

сурского, проект «Востребованное образование» предполагает, что работодатели будут формулировать запрос на решение актуальных проблем своего бизнеса, социальных и практических задач в виде тем для проведения конкурсов учебных и дипломных работ. В следующем учебном году начиная с сентября больше десяти вузов примет участие в пилотном, добровольном этапе проекта. Работы выпускников будут опубликованы, а их учащиеся смогут с помощью учебной работы построить себе карьеру — хотя бы в виде практики или стажировки, бюджетных мест в аспирантуре или гранта на продолжение исследований. «Развитие электронных систем для студентов, в том числе для публикации научных работ, безусловно, сдвинет процесс в лучшую сторону», — резюмирует Антон Меркуров, эксперт Institute for State Ideologies.

**БЛИЗКО К ПРОВАЛУ** Отдельная категория сотрудников, которая очень нужна оборонке, — специалисты в области информационных технологий по самым разным направлениям. Сегодня невозможно выпускать современную промышленную продукцию без интенсивного внедрения ИТ в процессы разработки и производства. Поэтому достижение цели новой индустриализации невозможно без перевода в цифровой формат инженерно-конструкторской, производственно-технологической и финансово-экономической деятельности высокотехнологичных предприятий. «К сожалению, руководство промышленных предприятий относится к ИТ не как к стратегической задаче изменения технологического уклада и перехода к новому формату деятельности, а как к второстепенному фактору производства», — отмечает Владимир Рубанов, член общественного совета при Минпромторге РФ. По его словам, топ-менеджеры слабо представляют роль, место и возможности ИТ, а также требования к соответствующей реорганизации предприятия и подготовке кадров при их внедрении. Это требует включения в образовательный стандарт для руководящих кадров компетенции заказчика информационных технологий и систем производственно-го назначения.

Это критически важная задача, ведь промышленные предприятия сейчас часто работают на устаревших системах, что повышает риск подвергнуться нападению хакеров. В XXI веке задачи ОПК во многом переместились в область кибернетической безопасности. «Для повышения обороноспособности и в том числе кадровой безопасности страны предприятия ОПК должны не только формировать заказ, но и предугадывать его на будущее. Сегодня большой акцент в этой сфере стоит на машиностроении (двигатели, летательные аппараты, спелтехника), последние конфликты показали, что война будущего — это в первую очередь кибербезопасность», — говорит Антон Меркуров. В эту сферу, по его словам, попадают как защита стратегические объекты, так и наступательные функции. Если раньше нам нужны были солдаты на поле боя, то в ближайшем будущем воевать они будут не выходя из-за компьютера. И задача государства в этой сфере — обеспечить привлекательные рабочие места и формулировать задачи, нацеленные на развитие собственных продуктов для защиты.

В идеале в каждой автоматизированной системе управления (АСУ) материальными и людскими ресурсами уже должны быть встроены средства кибербезопасности. В устаревших решениях их, конечно, нет. При этом ущерб от неправильной работы таких систем, от последствий их взлома может быть огромен. К примеру, подобные АСУ, которые в XXI веке все чаще становятся мишенью кибертеррористов, используются на критически важных объектах: транспортных узлах, АЭС, ТЭС, ГЭС, на крупных производственных предприятиях и т. п.

В большинстве случаев такие АСУ построены на программно-аппаратном обеспечении зарубежного произ-



В РОССИЙСКОЙ ПРОМЫШЛЕННОСТИ ВСЕ ЕЩЕ НАБЛЮДАЕТСЯ ДЕФИЦИТ МОЛОДЫХ СПЕЦИАЛИСТОВ

водства, которое, как говорят эксперты, во-первых, не является доверенным, во-вторых, имеет множественные уязвимости. На всем жизненном этапе АСУ — от проектирования до эксплуатации — задействованный в процессах персонал ввиду не очень высокой компетенции и отсутствия специальных знаний может допускать существенные ошибки, что негативно сказывается на защищенности подобных систем. Во многом подобная ситуация складывается ввиду отсутствия систематизированной подготовки кадров.

Эта проблема касается не только предприятий ОПК, но также и других системообразующих отраслей российской экономики, например нефтегазовой и электроэнергетической. Учитывая особенный характер получаемых при обучении знаний и умений, связанный с двойным вариантом их применения, эта область образовательной деятельности должна иметь особый уровень контроля качества, говорят в «Ростехе». Речь идет не о совершенствовании федерального контроля качества образования в области информбезопасности, а о создании дополнительной системы контроля, основанной на сертификации квалификационного уровня выпускников образовательных учреждений. Для этого необходимо создать комплекс сертификационных требований, определить совокупность доверенных независимых сертификационных центров и предоставить всем желающим возможности пройти испытания и подтвердить соответствующий сертификационный уровень. Разработка сертификационных программ должна вестись на основе создаваемых профессиональных стандартов в области информационной безопасности.

Помимо этого ни у кого не возникает сомнений в том, что нужно обязательно внедрять в сферу подготовки ИТ в России современные образовательные технологии. Есть и такое мнение, что необходимо использовать два вида образовательных программ на каждом уровне обучения: одна — для целевой подготовки обучаемых, выпускаемых на предприятия госсектора (национальная система сертификации), другая — для обучаемых, связавших свою карьеру с коммерческими предприятиями (международная система сертификации). Также нужно выстраивать продуманную кооперацию между образованием, наукой и промышленностью, которая должна формировать заказ на подготовку кадров.

В отличие от многих других областей информационной безопасности, в сфере кибернетической безопасности АСУ ТП критически важных объектов для качественной подготовки кадров требуются большие инвестиции в создание современных учебно-лабораторных баз и испытательно-диагностических лабораторий. Такое положение дел связано с дороговизной систем АСУ зарубежного производства (Siemens, ABB, Schneider Eclectic и т. п.), а также тем фактом, что для подготовки специалистов требуется работа не только с компьютерной системой, но и со сложной иерархической системой контроллеров, причем как на уровне разработки программного кода, так и на аппаратном уровне.

