Психология и право
2022. Том 12. № 2. С. 194–206.
DOI: https://doi.org/10.17759/psylaw.2022120214
ISSN: 2222-5196 (online)

Psychology and Law
2022. Vol. 12, no. 2, pp. 194–206.
DOI: https:///doi.org/10.17759/psylaw.2022120214
ISSN: 2222-5196 (online)

Психологические особенности лиц, склонных к кибервиктимному поведению

Власова Н.В.
Московский государственный психолого-педагогический университет (ФГБОУ ВО МГППУ), г. Москва, Российская Федерация
ORCID: https://orcid.org/0000-0002-3452-1133, e-mail: L1025173@yandex.ru

Буслаева Е.Л.
Московский государственный лингвистический университет (ФГБОУ ВО МГЛУ), г. Москва, Российская Федерация
ORCID: https://orcid.org/0000-0002-1913-9198, e-mail: moselena2201@yandex.ru

В статье обсуждаются результаты эмпирического исследования психологических особенностей лиц, склонных к кибервиктимному поведению. Теоретическими основаниями работы выступает анализ результатов исследований современных зарубежных и отечественных ученых, свидетельствующих о возможности выделения специфических характеристик жертвы киберпреступления. В исследовании приняли участие 78 совершеннолетних пользователей социальной сети «ВКонтакте». В качестве лиц, склонных к кибервиктимному поведению, выступила группа респондентов, которые за последние 3 года не менее двух раз становились жертвами кибермошенничества. Для сбора эмпирических данных использованы следующие методики: опросник «Многофакторное исследование личности (16 PF)» Р. Б. Кэттелла, тест «Уровень субъективного контроля» (авторы В.Ф. Бажин, Е.А. Голынкина, А.М. Эткинд) и «Шкала реактивной и личностной тревожности» Ч. Спилбергера (в адаптации Ю.Л. Ханина). Результаты проведенного исследования показали, что склонность к кибервиктимному поведению обусловлена наличием определенных психологических особенностей эмоционального и межличностного характера. Полученные данные могут быть использованы в качестве основных мишеней при разработке программ по профилактике противозаконных действий в киберпространстве.

Ключевые слова: кибервиктимное поведение, киберпреступления, кибермошенничество, личностные особенности, субъективный контроль.

Для цитаты: *Власова Н.В., Буслаева Е.Л.* Психологические особенности лиц, склонных к кибервиктимному поведению [Электронный ресурс] // Психология и право. 2022. Том 12. № 2. С. 194–206. DOI:10.17759/psylaw.2022120214

Psychological Features of Individuals Prone to Cyber Victimization

Nataliya V. Vlasova
Moscow State University of Psychology & Education, Moscow, Russia
ORCID: https://orcid.org/0000-0002-3452-1133, e-mail: L1025173@yandex.ru

Elena L. Buslaeva
Moscow State Linguistic University, Moscow, Russia.
ORCID: https://orcid.org/0000-0002-1913-9198, e-mail: moselena2201@yandex.ru

The article discusses the results of the empirical research into the psychological features of individuals prone to cyber victimization. As a theoretical basis, this paper uses the analysis of the findings of the studies conducted by the Russian as well as foreign researchers, that indicate presence of the specific traits among victims of cyber crime. The focus group that took part in the research includes 78 adult users of the VK social network. The respondents who became victims of cyber scams more than twice over the past three years were identified as the individuals prone to cyber victimization. The following techniques were used for the empirical data collection: Multifactorial personality questionnaire (16 PF) by R.B. Cattell, "Level of subjective control" test by V.F. Bazhin, E.A. Golynkina and A.M. Atkind and State-Trait anxiety inventory by C. Spielberger (adapted by Y. Khanin). The results of the conducted research show that one's tendency towards cyber victimization can be explained by the presence of certain specific emotional and interpersonal traits. The findings of this study could be used as major targets for designing preventive programs against crimes in cyber space.

Keywords: cyber victimization, cyber crime, personality traits, subjective control.

For citation: Vlasova N.V., Buslaeva E.L. Psychological Features of Individuals Prone to Cyber Victimization. *Psikhologiya i pravo = Psychology and Law*, 2022. Vol. 12, no. 2, pp. 194–206. DOI:10.17759/psylaw.2022120214 (In Russ.).

Введение

Нестабильная социально-экономическая и санитарно-эпидемиологическая ситуация в мире, вызванные этим ограничения в общественной сфере и естественное в этих обстоятельствах резкое сокращение взаимодействий межличностного характера, безусловно, оказывают негативное влияние на возможности профилактики киберпреступности. В связи с этим в настоящее время особенно актуальным становится изучение условий и факторов, способствующих защите личности от киберугроз различного характера. Согласно данным пресс-службы МВД России, за последние два года примерно в 1,5 раза выросло количество преступлений с использованием IT-технологий. При этом наиболее распространенными среди них становятся все более изощренные попытки кибермошенничества, часто сопровождаемые созданием криминальных сообществ и вовлечением в них несовершеннолетних [4].

