ЛИЧНОСТНЫЕ ОСОБЕННОСТИ ЖЕРТВ ТЕЛЕФОННОГО МОШЕННИЧЕСТВА

О.Н. ПЕРВУШИНА, А.А. ФЁДОРОВ
Новосибирский государственный университет

В статье представлены результаты исследования, посвященного изучению личностных особенностей жертв телефонного мошенничества (вишинга). В нем приняли участие 374 человека. Приблизительно 86% участников исследования (n = 321) сталкивались с попытками мошенничества, из них мошенникам удалось обмануть 18% (n = 57). Установлено, что по сравнению с теми, кому удалось избежать обмана, жертвы вишинга характеризуются более высокими уровнями доброжелательности, доверчивости и внушаемости, а также менее высоким уровнем эмоциональной стабильности. Хотя эти же личностные особенности более характерны для женщин, чем для мужчин, тем не менее процент обманутых среди женщин статистически значимо не отличается от процента обманутых среди мужчин. Возрастные различия между теми, кто стал жертвой мошенников, и теми, кому удалось избежать обмана, также отсутствуют. При этом чем старше люди, тем в большей степени они уверены: человек сам виноват в том, что его обманули. В рамках построенной авторами модели значимыми для предсказания возможности быть обманутым оказались доброжелательность и доверчивость. Данная модель характеризуется высокой специфичностью, но низкой чувствительностью, а это не позволяет рассматривать указанные личностные особенности в качестве предикторов того, что человека действительно обманут. Скорее низкие уровни доверчивости и доброжелательность снижают риск быть обманутым. Делается вывод: важным аспектом работы с потенциальными жертвами вишинга является повышение финансовой грамотности и развитие поведенческих навыков, уменьшающих риск стать объектом манипуляций кибермошенников.

Ключевые слова: телефонное мошенничество, кибермошенничество, вишинг, доверчивость, внушаемость, Большая пятерка.

Проблема мошенничества существовала во все времена человеческой истории, и, вероятно, не будет большой ошибкой сказать, что с развитием цивилизации формы мошенничества становились только изощреннее. В настоящее время особое место в его способах и методах играет кибермошенничество. Размах и темпы этого вида мошенничества впечатляют. РИА Новости, ссылаясь на материалы Центробанка, сообщило, что за девять месяцев 2021 г. злоумышленники похитили у клиентов банков 9 млрд руб., что в 1,3 раза больше, чем за аналогичный период 2020 г. Ежегодно от мошенников страдают сотни тысяч россиян. В подавляющем большинстве случаев преступники связываются со своими жертвами *по телефону* и используют методы социальной инженерии, т.е. с помощью психологических приемов втираются к людям в доверие[1].

В 2021 г. мошенникам удалось провести свыше миллиона банковских операций без согласия клиентов. Это на 33,8% больше, чем в 2020 г., и на 326% больше, чем в 2017 г.[2]. Статистика свидетельствует, что речь идет о проблеме мирового масштаба. С 2001 г. число жертв онлайн-преступлений увеличилось в 17 раз (с 6 до 97 жертв в час), а финансовые потери выросли почти в 400 раз (с 2 тыс. до 788 тыс. долларов в час).

[1] Названы новые схемы кибермошенников в 2022 г. (2022, 8 января) // ПРАЙМ website: https://1prime.ru/telecommunications_and_technologies/20220108/835716523.html

[2] Сколько и как крадут деньги с банковских карт россиян. (2022, 6 июня) // Тинькофф Журнал website: https://journal.tinkoff.ru/short/cyber-fraud-2021/

В общей сложности киберпреступность затронула не менее 6 502 323 жертв, которые потеряли в совокупности 26 116 млн долларов США за 21-летний период[3].

Почти половину всех хищений кибермошенники совершают с помощью психологических трюков: жертвы сами переводят деньги или сообщают необходимые для кражи сведения. Основным приемом злоумышленников является социальная инженерия – психологический инструмент, направленный на манипулирование людьми, заставляющий их действовать в целях злоумышленников. Этот метод связан с развитием и совершенствованием информационных технологий. Основной целью социальной инженерии является получение доступа к конфиденциальной информации, паролям, банковским данным и другим защищенным сведениям (Комаров, 2013).

Крупнейший авторитет по проблеме защиты от мошенничества и в сфере развития социальной инженерии Кевин Митник полагает безопасность иллюзией, которая иногда может быть хуже легковерия, наивности или невежества (Митник, Саймон, 2004). Альберту Эйнштейну приписывают фразу (хотя и имеются сомнения, что он ее действительно произносил): «Есть только две бесконечные вещи: Вселенная и глупость. Хотя насчет Вселенной я не вполне уверен».

Почему люди подчиняются манипуляторам? Почему они зачастую становятся легкой добычей для мошенников? К ответам на эти вопросы необходимо подходить, имея в виду и особенности ситуации, в которой осуществляется жульничество, и способы, которыми пользуется мошенник, и его способности к управлению собеседником. Немаловажную роль в успехе мошенничества играет личность потенциальной жертвы.

О влиянии ситуации на поведение человека и о методах, с помощью которых можно манипулировать его поведением, написано немало статей и книг. В многочисленных исследованиях показано, как ситуативные факторы становятся предикторами поведения, а множество манипулятивных приемов увеличивает вероятность человека стать жертвой обмана, нежелательного влияния. При этом шансы сделаться объектом манипуляции у разных людей различны. Вклад индивидуально-психологических, личностных особенностей в поведение человека, в его выбор представляется весьма значительным.

