А. И. Толстой (к. т. н., доцент)
Московский инженерно-физический институт (государственный университет)

ОСНОВЫ ФОРМИРОВАНИЯ ПРОФЕССИОНАЛЬНЫХ КОМПЕТЕНЦИЙ ВЫПУСКНИКОВ УЧЕБНЫХ ЗАВЕДЕНИЙ ПО НАПРАВЛЕНИЯМ И СПЕЦИАЛЬНОСТЯМ ПОДГОТОВКИ, ВХОДЯЩИМ В УКРУПНЕННОЕ НАПРАВЛЕНИЕ 090000 – ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

Введение

Разработка Федеральных государственных образовательных стандартов (ФГОС) третьего поколения основывается на компетентностном подходе, который предполагает наличие в таких стандартах формулировок, отражающих способности выпускников высшего учебного заведения применять знания, умения и личностные качества для успешной деятельности в определенной области. Особенности направления подготовки специалистов с высшим и средним профессиональным образованием отражаются в профессиональных компетенциях. Для их формирования, прежде всего, необходимо рассмотреть основные характеристики образовательной области, соответствующей конкретному направлению подготовки, определить структуру предметной области, связанной с определенной образовательной областью, и определить исходные данные, необходимые для формулирования профессиональных компетенций. Данная работа посвящена решению выделенных выше задач для формирования профессиональных компетенций выпускников учебных заведений по направлениям и специальностям подготовки, входящими в укрупненное направление 090000 – Информационная безопасность.

1. Особенности образовательной области «Информационная безопасность»

В настоящее время в Общероссийском классификаторе специальностей по образованию (ОКСО) образовательной области «Информационная безопасность» соответствует укрупненная группа специальностей и направлений подготовки 090000 – Информационная безопасность, в которую входят семь специальностей высшего профессионального образования – ВПО (090101 – 090107) и одна специальность среднего профессионального образования – СПО (090108). При формировании нового перечня планируется включение в укрупненную группу направления подготовки 090100 – Информационная безопасность с квалификациями бакалавр и магистр информационной безопасности, а также двух новых специальностей СПО (090109, 090110).

Существующие в настоящее время ФГОС второго поколения по специальностям, входящим в укрупненную группу 090000 – Информационная безопасность, а также разработанные основные образовательные программы по данным специальностям составляют учебно-методическую основу государственной системы подготовки кадров в области обеспечения информационной безопасности (ИБ).

В решении секции по информационной безопасности совета при Совете Безопасности Российской Федерации (от 29 января 2008 г.) определены принципы формирования нового Перечня направлений подготовки в образовательной области «Информационная безопасность», которые необходимо учесть при формулировании профессиональных компетенций. К ним относятся:

1. Для направлений подготовки:

· полный охват направлениями подготовки предметной области «Информационная безопасность»;

· объединение направлений, имеющих общую фундаментальную подготовку, с возможностью дальнейшей их профилизации;

· объединение направлений, общую прикладную (отраслевую) ориентацию подготовки;

2. Для специальностей:

· направление содержания подготовки на реализацию государственных подходов к обеспечению безопасности личности, общества, государства;

· учет требований основных потребителей (заказчиков) к квалификации выпускника;

· учет особенностей, связанных с междисциплинарным характером профессиональной области данной группы и каждой специальности в отдельности.

Анализ выше перечисленных принципов позволяет выделить следующие ключевые моменты, влияющие на формулирование профессиональных компетенций: структура предметной области «Информационная безопасность», прикладной характер направлений подготовки, учет требований потребителей и междисциплинарный характер профессиональной области.

2. Структура предметной области «Информационная безопасность»

Для определения структуры предметной области «Информационная безопасность» проанализируем сначала термин, определяющий ее название. В таблице 1 приведены некоторые определения термина «информационная безопасность» с указанием соответствующих информационных источников. Анализ приведенных определений термина «информационная безопасность» позволяет сделать следующие выводы:

· отсутствует единственное общепринятое определение;

· наиболее предпочтительным является связывать информационную безопасность с состоянием защищенности определенного объекта;

· состояние защищенности объекта непосредственно связано с обеспечением неизменности таких свойств информации, как конфиденциальность, целостность и доступность (в последнее время добавляют неотказуемость, подотчетность, аутентичность и достоверность).

