УДК 371.126+004.05

МОДЕЛЬ ПОДГОТОВКИ СТУДЕНТОВ ВУЗА К ПРОТИВОДЕЙСТВИЮ КИБЕРЭКСТРЕМИСТСКОЙ ДЕЯТЕЛЬНОСТИ

Савва Л.И.[1], Доколин А.С. [1]

[1]*ФГБОУ ВПО «Магнитогорский государственный технический университет им. Г.И. Носова», Магнитогорск, Россия (455000, Магнитогорск, пр. Ленина, 38), e-mail: a.dokolin@gmail.com*

Существует множество угроз внутри сети Интернет, наиболее опасной мы выделяем киберэкстремизм. Киберэкстремизм – это явление, возникающее в киберпространстве, основанное на реализации чрезвычайных, решительных взглядов и мер с использованием информационных технологий, направленных против существующих в обществе норм, правил, принципов, обычаев и традиций. Для сведения этой угрозы к минимуму требуется комплексные методы противодействия. Прежде всего эти методы должны быть направлены на формирование сильной и гражданской личности, работа должна проводиться с молодежью. Цель нашей работы – моделирование процесса подготовки студентов вуза к противодействию киберэкстремистской деятельности, результатом этой работы служит структурно-функциональная модель данного процесса. Модель рассматривается как открытая подсистема, встроенная в контекст образовательной подготовки студентов, и содержит следующие компоненты: социально-целевой, теоретическо-методологический, процессуально-методический и оценочно-результативный. Структурно-функциональная модель характеризуется целостностью, так как все указанные компоненты взаимосвязаны между собой, несут определенную смысловую нагрузку, и открытостью, так как модель встроена в контекст системы профессиональной подготовки студентов вуза. Суть разработанной модели подготовки студентов вуза к противодействию киберэкстремистской деятельности заключается в обеспечении перехода на более высокий, качественно новый уровень готовности студента к противодействию киберэкстремистской деятельности.

Ключевые слова: моделирование, профессиональная подготовка студентов, киберэкстремизм, экстремизм, противодействие киберэкстремистской деятельности, структурно-функциональная модель

THE MODEL OF TRAINING STUDENTS TO CONFRONT CYBER EXTREMIST ACTIVITY

Savva L.I.[1], Dokolin A.S.[1]

[1]*Nosov Magnitogorsk state technical University, Magnitogorsk, Russia (455000, Magnitogorsk, street Lenin, 38), e-mail: a.dokolin@gmail.com*

There are many threats within the Internet, the most dangerous we highlight the cyber extremism. Cyber extremism is a phenomenon that occurs in cyber space, based on the implementation of the emergency, decisive views and measures using information technology directed against the existing social norms, rules, principles, customs and traditions. For details of this threat to the very minimum required complex methods of counteraction. First of all, these methods should be aimed at building a strong and civil personality, work should be carried out with young people. The goal of our work is the modeling of the process of students' preparation to address cyber extremism activity, the result of this work is the structural-functional model of this process. The model is regarded as an open subsystem integrated within the context of the educational preparation of students and contains the following components: social-target, theoretical and methodological, procedural, methodological, and assessment-effective. Structural-functional model is characterized by integrity, since all these components are interconnected, carry some meaning, and openness, as the model is embedded in the context of the system of professional training of students of the University. The essence of the developed models for training students to confront cyber extremism activities is to ensure the transition to a higher, qualitatively new level of the student's readiness to counter cyber extremism activity.

Keywords: simulation, training students, cyber extremism, extremism, countering cyber extremist activity, structural-functional model.

В современных условиях глобальная сеть Интернета, с одной стороны, объединяет людей, с другой — несет серьезные угрозы, которые распространяются со скоростью вируса: киберпреступность, киберэкстремизм, кибертерроризм. Особенность всех явлений с приставкой «кибер» заключается в том, что их очень сложно контролировать в огромной

информационной Сети, при этом они с молниеносной скоростью находят своих сторонников и получают активную поддержку [1].

Экстремизм – это один из типов девиантного поведения личности, направленного против существующих в обществе норм, правил, принципов, обычаев, традиций [2]. Киберэкстремизм же – частое явление в социальных сетях, блогосфере, форумах и сетевых сообществах. Мы определяем данное понятие как явление, возникающее в киберпространстве, основанное на реализации чрезвычайных, решительных взглядов и мер, с использованием информационных технологий, направленных против существующих в обществе норм, правил, принципов, обычаев и традиций.

Киберэкстремистскую деятельность мы рассматриваем как деятельность экстремистов, связанную с реализацией системы мер, сосредоточенных против существующих в обществах норм, правил, принципов, обычаев и традиций, с применением информационных технологий. Наиболее подвержены влиянию киберэкстремизма такие слои населения, как учащиеся школ и студенты, так как данная социальная группа, хотя и является активным пользователем, но не обучена самостоятельно и осознанно воспринимать и обрабатывать тот информационный поток, который находится в сети Интернет. Вышестоящее актуализирует рассматриваемую проблему.

