными профилями риска был применен апостериорный анализ, по Тьюки (Tukey HSD), который позволил выявить следующие достоверные статистически значимые различия (табл. 6).

Таблица 6 / Table 6

Результаты апостериорного анализа по Тьюки (Tukey HSD)
на основе опроса с применением методики «УкСИ»
Post hoc Tukey HSD analysis of the "UkSI" survey data

№ строки / Cell No	*Переменная «Уязвимость к технике социальной инженерии "Bait"»; Межгрупповая дисперсия ошибки = 16,626 / Variable «Vulnerability to the social engineering technique "Bait"»; Error: Between MS = 16,626*					
	Кластер / Cluster	{1} 20,958	{2} 26,355	{3} 17,167	{4} 18,327	{5} 14,556
1	1		**0,000017**	**0,000628**	**0,012888**	**0,000017**
2	2	**0,000017**		**0,000017**	**0,000017**	**0,000017**

3	3	**0,000628**	**0,000017**		0,735575	0,111498
4	4	**0,012888**	**0,000017**	0,735575		**0,001088**
5	5	**0,000017**	**0,000017**	0,111498	**0,001088**	
№ строки / Cell No	*Переменная «Уязвимость к технике социальной инженерии "Vishing"»; межгрупповая дисперсия ошибки = 11,263 / Variable «Vulnerability to the social engineering technique "Vishing"»; Error: Between MS = 11,263*					
	Кластер / Cluster	{1} 23,021	{2} 25,387	{3} 16,333	{4} 19,918	{5} 14,778
1	1		**0,018819**	**0,000017**	**0,000067**	**0,000017**
2	2	**0,018819**		**0,000017**	**0,000017**	**0,000017**
3	3	**0,000017**	**0,000017**		**0,000055**	0,404873
4	4	**0,000067**	**0,000017**	**0,000055**		**0,000017**
5	5	**0,000017**	**0,000017**	0,404873	**0,000017**	
№ строки / Cell No	*Переменная «Уязвимость к технике социальной инженерии "Scareware"»; межгрупповая дисперсия ошибки = 16,009 / Variable «Vulnerability to the social engineering technique "Scareware"»; Error: Between MS = 16,009*					
	Кластер / Cluster	{1} 23,646	{2} 24,871	{3} 13,867	{4} 18,163	{5} 12,963
1	1		0,673135	**0,000017**	**0,000017**	**0,000017**
2	2	0,673135		**0,000017**	**0,000017**	**0,000017**
3	3	**0,000017**	**0,000017**		**0,000051**	0,914345
4	4	**0,000017**	**0,000017**	**0,000051**		**0,000018**
5	5	**0,000017**	**0,000017**	0,914345	**0,000018**	
№ строки / Cell No	*Переменная «Уязвимость к технике социальной инженерии "Quid Pro Quo"»; межгрупповая дисперсия ошибки = 17,029 / Variable «Vulnerability to the social engineering technique "Quid Pro Quo"»; Error: Between MS = 17,029*					
	Кластер / Cluster	{1} 22,833	{2} 28,968	{3} 20,200	{4} 20,449	{5} 17,222
1	1		**0,000017**	**0,048108**	**0,035939**	**0,000017**
2	2	**0,000017**		**0,000017**	**0,000017**	**0,000017**
3	3	**0,048108**	**0,000017**		0,998993	0,051058
4	4	**0,035939**	**0,000017**	0,998993		**0,009753**
5	5	**0,000017**	**0,000017**	0,051058	**0,009753**	
№ строки / Cell No	*Переменная «Уязвимость к технике социальной инженерии "The Apple of the Road"»; межгрупповая дисперсия ошибки = 17,438 / Variable «Vulnerability to the social engineering technique "The Apple of the Road"»; Error: Between MS = 17,438*					
	Кластер / Cluster	{1} 21,375	{2} 21,935	{3} 16,333	{4} 19,245	{5} 14,000
1	1		0,977694	**0,000019**	0,087977	**0,000017**
2	2	0,977694		**0,000019**	**0,040020**	**0,000017**
3	3	**0,000019**	**0,000019**		**0,022143**	0,217223
4	4	0,087977	**0,040020**	**0,022143**		**0,000019**

