обзоры и современные исследования. – 2023. – Т. 12. – № 3А-4А. – С. 22-33. DOI: 10.34670/AR.2023.37.13.003.

6. Дикая, Л.Г. Психическая саморегуляция функционального состояния человека (системно-деятельностный подход) / Л.Г. Дикая. – М.: Институт психологии РАН, 2003. – 320 с.

7. Прохоров А.О. Образ психического состояния / А.О. Прохоров. – М.: Институт психологии РАН, 2016. – 245 с.

8. Прохоров, А.О. Опросник «Факторы психических состояний» / А.О. Прохоров, А.В. Макарчева // Психология психических состояний: сборник материалов XVI Международной научнопрактической конференции для студентов, магистрантов, аспирантов, молодых ученых и преподавателей вузов. – Казань: Изд-во Казанского университета, 2022. – Вып. 16. – С. 266-272.

9. Карпов, А.В. Рефлексивность как психическое свойство и методика её диагностики / А.В. Карпов // Психологический журнал. – 2003. – Т. 24. – № 5. – С. 45-57.

10. Прохоров, А.О. Методики диагностики и измерения психических состояний личности / А.О.Прохоров. – М.: ПЕР СЭ, 2004. – 176 с.

11. Андреева, И.Н. Биологические и социальные предпосылки эмоционального интеллекта [текст] / И.Н. Андреева // Когнитивная психология: сб. статей; под ред. А.П. Лобанова, Н.П. Радчиковой. – Мн.: БГПУ, 2006. – С. 7-11.

12. Леонова, А.Б. Структурно-интегративный подход к анализу функциональных состояний: история создания и перспективы развития / А.Б. Леонова, А.С. Кузнецова // Вестник Московского университета. – 2019. – Серия 14. Психология. – №1. – С. 13-33.

13. Дегтярев, В.П. Взаимосвязь успешности обучения и индивидуально-типологических свойств студентов / Вестник РАМН. – 2007. – №1. – С. 30-36.

14. Андреева, Е.А. Особенности проявления стресса у студентов во время сдачи экзаменационной сессии / Е.А. Андреева, С.А. Соловьева // Азимут научных исследований: педагогика и психология. – 2016. – № 1. – С. 140-143.

УДК 004.056.5

КОГНИТИВНЫЕ АСПЕКТЫ КИБЕРБЕЗОПАСНОСТИ

Джумагулов Нуржанат Нуржанович[1], Карникова Ольга Павловна[1,2]

[1]Самарский национальный исследовательский университет имени академика С.П. Королева
[2]Самарский государственный институт культуры

Аннотация: *Статья посвящена исследованию когнитивных аспектов кибербезопасности, влияния особенностей мышления и поведения на процесс принятия рискованных решений в онлайн-среде. Рассмотрены ошибки, приводящие к небезопасным действиям в сети Интернет, способы повышения уровня киберграмотности студентов как активных пользователей цифровых инструментов, методы защиты от современных киберугроз.*

Ключевые слова: *когнитивные технологии, информационная безопасность, киберпсихология, человеческий фактор, киберграмотность.*

Кибербезопасность стала одной из наиболее актуальных проблем современного мира, включая устранение уязвимостей информационных систем, обеспечение их защиты от киберугроз, хакерских атак, вирусов, фишинга и других видов киберпреступности. В эпоху цифровизации и всеобщей доступности онлайн-среды защита своих данных и личной информации становится все более сложной задачей. Несмотря на развитие технических средств, разнообразие методов и практик защиты от атак злоумышленников, несанкционированного доступа, повреждения компьютеров, серверов и мобильных устройств, большую роль в обеспечении кибербезопасности продолжает играть человеческий фактор. Недостаточная осведомленность пользователей, их уязвимость перед социальной инженерией, отсутствие навыков применения критического мышления в информационном пространстве зачастую приводят к принятию рискованных решений в цифровой среде. Как показали современные исследования, в последние годы увеличивается доля россиян, которые выражают тревогу по поводу защиты своих личных данных в онлайн-пространстве [1], что свидетельствует о недостаточно высоком уровне их цифровой компетенции, навыков использования информационных и коммуникационных технологий, безопасного взаимодействия в онлайн-среде.