Цель исследования

В данной статье мы представляем описание разработанной нами модели подготовки студентов вуза к противодействию киберэкстремистской деятельности, которую мы определяем как структурно-функциональную. Целью создания модели является описание рассматриваемого процесса с целью дальнейшего управления им, а цель самой модели заключается в подготовке студентов вуза к противодействию киберэкстремистской деятельности.

Материал и методы исследования

Разработанная модель рассматривается нами как открытая подсистема, встроенная в контекст образовательной подготовки студентов, и содержит следующие компоненты: социально-целевой, теоретическо-методологический, процессуально-методический и оценочно-результативный, каждый из которых выполняет соответствующие функции.

При выделении социально-целевого компонента исходили из того, что организация процесса начинается с формулирования его цели, которая определяется социальным заказом общества – выпускник вуза с высоким уровнем подготовки к противодействию киберэкстремистской деятельности. Данный социальный заказ отражается в нормативных образовательных документах, направленных на специальную подготовку специалистов в этой области с учетом требований современного периода.

Рассматриваемый компонент включает структурные блоки готовности: мотивационно-ценностный блок, представленный патриотическими и культурными ценностями, потребностями в превенции явлений киберэкстремизма; содержательно-процессуальный блок, содержащий знания и умения по превенции явлений киберэкстремизма среди студентов; блок эмоционально-нравственный, который содержит личные и профессиональные ценности.

Теоретико-методологический компонент модели включает подходы и вытекающие из них принципы к подготовке студентов вуза к противодействию киберэкстремистской деятельности. В качестве методологической основы рассматриваемого процесса были выбраны системный, компетентностный, личностно-деятельностный и культурологический подходы.

Значение системного подхода в нашем исследовании состоит в том, что он позволяет: рассмотреть подготовку студентов вуза к противодействию киберэкстремистской деятельности как целостную систему; четко задать цели данной системы; определить содержание компонентов, из которых образована система, определив функции, уровни и этапы рассматриваемого процесса; динамику ее функционирования и раскрыть взаимосвязь всех составляющих компонентов.

Компетентностный подход в нашем процессе позволяет обеспечить главный результат – сформировать у студентов соответствующие компетентности, обеспечивающие им эффективное противодействие киберэкстремистской деятельности и, как отмечает И.А. Зимняя, способствует ее практической, прагматической и гуманистической направленности [3].

Подготовка студентов вуза к противодействию киберэкстремистской деятельности на основе личностно-ориентированного подхода обеспечивает опору на потенциал личности студента и развитие ее задатков и способностей, представляет органичное взаимодействие преподавателя и обучающихся, в ходе которого педагог создает условия к саморазвитию студента. Личностно-деятельностная дидактическая система позволяет при этом ввести студента в ситуацию, побуждающую выбор ценностных оснований собственного поведения, поиск смысла происходящего, рефлексию собственного поведения, принятие собственных решений [4].

В связи с выбранными подходами нами определены в модели следующие принципы:

1) принцип целостности;

2) принцип культуросообразности;

3) принцип интеграции педагогических и информационных технологий;

4) принцип сотрудничества;

5) принцип деятельности;

6) принцип профессиональной мобильности.

Принцип целостности предполагает целостное восприятие студентом окружающего мира в системе Интернет через виртуальное общение в информационных сетях. Принцип культуросообразности направлен на культивирование определенных этических установок по отношению к существующим в обществе нормам, правилам, принципам, обычаям и традициям. Становясь носителем культурно-исторических ценностей страны, студент воспринимает, репродуцирует эти ценности и стремится к творчеству новых культурных реалий, что является необходимым критерием эффективного противодействия явлениям киберэкстремизма.

Принцип интеграции педагогических и информационных технологий обеспечивает повышение качества подготовки студентов вуза в соответствии с требованиями современного информационного общества путем использования новейших информационных технологий в образовательном процессе. Принцип сотрудничества обеспечивает формирование субъект-субъектных отношений между участниками образовательного процесса, признание равноценности друг друга, проявление уважения, доверия и индивидуальной ответственности за выстраивание диалогических отношений в процессе реального и виртуального общения в сети Интернет, самореализации своей гражданской позиции и толерантного отношения к партнерам.

Принцип деятельности предполагает, что подготовка студентов вуза к противодействию киберэкстремистской деятельности происходит успешно за счет активной жизненной позиции и самореализации себя в учебно-профессиональной деятельности, направленной на получение новых знаний, приобретение, осмысление ценностей и процессов получения, обработки и переработки информации.

