УДК 377

ФОРМИРОВАНИЕ КУЛЬТУРЫ КИБЕРБЕЗОПАСНОСТИ В СИСТЕМЕ ПРОФЕССИОНАЛЬНОЙ ПОДГОТОВКИ ОБУЧАЮЩИХСЯ КОЛЛЕДЖА КАК ПЕДАГОГИЧЕСКАЯ ПРОБЛЕМА

[1]Воскрекасенко О.А., [1]Киреева А.А., [2]Щелина Т.Т.

[1]ФГБОУ ВО Пензенский государственный университет, Пенза, e-mail: voskr99@rambler.ru, anyaakireeva@gmail.com;

[2]Арзамасский филиал ФГАОУ ВО «Национальный исследовательский Нижегородский государственный университет им. Н.И. Лобачевского», Арзамас, e-mail: arz65@mail.ru

В статье актуализируется необходимость формирования культуры кибербезопасности обучающихся учреждений среднего профессионального образования. Представлен анализ научной психолого-педагогической литературы по проблеме кибербезопасного поведения студентов колледжа и формирования у них культуры кибербезопасности. Осуществлен анализ понятий «кибербезопасность» и «культура кибербезопасности». Определены компоненты культуры кибербезопасности студентов. Выделены угрозы и опасности, подстерегающие обучающихся колледжа в киберпространстве. Охарактеризованы направления в системе деятельности образовательной организации СПО по обеспечению кибербезопасности обучающихся колледжа и формированию у них культуры кибербезопасного поведения. Среди них: непосредственное взаимодействие педагогов с обучающимися посредством реализации разнообразных форм, методов и технологий, нацеленных на формирование культуры кибербезопасности; организация и осуществление взаимодействия между педагогами и родителями студентов по вопросам обеспечения их кибербезопасности; построение партнерского сотрудничества образовательной организации СПО со сторонними организациями; взаимодействие между законодательными и исполнительными органами (разного уровня) и образовательными организациями СПО, направленное на нормативно-правовое обеспечение и кадровое обеспечение кибербезопасности обучающихся. Утверждается, что эффективность стоящих перед образовательной организацией СПО задач определяется системным характером деятельности, тесным сотрудничеством и взаимодействием субъектов образовательного процесса.

Ключевые слова: обучающиеся, колледж, кибербезопасность, киберпространство, культура кибербезопасности, образовательный процесс, профессиональная подготовка, взаимодействие субъектов образовательного процесса

FORMING A CULTURE OF CYBER SECURITY IN THE SYSTEM OF VOCATIONAL TRAINING OF COLLEGE STUDENTS AS A PEDAGOGICAL PROBLEM

[1]Voskrekasenko O.A., [1]Kireeva A.A., [2]Shchelina T.T.

[1]Penza State University, Penza, e-mail: voskr99@rambler.ru, anyaakireeva@gmail.com;

[2]Arzamas branch of the Federal State Autonomous Educational Institution of Higher Education "National Research Nizhny Novgorod State University named after N.I. Lobachevsky", Arzamas, e-mail: kireevaaa@pnzgu.ru

The article actualizes the need to form a culture of cybersecurity in students of institutions of secondary vocational education. An analysis of the scientific psychological and pedagogical literature on the problem of cybersecurity behavior of college students and the formation of a culture of cybersecurity among them is presented. The analysis of the concepts of «cybersecurity» and «cybersecurity culture» is carried out. The components of the cybersecurity culture of students are determined. The threats and dangers that lie in wait for college students in cyberspace are highlighted. The directions in the system of activities of the educational organization of secondary vocational education to ensure the cybersecurity of college students and the formation of a culture of cybersafe behavior are characterized. Among them: direct interaction of teachers with students through the implementation of various forms, methods and technologies aimed at creating a culture of cybersecurity; organization and implementation of interaction between teachers and parents of students on issues of ensuring their cybersecurity; building partnerships between an educational organization of free software and third-party organizations; interaction between legislative and executive bodies (of different levels) and educational organizations of secondary vocational education, aimed at legal support and staffing of students' cybersecurity. It is argued that the effectiveness of the tasks facing the educational organization of SVE is determined by the systemic nature of the activity, close cooperation and interaction of the subjects of the educational process.