В настоящее время с целью осознания необходимости повышения компьютерной безопасности проводятся исследования, посвященные динамике инцидентов успешных кибератак [2], изучается уровень киберграмотности в современном обществе (Ю.Б. Надточий, М.Е. Гурова) [3], особенности и проблемы внедрения когнитивных технологий в модель обеспечения информационной безопасности (Д.О. Сулейманова, Т.Р. Магомаев) [4]. В ряде статей подробно рассматриваются формы кибервиктимизации, как процесса или конечного результата «становления жертвы преступления в сфере объединённых компьютерных сетей» [5, с. 111], выявления ее масштабов, детерминирующей роли гендерных, возрастных, поведенческих и личностных факторов (Д.В. Жмуров [5], Никешин [6]). Опубликованы работы, в которых раскрываются способы внедрения учебных мероприятий по повышению уровня киберграмотности населения (А.А. Бердюгин, П.В. Ревенков [7]), повышению уровня цифровой грамотности студентов (А.М. Юдина, А.У. Менциев, А.В. Кисиленко [8]), детей, начиная с младшего возраста (М.Г. Пономарева, А.В. Янкевский [9]).

Однако в современных исследованиях недостаточное внимание уделяется теоретическому анализу когнитивных аспектов кибербезопастности, влияния личностных особенностей на принятие рискованных решений в цифровой среде. Цель данной статьи заключается в теоретическом изучении когнитивных аспектов кибербезопасности, характеристик наиболее эффективных способов повышения уровня киберграмотности студентов высших учебных заведений как пользователей современных цифровых технологий.

Изучение безопасного поведения человека в цифровой среде позволяет выделить основную психологическую особенность данного процесса: сформированность знаний и умений в области цифровых технологий помогает пользователям справиться со сложными и опасными ситуациями (например, умение принимать решения, анализировать информацию, управлять стрессом, обращаться за помощью и принимать ее и т.д.). Среди параметров, существенно влияющих на способность людей эффективно защищать себя в сети (верно оценить подозрительное поведение устройств, использовать доступные ресурсы и верные стратегии защиты), следует отметить уровень образования, опыт работы с компьютерами, когнитивные способности, уровень самосознания. К когнитивным аспектам кибербезопастности можно отнести и заниженную самооценку, которая способна привести к низкому уровню мотивации к обучению и

формированию критического мышления, отсутствие желания соблюдения этических норм в информационной среде.

Активное применение цифровых технологий в системе высшего образования актуализирует вопрос осведомленности обучающихся о методах защиты их личной информации, предотвращении кибератак и обеспечении конфиденциальности данных. Однако, действия молодых людей в онлайн-среде часто подвержены ошибкам мышления, которые могут привести к небезопасным последствиям. Среди таких ошибок следует выделить: эффект подтверждения, который заключается в поиске информации на основе уже имеющихся убеждений или предпочтений; эвристика доступности, определяющая склонность придавать большее значение информации, которая легко доступна в памяти [10]; эффект Барнума-Форера, характеризующийся повышенным доверием к предложениям и запросам неизвестных или малоизвестных источников [11]; эффект социального доказательства, обозначающий следование за поведением других пользователей, не задумываясь о возможных рисках [12]. К основным методам кибербезопастности, которые должны освоить студенты в период обучения в высших учебных заведениях, относятся: соблюдение политики безопасности учебного заведения и регулярное обновление знаний о новых методах атак; использование разных паролей для различных аккаунтов, их хранение вне на компьютера; использование двухфакторной аутентификации, которая требует ввода дополнительного кода при входе в аккаунт или сложных паролей; шифрование данных; проведение мониторинга сетевой активности. Данные методы позволят предотвратить несанкционированный доступ к личной информации.

