А. Б. Костина, Н. Г. Милославская, А. И. Толстой

АСПЕКТЫ УПРАВЛЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ В УЧЕБНЫХ ПЛАНАХ ПОДГОТОВКИ КАДРОВ В ОБЛАСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Введение

В начале 80-х годов XX в. защита информации эффективно обеспечивалась специально разработанными организационными мерами и программно-аппаратными средствами шифрования. С появлением локальных и глобальных сетей, каналов спутниковой связи вопрос об информационной безопасности (ИБ) встал острее. Выборочная и бессистемная реализация защитных мер не может обеспечить требуемый организации уровень ИБ. Чтобы надежно защитить свою информацию, необходимо интегрировать решение вопросов ИБ в единый для всей организации процесс — процесс управления ИБ организации, связанный с собственно обеспечением ИБ и снижением выявленных рисков ИБ для ее бизнеса.

Любая информация, которая может повлиять на ИБ, качество, график, стоимость и окружение, должна быть объектом такого процесса управления. Любые действия, совершаемые в рамках выполнения какой-либо деятельности, должны быть вовлечены в процесс управления ИБ.

Управление ИБ не может рассматриваться только с технической и технологической точек зрения, хотя ответ на вопрос, является ли ИБ по существу информационной технологией (ИТ), или ИТ — это всего лишь одна из областей, в которой ИБ играет существенную роль, также очень важен. Управление ИБ — это комплексный, непрерывно выполняемый процесс, обязательно имеющий правовую, организационную, документальную и другие составляющие.

Все это доказывает необходимость тщательного изучения вопросов управления ИБ. Поэтому определение аспектов управления ИБ, которые обязательно нужно отразить в учебных планах подготовки специалистов в области ИБ, является актуальным на современном этапе реформы национальной системы высшего образования.

В статье определяются особенности требований к уровню подготовки кадров в части аспектов управления ИБ, выбирается нормативная база, относящаяся к различным аспектам управления ИБ, формируется перечень блоков тем изучения основных подходов к созданию систем управления ИБ (СУИБ) и даются рекомендации по разработке и реализации учебных программ соответствующих дисциплин.

1. Особенности учебных планов подготовки кадров с высшим образованием в области информационной безопасности

Повышение роли процессов управления при обеспечении ИБ систем и объектов было учтено при разработке соответствующих Федеральных государственных образовательных стандартов (ФГОС) третьего поколения, относящихся к направлениям и специальностям подготовки кадров с высшим образованием. Анализ ФГОС укрупненного направления подготовки 090000 — «Информационная безопасность» позволил выделить области профессиональной деятельности и рекомендуемые учебные дисциплины, относящиеся к управлению ИБ (таблица 1).

При подготовке бакалавров и магистров направления 090900 — «Информационная безопасность», а также специалистов по специальностям 090301, 090302, 090303 и 090915 среди объектов профессиональной деятельности указаны или процессы, или системы управления ИБ. Формирование при этом необходимых профессиональных компетенций ФГОС рекомендуют в рамках соответствующих учебных дисциплин, относящихся к базовой части ФГОС (бакалавры, магистры, специальности 090303, 090915) или к частям ФГОС, относящимся к определенным специализациям специальностей 090301, 090302 и 090303.

Таблица 1. Направления подготовки, объекты профессиональной деятельности и учебные дисциплины, относящиеся к управлению ИБ