Keywords: students, college, cybersecurity, cyberspace, cybersecurity culture, educational process, professional training, interaction of subjects of the educational process

Проникновение современных технологий во все сферы жизнедеятельности общества и во все его возрастные группы неизбежно привело к вовлечению в информационное пространство подрастающего поколения. На сегодняшний день киберпространство стало неотъемлемой частью реальной жизни современной мо-

лодежи, позволяющей ей удовлетворить не только информационную потребность, но потребность в общении посредством киберкоммуникации.

Подрастающее поколение использует возможности киберпространства для поиска информации, подготовки домашних заданий, прослушивания музыки, просмотра кинофильмов, онлайн-игр, общения в социальных сетях, попыток заработать первые деньги, заявить о себе, творчески самореализоваться и многого другого. Подобного рода взаимодействие молодого человека с киберпространством сопряжено с подстерегающими его на каждом шагу киберопасностями – фишингом, травлей в сети, нежелательным контентом, мошенниками различного уровня, манипуляциями сознанием и др. В связи с этим встает вопрос о защите детей и молодежи от киберопасностей, что нашло свое отражение в таких нормативно-правовых документах, как «Концепция информационной безопасности детей» и проект «Концепции стратегии кибербезопасности Российской Федерации», нацеливающих образовательные организации на формирование у подрастающего поколения культуры кибербезопасного поведения.

В силу возрастных особенностей студенческой молодежи, обучающейся в учреждениях среднего профессионального образования, ее социально-психологической незрелости, податливости к информационным воздействиям в сочетании с ее активностью в киберпространстве решение задачи формирования культуры кибербезопасности обучающихся колледжа приобретает особую значимость. Решение этой задачи осуществляется в специально организованной образовательной среде, обладающей потенциалом для эффективного формирования у обучающихся колледжа системы практикоориентированных знаний основ кибербезопасного поведения, а также умений и навыков их реализации в киберпространстве. В связи с этим формирование культуры кибербезопасности должно стать важной составляющей профессиональной подготовки и неотъемлемой профессиональной компетенцией обучающихся колледжа.

Цель исследования – определить роль культуры кибербезопасности в защите обучающихся колледжа от угроз в киберпространстве и наметить направления деятельности по ее формированию в ходе профессиональной подготовки.

Материалы и методы исследования

Методами исследования выступили анализ, обобщение и систематизация научной литературы по проблеме кибербезопасного поведения обучающихся колледжа и формирования у них культуры кибербезопасности.

Результаты исследования и их обсуждение

Проблема формирования у студентов колледжа культуры кибербезопасного поведения при всей ее значимости на сегодняшний день остается малоизученной. Вместе с тем отдельные ее аспекты нашли свое отражение в научной литературе. Так, значительная часть исследований, связанных с проблемой кибербезопасности, посвящена ее технологической (Н.Н. Акимов, И.А. Байгутлина, Н.И. Воропай, М.А. Гудков, П.А. Замятин, И.Н. Колосок, В.А. Кольцов, Е.С. Коркина, О.С. Лаута, В.Р. Милов, В.М. Московченко, С.А. Петренко, Р.Л. Шиберт и др.), правовой (П.Г. Горкавой, Е.О. Елизарова, О.Г. Ковалев, К.А. Краснова, В.М. Настич, Н.В. Семенова, В.В. Хоружий, С.С. Чекулаев, А.В. Яковлева и др.), экономической (А.П. Гарнов, Б.А. Калакуток, Е.Ю. Карелина, Э.Ш. Шацкая, Ю.А. Шитов, Ю.Ю. Шитова и др.), социально-гуманитарной составляющей (Е.Г. Бессонов, Т.А. Бороненко, Ю.В. Горелова, А.В. Кайсина, И.Н. Пальчикова, Е.И. Пустовая, А.З. Узденова, Е.В. Федоркевич, В.С. Федотова, Т.Н. Шарыпова и др.).

В последние годы появился целый ряд собственно педагогических исследований по кибербезопасности. Так, общие вопросы кибербезопасности с позиции педагогики рассматриваются в работах А.С. Зуфаровой, М.В. Лысенко, Н.А. Моисеевой, А.Х. Мутагаровой, Г.Ю. Яламова. Кибербезопасность в современных образовательных учреждениях (К.С. Итинсон, В.М. Чиркова и др.) многими авторами рассматривается в контексте цифровой грамотности субъектов образовательного процесса (Н.А. Моисеева, Л.Ю. Монахова, В.П. Топоровский и др.). В свою очередь, кибербезопасность в цифровой образовательной среде изучается такими авторами, как А.Ю. Буров, В.Е. Быков, Н.П. Дементиевская, Н.Н. Паньгина и др.

