DOI: 10.31079/1992-2868-2020-17-4-150-157

ПСИХОЛОГИЧЕСКИЕ РЕСУРСЫ КИБЕРБЕЗОПАСНОСТИ ЧЕЛОВЕКА

К.И. Воробьева

М.В. Долгачев

Д.А. Заславский

В статье представлен анализ современных психологических исследований в области психологии кибербезопасности, на основе которого определены основные психологические ресурсы безопасной жизнедеятельности человека в цифровом мире, намечены перспективы их дальнейшего изучения.

Ключевые слова: киберпсихология, кибербезопасность, киберугроза, контентные и коммуникативные риски, ответственность, цифровая компетентность.

PSYCHOLOGICAL RESOURCES OF HUMAN CYBERSECURITY

K.I. Vorobyova

M.V. Dolgachev

D.A. Zaslavsky

The article presents an analysis of modern psychological research in the field of cybersecurity psychology, on the basis of which the main psychological resources of safe human life in the digital world are identified, and prospects for their further study are outlined.

Key word: cyberpsychology, cyber security, cyber threat, content and communication risks, responsibility, digital competence.

Актуальность названной темы обусловлена глобальной цифровизацией мирового пространства. Неоспоримый факт, что и компьютеры, и Интернет стали важнейшим достижением современного общества. Они совершают революцию в повседневной жизни человека и пронизывают все сферы жизнедеятельности: промышленность, сферу услуг, государственное управление, образование, досуг, творчество, устраняют расстояния и предлагают немедленный доступ к информации и общению. Значительная часть социальной активности современных людей реализуется в интернет-сообществах посредством использования интернет-техноло-

гий. Сегодня в социальных сетях Интернета как минимум каждый второй взрослый житель Земли проводит часть своей жизни. В июне 2017 г. только пользователями Facebook оказалось два миллиарда человек, и сеть растёт примерно на 17 % каждый год.

Несомненное позитивное значение для прогрессивного развития общества существенных цивилизационных изменений, связанных с цифровизацией жизни современного человека, порождает не только спектр новых технологических возможностей, но и новых угроз, определяет появление новых рисков для жизнедеятельности человека, что вызывает настоятельную необходимость их научного осмысления.

Воробьева Клариса Ивановна – доктор психологических наук, профессор кафедры социальной работы и психологии Тихоокеанского государственного университета (г. Хабаровск).

Vorobyova Klarisa Ivanovna – Doctor of Psychology, Professor of the Department of Social Work and Psychology at Pacific National University (Khabarovsk).

E-mail: klarisav2011@mail.ru

Долгачев Михаил Владимирович – кандидат технических наук, доцент кафедры промышленного и гражданского строительства Тихоокеанского государственного университета (г. Хабаровск).

Dolgachev Mikhail Vladimirovich – Candidate of Technical Sciences, Associate Professor of the Department of Industrial and Civil Engineering at Pacific National University (Khabarovsk).

E-mail: 007428@pnu.edu.ru

Заславский Дмитрий Александрович – аспирант кафедры социальной работы и психологии Тихоокеанского государственного университета (г. Хабаровск).

Zaslavsky Dmitrii Aleksandrovich – Postgraduate Student of the Department of Social Work and Psychology at Pacific National University (Khabarovsk).

E-mail: 2107_dima@mail.ru1.

«Вопреки распространенному мнению о том, что информационные воздействия (в частности, в рамках так называемых "информационных войн") имеют преимущественно "кибернетическую" природу, мы считаем, что исследования информационной безопасности должны опираться и на психологические данные» [4: с. 48].

Цель настоящей статьи – выявление психологических ресурсов кибербезопасности человека на основе анализа современных исследований в области психологии безопасности и определение перспектив их дальнейшего изучения.

Прежде чем перейти к анализу психологических ресурсов кибербезопасности человека, следует определить основные понятия, связанные с предметом настоящего исследования, появившиеся в научной литературе в конце 90-х гг. XX в.: киберпсихология, кибербезопасность, киберугрозы.

Киберпсихология определяется как отрасль психологии, объединяющая методологию, теорию и практику исследования видов, способов и принципов применения людьми социальных сервисов Интернет, где под социальными сервисами понимаются не только социальные сети (ru.wikipedia.org).

Кибербезопасность – процесс использования мер безопасности для обеспечения конфиденциальности, целостности и доступности данных (ru.wikipedia.org). Понятие кибербезопасности подразумевает под собой совокупность методов, технологий и процессов, предназначенных для защиты целостности сетей, программ и данных от цифровых атак.

