©Depositphotos/nenovbrothers

Кадровая модель

Инструкция по сборке

В перечне приоритетных для модернизации экономики России специальностей — всего три позиции, которые имеют отношение к безопасности. Да и те охватывают лишь отдельные аспекты: методы и системы защиты информации, ядерная/радиационная безопасность, а также химическая, биологическая и бактериологическая безопасность. Нужно ли говорить, что реалии российского бизнеса в какой-то степени отражены далеко не полностью? Оказывается, нужно. При обилии технических вузов в стране лишь немногие выстраивают обучение с прицелом на отраслевые рынки труда. И совсем единицы пытаются наладить прямой диалог с потенциальными работодателями будущих выпускников.

Текст: Григорий Дитятев

Расходы федерального бюджета на высшее профессиональное образование в РФ

Год	Расходы федерального бюджета, млн руб.	В расчете на 1 студента, руб.
2005	116 951,0	19 539,7
2006	159 940,0	26 078,2
2007	221 501,0	35 677,6
2008	280 021,6	45 057,2
2009	328 623,7	53 560,2
2010	316 228,9	54 068,2
2011	393 307,1	55 789,83
2012	437 906, 0	67 473,97
2013	477 238,4	79 539,75
2014	484 106,1	84 192,37
2015	513 536,9	93 370,35

Данные порталов www.sdo.rea.ru, www.ecpol.ru, www.rbc.ru, www.ria.ru, www.rosbalt.ru, www.infostat.ru

Бакалавр или специалист?

В соответствии с проводимой реформой высшего образования российские вузы внедряют новый европейский формат обучения — бакалавриат. Образовательное новшество означает ускоренно-упрощенную систему выпуска специалистов, «заточенных» непосредственно под работу в конкретных сегментах и рынках. Во-первых, нововведение призвано экономить год при получении высшего образования. Вместо традиционных пяти лет обучение длится четыре года. Во-вторых, остальные знания по профессии, как предполагается, свежеиспеченный бакалавр получит в буквальном смысле слова на практике или на стажировке. Диплом бакалавра не позволяет выпускнику «на автомате» поступать в аспирантуру и получать кандидатскую степень — стране нужны рабочие руки. Умные рабочие руки.

При этом нельзя сказать, что программы высшего образования начинают идти навстречу потребностям бизнес-сообщества. Самый яркий пример — информационные технологии. Центр принятия решений по построению систем безопасности все чаще смещается на практике от служб безопасности к IT-департаментам. И вопрос всего нескольких лет, когда возникнут и укрепятся новые отраслевые стандарты, объединенные приставкой «IT». Именно здесь, очевидно, и будет востребован общий подход к профессиональной подготовке специалистов. Но его у вузов до сих пор нет.

Простой пример. Специальность «информационная безопасность» прочно закрепилась в высших учебных заведениях России; от столицы до периферии. Однако даже сама формулировка «информационная безопасность» в разных вузах звучит по-разному. В Московском институте электроники и математики (МИЭМ) это «компьютерная безопасность», в Московском техническом университете связи и информатики (МТУСИ) — «информационная безопасность телекоммуникационных систем», в Московском физико-техническом институте (МФТИ) или Саратовском государственном техническом университете (СГТУ) — «информационная безопасность автоматизированных систем». Понятно, что полной идентичности не достичь, различия не случайны и связаны с генетикой каждого вуза. Однако гораздо логичней было бы положить подготовку IT-специалистов на некую общую научно-теоретическую базу, понятную в итоге всем одинаково, с последующей специализацией в рамках дополнительных курсов по направлениям — основы видеонаблюдения и видеоаналитики, СКУД, ОПС.

В интернете на специализированных форумах студенты немало пишут о недостатках подготовки по специальности «информационная безопасность». Главные претензии: недостаточное количество часов на профильные предметы, устаревшие учебные курсы, отсутствие должной компетенции преподавателей. Есть и позитивные предложения, в частности, ввести тему аудита информационной безопасности, обучать методам оценки финансовой целесообразности и экономической эффективности используемых систем защиты. Читать эти пожелания студентов особенно грустно на фоне реально существующей в индустрии проблемы: нет ясных единых, обоснованных критериев полезности при построении систем безопасности. Отсутствие профессиональной цеховой культуры приводит к тому, что огромное количество выпускаемых из разных институтов специалистов говорят каждый на своем языке. И масштабные федеральные программы — например, концепции «Безопасных городов» — вынуждены использовать количественный подход при выборе решений, закладывая объемы оборудования «с запасом», а не «на результат». Таким образом, буксует не только развитие тех или иных бизнес-направлений, но и напрямую снижается уровень технической безопасности в обществе.