Результаты современных исследований в области киберпреступности позволили выделить четыре основные формы кибермошенничества.

Фишинг — использование различных инструментов и схем в сети Интернет для получения доступа к конфиденциальной информации пользователей, например, к данным их логи-

нов и паролей банковских карт. Чаще всего в этом случае преступники используют схожие по интерфейсу фиктивные сайты популярных компаний.

Вишинг — реализуется посредством телефонной связи и разыгрыванием определенных социальных ролей (работника банка, сотрудника социальных служб и т. д.) с целью получения от абонента конфиденциальной информации платежных карт или осуществления им добровольных денежных переводов на реквизиты мошенников.

Письма «выигрыши» — использование специальных уведомлений, рассылаемых по электронной почте, в которых адресаты информируются о получении ими приза или крупного денежного выигрыша. При этом для их получения абоненту необходимо совершить определенные финансовые операции, например, открыть счет в банке и положить на него заранее оговоренную сумму, после чего сообщить отправителю письма реквизиты данного счета со всей конфиденциальной информацией.

«Романтическое» мошенничество — реализуется через сайты знакомств, зачастую специально создаваемые для поиска лиц, стремящихся найти потенциального партнера. Целями этих действий являются манипуляция и вымогательство у таких людей материальных средств в виде подарков, денежных сумм или доступа к их банковским счетам.

По мнению большинства как зарубежных, так и отечественных исследователей в области изучения природы киберпреступности, распространенность всех приведенных выше форм кибермошеничества и невысокая степень их раскрываемости обусловлены, прежде всего, незначительным числом обращений жертв в правоохранительные органы. Так, потерпевшие довольно часто обвиняют себя в сложившейся ситуации, считая, что были излишне доверчивы. В то же время они испытывают страх перед возможным общественным осуждением, считая, что своими действиями продемонстрировали собственную неосторожность, простодушие, наивность и, таким образом, подверглись влиянию манипулятора. И, наконец, пострадавшие не верят в эффективность расследования совершенного в их отношении преступления [11].

Следовательно, можно говорить о том, что жертвы кибермошеничества обладают определенными специфическими для виктимной личности качествами. В то же время невозможно «…рассматривать виктимность личности и ее ситуационное поведение в изоляции от категории личностного отношения человека к самому себе и другим людям, так как в ситуации совершения преступления жертва — уже «обладатель» определенных виктимных предрасположений» [7, с. 37].

Как отмечает А.В. Мудрик: «Виктимность определяется совокупностью эмоционально-личностных особенностей, способствующих дезадаптивному стилю реагирования субъекта, приводящему к ущербу для его физического или эмоционально-психического здоровья» [8, с. 78].

Наиболее подробную классификацию психологических особенностей виктимной личности предлагает Д.В. Ривман. Так, он выделяет активный тип поведения жертвы, когда вред причиняется при ее же участии и даже содействии. Этим людям присущ высокий уровень вербальной агрессии, вспыльчивость, раздражительность, импульсивность, склонность к риску и необдуманным поступкам. К пассивному типу автор относит потерпевших, не способных оказывать сопротивление преступнику, как в силу определенных личностных особенностей (высокий уровень тревожности, робость, застенчивость, заниженная самооценка), так и по причине ситуативно обусловленного неблагополучного физического или психического состояния. Также Д.В. Ривман выделяет некритичный тип виктимного поведения. К нему он относит лиц, склонных к излишней доверчивости, неосмотрительности, не способ-

ных адекватно оценивать жизненные ситуации, либо в силу невысокого уровня интеллектуальных способностей, либо в связи с возрастными, физиологическими или психологическими особенностями [9].

К таким же выводам о свойствах личности, связанных с виктимностью, приходит коллектив авторов: Т.Е. Яценко, Н.И. Олифирович, Н.К. Плавник, И.В. Шматкова, О.В. Белановская, Л.А. Русецкая. К выраженности изучаемого феномена они относят: «…неэффективное сопротивление нарушению границ своего психологического пространства и уклонение от позиции субъекта жизнедеятельности, обусловливающие их психологическую виктимизацию или ревиктимизацию в межличностном взаимодействии» [12, с. 132].

Анализ исследований, посвященных кибервиктимному поведению, позволяет заметить, что их теоретическую основу, так же как и при исследовании поведения жертв, не связанного с IT-технологиями, составляют как теория повседневной деятельности, так и общая теория преступного поведения. Это, в свою очередь, предоставляет возможность выделить те же индивидуальные особенности личности для понимания ее предрасположенности к онлайн-виктимизации.

Так, например, T.J. Holt, A.M. Bossler приходят к выводу о том, что наиболее важным предиктором кибервиктимизации является низкий уровень самоконтроля. При этом авторы акцентируют внимание на том, что данный психологический феномен присущ лишь тем жертвам, которые напрямую контактировали с мошенниками посредством различных технических средств (компьютеров, телефонов и т. д.) [15].