Принцип профессиональной мобильности обеспечивает развитие готовности студентов вуза быстро осваивать информационные технологии, перенос знания в реальную профессиональную деятельность, гибкое реагирование на нововведения, развитие потребности в непрерывном самообразовании в области новых информационных технологий и новейших методов превенции явлений киберэкстремизма.

Процессуально-методический компонент включает в себя методы и средства, формы обучения, функции, содержание и этапы реализации подготовки студентов вуза к противодействию киберэкстремистской деятельности. Методы подготовки студентов включают в себя: дискуссии (круглые столы, дебаты, мозговые штурмы), доказательство, критику, упражнения, защиты проектов, кейс-стади, проблемные методы, методы проектов и др. В качестве основных педагогических средств выступают: компьютерные средства

обучения, средства информационного взаимодействия и технические средства. Кроме того, при подготовке студентов важную роль играют разнообразие и богатство организационных форм обучения: мультимедиа-лекции, защиты групповых и индивидуальных проектов, совместное ведение блогов, дискуссии, практические занятия, защиты презентаций и курсовых работ.

Процессуально-методический компонент включает в себя такие функции подготовки студентов вуза, как обучающая, воспитательная, организационная, развивающая, интегративно-дифференцированная. Обучающая функция направлена на формирование у студентов профессиональных знаний, умений и навыков в сфере противодействия киберэкстремизму. Воспитательная функция заключается в гражданском, патриотическом и нравственном воспитании студентов. Развивающая функция состоит в развитии у студентов их интеллектуальной и эмоционально-волевой сферы. Организационная функция направлена на формирование умений студентов по организации противодействия киберэкстремистской деятельности среди молодежи. Интегративно-дифференцированная функция обеспечивает результативность учебно-познавательной деятельности в сфере превенции киберэкстремизма за счет дифференциации и индивидуализации обучения.

Содержание программы подготовки студентов вуза к противодействию киберэкстремистской деятельности может быть включено в учебные программы следующих курсов: «Информационная безопасность и защита информации», «Социальная информатика», «Информационная безопасность в образовании». Данный компонент включает следующие этапы подготовки студентов вуза к противодействию киберэкстремистской деятельности: адаптационно-ознакомительный, поисково-информирующий, практико-моделирующий, аналитико-обобщающий. Каждый этап направлен на достижение различных задач; каждый из последующих этапов включает результаты предыдущего и может существовать только на их основе.

Оценочно-результативный компонент модели включает уровни, критерии и показатели готовности студентов вуза к противодействию киберэкстремистской деятельности.

Следуя логике нашего исследования, мы остановились на трех уровнях готовности студентов – пассивно-адаптивном (низкий), ситуативно-репродуктивном (средний) и креативно-ценностный (высокий). Каждый уровень определяется по четырем критериям: когнитивному, операционно-деятельностному, личностному, аксиологическому. Эффективность функционирования любой модели зависит от реализации определенного комплекса условий [4]. Нами предложен комплекс педагогических условий:

1) формирование личностных и культурных ценностей обучающихся путем широкого применения на занятиях интерактивных методов;

2) формирование гражданской позиции студентов в процессе развития диалоговых умений через виртуальное общение;

3) развитие исследовательских навыков студентов в работе с информацией на основе метода проектов.

Выявленные педагогические условия характеризуются взаимозависимостью и взаимодополнением друг друга.

Разработанная нами модель подготовки студентов вуза к противодействию киберэкстремистской деятельности представлена на рисунке 1.

Заключение

Структурно-функциональная модель характеризуется:

1) целостностью, так как все указанные компоненты взаимосвязаны между собой, несут определенную смысловую нагрузку и работают на конечный результат — переход студента вуза на более высокий, качественно новый уровень противодействия киберэкстремистской деятельности;

2) открытостью, так как модель встроена в контекст системы профессиональной подготовки студентов вуза.

Суть разработанной модели подготовки студентов вуза к противодействию киберэкстремистской деятельности заключается в обеспечении перехода на более высокий уровень готовности студента к противодействию киберэкстремистской деятельности.