· обилие существующих объектов, состояние которых может определять информационная безопасность, приводит к разнообразию определений термина «информационная безопасность».

· структура предметной области «Информационная безопасность» будет определяться структурой объектов, состояние защищенности которых определяет информационная безопасность

В качестве примера индивидуального подхода к определению термина «информационная безопасность» можно привести формулировку этого термина в стандарте Банка России СТО БР ИББС-1.0 [10] (Табл. 1).

Таблица 1.

Определение	**Источник**
Под информационной безопасностью Российской Федерации понимается состояние защищенности ее национальных интересов в информационной сфере, определяющихся совокупностью сбалансированных интересов личности, общества и государства.	[1]
Информационная безопасность – состояние защищенности информационной среды общества, обеспечивающее ее формирование, использование и развитие в интересах граждан, организаций, государства.	[2]
Информационная безопасность: защита конфиденциальности, целостности и доступности информации. Информационная безопасность — механизм защиты, обеспечивающий: - конфиденциальность: доступ к информации только авторизованных пользователей; - целостность: достоверность и полноту информации и методов ее обработки; - доступность: доступ к информации и связанным с ней активам авторизованных пользователей по мере необходимости.	[3]
Информационная безопасность: свойство информации сохранять конфиденциальность, целостность и доступность. Кроме того, данное понятие может включать в себя также свойство сохранять аутентичность, подотчетность, неотказуемость и надежность.	[4]
Информационная безопасность: все аспекты, связанные с определением, достижением и поддержанием конфиденциальности, целостности, доступности, неотказуемости, подотчетности, аутентичности и достоверности информации или средств ее обработки.	[5]
Под информационной безопасностью понимается защищенность информации и поддерживающей инфраструктуры от случайных или преднамеренных воздействий	[6]

естественного или искусственного характера, чреватых нанесением ущерба владельцам или пользователям информации и поддерживающей инфраструктуры.	
Безопасность информации (Information security) – состояние защищенности информации, обрабатываемой средствами вычислительной техники или автоматизированной системы, от внутренних или внешних угроз.	[7]
Безопасность информации [данных]: состояние защищенности информации [данных], при котором обеспечиваются ее [их] конфиденциальность, доступность и целостность (information [data] security). Безопасность информации (при применении информационных технологий): состояние защищенности информационной технологии, обеспечивающее безопасность информации, для обработки которой она применяется, и информационную безопасность автоматизированной информационной системы, в которой она реализована. IT security.	[8]
Безопасность информации (данных): состояние защищенности информации (данных), при котором обеспечиваются ее (их) конфиденциальность, доступность и целостность.	[9]
Информационная безопасность организации банковской системы Российской Федерации – состояние защищенности интересов (целей) организации банковской системы Российской Федерации в условиях угроз в информационной сфере.	[10]

Основываясь на сделанных выводах, можно предложить формулировку определения термина «информационная безопасность», относящуюся к рассматриваемой предметной области:

Информационная безопасность объекта — это состояние его защищенности в условиях угроз в информационной сфере.

При этом защищенность достигается обеспечением совокупности свойств информационной безопасности — конфиденциальностью, целостностью, доступностью информационных активов и поддерживающей их инфраструктуры.

В данном определении под информационной сферой будем понимать «…совокупность информации, информационной инфраструктуры, субъектов, осуществляющих сбор, формирование, распространение и использование информации, а также системы регулирования возникающих при этом общественных отношений» [1].

Активы («все, что имеет ценность для организации» [3]), в общем случае, включают в себя «(но не ограничиваются): материальные активы (например, вычислительные средства, средства связи, здания); информацию (данные) (например, документы, базы данных); программное обеспечение; способность производить продукт или предоставлять услугу; людей; нематериальные ресурсы (например, престиж фирмы, репутацию)» [3].

Исходя из этого можно рекомендовать для рассматриваемой области использование термина «информационные активы», приведенный в [10]: «информационные активы» обозначает различного вида информацию, которой обладает объект, на следующих фазах жизненного цикла: генерация (создание), обработка, хранение, передача, уничтожение.

Сформулированное выше определение термина «информационная безопасность» можно учесть при определении обобщенной структуры предметной области «Информационная безопасность» (Рис. 1).