Направление/ Специальность	**Объект профессиональной деятельности**	**Дисциплина**
Направление 090900 — «Информационная безопасность» (подготовка бакалавров)	Процессы управления ИБ защищаемых объектов	«Управление ИБ»
Направление 090900 — «Информационная безопасность» (подготовка магистров)	Процессы управления ИБ защищаемых объектов, методы и средства оптимизации процессов управления	«Управление ИБ»
Специальность 090301 — «Компьютерная безопасность»	СУИБ компьютерных систем	«Теория управления ИБ распределенных компьютерных систем», «Методы анализа рисков» (специализация «Безопасность распределенных компьютерных систем»)
Специальность 090302 — «Информационная безопасность телекоммуникационных систем»	Управление ИБ информационно-телекоммуникационных сетей и систем	«Планирование и управление ИБ» (специализация «Защита информации в системах связи и управления»); «Управление ИБ телекоммуникационных систем» (специализация «Разработка защищенных телекоммуникационных систем»)
Специальность 090303 — «Информационная безопасность автоматизированных систем»	СУИБ автоматизированных систем (АС)	«Управление ИБ» (специальность), «Аудит информационных технологий и систем обеспечения ИБ» (специализация «Безопасность открытых информационных систем»); «Менеджмент инцидентов ИБ защищенных АС управления» (специализация «Защищенные АС управления»); «Мониторинг безопасности ИС», «Анализ рисков ИБ» (специализация «Анализ безопасности информационных систем»); «Угрозы ИБ АС», «Оценка ИБ АС в защищенном исполнении» (специализация «Создание АС в защищенном исполнении»)

Специальность 090915 «Безопасность информационных технологий в правоохранительной области»	Процесс управления системами, обеспечивающими ИБ на защищаемых объектах, методы и средства оптимизации процессов управления	«Управление ИБ» (специальность)

Учитывая эти особенности, необходимы разделы, которые могут быть полезны при разработке и реализации указанных в таблице 1 учебных дисциплин, относящихся к различным направлениям и специальностям подготовки, и которые направлены на изучение основных положений, связанных с управлением ИБ, и подходов к разработке, реализации, эксплуатации, анализу, сопровождению и совершенствованию СУИБ определенного объекта.

Основная задача реализации относящихся к управлению ИБ учебных дисциплин — представить обучающимся систематизированный подход к проблеме управления ИБ, ознакомить их с возможными вариантами решений, показать главные составляющие процесса управления ИБ, изложить базовые концептуальные подходы к правильной организации управления ИБ на основе создания СУИБ с учетом выявленных рисков ИБ, а также научить квалифицированно разрабатывать документальное обеспечение для СУИБ, оценивать уровень функционирования СУИБ, выбирать, применять и самостоятельно разрабатывать защитные меры и средства защиты информации (СЗИ) для обеспечения требуемого уровня ИБ. Освоение обучающимися этих дисциплин должно способствовать эффективному формированию у них следующих профессиональных компетенций:

- способность участвовать в управлении ИБ объекта;
- способность участвовать в проектировании и разработке системы управления ИБ объекта;
- способность участвовать в проведении контрольных мероприятий по определению эффективности и результативности СУИБ объекта.

Эти профессиональные компетенции необходимы для решения задач, относящихся к таким видам профессиональной деятельности в сфере управления ИБ, как организационно-управленческая, проектно-конструкторская или контрольно-аналитическая.

При этом выпускник образовательного учреждения, прошедший обучение, должен:

«иметь представление»:

- о принципах построения СУИБ объекта;
- о современных подходах к управлению ИБ объекта и направлениях их развития;
- о взаимосвязи отдельных процессов управления ИБ в рамках СУИБ;

«знать»:

- основные международные и российские стандарты, регламентирующие управление ИБ;
- принципы разработки процессов управления ИБ;
- принципы создания основных документов, регламентирующих вопросы управления ИБ;
- подходы к интеграции СУИБ в общую систему управления организации;

«уметь»:

- анализировать текущее состояние ИБ на предприятии с целью установления требований к разрабатываемым процессам управления ИБ;
- определять цели и задачи, решаемые разрабатываемыми процессами управления ИБ;
- применять процессный подход к управлению ИБ в различных сферах деятельности;
- используя современные методы и средства, разрабатывать процессы управления ИБ,

учитывающие особенности функционирования предприятия и решаемых им задач, и оценивать их эффективность;

• практически решать задачи формализации разрабатываемых процессов управления ИБ;

• разрабатывать документальное обеспечение для процессов управления ИБ, включая различные политики ИБ, и применять его на практике;

«владеть»:

• терминологией и процессным подходом построения СУИБ;

• навыками анализа активов организации, их угроз ИБ и уязвимостей в рамках области действия СУИБ;

• навыками построения как отдельных процессов управления ИБ, так и системы процессов в целом.

