УДК 378

ПОДГОТОВКА СПЕЦИАЛИСТОВ В ОБЛАСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ: ИННОВАЦИОННЫЙ ПОДХОД К ФОРМИРОВАНИЮ ОБРАЗОВАТЕЛЬНОЙ СРЕДЫ[1]

М.С. Чванова
Московский государственный университет технологий и управления имени К.Г. Разумовского, Россия, Москва
e-mail: tmbtsu@gmail.com

М.С. Анурьева, В.Ю. Лыскова, Н.А. Котова, А.А. Молчанов
Тамбовский государственный университет имени Г.Р. Державина, Россия, Тамбов
e-mail: anuryeva@mail.ru, veronikalyskova@ya.ru, nkotova01@yandex.ru, ykdosto@gmail.com

В статье рассматриваются возможности инновационного подхода к формированию образовательной среды в вузе при подготовке специалистов в области информационной безопасности. Актуальность применения подхода востребована динамикой современного технологического развития. Инновационный подход становится в современных условиях методологической платформой для организации исследовательской и проектной работы студентов, их научного общения с профессиональным сообществом, результативности совместной инновационной деятельности.

Целевая и содержательная компоненты подготовки специалистов диктуют направленность формирования образовательной среды. Поэтому особое внимание уделяется сравнительному анализу целей и содержания обучения в вузах в области информационной безопасности в Российской Федерации и передовых технологических странах: США, Франции, Германии, Англии.

На основе анализа авторы делают вывод о необходимости применения инновационного подхода к формированию образовательной среды вуза и включении компонентов, характерных для специалистов информационной безопасности.

Ключевые слова: инновационный подход, инновационная инфраструктура, образовательная среда, сравнительный анализ, информационная безопасность, социальное партнерство.

Экономика страны ориентируется на инновационную стратегию развития, что отражено в правительственных документах, в частности – Стратегии инновационного развития РФ до 2020 г. Потребность в выпускниках, способных создавать инновационный продукт или услугу, заставляет вузы формировать соответствующую инновационную инфраструктуру (студенческие конструкторские бюро, центры коммерциализации технологий, центры инжиниринга и маркетинговых исследований, центры трансферта технологий, малые инновационные предприятия и др.). Рассмотрим с этих позиций проблемы формирования современной образовательной среды в вузе для подготовки специалистов в области информационной безопасности.

На сегодняшний день существует необходимость глубокого анализа интеграционных процессов в различных направлениях подготовки по информационной безопасности в связи с развитием IT-отрасли и ее проникновением как в ключевые компоненты профессиональной деятельности, так и в компоненты образовательной среды самого вуза. Кроме того, стремительно развиваются инновационные разработки в направлении интеллектуализации инструментов профессиональной деятельности специалиста по информационной безопасности, что неизбежно заставляет задуматься о необходимости включения в образовательную среду инфраструктурные компоненты развития инновационной деятельности студентов и ее результативности.

Сегодня освоение механизмов развития инновационной деятельности в вузе происходит на фундаменте старого методологического базиса. Имеющаяся практика и большое количество исследований в области инновационных процессов в высшем образовании позволяют обобщить определенный опыт. Вместе с тем, эти процессы не приводят к существенным изменениям образовательной среды, способствующей формированию специалиста для инновационной экономики. В конечном итоге нарушается замкнутый процесс от создания до продвижения инноваций в экономику страны. Создается эффект

[1] Отдельные результаты исследования получены при финансовой поддержке РГНФ в рамках научно-исследовательского проекта «Инновационный подход к формированию образовательной среды в вузе и его реализация в IT-сервисах», проект № 15-06-10306, 2015-2017.

«холостого хода». Обращение к практике ведущих стран (Южной Кореи, США, Германии, Китая, Канады и др.) в области инновационного развития не дали исчерпывающего ответа на вопрос возможного переноса идей построения моделей современной образовательной среды в вузе применительно к российской системе образования. Каждая страна решает задачи по-своему. Для особенностей России с ее протяженностью важно найти решение, приемлемое для разных регионов.

По нашему мнению, новым базисом к формированию образовательной среды вуза, на котором будет выстраиваться подготовка специалистов в области информационной безопасности, становится инновационный подход. Этот методологический фундамент должен включать платформу для построения теоретических основ формирования образовательной среды вуза и учитывать необходимость развития инновационной проектной деятельности, формирования инновационного мышления, навыков работы в команде по созданию инновационного продукта или услуги, развития механизмов социального партнерства и взаимодействия с производством и бизнесом, умения находить оптимальное решение, договариваться с партнерами, работать на международном уровне в области создания и продвижения инноваций и многое другое.

Значительная часть исследователей в области инновационных процессов в образовании транслируют традиционно используемые методологические подходы (системный, синергетический, кластерный и др.) так или иначе для создания инновационной инфраструктуры и образовательных технологий. Вместе с тем, активное развитие инновационных процессов требует поиска и исследования методологического базиса, на котором эти процессы эффективно функционируют. Как мы полагаем, им (базисом) является инновационный подход, имеющий свои специфические особенности.

Инновационные процессы в высшем образовании опираются на принцип «новых задач», базируются на подготовке специалиста, умеющего генерировать новые идеи, разрабатывать новые технологии, создавать инновационные продукты и услуги. Передовые технологии несут в себе новое решение, новые методы, новые подходы, новые возможности, еще не известные системе образования. Очевидно, что «традиционная лекция» и «традиционный учебник» – малоэффективны при развитии инновационной экономики. Нужен организованный и направленный доступ к динамичным системам актуальной информации, нужны доступные в любое время «автоматизированные консультации», нужны новые способы и приемы организации совместной проектной деятельности и многое другое.

Прежде всего, важно проанализировать целевую и содержательную направленность подготовки студентов в вузах по информационной безопасности в развитых странах. С этой целью нами проведен анализ по данному направлению в России, Великобритании, Германии, Франции и США.

Отечественная система подготовки специалистов представлена государственными образовательными стандартами, учебными планами, подготовленными учебно-методическим объединением по образованию в области информационной безопасности. На сегодняшний день высшее образование в области защиты информации ведется по следующим направлениям подготовки.

Специальность «Компьютерная безопасность» в большей степени отражает особенности использования методов защиты в различных информационных технологиях. К объектам профессиональной деятельности можно отнести информационные технологии, технологии обеспечения информационной безопасности и системы управления информационной безопасностью.

Специальность «Информационная безопасность телекоммуникационных систем» содержит набор специализированных дополнительных дисциплин. Это объясняется тем, что телекоммуникационные системы выполняют «транспортные функции».