Анализируя влияние личностных черт человека в формирование виктимности, И.Г. Малкина-Пых указывает на такие базовые эмоциональные состояния, как подавленность, печаль, тревога. При этом она обращает внимание на то, что «при совершении любого типа мошенничества имеют место обман или злоупотребление доверием (а следовательно, и чрезмерная доверчивость потерпевшего), однако наибольшее криминологическое значение здесь все же имеет корыстная заинтересованность жертвы, использованная преступником» (Малкина-Пых, 2017, с. 448). «Легковерность и некритичность являются типичными личностными качествами большей части потерпевших от мошенничества, корысть, жадность, эгоистичность – значительной части» (Там же, с. 451). К потенциальным жертвам жульничества относятся люди, которые демонстрируют неосмотрительность и не способны в силу различных особенностей (низкий образовательный уровень и интеллект, юный или преклонный возраст, наличие психического заболевания и т.д.) правильно оценивать жизненные ситуации. Следует отметить, что в данном случае речь идет о мошенничестве, предполагающем реальный контакт, не опосредованный информационными или коммуникационными технологиями.

---

[3] Cybercrime statistics. URL: https://surfshark.com/research/data-breach-impact/statistics

Спецификой ситуации кибермошенничества является опосредствованность контакта мошенника и потенциальной жертвы современными коммуникационными и информационными технологиями, а также стремление мошенников вовлечь потенциальную жертву в процесс коммуникации. Эти особенности могут влиять и на портрет наиболее вероятной жертвы кибермошенничества.

Имеющиеся исследования по данной теме выделяют доверчивость, беспечность, низкий уровень знаний, касающихся собственной информационной безопасности, стремление к быстрому и высокому заработку и другие характеристики жертв (Попов, 2014). В исследованиях Ф.С. Сафуанова и Н.В. Докучаевой (2015) был выявлен специфический симптомокомплекс индивидуально-психологических особенностей жертв кибермошенничества, включающий повышенный уровень ситуативной и личностной тревожности, агрессивности, а также локуса контроля.

Анализ поведения более 11 500 интернет-пользователей показал, что более высокий риск стать жертвой мошенников связан с высокой импульсивностью и толерантностью к риску (Chen, Beaudoin, Hong, 2017). Аналогичные результаты были получены также М. Уитти (Whitty, 2019). Шансы мошенников на успех их манипуляций уменьшаются, если они имеют дело с лицами, обладающими высоким уровнем когнитивных способностей, и если эти люди внимательны и имеют достаточно времени для размышления, когда от них требуется принятие решения (Jones и др., 2019).

Однако есть другие исследования, в которых получены данные, не подтверждающие эти выводы. Например, совместная работа Стэнфордского центра долголетия в Калифорнии, бизнес-школы Университета Джорджа Вашингтона и Уортонской школы бизнеса Пенсильванского университета не обнаружила связи между уровнем когнитивных способностей и вероятностью стать жертвой мошенничества (DeLiema et al., 2020).

В недавней работе отечественные исследователи показали, что группой риска в контексте телефонного мошенничества являются люди с высокими показателями добросовестности, наивного оптимизма и ценности безопасности (Мешкова, Кудрявцев, Ениколопов, 2022). При этом следует отметить два момента. Во-первых, исследование было ограничено респондентами возраста старше 50 лет, поэтому на его основе нельзя сделать выводы о том, что те же личностные особенности будут значимы и для людей младшего возраста. Во-вторых, в фокусе исследования находились не те, кто действительно стал жертвами телефонного мошенничества, а люди, склонные к определенному поведению при «звонке из банка» (например, готовые «внимательно выслушать и обстоятельно отвечать на вопросы звонящего» (Там же, с. 146)).

Анализ исследований, направленных на выявление личностных особенностей жертв кибермошенников, показывает достаточно разрозненный и хаотичный характер исследуемых характеристик, наличие противоречивых результатов. В то же время во многих исследованиях повторяются некоторые характеристики, увеличивающие риск стать жертвой мошенников. К таким характеристикам относятся доверчивость людей, добросовестность, нестабильное эмоциональное состояние, повышенный уровень тревожности, импульсивность, толерантность к риску и др. Мы обобщили имеющиеся данные и произвели их проверку в собственном эмпирическом исследовании, которое было направлено на изучение личностных характеристик людей, *ставших жертвами* мошенничества с применением телефонных звонков, т.е. вишинга.

ПОСТРОЕНИЕ ИССЛЕДОВАНИЯ

Выборка. Всего в исследовании приняли участие 374 человека. 52 из них

указали в анкете, что со случаями обмана с использованием телефонных звонков не сталкивались; еще один бланк ответов был неполным. Таким образом, итоговая выборка состояла из 321 человека в возрасте от 16 до 90 лет (M = 37,05; SD = 16,41), 93 мужчин и 228 женщин; из них мошенникам удалось обмануть 57 человек, т.е. приблизительно 86% участников исследования сталкивались с попытками мошенничества, из них удалось обмануть ≈18%.

Инструментарий. Участникам исследования были предложены для прохождения следующие методики, оценивающие различные аспекты их личности.

1. Краткий пятифакторный опросник личности (TIPI-RU) в апробации А.С. Сергеевой и соавт. (Сергеева, Кириллов, Джумагулова, 2016) для оценки факторов Большой пятерки (экстраверсия, эмоциональная стабильность, открытость новому опыту, доброжелательность (дружелюбие) и добросовестность).

