УДК 377.131.11
DOI: 10.26140/anip-2020-0903-0056

МЕТОДИЧЕСКИЕ АСПЕКТЫ ФОРМИРОВАНИЯ ГОТОВНОСТИ ОБУЧАЮЩИХСЯ IT-СПЕЦИАЛЬНОСТЕЙ ПЕДАГОГИЧЕСКОГО КОЛЛЕДЖА К ПРОТИВОДЕЙСТВИЮ ВОВЛЕЧЕНИЮ В КИБЕРЭКСТРЕМИСТСКУЮ ДЕЯТЕЛЬНОСТЬ

SPIN-код: 6248-2159
AuthorID: 639988
Степанова Оксана Александровна, кандидат педагогических наук, доцент кафедры математики, медицинской информатики, информатики и статистики, физики
SPIN-код: 1448-7003
AuthorID: 656944
Диденко Галина Александровна, кандидат педагогических наук, доцент кафедры математики, медицинской информатики, информатики и статистики, физики
Южно-Уральский государственный медицинский университет
(454092, Россия, Челябинск, улица Воровского, 64, e-mail: pga80@mail.ru)
SPIN-код: 5424-3966
AuthorID: 758379
Шварцкоп Ольга Николаевна, магистр педагогики и психологии, магистр профессионального обучения, старший преподаватель кафедры автомобильного транспорта, информационных технологий и методики обучения техническим дисциплинам
Южно-Уральский государственный гуманитарно-педагогический университет
(454074, Россия, Челябинск, ул. Бажова, 46а, e-mail: lelik877_87@mail.ru)

Аннотация. Расширенные возможности доступа к различным сетевым цифровым ресурсам и активное использование при этом мобильных устройств привели к появлению такого деструктивного явления как киберэкстремизм. В статье актуализирована проблема формирования готовности обучающихся колледжа к противодействию вовлечению в киберэкстремистскую деятельность, которые находятся в группе риска в силу своих психологических характеристик и высокой информационной активности. Авторами рассматривается реализация процессуального компонента методики формирования готовности обучающихся IT-специальностей, который интегрирует в себе методы обучения, организационные формы учебного процесса и средства обучения, выделенные для всех педагогических условий комплекса. В качестве примера рассматривается реализация конкретных методов: словесных (беседа, мозговой штурм, рефлексивный диалог), наглядных (метод демонстрации, наблюдения) и практических (анализ конкретных ситуаций, «кейс-стади», метод «инцидента», метод проигрывания ситуаций (инсценировки) и дидактической игры, метод проектных заданий и рефлексивных дискуссий) при изучении дисциплин информационного цикла. Результаты проведенного исследования подтверждают целесообразность применения данных методов обучения в процессе формирования готовности обучающихся IT-специальностей педагогического колледжа к противодействию вовлечению в киберэкстремистскую деятельность.

Ключевые слова: киберэкстремизм, формирование готовности обучающихся колледжа, метод упражнений и дидактической игры, метод ситуационного анализа (кейс-стади), метод «инцидента», метод проектов.

METHODOLOGICAL ASPECTS OF THE FORMATION OF THE READINESS OF STUDENTS OF IT SPECIALTIES OF A TEACHER TRAINING COLLEGE TO COUNTERACT INVOLVEMENT IN CYBER EXTREMISM

Stepanova Oksana Alexandrovna, candidate of Pedagogical Sciences, Associate Professor of the Department of Mathematics, Medical Informatics, Informatics and Statistics, Physics
Didenko Galina Alexandrovna, candidate of Pedagogical Sciences, Associate Professor of the Department of Mathematics, Medical Informatics, Informatics and Statistics, Physics
South Ural State Medical University
(454092, Russia, Chelyabinsk, Vorovsky st., 64, e-mail: okalst@mail.ru)
Shvartskop Olga Nikolaevna, master of Pedagogy and Psychology, master of professional training, senior teacher of the Department of Automobile transport, Information technologies and Methods of Teaching technical disciplines
South Ural State Humanitarian and Pedagogical University
(454074, Russia, Chelyabinsk, Bazhova st., 46a, e-mail: lelik877_87@mail.ru)