Результаты проведенных N. Gilboa исследований в отношении лиц, компьютеры которых были подвергнуты взлому мошенниками с целью получения конфиденциальной информации, подтверждают его выводы о том, что чаще всего кибератакам подвергались люди, имеющие низкий уровень социального интеллекта. Жертвам киберпреступлений, по мнению автора, свойственны недостаточная степень понимания истинных мотивов поведения других людей, неспособность критически оценивать поступающую от них информацию, наивность и доверчивость [14].

К подобным выводам приходят C.J. Schreck, R.A.Wright, J.M. Miller, которые указывают, что люди, обладающие низким уровнем эмоциональной восприимчивости, с большей вероятностью могут подвергнуться киберпреследованиям. Они, во-первых, значительно реже используют специальные программы для защиты своих технических устройств. Во-вторых, такие люди чаще, чем другие, проявляют неосмотрительность при соблюдении мер предосторожности, необходимых для защиты себя и своей собственности при непосредственном контакте с онлайн-преступником [17].

Эти данные подтверждаются и заключениями, к которым приходят в своих работах Е.А. Антонян и Е.Н. Клещина. Исследователи установили, что готовность стать жертвой киберпреступления определяется чрезмерным времяпрепровождением в Сети, а также незнанием элементарных правил безопасности либо пренебрежением ими, даже если они были заведомо известны пострадавшему.

Проведя анализ особенностей личности жертв противоправных посягательств в Интернете, Ф.С. Сафуанов и Н.В. Докучаева выделили определенный «симптомокомплекс индивидуально-психологических особенностей, включающий беспокойство, неуверенность в себе, подверженность настроению, неусидчивость, неустойчивость настроения, гневливость, определенные способы совладания и психологические защиты в психотравмирующих ситуациях: поиск эмоциональной социальной поддержки, фокусировка на эмоциях, самоограничение и проекция» [10, с. 89].

А.О. Жакупжанов относит к совокупности личностных качеств, формирующих виктимное поведение в области киберпространства, следующие черты: доверчивость, беспечность, низкий уровень знаний в сфере информационной безопасности, стремление к легкому и высокому заработку, к которому абоненты Всемирной сети часто побуждаются [5].

Интересными являются также выводы, сделанные Л.Э. Кузнецовой. Согласно результатам ее исследования особенностей виктимного поведения у современной молодежи, автор утверждает, что молодым людям, склонным к данному виду девиации, в том числе и подвергавшимся кибербуллингу, свойственны следующие характеристики: «пониженное принятие себя, неспособность отказывать другим людям и сниженный уровень эмоционального комфорта» [6].

В то же время B.W. Reyns, B.S. Fisher, A.M. Bossler, T.J. Holt в своем последнем совместном исследовании, проведенном на разновозрастной выборке (от 18 до 62 лет), пытались установить связь между склонностью к кибервиктимности и особенностями самоконтроля. Они пришли к выводу об отсутствии корреляции между данными психологическими феноменами [16]. При этом в своей работе авторы используют опросник диагностики самоконтроля Р. Грасмика. Адаптированная версия данной методики представлена В.Г. Булыгиной, А.М. Абдразяковой, И.В. Коваленко [3] и направлена на изучение «…многомерного конструкта, включающего в себя разные элементы, образующие устойчивую характеристику — самоконтроль, которая является латентной чертой» [2, с. 5].

К еще более категоричным выводам, сделанным в соответствии с результатами своих исследований, приходят F.T. Ngo и R. Paternoster. Авторы обоснованно доказывают, что ни индивидуальные, ни ситуационные факторы не оказывают значимого влияния на вероятность стать жертвой мошенничества в киберпространстве [13].

Таким образом, несмотря на довольно обширный опыт проведенных в этой сфере исследований, проблема выделения личностных особенностей людей, склонных к кибервиктимному поведению, в настоящее время имеет отличающиеся друг от друга подходы, разнятся и результаты используемой в этих исследованиях диагностики.

Также важно отметить, что современные исследования в области киберпреступлений не были дифференцированы с учетом отдельных их видов. Особенности кибервиктимного поведения либо изучались как подверженность в целом любым преступлениям, совершаемым посредством технических средств и реализуемым через киберпространство, либо ограничивались анализом виктимности только в сфере кибербуллинга.

Все вышесказанное и определило цель нашего исследования — выявить психологические особенности лиц, подверженных кибермошенничеству.

Материалы и методы исследования

В исследовании приняли участие совершеннолетние пользователи социальной сети «ВКонтакте», которые согласились пройти специальный опрос о том, подвергались ли они целенаправленному воздействию со стороны кибермошенников. Средний возраст опрашиваемых составил 31,5 (+/-8,5) лет.