Киберугроза – это незаконное проникновение или угроза вредоносного проникновения в виртуальное пространство для достижения политических, социальных или иных целей (ru.wikipedia.org).

Понятие кибербезопасности возникло с момента распространения такого явления, как кибератаки, цель которых является получение несанкционированного доступа к конфиденциальной информации, ее копирование, изменение или уничтожение. По данным Forbes, глобальный рынок кибербезопасности достиг \$75 млрд в 2015 г. и \$170 млрд в 2020 г. Этот стремительный и быстрый рост рынка обусловлен множеством технологических инноваций и тенденций, в том числе и постоянно меняющимися требованиями к безопасности. Киберугрозы могут иметь различные формы, основные из них: вредоносные программы (вид программного обеспечения (ПО), предназначенный для получения несанкционированного доступа к конфиденциальной информации или нанесения ущерба компьютеру, данным); социальная инженерия (методы, которые злоумышленники могут применять, чтобы обмануть человека, с целью получения конфиденциальной информации или несанкционированного доступа к системе информационных технологий);

фишинг (одна из самых популярных техник кибератаки, которая заключается в основном в обмане пользователя путем отправки поддельных электронных писем); вирусы-вымогатели (вымогательство денежных средств, которое осуществляется шифрованием и блокированием доступа к данным или компьютерной системе в целом, до тех пор, пока выкуп не будет выплачен. В случае выплаты выкупа нет 100%-ной гарантии, что данные и система будут восстановлены в исходное состояние).

Наиболее полная классификация видов киберугроз представлена в систематизированном перечне Ч. Ли [25], включающем: нарушение конфиденциальности и вторжение в частную жизнь; кражу идентичности; кражу интеллектуальной собственности; кибербуллинг, киберхарассмент, stalking; преднамеренный обман (клевета); спам; вторжение в область финансовых транзакций онлайн; вредоносное программное обеспечение и компьютерные вирусы; инвестиционные аферы и жульничество; виртуальные преступления (порнография и проституция, азартные игры и мошенничество с использованием аватара, реализация агрессивного и жестокого поведения в игровых виртуальных взаимодействиях и т.д.).

Существуют киберугрозы, которые нацелены на государственные, секретные, военные, политические инфраструктурные активы целого народа какого-либо государства. К таким угрозам относятся: кибертерроризм (нападение осуществляется на компьютерные сети или инфраструктуру террористическими организациями с целью идеологической и политической пропаганды); кибершпионаж (вид атаки на информационные технологии, выполняемый путем взлома и вредоносного ПО, для получения секретной государственной, стратегической, политической, экономической и военной информации без предварительного разрешения на ознакомление с этим данными); кибервойна (массштабная международная атака, которая осуществляется высококвалифицированными специалистами (хакерами), работающими под эгидой государства. Осуществляется проникновение в стратегически важные информационные системы другой страны с целью скомпрометировать конфиденциальные данные, нанести ущерб инфраструктуре, нарушить связь и т.д.).

Современные исследователи подчеркивают, что как бы ни совершенствовались технические средства и способы защиты от постоянно меняющихся технических киберугроз, наиболее уязвимым звеном безопасного взаимодействия в цифровой среде остается человек. По данным социологических исследований, в последние годы наблюдается динамика изменения характера кибератак. Применение эксплоитов за 2015–2018 гг. сократилось в 55 раз, а

использование методов социальной инженерии за тот же период увеличилось более чем в 25 раз (Отчет компании Trend Micro за 2018 г.), что свидетельствует о направленности кибератак на уязвимые человеческие качества. В конце июля 2019 г. в Орландо (штат Флорида, США) прошла Первая международная конференция HCI for Cybersecurity, Privacy and Trust по вопросам безопасности человека-компьютерного взаимодействия. В 2019 г. в Вашингтоне (США) состоялась ежегодная Международная конференция ANFE, посвященная проблеме человеческого фактора в кибербезопасности. Огромное количество конференций, проведенных в России за 2018–2020 гг. по проблемам кибербезопасности, содержат в своих программах обсуждение проблем, связанных с человеческим фактором в обеспечении безопасности в онлайн-среде. Анализ содержания представленных на конференциях докладов позволяет говорить о направленности научного интереса современных психологов и специалистов в области информационной безопасности на изучение психологических факторов, в частности на анализ индивидуально-личностных качеств пользователя Интернета (специфика эмоционального реагирования, мотивационно-ценностные аспекты, персональный жизненный опыт и его рефлексивная оценка и т.д.), определяющих психологическую устойчивость к киберугрозам в процессе взаимодействия человека с IT-технологиями.