Abstract. Enhanced access to various digital network resources and the active use of mobile devices at the same time led to the emergence of such a destructive phenomenon as cyber extremism. The article actualizes the problem of forming the readiness of students in colleges to counteract involvement in cyber extremist activities, which are at risk due to their psychological characteristics and high activity. Automated preparation of the educational process and teaching aids allocated for all pedagogical conditions of the complex. As an example, specific methods are given: verbal (conversational, brainstorming, reflective dialogue), visual (method of demonstration, observations) and practical (analysis of specific situations, "case studies", "incident" method, method of playing situations (dramatization) and didactic games), method of design tasks and reflective discussions) in the study of the disciplines of the information cycle. The results of the study confirm the appropriateness of using these teaching methods in the process of formation of students. The information and pedagogical college counteract participation in cyber-extremist activities.

Keywords: cyber extremism, an open training course, the method of exercises and didactic games, the method of situational analysis (case study), the method of "incident", the method of projects.

ВВЕДЕНИЕ

В условиях активного развития информационной инфраструктуры современного общества, широкого использования информационных сетевых сервисов во всех сферах деятельности, особую актуальность приобретают вопросы защиты от информационных угроз. Одним из опасных и деструктивных проявлений таких угроз является киберэкстримизм.

Самой уязвимой группой, подверженной влиянию экстремистских группировок в сети Интернет и распространению киберэкстремизма в целом, является молодежь, в силу психолого-физиологических особенно-

стей, а так же способности быстро осваивать различные информационные технологии. В связи с этим, особую актуальность приобретает проблема подготовки компетентных специалистов к противодействию вовлечению в киберэкстремистскую деятельность на всех уровнях профессионального образования, в том числе и обучающихся колледжа.

На сегодняшний день ведется активная работа по противодействию вовлечению в киберэкстремистскую деятельность по различным направлениям [1-4]. Нормативно-правовое направление связано с совершенствованием правовых инструментов в сфере борьбы с экстремизмом.

Актуальность исследования на научно-теоретическом уровне определяется нормативными документами противодействия экстремистской деятельности в сфере образования. Так, основные направления, которые должны быть реализованы в образовании по повышению эффективности мер профилактики и пресечения правонарушений экстремистской характера, обозначены в Стратегии противодействия экстремизму в Российской Федерации:

1. Проведение в образовательных организациях занятий по воспитанию патриотизма, культуры мирного поведения, межнациональной и межконфессиональной дружбы, по обучению навыкам бесконфликтного общения, а также умению отстаивать собственное мнение, противодействовать социально опасному поведению, в том числе вовлечению в экстремистскую деятельность, всеми законными средствами;

2. Включение в учебные планы, учебники, учебно-методические материалы тем, направленных на воспитание традиционных для российской культуры ценностей;

3. Повышение профессионального уровня педагогических работников, разработка и внедрение новых образовательных стандартов и педагогических методик, направленных на противодействие экстремизму [5].

Социально-педагогическое, как и научно-теоретическое направление, обусловлено системным представлением педагогического и методического обеспечения процесса формирования готовности обучающихся к противодействию вовлечению в киберэкстремистскую деятельность.

МЕТОДОЛОГИЯ

Рассмотрим методические аспекты реализации комплекса педагогических условий эффективного функционирования формирования готовности обучающихся IT-специальностей педагогического колледжа к проти-водействию вовлечению в киберэкстремистскую деятельность в процессе изучения дисциплин информационного цикла: «Информационные технологии», «Информационная безопасность».