Одним из эффективных способов повышения осведомленности и киберграмотности будущих специалистов является внедрение в педагогическую практику образовательных программ, включающих лекции, семинары, тренинги по защите персональных данных, безопасному поведению в социальных сетях, правилам общения в цифровой среде, стратегиям реагирования на фишинговые атаки, борьба с вирусами и другим вопросам кибербезопасности [13]. Подобные образовательные программы должны содержать модули по формированию цифровых компетенций, например, тестированию приложений, отслеживанию сетевого трафика для обеспечения сетевой безопасности, основ предотвращения таких угроз для конечных точек (например, сервера), как несанкционированный доступ и использование уязвимостей операционной системы и браузера [14]. Кроме этого, программы должны включать и блоки по выявлению и осознанию собственных психологических уязвимостей, проработке их с помощью специалистов, развитию критического мышления, формированию умений адекватно оценивать и проверять достоверность информации из множества источников, отличать факты от мнений [15, с. 289]. Кроме того, использование практических заданий и симуляций может помочь студентам развить навыки принятия решений в контролируемой среде.

Таким образом, сегодня кибербезопасность является крайне актуальной проблемой, так как с развитием цифровых технологий и интернета количество киберугроз значительно увеличивается. Сложные кибератаки становятся все более частыми и изощренными, поэтому защита информации и личных данных в сети становится важнейшим аспектом в современном мире. Кроме технических средств, важную роль играют когнитивные аспекты, такие как обучение пользователей распознавать потенциальные угрозы, понимание основных принципов безопасного поведения в сети, навыки критического мышления при работе в киберпространстве, цифровая грамотность, пропаганда безопасного поведения в сети, развитие навыков защиты информации. Данные особенности должны стать основой для разработки образова-

тельных программ по освоению студентами высших учебных заведений основ кибербезопасности, что является важнейшим условием реализации эффективной и безопасной коммуникации в онлайн-среде.

Библиографический список

1. Скурат, К. Для киберзащиты не хватает знания / К. Скурат // Новости цифровой трансформации, телекоммуникаций, вещания. – 2021. – Текст электронный. – URL: https://www.comnews.ru/content/217780/2021-12-06/2021-w49/dlya-kiberzaschity-ne-khvataet-znaniya (дата обращения: 12.04.2023).
2. Новая кибербезопасность: от процесса к понятному результату // Positive Technologies. – Текст электронный. – 2023. – URL: https://www.ptsecurity.com/ru-ru/research/analytics/new-cybersecurity-from-process-to-result/ (дата обращения: 12.04.2023).
3. Надточий, Ю.Б. Киберграмотность в эпоху цифровизации / Ю.Б. Надточий, М.Е. Гурова. – Текст непосредственный // Глобальные социальные процессы 3.0.: Социальное управление и экономическое развития в цифровом обществе. – «Российско-Китайский Центр сравнительных социальных, экономический и политический исследований правления «Социология» СПбГУ. – Санкт-Петербург, 2022. – С. 225-230.
4. Сулейманова, Д.О. Когнитивная безопасность: исследование когнитивной науки в области кибербезопасности / Д.О. Сулейманова, Т.Р. Магомаев. – Текст непосредственный // Общество, экономика, управление. – 2022. – Том 7. – № 3. – С.58-63.
5. Жмуров, Д.В. Кибервиктимизация. Исследовательская матрица / Д.В. Жмуров. – Текст непосредственный // Пролог: журнал о праве. – 2021. – №3. – С. 109-121.
6. Никешин, Д. Е. Кибервиктимность и кибербуллинг / Д. Е. Никешин. – Текст: непосредственный // Молодой ученый. – 2020. – № 18 (308). – С. 403-404. – URL: https://moluch.ru/archive/308/69562/ (дата обращения: 12.04.2024).
7. Ревенков, П.В. Киберграмотность как составная часть обеспечения кибербезопасности общества / П.В. Ревенков, А.А. Бердюгин // Педагогика, психология, общество: современные тренды: сборник материалов Всероссийский научно-практической конференции с международным участием. – Чебоксары, 2020. – С. 282-285.
8. Юдина, А.М. Цифровая трансформация высшего гуманитарного образования: концептуальные основы, опыт, перспективы / А.М. Юдина, А.У. Менциев // Перспективы науки. – 2021. – №3 (138). – С. 151-153.
9. Пономарева, М.Г. Образование как важнейший фактор кибербезопасности / М.Г. Пономарева // Актуальные вопросы современной науки: сборник трудов по материалам VI Всероссийского конкурса научно-исследовательских работ. – Уфа, 2021. – С. 102-106.
10. Фомин, А.Е. Эвристика доступности и метакогнитивный мониторинг решения учебный задач студентами / А.Е. Фомин // Вестник Брянского государственного университета. – 2012. – №1-2. – С. 175-180.
11. Колесникова, Т.В. Психология ошибки «Эффект Барнума-Форера» / Т.В. Колесникова, А.Ю. Шатохина. – Текст непосредственный // Современные технологии: актуальные вопросы, достижения и инновации. XV международная научно-практическая конференция. – «НАУКА И ПРОСВЕЩЕНИЕ», Пенза. – 2018. – С. 144-146.