По мнению отечественных психологов, наибольшую опасность, особенно для молодежи, представляют контентные, коммуникативные риски и риск интернет-зависимости (Исследования Фонда развития Интернета, Г.У. Солдатов, Е.И. Рассказова и др., 2009–2012).

1. Контентные риски. Контентные риски возникают в процессе использования находящихся в сети материалов, содержащих противозаконную, неэтичную и вредоносную информацию (насилие, агрессия, порнография, ненавистнический контент, нецензурная лексика, информация, разжигающая расовую ненависть, пропаганда анорексии и булимии, суицида, азартных игр, наркотических веществ и т.д.). Столкнуться с ними можно в социальных сетях, блогах, на персональных сайтах, видеохостингах.

Отмечается отрицательное воздействие негативного контента на личность молодого человека. Навязывание через социальные сети новых образцов опасного поведения (например, суицидального поведения), искажение представлений о мире, девальвация традиционных ценностей; пропаганда нездоровых интересов и увлечений, средств соблазна и совращения привели к росту суицидов в среде подростков и юношества, повышению агрессивности и цинизма в молодежной среде, формированию асоциального поведения [10].

2. Интернет-зависимость. Говоря о рисках цифровой среды, как российские так, и зарубежные исследователи отмечают проблему чрезмерного использования Интернета. Интернет-зависимость – применение IT-технологий во вред себе и другим, порождающее конфликт с другими сферами жизни и вызывающее переживание потери контроля над собой (К. Янг). Наиболее используемый в современных исследованиях термин – «расстройство, связанное с использованием Интернета» (Internet Use Disorder – IUD).

Большинство исследователей феномена интернет-зависимости единодушны во мнении, что чрезмерное использование Интернета связано с неблагоприятными эмоциональными состояниями и целым рядом психических нарушений [11; 20; 22]. Имеются достоверные данные о наличии значимой обратной связи между удовлетворенностью жизнью и IUD, а также прямой связи между IUD и такими расстройствами, как депрессия, синдром дефицита внимания и гиперактивности, бессонница и/или чрезмерная сонливость в дневное время, злоупотребление психоактивными веществами. Установлена причинно-следственная связь между реактивной депрессией и IUD [20].

М. Бранд и соавторы разработали процессуальную модель, которая раскрывает сложные динамические аспекты целого ряда специфических нарушений, возникающих в результате взаимодействия человека и информационной среды. Модель реализует диатез-стрессовый подход к этиологии расстройств, связанных с избыточным присутствием в киберпространстве, согласно которому разного рода интернет-аддикции являются следствием взаимодействия определенных конституциональных черт пользователя, его личностных характеристик, когнитивных особенностей, с одной стороны, и неблагоприятных жизненных обстоятельств, с другой стороны. Причем ключевую роль играют именно внутренние факторы, которые определяют уязвимость психики по отношению к стрессовым средовым воздействиям [21]. В рамках названного подхода Д. Кардефельт-Винтер [22] установил, что чрезмерная вовлеченность в киберкоммуникации является реакцией человека на негативную жизненную ситуацию: увеличение времени, проводимого в интернет-среде, позволяет смягчить тяжелые переживания и снизить уровень стресса за счет переключения на деятельность, вызывающую приятные эмоции. Однако, как справедливо отмечает Г. Солдатов, стратегия избегания во многих случаях является неэффективной, так как вместо поиска конструктивных способов преодоления жизненных трудностей человек сосредоточивает свои усилия на избегании контакта с травмирующей реальностью, всё более погружаясь в кибермир, пребы-

вание в котором создает иллюзию эмоционального баланса [10].

Отмечается неоднозначность оценки времени, проведенного пользователем в цифровой среде, и его влияния на психику человека. В этой связи современные исследования интернет-зависимости направлены на анализ взаимосвязи пользовательской активности человека и продолжительности нахождения в киберпространстве с содержательной стороной социальной ситуации развития и особенностей деятельности. Доказано, что одно и то же время пребывания в Интернете может быть связано как с творческой и развивающей деятельностью, так и с разрушающими социальными связями проявлением интернет-аддикции (М. Гриффитс).