5	5	**0,000017**	**0,000017**	0,217223	**0,000019**	
№ строки / Cell No	*Переменная «Уязвимость к технике социальной инженерии “Imposture”»; межгрупповая дисперсия ошибки = 17,834 / Variable «Vulnerability to the social engineering technique “Imposture”»; Error: Between MS = 17,834*					
	Кластер / Cluster	{1} 23,646	{2} 29,258	{3} 20,700	{4} 22,041	{5} 17,037
1	1		**0,000017**	**0,022860**	0,332794	**0,000017**
2	2	**0,000017**		**0,000017**	**0,000017**	**0,000017**
3	3	**0,022860**	**0,000017**		0,647249	**0,009517**
4	4	0,332794	**0,000017**	0,647249		**0,000024**
5	5	**0,000017**	**0,000017**	**0,009517**	**0,000024**	
№ строки / Cell No	*Переменная «Уязвимость к технике социальной инженерии “Offer”»; межгрупповая дисперсия ошибки = 16,942 / Variable «Vulnerability to the social engineering technique “Offer”»; Error: Between MS = 16,942*					
	Кластер / Cluster	{1} 23,396	{2} 28,323	{3} 18,667	{4} 26,041	{5} 23,889
1	1		**0,000019**	**0,000024**	**0,013490**	0,987581
2	2	**0,000019**		**0,000017**	0,111081	**0,000423**
3	3	**0,000024**	**0,000017**		**0,000017**	**0,000033**
4	4	**0,013490**	0,111081	**0,000017**		0,186713
5	5	0,987581	**0,000423**	**0,000033**	0,186713	
№ строки / Cell No	*Переменная «Уязвимость к технике социальной инженерии “Phishing”»; межгрупповая дисперсия ошибки = 15,729 / Variable «Vulnerability to the social engineering technique “Phishing”»; Error: Between MS = 15,729*					
	Кластер / Cluster	{1} 24,333	{2} 29,935	{3} 26,333	{4} 29,367	{5} 30,778
1	1		**0,000017**	0,192398	**0,000017**	**0,000017**
2	2	**0,000017**		**0,003604**	0,971250	0,928645
3	3	0,192398	**0,003604**		**0,008592**	**0,000245**
4	4	**0,000017**	0,971250	**0,008592**		0,573070
5	5	**0,000017**	0,928645	**0,000245**	0,573070	
№ строки / Cell No	*Переменная «Ригидность»; межгрупповая дисперсия ошибки = 19,964 / Variable «Rigidity»; Error: Between MS = 19,964*					
	Кластер / Cluster	{1} 46,188	{2} 55,129	{3} 47,800	{4} 56,184	{5} 54,111
1	1		**0,000017**	0,529383	**0,000017**	**0,000017**
2	2	**0,000017**		**0,000017**	0,842264	0,909537
3	3	0,529383	**0,000017**		**0,000017**	**0,000018**
4	4	**0,000017**	0,842264	**0,000017**		0,298515
5	5	**0,000017**	0,909537	**0,000018**	0,298515	

Примечание: в таблице приведены аппроксимированные вероятности для апостериорных тестов, число степеней свободы = 180. Полужирным шрифтом отмечены значения, не

превышающие выбранный уровень значимости (например, $p < 0,001$). Это указывает на то, что различия между соответствующими кластерами статистически значимы.
Note: the table shows the approximate probabilities for the post hoc tests, degrees of freedom = 180. Boldface indicates p-values that do not exceed the chosen significance level (e.g., $p < 0.001$), meaning that the differences between the respective clusters are statistically significant.