Особое место в педагогических исследованиях по кибербезопасности занимают работы, в которых рассматриваются риски в обучении и воспитании подрастающего поколения в эпоху цифрового образования, в условиях дистанционного обучения, в том числе обусловленного пандемией COVID-19. Среди них работы таких авторов, как И.Д. Алекперов, А.И. Алекперова, Д.Р. Ахметшин, О.С. Возженикова, Э.Р. Галиуллина, М.В. Гудков, В.А. Егоров, Р.С. Зарипова, А.Д. Кириллова, А.Р. Халиуллин, О.А. Чераева и др.

В свою очередь, еще одним важным направлением в современных педагогических исследованиях стало формирование умений и навыков кибербезопасного поведения у дошкольников (Т.С. Валеуллаева, С.Г. Шабас и др.), школьников (О.Л. Безумова, М.В. Бердник, Е.Д. Вохтомина, М.В. Гудков, Д.Б. Дубинина, Ю.А. Емельянова, О.Е. Кадеева, Е.А. Лыткина, Н.Н. Паньгина, О.Н. Троицкая, Т.С. Ширикова, В.В. Яновский и др.), а также студенческой молодежи (А.В. Белоус, А.В. Воронов, А.А. Воронова, Д.Б. Дубинина, Т.В. Рихтер, Т.В. Романова, А. Шеллер и др.).

Значимый пласт современных педагогических исследований посвящен поиску эффективных форм, методов, средств и технологий, направленных на решение задачи обеспечения кибербезопасности обучающихся разных возрастных групп (Э.Д. Алисултанова, О.Л. Безумова, А.В. Белоус, Е.Д. Вохтомина, М.А. Герасимова, Л.Н. Гришина, С.М. Емельянова, А.А. Идрисова, М.З. Исаева, А.В. Калач, А.С. Кравченко, А.А. Масленникова, Ю.А. Микацадзе, Т.В. Рихтер, В.А. Рунова, О.Н. Троицкая, И.С. Тулупова, Л.К. Хаджиева, Т.С. Ширикова, О.В. Шулежко, В.Г. Шевченко, М.В. Шевчук и др.). В качестве такого инструментария ими предлагается использовать: технологии дистанционного обучения; конкурсы; геймификацию; веб-квесты; профориентационные школьные лаборатории; психологическое просвещение; тематические видеоигры; онлайн-тренажеры; облачные технологии; образовательные курсы по кибербезопасности, в том числе дистанционные; дидактические игры и др.

В работах М.В. Гудкова, Д.С. Каниной, Е.Г. Копалкиной, С.Г. Манаенко раскрывается роль педагога в обеспечении кибербезопасного поведения обучающихся. В свою очередь, в исследованиях О.В. Пшеничной, И.В. Челышевой и С.Г. Шабас изучается роль родителей школьников. В связи с этим работу с семьей исследователи рассматривают как одно из условий формирования у обучающегося умений и навыков кибербезопасного поведения. В свою очередь, готовность будущих учителей, включая учителей информатики и математики (Е.Д. Вохтомина, Д.О.О. Куулар, А.А. Нечай, Е.Ю. Огурцова, М.И. Рагулина, О.Н. Троицкая, Р.Н. Фадеев, А.М. Яворская и др.), к решению проблемы кибербезопасности обучающихся также выступает одним из ключевых условий эффективности данной деятельности. Результат педагогической деятельности по обеспечению кибербезопасности обучающихся, выраженный в такой личностной характеристике, как культура кибербезопасности, представлен в исследованиях О.А. Веденеевой, М.А. Гарипова, М.А. Комаровой, Д.В. Редникова, Н.Я. Сайгушева и др. Однако проблема кибербезопасности обучающихся колледжа и формирования у них культуры кибербезопасности на сегодняшний день так и не стала предметом самостоятельно педагогического исследования.

Само понятие «кибербезопасность» имеет целый ряд толкований. Так, в исследовании Д.Б. Дубининой под кибербезопасностью понимается «реализация мер по защите систем, сетей и программных приложений от цифровых атак, направленных на получение доступа к конфиденциальной информации, ее изменение и уничтожение, а также на вымогательство у пользователей денег» [1, с. 98]. В свою очередь, Н.А. Моисеева под кибербезопасностью понимает «знания и умения оценивать риски социальной инженерии при работе в цифровом пространстве, знание мер по организации безопасности персональных данных, осознание негативного влияния цифровых устройств и гаджетов на окружающую среду, физическое и психическое здоровье человека» [2, с. 194].