Специальность «Информационная безопасность автоматизированных систем» обладает широким спектром охвата различных вопросов профессиональной деятельности. Это объясняется тем, что, обеспечивая безопасность автоматизированной системы, надо рассматривать систему в целом, ее часть и даже определенный компонент.

Специальность «Информационно-аналитические системы безопасности» в большей степени ориентирована на информационно-

аналитическое обеспечение информационной безопасности, автоматизированных информационных систем, баз данных и информационных систем, финансовых и правоохранительных структур.

Специальность «Безопасность информационных технологий в правоохранительной сфере» ориентирована на использование информационных технологий, методов управления информационной безопасности и средств защиты информации, а также информационно-аналитического обеспечения правоохранительной деятельности.

Бакалавриат и магистратура по направлению подготовки «Информационная безопасность» содержит набор дисциплин, охватывающих широкий круг вопросов информационной безопасности.

При рассмотрении видов деятельности и содержания образовательных программ в двухуровневой системе подготовки (бакалавриат – магистратура) и моноуровневой системе (специалитет) можно сделать вывод о том, что главное отличие проявляется, прежде всего, в полноте набора дисциплин двухуровневой системы. Это говорит о том, что бакалавры (магистры) должны отличаться широтой спектра профессиональных компетенций, а специалисты – их глубиной.

Рассмотрим образование в области информационной безопасности в Великобритании. Подготовкой специалистов занимаются не менее чем в 64 университетах (колледжах), которые имеют более 220 образовательных программ, связанных с защитой информации. После завершения обучения выпускник получит соответствующую степень: бакалавра гуманитарных, или естественных, или технических наук; магистра гуманитарных, или естественных, или технических наук; магистра права; магистра философии. Также после получения степени бакалавра имеется возможность получить Сертификат (PgCert) или Диплом (PgDip) о поствысшем образовании.

При рассмотрении предметной области подготовки бакалавров и магистров нами выделены шесть направлений (профилей) подготовки, охватывающих: сферу законодательства в области информационных систем; сферу компьютерной безопасности; безопасности информационных технологий; расследования компьютерных инцидентов; сферу безопасности компьютерных сетей; менеджмент информационной безопасности.

Подавляющее большинство программ подготовки бакалавров представлены по направлению, связанному с расследованием компьютерных инцидентов – 3% – и безопасностью информационных технологий – 27%, что, возможно, свидетельствуют о потребности общества в многообразии сфер деятельности или специалистах данного профиля.

Среди магистерских программ направление «Безопасность информационных технологий» возрастает до 33%. Почти вдвое уменьшается число магистерских программ по расследованию компьютерных инцидентов до 17%, возрастает количество программ по безопасности компьютерных сетей до 17%, сократилось количество программ по законодательству в сфере информационных технологий до 9%. Возможно, это связано с потребностью профессиональной сферы в высокообразованных специалистах данного направления и устойчивых тенденциях их подготовки.

Проанализированы наборы дисциплин в каждом укрупненном блоке как в системе подготовки бакалавров, так и в системе поствысшего образования, в том числе магистратуре. Программы, входящие в укрупненный блок, имеют схожий набор предметов и включают в себя дисциплины, связанные в основном со специальными вопросами информационной безопасности.

Рассмотрим образовательные программы в Германии [1-3]. Анализ показывает, что обучение по данному направлению строится в рамках Болонского процесса. Университеты в своих образовательных программах придерживаются принципа автономии. Набор дисциплин в каждом вузе по направлению подготовки различен, вузы сами определяют содержание образования, методику преподавания, штатное расписание [4]. Обучение имеет двухступенчатую структуру. В бакалавриате дают относительно широкую подготовку, учат пополнять, обновлять знания, умения и навыки по мере необходимости. Магистратура предполагает более узкую и глубокую специализацию, магистрант ориентирован на научно-исследова-

тельскую работу в области информационной безопасности.

Отличительной особенностью немецких программ является свобода выбора студентами достаточно широкого набора вариативных дисциплин. Вуз устанавливает, какие курсы выступают обязательными. Так, для направления подготовки «Компьютерные науки (Информационная безопасность)» (бакалавриат) в Боннском университете к общим обязательным дисциплинам относятся: основы физики и математики, теоретическая информатика, введение в программирование, анализ и числовые методы, базы данных и системы управления, структуры данных и алгоритмы, разработка программного обеспечения, информационная безопасность. Обязательные специализированные дисциплины включают: электронные ключи, прикладную криптографию, безопасность мобильных устройств, управление информационной безопасностью. В то же время студенты могут осваивать дисциплины по выбору: беспроводные локальные сети, аппаратные средства безопасности, основы управления ИТ-рисками, поиск информации, мобильные информационные системы, объектно-ориентированные системы программирования, программирование, безопасную разработку программных систем, статистический анализ данных, основы бизнеса, операционные системы, управление сетями, распределенные и параллельные системы.

Обучение в магистратуре по направлению подготовки «Информационная безопасность» базируется на программе подготовки бакалавра, но отличается технологической широтой, глубиной изучения специализированных предметов. Кроме того, программа подготовки магистра дает большую гибкость в выборе дисциплин для изучения и, следовательно, большую свободу при индивидуальном обучении. Блок обязательных дисциплин незначителен и в него входят информационная безопасность, криптография и безопасность сетей. В то же время дисциплины по выбору имеют явную специализацию: безопасность компьютерных сетей, безопасность программного обеспечения информационных систем, информационное законодательство, ИТ-безопасность бизнес-приложений. И в конце обучения магистрант выбирает одно из факультативных направлений, включающее несколько специализированных курсов.

Отметим, что в образовательных программах по информационной безопасности полностью отсутствует привычный для российского образования блок гуманитарных дисциплин (философия, психология, история), зато много дисциплин, связанных с законодательством и правом на интеллектуальную собственность, бизнес-процессы, межличностные отношения и управление персоналом. Эти знания и навыки дают возможность выпускникам взаимодействовать с бизнес-сообществом, например обосновывать перед руководством необходимость инвестирования в безопасность, увязывать политику информационной безопасности с общей стратегией развития бизнеса.

Формы обучения имеют классические черты – лекции, работа над заданиями в компьютерных классах, семинары, выступления студентов, но существуют и особенности, среди них самостоятельная работа в небольших группах при реализации конкретных проектов, связанных с информационной безопасностью и разработкой опытных образцов, ролевые игры. Широко применяется приглашение сторонних докладчиков для объяснения соответствующих практических примеров. Отметим практическую направленность и ориентацию на бизнес стажировки бакалавров и магистрантов, зачастую именно компании и организации формулируют цели и задачи стажировок и производственных практик.

