

ФОРМИРОВАНИЕ СТРУКТУРЫ ПОДГОТОВКИ СПЕЦИАЛИСТА ПО ПРИКЛАДНОЙ ИНФОРМАТИКЕ В ОБЛАСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

И.В. Белова

Россия, г. Москва

Исторически информация всегда имела большое значение в жизни людей, а в современном мире информация не просто представляет собой ценность, но и является движущим фактором развития общества. Информационные процессы играют все более важную роль в основных областях общественной деятельности. Это повлияло на то, что информационная безопасность (ИБ) стала одной из главных проблем, с которой в настоящее время сталкивается общество.

Словосочетание ИБ в разных контекстах может иметь различный смысл. В Доктрине информационной безопасности Российской Федерации термин ИБ используется в широком смысле. Имеется в виду состояние защищенности национальных интересов в информационной сфере, определяемых совокупностью сбалансированных интересов личности, общества и государства [3]. В государственном стандарте РФ содержится следующее определение ИБ: «все аспекты, связанные с определением, достижением и поддержанием конфиденциальности, целостности, доступности, неотказуемости, подотчетности, аутентичности и достоверности информации или средств ее обработки» [6]. ИБ с точки зрения информационных технологий – это состояние, обеспечивающее защищенность информации (данных) и ИБ автоматизированной информационной системы, применяющейся для обработки и передачи данных на локальном и сетевом уровнях [7]. Практически во всей иностранной и учебной литературе понятие ИБ используется в узком смысле. Под ним понимается защищенность информации и поддерживающей инфраструктуры от случайных или преднамеренных воздействий естественного или искусственного характера, которые могут нанести неприемлемый ущерб

субъектам информационных отношений, в том числе владельцам и пользователям информации и поддерживающей инфраструктуры. Под поддерживающей инфраструктурой в данном определении понимаются, например системы электро-, водо- и теплоснабжения, кондиционеры, средства коммуникаций и обслуживающий персонал [3]. ИБ может быть достигнута только за счет осуществления безопасной информационной деятельности на трех уровнях: личность, общество, государство.

Зачастую понятие ИБ подменяется словосочетанием «компьютерная безопасность», которая является всего лишь одной из составляющих ИБ, что отмечено, например, в работах П. Н. Башлы, А. В. Бабаха, Е. К. Барановой [1] и Н. В. Мельникова, И. В. Беловой [5]; в сфере образования.

Рассмотрим уровень среднего профессионального образования на примере специальности 230701 – Прикладная информатика (по отраслям) (до 2011 г. – 080802 Прикладная информатика (по отраслям)). Согласно государственному стандарту, перечень дидактических единиц дисциплины «Информационная безопасность» выглядит следующим образом: «основные понятия и определения, эволюция подходов к обеспечению информационной безопасности; информационные, программно-математические, физические и организационные угрозы; защита от несанкционированного доступа, модели и основные принципы защиты информации; проблема вирусного заражения программ, структура современных вирусных программ, основные классы антивирусных программ, перспективные методы антивирусной защиты; защита от утечки информации по техническим каналам; организационно-правовое обеспечение ИБ».

Рабочая программа строится на основе примерной программы учебной дисциплины «Информационная безопасность» для специальности 2203 – Программное обеспечение вычислительной техники и автоматизированных систем, в которой приведен следующий примерный тематический план:

Раздел 1. Борьба с угрозами несанкционированного доступа к информации.

Тема 1.1. Актуальность проблемы обеспечения информационной безопасности.

Тема 1.2. Виды мер обеспечения информационной безопасности.

Тема 1.3. Основные принципы построения систем защиты информации.

Раздел 2. Борьба с вирусным заражением информации.

Тема 2.1. Проблема вирусного заражения и структура современных вирусов.

Тема 2.2. Классификация антивирусных программ.

Раздел 3. Организационно-правовое обеспечение информационной безопасности.

Тема 3.1. Международные, российские и отраслевые правовые документы.

Как следует из вышесказанного, в образовательном стандарте и учебной программе основное внимание уделено компьютерной безопасности. Однако компьютер – лишь часть информационной системы, причем не самая уязвимая. В большинстве случаев наиболее уязвимым звеном является человек [5]. Кроме того, в современном обществе информационная сфера имеет две составляющие: информационно-техническую (искусственно созданный человеком мир техники, технологий и т.п.) и информационно-психологическую (естественный мир живой природы, включающий и самого человека). Соответственно, в общем случае информационную безопасность необходимо представлять двумя составными частями: информационно-технической безопасностью и информационно-психологической (психофизической) безопасностью [4].

Еще одной проблемой существующей системы образования в области защиты информации является то, что она ориентирована в основном на подготовку специалистов, чья профессиональная деятельность будет напрямую связана с защитой информации. Для других специальностей, выпускникам которых предстоит использовать как в своей работе, так и в повседневной жизни информационные и коммуникационные технологии, система профессионального обучения ИБ только складывается, как было показано выше, на основе лишь одной из составляющих – компьютерной безопасности. Это сильно усложняет задачу формирования профессиональной компетентности специалистов в области информационных технологий, поскольку ее формирование невозможно без компетентности в области ИБ.