2. Шкала доверчивости (Gullibility Scale, GS) (Teunisse et al., 2020), включающая подшкалы *склонность поддаваться убеждению* (GS.P) и *нечувствительность к подсказкам* (GS.I).

3. Опросник для выявления склонности к развитию индуцированных состояний (ОВ), позволяющий оценить внушаемость (Клаучек, Деларю, 2017).

4. Шкала диспозиционной жадности (Dispositional Greed Scale) (Seuntjens et al., 2015);

5. Модифицированная шкала межличностного доверия Дж. Роттера, включающая наряду с общим показателем социального доверия подшкалу институционального доверия (Леонова, Леонов, 2016).

6. Шкала удовлетворенности жизнью Э. Динера (Осин, Леонтьев, 2020).

Полученные данные (n = 321) обрабатывались с помощью методов математической статистики (межгрупповой и корреляционный анализ; бинарная логистическая регрессия) в свободном статистическом пакете JASP 0.16.1.

РЕЗУЛЬТАТЫ

Учитывая отклонение данных от нормального распределения, с помощью непараметрического U-критерия Манна–Уитни были получены следующие значимые различия между группами обманутых и тех, кому удалось избежать обмана (табл. 1). По уровням экстраверсии, открытости к опыту, добросовестности, жадности, удовлетворенности жизнью, социального и институционального доверия значимые различия выявлены не были. Графики с описательными характеристиками для шкал, по которым были получены различия, приведены на рис. 1.

Таким образом, для усредненного личностного профиля жертвы кибермошенничества в сравнении с людьми, которым удалось избежать обмана, характерны:

Таблица 1

Результаты сравнения групп обманутых и тех, кому удалось избежать обмана (U-критерий Манна–Уитни)

Личностные черты / измеряющий инструмент	W	*p*	Rank-Biserial Correlation
Доброжелательность / TIPI.A	5681,5	0,003	–0,245
Эмоциональная стабильность / TIPI.ES	9016,5	0,018	0,198
Доверчивость / GS	4820,0	< 0,001	–0,359
Склонность поддаваться убеждению / GS.P	4915,0	< 0,001	–0,347
Нечувствительность к подсказкам / GS.I	5350,5	< 0,001	–0,289
Внушаемость / ОВ	6219,5	0,039	–0,173
Примечание. Для теста Манна–Уитни сила эффекта дана как ранговая бисериальная корреляция.			

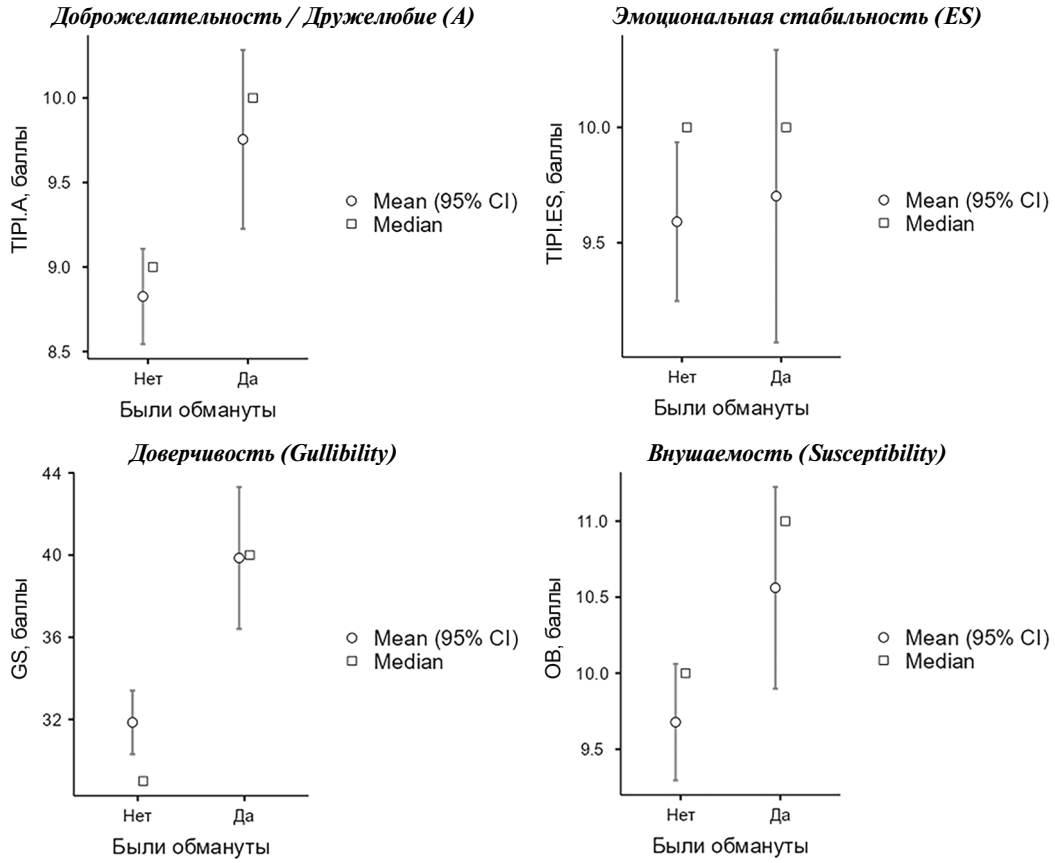

Рис. 1. Описательные графики результатов межгруппового сравнения для шкал *дружелюбие*, *эмоциональная стабильность*, *доверчивость* и *внушаемость*

• более высокий уровень доброжелательности;

• менее высокий уровень эмоциональной стабильности;

• более высокий уровень доверчивости;

• более высокий уровень внушаемости.