Следует различать также интернет-зависимость от продолжительной во времени деятельности субъекта в Интернете, которая обусловлена переживанием так называемого опыта потока. М. Чиксентмихайи и его последователи понимают опыт потока как специфическое состояние полной поглощенности деятельностью, в котором действие следует за действием согласно своей внутренней логике, а результат деятельности и ее реальная продолжительность отходят в сознании субъекта на второй план. При этом деятельность выполняется субъектом с удовольствием, без заботы о ее конечном результате. «Опыт потока и радость от его переживания способствуют возникновению мотивации, побуждающей и в дальнейшем переживать этот опыт, стремиться выполнять соответствующую деятельность» [15].

3. Коммуникационные риски. Специалисты утверждают, что зоной повышенной опасности в интернет-пространстве является коммуникация. Прежде всего, отмечается нарастание агрессивных форм интернет-взаимодействия. Исследователями определены наиболее распространенные в Интернете виды агрессии: флейминг, троллинг, хейтинг, киберсталкинг, кибербуллинг, онлайн-груминг.

Ряд отечественных и зарубежных авторов выделяют в качестве самостоятельной киберугрозы травлю в сетевых коммуникациях – кибербуллинг [2; 10; 23]. Кибербуллинг охватывает использование форумов, чатов, блогов, веб-страниц, электронной почты, сетевых компьютерных игр и приложений, мобильных сообщений (MMS и SMS) и любых других информационно-коммуникационных технологий [3]. Согласно данным, полученным исследователями разных стран, наиболее уязвимой группой для кибербуллинга являются подростки [2; 10; 23]. Зафиксированы случаи суицида студентов университетских колледжей США, ставших жертвами кибербуллинга [32]. Среди наиболее распространенных форм кибербуллинга, с которыми они сталкивались, респонденты называли сплетни в социаль-

ных сетях, издевки, насмешки и обидные прозвища, транслируемые онлайн [32].

Кэтфишинг – один из видов современных угроз, заключается в создании некой виртуальной личности для вовлечения своих подписчиков в какие-либо отношения с целью вымогательства денежных средств, использования их персональных данных для последующего шантажа и т.д. Человек, который притворяется тем, кем он не является, и создает ложные личные профили, например на Facebook или в других социальных сетях, со злонамеренными целями, называется *catfish*. Среди его мотивов следует назвать одиночество, скуку и зависть. Жертвы кэтфишинга испытывают смущение, гнев, раздражение и другие разнообразные негативные эмоции, когда в конце концов узнают, что стали жертвой обмана со стороны персонажа, в отношениях с которым они находились длительное время и которого считали реальным человеком [27].

Столкновение с коммуникационными рисками – наиболее серьезная проблема для молодых пользователей и по сравнению с другими видами онлайн-рисков чаще причиняет им ощутимый вред. В настоящее время отмечается высокая интенсивность взаимодействия молодежи в виртуальной среде. Личное пространство старшеклассников и студентов переполнено виртуальными друзьями. По данным исследователей Фонда развития Интернета, каждый второй подросток имеет виртуальных друзей, с которыми он ни разу не встречался в реальной жизни, однако предоставляет им доступ к персональной информации, поддерживает регулярную и близкую коммуникацию, а также рассматривает возможность реальной встречи с ними. Виртуальный друг становится более предпочтительным, чем знакомый. Виртуальные друзья в иерархии межличностных связей старшеклассников занимают второе место. Из числа школьников, имеющих виртуального друга, доля тех, кто доверит ему тайну, более чем в семь раз превышает число тех, кто расскажет секрет знакомому [10].

Таким образом, современная ситуация, сложившаяся в цифровой среде, предполагает изучение не только технических возможностей предотвращения угрожающего взаимодействия человека в цифровой среде, но и необходимых для безопасного поведения в киберпространстве психологических качеств пользователя ИТ-технологиями.

Анализ исследований безопасного поведения человека в цифровой среде позволяет выделить его основные психологические компоненты:

- сформированные знания умения и навыки в области цифровых технологий;
- сформированные представления человека об интернет-угрозах, возможностях их минимизации и преодоления;

– сформированные стратегии преодоления интернет-угроз, а именно способность адекватно оценить степень опасности, провести анализ собственных внутренних и доступных внешних ресурсов, необходимых для ее преодоления, грамотно выбрать стратегию и технологию поведения, в случае необходимости привлечь носителей внешних ресурсов, самостоятельно или с доступной поддержкой осуществить необходимые действия, нести ответственность за любые (в том числе и негативные) последствия собственной цифровой активности.

Названные психологические характеристики безопасного поведения в киберпространстве говорят о том, что реализация такого поведения возможна лишь при наличии развитых личностных ресурсов, помогающих преодолеть сложную, опасную ситуацию (ответственность, критическое мышление, стрессоустойчивость, умение попросить помощь и принять ее и т.д.).