Сформулированные выше квалификационные характеристики формируются в рамках образовательного процесса с использованием определенного контента обучения, который должен быть выделен для рассматриваемой предметной области.

2. Методическая база формирования контента обучения вопросам управления информационной безопасностью

Разработка учебно-методической поддержки обучения дисциплинам, связанным с управлением ИБ, находится на начальном этапе. В настоящее время практически отсутствуют необходимые для этого учебники, учебные и учебно-методические пособия. Некоторую полезную информацию, относящуюся к проблемам управления ИБ, можно найти в ограниченном количестве отечественных изданий [1–5]. Поэтому единственной альтернативой для формирования контента обучения вопросам управления ИБ является использование опыта (лучших практик), который отражают существующие стандарты, относящиеся к рассматриваемой сфере.

Особую роль в обобщении этого опыта играют Международная организация по стандартизации ISO (ИСО) и Международная электротехническая комиссия IEC (МЭК), которые формируют специализированную систему всемирной стандартизации.

На данный момент можно с уверенностью сказать, что мировое сообщество проделало существенную работу в направлении стандартизации СУИБ и отдельных процессов управления ИБ и по-прежнему весьма активно продолжает эту работу.

Основоположником подобной стандартизации стала серия стандартов ИСО 9000, предъявляющих требования к системам менеджмента качества, соблюдение которых позволяет контролировать качество выпускаемой продукции или предоставляемых услуг. При разработке стандартов на СУИБ многое было взято за основу именно из стандартов серии ИСО 9000, например основной подход — процессный подход и использование циклической модели PDCA для непрерывного совершенствования как самой системы, так и отдельных ее процессов. Помимо этого отличительной особенностью стандартов ИСО 9000, которая была перенята при стандартизации СУИБ, является то, что они устанавливают степень ответственности руководства организации за качество. Причем руководство организации отвечает как за разработку политики в области качества, так и за внедрение и поддержание в рабочем состоянии системы менеджмента качества. Очень большое количество процессов управления из систем менеджмента качества с некоторыми изменениями присутствует и в СУИБ, например внутренние аудиты ИБ, корректирующие и предупреждающие действия и т. д.

Особое место в настоящее время занимает серия стандартов ИСО/МЭК 27000 «Информационные технологии. Методы обеспечения безопасности». История развития этой серии началась в 1999 г., когда обновленная первая часть британского стандарта BS 7799:1995 (BS

7799-1:1999) была передана в ИСО и в 2000 г. впервые утверждена в качестве международного стандарта как ИСО/МЭК 17799:2000. Следующей его версией стал стандарт ИСО/МЭК 17799:2005.

В том же 1999 г. вышла в свет вторая часть стандарта BS 7799 — BS 7799-2:1999 «Information Security Management. Specification for ISMS» для СУИБ (Information Security Management System). В 2002 г. стандарт был усовершенствован и выпущена его новая редакция — BS 7799-2:2002. На ее основе в 2005 г. был принят стандарт ИСО/МЭК 27001:2005.

Дальнейшее развитие стандартов серии 27000 включает в себя стандарты, более подробно раскрывающие требования к отдельным процессам управления ИБ. Базируясь на единой структуре и методологии, заложенной в ИСО/МЭК 27001:2005, они представляют собой руководства по управлению ИБ для различных сфер деятельности, включая финансовый и страховой сектор, здравоохранение, телекоммуникации и т. д.

На сегодня существуют и планируются к ближайшему принятию стандарты серии, перечисленные в таблице 2 (индекс утвержденных стандартов содержит год ввода в действие).