В связи с вышеперечисленным необходимо введение соответствующего требованиям современного информационного общества курса дисциплины «Информационная безопасность». Это поможет решить следующие вопросы:

- повысить конкурентоспособность выпускников на рынке труда;
- снизить возможности реализации угроз информационной безопасности;
- уменьшить информационную зависимость личности за счет формирования навыка фильтрации информации и др.

Например, для специальности 230701 – Прикладная информатика (по отраслям) автор в данном курсе предлагает уделить внимание не только компьютерной безопасности и антивирусной защите информации, но и следующим вопросам:

- нормативно-правовые основы обеспечения ИБ; основополагающие нормативные документы российского и зарубежного законодательства; ответственность за нарушения в области защиты информации;
- защита информации и интеллектуальная собственность;
- организационно-распорядительная защита информации в контексте отдельно взятой организации и государства;
- локальные сетевые угрозы, осуществляемые в пределах одного узла; удаленные сетевые угрозы, обусловленные распределенностью сетевых и информационных ресурсов в пространстве;
- защита человека от информации, дезинформации и неинформированности и др.

На первый план в данном курсе предлагается поставить практические занятия с целью наглядного ознакомления выпускников с существующими угрозами и путями их решения, а также с моделирования реальных ситуаций и вариантов поведения в зависимости от существующих окружающих факторов. Такая направленность учебного курса позволит подготовить будущих специалистов к работе в реальных условиях, к их вхождению в производственный процесс.

В рамках организации учебного процесса и обучения студентов именно тем аспектам ИБ, которые характерны для выбранной ими профессиональной

отрасли, предлагается разбить предлагаемый курс на инвариантный и вариативный блоки, которые могут включать следующие модули:

Модули инвариантного блока:

- понятие информационной безопасности, ее основные составляющие (определение информационной безопасности, характеристика основных ее составляющих);
- классификация угроз ИБ (определение угрозы, понятия злоумышленник, атака, уязвимость, окно опасности и др.; различные классификации угроз);
- характеристика уровней защиты информации (краткая характеристика основных уровней формирования информационной безопасности: программно-технический, нормативно-правовой, организационно-распорядительный; защита человека от информации, дезинформации и неинформированности (психологический уровень обеспечения ИБ)).

Модули вариативного блока:

- нормативно-правовой уровень ИБ (основные законы Российской Федерации и других стран в области информационной безопасности; стандарты ИБ);
- организационно-распорядительный уровень ИБ (правила построения организационно-распорядительной защиты на предприятии; информационная безопасность государства);
- психологический уровень ИБ (защита человека от информации, дезинформации, неинформированности);
- программно-технический уровень защиты информации.

В связи с тем, что программно-технический уровень защиты информации в настоящее время достаточно обширен, этот модуль можно разбить на отдельные составляющие, например:

- физическая защита информации;
- антивирусная защита информации;
- криптографические и стеганографические методы защиты информации;
- защита информации в компьютерных сетях.

Выбор определенных модулей может зависеть как от интересов студентов и преподавателя, так и от выбранной студентами специальности. Например, для

студентов специальности «Прикладная информатика в менеджменте» рекомендован модуль, посвященный организационно-распорядительному уровню, «Прикладная информатика в психологии» – психологическому уровню организации информационной безопасности.

Предлагаемый автором курс учебной дисциплины «Информационная безопасность» построен на основе современного уровня развития ИБ и требований развивающегося информационного общества. Он направлен на решение вопросов, связанных с повышением компетентности специалистов, обеспечения их трудоустройства. Помимо вышесказанного, данный курс строился в соответствии с требованиями ФГОС СПО третьего поколения и будет полезен для полноценного овладения специалистами по прикладной информатике перечисленными в государственном стандарте профессиональными компетенциями.

Литература

1. Башлы П. Н., Бабаш А. В., Баранова Е. К. Информационная безопасность: Учеб.-практ. пособие. М.: Изд. Центр ЕАОИ, 2010.
2. Галатенко В. А. Основы информационной безопасности. М.: Интернет-университет информационных технологий – ИНТУИТ.РУ, 2003.
3. Доктрина информационной безопасности Российской Федерации. М.: 2000.
4. Информационная безопасность (2-я книга социально-политического проекта «Актуальные проблемы безопасности социума»). М.: Оружие и технологии, 2009.
5. Мельников Н. В., Белова И. В. Информационная безопасность и защита информации: основные понятия и нормативные документы: Учеб.-метод. пособие. М.: РГСУ, 2011.
6. Национальный стандарт РФ «Методы и средства обеспечения безопасности. Часть 1. Концепция и модели менеджмента безопасности информационных и телекоммуникационных технологий» (ГОСТ Р ИСО/МЭК 13335-1 – 2006), 2006.
7. Примерная программа учебной дисциплины «Информационная безопасность». М.: Издательский отдел ИПР СПО, 2002.