На основе выделенных характеристик с помощью бинарной логистической регрессии была построена предсказательная модель. Хотя для двух личностных характеристик: доброжелательность и доверчивость – были получены значимые результаты ($p < 0{,}01$), в целом полученная модель обладает очень низкой предсказательной силой ($R^2McF = 0{,}08$).

Были построены графики, связывающие вероятность события обмана с уровнями доброжелательности и доверчивости (рис. 2). Из этих графиков видно, что даже высокие уровни доброжелательности и доверчивости не позволяют с высокой вероятностью предсказать, что человек будет обманут кибермошенниками, хотя очевидно: при низких уровнях доброжелательности и доверчивости вероятность быть обманутым крайне мала. Таким образом, полученная модель обладает высокой специфичностью (0,992), но низкой чувствительностью (0,035). Иными словами, модель хорошо распознает отрицательные наблюдения (число ложноположительных близко к нулю), но плохо распознает положительные (большое число ложноотрицательных).

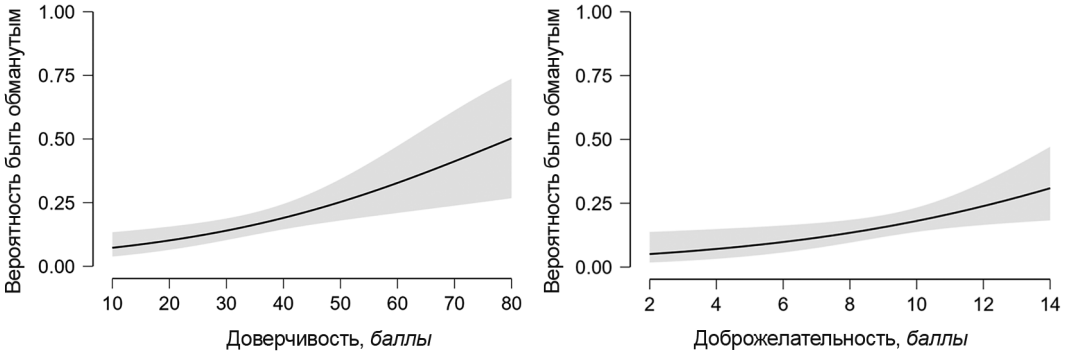

Рис. 2. ICE-графики для доверчивости и доброжелательности

На основе полученных данных было проведено сравнение групп мужчин и женщин. По всем личностным характеристикам, которые были отнесены к возможным рискам, получены значимые различия:

• женщины более доброжелательны, чем мужчины ($p = 0{,}006$);

• женщины менее эмоционально стабильны, чем мужчины ($p < 0{,}001$);

• женщины более доверчивы, чем мужчины ($p = 0{,}006$);

• женщины более внушаемы, чем мужчины ($p < 0{,}001$).

Это позволяет предположить, что для женщин вероятность быть обманутыми кибермошенниками может быть выше, чем для мужчин. Эта гипотеза была подвергнута проверке и опровергнута: хотя процент обманутых среди женщин выше (≈ 20% против ≈ 13% среди мужчин), данное различие не является статистически значимым: χ^2 (df = 1, N = 321) = 2,1, p = 0,146.

Данные по распределению долей обманутых в разных возрастных группах (табл. 2) позволяют предположить, что пожилой возраст может быть фактором риска, увеличивающим вероятность того, что мошенникам удастся обмануть человека. Однако малое число участников исследования в этой возрастной группе (N = 10 среди тех, кто сталкивался с попытками обмануть) не позволяет сделать однозначных выводов. В целом полученные в исследовании данные свидетельствуют, что возрастные различия между теми, кто стал жертвой мошенников, и теми, кому удалось избежать обмана, отсутствуют ($p = 0{,}224$). Тем не менее интересно, что чем старше респондент, тем в большей степени он уверен: человек сам виноват в том, что его обманули ($\rho = 0{,}39$, $p < 0{,}001$).

Таблица 2

Распределение долей респондентов, которых удалось и не удалось обмануть, в разных возрастных группах, %

Возраст респондентов	Доля респондентов, которых удалось обмануть	Доля респондентов, которых не удалось обмануть
Младше 25 лет	17,1	82,9
От 25 до 34 лет	11,1	88,9
От 35 до 44 лет	15,8	84,2
От 45 до 54 лет	19,1	80,9
От 55 до 64 лет	23,8	76,2
65 лет и старше	40,0	60,0

ОБСУЖДЕНИЕ РЕЗУЛЬТАТОВ

Проведенное исследование показывает, что телефонное мошенничество является проблемой, с которой сталкиваются большинство людей, причем пятую часть из них (около 18%) мошенникам удается обмануть. При этом можно предположить, что возраст старше 65 лет является фактором риска (доля обманутых в этой возрастной группе – порядка 40%), но статистическая проверка данной гипотезы требует увеличения числа респондентов этой возрастной группы. Полученное же в данном конкретном исследовании распределение респондентов по возрастным и половым группам не позволяет признать пол или возраст специфическими факторами, которые связанны с вероятностью быть обманутым в результате телефонного мошенничества.