Таблица 2. Стандарты серии ИСО/МЭК 27000

Индекс	Название
27000:2009	СУИБ. Определения и основные принципы.
27001:2005	СУИБ. Требования (на основе BS 7799-2:2005).
27002:2005	Практические правила управления ИБ (ранее ИСО/МЭК 17799:2005).
27003:2010	Руководство по внедрению СУИБ.
27004:2009	Управление ИБ. Оценка СУИБ.
27005:2008	Управление рисками ИБ (на основе BS 7799-3:2006).
27006:2007	Требования к органам, обеспечивающим аудит и сертификацию СУИБ.
27007	Руководство по аудиту СУИБ. Выпуск планируется в 2011 г.
27008	Руководство по аудиту средств управления ИБ, реализованных в СУИБ. Выпуск планируется в 2011 г.
27010	Управление ИБ при коммуникации между секторами (в нескольких частях, представляющих собой руководство по совместному использованию информации о рисках ИБ, средствах управления, проблемах и/или инцидентах ИБ, выходящих за границы отдельных секторов экономики и государств, особенно в части, касающейся критичных инфраструктур).
27011:2008	Руководство по управлению ИБ для телекоммуникационных компаний на основе ИСО/МЭК 27002.
27013	Руководство по интегрированному внедрению ИСО 20000 и ИСО 27001. Выпуск планируется в 2011 г.
27014	Базовая структура управления ИБ.
27015	Руководство по внедрению СУИБ для финансовых сервисов (банков, страховых компаний, кредитных организаций и т. д.).
27031:2011	Руководство по готовности информационных и телекоммуникационных технологий для обеспечения непрерывности бизнеса (на базе BS 25699:2006/2007).
27032	Руководство по обеспечению кибербезопасности.

27033	27033-1:2009 Безопасность сетей. Часть 1 — Общие положения и концепции. 27033-2 Руководство по проектированию и внедрению системы обеспечения безопасности сетей. Выпуск планируется в конце 2011 г. 27033-3:2010 Базовые сетевые сценарии — угрозы, методы проектирования и средства управления. 27033-4 Обеспечение безопасности межсетевых взаимодействий при помощи шлюзов безопасности — угрозы, методы проектирования и средства управления. 27033-5 Обеспечение безопасности виртуальных частных сетей — угрозы, методы проектирования и средства управления. 27033-6 Конвергенция в IP-сетях (определение угроз, методов проектирования и средств управления в IP-сетях с конвергенцией данных, голоса и видео). 27033-7 Руководство по обеспечению безопасности беспроводных сетей — риски, методы проектирования и средства управления.
27034	27034-1 Безопасность приложений. Часть 1 — Обзор и основные концепции в области обеспечения безопасности приложений. 27034-2 Нормативная база организации. 27034-3 Процесс управления безопасностью приложений. 27034-4 Оценка безопасности приложений. 27034-5 Протоколы и структура управляющей информации для обеспечения безопасности приложений (XML-схема). 27034-6 Руководство по обеспечению безопасности конкретных приложений.
27035	Управление инцидентами безопасности (заменит ИСО/МЭК ТО 18044). Выпуск планируется в 2011 г.
27036	Руководство по аутсорсингу безопасности. Выпуск планируется в 2012 г.
27037	Руководство по идентификации, сбору и/или получению и обеспечению сохранности свидетельств, представленных в электронной форме (на базе BS 10008:2008).
27799:2008	Управление ИБ в сфере здравоохранения.

Что касается собственно российских стандартов по управлению ИБ, то сначала были приняты стандарт ГОСТ Р ИСО/МЭК 17799-2005, идентичный 17799:2000 и актуализированный 01.01.2008, и стандарт ГОСТ Р ИСО/МЭК 27001-2006, идентичный 27001:2005. В настоящее время российская стандартизация в области управления ИБ проходит некоторую промежуточную стадию своего формирования и является еще недостаточно зрелой, однако уже сейчас намечаются положительные тенденции в развитии данной области.

Взаимосвязь российских, международных и британских стандартов, посвященных СУИБ, отражена в таблице 3.