В современных отечественных и зарубежных исследованиях в области психологии кибербезопасности имеется ряд доказательств влияния когнитивных, личностных и мотивационных характеристик на кибербезопасное поведение человека.

В научных исследованиях зарубежных ученых (например, Junglas, Johnson, & Spitzmüller, 2008; Korzaan & Boswell, 2008; Taddicken, 2014) отмечается, что забота о кибербезопасности связана с личностными качествами пользователя Интернета и других социальных сетей. Так, например, установлено, что излишняя доверчивость пользователя приводит к снижению уровня личной цифровой безопасности.

Экспериментально установлено влияние самооценки на безопасное поведение в цифровом пространстве. Как утверждают исследователи, адекватная самооценка позволяет критично относиться к информации, в случае киберугроз использовать эффективные копинг-стратегии, принимать адекватные ситуации решения. Заниженная самооценка приводит к высокому уровню тревожности при возникновении киберугрозы, к неэффективным стратегиям совладания, к ошибочным действиям [18; 29].

Отдельное внимание обращается на такие явления, как киберфобия, компьютерная тревожность, техностресс и др. Чаще всего означенные явления наблюдаются среди пользователей пожилого возраста, которые испытывают «комплекс неполноценности» в цифровой среде, боязнь перед современными технологиями, в основе которых лежат: страх выйти за пределы личной зоны комфорта, страх совершить ошибку. При этом пожилые пользователи испытывают не боязнь новых навыков как таковых, а страх оказаться не способными их освоить, потерять самоуважение, лишиться уже достигнутого. Заниженная самооценка своих возможно-

стей в овладении цифровыми технологиями, отсутствие планов успешного преодоления цифровых барьеров исходят из сопротивления мысли о том, что изменения, связанные с цифровизацией жизни современного человека, не вопрос будущего, а вопрос настоящего, и что эти изменения происходят с ними уже здесь и сейчас [18].

Что касается завышенной самооценки пользователя, исследования Фонда развития Интернета выявили ее отрицательную связь с мотивацией повышения уровня цифровой грамотности у подростков. «Иллюзорная компетентность» в области цифровых технологий, ярко выраженная у подростков, приводит к отрицанию киберугроз, пренебрежению мерами безопасности и в итоге к безответственному поведению в цифровой среде [10].

В зарубежных исследованиях, посвященных влиянию нарциссизма на кибербезопасное поведение пользователя, отмечается, что люди с выраженной степенью нарциссизма чаще сталкиваются с киберугрозами и забывают о мерах собственной безопасности в онлайн-пространстве. Личностная черта нарциссизма концептуализируется как саморегулирующий процесс, в котором лица с высокой степенью нарциссизма самосовершенствуются для получения обратной связи в соответствии с их завышенными самооценками (Morf and Rhoewalt, 2001; Campbell and Foster, 2007). Виртуальные среды предоставляют больше возможностей для самопрезентации, чего нет в реальной среде, и, таким образом, становятся главной социальной площадкой для процветания нарциссизма (Campbell, Reeder, Sedikides, & Elliot, 2000). Нарциссизм становится все более распространенным в молодом поколении. В погоне за лайками «молодые нарциссы» игнорируют меры личной кибербезопасности (Твенге Конрат, Foster, Campbell, & Bushman, 2008) [26].

С другой стороны, люди с высокими баллами по Черной триаде (нарциссизм, психопатия, макиавелизм), не достигшие уровня клинического расстройства, часто проявляют киберагрессию в цифровом мире и являются организаторами интернет-троллинга [26].

Эмпирические исследования, проведенные зарубежными психологами, доказывают, что важными психологическими ресурсами кибербезопасности человека являются: удовлетворенность собственным благополучием, наличие семейного и дружеского круга общения, социальная активность пользователя, коммуникативная компетентность. Отсутствие дружеских отношений, трудности в общении, завязывании новых контактов, одиночество приводят к повышению уровня тревоги и депрессии, имеющему прямую взаимосвязь с опасным поведением в киберсреде. Имеется целый ряд исследований, доказывающих, что тревога и де-

прессия чаще всего связаны с интернет-зависимостью [18].