Такое представление обосновывает классификацию объектов предметной области «Информационная безопасность. В данном случае объектами рассматриваемой предметной области являются:

· системы, функционирующие в условиях существования угроз в информационной сфере и обладающие активами, подлежащими защиты;

· объекты как часть системы, функционирующие в условиях существования угроз в информационной сфере и обладающие активами, подлежащими защиты;

· компоненты объектов, входящих в систему, функционирующие в условиях существования угроз в информационной сфере и обладающие активами, подлежащими защиты;

· информационные технологии, формирующие информационную инфраструктуру, функционирующие на объектах различного уровня (система, объект системы, компонент объекта) в условиях существования угроз в информационной сфере и взаимодействующие с активами, подлежащими защиты;

· технологии обеспечения информационной безопасности объектов различного уровня (система, объект системы, компонент объекта), которые связаны с информационными технологиями, используемыми на этих объектах (технологии обеспечения информационной безопасности могут быть встроены в информационные технологии;

· системы менеджмента информационной безопасности (СМИБ) объектов различного уровня (может быть встроена в систему менеджмента этих объектов).

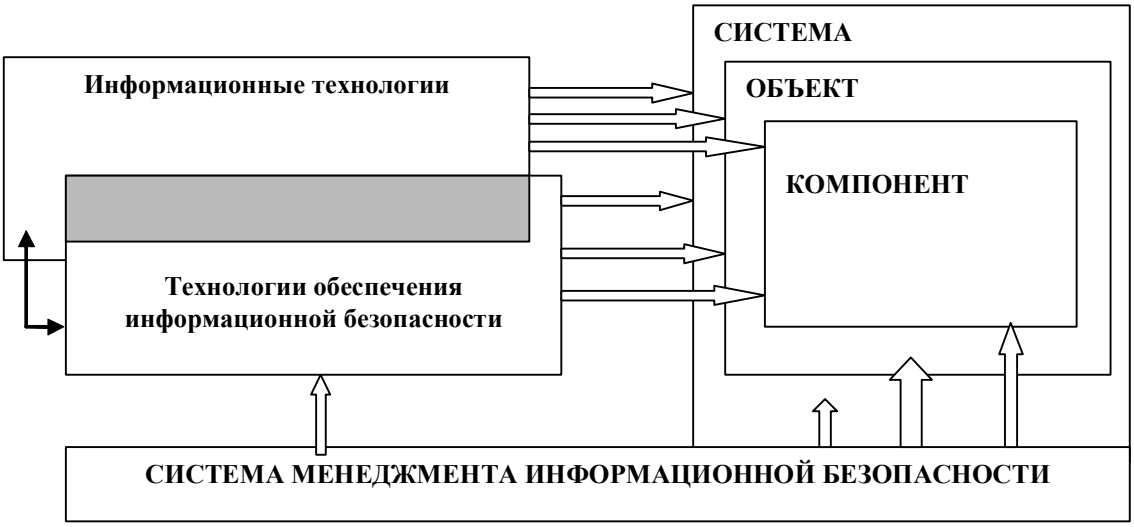

Рис. 1. Структура предметной области «Информационная безопасность»

3. Исходные данные для формулирования профессиональных компетенций

Рассмотрев особенности образовательной области и структуру предметной области «Информационная безопасность», можно определить исходные данные для формулирования профессиональных компетенций выпускников вузов по направлениям и специальностям, входящим в укрупненное направление 090000 – Информационная безопасность.

К ним относятся определение области, объектов и видов профессиональной деятельности выпускников, а также задач профессиональной деятельности специалиста на объекте профессиональной деятельности, определенных по видам профессиональной деятельности.

Область профессиональной деятельности выпускников по направлению подготовки 090000 – Информационная безопасность включает: области науки, техники и технологии, охватывающие совокупность проблем, связанных с обеспечением состояния защищенности различных объектов в условиях существования угроз в информационной сфере (учитывает определение термина «информационная безопасность»).

Приведенная выше классификация объектов предметной области «Информационная безопасность» позволяет построить модель *объектов профессиональной деятельности* выпускников высшего и среднего профессионального образования по укрупненному направлению подготовки 090000 – Информационная безопасность. Составляющими этой модели являются: системы (С), объекты как часть системы (ОС) и компоненты объектов (КОС), входящих в систему, функционирующие в условиях существования угроз в информационной сфере и обладающие активами, подлежащими защиты, а также информационные технологии (ИТ), технологии обеспечения информационной безопасности (ТОИБ) и СМИБ объектов различного уровня.