Таблица 3. Взаимосвязь стандартов, посвященных СУИБ

Российский стандарт	**Международный стандарт**	**Британский стандарт**
ГОСТ Р 17799:2005	ИСО/МЭК 27002:2007	BS 7799-1:2005
-	ИСО/МЭК 17799:2005	
ГОСТ Р 27001:2005	ИСО/МЭК 27001:2005	BS 7799-2:2005
	ИСО/МЭК 27005:2008	BS 7799-3:2005

Кроме серии стандартов ИСО/МЭК 27000 имеются стандарты на отдельные процессы управления ИБ и оценку безопасности ИТ. К ним можно отнести:

1. Стандарт ИСО/МЭК 13335 «Information technology. Security techniques. Management of information and communications technology security» (Информационная технология. Методы и средства обеспечения безопасности. Менеджмент безопасности ИТТ). Он состоит из четырех частей, которые адаптированы в стандарты РФ:

1.1. ГОСТ Р ИСО/МЭК 13335-1-2006 «Концепция и модели менеджмента безопасности информационных и телекоммуникационных технологий» (аутентичный текст с ИСО/МЭК 13335-1:2004);

1.2. ГОСТ Р ИСО/МЭК ТО 13335-3-2007 «Методы менеджмента безопасности информационных технологий» (аутентичный текст с ИСО/МЭК ТО 13335-3:1998);

1.3. ГОСТ Р ИСО/МЭК ТО 13335-4-2007 «Выбор защитных мер» (аутентичный текст с ИСО/МЭК ТО 13335-4:2000);

1.4. ГОСТ Р ИСО/МЭК ТО 13335-5-2006 «Руководство по менеджменту безопасности сети» (аутентичный текст с ИСО/МЭК ТО 13335-5:2001);

2. Британский стандарт BS 7799-3:2006 «Information security management systems. Guidelines for information security risk management» (Системы менеджмента ИБ. Руководство по управлению рисками ИБ);

3. Стандарт ИСО 19011:2002 «Guidelines for quality and/or environmental management systems auditing» (Руководство по аудиту систем менеджмента качества и/или окружающей среды) и аутентичный ему ГОСТ Р ИСО 19011-2003 «Руководящие указания по аудиту систем менеджмента качества и/или систем экологического менеджмента»;

4. Британские стандарты BS 25999-1:2006 «Business continuity management. Code of practice» (Управление непрерывностью бизнеса (УНБ). Практические правила), BS 25999-2:2007 «Business continuity management. Specification» (УНБ. Спецификация) и аналогичные им отечественные стандарты: ГОСТ Р 53647.1-2009 «Менеджмент непрерывности бизнеса. Часть 1. Практическое руководство» и ГОСТ Р 53647.2-2009 «Менеджмент непрерывности бизнеса. Часть 2. Требования»;

5. Стандарт ИСО/МЭК ТО 18044:2004 «Information technology. Security techniques. Information security incident management» (Информационная технология. Методы и средства обеспечения безопасности. Менеджмент инцидентов ИБ) и идентичный ему ГОСТ Р ИСО/МЭК ТО 18044-2007 «Информационная технология. Методы и средства обеспечения безопасности. Менеджмент инцидентов информационной безопасности»;

6. Три части стандарта ИСО/МЭК 15408 «The Common Criteria for Information Technology Security Evaluation» (Общие критерии оценки безопасности ИТ) и идентичные им ГОСТ Р ИСО/МЭК 15408-1-2008 «Введение и общая модель», ГОСТ Р ИСО/МЭК 15408-2-2008 «Функциональные требования безопасности», ГОСТ Р ИСО/МЭК 15408-3-2008 «Требования доверия к безопасности»;

7. Стандарт ИСО/МЭК 18045:2005 и идентичный ему ГОСТ Р ИСО/МЭК 18045-2008 «Информационная технология. Методы и средства обеспечения безопасности. Методология оценки безопасности информационных технологий»;

8. Отраслевые стандарты в области управления ИБ — серия стандартов (СТО БР ИББС) и рекомендации (РС БР ИББС) Банка России в области стандартизации «Обеспечение информационной безопасности организаций банковской системы РФ»:

8.1. СТО БР ИББС-1.0 «Общие положения»;

8.2. СТО БР ИББС-1.1 «Аудит информационной безопасности»;

8.3. СТО БР ИББС-1.2 «Методика оценки соответствия информационной безопасности организаций БС РФ требованиям СТО БР ИББС-1.0»;