В настоящее время в зарубежной психологии изучение когнитивно-мотивационных ресурсов кибербезопасного поведения человека активно развивается в рамках теории мотивации защит (Rogers, 1975). В частности, проводятся исследования взаимосвязи индивидуального восприятия киберугрозы и способов совладающего поведения. Основные аспекты теории мотивации защиты включают в себя:

- воспринимаемую человеком серьезность угрожающего сценария;
- воспринимаемую человеком собственную уязвимость в этом сценарии;
- воспринимаемую человеком эффективность собственного защитного поведения в снижении уязвимости к угрожающему сценарию (эффективность реагирования);
- воспринимаемую человеком собственную способность к соответствующему защитному поведению (самоэффективность) [33].

По мнению исследователей, эффективность кибербезопасности в обществе, на конкретном предприятии, в частной жизни зависит от личной осознанности каждым человеком реальности угрозы для себя и своих близких, способности оценивать серьезность угроз и их последствия как для себя, так и в масштабах учреждения, предприятия, общества в целом. Таким образом, сторонники теории мотивации среди множества индивидуально-личностных качеств человека – пользователя Интернета определяют в качестве основных мотивационные характеристики.

Результаты научных исследований сторонников теории мотивации защит находят практическое применение в обучающих и тренинговых программах по развитию способности адекватного восприятия угроз, их последствий, оценки своих ресурсов для их преодоления, по формированию и развитию навыков безопасного поведения человека в цифровой среде.

Следует отметить, что в отечественной психологии в рамках Фонда развития Интернета проводятся широкомасштабные исследования в области киберпсихологии, в том числе кибербезопасности, на большой выборке российских подростков и их родителей [10]. Особое внимание коллектива ученых, работающих под руководством профессора МГУ им. Ломоносова Г. Солдатовой, направлено на изучение цифровой компетентности как системообразующего свойства личности, обеспечивающего кибербезопасное поведение человека в цифровой среде [10].

Рассматривая цифровую компетентность как сложный комплексный феномен, определяющий сегодня жизнедеятельность человека в разных сфе-

рах информационного общества, ученые выделяют в ней соответственно четыре вида компетентности.

1. Информационная и медиакомпетентность: знания, умения, мотивация и ответственность, связанные с поиском, пониманием, организацией, архивированием цифровой информации и ее критическим осмыслением, а также с созданием информационных объектов с использованием цифровых ресурсов (текстовых, изобразительных, аудио и видео).

2. Коммуникативная компетентность: знания, умения, мотивация и ответственность, необходимые для различных форм коммуникации (электронная почта, чаты, блоги, форумы, социальные сети и др.) и с различными целями.

3. Техническая компетентность: знания, умения, мотивация и ответственность, позволяющие эффективно и безопасно использовать технические и программные средства для решения различных задач, в том числе использования компьютерных сетей, облачных сервисов и т.п.

4. Потребительская компетентность: знания, умения, мотивация и ответственность, позволяющие решать с помощью цифровых устройств и Интернета различные повседневные задачи, связанные с конкретными жизненными ситуациями, предполагающими удовлетворение различных потребностей.

Следует обратить внимание, что названные виды компетентности включают в свое содержание мотивацию и ответственность, что согласуется с выводами представителей теории мотивации защит. Несмотря на важность и необходимость знаний в области IT-технологий, наличие развитых умений и навыков пользования современными цифровыми средствами, достижение безопасности в киберпространстве возможно лишь в их сочетании с ответственным поведением в киберпространстве и личным убеждением человека в необходимости соблюдения необходимых правил цифровой безопасности.

Несомненным достоинством названных исследований является создание моделей цифровой компетентности, которые могут служить основанием дальнейшего теоретического анализа проблем безопасности человека в цифровой среде, построения экспериментальных программ и сбора эмпирических данных.

Выводы

В новом тысячелетии изменение образа жизни человека, связанное со стремительным и повсеместным внедрением IT-технологий в обыденную жизнь, расширяет поле научных исследований в области кибербезопасности. Фокус внимания смещается на изучение многочисленных киберугроз и способов их предупреждения, развитие навыков безопасного поведения человека и поиск психоло-

гических ресурсов кибербезопасного поведения и сохранения благополучия в цифровом мире.

Безусловно, за последние 20 лет отечественными и зарубежными психологами собран богатый эмпирический и экспериментальный материал по психологии безопасности человека в цифровой среде. На наш взгляд, дальнейшие исследования в названной отрасли психологии должны быть направлены:

- на разработку методологических оснований психологических исследований в области психологии безопасности человека в цифровом мире с учетом междисциплинарности проблемы;
- создание психометрического инструментария, соответствующего предмету исследования;
- дальнейшее более глубокое изучение механизмов безопасного поведения человека в киберпространстве, психологических факторов, способствующих безопасной жизнедеятельности и благополучию в новой для человека цифровой среде, психологических ресурсов противодействия кибервиктимизации человека, возможностей самореализации и творчества в цифровом мире и т.д.