То есть компетенции профессионально-кадрового состава сферы ИТ в России сконцентрированы на решении задач локализации и адаптации импортных решений, программных продуктов и электронной техники, навыках программирования и системной интеграции. Однако как подчеркивает Владимир Рубанов, сегодня общемировой вектор развития ИТ связан с умениями управления информацией, концептуального и логического моделирования и архитектурного проектирования сложных информационных систем. Ожидания от прорывов в сфере ИТ путем концентрации усилий только на индустрии программирования представляются неоправданными, так как успехи в сфере ИТ связаны со знанием предметных областей их применения, умением поставить и формализовать задачи для программирования. Это требует смещения образовательных программ от технических навыков программирования к умениям моделирования и формализации описания деятельности в предметных областях применения ИТ.

Как говорят в «Ростехе», учитывая существующие проблемы с государственным финансированием бюджетных отраслей, можно прийти к единственному оптимальному решению на данный момент, связанному с формированием контингента обучающихся на бюджетной основе исключительно на основе государственного заказа с обязательным распределением выпускников в государственные учреждения. Подготовка специалистов для негосударственных организаций должна вестись на платной основе или при наличии компенсации затрат на обучение, если выпускник, прошедший обучение на бюджетной основе, по тем или иным причинам вынужден трудоустроиться в негосударственную организацию.

«Подходы к организации научно-образовательных экосистем в случае с гражданским сектором и оборонкой

действительно разные. И там, и там огромную роль сыграют системы открытой публикации и доступа к исследованиям, но в случае с оборонкой реализация потенциала этих систем упирается в уровни доступа. Понятна потребность в закрытии информации для «внешних» специалистов не только по принципу страновой принадлежности, но и вообще за рамками ОПК или конкретных концернов. Однако сам принцип открытого информационного обмена и конкурсного трудоустройства будет в итоге реализован и там, и там. А образовательные программы должны быть привязаны, на мой взгляд, к конкретным потребностям каждого сектора индустрии», — комментирует Иван Засурский.

**ОБМЕН РАЗУМОВ** Еще одной из причин огромного дефицита качественных ИТ-специалистов на производствах является наследие системы рекрутинга специалистов, ориентированной на несколько вузов, у которых есть соответствующие базовые кафедры по подготовке специалистов. «Вы не можете попасть на работу, к примеру, в ЦАГИ, если вы не учились там, где они набирают специалистов. Поэтому набор ограничен вузами, где такая возможность есть, и теми студентами, которые, поступая в вуз, уже знали, где они хотят работать. Люди из других вузов, даже если они хотят работать, не имеют шансов устроиться в оборонно-промышленный сектор, потому что нет системы рекрутинга, который бы позволил брать специалистов, которые компаниям действительно нужны», — поясняет Иван Засурский. По мнению эксперта, необходимо выстраивать систему рекрутинга по новому, открывать входы в карьеру в ОПК и индустрию на новых уровнях. В ситуации экономического кризиса карьера в ОПК может оказаться интересным предложением для молодых людей, особенно в сочетании с программой поддержки в плане жилищно-бытовых условий. К сожалению, пока, по словам Антона Меркурова, «в короткой перспективе ИТ-образование в России — это в первую очередь билет в Европу или Силиконовую долину. В технологических вузах все еще сильное академическое образование, что до сих пор делает российских специалистов востребованными за рубежом».

Но, как говорилось выше, хорошие специалисты не всегда уезжают только из материальных соображений — большую роль играет возможность самореализации, шанс участвовать в интересном научном проекте в сотрудничестве с экспертами, у которых можно многому научиться. Сегодня одним из главных направлений совершенствования подготовки кадров, в частности, в сфере информационной безопасности является создание на базе ведущих учебных заведений современной лабораторной базы, которая позволила бы, во-первых, получить глубокие знания в данной области, а во-вторых, осуществлять качественную подготовку кадров самого различного профиля: проектировщиков, эксплуатационников и специалистов, в том числе в области кибернетической безопасности АСУ. Среди возможных путей за счет начального госфинансирования на базе ведущих вузов могут быть созданы коллективные центры прорывных решений в сфере ИТ (например, кибербезопасности), которые по материально-техническому оснащению находились бы на передовом мировом уровне и в перспективе за счет выполнения НИР и НИ-ОКР смогли бы обеспечить свое последующее финансирование и развитие.

Кроме того, необходимо шире использовать возможности сетевого обучения, отмеченные в новом законе «Об образовании», которые позволят сконцентрировать усилия профессионалов из различных областей (техническая, финансово-экономическая, лингвистическая и др.) по ряду направлений подготовки в сфере ИТ для достижения максимального эффекта по уровню знаний и умений. ■

**В СФЕРЕ КИБЕРНЕТИЧЕСКОЙ БЕЗОПАСНОСТИ АСУ ТП КРИТИЧЕСКИ ВАЖНЫХ ОБЪЕКТОВ ДЛЯ КАЧЕСТВЕННОЙ ПОДГОТОВКИ КАДРОВ ТРЕБУЮТСЯ БОЛЬШИЕ ИНВЕСТИЦИИ В СОЗДАНИЕ СОВРЕМЕННЫХ УЧЕБНО-ЛАБОРАТОРНЫХ БАЗ И ИСПЫТАТЕЛЬНО-ДИАГНОСТИЧЕСКИХ ЛАБОРАТОРИЙ**



ЧЕЛОВЕЧЕСКИЙ РЕСУРС