Существуют личностные особенности, отличающие тех, кого кибермошенникам обмануть удалось, от тех, кто распознал обман: в среднем первые более доброжелательны, доверчивы, внушаемы и менее эмоционально стабильны. При этом нельзя сказать, что эти личностные особенности могут выступать предикторами того, что человека действительно обманут. Скорее, следует говорить о том, что низкие доверчивость и доброжелательность, которые проявляются в скептицизме по поводу мотивов других людей, а также заставляют человека быть подозрительным и недружелюбным, существенно снижают риск быть обманутым. Однако высокие доверчивость и доброжелательность потенциальной жертвы не гарантируют того, что ее действительно удастся обмануть.

Итак, по результатам проведенного исследования для усредненного личностного профиля жертвы вишинга характерны:

- более высокий уровень доверчивости;
- более высокий уровень доброжелательности;
- менее высокий уровень эмоциональной стабильности;
- более высокий уровень внушаемости.

Рассмотрим эти характеристики подробно.

Более высокий уровень доверчивости. Более доверчивые люди склонны принимать ложную информацию за истинную при наличии признаков недостоверности. Иными словами, для них характерна нечувствительность к сигналам/подсказкам о том, что человек или информация не заслуживают доверия. В каком-то смысле такую доверчивость можно охарактеризовать как «слепоту к обману». Вопрос, почему человек оказывается нечувствительным в этом смысле, представляет огромный интерес как в теоретическом, так и в практическом плане. Тимоти Левайн, объясняя феномен нечувствительности к обману, вводит понятие презумпции правдивости (Levine, 2014). Основываясь на экспериментах, проведенных совместно со студенткой Хе Сан Пак, он показывает, что люди склонны почти безошибочно угадывать говорящих правду и очень часто не распознавать лжецов. Получается, что они скорее готовы взаимодействовать с другими, опираясь на презумпцию правдивости. У каждого существует своя «зона доверия» (или «кредит доверия») в отношении к миру, а также к другим людям, и выход за пределы этой «зоны доверия» происходит в случае, если человек получает достаточно тревожных сигналов.

В нашем исследовании выяснилось, что лица с низкими показателями доверчивости имели минимальные шансы оказаться жертвами кибермошенников. Почему же тогда в процессе эволюции не был сформирован механизм распознавания обмана? Т. Левайн, разработавший теорию истины (правды) по умолчанию (Truth-Default Theory, TDT), считает, что это не являлось насущной необходимостью: «...в основе TDT лежит мнение, что компромисс между эффективным общением

и уязвимостью к случающемуся время от времени обману более чем оправдан. Иными словами, преимущества, получаемые от эффективной коммуникации и сотрудничества в группе, значительно перевешивают издержки случающегося изредка обмана как для отдельного человека, так и для коллектива» (Levine, 2014, p. 385). В современных условиях трудно согласиться с Левайном, поскольку размах обмана, мошенничества приобретает колоссальные размеры и говорить о ничтожности издержек становится не очень корректно. Тем не менее Левайн полагает, что отказ от презумпции правдивости обошелся бы людям значительно дороже.

Итак, поведение лжецов содержит сигналы обмана, к которым мы зачастую оказываемся нечувствительны. Люди склонны обманываться вследствие иллюзии прозрачности, т.е. тенденции переоценивать собственную способность понимать других и способность других понимать себя (Gilovich, Savitsky, Medvec, 1998). «Иллюзия прозрачности сродни презумпции правдивости. Проблема в том, что наши стратегии взаимодействия с незнакомцами глубоко ошибочны, но при этом социально необходимы. <...> Однако требование человечности означает, что приходится мириться с морем ошибок. В этом и заключается парадокс общения с незнакомцами. Мы сплошь и рядом справляемся с этой задачей просто ужасно» (Гладуэлл, 2021, с. 189). Когда человек принимает звонок от «представителей банка», ему хочется думать, что он в данном случае является объектом заботы, а не обмана. При этом чем более стереотипным является поведение человека (т.е. вписывается в наше представление о том, как должно себя вести в данной ситуации представителю банка), тем в большей степени при взаимодействии с ним срабатывает «иллюзия прозрачности»: человек ведет себя в соответствии с нашими ожиданиями, и мы склонны ему доверять. Дело, однако, в том, что когда мы говорим о подлинных намерениях, мы крайне плохо их интерпретируем, если поведение человека им не соответствует. В данном примере мы ожидаем от «представителя банка» поведение именно представителя банка, и в результате неверно истолковываем его подлинные намерения (поскольку здесь мы наблюдаем несовпадение видимого честного поведения и намерения обмануть). Т. Левайн показал, что даже специалисты (профессиональные следователи, судьи) оказываются не способными отличить ложь от правды, если они сталкиваются с несогласованным (mismatched) поведением говорящего (т.е. когда манера вести себя не совпадает с тем, лжет человек или нет). Так, в одном из его экспериментов участвовала небольшая группа правительственных агентов, которая распознала только 14,3% лжецов, притворяющихся честными людьми (так называемых sincere liars) (Levine, 2019, p. 247).

Более высокий уровень доброжелательности. Согласно концепции Большой пятерки, такие люди с оптимизмом смотрят на природу человека, считая, что окружающие в основном порядочны, честны и заслуживают доверия. Являясь доброжелательными сами, они рассчитывают на проявление аналогичных установок у партнеров по коммуникации. Однако отношение к этим партнерам зависит от того, насколько они компетентны (или производят такое впечатление), а также от их доминирующих установок. Умение распознать доброжелательность очень важно с эволюционной точки зрения. Однако здесь же мы сталкиваемся и с обратной стороной медали: доброжелательностью партнера легко воспользоваться.