Если предположить, что приведенный выше перечень объектов профессиональной деятельности выпускников по укрупненному направлению подготовки 0900000 – Информационная безопасность

обладает полнотой, то представляется целесообразным попытаться связать эти объекты с существующими направлениями (специальностями) подготовки специалистов в области ИБ. В табл. 2 представлена информация, поясняющая привязку направлений подготовки (бакалавр, магистр) и специальностей ВПО и подготовки техников по защите информации СПО с объектами профессиональной деятельности.

Таблица 2.

№	Направление/ специальность, квалификация	СМИБ	ТОИБ	ИТ	КОС	ОС	С
090100	Информационная безопасность, бакалавр информационной безопасности	**x**	**x**	**x**	**x**	**x**	**x**
090100	Информационная безопасность, магистр информационной безопасности	**x**	**x**	**x**	**x**	**x**	**x**
090101	Криптография, математик	**x**	**x**				
090102	Компьютерная безопасность, математик	**x**	**x**	**x**			
090103	Организация и технология защиты информации, специалист по защите информации	**x**	**x**				**x**
090104	Комплексная защита объектов информатизации, специалист по защите информации	**x**	**x**	**x**			**x**
090105	Комплексное обеспечение информационной безопасности автоматизированных систем, специалист по защите информации	**x**	**x**	**x**	**x**	**x**	**x**
090106	Информационная безопасность телекоммуникационных систем, специалист по защите информации	**x**	**x**	**x**	**x**	**x**	
090107	Противодействие иностранным разведкам, специалист по защите информации	**x**	**x**	**x**			**x**
090108	Информационной безопасности автоматизированных систем, техник по защите информации		**x**	**x**	**x**	**x**	

Следует отметить, что предложенная классификация объектов профессиональной деятельности носит экспертный характер и обладает, вследствие этого, определенными недостатками (на практике можно встретить варианты, которые не вписывается в данную классификацию). Тем не менее, такая классификация позволяет сделать определенные выводы об индивидуальных отличительных особенностях отдельных направлений подготовки. К ним относятся следующее:

1. Объектами профессиональной деятельности специалистов со средним профессиональным образованием чаще всего не могут быть объект в целом (система) и СМИБ объектов различного уровня. Это одно из отличий от специалистов с ВПО.

2. Отличие бакалавров (магистров) ИБ от специалистов ВПО проявляется, прежде всего, в полноте видов объектов профессиональной деятельности. Это говорит о том, что бакалавры (магистры) должны отличаться широтой спектра профессиональных компетенций, а специалисты — их глубиной.

3. Большинство специальностей имеют ограниченный перечень объектов профессиональной деятельности, что лежит в основе не только отличий от направления подготовки бакалавр (магистр), но и обосновывает отличие специальностей друг от друга.

4. Специальность 090101 чаще всего имеет дело с математическими методами защиты информации (объектом профессиональной деятельности является технология обеспечения ИБ) с элементами управления (например, распределение и управление криптографическими ключами), которые могут быть отнесены к СМИБ как объекту профессиональной деятельности.

5. Специальность 090102 в большей степени отражает особенности использования методов защиты в различных информационных технологиях (например, защищенные операционные системы,

защищенные системы управления базами данных) при безусловной важности процессов управления. Поэтому объектами профессиональной деятельности, относящимися к данной специальности, будут информационные технологии, технологии обеспечения ИБ и СМИБ.

6. Специальность 090103 носит явно выраженный управленческий характер. Причем управление направлено на объект (организацию) в целом с учетом использования различных мер (методов, средств) по защите информации. Таким образом, объектами профессиональной деятельности выпускников по данной специальности будут СМИБ, технологии обеспечения ИБ и система (объект в целом).

7. Отличие специальности 090104 от специальности 090103 заключается в более тесном взаимодействием с информационными технологиями, которые используются в организации, в оптимальном выборе мер защиты и в эффективном управлении системой обеспечения ИБ всей организации. Поэтому объектами профессиональной деятельности, относящихся к данной специальности, будут СМИБ, технологии обеспечения ИБ, информационные технологии и система (объект в целом).