Перейдем к анализу национальной системы подготовки специалистов в области информационной безопасности во Франции. Рассмотренные образовательные программы показывают, что обучение во Франции строится в рамках национальных стандартов и имеет свои особенности [5]. Так, подготовка специалистов по областям, связанным с информационной безопасностью, ведется только в рамках «длинного» цикла с присуждением дипломов профессиональной лицензии (аналог диплома бакалавра) и магистра. Следует отметить, что во Франции практически нет программ лицензиата в сфере защиты информации, такие программы в основном относят-

ся к магистерским. Причем в магистратуру можно поступить, имея профессиональную лицензию по математике или информатике.

Специалистов по информационной безопасности готовят по направлениям: «Информационные системы аудита, специального программного обеспечения, безопасность информационных систем и технологий» [6], «Управление информационной безопасностью» [7], «Кибербезопасность» [8], «Криптология и информационная безопасность» [9], «Аудит безопасности и компьютерная экспертиза» [10], «Информационная безопасность, криптография и кодирование информации» [11], «Организации защиты информационных систем в бизнесе» [12], «Безопасность и администрирование сетей» [13], «Математическая информатика и криптография» [14], «Защита контента, сетей и телекоммуникаций» [15].

Рассмотренные учебные планы французских вузов показывают, что студенты самостоятельно могут выбирать не более двухтрех предметов. В этом проявляется определенное сходство с формами работы российских вузов, в которых студенты тоже не могут варьировать изучаемые предметы, и существенное отличие от учебных планов немецких университетов.

Французская подготовка ориентируется на изучение вопросов, связанных с криптографией, сетевой безопасностью и аудитом информационных систем. Среди особенностей «французской школы» – студентам дается серьезное математическое образование, необходимое для освоения математических аспектов криптологии и компьютерной безопасности. Обучение сетевой безопасности полностью строится на моделях реальных сетей, сетевых архитектурах, включая подсистемы безопасности и аутентификации, использовании реального оборудования. Подготовка экспертов в области компьютерной безопасности включает разделы аудита на наличие уязвимостей, построение систем защиты от вторжений. В отличие от Германии и Великобритании, мало внимания уделяется дисциплинам, связанным со сбором доказательств и расследованием инцидентов компьютерной безопасности, применением программно-аппаратной защиты информации, в том числе электронных ключей.

Учебный план состоит из общих и специализированных дисциплин, полугодовой производственной стажировки и практических проектов. При обучении акцент делается на самостоятельную или в малых группах работу. Студенты принимают участие в стажировках (от 4 до 6 месяцев) в компании или научно-исследовательской лаборатории, стажировку проходят по месту будущего трудоустройства. В конце каждого года результаты оцениваются на основании письменного экзамена и проекта. Получить диплом можно, набрав средний бал не менее 10 из 20 по всем дисциплинам, в том числе и по проекту.

Рассмотрим национальную систему высшего образования [16], образовательные программы бакалавриата и магистратуры в области информационной безопасности в США [17-19]. Система имеет особенность – децентрализацию управления образованием на уровне штатов. Практически все вопросы образовательной политики решаются именно на этом уровне, хотя существуют и отдельные федеральные программы, финансируемые и контролируемые Министерством образования США.

Система высшего образования включает в себя колледжи и университеты, общее число которых превышает 4300. Четырехгодичное образование в США (университеты и колледжи) дает возможность получить академические степени ассоциата или бакалавра, профессиональные квалификации, профессионально-технические квалификации. После этого можно получить научные степени магистра или доктора.

Наиболее востребованными программами бакалавриата являются: «*Расследование компьютерных инцидентов», «Информационная безопасность», «Компьютерная безопасность», «Безопасность компьютерных сетей».*

Программы подготовки бакалавров рассчитаны на четыре года обучения, после чего присуждается степень бакалавра компьютерных наук со специализацией в выбранной области. Программы включают дисциплины общего образования (гуманитарные – английский язык, публичные выступления, этику бизнеса, естественные – математику, статистику, информатику – языки программирования, программное обеспечение систем,

компьютерную архитектуру, вычислительные алгоритмы). Значительное число дисциплин составляют обязательные курсы для изучения, которые являются специализированными. Например, для направления подготовки «Расследование компьютерных инцидентов» основные дисциплины составляют компьютерную криминалистику, файловые системы, проектирование баз данных, компьютерные сети, экспертизу мошенничества.

Студенты могут самостоятельно выбрать незначительное (три-четыре) количество дисциплин по выбору, направленных на освоение дополнительных знаний и умений в выбранной области подготовки. Так, для студентов, обучающихся расследованию компьютерных инцидентов, дисциплины по выбору составляют – преступность среди несовершеннолетних, пен-тесты, методы борьбы с должностными преступлениями, специальные темы законодательства, судебный процесс, судебную антропологию, судебную экспертизу, объектно-ориентированное программирование, экспертизу мошенничества. Видно, что блок дисциплин по выбору охватывает несколько возможных специализаций расследований компьютерных преступлений – социальные подходы, судебные экспертизы, законодательство, технологии проникновения, программирование. Таким образом, студенты самостоятельно выбирают свою узкую специализацию в рамках общей подготовки.

Как правило, студенты проходят практику в течение всего курса обучения. В первом семестре студенты в рамках практики проводят поиск литературы, составляют план исследований и инициируют научные исследования или конструкторские работы по специальности. На старших курсах студенты в рамках практики проводят исследования или конструкторские работы. Другой частью обучения являются стажировки, направленные на возможность приобретения значимых навыков и профессиональных качеств и изучения опыта в промышленности, государственных, частных или бизнес-структурах. В конце обучения студенты предоставляют проект или диссертацию по тематике специализации.

Отметим, что много интегрированных направлений подготовки, таких как «Информационная безопасность и управление рисками», «Биометрика и информационная безопасность», «Компьютерная безопасность и расследование инцидентов», «Сети и информационная безопасность» и ряд других. Это говорит о заинтересованности в специалистах смежных областей, что находит свое отражение в наборе дисциплин для изучения. Так, в одном блоке могут соседствовать такие предметы, как биометрия и криптография; управление информационной безопасностью, анализ уязвимостей и аудит; безопасность баз данных и аудит, протокол безопасности, проектирование распределенных систем.

Такой подход к построению обучения позволяет выпускникам обладать широкими ключевыми компетенциями: способностью инсталлировать и администрировать ресурсы стандартных операционных систем и устройств хранения данных, способностью выполнять административные функции, связанные с доступностью информации и информационных технологий, способностью определить отношения между информационными технологиями и юридическим аспектом компьютерной экспертизы, способностью применять навыки, связанные с документированием отчетности данных, полученных с цифровых устройств, способностью применять фундаментальные судебные методы в области информационных технологий, способностью применять политику для защиты компьютерных систем от угроз.

