Секция: ИНФОРМАТИКА И ИНФОРМАТИЗАЦИЯ ОБРАЗОВАНИЯ

УДК 004.056(43)

# НАПРАВЛЕНИЯ РАЗВИТИЯ ОТЕЧЕСТВЕННОЙ СИСТЕМЫ ПОДГОТОВКИ СПЕЦИАЛИСТОВ ПО ЗАЩИТЕ ИНФОРМАЦИИ

**© М.С. Анурьева**

*Ключевые слова*: информационная безопасность; специалист по защите информации; развитие системы подготовки специалистов по защите информации.

Рассмотрены возможные направления развития отечественной системы подготовки специалистов в области информационной безопасности.

Современное содержание подготовки специалистов в области информационной безопасности сформировалось в России на основе исторически сложившихся особенностей. Защита информации отождествлялась с охраной государственной тайны и сводилась в основном к физической защите по жестким правилам государственных структур безопасности. В то же время активные процессы информатизации, вовлечение частного сектора в процессы обработки информации требуют совершенствования как содержания, так и образовательных технологий при подготовке специалистов по защите информации, которая должна отвечать современным тенденциям и развитию новейших методов в этой области (правовых, инженерно-технических, компьютерных, управленческих).

В России на сегодняшний день проводится большая работа по разработке правовых и научно-методических основ реформирования высшего профессионального образования, в т. ч. в области информационной безопасности. В данной статье рассмотрены возможные направления развития отечественной системы подготовки специалистов в области информационной безопасности. Среди направлений выделены следующие.

*Переход от ориентации подготовки специалистов в большей степени на требования государственных режимных структур к ориентации в т. ч. на открытое бизнес-сообщество*. Компенсировать недостаточные знания специалистов в области бизнес-процессов и удовлетворять растущие требования коммерческих организаций можно путем включения и увеличения во всех направлениях подготовки и специальностях доли дисциплин, связанных с внедрением технологий информационной безопасности в бизнес, электронную коммерцию, коммерческим применением интеллектуальных прав. Примерами таких дисциплин могут быть «Бизнес и безопасность информационных технологий», «Безопасность интернет-бизнеса», «Безопасность электронного бизнеса» и др. Внедрение подобных дисциплин будет способствовать росту квалификации выпускников, необходимой для решения современных задач обеспечения информационной безопасности в государственных и коммерческих структурах.

*Развитие содержательной линии направлений подготовки и специальностей в области информационной безопасности.* Назрела необходимость внедрения во все направления подготовки и специальности дисциплин, связанных с обучением базовым теоретическим и практическим навыкам расследования компьютерных инцидентов. В настоящее время специалисты, способные проводить компьютерную экспертизу, в большей степени востребованы в правоохранительных органах, органах следствия, прокуратуры и судах. Между тем крупные и средние коммерческие структуры заинтересованы в борьбе с инцидентами в сфере компьютерной безопасности как силами сторонних организаций, так и штатными средствами и силами своих сотрудников.

Таким образом, в настоящее время в России существует необходимость внедрения во все направления подготовки и специальности дисциплин, связанных с обучением базовым теоретическим и практическим навыкам расследования компьютерных инцидентов.

Также отличием в содержательной линии отечественных и зарубежных направлений подготовки специалистов в области информационной безопасности является отсутствие в российской системе подготовки дисциплин, связанных с правоприменительными технологиями в области информационной безопасности, в т. ч. основанных на применении международного права. Примерами дисциплин могут выступать: «Законодательство в сфере коммерческих компьютерных систем», «Законодательство в сфере компьютерных систем и информационных технологий», «Законодательство в сфере использования Интернета», «Киберправо (информационные технологии, право и гражданская ответственность)».

Отметим также, что необходимых изменений в содержательной линии требует рассмотренная выше переориентация на потребности коммерческих структур и бизнес-сообщества.

*Взаимодействие учебного заведения с разного рода производственными и коммерческими компаниями в т. ч. в области проектной деятельности по обеспечению информационной безопасности на объекте.* Необходимые навыки в области информационной безопасности, такие как разработка принципов и методов надежной защиты информационных ресурсов сложной структуры, защита информации по внутреннему каналу утечки информации, администрирование систем защиты информации, связанных с доступностью информации и информационных технологий, определение отношения между информационными технологиями и юридическим аспектам и др., можно получить только в реальных условиях производственного процесса. Моделирование подобных ситуаций в стенах высшего образовательного учреждения ведет к узкому и порой далекому от истины пониманию вопросов, связанных с внедрением элементов системы защиты информации на предприятии, организации и коммерческой структуре.

Одним из механизмов взаимодействия учебного заведения с разного рода производственными и коммерческими компаниями в последнее время можно считать т. н. *кластерный подход* [1]. Речь идет об объединении, укрупнении, своеобразной агломерации в функциональном, а чаще всего – в географическом смысле разных учреждений и производств вокруг интеллектуального, мозгового центра (в данном случае, например, выпускающая кафедра).