8. Среди специальностей спектром охвата объектов профессиональной деятельности выделяется специальность 090105. Это объясняется тем, что автоматизированная система организации как объект может быть и системой (информационная система организации), и частью системы (автоматизированная система одного из процессов организации), и компонентом части системы (информационная система подразделения организации), а также может использовать различные информационные технологии, различные технологии обеспечения ИБ и, наконец, должна обладать СМИБ как части системы управления всей автоматизированной системой.

9. Специальность 090106 отличается от специальности 090105 отсутствием такого объекта профессиональной деятельности, как система. Это объясняется тем, что телекоммуникационные системы, выполняя транспортные функции, не являются полностью самостоятельными и являются частью объекта (например, частью отдельной автоматизированной системы организации), решающей отдельную задачу для организации в целом. В остальном различия между объектами «автоматизированная система» и «телекоммуникационная система» незначительны и связаны с отдельными особенностями информационных технологий, технологий обеспечения ИБ и технологий управления ИБ.

10. Специальность 090107 по объектам профессиональной деятельности очень похожа на специальность 090104. Различия, возможно, лежат в области использования информационных технологий и технологий обеспечения ИБ. На практике разнообразие этих технологий не отличается широтой. Поэтому представляется важным найти веские аргументы для доказательства уникальности специальности 090107.

Уточнение выявленных моментов возможно при рассмотрении видов профессиональной деятельности и привязки их к направлениям подготовки и специальностям, а значит и к объектам профессиональной деятельности.

Направление подготовки 090000 – Информационная безопасность можно характеризовать следующими *видами профессиональной деятельности* выпускников:

· эксплуатационная;

· организационно-управленческая;

· проектная;

· экспериментально-исследовательская деятельность;

· научно-исследовательская.

Основываясь на анализе существующих образовательных стандартов, учитывая особенности создаваемой в России многоуровневой профессиональной подготовки специалистов, можно предложить модель, описывающую связь видов профессиональной деятельности с уровнями подготовки специалистов (бакалавры ИБ, магистры ИБ, математики и специалисты по защите информации, относящиеся к различным специальностям ВПО, и техники по защите информации СПО).

Информация, приведенная в таблице 3, поясняет особенности предлагаемой модели. Ее анализ позволяет сделать следующие выводы:

1. Дополнительным отличием между бакалаврами (магистрами) и специалистами является отсутствие у первой группы эксплуатационной деятельности. Это позволяет сформулировать определенные аргументы для определения места работы бакалавра (магистра) и специалиста.

2. Отличие специалистов с ВПО от специалистов со СПО заключается не только в объектах, но и в видах профессиональной деятельности. Последней группе характерна в большей степени эксплуатационная деятельность. Привлечение специалистов этой группы к некоторым другим видам деятельности возможно только при дополнительном обучении.

3. Отличие магистра от бакалавра ИБ лежит в количестве видов профессиональной деятельности. Для магистров характерным является экспериментально-исследовательская и научно-исследовательская деятельность и больший по сравнению с бакалаврами профессиональный уровень организационно-управленческой и проектной деятельности.

4. Для специалистов всех специальностей характерным являются проектная, экспериментально-исследовательская и научно-исследовательская деятельность с учетом специфики объектов профессиональной деятельности.

5. Организационно-управленческая деятельность в большей степени характерна тем специальностям, которые имеют дело с объектами высокого уровня (системы, объекты системы): 090103 – 090107.

6. Организационно-управленческая деятельность в меньшей степени характерна тем специальностям, которые не имеют дело с объектами высокого уровня (системы, объекты системы): 090101, 090102.

7. Единственная специальность, для которой в меньшей степени характерна эксплуатационная деятельность, — это специальность 090103. Сравнение видов профессиональной деятельности магистров ИБ и специалистов по защите информации по специальности 090103 выявляют их идентичность. С учетом совпадений по объектам профессиональной деятельности (Таблица 2) можно сделать вывод о наличии проблем с доказательством уникальности специальности 090103.

8. Совпадение видов профессиональной деятельности, а также объектов профессиональной деятельности у специальностей 090104 и 090107, а также у специальностей 090105 и 090106 иллюстрирует их близость. Доказательство различий, видимо, лежит в плоскости отличий в технологиях (информационных и обеспечения ИБ), что весьма проблематично доказать при предполагаемом уровне объемов обязательных дисциплин (порядка 70% учебного времени).

Таблица 3.