Для решения объективной проблемы в системе профессиональной подготовки студентов колледжа к противодействию вовлечению в киберэкстремистскую деятельность нами был разработан следующий комплекс педагогических условий:

1) рефлексивно-ценностное сопровождение студентов при анализе ситуаций и выполнении заданий по информационной безопасности в киберпространстве;

2) формирование системы внутреннего противодействия вовлечению в киберэкстремистскую деятельность посредством реализации принципа предосторожности во время рефлексивно-ценностного сопровождения в учебной и внеучебной деятельности;

3) включение в проектные задания по дисциплинам информационного цикла в качестве содержательного контента информации юридического, технологического и акмеологического направлений профилактики киберэкстремизма [6].

Структура методики представлена совокупностью и целостностью взаимосвязанных компонентов: целевого, содержательного, процессуального и результативного, выделенных для каждого педагогического условия с целью активного взаимодействия участников образовательного процесса по формированию готовности обучающихся к противодействию вовлечению в киберэкстремистскую деятельность.

Целевой компонент методики является системообразующим и состоит из системы взаимосвязанных целей. Содержательный компонент регламентирован целевым компонентом методики и состоит из учебных тем дисциплин, на которых обучающиеся, выполняя задания, знакомятся с информацией по противодействию вовлечению в киберэкстремистскую деятельность. Процессуальный компонент интегрирует в себе методы обучения, организационные формы учебного процесса и средства обучения, выделенные отдельно для каждого педагогического условия. Результативный компонент методики включает в себя систему результатов сформированности отдельных компонентов готовности студентов колледжа к противодействию вовлечению в киберэкстремистскую деятельность (аксиологического, процессуально-рефлексивного и когнитивно-целевого).

РЕЗУЛЬТАТЫ

Первое педагогическое условие комплекса реализуется в процессе рефлексивно-ценностного сопровождения процесса формирования готовности студентов колледжа к противодействию вовлечению в киберэкстремистскую деятельность через проблемно-рефлексивные лекции, мультимедиа-лекции, практические занятия, самостоятельную работу обучающихся с применением словесных (рассказ, объяснение, беседа, рефлексивный диалог), наглядных (метод наблюдения, видеометод) и практических методов (упражнения, дидактические игры) при изучении информационных дисциплин на первом и втором курсах. В качестве средств обучения использовались аудиовизуальные и технические средства (мультимедийный проектор, компьютер), информационные образовательные ресурсы, облачные сервисы.

Важным этапом является рефлексия содержания учебного материала, самоанализ студентами внутреннего состояния, собственных мыслей и точки зрения на изложенный материал. На этапе рефлексии применялись различные методики, такие как «ПОПС-формула», «Плюс, минус, интересно», «Рефлексивный экран», «Рефлексивная мишень» и другие. Так, суть методики «ПОПС-ФОРМУЛА» заключается в следующем: студентам предлагается раскрыть содержание ПОПС-формулы: П – позиция («Я считаю, что …»); О – объяснение («Потому что …»); П – пример («Можно привести такой пример …»); С – следствие («Исходя из этого, можно прийти к такому выводу, что …»). Данные методики позволяют получить информацию о степени погруженности студента в материал, о степени понимания изучаемой проблемы и узнать собственное мнение студентов.

Реализация первого педагогического условия на практических занятиях осуществлялась посредством методов упражнений и дидактической игры. Так, например, обучающимся на практических занятиях по дисциплине «Информационные технологии» были предложены следующие задания:

1) Сделать подборку статей в сети Интернет по проблемам киберэкстремизма в России и в мире, указав название статьи, автора, точный адрес сайта и ответить на следующие вопросы: какие основные проблемы киберэкстремизма и кибертерроризма в России затронуты в статьях; какую роль играет сеть Интернет в процессе вовлечения молодежи в киберэкстремизм (кибертерроризм); какие ценности нужно формировать у молодого поколения для противодействия киберэкстремизму; какие методы превенции киберэкстремизма были предложены в статьях; какие сложности могут возникнуть в будущем, если не принимать своевременно меры по противодействию явлений киберэкстремизма?