Кибербезопасность человека – проблема междисциплинарная и требует комплексного подхода в ее изучении, объединения усилий ученых разных научных направлений по разработке эффективных и доступных способов защиты человека от киберугроз.

Кибербезопасность человека – проблема государственной важности, требующая поддержки в ее решении на всех уровнях государственной власти, совместной деятельности работников и руководителей различных учреждений и ведомств, представителей общественных организаций, СМИ и т.д. Уже сегодня необходимо предпринимать активные действия:

- по повышению уровня цифровой культуры и ответственности каждого человека за поведение в цифровом пространстве;
- активной пропаганде важности и необходимости соблюдения правил безопасного поведения в цифровой среде каждым пользователем;
- развитию умений и навыков безопасного поведения в цифровом пространстве через специальные обучающие программы как для детей, так и для взрослых и т.д.

Повышение уровня кибербезопасности каждого человека – это задача сегодняшнего дня. Завтра будет поздно.

ЛИТЕРАТУРА

1. Айсина, Р.М. Психологическая безопасность взрослых: анализ современных исследований интернет-пользователей / Р.М. Айсина // Вестник Омского университета. – 2019. – № 1. – С. 28–38. – (Серия «Психология»).
2. Бочавер, А.А. Кибербуллинг: травля в пространстве современных технологий / А.А. Бочавер, К.Д. Хломов //

Психология. Журнал Высшей школы экономики. – 2014. – Т. 11, № 3. – С. 177–191.

3. Брижак, С.Н. Когнитивная безопасность в кибербезопасности / С.Н. Брижак // Передовые научные исследования: опыт и актуальные вопросы : сборник докладов Междунар. науч.-практ. конф. / под ред. Р.Д. Иванова. – Санкт-Петербург : ЕНМЦ «Мультидисциплинарные исследования», 2019. – С. 63–72.

4. Войсунский, А.Е. Информационная безопасность: психологические аспекты / А.Е. Войсунский // Национальный психологический журнал. – 2010. – № 1 (3). – С. 48–53.

5. Войсунский, А.Е. Концепции зависимости и присутствия применительно к поведению в Интернете / А.Е. Войсунский // Медицинская психология в России. – 2015. – № 4 (33). – С. 6. – URL: http://mprj.ru/archiv_global/2015_4_33/nom_er07.php (дата обращения: 05.05.2018).

6. Канеман, Д. Думай медленно... Решай быстро / Д. Канеман. – Москва : АСТ, 2013.

7. Маклюэн, М. Галактика Гуттенберга. Становление человека печатающего / М. Маклюэн. – Москва : Академический проект, 2005. – 288 с.

8. Нестик, Т.А. Технофобы и технофилы: разные модели цифровой компетентности / Т.А. Нестик, Г.У. Солдатова // Человеческий фактор: проблемы психологии и эргономики. – 2016. – № 1 (77). – С. 15–20.

9. Ротман, Ю.А. Человек и стратегии вмешательства: подход к пониманию поведения, связанного со здоровьем / Ю.А. Ротман, С.А. Болдуин // Ученые записки Оксфордского университета по психологии личности и социальной психологии. – 2012. – С. 729–752.

10. Нестик, Т.А. Цифровое поколение России: компетентность и безопасность / Т.А. Нестик, Г.У. Солдатова, Е.И. Рассказова. – 2-е изд. – Москва : Смысл, 2018. – 375 с.

11. Связь опыта потока с психологической зависимостью от компьютерных игр / Ш.Л. Ван [и др.] // Психология. Журнал Высшей школы экономики. – 2011. – Т. 18, № 4. – С. 73–101.

12. Benson, V. Emerging Cyber Threats and Cognitive Vulnerabilities. / V. Benson, J. McAlaney // Elsevier Inc. 2020. Chapter 1 – Factors leading to cyber victimization. Academic Press. – 2020. – P. 1–25.

13. Benson, V. Emerging Cyber Threats and Cognitive Vulnerabilities / V. Benson, J. McAlaney // Elsevier Inc. 2020. Chapter 4 – The social and psychological impact of cyberattacks. Academic Press. – 2020. – P. 73–92.

14. Bone, J. Cognitive Hack. The New Battleground in Cybersecurity... the Human Mind / J. Bone // Taylor & Francis Group, LLC. – P. 10–17.

