С.Н. Маловечко

Южно-Уральский государственный университет
Факультет «Экономика и предпринимательство»
Кафедра «Информационная безопасность»
labsec@susu.ac.ru

ФОРМИРОВАНИЕ ТЕХНИЧЕСКИХ КОМПЕТЕНЦИЙ БУДУЩИХ СПЕЦИАЛИСТОВ ПО ЗАЩИТЕ ИНФОРМАЦИИ

Широкомасштабная информатизация российского общества, совпавшая с переходом к новой общественно-экономической формации и активным вовлечением частного сектора в процессы обработки информации, обусловила разработку комплекса организационных, правовых и технологических мер защиты информации. Естественно возникла и потребность в специалистах, обладающих достаточными профессиональными знаниями для проектирования и технического сопровождения систем информационной безопасности предприятий любой формы собственности и направленности.

Более 120 вузов страны сегодня осуществляют подготовку специалистов в области защиты информации по семи направлениям:

- организация и технология защиты информации (код 090103);
- комплексная защита объектов информатизации (код 090104);
- информационная безопасность телекоммуникационных систем (код 090106);
- защищенные системы связи (код 210403);
- криптография (код 090101);
- компьютерная безопасность (код 090102);

- комплексное обеспечение информационной безопасности автоматизированных систем (код 090105).

Согласно государственным образовательным стандартам высшего профессионального образования, определяющим направления и требования к подготовке специалистов в данной области, студент должен не просто получить некоторый набор теоретических знаний и практических навыков, у него должны быть сформированы определенные *профессиональные компетенции*, соответствующие задачам и потребностям, которые ставят перед выпускниками вузов потенциальные работодатели.

Как отмечает заместитель председателя Совета УМО вузов РФ по образованию в области информационной безопасности Евгений Белов[1], именно компетентностный подход ориентирует образовательные программы на практическую подготовку, выработку у студентов умения решать реальные задачи в определенных областях деятельности. И хотя в образовательном сообществе идет дискуссия по поводу оправданности переноса акцента в обучении на потребности рынка, звучат опасения, что мы рискуем потерять один из основных козырей отечественного образования — его фундаментальность, при создании стандартов по информационной безопасности за основу взят именно компетентностный подход.

Поскольку деятельность специалистов по защите информации непосредственно связана со специальной техникой, перед ними всегда будет вставать ряд вопросов, связанных со знаниями в технической области:

- какому техническому средству отдать предпочтение?
- какими параметрами должно обладать техническое средство для защиты информации в конкретных условиях?

---

[1] Белов Е. Траектории образования в области информационной безопасности // Information Security / Информационная безопасность. 2007. № 2.

- какими техническими средствами необходимо организовать защиту информации в конкретном проекте?

Следовательно, при подготовке специалиста особое внимание необходимо уделять формированию технических компетенций.

Под *техническими компетенциями* мы будем понимать специальные (профессиональные) знания, умения и навыки, необходимые для эффективного выполнения специалистами своих должностных обязанностей.

При этом важно не столько умение демонстрировать глубокое понимание теории, сколько способность применять эти знания на практике. Естественно предположить, что чем выше техническая компетентность специалиста, тем более сложные задачи способен он решать.

Формирование технических компетенций в рамках подготовки специалиста в вузе следует начинать с первых курсов. Учитывая, что, при приеме на работу молодому специалисту, скорее всего, придется пройти оценку компетенций в рамках процедуры Assessment center, целесообразно применять что-то подобное и в вуз при оценке знаний студентов на каждом этапе его обучения.

Процедура оценки Assessment center предполагает использование различных методик, таких, как психометрические тесты, анкетирование, специальные упражнения, разного рода групповые упражнения, моделирующие ключевые моменты деятельности, и основывается на соблюдении ряда принципов:

- Оценка производится на основании системы критериев (компетенций), разрабатываемых специально для каждого Assessment center на основании анализа деятельности.