2) Используя сеть Интернет, зайдите на сайт Кон-

сультантПлюс и сделайте подборку нормативных документов по теме «Экстремизм». Ознакомьтесь более детально с Федеральным законом «О противодействии экстремистской деятельности» от 25.07.2002 N 114-ФЗ и ответьте на следующие вопросы: согласно данного ФЗ какие основные принципы противодействия экстремизма; согласно данного ФЗ назовите основные направления противодействия экстремистской деятельности; какую ответственность несут граждане РФ, иностранные граждане и лица без гражданства за осуществление экстремистской деятельности согласно данного ФЗ?

3)На сайте КонсультантПлюс изучите Стратегию противодействия экстремизма в РФ до 2025 года и укажите основные источники угроз экстремизма в современной России, обратив особое внимание на сеть Интернет.

Метод дидактической игры, игры-предположения заключается в проведении опроса: «Если было бы…» или «Что бы я сделал…». Игровая задача содержится в самом названии. Перед студентами создается проблемная ситуация, требующая анализа и последующего действия, преподаватель оказывать помощь, сопровождение при решении задачи. Например, студентам были предложены такие проблемные ситуации: «что бы я сделал, если в социальной сети мне поступило предложение вступить в ряды экстремисткой организации»; «что было бы, если бы не осуществлялось государственное регулирование работы общественных или религиозных объединений»; «что бы я сделал, если мой друг активно поддерживал экстремистские идеи» и др.

Рефлексивно-ценностное сопровождение студентов преподавателем осуществляется при анализе ситуаций во время проведения рефлексивных дискуссий по информационной безопасности в киберпространстве. Проведение рефлексивных дискуссий в виде «круглого стола» способствует стимулированию познавательного интереса студентов по противодействию вовлечению в киберэкстремистскую деятельность, формированию рефлексивной позиции студента, ценностей, умений оценивать реальную действительность, регулировать свое поведение.

Рассмотрим методику реализации следующего педагогического условия. Система внутренних мотивов к противодействию вовлечению в киберэкстремистскую деятельность формируется посредством реализации принципа предосторожности во время рефлексивно-ценностного сопровождения и воспитательного воздействия в учебной и внеучебной деятельности.

Отметим, что принцип предосторожности заключается в том, чтобы рационально оценивать информацию, на основе ее принимать решения и признавать ответственность за свою деятельность, не просто следуя цензуре и введенным ограничениям, а только осознанно и добровольно, исходя из собственной системы нравственных ценностей.

Система внутреннего противодействия вовлечению в киберэкстремистскую деятельность формировалась через лекции-дискуссии, лекции-провокации (с заранее запланированными ошибками), лекции-консультации, практические занятия, самостоятельную работу, внеучебные мероприятия (беседы, встречи, тренинги и др.) с применением словесных (беседа и мозговой штурм), наглядных (метод демонстрации) и практических методов (анализ конкретных ситуаций, метод ситуационного анализа (кейс-стади), метод «инцидента», метод проигрывания ситуаций (инсценировки)) при изучении дисциплин.

Остановимся более подробно на реализации метода анализа конкретных ситуаций и его разновидностях: методе ситуационного анализа (кейс-стади), методе «инцидента», методе проигрывания ситуаций (инсценировки). Метод кейс-стади основан на моделях реальных случаев и прецедентов. Рассматривая фактический материал конкретной ситуации, необходимо найти не только правильное решение проблемы, но и указать возможные различные пути. Кейсы имеют множество вариантов решений и разных путей, приводящих к ним, в зависимости от исходных условий. Так, студентам были предложено разработать следующие кейсы:

- Роскомнадзор в 2017 году на основании требований Генпрокуратуры ограничил доступ к 13,5 тысячи сайтов с призывами к экстремизму, массовым беспорядкам и несанкционированным митингам, сообщил руководитель Роскомнадзора А. А. Жаров [7].

- Почти 90 тысяч сайтов, содержащих противоправную информацию, в том числе террористического и экстремистского характера, было заблокировано в Южном федеральном округе РФ за 2018 год, сообщил секретарь Совета безопасности России Н. П. Патрушев [8].

- Более 12 тысяч зарубежных сайтов, которые угрожали интересам России, были заблокированы в 2019 году, рассказал замдиректора Национального координационного центра по компьютерным инцидентам Николай Мурашов [9].