Проведенный анализ образовательных программ магистратуры показывает, что в отличие от бакалавриата, при рассмотрении подготовки магистранта в сфере информационной безопасности, можно выделить до шести укрупненных блоков: «Информационная безопасность», «Компьютерная безопасность», «Расследование компьютерных инцидентов», «Безопасность компьютерных сетей», «Управление информационной безопасностью», «Экономика информационной безопасности».

Отметим, что в магистратуре, в отличие от бакалавриата, наиболее востребованными являются «Информационная безопасность», «Компьютерная безопасность», «Управление информационной безопасностью».

Получение степени магистра наук в области информационной безопасности подра-

зумевает теоретическую и практическую подготовку. Студенты осваивают технические и аналитические возможности для защиты данных, файлов, ресурсов компьютера, компьютерной сети, применение разумной политики безопасности в бизнесе и государственных органах, а также защиту критически важных национальных электронных инфраструктур. Студенты обучаются установке программного обеспечения систем безопасности, мониторингу сети в целях обнаружения вторжений, реагированию на кибератаки, сбору данных и доказательств.

Для каждого направления подготовки характерно сочетание дисциплин из различных областей. Например, для направления подготовки «Информационная безопасность» основными обязательными дисциплинами являются: информационная безопасность, расследование компьютерных инцидентов, управление информационной безопасностью, межсетевые экраны и обнаружение вторжений, безопасность беспроводных сетей, ИТ-аудит. К дисциплинам по выбору относятся: социальные аспекты информационной безопасности, данные и интеллектуальный анализ, безопасность распределенных баз данных, безопасность электронной коммерции, политика информационной безопасности, прикладная криптография, практические вопросы безопасности, специальные вопросы информационной безопасности, независимые исследования. Видно, что в американской системе обучения специалистов в области информационной безопасности придерживаются широкого профиля подготовки.

Заканчивается обучение в магистратуре выполнением магистерского проекта или диссертации под руководством преподавателя или группы профессорско-преподавательского состава. Как правило, в конце магистратуры студент имеет возможность получить один из профессиональных сертификатов, что повышает его конкурентоспособность на рынке труда.

Выявлены различия в вариантах образовательных маршрутов, в формах организации и способах итоговой аттестации, в соотношении объемов вариативной и инвариантной частей, в формах обучения в зарубежных странах [20]. Так, например, в Великобритании и США самыми популярными среди студентов являются программы, связанные с расследованием компьютерных инцидентов (компьютерная форензика). Темы по расследованию компьютерных инцидентов распространены во всех странах, что является заметным отличием от содержания подготовки в российских вузах (схожая дисциплина «Компьютерная экспертиза» встречается только в специальности 090915 – Безопасность информационных технологий в правоохранительной сфере, готовят по ней студентов в небольшом количестве).

В зарубежных программах отсутствуют дисциплины по физической защите и инженерно-технической защите информации, традиционные для российских программ (которые ориентированы на сохранение конфиденциальности информации). Во всех зарубежных странах много времени отводится на изучение дисциплин, связанных с обеспечением информационной безопасности в открытых бизнес-системах и электронной коммерции.

На основе выявленных ключевых различий в рассмотренных образовательных системах можно проследить основные направления развития содержания обучения:

– внедрение дисциплин, связанных с расследованием компьютерных инцидентов («Расследование компьютерных инцидентов», «Компьютерная форензика»);

– увеличение доли материала, ориентированного на правоприменительные технологии в области информационной безопасности, в том числе основанные на международном праве («Законодательство в сфере коммерческих компьютерных систем», «Законодательство в сфере информационных технологий», «Законодательство в сфере использования сети Интернет», «Киберправо»);

– включение дисциплин, связанных с внедрением технологий информационной безопасности в бизнес, электронную коммерцию, коммерческим применением интеллектуальных прав («Безопасность электронной коммерции», «Безопасность Интернет-бизнеса», «Безопасный электронный бизнес» и др.).

Внедрение подобных дисциплин будет способствовать росту квалификации выпускников, необходимой для решения современных задач обеспечения информационной

безопасности в государственных и коммерческих структурах.

Таким образом, анализ содержательной компоненты показал, что независимо от ментальности и традиций формирования содержания образовательных программ в разных странах им присуще общее: во-первых, ориентация на динамичные изменения профессиональной среды; во-вторых, на саму среду накладываются все новые задачи, порожденные развитием информационного общества.

Вместе с тем, на современном этапе университет становится не столько местом «передачи знаний», сколько местом, где происходит «генерация инновационных идей». Именно в университете студенту помогут сформулировать его инновационную идею и довести ее до опытного образца, а в идеале – создать условия ее реализации на рынке инновационных товаров и услуг.

Для реализации таких планов следует внести изменения в процесс обучения студентов не только в целевом и содержательном плане, но и пересмотреть процесс формирования инновационной образовательной среды, способствующей творческому самовыражению и самореализации личности обучающегося, а также обеспечивающей каждому студенту более полное раскрытие своих способностей. Фактически речь идет о системе образовательной деятельности, где линейность соподчиненности различных этажей иерархии системы образования заменяется формированием неформальных центров, консолидирующих различные образовательные структуры независимо от их организационно-правовой формы и схемы финансирования, в единый организм, связанный общностью целей и сбалансированной реализацией интересов каждого, в рамках достижения своей наивысшей эффективной конкурентоспособности при четкой ориентации на создание инновационно-образовательного комплекса ускоренного развития приоритетных направлений социальной сферы и реального сектора экономики [21].

Российские университеты, стараясь ответить на вызовы времени, активно приступили к внедрению элементов инновационной деятельности и формированию инновационной инфраструктуры (центров коммерциализации технологий, маркетинговых исследований, малых инновационных предприятий и др.). Однако в стране еще не создана институциональная инновационная система, которая позволила бы реализовать «замкнутый инновационный цикл». Цепочка управления инновациями – от идеи до коммерциализации – имеет многочисленные разрывы. Именно эти разрывы создают эффект «холостого хода» и пока не приводят к зримым экономическим результатам [22].

На развитие инновационных процессов и успешной коммерциализации научно-технических достижений (как в стране, так и в стенах вуза) влияет наличие развитой инновационной инфраструктуры, центров коммерциализации технологий, маркетинговых исследований на рынке товаров и услуг и многое другое. Одной из основных проблем низкой эффективности использования научно-технологических возможностей университета как одного из производителей интеллектуального продукта является его слабое взаимодействие с рынком. Для обеспечения конструктивного диалога между работодателями и учебными заведениями требуется развитие механизмов социального партнерства, которые предусматривают не только совместную работу в области формирования вариативной составляющей образовательного стандарта, совместную аттестацию специалистов и выпускников, новую систему оценки качества подготовки выпускников, но и разработку экономических механизмов научно-исследовательского и профессионального сотрудничества на основе системы договоров и отработки механизмов инвестиций в систему подготовки специалистов [23].