- В специально созданных ситуациях моделируются ключевые моменты деятельности, что позволяет непосредственно наблюдать и оценивать поведение, а не гипотезы о его причинах.
- Процедура предусматривает испытание различными взаимодополняющими техниками и упражнениями (в каждом упражнении оценивается несколько критериев и каждый критерий оценивается в нескольких упражнениях). Оценка производится не только специалистами, но и специально подготовленными наблюдателями — сотрудниками организации, в которой проводится оценка, что делает возможным учет таких сложно поддающихся описанию факторов, как, например, культура и философия организации.
- Каждый участник Assessment center оценивается несколькими наблюдателями и каждый наблюдатель оценивает нескольких участников, что позволяет минимизировать возможную необъективность и выставить баллы по каждому критерию каждому участнику после обсуждения и взаимного согласования данных, полученных разными методами.

Алгоритм разработки модели технических компетенций и проектирования процедуры ассессмента принципиально не отличается от общепринятого. Однако на каждом этапе разработки в нем учитывается специфика данного этапа. Наибольшее значение имеет проведение анализа деятельности, поскольку от его точности зависит все последующие результаты.

При анализе деятельности студента можно использовать совокупность таких методов, как наблюдение на рабочем месте студента (его месте в учебной лаборатории по ИБ или ИТ), анализ документов (письменные работы студента по специальности, тесты, лабораторные работы по ИБ и ИТ, подготовленные им учебные программы), иерархический анализ задач, стоящий перед студентом при изучении дисциплин (соответствие принципу «от простого к сложному» — от курса к курсу), реже анкетирование.

Задача преподавателя высшей школы при организации контроля оценить не только теоретические знания студента, но и умение их использовать; поэтому, кроме традиционных контрольных мероприятий (тестирование, контрольная работа, зачет, экзамен), логично использовать специальные упражнения, моделирующие деятельность специалиста по информационной безопасности. Так, при моделировании систем защиты информации в различных системах в качестве обязательного элемента следует предусмотреть теоретическое обоснование принятых технических решений. Таким образом, мы получаем возможность, например, с помощью тестов, письменных работ оценить усвоение теоретических знаний; с помощью специальных упражнений — умения и навыки, которые студент приобрел, а с помощью активных упражнений (дискуссии, презентации, темы которых связаны с обсуждением профессиональных вопросов в области ИБ и защиты информации) — как знания, так и умения.

Несмотря на то, что техническая компетентность является основой деятельности специалиста по защите информации, необходимо оценивать все компетенции в комплексе. Это позволит более точно прогнозировать успешность деятельности студентов как будущих специалистов. Например, если у студента достаточно низкие мыслительные способности (в терминах компетенций — «системность мышления», «гибкость мышления»), то он сможет решать только задачи определенного типа сложности. Возможно, он справится с решением типовых задач по специальности с небольшим объемом условий, действуя строго по заданному алгоритму, но для решения задач более высокого уровня сложности ему необходимо обучиться конкретным способам и навыкам. Аналитические задачи, требующие самостоятельного доопределения условий, поиска нестандартных решений, скорее всего, окажутся ему не под силу. Развивать только техническую компетенцию (то есть обучать такого студента конкретным знаниям) по данному направлению нецелесообразно, так как низкий уровень мыслительных способностей не позволит ему

реализовывать эти знания на практике. И наоборот, студент с высокими мыслительными способностями, но не обладающий необходимыми знаниями, при обучении самостоятельно приобретет нужные умения и навыки. Очевидно, что есть смысл вкладывать дополнительные средства в обучение такого студента, повышать уровень развития его технической компетенции.

В деятельности, связанной с непосредственным общением (чаще всего общение с клиентами), студент, обладающий ограниченным набором средств коммуникации, но имеющий высокие показатели по развитию технической компетенции (например, отличное знание ассортимента), будет более успешен при целенаправленном развитии его коммуникативной компетенции. В данном случае особую значимость приобретают дисциплины социально-гуманитарного цикла, но только при условии их практической направленности.

Таким образом, комплексная оценка компетенций позволяет более эффективно реализовать индивидуальный и интегративный подход при обучении студентов.