По результатам проведенного опроса были сформированы две группы респондентов — проблемная и контрольная. Проблемную группу составили 38 человек (18 мужчин и 20 женщин), которые не менее двух раз за последние 3 года становились жертвами кибермошенничества. В контрольную группу вошли 40 респондентов (20 мужчин и 20 женщин), контактировавших с мошенниками в киберпространстве, но сумевших противостоять манипуляциям и не стать жертвами преступных действий.

С целью выявления психологических особенностей лиц, проявивших кибервиктимное поведение, был проведен сравнительный анализ результатов исследуемых групп, полученных с использованием следующих методик: опросник «Многофакторное исследование личности (16 PF)» Р. Б. Кэттелла, тест «Уровень субъективного контроля» (авторы В.Ф. Бажин, Е.А. Голынкина, А.М. Эткинд) и «Шкала реактивной и личностной тревожности» Ч. Спилбергера (в адаптации Ю.Л. Ханина). Для обработки полученных результатов применялся статистический критерий проверки гипотез в пакете SPSS Statistics-26: непараметрический критерий Манна—Уитни для независимых выборок.

Результаты и их обсуждение

Результаты, полученные с использованием методики «Многофакторное исследование личности (16 PF)» Р.Б. Кэттелла, представлены в табл. 1.

Согласно данным сравнительного анализа можно констатировать, что наиболее значимые различия в исследуемых группах были получены по показателям эмоциональных характеристик личности, таких как: эмоциональная стабильность, самоконтроль, напряженность и тревожность. Так, у респондентов, подвергавшихся кибермошенническим действиям, были выявлены сниженный уровень контроля эмоциональных реакций и эмоциональной стабильности. В то же время в данной группе обследуемых результаты по показателям внутреннего эмоционального напряжения и тревожности оказались значимо выше, чем в контрольной группе.

Подобные эмпирические данные свидетельствуют о том, что жертвам кибермошенничества свойственны сочетание довольно низкого порога фрустрации и такого же уровня самоконтроля, что может быть расценено как высокая подверженность неблагоприятным внешним и внутренним эмоциональным факторам, оказывающим негативное влияние на оценку ситуации и принятие решений. При этом, в сравнении с представителями контрольной группы, в условиях возникновения каких-либо жизненных проблем и затруднений они чаще испытывают тревогу и беспокойство, что не позволяет им осуществлять эффективные действия по разрешению возникших проблем.

Значимые различия в исследуемых группах были получены также по показателям коммуникативных свойств личности. В проблемной группе были обнаружены более низкие результаты по шкалам дипломатичности, общительности и подозрительности при их сравнении с данными представителей контрольной группы. При этом в сочетании с выявленными более высокими показателями по шкале беспечности в группе респондентов, ставших жертвами кибермошенничества, полученные данные свидетельствуют о том, что для лиц, склонным к кибервиктимному поведению, характерен сниженный уровень развития коммуникативных способностей. Следовательно, представителям проблемной группы свойственны излишняя доверчивость, наивность, неспособность адекватно оценивать истинные мотивы поступков и цели окружающих. Данные личностные особенности не могут быть продуктивными при попытках построить равноправный диалог с собеседником, что предоставляет кибермошенникам возможность для манипуляций своими жертвами и совершения в их отношении преступных действий.

В то же время важно отметить, что значимых различий в показателях компонентов познавательной сферы между исследуемыми группами выявлено не было. Это свидетельствует о том, что уровень интеллекта не оказывает существенного влияния на возможность человека подвергаться воздействию кибермошеннических манипуляций.

Таблица 1

Результаты методики многофакторного исследования личности (16 PF) Р.Б. Кэттелла (N = 78)

Показатели методики	**Группа**	**Средний ранг**	**Асимптотическая значимость**
Общительность (A)**	Контрольная группа	46,18	0,007
	Проблемная группа	32,47	
Интеллект (B)	Контрольная группа	42,21	0,267
	Проблемная группа	36,64	
Эмоциональная стабильность (C)***	Контрольная группа	52,25	0,000
	Проблемная группа	26,08	
Доминантность (E)	Контрольная группа	38,69	0,736
	Проблемная группа	40,36	
Беспечность (F)**	Контрольная группа	31,12	0,001
	Проблемная группа	48,32	
Моральная нормативность (G)	Контрольная группа	43,04	0,149
	Проблемная группа	35,78	
Смелость в социальных контактах (H)	Контрольная группа	42,61	0,204
	Проблемная группа	36,22	
Эмоциональная чувствительность (I)	Контрольная группа	36,90	0,284
	Проблемная группа	42,24	
Подозрительность (L)**	Контрольная группа	32,50	0,004
	Проблемная группа	46,87	
Мечтательность (M)	Контрольная группа	35,79	0,132
	Проблемная группа	43,41	
Дипломатичность (N)**	Контрольная группа	48,62	0,001
	Проблемная группа	29,89	
Тревожность (O)**	Контрольная группа	30,68	0,001
	Проблемная группа	48,79	
Радикализм (Q1)	Контрольная группа	40,44	0,703
	Проблемная группа	38,51	
Самостоятельность (Q2)	Контрольная группа	40,66	0,631
	Проблемная группа	38,28	
Самоконтроль (Q3)**	Контрольная группа	49,06	0,001
	Проблемная группа	29,43	
Напряженность (Q4)***	Контрольная группа	28,95	0,000
	Проблемная группа	50,61	

Примечание: «*» — $p<0,05$; «**» — $p<0,01$; «***» — $p<0,001$.