В процессе разработки кейса студенты должны ответить на такие вопросы: какие выводы можно сделать по данной информации; в соответствии с какими нормативными актами осуществляется блокировка сайтов экстремистского толка; почему информация в руках экстремистов является опасным оружием преступления; почему киберпреступления, совершаемые экстремистами, являются источником угрозы национальной безопасности всему миру?

Принцип работы с кейсами следующий: студенты в группах выполняют анализ ситуации, выявляют проблему, предлагают свои идеи и решения в дискуссии с другими обучаемыми и вырабатывают совместное практическое решение. По итогам анализа студенты разрабатывают презентацию, содержащую решение проблемной ситуации. Задачей преподавателя при решении кейсов является оказание своевременной помощи и поддержки студентов при разборе проблемной ситуации и выборе различных альтернатив ее решения. В ходе анализа кейса студенты учатся работать «в команде», защищать свою точку зрения, слушать, аргументированно убеждать, проводить анализ ситуации и принимать решения, предусматривающие оценку положительных и отрицательных последствий принятых решений, возможных рисков и потенциальных проблем в будущем развитии событий. Так в процессе обучения реализуется принцип предосторожности.

Целью следующего метода, метода инсценировки, является формирование способностей принимать решения в неожиданной ситуации, импровизировать. С помощью проигрывания ролей воссоздается перед аудиторией правдивая ситуация, в которой студенты играют самих себя, демонстрируя свои ценности, культуру. Перед началом мероприятия обучающимся предлагаем ответить на вопросы анкет «Уровень конфликтности», «Диагностика склонности к нарушению социальных норм и правил», «Проявляешь ли ты толерантность?», созданных в облачном сервисе Google формы. Студенты выполняют анализ ситуации с помощью разыгрывания ситуации в ролях (role playing), т.е. инсценировки, которая записывается на видео и потом критически анализируется совместно со всеми студентами.

Перейдем к рассмотрению методики реализации третьего педагогического условия формирования готовности студентов колледжа к противодействию вовлечению в киберэкстремистскую деятельность: включение в проектные задания по дисциплинам информационного цикла в качестве содержательного контента информации юридического, технологического и акмеологического направлений профилактики киберэкстремизма.

В данном случае ведущим выступил метод проектов. Метод проектов является творческим заданием, направленным на развитие самостоятельной учебно-познава-

тельной деятельности обучающихся: умение самостоятельно формулировать проблему и находить ее решение, работать с различными источниками информации, оформлять разработанный проект, используя различные программные средства и технологии. Практическим результатом проектного задания по дисциплинам информационного цикла являются конкретные знания и идеи обучающихся по профилактике вовлечения в киберэкстремистскую деятельность, которые будут представлены в виде комплексного информационного объекта (базы данных, мультимедийных презентаций, электронных учебных пособий, компьютерных тестов, сайтов и др.).

Разработка и защита проектных заданий позволяет сформировать у обучающихся представление о возможных способах вовлечения в киберэкстремистскую деятельность и методах борьбы с этим асоциальным явлением, сформировать обобщенные информационные умения противодействия информационным угрозам, а также ценностные качества и установки личности, позволяющие противостоять вовлечению в киберэкстремистскую деятельность.

Разработанная и экспериментально проверенная методика реализации комплекса педагогических условий, была систематизирована и представлена также в виде электронного образовательного ресурса для самостоятельной работы студентов [10]. Данный электронный образовательный ресурс (ЭОР) включает следующий контент:

- Основной лекционный материал по темам курса.
- Дополнительный материал по профилактике киберэкстремизма среди молодежи, который можно получить с помощью ссылки на информационные и видеоматериалы проекта «Экстремизму.нет».
- Практические интерактивные задания, разработанные в облачном сервисе LearningApps.
- Тесты-опросники, разработанные в облачном сервисе Google Формы, результаты которых могут быть автоматически отправлены в таблицы MS Excel для статистической обработки.
- Методические рекомендации по формированию готовности обучающихся колледжа к противодействию вовлечению в киберэкстремистскую деятельность.