12. Недошивина, М.А. Эффект социального доказательства и альтруистическая направленность личности как факторы просоциального поведения / М.А. Недошивина. – Текст непосредственный // Известия РГПУ им. А.И. Герцена. – 2019. – № 194. – С. 210-241.

13. Казинец, В.А. Повышение уровня подготовки студентов педагогических вузов и учителей в области информационной безопасности / В.А. Казинец, О.А. Малыхина. – Текст непосредственный // Современное педагогическое образование. – 2021. – № 4. – С. 162-166.

14. Аверкиев, А.А. Кибербезопасность: виды и методы / А.А. Аверкиев, Д.А. Камбулов. – Текст электронный // Научно-образовательный журнал для студентов и преподавателей «StudNet». – 2022. – №1. – URL: https://cyberleninka.ru/article/n/kiberbezopasnost-vidy-i-metody/viewer (дата обращения: 12.04.2024).

15. Кожогелдиева, М.А. Развитие информационной грамотности студентов в эпоху цифровых технологий / М.А. Кожогелдиева, Т.М. Бектуров. – Текст непосредственный // Эпоха науки. – 2024. – № 37. – С. 287-292.

УДК 159.955

ДОКАЗАТЕЛЬСТВО ЭФФЕКТИВНОСТИ РАЗРАБОТАННОЙ СИСТЕМЫ ФОРМИРОВАНИЯ ЦИФРОВОЙ КОМПЕТЕНТНОСТИ СПЕЦИАЛИСТА ПО УПРАВЛЕНИЮ ПЕРСОНАЛОМ РЕЗУЛЬТАТАМИ КОРРЕЛЯЦИОННОГО АНАЛИЗА

Ежков Дмитрий Олегович

Самарский национальный исследовательский университет имени академика С.П. Королева

Аннотация: *в статье представлены содержание и структура цифровой компетентности будущего специалиста по управлению персоналом, а также описаны связи показателей компонентов цифровой компетентности, полученных в ходе анализа констатирующего и формирующего экспериментов опытно-экспериментальной работы по формированию цифровой компетентности будущего специалиста по управлению персоналом.*

Ключевые слова: *корреляционный анализ, цифровая компетентность, структура цифровой компетентности, специалист по управлению персоналом.*

В связи с развитием цифровой экономики и управленческих процессов в организациях, актуальным и необходимым становится формирование цифровой компетентности у будущих специалистов по управлению персоналом, в структуру которой включены некоторые универсальные компетенции, определенные федеральным государственным стандартом: коммуникация, системное и критическое мышление, самоорганизация, саморазвитие. Данные характеристики включены в показатели компонентов цифровой компетентности как необходимые свойства специалистов по управлению персоналом, участвующих в цифровизации управленческих процессов [1]. Учтены трудовые функции специалиста по управлению персоналом из Профстандарта [2]. В ходе исследования определены содержание и структура цифровой компетентности, включающая компоненты (ценностно-мотивационный, когнитивный, инструментально-технологический, коммуникативный и рефлексивно-аналитический) и их показателей (табл. 1).