Менее высокий уровень эмоциональной стабильности. Жертвы кибермошенничества более эмоционально реактивны, а характерные для них проблемы с упорядочением эмоций могут ослабить

способность принимать решения и эффективно справляться со стрессом.

В 1990-х гг. Лиза Фельдман Барретт предложила для конкретизации и упорядочивания эмоций термин «эмоциональная гранулярность», который обозначает способность человека различать нюансы и специфику собственных эмоций (Barrett, 2017). В ее исследованиях было показано: люди, обладающие высоким уровнем эмоциональной гранулярности, способны лучше понимать себя и находить оптимальные решения во взаимодействии со своим окружением, что ведет к уменьшению эмоционального напряжения. В случае неспособности произвести дифференциальную диагностику своих эмоций человек испытывает дискомфорт и желание уменьшить присутствующее напряжение, а это может способствовать неадекватным реакциям, работающим на сохранение или усиление стресса. Находясь в таком состоянии, человек ослабляет способность анализировать и контролировать ситуацию.

Более высокий уровень внушаемости. Внушаемость понимается как склонность к развитию психогенно индуцированных состояний. Люди, которым присуща эта черта, характеризуются некритической податливостью и готовностью подчиниться внушающим воздействиям, даже если они противоречат их собственным убеждениям и интересам.

Как указывал В.М. Бехтерев, «под внушением обыкновенно принято понимать воздействие одного лица на другое, которое, очевидно, происходит при посредстве пассивного восприятия, то есть помимо участия личного сознания, или “я”, субъекта» (Бехтерев, 1908, с. 14). Внушаемость – это подверженность внушению, т.е. отсутствие склонности к активному вниманию, работе логического мышления, критичности в процессе взаимодействия.

Подверженность внушению присутствует у большого числа людей, поскольку «наш мозг так сильно жаждет определенности, что воспринимает ее как награду. А неопределенность воспринимается как угроза, которую нужно устранить. И чем скорее мы устраним факты, угрожающие определенности, тем лучше, и неважно, насколько непрочен ее фундамент» (Кинг, 2022, с. 11). При этом человек, берущий инициативу в свои руки, активный, демонстрирующий уверенность в своей позиции или убеждении, воспринимается как знающий истину, компетентный, заслуживающий доверия.

Полученные нами данные показывают особую роль доверчивости и доброжелательности человека, а также значимость его эмоционального состояния и внушаемости. На что же влияют эти особенности личности?

Поведение людей изобилует множеством ошибок. Нобелевский лауреат Ричард Талер, анализируя экономическое поведение людей, пришел к выводу, что эти ошибки имеют неслучайный и предсказуемый характер. Именно поэтому, говоря о своей знаменитой работе «Nudge. Архитектура выбора», написанной совместно с К. Санстейном, он писал: «...мошенникам не нужно читать нашу книгу, чтобы знать, как проворачивать свои делишки» (Thaler, 2015). Кевин Митник, известнейший компьютерный мошенник, являющийся в настоящее время успешным консультантом по безопасности, полагает, что человеческий фактор является главным в действиях мошенника (Митник, Саймон, 2004).

Представляется, что помимо изученных в настоящем исследовании личностных диспозиций стоит также учитывать способ принятия решения человеком. Д. Канеман, анализируя особенности принятия решений, разработал модель, объясняющую этот процесс в различных ситуациях (Канеман, 2014). В случае знакомой ситуации включается Система 1 – это так называемое быстрое мышление, происходящее без дополнительно-

го обдумывания, анализа. Эта же система срабатывает в эмоционально нагруженной ситуации, требующей быстрого ответа. Она работает на основе прошлого опыта, воспринимая данную ситуацию как знакомую, не требующую анализа. Это экономное мышление, не отнимающее большого количества времени и энергии.

Система 2 – это система медленного мышления. Она требует времени и является энергозатратной, включается в ситуациях со значимыми последствиями, требует концентрации внимания, усилий по переработке новой информации. Канеман указывает на чрезвычайно важную черту разнообразных функций Системы 2: необходимость внимания и прерывание при переключении такового (Там же).

«Система мышления 1 в конечном итоге обладает ограничивающим воздействием, и это плохо, поскольку именно сюда в первую очередь устремляет свое внимание наш мозг. Мы становимся восприимчивы к вещам и ситуациям, которые попадаются нам на глаза; никакого скептицизма, сплошное легковерие и в результате – искаженное мышление. Мы импульсивны, мы спешим, не думая о последствиях и скрытых смыслах. Мы думаем, как тупицы» (Кинг, 2022, с. 87–88). Очень часто мы склонны идти по пути наименьшего сопротивления, упрощать ситуацию и не включать систему медленного мышления. Быстрое мышление нередко оказывается связанным с когнитивными искажениями.

В условиях дефицита времени, когда мошенник требует незамедлительной реакции, далеко не каждый готов замедлиться и проанализировать ситуацию, обращая внимание на все ее детали. Добавим сюда доверчивость, доброжелательность, эмоциональную нестабильность, внушаемость – и портрет потенциальной жертвы готов. Быстрое мышление в данном случае может сослужить плохую службу.