8.4. РС БР ИББС-2.0 «Методические рекомендации по документации в области обеспечения информационной безопасности в соответствии с требованиями СТО БР ИББС-1.0»;

8.5. РС БР ИББС-2.1 «Руководство по самооценке соответствия информационной безопасности организаций БС РФ требованиям СТО БР ИББС-1.0»;

8.6. РС БР ИББС-2.2 «Методика оценки рисков нарушения информационной безопасности»;

8.7. РС БР ИББС-2.3. «Требования по обеспечению безопасности персональных данных в информационных системах персональных данных организаций БС РФ»;

8.8. РС БР ИББС-2.4. «Отраслевая частная модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных организаций БС РФ».

Перечисленные нормативные документы непосредственно определяют и структурируют основные направления, подходы и методы, связанные с управлением ИБ.

3. Составляющие проблемы управления информационной безопасностью

Анализ лучших практик управления ИБ, изложенных в перечисленных выше стандартах, позволил определить следующие блоки тем изучения основных подходов к созданию и эксплуатации СУИБ:

1. Основы управления ИБ (базовая терминология, стандартизация систем и процессов управления ИБ, политика ИБ, управление и система управления ИБ).

2. Управление рисками ИБ (определение риска ИБ, понятие управления рисками ИБ, составляющие процесса управления, системный подход к управлению, установление контекста управления, оценка рисков ИБ, обработка рисков ИБ, принятие рисков ИБ, коммуникация рисков ИБ, мониторинг и пересмотр рисков ИБ, документальное обеспечение управления рисками ИБ, инструментальные средства управления рисками ИБ).

3. Управление инцидентами ИБ (событие и инцидент ИБ, цели и задачи управления инцидентами ИБ, система управления инцидентами ИБ, этапы процесса управления инцидентами ИБ, обнаружение событий и инцидентов ИБ, обработка событий и инцидентов ИБ, реагирование на инциденты ИБ, документация системы управления инцидентами ИБ, группа реагирования на инциденты ИБ, обеспечение осведомленности и обучение в области управления инцидентами ИБ, сохранение доказательств инцидентов ИБ, средства управления инцидентами ИБ).

4. ИБ и обеспечение непрерывности бизнеса (НБ) (определения НБ и управления ею, система управления НБ, жизненный цикл управления НБ, документация и записи в области НБ, готовность информационных технологий к обеспечению НБ).

5. Технические аспекты управления ИБ (управление логическим доступом к активам организации, управление защищенной передачей данных и операционной деятельностью, разработка и обслуживание информационных систем, управление конфигурациями, изменениями и обновлениями, физическая защита и защита от воздействия окружающей среды).

6. Организационные и кадровые вопросы управления ИБ (модели организационного управления, организационная инфраструктура управления, организационные мероприятия по управлению, служба ИБ организации, задачи, функции, обязанности, права и ответственность администратора ИБ, группы компетенций, должности и направления деятельности специалистов в области ИБ, учет вопросов ИБ при работе с персоналом, сотрудничество между организациями и консультации со специалистами в области ИБ).

7. Проверка и оценка деятельности по управлению ИБ (процессы проверки системы управления ИБ (мониторинг, самооценка, внутренний и внешний аудит, анализ СУИБ со стороны высшего руководства организации, инструментальные средства проверки ИБ), оценка

деятельности по управлению ИБ (оценка эффективности и результативности деятельности по управлению ИБ, измерения, показатели и метрики), зрелость процессов СУИБ).

Перечисленные выше составляющие проблемы управления ИБ могут быть рассмотрены как отдельные вопросы или темы, формирующие предметную область обучения при подготовке профессионалов в области ИБ.

4. Особенности разработки и реализации учебных программ дисциплин, относящихся к управлению информационной безопасностью

При формировании программ учебных дисциплин, относящихся к управлению ИБ, необходимо учитывать направления подготовки кадров с высшим образованием в области ИБ. В соответствии с требованиями ФГОС содержание таких программ будет различаться в части глубины рассмотрения отдельных вопросов и тем.