Как видно из сводной табл. 6, профиль 2 продемонстрировал наивысшую уязвимость к технике «Bait», достоверно отличаясь от всех остальных профилей ($p < 0,001$). Профиль 1 также показал высокую уязвимость, значимо превышая профили 3, 4 и 5. Профили 3 и 4 не показали различий между собой ($p = 0,736$), но оба были значимо менее уязвимы, чем профили 1 и 2. Профиль 5 показал наименьшую уязвимость к технике «Bait», достоверно отличаясь от профилей 1, 2 и 4.

Относительно уязвимости к технике «Vishing», наибольшую уязвимость вновь проявили профили 2 и 1. Профили 3 и 5 показали наименьшую уязвимость, при этом не отличаясь друг от друга ($p = 0,405$). Это ключевой результат, объединяющий адаптивных и ригидно-осторожных респондентов в их устойчивости к телефонным манипуляциям. Профиль 4 «занял» среднюю позицию, уступая профилям 1 и 2, но превосходя профили 3 и 5.

Касательно уязвимости к технике «Scareware», картина аналогична предыдущей: профили 1 и 2 — наиболее уязвимы (без различий между собой, $p = 0,673$). Профили 3 и 5 — наименее уязвимы (без различий между собой, $p = 0,914$). Это подтверждает идею о том, что как когнитивная гибкость (профиль 3), так и избирательная ригидная бдительность (профиль 5) являются защитой против тактик запугивания. Профиль 4 вновь занимает промежуточное положение.

В отношении уязвимости к технике «Quid Pro Quo», профиль 2 обладает ярко выраженной, наивысшей уязвимостью. Профили 3 и 4 демонстрируют средний и идентичный уровень уязвимости ($p = 0,999$), что является их отличительной чертой. Профили 1 и 5 показали наименьшую уязвимость, при этом профиль 1 значимо отличается от профиля 2, а профиль 5 — от профилей 2 и 4.

Уязвимость к технике «The Apple of the Road». В данном случае профили 1 и 2 имеют схожий, высокий уровень уязвимости ($p = 0,978$). Профиль 3 показал достоверно более низкую уязвимость по сравнению с профилями 1, 2 и 4. Профиль 5 имеет наименьшую уязвимость, значимо отличаясь от всех, кроме профиля 3 ($p = 0,217$).

Уязвимость к технике «Imposture»: профиль 2 — наивысшая уязвимость. Профили 1, 3 и 4 образуют группу со средним уровнем уязвимости, внутри которой нет значимых различий ($p > 0,05$ для пар 1—4, 3—4, 1—3). Профиль 5 — наименьшая уязвимость.

Уязвимость к технике «Offer». Данная техника выявляет уникальную структуру различий. Профили 1 и 5 демонстрируют схожую, высокую уязвимость ($p = 0,988$). Это важное открытие, объединяющее ригидно-отзывчивых и ригидно-осторожных респондентов в их восприимчивости к соблазнительным предложениям. Профили 2 и 4 также не отличаются по высокому уровню уязвимости ($p = 0,111$). Профиль 3 показал наименьшую уязвимость, достоверно отличаясь от всех остальных профилей.

При рассмотрении результатов уязвимости к технике «Phishing», наибольшую уязвимость проявляют профили 2, 4 и 5, не различаясь между собой ($p > 0,05$). Профиль 1 имеет среднюю уязвимость. Профиль 3 вновь демонстрирует наименьшую уязвимость, значимо отличаясь от профилей 2, 4 и 5.

Отметим, что профили 2, 4 и 5 имеют статистически схожий, высокий уровень ригидности ($p > 0,05$ для попарных сравнений). Это подтверждает их принадлежность к «ригидным» профилям, несмотря на разницу в проявлениях уязвимостей. Профили 1 и 3 демонстрируют статистически схожий, низкий уровень ригидности ($p = 0,529$). Это ключевой результат, указывающий на то, что низкая ригидность может быть связана как с адаптивной устойчивостью (профиль 3), так и с ригидно-отзывчивым паттерном (профиль 1), где иные механизмы (например, потребность в одобрении) определяют уязвимость.