ЗАКЛЮЧЕНИЕ

Как показали результаты исследования, по сравнению с теми, кому удалось избежать обмана, жертвы вишинга характеризуются более высокими уровнями доброжелательности, эмоциональной нестабильности, доверчивости и внушаемости. Построенная предсказательная модель, однако, имеет низкий уровень чувствительности, а это обстоятельство не позволяет рассматривать указанные личностные особенности в качестве предикторов того, что человека действительно обманут.

Можно ли уменьшить риск попасть в сети кибермошенников? Культивировать в себе поведенческие навыки, связанные с менее высокими уровнями доверия и доброжелательности, вряд ли является эффективной стратегией, поскольку она может негативно сказаться на социальных взаимодействиях человека. Повысить уровень эмоциональной стабильности и понизить уровень внушаемости было бы неплохо, но как быстро этого можно достичь, реально ли это вообще? Что же тогда делать? На помощь приходят сами участники исследования, когда основным фактором, способным помочь в разрешении данной ситуации, они называют повышение финансовой грамотности. Безусловно, это важный аспект работы с людьми, но помимо финансовой грамотности необходимо развитие системы медленного мышления и приобретение поведенческих навыков, уменьшающих риск стать объектом манипуляций кибермошенников. В этом контексте представляется перспективным бихевиористский подход к феномену принятия решения, предлагающий рассматривать выбор как форму оперантного поведения (Pierce, Cheney, 2017). Важно учитывать индивидуальные и культурные контингенции подкрепления[4], анализ которых будет

[4] https://znaniya.org/c/kontingentsii-podkrepleniia-f168a1

способствовать пониманию того, как формировать эффективные стратегии противодействия мошенничеству.

1. *Бехтерев В.М.* Внушение и его роль в общественной жизни. СПб.: К.Л. Риккер, 1908.
2. *Гладуэлл М.* Разговор с незнакомцем: Почему мы ошибаемся в людях и доверяем лжецам. М.: Альпина Паблишер, 2021.
3. *Канеман Д.* Думай медленно... решай быстро. М.: АСТ, 2014.
4. *Кинг П.* Практический интеллект. Как критически мыслить, моделировать ситуации, глубоко анализировать. М.: Библос, 2022.
5. *Клаучек С.В., Деларю В.В.* Разработка скринингового метода для выявления склонности к развитию индуцированных состояний // Психол. журн. 2017. Т. 18. № 2. С. 123–128.
6. *Комаров А.А.* Интернет-мошенничество: проблемы детерминации и предупреждения. М.: Юрлитинформ, 2013.
7. *Леонова И.Ю., Леонов И.Н.* Психометрическая проверка структуры методики «Шкала межличностного доверия» Дж. Роттера в адаптации С.Г. Достовалова и ее модификация // Вестн. Удмуртского ун-та. Сер. Философия. Психология. Педагогика. 2016. Т. 26. № 2. С. 93–111.
8. *Малкина-Пых И.Г.* Виктимология. Психология поведения жертвы. СПб.: Питер, 2017.
9. *Мешкова Н.В., Кудрявцев В.Т., Ениколопов С.Н.* К психологическому портрету жертв телефонного мошенничества // Вестн. Моск. ун-та. Сер. 14. Психология. 2022. № 1. С. 138–157.
10. *Митник К., Саймон У.Л.* Искусство обмана. М.: АйТи, 2004.
11. *Осин Е.Н., Леонтьев Д.А.* Краткие русскоязычные шкалы диагностики субъективного благополучия: психометрические характеристики и сравнительный анализ // Мониторинг общественного мнения: экономические и социальные перемены. 2020. № 1 (155). С. 117–142.
12. *Попов К.И.* Виктимологическая характеристика преступлений в сфере компьютерной информации // Виктимология. 2014. № 1 (1). С. 66–68.
13. *Сафуанов Ф.С., Докучаева Н.В.* Особенности личности жертв противоправных посягательств в Интернете // Психология и право. 2015. Т. 5. № 4. С. 80–93.
14. *Сергеева А.С., Кириллов Б.А., Джумагулова А.Ф.* Перевод и адаптация краткого пятифакторного опросника личности (TIPI-RU): оценка конвергентной валидности, внутренней согласованности и тест-ретестовой надежности // Эксперим. психол. 2016. Т. 9. № 3. С. 138–154.
15. *Barrett L.F.* How emotions are made: The secret life of the brain. Boston, MA: Houghton Mifflin Harcourt, 2017.
16. *Chen H., Beaudoin C.E., Hong T.* Securing online privacy: An empirical test on Internet scam victimization, online privacy concerns, and privacy protection behaviors // Computers in Hum. Behav. 2017. V. 70. P. 291–302.
17. *DeLiema M.* et al. Financial fraud among older Americans: Evidence and implications / DeLiema M., Deevy M., Lusardi A., Mitchell O.S. // J. Gerontology. Ser. B: Psychol. Sci. and Soc. Sci. 2020. V. 75. N 4. P. 861–868.
18. *Gilovich T., Savitsky K., Medvec V.H.* The illusion of transparency: Biased assessments of others' ability to read one's emotional states // J. Pers. and Soc. Psychol. 1998. V. 75. N 2. P. 332–346.
19. *Jones H.S.* et al. Email fraud: The search for psychological predictors of susceptibility / Jones H.S., Towse J.N., Race N., Harrison T. // PLoS One. 2019. V. 14. N 1. P. e0209684.
20. *Levine T.R.* Duped: Truth-default theory and the social science of lying and deception. Tuscaloosa, Alabama: Univ. of Alabama Press, 2019.
21. *Levine T.R.* Truth-default theory (TDT): A theory of human deception and deception detection // J. Language and Soc. Psychol. 2014. V. 33. N 4. P. 378–392.
22. *Pierce W.D., Cheney C.D.* Behavior analysis and learning: A biobehavioral approach. N.Y.: Routledge, 2017.
23. *Seuntjens T.G.* et al. Dispositional greed / Seuntjens T.G., Zeelenberg M., Ven N. van de, Breugelmans S.M. // J. Pers. and Soc. Psychol. 2015. V. 108. N 6. P. 917–933.
24. *Teunisse A.K.* et al. I Should have known better: development of a self-report measure of gullibility / Teunisse A.K., Case T.I., Fitness J., Sweller N. // Pers. and Soc. Psychol. Bull. 2020. V. 46. N 3. P. 408–423.
25. *Thaler R.H.* Misbehaving: The making of behavioral economics. N.Y., NY: W.W. Norton & Co, 2015.
26. *Whitty M.T.* Predicting susceptibility to cyber-fraud victimhood // J. Financial Crime. 2019. V. 26. N 1. P. 277–292.