Для выявления особенностей самоконтроля в различных сферах жизнедеятельности у респондентов сравниваемых групп использовался тест-опросник «Уровень субъективного контроля» (авторы: В.Ф. Бажин, Е.А. Голынкина, А.М. Эткинд). Полученные результаты представлены в табл. 2.

Таблица 2

Результаты тест-опросника «Уровень субъективного контроля» (В.Ф. Бажин, Е.А. Голынкина, А.М. Эткинд) (N = 78)

Показатели опросника	**Группа**	**Средний ранг**	**Асимптотическая значимость**
Общая шкала интернальности**	Контрольная группа	46,19	0,007
	Проблемная группа	32,46	
Шкала интернальности в области достижений	Контрольная группа	40,92	0,561
	Проблемная группа	38,00	
Шкала интернальности в области неудач	Контрольная группа	41,86	0,336
	Проблемная группа	37,01	
Шкала интернальности в семейных отношениях	Контрольная группа	41,34	0,453
	Проблемная группа	37,57	
Шкала интернальности в производственных отношениях	Контрольная группа	31,12	0,745
	Проблемная группа	38.66	
Шкала интернальности в межличностных отношениях**	Контрольная группа	46.84	0,003
	Проблемная группа	31,78	
Шкала интернальности в отношении здоровья и болезни	Контрольная группа	38,40	0,656
	Проблемная группа	40,66	

Примечание: «*» — $p<0,05$; «**» — $p<0,01$; «***» — $p<0,001$.

Сравнительный анализ полученных результатов позволил выявить значимые различия в показателях по шкале общей интернальности, что свидетельствует о сниженном уровне самоконтроля поведения, свойственном жертвам кибермошенничества. В сравнении с респондентами контрольной группы они чаще принимают решения и совершают действия под влиянием внешних факторов и условий. Следовательно, для кибервиктимной личности характерны тенденция к снижению личной ответственности, неготовность проявлять активность и настойчивость при выборе цели и методов ее достижения.

Также статистически значимые различия в сравниваемых группах были получены по показателям шкалы интернальности в межличностных отношениях. Данные результаты указывают на тот факт, что потерпевшим от кибермошенничества свойственно внутреннее ощущение дефицита возможностей контролировать свои социальные контакты. Они чаще других идут на уступки и отдают инициативу окружающим в формировании социальных отношений, проявляют доверчивость и подчиняемость, а возникающие межличностные конфликты объясняют неудачно сложившимися обстоятельствами или особенностями поведения других людей.

Для проверки сформулированной выше гипотезы в части выделения тревожности как психологической особенности, характерной для лиц с кибервиктимным поведением, была

использована методика «Шкала реактивной и личностной тревожности» Ч. Спилбергера (в адаптации Ю.Л. Ханина). Результаты сравнительного анализа не выявили значимых различий в показателях шкал, как реактивной тревожности (U=**713.5**), так и личностной тревожности (U=**656**). Таким образом, согласно полученным данным, нельзя однозначно утверждать, что людям с выраженной склонностью к тревожным реакциям в стрессовых ситуациях или высокой готовностью к ним при любой внешней угрозе свойственно кибервиктимное поведение. Этот несколько неожиданный результат исследования может быть воспринят как противоречащий полученным данным сравнительного анализа по шкале «Тревожность» методики «16 PF» Р.Б. Кэттелла. В то же время, при качественном сравнении показателей по данным методикам, можно заметить, что они определяют разные характеристики такой личностной особенности, как тревожность. Так, согласно описательным характеристикам, изложенным в методике Р.Б. Кэттелла, показатель шкалы «Тревожность» определяется как субъективная оценка собственных сил и ресурсов для преодоления фрустрирующей ситуации, что, видимо, больше связано с самооценкой и внутренней уверенностью в себе и своих силах. Исследуя же этот показатель по методике Ч. Спилберга, можно трактовать описание анализируемого феномена или как непосредственную реакцию на стресс (реактивная тревожность), или как конституциональную черту личности (личностная тревожность). При этом реактивная тревожность проявляется в повышении внутреннего напряжения, беспокойстве и психомоторном возбуждении, а личностная тревожность коррелирует с наличием внутриличностного конфликта, склонностью к невротизации и психосоматическим заболеваниям.