Таким образом, методами кластерного анализа и многомерного дисперсионного анализа (MANOVA) с апостериорными сравнениями Тьюки показано, что уязвимость к различным техникам социальной инженерии имеет многомерную структуру и связана с различными психологическими механизмами. Обнаружена нелинейная связь между ригидностью и уязвимостями к техникам социальной инженерии.

Обсуждение результатов

Проведенное исследование было направлено на разработку и первичную апробацию авторской методики диагностики уязвимости к техникам социальной инженерии (УкСИ), основанной на индивидуально-типологическом подходе Л.Н. Собчик. Полученные результаты позволяют утверждать, что поставленные задачи решены, а гипотеза исследования нашла свое эмпирическое подтверждение.

Прежде всего, анализ психометрических свойств методики «УкСИ» свидетельствует о ее высокой надежности и валидности. Значение коэффициента α Кронбаха (0,902) указывает на отличную внутреннюю согласованность пунктов опросника, что является необходимым условием для его использования в исследовательских и диагностических целях. Важнейшим результатом является подтверждение конвергентной и дискриминантной валидности. Обнаруженные сильные и статистически значимые корреляции между шкалами «УкСИ» и концептуально близкими шкалами опросника «ИТО» (например, «Уязвимость к технике “Imposture”» и «Агрессивность» ($r = 0,92$); «Уязвимость к технике “Vishing”» и «Интроверсия» ($r = 0,84$)) эмпирически обосновывают предложенную теоретическую модель. Это означает, что методика действительно измеряет целевые конструкты — специфические уязвимости, обусловленные глубинными личностными тенденциями, а не просто фиксирует общую тревожность или социальность.

Ключевым результатом работы стало выделение пяти устойчивых профилей риска, что подтверждает основную гипотезу о существовании статистически значимой связи между профилем ведущих личностных тенденций и уязвимостью к социальной инженерии. Результаты кластерного и дисперсионного анализа (MANOVA) демонстрируют, что уязвимость носит не случайный, а системный и многомерный характер. Выявленные профили — «Ригидно-импульсивный», «Ригидно-отзывчивый», «Ригидно-осторожный», «Адаптивно-устойчивый» и «Смешанный» — обладают уникальными конфигурациями «слабых мест».

Особый интерес представляет нелинейная роль ригидности в структуре уязвимости. Как и предполагалось, высокий уровень ригидности является системообразующим фактором для нескольких профилей риска («Ригидно-импульсивного», «Ригидно-отзывчивого», «Ригидно-осторожного»), однако его влияние опосредовано другими личностными тенденциями. Например, в «Ригидно-импульсивном» профиле ригидность в стрессе приводит к сбросу когнитивной нагрузки и необдуманным действиям, а в «Ригидно-осторожном» — создает иллюзию контроля и «когнитивную слепоту» к сложным, многоходовым атакам. При этом низкий уровень ригидности сам по себе не является гарантией устойчивости, что демонстрирует «Ригидно-отзывчивый» профиль, где уязвимость определяется гипертрофированной потребностью в социальном одобрении.

Результаты апостериорного анализа (Tukey HSD) детально раскрывают специфику каждого профиля, подтверждая принцип избирательности уязвимости. Так, было установлено, что техника «Scareware» наиболее эффективна против профилей с высокой тревожностью, в первую очередь против профиля 2 («Ригидно-импульсивный») и профиля 1 («Ригидно-отзывчивый»). В то же время, техника «Vishing» показала наибольшее воздействие на профиль 1 («Ригидно-отзывчивый») и профиль 2 («Ригидно-импульсивный»), что связывает эту уязвимость с сочетанием интровертированности и ригидности, характерным для этих групп. Напротив, «Адаптивно-устойчивый» профиль последовательно демонстрирует наименьшую уязвимость к большинству техник, что подтверждает гипотезу о когнитивной гибкости как ключевом защитном факторе. При этом такие техники, как «Phishing», оказались эффективны против широкого спектра профилей («Ригидно-импульсивный», «Ригидно-отзывчивый», «Смешанный» профиль), что подчеркивает их универсальность и высокую опасность, так как они эксплуатируют более общие модели поведения (например, откликаемость на внешние стимулы), присущие разным личностным конфигурациям.