№	Направление/специальность, Квалификация	эксплуатационная	организационно-управленческая	проектная	экспериментально-исследовательская деятельность	научно-исследовательская
090100	Информационная безопасность, бакалавр информационной безопасности		**x**	**x**		
090100	Информационная безопасность, магистр информационной безопасности		**x**	**x**	**x**	**x**
090101	Криптография, математик			**x**	**x**	**x**
090102	Компьютерная безопасность, математик	**x**		**x**	**x**	**x**
090103	Организация и технология защиты информации, специалист по защите информации		**x**	**x**	**x**	**x**
090104	Комплексная защита объектов информатизации, специалист по защите информации	**x**	**x**	**x**	**x**	**x**

090105	Комплексное обеспечение информационной безопасности автоматизированных систем, специалист по защите информации	**x**	**x**	**x**	**x**	**x**
090106	Информационная безопасность телекоммуникационных систем, специалист по защите информации	**x**	**x**	**x**	**x**	**x**
090107	Противодействие иностранным разведкам, специалист по защите информации	**x**	**x**	**x**	**x**	**x**
090108	Информационной безопасности автоматизированных систем, техник по защите информации	**x**				

Модель видов профессиональной деятельности можно дополнить задачами, которые должны решать выпускники укрупненного направления подготовки 090000 – Информационная безопасность. При этом возможности предложенной классификации объектов предметной области «Информационная безопасность» и особенности описанной выше модели объектов профессиональной деятельности выпускников позволяют сформулировать характерные (обобщенные) задачи, относящиеся в различной степени ко всем направлениям подготовки и специальностям укрупненного направления 090000.

Задачи профессиональной деятельности специалиста на объекте профессиональной деятельности по видам профессиональной деятельности:

а) эксплуатационная деятельность;

· обеспечение эффективного функционирования информационных технологий с учетом требований по обеспечению ИБ;

· обеспечение эффективного функционирования средств защиты информации в рамках отдельных подсистем ИБ объекта;

· администрирование отдельных подсистем ИБ объекта;

· проведение мониторинга защищенности объекта;

· обеспечение восстановления работоспособности систем объекта в режиме нештатных ситуаций.

б) организационно-управленческая деятельность:

· выявление особенностей функционирования объекта с целью определения информационной инфраструктуры и активов, подлежащих защите;

· формирование политики ИБ объекта на основе определения активов, подлежащих защите, разработки моделей угроз и нарушителя, проведения анализа информационных рисков и формулирования правил, процедур, практических приемов и руководящих принципов по обеспечению ИБ объекта;

· контроль эффективности реализации политики информационной безопасности объекта;

· эксплуатация СМИБ объекта;

· оценка эффективности функционирования СМИБ объекта на основе использования методов мониторинга и аудита;

· разработка предложений по совершенствованию СМИБ объекта;

· планирование и организация работы малых коллективов исполнителей;

в) проектная деятельность:

· участие в анализе технических заданий на проектирование, в выполнении технических и рабочих проектов подсистем ИБ объекта, с учетом действующих нормативных и методических документов.

· разработка системы обеспечения ИБ объекта;

· разработка и реализация методов и средств защиты информации для использования на объекте;

· разработка СМИБ объекта;

· разработка методов и средств оценки эффективности средств защиты как основы проведения их сертификации;

· разработка методов и средств мониторинга ИБ объекта;
· разработка методов и средств аудита ИБ объекта;
· разработка проектов нормативных и методических материалов, регламентирующих работу по обеспечению ИБ, а также положений, инструкций и других организационно-распорядительных документов.

г) экспериментально-исследовательская деятельность:

· проведение экспериментально-исследовательских работ при сертификации средств защиты;
· проведение экспериментально-исследовательских работ при аттестации объектов с учетом требований к обеспечению ИБ;
· проведение аудита (в том числе инструментального) защищенности объекта;
· экспериментальное исследование объекта с целью выявления уязвимостей в условиях существования угроз в информационной сфере;
· исследование информационных технологий с целью выявления их уязвимостей.