В общем контексте под социальным партнерством понимают совместную, коллективно распределенную деятельность различных социальных групп, которая приводит к позитивным и разделяемым всеми участниками данной деятельности эффектам [24]. Одной из форм социального партнерства является проектная деятельность студентов, аспирантов, преподавателей, которая позволяет создавать социально значимые инновационные проекты в сотрудничестве с различными предприятиями, организациями и людьми [25].

Инновационные процессы в высшем образовании должны опираться на принцип

«новых задач», которые несут в себе новые возможности [26]. На сегодняшний день вся инновационно-образовательная деятельность вузов, в лучшем случае, замыкается в кругу лабораторий. Необходимо не только сотрудничество с учреждениями, но и создание инновационной образовательной среды, способствующей формированию у студентов мотивирующей системы участия в инновационной деятельности. Обучаясь, они занимаются не только образовательной деятельностью, но и вовлекаются в процесс проектирования и совершенствования производственных разработок до опытных образцов. При подобном подходе студенты уже на этапе обучения включаются в решение актуальных задач и реализацию потребностей, стоящих перед бизнесом. По нашему мнению, только в этом случае бизнес-структуры начинают активно вкладывать свои средства в образование.

Важно акцентировать внимание на интеграции естественнонаучных и гуманитарных знаний, опираться на инновационный подход, в основе которого лежит идея усиления ресурсов участников социального партнерства в достижении общего интереса и интересов каждого. Исходя из такого понимания, осуществляется ориентация на концентрацию ресурсов партнеров в области информационной безопасности (кадровых, научных, инновационных, технологических, образовательных и др.) для достижения общих целей – подготовки высококвалифицированных специалистов и организации проектной деятельности в области информационной безопасности на основе создания «точки роста» в университете.

Остановимся на основных направлениях реализации инновационного подхода.

Во-первых, это направленность образовательного процесса на постоянную актуализацию целей и содержание подготовки специалистов по информационной безопасности и синхронизацию с потребностями региона. Например, в ТГУ имени Г.Р. Державина, учитывая потребность в квалифицированных кадрах в сфере защиты информации, лицензированы и реализуются следующие направления и специальности: с 2002 г. – 075300 – Организация и технология защиты информации; с 2012 г. – 090915 – Безопасность информационных технологий в правоохранительной сфере; с 2011 г. – 090900 – Информационная безопасность. В настоящее время на вышеперечисленных направлениях и специальностях обучается более 250 человек ежегодно.

Во-вторых, это обеспечение непрерывного повышения квалификации преподавателей, профессорско-преподавательский состав выпускающей кафедры систематически обновляет знания и черпает опыт по следующим направлениям подготовки: «Информационная безопасность: Современные технологии обеспечения компьютерной безопасности» (НОУДПО «Институт информационных технологий “АйТи”», г. Москва); «Защита информации ограниченного доступа», «Комплексная защита информации в организации», «Организация комплексной защиты информации на предприятиях, в учреждениях и организациях» (ООО «Центр безопасности информации «МАСКОМ», г. Москва); «Безопасность информационных систем» (Microsoft® Security Guidance I, г. Москва).

В-третьих, это участие вузовской общественности в общегосударственных событиях. Конкретный пример – решением Межведомственной комиссии по защите государственной тайны с 2003 г. ТГУ имени Г.Р. Державина включен в перечень учебных заведений, осуществляющих подготовку специалистов по вопросам защиты информации, свидетельство об окончании которых дает руководителям предприятий, учреждений и организаций право на освобождение от государственной аттестации. Включение в указанный перечень позволяет вузу взаимодействовать с реальным сектором экономики и систематизировать работу по подготовке работников режимных органов хозяйствующих субъектов в сфере защиты информации ограниченного доступа. К настоящему времени обучение на курсах прошли сотрудники более 100 организаций области.

Получены различные лицензии, которые также свидетельствуют о включенности вуза в государственные дела. Среди их многообразия: лицензия ФСТЭК России на осуществление мероприятий и (или) оказание услуг в области защиты государственной тайны; лицензия ФСТЭК России на проведение работ, связанных с созданием средств защиты информации; Аттестат ак-

кредитации органа по аттестации ФСТЭК России СЗИ. В 2002 г. создан Институт проблем информационной безопасности, который со временем оптимизировал и трансформировал свою организационную структуру. Он оснащен современными техническими средствами защиты информации, имеет квалифицированных специалистов и необходимую материально-техническую и нормативно-методическую базу.

В-четвертых, это активизация участия преподавателей и студентов в общегосударственных инновационных конкурсах как катализаторе результативности работы в данном направлении. Университет стал одним из победителей конкурса вузов, внедряющих инновационные образовательные программы, что позволило создать материально-техническую базу, включающую оборудование, предназначенное для образовательного процесса и осуществления работ в сфере информационной безопасности.

В-пятых, это мотивированное участие преподавателей и студентов в научно-исследовательских и инновационных проектах в области информационной безопасности. Это участие в научно-исследовательской деятельности по направлению информационной безопасности, поддерживаемой фондами РГНФ и РФФИ. Это вопросы, связанные с модернизацией содержания и технологий образования, работы по созданию принципиально новых программно-аппаратных разработок, моделей, алгоритмов. Активная позиция в данном направлении позволяет привлекать молодежь к инновационной деятельности и готовить высококвалифицированные кадры.

Особенностью и отличительной чертой деятельности университета является четкая ориентация на реализацию инновационных образовательных программ и повышение инвестиционной привлекательности вуза [23]. Он использует участие студенческой молодежи в образовательной, инновационной и научной деятельности. Для этого в университете ежегодно проводятся внутривузовские конкурсы на лучший инновационный проект и конкурс «Инновационные идеи и разработки». За последние семь лет было сформировано более 150 инновационных студенческих проектов по информационной безопасности. Ежегодно студенты становятся участниками молодежного научно-инновационного конкурса («У.М.Н.И.К.») Фонда содействия развитию малых форм предприятий в научно-технической сфере. Данный конкурс направлен на выявление молодых талантов и стимулирование массового участия молодежи в научно-технической и инновационной деятельности.

Значительная часть дипломных проектов и работ в области информационной безопасности базируется на обширных экспериментальных исследованиях, результатах производственных практик. Более 60% студентов вовлечены в постоянную активную исследовательскую работу, что находит отражение в их исследовательских публикациях и в участии в различных научных мероприятиях. Студенты выступают с докладами на международных и российских научно-практических конференциях. Научно-исследовательские работы выполняются в соответствии с реальными заданиями конкретных заказчиков и содержат элементы научных исследований. Это дает возможность последующего трудоустройства наиболее творческих и инициативных представителей студенческой молодежи.