Обнаруженные закономерности расширяют существующие представления о природе человеческого фактора в кибербезопасности. В отличие от редукционистских подходов, связывающих уязвимость с изолированными чертами, предлагаемая модель демонстрирует, что мишенью для манипуляции является целостный паттерн взаимодействия индивидуально-типологических свойств. Это объясняет, почему традиционные тренинги по осведомленности, не учитывающие личностные особенности, имеют ограниченную эффективность.

Заключение

В рамках данного исследования была успешно разработана, описана и прошла первичную апробацию авторская методика «УкСИ», направленная на диагностику индивидуальной уязвимости к техникам социальной инженерии на основе теории ведущих тенденций Л.Н. Собчик.

Подтверждена основная гипотеза исследования: установлено существование статистически значимой связи между профилем ведущих личностных тенденций и специфическими уязвимостями к манипулятивным техникам. Эмпирически доказано, что различные конфигурации личностных свойств (агрессивность, тревожность, интроверсия,

ригидность и др.) обусловливают избирательную восприимчивость к определенным сценариям атак, таким как «Самозванец», «Устрашение» или «Вишинг».

Методами кластерного анализа выделены пять устойчивых профилей риска («ригидно-импульсивный», «ригидно-отзывчивый», «ригидно-осторожный», «адаптивно-устойчивый» и «смешанный»), что подтверждает конструктную валидность и диагностическую ценность методики. Показано, что ригидность играет ключевую, но неоднозначную роль, выступая либо катализатором уязвимости, либо основой для избирательной бдительности.

Теоретическая значимость работы заключается в расширении понимания психологической природы уязвимости в кибербезопасности за счет перехода от анализа изолированных черт к целостным личностным профилям. Практическая ценность состоит в том, что разработанная методика открывает путь к созданию персонализированных программ повышения осведомленности и тренировок по информационной безопасности, учитывающих индивидуальные «зоны риска» пользователя.

Перспективы дальнейших исследований видятся в увеличении выборки и ее стратификации, в проведении лонгитюдных исследований для оценки прогностической валидности методики, а также в разработке и апробации на основе выделенных профилей риска адресных тренинговых и коррекционных программ.

Ограничение. Из-за определенных технических ограничений на платформе «Onlinetestpad», озвученные в статье профили риска определялись посредством автоматического расчета в программе Excel для работы с электронными таблицами от компании Microsoft. При личном обращении к авторам методики в ответ будет предоставлен необходимый инструментарий для дальнейших расчетов.

Limitations. Due to certain technical limitations on the “Onlinetestpad” platform, the risk profiles mentioned in the article were determined through automatic calculation in Microsoft Excel. When contacting the methodology authors directly, the necessary tools for further calculations will be provided upon request.