Такие преимущества ЭОР, как интерактивность, мобильность, доступ к материалам с различных устройств, позволили дифференцировать подход к формированию готовности студентов к противодействию вовлечению в КД. Спроектированный ЭОР позволил систематизировать адаптированные методические разработки и представить их в виде целостной, структурированной системы.

ВЫВОДЫ

Таким образом, представленная методика формирования готовности к противодействию вовлечению в киберэкстремистскую деятельность была апробирована в процессе опытно-экспериментальной работы на базе Южно-Уральского государственного колледжа при подготовке обучающихся ИТ-специальностей: 09.02.07 «Информационные системы и программирование», 09.02.03 «Программирование в компьютерных системах».

Результаты экспериментальной работы позволили оценить с помощью оценочно-диагностического инструментария начальный уровень готовности и отследить динамику изменения, темпы повышения уровня готовности обучающихся колледжа к противодействию вовлечению в киберэкстремистскую деятельность. Сравнительный анализ результатов экспериментальных данных, полученных на начало и конец формирующего эксперимента в экспериментальных и контрольной группах, показал, что более эффективному повышению уровня готовности студентов колледжа к противодействию вовлечению в киберэкстремистскую деятельность способствует комплексное воздействие всех педагогических условий (ЭГ-3), чем их применение по отдельности (ЭГ-1, ЭГ-2). Объективность проверки выдвинутой научной гипотезы исследования подтверждена с помощью статистических методов [6].

Проведенное исследование позволило получить дальнейшее развитие знаний о потенциале методического аспекта при формировании готовности студентов к противодействию вовлечению в киберэкстремистскую деятельность в процессе профессиональной подготовки в колледже.

СПИСОК ЛИТЕРАТУРЫ:

1. Гонсалес С.Х.И. Поиск идентичности дисфункционального общества и его влияние на возникновение экстремизма // Азимут научных исследований: экономика и управление. 2018. Т. 7. № 3 (24). С. 353-355.

2. Роговая А.В. Противодействие идеологии экстремизма и терроризма на российском Кавказе (по материалам социологических исследований) // Ойкумена. Регионоведческие исследования. 2016. № 3 (38). С. 45-54.

3. Глухова А.А., Шпилев Д.А. Роль модераторов сайтов, посвященных тематике АУЕ, в формировании социопатических и противоправных установок у подростков и молодежи // Актуальные проблемы экономики и права. 2019. Т. 13. № 4. С. 1646-1660.

4. Дзагурова Н.Х. Гражданская позиция и оценка экстремистских настроений студентов в современных условиях // Балтийский гуманитарный журнал. 2018. Т. 7. № 3 (24). С. 342-345.

5. Стратегия противодействия экстремизму в Российской Федерации до 2025 года (утв. Президентом РФ 28.11.2014 N Пр-2753) URL: http://www.consultant.ru/document /cons_doc_LAW_194160/ (дата обращения: 26.01.2020).

6. Диденко Е.В., Гафарова Е.А., Степанова О.А., Диденко Г.А., Шамаева Т.Н. Анализ результатов экспериментальной работы по формированию готовности обучающихся колледжа к противодействию вовлечения в киберэкстремистскую деятельность // Современные наукоемкие технологии. 2019. № 8. С. 112-116; URL: http://www.top-technologies.ru/ru/article/view?id=37640 (дата обращения: 26.01.2020).

7. URL: https://www.rosbalt.ru/russia/2018/02/20/1683720.html (дата обращения: 26.01.2020).

8. URL: https://ria.ru/20190913/1558642718.html (дата обращения: 26.01.2020).

9. URL: https://radiomayak.ru/news/article/id/1250977/ (дата обращения: 26.01.2020).

10. URL: https://studentit.ucoz.net (дата обращения: 26.01.2020).

Статья поступила в редакцию 01.04.2020
Статья принята к публикации 27.08.2020