В соответствии с проектом «Концепции стратегии кибербезопасности Российской Федерации» кибербезопасность определяется как «совокупность условий, при которых все составляющие киберпространства защищены от максимально возможного числа угроз и воздействий с нежелательными последствиями» [3].

В ряду угроз и опасностей, подстерегающих обучающихся колледжа, в научной литературе выделяются следующие:

– киберпреступления (кража денег со счета с помощью фишинговых писем или вирусов-троянов, обман, вымогательство и др.);

– кибербуллинг (намеренные травля, оскорбления, угрозы, сообщение компрометирующих данных с помощью современных средств коммуникации);

– киберсуицид (групповое или индивидуальное самоубийство, согласованное при помощи интернет-ресурсов);

– киберэкстремизм (завуалированная или открытая пропаганда экстремистских взглядов в киберпространстве);

– угрозы для морали и нравственности, нежелательная информация (сцены жестокости и насилия, употребления алкоголя и наркотиков, порнография и др.);

– агрессивное информационное пространство, манипуляции сознанием и пропаганда (от навязчивой рекламы товаров и услуг до навязывания политических взглядов);

– интернет-зависимость (аддиктивная форма поведения, сопровождающаяся множеством проблемных поведенческих ре-

акций, проявляющаяся в потере контроля над собой и неспособности вовремя выйти из сети);

− нарушение режима учебы и отдыха, проблемы со здоровьем и др. [1, 2, 4].

В условиях нарастающего воздействия на обучающихся колледжа вышеназванных угроз и опасностей актуализируется необходимость формирования у них культуры кибербезопасности, включающей в себя «умения и набор установок, которыми пользуется человек, защищая различные сферы своей жизни от угроз безопасности информации» [5, с. 27].

Культура кибербезопасности обучающегося начинается с системы знаний ее основных правил, но без понимания необходимости неукоснительного следования им, без устойчивого убеждения в их значимости их соблюдение не станет привычкой [6]. Одновременно знания и убеждения не помогут в конкретной ситуации киберопасности, если не сформированы устойчивые умения и навыки их распознавания и реагирования. В связи с этим деятельность преподавателей колледжа должна быть направлена на формирование у обучающихся: системы знаний правил поведения в киберпространстве, предостерегающих их киберопасностях и способах реагирования на них; осознания и принятия ответственности за свою кибербезопасность и устойчивой установки на неукоснительное соблюдение правил поведения в киберпространстве; умений и навыков их реализации.

В системе деятельности образовательной организации СПО по обеспечению кибербезопасности обучающихся колледжа и формированию у них культуры кибербезопасного поведения можно выделить несколько взаимосвязанных направлений.

Первое направление включает в себя непосредственное взаимодействие педагогов с обучающимися посредством реализации разнообразных форм, методов и технологий, нацеленных на формирование культуры кибербезопасности. К ним можно отнести:

− проведение кураторских часов, затрагивающих проблемы кибербезопасного поведения (например, «Интернет – друг или враг?», «Золотые правила безопасного поведения в сети», «Основы финансовой безопасности в киберпространстве», «Осторожно, кибермошенники!» и др.);

− размещение в электронной информационно-образовательной среде колледжа «Памятки по безопасному поведению в сети Интернет»;

− проведение в колледже «Недели кибербезопасности» (комплекс мероприятий, включая классные часы, конкурсы, круглые столы с приглашенными специалистами, квесты по кибербезопасности и др.);

− привлечение обучающихся колледжа к участию в онлайн-конкурсах и олимпиадах по кибербезопасности (например, на сайте Сетевичок.рф);

− организацию образовательных курсов по кибербезопасности, в том числе дистанционных;

− модернизацию программ учебных дисциплин под задачи формирования культуры кибербезопасности обучающихся;

− киберобучение в формате симуляции типичных жизненных ситуаций – встречи с киберопасностями (поиск и скачивание информации, проверка электронной почты, покупка в интернет-магазине, поиск работы через интернет-сайты, интернет-знакомства и предложения о личной встрече и др.);

− решение кейсов по проблемам угроз кибербезопасности с учетом специфики будущей профессиональной деятельности и др.

Независимо от формы работы очень важно, чтобы обсуждаемые со студентами вопросы не носили абстрактный характер, а соответствовали встречающимся в реальной жизни обучающихся ситуациям, органически вписывались в процесс профессиональной подготовки будущих специалистов.