Список источников / References

1. Власова, Н.В., Буслаева, Е.Л. (2022). Психологические особенности лиц, склонных к кибервиктимному поведению. *Психология и право, 12*(2), 194—206. https://doi.org/10.17759/psylaw.2022120214
   Vlasova, N.V., Buslaeva, E.L. (2022). Psychological Features of Individuals Prone to Cyber Victimization. *Psychology and Law, 12*(2), 194—206. (In Russ.). https://doi.org/10.17759/psylaw.2022120214
2. Вознесенская, К.В. (2025). Психологические особенности киберпреступного поведения и его детерминанты. В: А.А. Марголис, Н.В. Дворянчиков, Н.В. Богданович, О.Р. Бусарова, М.Г. Дебольский, Е.Г. Дозорцева, Л.М. Карнозова, И.Н. Коноплева, Е.Г. Пастухова, Ф.С. Сафуанов (Ред.), *Межвузовская научно-практическая интернет-конференция по юридической психологии. Сборник тезисов участников научно-практической интернет-конференции по юридической психологии (15-23 мая 2025 года)* (с. 82—85). М.: ФГБОУ ВО МГППУ. URL: https://psyjournals.ru/nonserialpublications/jurpsyconf2025/ (дата обращения: 05.11.2025).
   Voznesenskaya, K.V. (2025). Psychological Features of Cybercriminal Behavior and Its

Determinants. In: A.A. Margolis, N.V. Dvoryanchikov, N.V. Bogdanovich, O.R. Busarova, M.G. Debolsky, E.G. Dozortseva, L.M. Karnozova, I.N. Konopleva, E.G. Pastukhova, F.S. Safuanov (Eds.), *Interuniversity Scientific-Practical Internet Conference on Legal Psychology: Collection of Abstracts from the Scientific-Practical Internet Conference on Legal Psychology (May 15-23, 2025)* (pp. 82—85). Moscow: MSUPE Publ. (In Russ.). URL: https://psyjournals.ru/nonserialpublications/jurpsyconf2025/ (viewed: 05.11.2025).

3. Монахова, Э., Городничева, Ю.М., Морозова, А.Н., Шестакова, А.Н., Моисеева, В.В., Ключарев, В.А. (2024). Доверие к манипулятивной информации: от восприятия к принятию решений. *Мониторинг общественного мнения: экономические и социальные перемены,* 3, 42—66. https://doi.org/10.14515/monitoring.2024.3.2544
   Monakhova, E., Gorodnicheva, J.M., Morozova, A.N., Shestakova, A.N., Moiseeva, V.V., Klucharev, V.A. (2024). Trust in Manipulative Information: From Perception to Decision Making. *Monitoring of Public Opinion: Economic and Social Changes,* 3, 42—66. (In Russ.). https://doi.org/10.14515/monitoring.2024.3.2544
4. Розенова, М.И., Огнев, А.С., Лихачева, Э.В. (2025). Психологические механизмы деструктивного манипулирования и стратегии профилактики цифрового мошенничества. *Современная зарубежная психология*, *14*(2), 26—37. https://doi.org/10.17759/jmfp.2025140203
   Rozenova, M.I., Ognev, A.S., Likhacheva, E.V. (2025). Psychological mechanisms of destructive manipulation and strategies for preventing digital fraud. *Journal of Modern Foreign Psychology, 14*(2), 26—37. (In Russ.). https://doi.org/10.17759/jmfp.2025140203
5. Розова, Е.А., Хитина, А.А., Еремеева, А.С., Семенова, Л.Э. (2020). Склонность к манипуляции и потребность в острых ощущениях лиц женского и мужского пола. *Нижегородский психологический альманах, 1*(2), 135—143. URL: https://www.elibrary.ru/zwgylp (дата обращения: 05.11.2025).
   Rozova, E.A., Khitina, A.A., Eremeeva, A.S., Semenova, L.E. (2020). The tendency to manipulation and the need for thrills of female and male persons. *Nizhny Novgorod Psychological Almanac, 1*(2), 135—143. (In Russ.). URL: https://www.elibrary.ru/zwgylp (viewed: 05.11.2025).
6. Собчик, Л.Н. (2022). Теория и практика психологии индивидуальности. *Психологический журнал, 43*(6), 119—130. https://doi.org/10.31857/S020595920023651-2
   Sobchik, L.N. (2022). Theory and practice of psychology of individuality. *Psychological Journal, 43*(6), 119—130. (In Russ.). https://doi.org/10.31857/S020595920023651-2
7. Milgram, S. (1963). Behavioral study of obedience. *The Journal of Abnormal and Social Psychology, 67*(4), 371—378.
8. Sleep, C.E., Lynam, D.R., Miller, J.D. (2021). A comparison of the validity of very brief measures of the big five / fivefactor model of personality. *Assessment, 28*(3), 739—758. http://doi.org/10.1177/1073191120939160
9. Stanovich, K.E., West, R.F. (2000). Individual differences in reasoning: Implications for the rationality debate? *Behavioral and Brain Sciences, 23*(5), 645—665. http://doi.org/10.1017/s0140525x00003435
10. Starcke, K., Brand, M. (2012). Decision making under stress: A selective review. *Neuroscience & Biobehavioral Reviews, 36*(4), 1228—1248. http://doi.org/10.1016/j.neubiorev.2012.02.003