References in Russian:

1. *Bekhterev V.M.* Vnushenie i ego rol v obshchestvennoy zhizni [Suggestion and its role in public life]. SPb.: K.L. Rikker, 1908.
2. *Gladwell M.* Razgovor s neznakomtsem: Pochemu my oshibaemsya v lyudyakh i doveryaem lzhetsam [Talking to strangers: What we should know about the people we don't know]. M.: Alpina Pablisher, 2021.

3. *Kahneman D.* Dumay medlenno... reshay bystro [Thinking, Fast and Slow]. M.: AST, 2014.
4. *King P.* Prakticheskiy intellekt. Kak kriticheski myslit, modelirovat situatsii, gluboko analizirovat [Practical intelligence: How to think critically, deconstruct situations, analyze deeply, and never be fooled]. M.: Biblos, 2022.
5. *Klauchek S.V., Delaryu V.V.* Razrabotka skriningovogo metoda dlya vyyavleniya sklonnosti k razvitiyu indutsirovannykh sostoyaniy [Development of a screening method for identifying the propensity to develop induced states] // Psikhol. zhurn. 2017. T. 18. N 2. S. 123–128.
6. *Komarov A.A.* Internet-moshennichestvo: problemy determinatsii i preduprezhdeniya [Internet Fraud: Problems of Determination and Prevention]. M.: Yurlitinform, 2013.
7. *Leonova I.Yu., Leonov I.N.* Psikhometricheskaya proverka struktury metodiki «Shkala mezhlichnostnogo doveriya» Dzh. Rottera v adaptatsii S.G. Dostovalova i ee modifikatsiya [Psychometric verification of the structure of the method "Interpersonal Confidence Scale" by J. Rotter in adaptation by S.G. Dostovalov and its modification] // Vestn. Udmurtskogo un-ta. Ser. Filosofiya. Psikhologiya. Pedagogika. 2016. T. 26. N 2. S. 93–111.
8. *Malkina-Pykh I.G.* Viktimologiya. Psikhologiya povedeniya zhertvy [Victimology. Psychology of victim behavior]. SPb.: Piter, 2017.
9. *Meshkova N.V., Kudryavtsev V.T., Enikolopov S.N.* K psikhologicheskomu portretu zhertv telefonnogo moshennichestva [To the psychological portrait of victims of telephone fraud] // Vestn. Mosk. un-ta. Ser. 14. Psikhologiya. 2022. N 1. S. 138–157.
10. *Mitnick K., Simon W.L.* Iskusstvo obmana [The Art of Deception]. M.: AyTi, 2004.
11. *Osin E.N., Leontiev D.A.* Kratkie russkoyazychnye shkaly diagnostiki subyektivnogo blagopoluchiya: psikhometricheskie kharakteristiki i sravnitelnyy analiz // Monitoring obshchestvennogo mneniya: ekonomicheskie i sotsialnye peremeny [Short Russian-language diagnostic scales of subjective well-being: psychometric characteristics and comparative analysis]. 2020. N 1 (155). S. 117–142.
12. *Popov K.I.* Viktimologicheskaya kharakteristika prestupleniy v sfere kompyuternoy informatsii [Victimological Characteristics of Crimes in the Field of Computer Information] // Viktimologiya. 2014. N 1 (1). S. 66–68.
13. *Safuanov F.S., Dokuchaeva N.V.* Osobennosti lichnosti zhertv protivopravnykh posyagatelstv v Internete [Features of the personality of victims of unlawful encroachments on the Internet] // Psikhologiya i pravo. 2015. T. 5. N 4. S. 80–93.
14. *Sergeeva A.C., Kirillov B.A., Dzhumagulova A.F.* Perevod i adaptatsiya kratkogo pyatifaktornogo oprosnika lichnosti (TIPI-RU): otsenka konvergentnoy validnosti, vnutrenney soglasovannosti i test-retestovoy nadezhnosti [Ranslation and adaptation of short five factor personality questionnaire (TIPI-RU): convergent validity, internal consistency and test-retest reliability evaluation] // Eksperim. psikhol. 2016. T. 9. N 3. S. 138–154.

Поступила в редакцию 18. V 2022 г.