Анализ составляющих проблемы управления ИБ, перечень которых приведен выше, позволяет сформулировать следующие рекомендации, которые необходимо учитывать при разработке программ учебных дисциплин.

1. Учебные программы должны отражать все перечисленные проблемы.

2. Общей частью для различных учебных программ с одинаковой глубиной рассмотрения должен быть раздел «Основы управления ИБ».

3. При подготовке бакалавров (направление 090900 — «Информационная безопасность») и специалистов (специальности 090301, 090302, 090303, 090315) такие разделы, как «Управление рисками ИБ», «Управление инцидентами ИБ», «ИБ и обеспечение непрерывности бизнеса», «Проверка и оценка деятельности по управлению ИБ», могут содержать только базовую информацию.

4. Глубина рассмотрения разделов «Технические аспекты управления ИБ» и «Организационные и кадровые вопросы управления ИБ» будет определяться профилем подготовки бакалавров и выбором соответствующих специальностей и их специализаций.

5. При подготовке магистров (направление 090900 — «Информационная безопасность») детальность проработки отдельных вопросов, относящихся к разделам «Управление рисками ИБ», «Управление инцидентами ИБ», «ИБ и обеспечение непрерывности бизнеса», «Проверка и оценка деятельности по управлению ИБ», «Технические аспекты управления ИБ» и «Организационные и кадровые вопросы управления ИБ», будет зависеть от выбранной магистерской программы.

6. Для закрепления обучающимися практических навыков целесообразно предусмотреть в программе учебных дисциплин не только лекции, но и семинары по тем разделам дисциплины, которые являются профильными для соответствующих направлений подготовки и определенных специальностей.

Следует отметить, что в настоящее время, к сожалению, отсутствует учебно-методическая база, необходимая для подготовки и реализации учебных дисциплин, относящихся к управлению ИБ. Разработка соответствующих учебных и методических пособий является актуальной проблемой, от решения которой зависит уровень подготовки специалистов в области ИБ.

Заключение

При рассмотрении требований к профессиональным компетенциям выпускников высшей школы в области ИБ в части аспектов, относящихся к управлению ИБ, было показано, что процессы или системы управления ИБ являются базовыми объектам профессиональной деятельности бакалавров и магистров направления 090900 — «Информационная безопасность», а также специалистов по специальностям 090301, 090302, 090303 и 090915.

При отсутствии учебно-методической базы реализации учебных дисциплин, относящихся к управлению ИБ, единственным подходом к определению содержания обучения является использование современной нормативной базы. Ее анализ позволил сформировать перечень международных и национальных стандартов, отраслевых стандартов и нормативных документов, в которых описаны лучшие практики в области управления ИБ.

Результатом анализа этих документов является определение базовых блоков тем, предназначенных для изучения основных подходов к созданию и использованию СУИБ.

Проведенный анализ профессиональных компетенций, определенных в соответствующих ФГОС, дал возможность сформулировать рекомендации по разработке и реализации учебных программ дисциплин, относящихся к управлению ИБ, в зависимости от направлений и специальностей подготовки профессионалов с высшим образованием в области ИБ. Данные рекомендации могут быть полезны преподавателям и организаторам учебного процесса.

СПИСОК ЛИТЕРАТУРЫ:

1. *А. П. Курило, С. Л. Зефиров, В. Б. Голованов и др.* Аудит информационной безопасности. М.: Издательская группа «БДЦ-пресс», 2006. – 304 с.
2. Обеспечение информационной безопасности бизнеса / Под ред. А. П. Курило. М.: Альпина Паблишерз, 2011. – 392 с.
3. Проблемы управления информационной безопасностью / Под ред. Д. С. Черешкина. М.: Изд. группа URSS, 2002. – 192 с.
4. *Петренко С. А.* Анализ рисков в области защиты информации. Информационно-методическое пособие по курсу повышения квалификации «Управление информационными рисками». СПб.: ООО «Издательский дом "Афина"», 2009. – 153 с. Оставить в таком написании
5. *Астахов А. М.* Искусство управления информационными рисками. М.: ДМК Пресс, 2010. – 312 с.