Особенность подготовки специалистов по защите информации состоит в том, что он должен сочетать в себе знания как из области естественных наук и технологий, так и из области юриспруденции, менеджмента, ряда гуманитарных наук. В ограниченные рамки учебного плана, кроме курсов по методам и средствам защиты данных, входят фундаментальные математические дисциплины, углубленная подготовка по ИТ, изучение организационных и правовых аспектов обеспечения информационной безопасности.

Высокий уровень подготовки специалиста по ИТ может быть обеспечен при выполнении как минимум четырех условий:

1) компетентности профессорско-преподавательского состава вуза;
2) теоретической разработанности и методической обеспеченности учебного процесса;

3) оптимальном соотношении учебных часов, отведенных на изучение фундаментальных дисциплин, и дисциплин, обеспечивающих формирование технических компетенций;
4) материально-техническом оснащении учебного процесса.

Решение данных проблем сегодня зависит не только от политики вуза и тех материальных вложений, которые он готов потратить на цели обучения данной специальности, но и от государственной политики в сфере образования в целом.

Реализацию двух первых условий в принципе может обеспечить вуз. А вот количество часов, отведенное на изучение той или иной дисциплины, закреплено в Государственном стандарте — документе, обязательном для исполнения всеми образовательными учреждениями.

Проанализируем распределение часов между дисциплинами на примере специальности 090103 — Организация и технология защиты информации.

Всего Государственным образовательным стандартом высшего профессионального образования по специальности 090103 предусмотрено 8260 часов теоретического обучения.

- По дисциплинам гуманитарного и социально-экономического — 1800 часов
- На общие математические и естественнонаучные дисциплин — 1400 часов.
- На общие профессиональные дисциплины (ОПД) — 3640 часов
- На дисциплины специализации — 970 часов
- другие дисциплины — 450 часов

Из них на изучение дисциплин, связанных с изучением теоретических и практических основ, направленных на формирование технических компетенций, отводится:

- на дисциплины гуманитарного и социально-экономического цикла:
  - иностранный язык — 340 часов
- на общие математические и естественнонаучные дисциплины — 1400 часов, в том числе:
  - физику — 250 часов,
  - математику — 300 часов,
  - информатику — 200 часов;
- на общие профессиональные дисциплины:
  - вычислительную технику и программирование — 220 часов,
  - инженерно-техническую защиту информации — 220 часов,
  - средства и системы технического обеспечения обработки, хранения и передачи информации — 200 часов
  - криптографическая защита информации — 120 часов
  - программно-аппаратная защита информации — 120 часов
  - защита информационных процессов в компьютерных системах — 90 часов
  - комплексная система защиты информации на предприятии — 220 часов.

Если рассматривать распределение часов на изучение дисциплин с точки зрения формирования компетенций специалиста (т.е. получения знаний, непосредственно используемых в профессиональной деятельности), то получится следующая картина:

- по дисциплинам гуманитарного и социально-экономического — из 1800 часов — 340 часов, то есть 18 %
- на общие математические и естественнонаучные дисциплины — из 1400 часов — 750 часов, то есть 53 %.
- на общие профессиональные дисциплины (ОПД) — из 3640 часов — 1090 часов, то есть 30%

Таким образом, технические и сопутствующие дисциплины занимают не более 27% от общего учебного времени. Здесь также необходимо учитывать, что отведенные Госстандартом на изучение конкретной дисциплины часы, в свою очередь, разбиваются на часы, отведенные на изучение теоретических вопросов, практические и лабораторные занятия и самостоятельную работу. При тех высоких требованиях, которые работодатель сегодня предъявляет к нанимаемым специалистам (он хочет иметь работника, способного без усилий разбираться в самой новой технике или технологии именно с технической, инженерной точки зрения) этого явно недостаточно.

На наш взгляд, необходимо не только существенно повысить количество часов, отводимых на дисциплины, связанные с технологическими процессами в защищаемых системах, но и пересмотреть саму схему изучения дисциплин.