Важная роль в активизации деятельности студентов принадлежит студенческим объединениям. Университет четыре года подряд участвует в конкурсе Минобрнауки по Программе развития деятельности студенческих объединений (в 2012-2013, 2014, 2015 гг.), целью которой является развитие студенческого самоуправления и повышение роли студенчества в модернизации образовательной, научной, инновационной деятельности и социокультурной среды вуза. Коллектив университета включил в Программу проекты по созданию студенческого бизнес-инкубатора.

В-шестых, создание инновационной инфраструктуры. Безусловно, что элементы структуры отличные для каждого вуза и во многом определяются наличием людей, способных обеспечить развитие «точек роста». Так, в Центре компьютерной безопасности ведутся научные исследования по мониторингу и анализу пользовательских инфокоммуникационных угроз, разработке принципов и методов надежной защиты информационных ресурсов сложной структуры, мо-

делирования молекулярных систем, пригодных для квантовой криптографии и других приложений. Студенты могут получить знания мирового уровня и инструментальные компетенции, максимально приближенные к современной практике. Организован и поддерживается wiki-проект «Анализ угроз информационного характера для различных целевых групп», где проходят стажировку студенты старших курсов.

Студенческая проектная деятельность, осуществляемая в виде курсовых и дипломных работ, организована таким образом, что выполнение отдельной работы является решением законченной прикладной задачи или теоретической проблемы, и способна дать студенту понимание отдельного (зачастую, ключевого) элемента, необходимого для построения целостной системы безопасности.

Каждый год предлагается более сотни исследовательских тем. Инновационные разработки студентов, выполненные в Центре компьютерной безопасности, вполне успешно участвуют как во внутриуниверситетских, так и внешних конкурсах. Среди последних работ можно отметить следующие:

– «Разработка инновационной технологии проактивной защиты для обнаружения скрытного заражения ОС Windows». Проект направлен на комбинированное использование способов обнаружения скрытых процессов в режиме ядра и режиме пользователя для повышения эффективности обнаружения вредоносного программного обеспечения. Данная работа поддержана в 2011 г. «У.М.Н.И.К.».

– «Оригинальное программное обеспечение для создания электронно-цифровой подписи документов с помощью электронного ключа ruToken». Проект базируется на использовании самого стойкого на сегодняшний день криптоалгоритма RSA и наиболее стойких электронных ключей. Работа в 2012 г. заняла первое место на конкурсе инновационных проектов университета.

– «Динамическая фильтрация контента». Проект направлен на обеспечение безопасности пользователя ИКТ. Фильтрация контента происходит без вмешательства со стороны пользователя, в результате чего ему предоставляется только предназначенный (проверенный) онлайн-контент. Работа представлена в 2013 г. на IT-школе Центрального федерального округа (Программа Росмолодежи «It-start.pro»).

– «Анализ угроз инфокоммуникационного характера в России». В рамках проекта определены и охарактеризованы целевые группы пользователей инфокоммуникационных технологий. Проведен анализ интернет-ресурсов и периодической литературы, связанных с компьютерной безопасностью и угрозами информационного характера. Получена информация об актуальном уровне ИКТ-угроз для пользователя. Работа в 2012-2013 гг. поддержана РГНФ.

Таким образом, опора на инновационный подход к формированию образовательной среды дает возможность:

– использовать разные формы и методы поддержки инновационной деятельности молодежи и формировать у студентов мотивирующую способность;

– включать в содержание и организацию учебного процесса знания теоретических основ исследовательской, инновационной деятельности;

– ориентировать изначально проектную деятельность студента на конкретную профессионально ориентированную научно-исследовательскую задачу;

– использовать механизмы социального партнерства, что дает возможность конструктивного диалога между работодателями и учебными заведениями;

– ориентировать инновационную инфраструктуру университета (бизнес-инкубатор, технопарк, центры коллективного пользования, центры трансфера технологий и др.) в направлении продвижения инноваций от идеи до опытно-экспериментального образца и предложения на рынке инноваций.

Все перечисленное способствует подготовке высококвалифицированного специалиста в условиях развития инновационной экономики. Несмотря на трудности и проблемы настоящей ситуации, важно сохранить ориентацию на лучшие практики. В качестве аргумента, подтвержающего вышеизложенное, можно констатировать: в мире наиболее престижна и уважаема модель глобального исследовательского университета (global research university), который является актив-

ным игроком в производстве новых знаний, их распространении и практическом использовании. Ключевыми направлениями их развития являются:

– включение преподавателей и студентов в инновационную деятельность в качестве приоритетной;

– университет становится центром коммуникации бизнеса, общества и государства по вопросам прогнозирования и решения глобальных проблем;

– сотрудничество с реальным сектором экономики в поисках заказов на прикладные разработки;

– полидисциплинарность исследований;

– организация инновационных предприятий;

– создание международных исследовательских групп.

Российские университеты, обладая заметным потенциалом, только становятся одним из элементов национальной инновационной системы, осваивают не свойственные им ранее функции. Перенос опыта инновационной деятельности без учета особенностей университета (и территориальных особенностей России) невозможен. Но опора на инновационный подход с его инвариантной сущностью позволяет ориентировать развитие образовательной среды вуза с зарождающимися инновационными потребностями реального сектора экономики.