Сотрудничество с предприятиями в рамках кластерного подхода на основе проектной деятельности студентов старших курсов путем научно-технического сопровождения перспективных разработок в области информационной безопасности послужит основой для формирования благоприятных педагогических условий при подготовке специалистов в области информационной безопасности.

*Повышение академической мобильности студентов, обучающихся по направлениям (специальностям) в области информационной безопасности.* Программы академической мобильности разнообразны и могут включать в себя краткосрочные поездки с целью разработки совместных программ и проектов образовательного и исследовательского характера в области информационной безопасности, совместные образовательные программы по дисциплинам, связанным с информационной безопасностью, повышение квалификации и стажировки преподавателей, студентов и др. Причем формы обучения могут быть как дистанционными, так и очными.

*Внедрение вендорских и вендеронезависимых обучающих модулей в обучающий процесс по направлениям подготовки и специальностям в области информационной безопасности с возможной последующей сертификацией.* Сотрудничество вузов с крупными вендорами, внедрение в систему подготовки вендорских и вендеронезависимых решений на паритетной основе, подготовка будущих специалистов к международной сертификации позволит улучшить технологическую базу, а будущим специалистам – обрести целостный подход к информационной безопасности, требуемый профессиональной сертификацией.

*Повышение профессиональной квалификации преподавателей в области информационной безопасности.* Особенно остро проблема недостаточной квалификации преподавателей стоит в области подготовки специалистов для наукоемких отраслей (таких как информационная безопасность), которые требуют высококлассного профессорско-преподавательского состава, новейшего оборудования и динамичного обновления содержания обучения [2]. В российской системе подготовки специалистов в области информационной безопасности необходимо шире привлекать специалистов, имеющих высшее базовое образование в области информационной безопасности и успешно прошедших период становления и работы в крупных компаниях на должностях, связанных с информационной безопасностью. Несомненно, для привлечения высококлассных специалистов необходима их грамотная мотивация. Вместе с тем увеличение числа специализированных стажировок, академической мобильности, получение профессиональных сертификатов профессорско-преподавательского состава будет способствовать миграции от «преподавателя-теоретика» к «преподавателю-практику» и повышению качества подготовки специалистов в области информационной безопасности.

*Совершенствование форм и методов обучения, направленных на развитие компетенций в организационно-управленческой, контрольно-аналитической, информационно-аналитической деятельности при обеспечении информационной безопасности.* Новые формы и методы обучения российских специалистов в области информационной безопасности, направленные, в первую очередь, на развитие компетенций в организационно-управленческих, контрольно-аналитических, информационно-аналитических видах деятельности, могут включать активные методы обучения – тренинги, учебные групповые дискуссии, обучение методом кейсов (case-study), деловые и ролевые игры. Помимо активных методов и технологий будет полезно применять и другие механизмы развития системы подготовки специалистов, в т. ч. мастер-классы, выездные семинары, лекции с привлечением высококвалифицированных специалистов-практиков, работающих в области информационной безопасности.

*Развитие научно-исследовательской деятельности студентов и преподавателей для решения проблем в области гуманитарного и научно-технического обеспечения информационной безопасности.* Научно-исследовательская деятельность студентов и преподавателей может развиваться через участие в российских и интернациональных научно-исследовательских проектах, через систему грантов, выделяемых на проведение исследований в областях: гуманитарных проблем обеспечения информационной безопасности; развития правового обеспечения информационной безопасности; обеспечения безопасности индивидуального, группового и массового сознания; развития современных информационных технологий; разработки эффективных способов защиты информационных ресурсов, информационных и телекоммуникационных систем и др. [3].

## ЛИТЕРАТУРА

1. *Чванова М.С., Малышева Н.В., Киселева И.А., Передков В.М., Самохвалов А.В.* Проектная деятельность студентов и школьников на основе кластерного подхода // Вестник Тамбовского университета. Серия Гуманитарные науки. Тамбов, 2009. Вып. 9 (77). С. 240-253.

2. *Юрьев В.М., Чванова М.С.* Кластерный подход в подготовке специалистов наукоемких специальностей // Вестник Тамбовского университета. Серия Естественные и технические науки. Тамбов, 2009. Т. 14. Вып. 5. С. 872-876.
3. *Шерстюк В.П.* МГУ: научные исследования в области информационной безопасности. URL: http://pycode.ru/2011/03/research/. Загл. с экрана.

Поступила в редакцию 23 ноября 2012 г.

Anuryeva M.S. TRENDS OF NATIONAL TRAINING OF INFORMATION PROTECTION SPECIALISTS

The possible directions of development of the national system of training in the field of information protection are discussed.

*Key words*: information security; information security specialists; development of training in information protection specialists.