15. Csikszentmihalyi, M. Beyond boredom and anxiety: experiencing flow in work and play / M. Csikszentmihalyi. – San Francisco : Jossey-Bass, 2000.

16. Davis, R.A. A cognitive-behavioral model of pathological internet use / R. A. Davis // Computers in Human Behavior. – 2001. – Vol. 17 (2). – P. 187–195.

17. Delaney, T. Friendship and Happiness: And the Connection Between the Two / T. Delaney, T. Madigan. – North Carolina : McFarland & Company, Inc., Publishers, 2017. – 296 p.

18. Diomidous, M. Social and Psychological Effects of the Internet Use / M. Diomidous [et al.] // Acta Informatica Medica. – February, 2016.

19. Dowling, N.A. Screening for internet dependence: Do the proposed diagnostic criteria differentiate normal from dependent internet use? / N.A. Dowling, K.L. Quirk // Cyberpsychology & Behavior. – 2009. – Vol. 12 (1). – P. 21–27.

20. *Gámez-Guadix, M.* Depressive symptoms and problematic internet use among adolescents: Analysis of the longitudinal relationships from the cognitive-behavioral model / *M. Gámez-Guadix* // *Cyberpsychology, Behavior and Social Networking*. – 2014. – Vol. 17 (11). – P. 714–719.
21. Integrating psychological and neurobiological considerations regarding the development and maintenance of specific internet-use disorders: An interaction of person-affect-cognition-execution (i-pace) model / *M. Brand* [et al.] // *Neuroscience & Biobehavioral Reviews*. – 2016. – Vol. 71. – P. 252–266.
22. *Kardefelt-Winther, D.A.* conceptual and methodological critique of internet addiction research: Towards a model of compensatory internet use / *D. Kardefelt-Winther* // *Computers in Human Behavior*. – 2014. – Vol. 31. – P. 351–354.
23. *Kowalski, R.M.* Cyberbullying: Bullying in the digital age (2nd ed.). / *R.M. Kowalski, S.P. Limber, P.W. Agatston*. – Chichester : Wiley-Blackwell, 2012. – 274 p.
24. *Kowalski, R.M.* Cyberbullying: Bullying in the digital age / *R.M. Kowalski, S.P. Limber, P.W. Agatston*. – 2nd ed. – Chichester : Wiley-Blackwell, 2012. – 274 p.
25. *Lee, C.Y.* Understanding Security Threats in Virtual Worlds / *C.Y. Lee* // *AMCIS*. – California, 2009. – 466 p. – URL: <http://aisel.aisnet.org/amcis2009/466> (accessed: 05.05.2018).
26. *Mccain, J.* Virtual worlds afford self-enhancement for narcissism Athens / *J. McCain*. – Georgia, 2018. – 257 p.
27. *Sharabi, L.L.* Deception in online dating: Significance and implications for the first offline date / *L.L. Sharabi, J.P. Caughlin* // *New Media & Society*. – 2018. – Vol. 21(1). – P. 1–19.
28. *Stavropoulos, V.* Physical, Emotional, and Identity User-Avatar Association with Disordered Gaming: A Pilot Study / *V. Stavropoulos* [et al.] // *International Journal of Mental Health and Addiction*. – 2019. – URL: <https://doi.org/10.1007/s11469-019-00136-8> (accessed: 05.05.2018)
29. The psychology of privacy in the digital age / *A. Stuart* [et al.] // *Engineering and Physical Sciences Research Council, Grant*. – URL: <https://doi.org/10.1111/spc3.12507> (accessed: 28.11.2020).
30. The relationship between Internet Use Disorder, depression and burnout among Chinese and German college students / *J. Peterka-Bonetta* [et al.] // *Addictive Behaviors*. – 2019. – Vol. 89. – P. 188–199.
31. *Walker, C.M.* An exploratory study of cyberbullying with undergraduate university students / *C.M. Walker, B.R. Sockman, S. Koehn* // *TechTrends*. – 2011. – Vol. 55 (2). – P. 31–38.
32. *Washington, E.T.* An Overview of Cyberbullying in Higher Education / *E.T. Washington* // *Adult Learning*. – 2015. – Vol. 26 (1). – P. 21–27.
33. *Williams, E.J.* How Do We Ensure Users Engage in Secure Online Behavior? A Psychological Perspective / *E.J. Williams, J. Noyes, B. Warinschi* // Paper presented at International Conference on Cognitive and Behavioral Psychology. – 2018. – URL: https://doi.org/10.5176/2251-1865_CBP18.49 (accessed: 28.11.2020).