

УДК 378.1

В.В. Поляков, Н.Н. Минакова

Россия, Барнаул, Алтайский государственный университет

ОСОБЕННОСТИ ПОДГОТОВКИ СПЕЦИАЛИСТОВ ПО ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В УСЛОВИЯХ ДИНАМИЧНО РАЗВИВАЮЩЕГОСЯ РЫНКА ТРУДА

В работе рассматривается модель образовательного процесса при подготовке специалистов по информационной безопасности, позволяющая выпускать востребованных для современного рынка труда специалистов. Показаны технологии обучения, позволяющие готовить конкурентоспособных специалистов. Подчеркивается недостаточность формирования умений и навыков только в технической (программной, программно-аппаратной) сфере деятельности.

Сделан вывод о том, что разработанная система обучения позволяет сформировать организационно-управленческие навыки и компетенции, необходимые для решения задач профессиональной сферы.

Ключевые слова: активное обучение; интерактивное обучение; деловые игры; творческое мышление; инновационный подход в образовании.

Российская Федерация идет по инновационному пути развития экономики. Организация инновационного бизнеса требует кооперации, устойчивых партнерских связей, работы с широким спектром предполагаемых инвесторов. Поэтому одной из составных частей инновационного развития является непрерывное усложнение информационных технологий, увеличение числа объектов информатизации. В этих условиях информация, становясь стратегическим ресурсом, выходит за пределы информационной системы коммерческой организации. Происходит ее интеграция в глобальные, национальные, транснациональные информационные системы. Поэтому информационный ресурс нуждается в постоянной защите.

В сложившейся ситуации необходимо готовить компетентного, конкурентоспособного специалиста по информационной безопасности, способного использовать полученные знания при решении профессиональных задач. Главные вопросы, которые возникают – чему и как учить? (рис.1).



Рис. 1 Компоненты технологии подготовки специалистов по информационной безопасности

Профессиональная деятельность специалистов по информационной безопасности может быть реализована во многих сферах: проектная, технологическая, эксплуатационная, исследовательская, организационная, управленческая [1]. В Алтайском государственном университете подготовка ведется с учетом динамично развивающегося рынка труда. Формирование технических (технологических) компетенций реализуется в рамках следующих основных разделов:

- Научно-технологическая основа решений по защите информации (физические методы защиты, криптография, многомерный анализ данных...).
- Технические и программные средства защиты информации.
- Компьютерные сети и сетевые технологии (сетевое администрирование).

В разделе по компьютерным сетям и сетевым технологиям рассматривается важнейший на сегодняшний день блок вопросов. Как известно, особую угрозу в современных условиях представляет лавинообразное развитие телекоммуникационных технологий, не связанных с проводными способами передачи информации.

Накапливаемый опыт защиты информации все больше подтверждает, что использование различных технологических решений на программном и аппаратном уровнях позволяет обеспечить защиту далеко не в полной мере. Определяющим образом влияет человеческий фактор. Значительный объем средств и методов защиты информации ориентирован на участие в этом персонала организации. Зачастую основную опасность для организации представляют случайные или преднамеренные действия персонала.

При подготовке специалистов в Алтайском государственном университете учитывается, что в будущем это могут быть как руководители, так и рядовые сотрудники, ответственные за деятельность по защите информации в коммерческой организации. Эффективность реализации процесса защиты информации требует повышения осведомленности каждого сотрудника организации в вопросах информационной безопасности. Специалист по информационной безопасности должен научить сотрудников организации правильному использованию имеющихся средств защиты, ответственности за утечку информации, основам обеспечения информационной безопасности при работе с интернет-ресурсами, особенностям использования антивирусных комплексов и т.д.

Будущему специалисту по информационной безопасности требуется большое количество умений и навыков, напрямую не связанных с технологической компонентой. К ним, на наш взгляд, в первую очередь относятся следующие

- организация работы коллектива исполнителей;
- разработка исполнительских решений в условиях спектра мнений;
- умение реализовать организационно-управленческую сторону, в том числе определение порядка выполнения работ.

Поэтому при подготовке специалистов по информационной безопасности широко используются активные и интерактивные методы обучения. Такая тенденция совершенствования образовательного процесса в высшей школе известна [2,3]. Важнейшей задачей является подборка вариантов практической реализации методов обучения.

При подготовке специалистов по информационной безопасности в Алтайском государственном университете активное обучение направлено не

только на знакомство и детальное рассмотрение технической стороны защиты информации, но и на изучение, например, системы оценивания при выработке и принятии управленческих решений по профилю специальности. Студенты знакомятся с широким спектром методов:

- методами анализа (метод сравнения, графический метод, метод цепных подстановок);
- методами моделирования (физического, математического, логического);
- методами прогнозирования (экспертные, параметрические, функциональные и т.д.) [4, 5].