Литература

1. Leibniz Universität Hannover [Электронный ресурс]. URL: http://www.uni-hannover.de/de/studium/studienfuehrer/it-recht/index.php (дата обращения 28.05.2015).
2. Master Internet-Sicherheit [Электронный ресурс]. URL: http://www.internet-sicherheit.de/de/lehrebereich/master-internet-sicherheit (дата обращения 28.05.2015).
3. Master SecMan – Security Management [Электронный ресурс]. URL: http://fbwcms.fh-brandenburg.de/de/5185 (дата обращения 28.05.2015).
4. Чванова М.С., Анурьева М.С. Система высшего образования в ФРГ. Подготовка специалистов в области информационной безопасности // Вестник Тамбовского университета. Сер.: Гуманитарные науки. Тамбов, 2012. Вып. 6 (110). С. 78-84.
5. Чванова М.С., Анурьева М.С. Подготовка специалистов в области информационной безопасности во Франции // Вестник Тамбовского университета. Сер.: Гуманитарные науки. Тамбов, 2012. Вып. 7 (111). С. 159-165.
6. Université de Caen Basse-Normandie Licence Pro Systèmes informatiques et logiciels spécialité Audit et sécurité des réseaux et des systèmes d'information [Электронный ресурс]. URL: http://www.unicaen.fr/formations/licence-pro-systemes-informatiques-et-logiciels-specialite-audit-et-securite-des-reseaux-et-des-systemes-d-information-388693.kjsp?RH=1272443206988 (дата обращения 28.05.2015).
7. Executive Master – Information Security Governance [Электронный ресурс]. URL: http://www.iae-aix.com/files/fiches/msc_gsi.pdf (дата обращения 28.05.2015).
8. CyberSecurity [Электронный ресурс]. URL: http://www.telecom-bretagne.eu/formations/masteres_specialises/cybersecurite/ (дата обращения 28.05.2015).
9. Cryptologie et sécurité informatique [Электронный ресурс]. URL: http://www.u-bordeaux1.fr/ufr/math-info/formation/mathematiques-pures/master/csi-cryptologie-et-securite-informatique.html (дата обращения 28.05.2015).
10. Master mention mathématiques, informatique – spécialité audit informatique legale safe [Электронный ресурс]. URL: https://www.ujf-grenoble.fr/formation/master-mention-mathematiques-informatique-specialite-securite-audit-informatique-legale-safe-p (дата обращения 28.05.2015).
11. Master mention mathématiques, informatique – spécialité sécurité, cryptologie et codage de l'information [Электронный ресурс]. URL: https://www.ujf-grenoble.fr/formation/master-mention-mathematiques-informatique-specialite-securite-cryptologie-et-codage-information-r-et (дата обращения 28.05.2015).
12. Organisation et Protection des Systèmes d'Information dans les Entreprises [Электронный ресурс]. URL: http://www.univ-lyon2.fr/master-2-organisation-et-protection-des-systemes-d-information-dans-les-entreprises-opsie-specialite-professionnelle-informatique-decisionnelle-et-statistique-ids--264018.kjsp?RH=WWW20202 (дата обращения 28.05.2015).
13. Professionnel Administration et Sécurité des Réseaux [Электронный ресурс]. URL: http://www.master-informatique.net/m2proasr.html (дата обращения 28.05.2015).
14. Mathématiques de l'information, Cryptographie [Электронный ресурс]. URL: http://etudes.univ-rennes1.fr/master-crypto/themes/Objectifs (дата обращения 28.05.2015).
15. Master 2 professionnel Sécurité des Contenus, des Réseaux, des Télécommunications et des

Systèmes (SeCReTS) [Электронный ресурс]. URL: http://www.uvsq.fr/formations-et-inscriptions/master-2-professionnel-securite-des-contenus-des-reseaux-des-telecommunications-et-des-systemes-secrets--117243.kjsp?RH=FORM2 (дата обращения 28.05.2015).
16. Чванова М.С., Анурьева М.С. Подготовка кадров в области информационной безопасности в США // Вестник Тамбовского университета. Сер.: Гуманитарные науки. Тамбов, 2012. Вып. 8 (112). С. 126-133.
17. Bloomsburg, Digital forensics [Электронный ресурс]. URL: http://www.bloomu.edu/digital_forensics (дата обращения 28.05.2015).
18. University of Tennessee At Chattanooga, IT Security [Электронный ресурс]. URL: http://www.utc.edu/information-technology/security/ (дата обращения 28.05.2015).
19. Master of Science in Information Assurance and Security [Электронный ресурс]. URL: https://www.mercy.edu/academics/school-of-liberal-arts/department-of-mathematics-and-cis/ms-in-information-assurance-and-security/ (дата обращения 28.05.2015).
20. Анурьева М.С. Общее и особенное в системах подготовки специалистов в области информационной безопасности в России и зарубежных странах // Гаудеамус. Тамбов, 2012. № 2 (20). С. 116-118.
21. Юрьев В.М., Чванова М.С., Передков В.М. Университет как центр инновационно-образовательного кластера // Вестник Тамбовского университета. Сер.: Гуманитарные науки. Тамбов, 2007. Вып. 5 (49). С. 7-12.
22. Юрьев В.М., Чванова М.С. Привлечение молодежи к научной, инновационной деятельности и развитию социально-культурной среды университета // Молодежь и социум. Тамбов, 2013. № 2 (14). С. 6-13.
23. Чванова М.С. Социальное партнерство в сфере профессионального образования // Гаудеамус. Тамбов, 2006. № 2 (10). С. 47-56.
24. Авво Б.В. Социальное партнерство в условиях профильного обучения: учебно-методическое пособие / под ред. А.П. Тряпицыной. СПб.: Каро, 2005. 96 с.
25. Чванова М.С., Храмова М.В., Молчанов А.А. Социальное партнерство – один из механизмов совершенствования социально-инновационной деятельности вуза // Образовательные технологии и общество. 2012. Т. 15. № 2. С. 581-601. URL: iFets.ieee.org/russian/depository/v15_i2/html/16.htm
26. Малыгин Е.Н., Фролова Т.А., Чванова М.С. Инженерная педагогика: учебное пособие для студентов вузов, обучающихся по непедагогическим специальностям. Тамбов: Издательство ТГТУ, 2005. 80 с.

References

1. Leibniz Universität Hannover [`Elektronnyj resurs]. URL: http://www.uni-hannover.de/de/studium/studienfuehrer/it-recht/index.php (data obrascheniya 28.05.2015).
2. Master Internet-Sicherheit [`Elektronnyj resurs]. URL: http://www.internet-sicherheit.de/de/lehrebereich/master-internet-sicherheit (data obrascheniya 28.05.2015).
3. Master SecMan – Security Management [`Elektronnyj resurs]. URL: http://fbwcms.fh-brandenburg.de/de/5185 (data obrascheniya 28.05.2015).
4. Chvanova M.S., Anur'eva M.S. Sistema vysshego obrazovaniya v FRG. Podgotovka specialistov v oblasti informacionnoj bezopasnosti // Vestnik Tambovskogo universiteta. Ser.: Gumanitarnye nauki. Tambov, 2012. Vyp. 6 (110). S. 78-84.
5. Chvanova M.S., Anur'eva M.S. Podgotovka specialistov v oblasti informacionnoj bezopasnosti vo Francii // Vestnik Tambovskogo universiteta. Ser.: Gumanitarnye nauki. Tambov, 2012. Vyp. 7 (111). S. 159-165.
6. Université de Caen Basse-Normandie Licence Pro Systèmes informatiques et logiciels spécialité Audit et sécurité des réseaux et des systèmes d'information [`Elektronnyj resurs]. URL: http://www.unicaen.fr/formations/licence-pro-systemes-informatiques-et-logiciels-specialite-audit-et-securite-des-reseaux-et-des-systemes-d-informa-tion-388693.kjsp?RH=1272443206988 (data obrascheniya 28.05.2015).
7. Executive Master – Information Security Governance [`Elektronnyj resurs]. URL: http://www.iae-aix.com/files/fiches/msc_gsi.pdf (data obrascheniya 28.05.2015).
8. CyberSecurity [`Elektronnyj resurs]. URL: http://www.telecom-bretagne.eu/formations/masteres_specialises/cybersecurite/ (data obrascheniya 28.05.2015).
9. Sryptologie et sécurité informatique [`Elektronnyj resurs]. URL: http://www.u-bordeaux1.fr/ufr/math-info/formation/mathematiques-pures/master/csi-cryptologie-et-securite-informatique.html (data obrascheniya 28.05.2015).
10. Master mention mathématiques, informatique – spécialité audit informatique legale safe [`Elektronnyj resurs]. URL: https://www.ujf-grenoble.fr/formation/master-mention-mathematiqu-es-informatique-specialite-securite-audit-informatique-legale-safe-p (data obrascheniya 28.05.2015).
11. Master mention mathématiques, informatique – spécialité sécurité, cryptologie et codage de l'information [`Elektronnyj resurs]. URL: https://www.ujf-grenoble.fr/formation/master-men-tion-mathematiques-informatique-specialite-securite-cryptologie-et-codage-information-r-et (data obrascheniya 28.05.2015).