з) научно-исследовательская деятельность:

· изучение и обобщение опыта работы других учреждений, организаций и предприятий по способам обеспечения ИБ с целью повышения эффективности и совершенствования работ по защите информации на конкретном объекте;
· подбор, изучение и обобщение научно-технической литературы, нормативных и методических материалов по методам обеспечения ИБ объектов;
· составление аналитических обзоров по вопросам обеспечения ИБ объектов;
· анализ ИБ современных информационных технологий, используемых на объекте;
· исследование и разработка методов защиты информации и систем, обеспечивающих ИБ объекта;
· исследование и разработка математических моделей средств защиты информации и систем, обеспечивающих ИБ объекта;
· обоснование и выбор оптимального решения по уровню обеспечения ИБ объекта как компромисса между различными требованиями.

4. Порядок формулирования профессиональных компетенций

Профессиональные компетенции должны быть сформулированы отдельно для каждого направления и специальности ВПО и СПО. Исходные данные, рассмотренные выше в рамках предложенных моделей объектов и видов профессиональной деятельности, могут быть использованы для формулирования профессиональных компетенций. При этом можно рекомендовать алгоритм, состоящий из упорядоченного выполнения следующих этапов:

1. Выбирается направление или специальность подготовки специалистов ВПО или СПО.
2. Определяется область профессиональной деятельности.
3. Определяются объекты профессиональной деятельности.
4. Уточняются виды профессиональной деятельности.
5. Формулируются задачи профессиональной деятельности на основе уточнения обобщенных задач, описанных выше.
6. Для каждой задачи профессиональной деятельности формулируется одна или несколько профессиональных компетенций.
7. Формулируются квалификационные характеристики (уровни знаний, умений и владений предметом), необходимые для овладения определенными профессиональными компетенциями.

Заключение

В данной работе предложен и описан общий подход, относящейся к укрупненному направлению профессиональной подготовки 090000 — Информационная безопасность, на базе которого возможно формулирование профессиональных компетенций отдельных направлений и специальностей, входящих в рассматриваемое направление.

Основываясь на уточнении термина «информационная безопасность» и предложенной классификации объектов предметной области «Информационная безопасность», были описаны модели объектов и видов профессиональной деятельности выпускников укрупненного направления 090000.

Предложенные модели использованы для определения списка характерных (обобщенных) задач по каждому из видов профессиональной деятельности.

Описанный в работе общий подход к определению исходных данных позволил предложить алгоритм, выполнение которого направлено на формулирование профессиональных компетенций конкретного направления или специальности, относящихся к ВПО и СПО. Этот алгоритм обладает универсальностью и не зависит от направления подготовки или специальности, входящих в укрупненное направление 090000 – Информационная безопасность.

Использование предложенных моделей дало возможность определить для предметной области «Информационная безопасность» различия между бакалаврами (магистрами) и специалистами ВПО, между выпускниками ВПО и выпускниками СПО, между бакалаврами ИБ и магистрами ИБ, между отдельными специальностями ВПО и выявить проблемные места в доказательности уникальности отдельных специальностей ВПО, вошедших в укрупненное направление 090000. К таким специальностям относятся специальности 090103, 090106 и 090107. При предполагаемом уровне объемов обязательных дисциплин (порядка 70 % учебного времени) учебный план специальности 090103 может быть полностью поглощен учебным планом подготовки магистров ИБ, учебные планы специальностей 090106 и 090107 могут быть полностью реализованы как учебные планы специализаций соответственно специальности 090105 и специальности 090104.

СПИСОК ЛИТЕРАТУРЫ:

1. Доктрина информационной безопасности РФ (9 сентября 2000 г.).
2. Федеральный закон от 4 июля 1996 г. № 85-ФЗ «Об участии в международном информационном обмене». Ст. 2.
3. ГОСТ Р ИСО/МЭК 17799-2005. Практические правила управлению информационной безопасностью.
4. ГОСТ Р ИСО/МЭК 27001-2006. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования.
5. ГОСТ Р ИСО/МЭК 13335-1-2006. Информационная технология. Методы и средства обеспечения безопасности. Часть 1. Концепция и модели менеджмента безопасности информационных и телекоммуникационных технологий.
6. Материалы Гостехкомиссии РФ.
7. Руководящий документ. Защита от несанкционированного доступа к информации. Термины и определения. Утверждено решением председателя ГТК России от 30 марта 1992 г.
8. ГОСТ Р 50.1.053-2005 Информационные технологии. Основные термины и определения в области технической защиты информации.
9. ГОСТ Р 50922-2006. Защита информации. Основные термины и определения.
10. Стандарт Банка России СТО БР ИББС-1.0 «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Общие положения».