Традиционно используются активные и интерактивные формы проведения занятий: разбор конкретных ситуаций, тренинги, мозговой штурм (атака), моделирование жизненных ситуаций, творческие задания и т.д. Формы проведения занятий постоянно совершенствуются: например, решение ситуационных задач – интервью, инсценировка, проигрывание ситуаций.

При изучении многих курсов используется решение оптимизационных задачи, например, по выбору средств защиты, приоритетных процессов управления информационной безопасностью и т.д. Используются групповые упражнения, моделирующие ключевые моменты деятельности, совместное решение проблем.

Изучается возможность многофункциональных решений, например, при рассмотрении вопросов конструирования комнаты для переговоров указывается на возможность применения материалов, которые наряду со звукопоглощающими свойствами могут иметь другие функциональные свойства (нагревательные, антистатические и т.п.) [6]. Хорошо зарекомендовали себя взаимодополняющие техники и упражнения (в каждом упражнении оценивается несколько критериев и каждый критерий оценивается в нескольких упражнениях) [3].

Среди известных технологий интерактивного обучения эффективными оказались профессиональные образовательные игры: имитационная, ролевая, деловая, комплексная и т. д. [1, 7]. Имитационная игра позволяет моделировать среду, определяющую поведение людей и механизмы их действий в различных ситуациях, в том числе экстремальных (рис. 2). Ролевая игра дает возможность проигрывания ролей (инсценировки). Деловая игра учит взаимодействию в процессе достижения целей, имитирующих решение комплексных задач в конкретной ситуации [3, 7].



Рис. 2. Использование технологии профессиональных игр при подготовке специалистов по информационной безопасности

Студенты учатся понимать самые, на первый взгляд, неочевидные взаимосвязи. Например, при изучении вопросов защиты периметра в качестве

одной из уязвимостей рассматривается нецелевой подбор компонентов (например, подбор материалов для датчиков давления) [8].

Применяются и нестандартные для подготовки специалистов по информационной безопасности приемы. К ним можно отнести обсуждение сюжетных рисунков (в курсе «Основы информационной безопасности»); действие по инструкции (в курсе «Управление информационной безопасностью») и др.

Описанные подходы позволяют совершенствовать систему подготовки для работы в условиях динамично меняющихся обстоятельств. Как известно, многие вопросы информационной безопасности (модель угроз, модель нарушителя и т.д.) носят прогностический характер [5]. Поэтому будущему специалисту крайне важно уметь адекватно реагировать на появляющиеся изменения.

Студент получает не только знания, умения и навыки в сфере своей будущей профессиональной деятельности, но и возможность развития кругозора. Повышается его инициативность, вырабатываются навыки работы в коллективе. В таком процессе обучения уровень профессиональной компетентности студентов постоянно эволюционирует.

Опыт работы показал, что разработанная и динамично изменяющаяся модель подготовки специалистов по информационной безопасности обеспечивает выпускникам множество мест работы: государственные и муниципальные органы, правоохранительные органы, коммерческие организации широкого профиля, в том числе и специализируемые. Современный выпускник умеет:

- формировать собственное мнение;
- совершать обдуманный выбор;
- аргументировано спорить;
- оценить чужую точку зрения и сознавать, что восприятие человека и его отношение к любому вопросу формируется под влиянием многих факторов.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Белов Е.Б., Лось В.П., Проскурин В.Г., Черемушкин А.В. О проекте образовательного стандарта «Специалист по безопасности компьютерных систем и сетей.// Информационное противодействие угрозам терроризма, 2015. Т. 3. № 25. С. 18-21.
2. Современные образовательные технологии /под ред. Бордовской В.В. и др. – М.: КНОРУС, 2010. – 432 с.
3. Жукова Г.С., Никитина Н.И., Комарова Е.В. Технологии профессионально-ориентированного обучения: учеб. пособие. – М.: Издательство РГСУ, 2012. – 165 с.
4. Минакова Н.Н. Расчетные модели прогноза свойств и анализа проводимости структурнонеоднородных композиционных материалов /Электротехника. 2000. №9. С.26-30.
5. Минакова Н.Н., Поляков В.В., Толстошеев С.Н. Методы технической и правовой защиты информации в сети Интернет. – Барнаул: изд-во Алт. ун-та, 2015. – 155 с.
6. Минакова Н.Н. Работа резистивных полимерных многокомпонентных материалов в электроустановках. – Барнаул, 1997.
7. Гуляев В.Н., Логинов И.П., Неволлина Н.А.: Технология профессионально ориентированного обучения в высшей школе (научные и прикладные основы). – М.: АТиСО, 2008.- 187 с.
8. Горелов В.П., Минакова Н.Н., Грунин В.К. Применение электропроводящего технического углерода для резисторов энергетического назначения //Получение и свойства электропроводящего технического углерода: Сб. научных трудов ВНИИТУ /ЦНИИТЭнефтехим. – М., 2008, С. 113-119.