Выводы

1. На основании результатов проведенного эмпирического исследования психологическими особенностями лиц, проявляющих виктимность от кибермошенничества, являются компоненты эмоциональной и коммуникативной сфер личности. Эмоциональными характеристиками кибервиктимной личности выступают: сниженный уровень самоконтроля, повышенный уровень эмоциональной лабильности, низкий порог фрустрации, неуверенность в себе. Особенностями коммуникативной сферы таких лиц являются: доверчивость и наивность, проявляемые в формировании межличностных отношений, неумение гибко и дипломатично выстраивать социальное взаимодействие, ориентироваться в истинных мотивах поступков собеседника.

2. Наиболее характерными чертами субъективного контроля лиц, способных пострадать от мошенничества в киберпространстве, являются приоритет эмоциональной оценки ситуаций, глубокое влияние на нее со стороны других людей, а также стремление в большей степени полагаться на внешние мнения и решения. При этом любая ситуация, вызывающая реакцию фрустрации, расценивается ими как непреодолимая. Она существенно снижает их веру в себя, в собственные возможности ее преодоления, затрудняет процесс адаптации, формирование новых социальных навыков и паттернов совладающего поведения.

3. Полученные в ходе исследования противоречивые результаты при выявлении тревожности как характеристики, определяющей кибервиктимное поведение, могут быть объяснены с позиции качественного анализа показателей использованных методик. Для определения связи кибервиктимизации и особенностей проявления тревожности необходимо провести более глубокое исследование.

4. Согласно полученным результатам к психологическим особенностям личности, которые помогают человеку противостоять кибермошенничеству, можно отнести: высокий уро-

вень самоконтроля эмоциональных реакций и поведения в субъективно значимых ситуациях, а также развитые коммуникативные способности.

Заключение

Кибермошенничество является одним из наиболее распространенных способов реализации преступных деяний в интернет-пространстве. Методы, которые в настоящее время используются для предупреждения данного вида криминального поведения, построены в основном на информировании людей о различных манипуляционных способах и приемах, применяемых мошенниками. Тем не менее, как свидетельствуют данные мониторинга криминальной ситуации МВД РФ, уведомление абонентов Интернета о возможных махинациях в Сети не дает желаемого результата.

Человек, склонный к кибервиктимному поведению, в ситуации стресса, даже обладая знаниями о мошеннических схемах и возможных манипуляциях в его отношении, легко поддается влиянию преступников, передавая конфиденциальную информацию, позволяющую им получать доступ к денежным средствам жертвы.

Результаты проведенного эмпирического исследования показывают, что склонность к кибервиктимному поведению обусловлена наличием определенных психологических особенностей эмоционального и межличностного характера. Выявление и уточнение данных особенностей позволит разработать эффективные программы по предупреждению преступности в киберпространстве. Как свидетельствуют результаты проведенного исследования, формирование и совершенствование таких личностных особенностей, как самоконтроль эмоциональных реакций и поведения, интернальность в межличностных отношениях, проницательность и дипломатичность, позволяют развивать способность противостоять преступным действиям мошенников в Интернете.

В то же время представляется важным отметить, что полученные результаты не могут быть экстраполированы на описание психологических особенностей кибервиктимной личности при совершении других преступных деяний в виртуальном пространстве. Следовательно, для выявления психологических характеристик, отражающих склонность к кибервиктимному поведению, необходимо расширить границы исследования, как в сторону привлечения большего количества респондентов, в том числе пострадавших от разных видов киберпреступлений, так и с включением других психодиагностических методик, которые позволят интерпретировать некоторые нюансы полученных результатов.

Литература

1. *Антонян Е.А., Клещина Е.Н.* Кибервиктимность // Вестник Пермского института ФСИН России. 2019. № 3 (34). С. 5–10.
2. *Белякова М.Ю., Булыгина В.Г., Токарева Г.М.* Социально-психологические и патопсихологические факторы риска совершения повторных общественно опасных деяний у лиц с негативно-личностными расстройствами [Электронный ресурс] // Психология и право. 2015. Том 5. № 1. С. 1–14. URL: https://psyjournals.ru/psyandlaw/2015/n1/76141.shtml (дата обращения: 16.01.2022).
3. *Булыгина В.Г., Абдразякова А.М., Коваленко И.В*. Методика оценки самоконтроля у несовершеннолетних // Судебная психиатрия. Судебно-психиатрическая экспертиза несовершеннолетних / Под ред. акад. РАМН Т.Б. Дмитриевой. М.: ФГУ «ГНЦ ССП Росздрава», 2008. Вып. 5. С. 14–28.