Информация об авторах

Ирина Фасхутовна Нурмухаметова, кандидат психологических наук, доцент кафедры общей психологии, Высшая школа философии, психологии и социологии, Институт гуманитарных и социальных наук, Уфимский университет науки и технологий (ФГБОУ ВО УУНиТ), Уфа, Российская Федерация, ORCID: https://orcid.org/0000-0003-2029-618X4, e-mail: if44@bk.ru

Эрнест Альбертович Нурмухаметов, кандидат психологических наук, психолог координационного центра, Уфимский университет науки и технологий (ФГБОУ ВО УУНиТ), Уфа, Российская Федерация, ORCID: https://orcid.org/0000-0003-2880-1275, e-mail: misall@mail.ru

Information about the authors

Irina F. Nurmukhametova, Candidate of Science (Psychology), Associate Professor of the Department of General Psychology, Higher School of Philosophy, Psychology and Sociology, Institute of Humanities and Social Sciences, Ufa University of Science and Technology, Ufa, Russian Federation, ORCID: https://orcid.org/0000-0003-2029-618X4, e-mail: if44@bk.ru

Ernest A. Nurmukhametov, Candidate of Science (Psychology), Psychologist at the Coordination Center, Ufa University of Science and Technology, Ufa, Russian Federation, ORCID: https://orcid.org/0000-0003-2880-1275, e-mail: misall@mail.ru

Вклад авторов

Нурмухаметов Э.А. — идея исследования; аннотирование, написание и оформление рукописи; планирование исследования; описание результатов статистико-математической обработки данных.

Нурмухаметова И.Ф. — проведение эмпирического исследования; контроль за проведением исследования, сбор и анализ данных; визуализация результатов исследования.

Все авторы приняли участие в обсуждении результатов и согласовали окончательный текст рукописи.

Contribution of the authors

Ernest A. Nurmukhametov — research concept; manuscript annotation, writing, and formatting; research planning; description of the results of statistical and mathematical data processing.

Irina F. Nurmukhametova — conducting the empirical research; research supervision, data collection and analysis; visualization of the research results.

All authors participated in the discussion of the results and approved the final text of the manuscript.

Конфликт интересов

Авторы заявляют об отсутствии конфликта интересов.

Conflict of interest

The authors declare no conflict of interest.

Нурмухаметова И.Ф., Нурмухаметов Э.А. (2026)
Разработка и апробация методики диагностики уязвимости к техникам социальной инженерии на основе индивидуально-типологического подхода Л.Н. Собчик
Психология и право, 16(1), 240—265.

Nurmukhametova I.F., Nurmukhametov E.A. (2026)
Development and testing of a methodology for diagnosing vulnerability to social engineering techniques based on L.N. Sobchik's individual-typological approach
Psychology and Law, 16(1), 240—265.

Поступила в редакцию 25.11.2025
Поступила после рецензирования 16.01.2026
Принята к публикации 26.01.2026
Опубликована 30.03.2026

Received 2025.11.25
Revised 2026.01.16
Accepted 2026.01.26
Published 2026.03.30