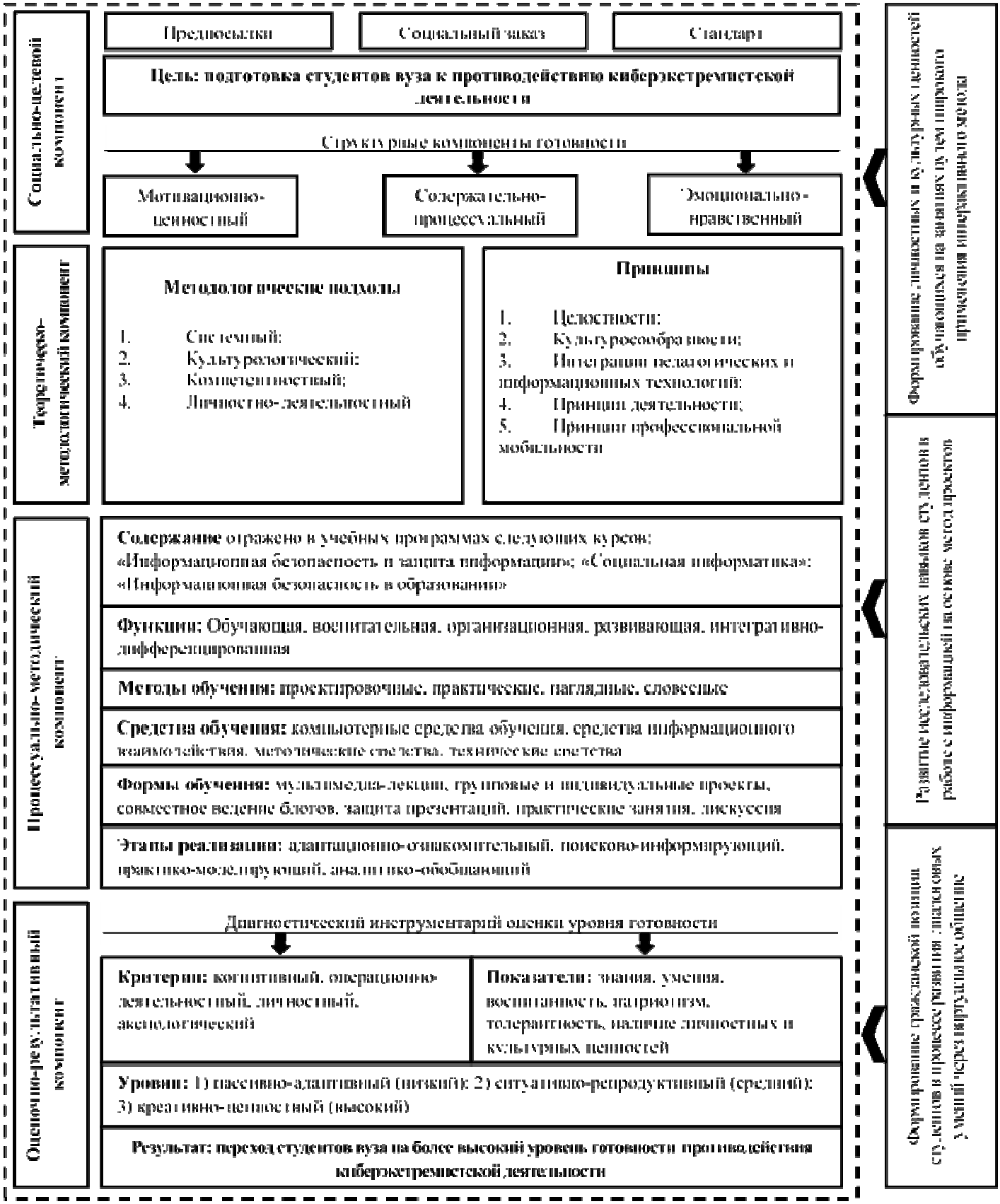

Рис. 1. Модель подготовки студентов вуза к противодействию киберэкстремистской деятельности

Список литературы

1. Чернова Е.В. Компетенции педагогических кадров в области превенции идеологии киберэкстремизма среди молодежи // Фундаментальные исследования. – 2013. – № 10. — Ч. 9. – С. 2075–2079.
2. Вехов И. В. Экстремизм как объект социологического исследования / И.В. Вехов // Известия РГПУ им. А.И. Герцена. – 2009. – № 111. – С. 284–290
3. Зимняя, И.А. Ключевые компетентности как результативно-целевая основа компетентностного подхода в образовании. Авторская версия / И.А. Зимняя. – М.: Исследовательский центр проблем качества подготовки специалистов, 2004. – 40 с.
4. Беликов, В.А. Личностная ориентация учебно-познавательной деятельности (дидактическая концепция) / В.А. Беликов. – Челябинск: Факел, 1995. – 141 с.
5. Социализация студентов в профессиональном образовании: монография / Л.И. Савва, А.Л. Солдатченко, Е.Б. Плотникова, Е.И. Рабина, Л.С. Рязанова // Под ред. Л.И. Савва. – М.: Издательский дом Академии Естествознания, 2012. – 300 с.

Рецензенты:

Сайгушев Н.Я., д.п.н., профессор кафедры педагогики профессионального образования ФГБОУ ВПО «Магнитогорский государственный университет им. Г.И. Носова», г. Магнитогорск;

Недосекина А.Г., д.п.н., профессор, зав. кафедрой педагогики и психологии ФГБОУ ВПО «Магнитогорская государственная консерватория им. М.И. Глинки», г. Магнитогорск.