4. *Власова Н.В.* Психологическая профилактика вовлечения молодежи в киберпреступные сообщества // Благополучие и безопасность в условиях социальных трансформаций: материалы X Международного симпозиума (9–10 июля 2019 г.). Екатеринбург, 2019. С. 203–206.
5. *Жакупжанов А.О.* Виктимологические факторы киберпреступности // Алтайский юридический вестник. 2019. № 3 (27). С. 75–82.
6. *Кузнецова Л.Э., Ерошенко А.Н.* Психологические особенности проявления виктимного поведения у современной молодежи // Актуальные вопросы современной психологии: материалы II Междунар. науч. конф. Челябинск: Два комсомольца, 2013. С. 73–75.
7. *Макаревская Ю.Э., Беленко С.С.* Психология жертвы: взаимосвязь тенденции к самообвинению конформности личности // Коченовские чтения — 2020. Психология и право в современной России: сб. тезисов участников Всероссийской конференции по юридической психологии с международным участием. М.: МГППУ, 2020. С. 36–38.
8. *Мудрик А.В.* Виктимология. М.: Магистр, 2002. 524 с.
9. *Ривман Д.В., Устинов В.С.* Виктимология. СПб: Гардарика, 2000. 320 с.
10. *Сафуанов Ф.С., Докучаева Н.В.* Особенности личности жертв противоправных посягательств в Интернете [Электронный ресурс] // Психология и право. 2015. Том 5. № 4. С. 80–93. doi:10.17759/psylaw.2015050407
11. *Тропина Т.Л.* Борьба с киберпреступностью: возможна ли разработка универсального механизма? // Международное правосудие. 2012. № 3 (4). С. 86–95.
12. *Яценко Т.Е.* Психологическая диагностика виктимности как социально-психологического свойства личности // Актуальные проблемы современной науки, техники и образования. 2019. Том 10. № 2. С. 128–133.
13. *Ngo F.T., Paternoster R.* Cybercrime Victimization: An examination of Individual and Situational level factors // International Journal of Cyber Criminology. 2011. Vol. 5(1). P. 773–793.
14. *Gilboa N.* Elites, Lamers, Narcs and Whores: exploring the computer underground. In L. Cherny, E. R. Weise (eds.). Wired Women: Gender and New Realities in Cyberspace. Seattle: Seal Press, 1996. P. 98–113.
15. *Holt T.J., Bossler A.M.* Examining the applicability of lifestyle-routineactivities theory for cybercrime victimization // Deviant Behavior. 2009. Vol. 30(1). P. 1–25. doi:10.1080/01639620701876577
16. *Reyns B.W., Fisher B.S., Bossler A.M., Holt T.J.* Opportunity and Self-Control: Do they Predict Multiple Forms of Online Victimization? // American Journal of Criminal Justice. 2018. Vol. 44(1). P. 63–82. doi:10.1007/s12103-018-9447-5
17. *Schreck C.J., Wright R.A., Miller J.M.* A study of individual and situational antecedents of violent victimization // Justice Quarterly. 2002.Vol. 19(1). P. 159–180. doi:10.1080/07418820200095201

References

1. Antonyan E.A., Kleshchina E.N. Kiberviktimnost’ [Cyber Visibility]. *Vestnik Permskogo instituta FSIN Rossii = Vestnik of Perm Institute of the Federal Penal Service*, 2019, no. 3 (34), pp. 5–10. (In Russ.).
2. Belyakova M.Yu., Bulygina V.G., Tokareva G.M. Sotsial’no-psikhologicheskie i patopsikhologicheskie faktory riska sovershenia povtornykh obshchestvenno opasnykh deyanii u lits s negativno-lichnostnymi rasstroistvami [Socio-psycological and pathopsychological factors of risk of reoffending among mentally ill with negative personality disorders] [Elektronnyi resurs].

Psikhologiya i parvo = Psychology and Law, 2015. Vol. 5, no. 1, pp. 1–14. URL: https://psyjournals.ru/psyandlaw/2015/n1/76141.shtml (Accessed 16.01.2022) (In Russ.).

3. Bulygina V.G., Abdrazyakova A.M., Kovalenko I.V. Metodika otsenki samokontrolya u nesovershennoletnikh. *Sudebnaya psikhiatriya. Sudebno-psikhiatricheskaya ekspertiza nesovershennoletnikh.* Moscow: FGU "GNTs SSP Roszdrava" Publ., 2008. Vol. 5, pp. 14–28. (In Russ.).

4. Vlasova N.V. Psikhologicheskaya profilaktika vovlecheniya molodezhi v kiberprestupnye soobshchestva [Psychological prevention of youth involvement into cybercriminal communities]. *Blagopoluchie i bezopasnost' v usloviyakh sotsial'nykh transformatsii: materialy X Mezhdunarodnogo simpoziuma (9–10 iyulya 2019 g.) = Wellbeing and security in the face of social transformations. Proceedings of the X International Symposium (July, 9–10, 2019)*. Yekaterinburg, 2019, pp. 203–206. (In Russ.).

5. Zhakupzhanov A.O. Viktimologicheskie faktory kiberprestupnosti [Victimological factors of cybercrime]. *Altaiskii yuridicheskii vestnik = Altai Law Journal*, 2019, no. 3 (27), pp. 75–82. (In Russ.).