От архаики к реальности

В сложившейся ситуации выглядит очевидным шаг к сотрудничеству институтов непосредственно с компаниями и предприятиями, из которых состоит та или иная отрасль, в том числе индустрия систем безопасности. Однако, за исключением подведомственных МЧС институтов, вузы упорно остаются в стороне от сотрудничества с рынком.

Редкие исключения лишь подтверждают общее правило. По итогам опроса мнений работодателей из разных регионов России можно отметить факультет радиотехники и электроники (РЭФ) Новосибирского государственного технического университета (НГТУ) и механико-математический факультет (ММФ) Новосибирского государственного университета (НГУ); эти институты являются донорами кадров для компаний по системам безопасности в Сибирском регионе.

Упомянутый выше МТУСИ осуществляет подготовку специалистов в области информационной безопасности. Представители университета утверждают, что его выпускники работают в госучреждениях и проектных организациях, во время обучения студенты изучают оборудование и технологии, реально применяемые компаниями.

В МИЭМе совместно с компанией QNAP студенты недавно получили возможность пройти двухдневный курс подготовки, разработанный учебным центром для партнеров фирмы. В Санкт-Петербурге также учебный центр QNAP сотрудничает с Национальным исследовательским университетом информационных технологий, механики и оптики (НИУ ИТМО).

По словам руководителя учебного центра Дениса Копранова, вузовская программа «QNAP Integrated» не входит в число обязательных учебных дисциплин для студентов. Обучение платное, хотя для студентов и партнеров фирмы предусмотрены скидки, продолжается два дня, содержит как теоретическую, так и практическую составляющие. По окончании курса слушатели получают сертификаты. Высшие учебные заведения могут использовать оборудование в учебном процессе по своему усмотрению. Взаимодействие QNAP с вузами продолжается уже более двух лет.

В то же время факультет радиотехники и кибернетики МФТИ в 2012 году завершил аналогичное сотрудничество с ЗАО «Безопасность». Оно продолжалось с 2006 года. Причины разрыва туманны: в компании уверяют, что во всем виноваты последние изменения к российскому «Закону об образовании», в институте эту версию отвергают, однако завершение проекта предпочитают не комментировать.

В целом высшее образование по-прежнему сохраняет архаичную основу (именно так сегодня выглядит то, что при СССР было принято считать академической традицией). Бакалавр-реформа затрагивает вопрос о том, КАК готовить людей с высшим образованием. Но оставляет открытым вопрос, КОГО и ДЛЯ ЧЕГО готовить. Ни в существующей системе, ни в рамках ее обновления не предусмотрены механизмы оценки и прогнозирования потребностей отраслей, также отсутствуют способы мониторинга навыков — квалификаций, реально востребованных работодателями.

В российских вузах практически не сформированы советы работодателей. Единственный результат поиска по соответствующему запросу в Google — создан совет работодателей при философском факультете Саратовского государственного университета имени Н.Г. Чернышевского. В остальном, по отзывам представителей бизнеса, их если и приглашают к сотрудничеству, то лишь для участия в деятельности попечительских советов. Кулуарно принимаемые учебные планы руководство вузов не считает нужным с кем-либо согласовывать. Практически все вузы заявляют, что проводят открытые защиты дипломов, однако что они собой представляют и кому конкретно адресованы — не уточняют.

Впрочем, справедливости ради следует отметить: кое-где такие защиты действительно носят неформальный характер. К примеру, Институт вычислительной математики и информационных технологий Казанского (Приволжского) федерального университета уже приобрел традицию проводить открытые защиты в режиме онлайн-конференций с потенциальными работодателями. Именно так бизнес-партнеры института, главный из которых — «Татнефть», подбирают специалистов по информационной безопасности. Представители других бизнес-направлений, за пределами ресурсодобывающих монополий, продолжают питать надежду, что такое сотрудничество с вузами со временем станет возможным и для них. Но произойдет это, очевидно, не на данном этапе реформы высшего образования.

©Depositphotos/perseomedusa