Второе направление деятельности включает в себя организацию и осуществление взаимодействия между педагогом и родителями студентов. Важность данного направления определяется тем, что значительную часть обучающихся в образовательных организациях СПО составляют несовершеннолетние. Здесь важно показать, что дома студент тоже может быть подвержен угрозам информационного характера, поэтому необходимо проводить с родителями работу для моделирования «цифровой гигиены». Главной формой психолого-педагогического и нормативно-правового просвещения по проблемам кибербезопасности является родительское собрание. В содержание родительских собраний можно включить следующие вопросы:

− нормативно-правовые основы защиты несовершеннолетних от киберопасностей;

− возрастные особенности обучающихся колледжа и их влияние на поведение в киберпространстве;

− причины, признаки и пути коррекции интернет-зависимости;

− модные в молодежной среде онлайн-игры, интернет-группы и сообщества, представляющие потенциальную опасность для психического и (или) физического здоровья, жизни и безопасности обучающихся;

− признаки, помощь и поддержка обучающихся, ставших жертвой кибербуллинга;

– поведенческие особенности студентов, попавших в сети под влияние религиозных сект, экстремистских организаций, и др.

Полученные родителями знания в области кибербезопасности позволят им защитить своих детей от киберугроз и научить их противостоять этим явлениям.

Третье направление деятельности образовательной организации СПО по обеспечению кибербезопасности студентов – построение взаимодействия со сторонними организациями. Так, например, различные компании, деятельность которых направлена на защиту от информационных угроз, могут оказывать свои услуги образовательным организациям либо предоставлять им программные продукты, осуществляющие защиту. Также это взаимодействие можно применить и в образовательном процессе, например путем приглашения экспертов по цифровой безопасности для работы со студентами, проведения различных тренингов и др.

Четвертое направление по обеспечению кибербезопасности обучающихся колледжа связано с взаимодействием между законодательными и исполнительными органами (разного уровня) и образовательными организациями. Рекомендуется на уровне образовательных стандартов ввести дисциплины, связанные с цифровой грамотностью и кибербезопасностью, а также регулярно проводить повышение квалификации и курсы профессиональной переподготовки для педагогических кадров системы СПО, направленные на совершенствование навыков безопасной работы с обучающимися в киберпространстве и формирование у них культуры кибербезопасного поведения.

Все перечисленные действия, направленные на обеспечение информационной защиты студентов в образовательном процессе колледжа, должны применяться в комплексе. Также необходимо назначать одного или нескольких лиц, ответственных за реализацию мер, определяющих кибербезопасность обучающихся.

Заключение

Активность обучающихся колледжа в киберпространстве, их возрастные особенности и недостаточная социально-психологическая зрелость определяют необходимость реализации комплекса мер по обеспечению их кибербезопасности, а также формированию культуры кибербезопасного поведения. Эффективность стоящих перед образовательной организацией среднего профессионального образования задач определяется системным характером деятельности, тесным сотрудничеством и взаимодействием субъектов образовательного процесса.

Список литературы

1. Дубинина Д.Б. Проблема медиабезопасности и кибербезопасности личности школьника и студента в современном информационном пространстве // Экология медиасреды: материалы IV Открытой межвузовской научно-практической конференции (Москва, 25 апреля 2019 года). М., 2019. С. 96–101.

2. Моисеева Н.А. Кибербезопасность как важный компонент цифровой грамотности поколения Z // Цифровизация и кибербезопасность: современная теория и практика: материалы Международной научно-практической конференции (Омск, 30 сентября – 01 октября 2021 года). Омск, 2021. С. 191–196.

3. Концепция стратегии кибербезопасности Российской Федерации [проект, по состоянию на 10 января 2014 г.]. [Электронный ресурс]. Режим доступа: http://council.gov.ru/media/files/41d4b3dfbdb25cea8a73.pdf (дата обращения: 05.09.2022).

4. Чернова Е.В. Потенциальные угрозы в ИКТ-насыщенной среде // Стратегия качества в промышленности и образовании: материалы VIII Международной конференции (Варна, Болгария, 8–15 июня 2012 года). Днепропетровск – Варна, 2012. С. 490–492.

5. Калач А.В., Кравченко А.С. Современные технологии формирования культуры кибербезопасности // Ведомости уголовно-исполнительной системы. 2019. № 11 (210). С. 26–30.

6. Редников Д.В., Комарова М.А. Проблемы формирования культуры кибербезопасности // Тенденции развития науки и образования. 2021. № 2 (80). С. 157–160.