6. Kuznetsova L.E., Eroshenko A.N. Psikhologicheskie osobennosti proyavleniya viktimnogo povedeniya u sovremennoi molodezhi. Aktual'nye voprosy sovremennoi psikhologii: materialy II Mezhdunar. nauch. konf. Chelyabinsk: Dva komsomol'tsa. 2013, pp. 73–75. (In Russ.).

7. Makarevskaya Yu.E., Belenko S.S. Psikhologiya zhertvy: vzaimosvyaz' tendentsii k samoobvineniyu konformnosti lichnosti. *Kochenovskie chteniya — 2020. Psikhologiya i pravo v sovremennoi Rossii. Sbornik tezisov uchastnikov Vserossiiskoi konferentsii po yuridicheskoi psikhologii s mezhdunarodnym uchastiem.* Moscow: MGPPU Publ., 2020, pp. 36–38. (In Russ.).

8. Mudrik A.V. Viktimologiya. Moscow: Magistr, 2002. 524 p. (In Russ.).

9. Rivman D.V., Ustinov V.S. Viktimologiya. Saint Peterburg: Gardarika, 2000. 320 p. (In Russ.).

10. Safuanov F.S., Dokuchaeva N.V. Osobennosti lichnosti zhertv protivopravnykh posyagatel'stv v Internete [Personality characteristics of victims of illegal attacks on the Internet] [Elektronnyi resurs]. *Psikhologiya i parvo = Psychology and Law*, 2015. Vol. 5, no. 4, pp. 80–93. doi:10.17759/psylaw.2015050407 (In Russ.).

11. Tropina T.L. Bor'ba s kiberprestupnost'yu: vozmozhna li razrabotka universal'nogo mekhanizma? [Addressing the problem of cybercrime: is it possible to develop universal legal framework on the international level?] *Mezhdunarodnoe pravosudie = International Justice*, 2012, no. 3 (4), pp. 86–95. (In Russ.).

12. Yatsenko T.E. Psikhologicheskaya diagnostika viktimnosti kak sotsial'no-psikhologicheskogo svoistva lichnosti. *Aktual'nye problemy sovremennoi nauki, tekhniki i obrazovaniya = Actual Problems of Contemporary Science, Technology and Education*, 2019. Vol. 10, no. 2, pp. 128–133. (In Russ.).

13. Ngo F.T., Paternoster R. Cybercrime Victimization: An examination of Individual and Situational level factors. *International Journal of Cyber Criminology*, 2011. Vol. 5, no. 1, pp. 773–793.

14. Gilboa N. Elites, Lamers, Narcs and Whores: exploring the computer underground. In L. Cherny, E. R. Weise (eds.). *Wired Women: Gender and New Realities in Cyberspace*. Seattle: Seal Press, 1996. P. 98–113.

15. Holt T.J., Bossler A.M. Examining the applicability of lifestyle-routineactivities theory for cybercrime victimization. *Deviant Behavior*, 2009. Vol. 30, no. 1, pp. 1–25. doi:10.1080/01639620701876577

16. Reyns B.W., Fisher B.S., Bossler A.M., Holt T.J. Opportunity and Self-Control: Do they Predict Multiple Forms of Online Victimization? *American Journal of Criminal Justice*, 2018. Vol. 44, no. 1, pp. 63–82. doi:10.1007/s12103-018-9447-5
17. *Schreck C.J., Wright R.A., Miller J.M.* A study of individual and situational antecedents of violent victimization. *Justice Quarterly*, 2002. Vol. 19, no. 1, pp. 159–180. doi:10.1080/07418820200095201

Информация об авторах

Власова Наталия Викторовна, кандидат психологических наук, доцент, кафедра юридической психологии и права, факультет юридической психологии, Московский государственный психолого-педагогический университет (ФГБОУ ВО МГППУ), г. Москва, Российская Федерация, ORCID: https://orcid.org/0000-0002-3452-1133, e-mail: L1025173@yandex.ru

Буслаева Елена Леонидовна, кандидат психологических наук, доцент, доцент, кафедра психологии и педагогической антропологии, Институт гуманитарных и прикладных наук, Московский государственный лингвистический университет (ФГБОУ ВО МГЛУ), г. Москва, Российская Федерация, ORCID: https://orcid.org/0000-0002-1913-9198, e-mail: moselena2201@yandex.ru

Information about the authors

Nataliya V. Vlasova, PhD in Psychology, Associate Professor, Department of Legal Psychology and Law, Faculty of Legal Psychology, Moscow State University of Psychology and Education, Moscow, Russia, ORCID: https://orcid.org/0000-0002-3452-1133, e-mail: L1025173@yandex.ru

Elena L. Buslaeva, PhD in Psychology, Docent, Associate Professor, Department of Psychology and Pedagogical Anthropology, Institute of Humanities and Applied Sciences, Moscow State Linguistic University, Moscow, Russia, ORCID: https://orcid.org/0000-0002-1913-9198, Russia, e-mail: moselena2201@yandex.ru

Получена 16.02.2022
Принята в печать 16.04.2022

Received 16.02.2022
Accepted 16.04.2022