Применяемый сегодня метод от теории к практике не всегда оправдывает себя. Современное школьное образование позволяет уже школьникам понять, хотя и в общих чертах, назначение элементов и принципы работы технических средств и методов, применяемых для решения поставленных задач. Обучаясь в вузе, студенты порой довольно успешно демонстрируют теоретические познания, но при этом не способны обосновать принятые ими же правильные решения. В этой связи представляется целесообразным начинать изучение дисциплин с конкретных технических и программных продуктов на практике, а теоретическую основу под принципы и алгоритмы действия приборов и программ давать, увязывая их с решением конкретной практической задачи. Это дает возможность исключить большой отрыв теоретических знаний от практического их применения.

Дополнительные трудности при подготовке специалистов по защите информации возникают и из-за жесткости существующих требований к материально-техническому обеспечению учебного процесса.

По мере развития и усложнения средств и методов обработки, хранения и передачи информации по каналам связи повышается потенциальная угроза

потери ее конфиденциальности. В связи с этим (несмотря на изменение международной обстановки) деятельность технических разведок иностранных государств по добыче информации не сокращается, что требует мер по повышению эффективности ее защиты. Следовательно, специалист в области защиты информации должен уметь обеспечивать:

- контроль над доступом к информационным системам и базам данных;
- защиту технических средств от утечки информации по побочным каналам и от возможного внедрения в них электронных устройств съема информации;
- защиту программных продуктов средств вычислительной техники информационных систем от внедрения программных «вирусов» и закладок;
- контроль настроек защиты операционных систем на рабочих станциях и серверах;
- оценку возможности проведения нарушителями атак на сетевое оборудование;
- сканирование сети с целью исследования ее топологии.

Для формирования перечисленных умений необходимо, чтобы практические и лабораторные занятия проводились в специально оборудованных помещениях, с применением современной вычислительной техники. Для обеспечения занятий по циклу дисциплин специализации нужны специальные технические средства (закладные устройства, сканирующие радиоприемники, приборы ночного видения, портативные металлодетекторы и т.д.), приобретение которых для большинства вузов просто не представляется возможным. Значительных затрат требует лицензионное программное обеспечение, расходные материалы, доступ в Интернет.

Многие вузы решают эту проблему путем интеграции с промышленными предприятиями, которые, с одной стороны, берут на себя материально-техническое снабжение вузов, а с другой, удовлетворяют собственные

потребности в молодых специалистах. С этой точки зрения заслуживает внимания опыт работы учебного центра «Информзащита»[2], в циклы курсов которого включено обучение практическим вопросам знакомства с отечественными разработками *(система «Гриф», «Кондор», электронный замок «Соболь» и др.).*

Таким образом, учитывая потребность страны в грамотных специалистах по защите информации, необходимо уже сегодня предпринять ряд государственных мер по финансированию образовательных программ, связанных с подготовкой кадров в области информационной безопасности. Эти меры должны предусматривать как постоянное повышение квалификации профессорско-преподавательского состава, так и материально-техническое оснащение учебного процесса. Относительная «молодость самой специальности» в России и, следовательно, сравнительно небольшой отечественный опыт подготовки специалистов по ИБ требуют более пристального внимания со стороны ученых в области педагогики, и, что не мене важно, оперативного внесения корректив в систему подготовки специалистов, начиная от Государственного стандарта и заканчивая непосредственной организацией учебного процесса в вузе.

[2] Учебный центр «Информзащита» — ведущий специализированный центр в области обучения информационной безопасности (лицензия Департамента образования Москвы № 017837, государственная аккредитация № 002687). Единственный авторизованный учебный центр компаний Internet Security Systems и Clearswift на территории России и стран СНГ. Авторизованный учебный центр компании Microsoft (специализация Security). Центром разработан широкий спектр учебных программ, в которых использован многолетний опыт профессиональной работы в области защиты информации, специальные методики интенсивного обучения. Программы обучения согласованы с государственными уполномоченными органами по защите информации (ФСТЭК России (Гостехкомиссия России), ФСБ России (ФАПСИ)). В центре проходят обучение и повышают квалификацию более чем по 60 тренинговым и комплексным курсам специалисты, ответственные за информационную безопасность организаций: руководители подразделений технической защиты информации, аналитики по компьютерной безопасности, системные и сетевые администраторы, администраторы безопасности и др. http://www.itsecurity.ru, http://www.kaspersky.ru/news?id=181889561