12. Organisation et Protection des Systèmes d'Information dans les Entreprises [`Elektronnyj resurs]. URL: http://www.univ-lyon2.fr/master-2-organisation-et-protection-des-systemes-d-information-dans-les-entreprises-opsie-specialite-professionnelle-informatique-decisionnelle-et-statistique-ids--264018.kjsp?RH=WWW20202 (data obrascheniya 28.05.2015).
13. Professionnel Administration et Sécurité des Réseaux [`Elektronnyj resurs]. URL: http:// www.master-informatique.net/m2proasr.html (data obrascheniya 28.05.2015).
14. Mathématiques de l'information, Cryptographie [`Elektronnyj resurs]. URL: http://etudes.univ-rennes1.fr/master-crypto/themes/Objectifs (data obrascheniya 28.05.2015).
15. Master 2 professionnel Sécurité des Contenus, des Réseaux, des Télécommunications et des Systèmes (SeCReTS) [`Elektronnyj resurs]. URL: http://www.uvsq.fr/formations-et-inscriptions/master-2-professionnel-securite-des-contenus-des-reseaux-des-telecommunications-et-des-systemes-secrets--117243.kjsp?RH=FORM2 (data obrascheniya 28.05.2015).
16. Chvanova M.S., Anur'eva M.S. Podgotovka kadrov v oblasti informacionnoj bezopasnosti v SShA // Vestnik Tambovskogo universiteta. Ser.: Gumanitarnye nauki. Tambov, 2012. Vyp. 8 (112). S. 126-133.
17. Bloomsburg, Digital forensics [`Elektronnyj resurs]. URL: http://www.bloomu.edu/digital_forensics (data obrascheniya 28.05.2015).
18. University of Tennessee At Chattanooga, IT Security [`Elektronnyj resurs]. URL: http://www.utc.edu/information-technology/security/ (data obrascheniya 28.05.2015).
19. Master of Science in Information Assurance and Security [`Elektronnyj resurs]. URL: https:// www.mercy.edu/academics/school-of-liberal-arts/ http://www.mercy.edu/academics/school-of-liberal-arts/department-of-mathematics-and-cis/ms-in-informa-tion-assurance-and-security/ (data obrascheniya 28.05.2015).
20. Anur'eva M.S. Obschee i osobennoe v sistemah podgotovki specialistov v oblasti informacionnoj bezopasnosti v Rossii i zarubezhnyh stranah // Gaudeamus. Tambov, 2012. № 2 (20). S. 116-118.
21. Yur'ev V.M., Chvanova M.S., Peredkov V.M. Universitet kak centr innovacionno-obrazovatel'nogo klastera // Vestnik Tambovskogo universiteta. Ser.: Gumanitarnye nauki. Tambov, 2007. Vyp. 5 (49). S. 7-12.
22. Yur'ev V.M., Chvanova M.S. Privlechenie molodezhi k nauchnoj, innovacionnoj deyatel'nosti i razvitiyu social'no-kul'turnoj sredy universiteta // Molodezh' i socium. Tambov, 2013. № 2 (14). S. 6-13.
23. Chvanova M.S. Social'noe partnerstvo v sfere professional'nogo obrazovaniya // Gaudeamus. Tambov, 2006. № 2 (10). S. 47-56.
24. Avvo B.V. Social'noe partnerstvo v usloviyah profil'nogo obucheniya: uchebno-metodicheskoe posobie / pod red. A.P. Tryapicynoj. SPb.: Karo, 2005. 96 s.
25. Chvanova M.S., Hramova M.V., Molchanov A.A. Social'noe partnerstvo – odin iz mehanizmov sovershenstvovaniya social'no-innovacionnoj deyatel'nosti vuza // Obrazovatel'nye tehnologii i obschestvo. 2012. T. 15. № 2. S. 581-601. URL: iFets.ieee.org/russian/depository/v15_i2/html/16.htm
26. Malygin E.N., Frolova T.A., Chvanova M.S. Inzhenernaya pedagogika: uchebnoe posobie dlya studentov vuzov, obuchayuschihsya po nepedagogicheskim special'nostyam. Tambov: Izdatel'stvo TGTU, 2005. 80 s.

PREPARATION OF SPECIALIST IN THE SPHERE OF INFORMATIONAL SECURITY: INNOVATIONAL APPROACH TO FORMATION OF EDUCATIONAL SPHERE

M.S. Chvanova
Moscow State University of Technologies and Management named after K.G. Razumovskiy, Russia, Moscow
e-mail: tmbtsu@gmail.com

M.S. Anuryeva, V.Y. Lyskova, N.A. Kotova, A.A. Molchanov
Tambov State University named after G.R. Derzhavin, Russia, Tambov.
e-mail: anuryeva@mail.ru, veronikalyskova@ya.ru, nkotova01@yandex.ru, ykdosto@gmail.com

The article deals with the possibility of an innovative approach to the formation of the educational environment in university during training in the field of information security. Topical application of the approach in demand dynamics of modern technological development. Innovative approach in modern conditions become a methodological platform for the organization of research and design work of students, their scientific dialogue with the professional community, the effectiveness of joint innovation.

Target and substantial component of training specialists dictate the direction of the formation of the educational environment. Therefore, special attention is paid to the comparative analysis of the objectives and content of education in universities in the field of information security in the Russian Federation and the advanced technological countries: USA, France, Germany, England.

Based on the analysis the authors conclude on the need for an innovative approach to the formation of the educational environment of the university and the inclusion of components specific to information security professionals.

Key words: innovative approach, innovation infrastructure, educational environment, comparative analysis, information security, social partnership.