А. А. Хорев

МАГИСТЕРСКАЯ ПРОГРАММА ПОДГОТОВКИ «АУДИТ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ АВТОМАТИЗИРОВАННЫХ СИСТЕМ»

С 2011 г. большинство вузов России, осуществляющих подготовку специалистов в области информационной безопасности, переходят на двухуровневую структуру образования: бакалавр (срок обучения 4 года) и магистр (срок обучения 2 года).

До сих пор не утихают споры о целесообразности такого перехода, так как двухуровневая подготовка имеет как положительные, так и отрицательные стороны.

Не будем останавливаться на отрицательной стороне, а сосредоточим свое внимание на том положительном, что дает такой переход.

На мой взгляд, при таком переходе выигрывают именно работодатели, т. е. те, в чьих интересах и готовятся такие специалисты.

Бакалавр и магистр — это уровни квалификации специалистов в области информационной безопасности.

Именно работодатели должны определить, какой уровень квалификации специалистов им нужен — бакалавр или магистр.

В основу Федеральных государственных образовательных стандартов высшего профессионального образования (ФГОС ВПО) третьего поколения положен компетентностный подход, хотя до настоящего времени в вузовской среде нет единого понимания, что же такое компетенция.

Есть десятки определений компетенции, существенно отличающихся не только по содержанию, но и по смыслу, что не позволяет разработать принципы формирования компетенций, показатели и критерии оценки их сформированности.

Я придерживаюсь следующего определения компетенции: **компетенция** — это совокупность взаимосвязанных знаний, умений и навыков, определяющих способность специалиста успешно решать конкретные профессиональные задачи в рамках своих должностных обязанностей.

По данному определению компетенция является одной из описательных характеристик, служащей для формирования квалификационных требований, предъявляемых к уровню квалификации специалистов в области информационной безопасности и защиты информации.

Такой подход позволяет каждому вузу сформировать основные образовательные программы магистратуры с учетом его возможностей, требований работодателей данного региона.

Формирование основной образовательной программы магистратуры целесообразно осуществлять в следующей последовательности:

– анализ рынка труда в регионе и востребованности специалистов в области информационной безопасности и защиты информации в регионе, прогноз потребностей специалистов в области информационной безопасности и защиты информации на 5–10 лет;

– анализ квалификационных требований, предъявляемых к специалистам по информационной безопасности и защите информации в организациях (на предприятиях, в учреждениях) региона;

– определение перечня должностей, квалификационные требования к которым могут быть реализованы только в рамках магистратуры;

– составление перечня организаций (предприятий, учреждений) региона, нуждающихся в магистрах в области информационной безопасности, заключение с ними договоров на подготовку магистров;

– разработка дополнительных профессиональных компетенций, не вошедших в ФГОС ВПО, обеспечивающих реализацию квалификационных требований, предъявляемых к магистрам;

– выбор направленности магистерской программы подготовки (аналог специализации);

– с учетом требований ФГОС ВПО и дополнительных профессиональных компетенций разработка перечней знаний, умений и навыков, которыми должен обладать выпускник магистратуры, группировка их по модулям и дисциплинам;

– разработка основной образовательной программы магистерской подготовки;

– разработка учебного плана подготовки магистров по выбранной программе подготовки;

– разработка рабочих программ учебных дисциплин.

Рассмотрим, как работает такая методика, на примере формирования основной образовательной программы магистерской подготовки по программе «Аудит информационной безопасности автоматизированных систем», реализуемой в Национальном исследовательском университете Московском государственном институте электронной техники (МИЭТ).

На сегодняшний день автоматизированные системы (АС) играют ключевую роль в хранении, обработке и передаче информации как на коммерческих, так и на государственных предприятиях (учреждениях).

В последние годы значительно возросло число автоматизированных систем обработки информации ограниченного доступа, и прежде всего информационных систем обработки персональных данных. В настоящее время зарегистрировано более 187 тысяч операторов персональных данных. Подавляющее большинство из них находятся в Центральном федеральном округе.

Использование автоматизированных систем для обработки информации, применение новых информационных технологий значительно расширяют возможности деятельности организации (учреждения), но одновременно с этим создают новые операционные риски, что приводит к повышению актуальности проблем, связанных с защитой информации.

Федеральной службой по техническому и экспортному контролю (ФСТЭК России) выдано более 1400 лицензий на деятельность по технической защите конфиденциальной информации и более 800 лицензий на деятельность по разработке и/или производству средств защиты конфиденциальной информации.

Для того чтобы гарантировать эффективную защиту информации, компаниям необходимо иметь объективную оценку текущего уровня информационной безопасности АС. Именно для этих целей и применяется аудит информационной безопасности АС.

Услуга аудита информационной безопасности в настоящее время становится все более востребованной на рынке безопасности. Проведенный опрос руководящего состава нескольких десятков организаций, проводящих аудит информационной безопасности, показал, что существует острый дефицит квалифицированных кадров именно в этой области (на сегодняшний день ни один из вузов страны специалистов в области аудита информационной безопасности автоматизированных систем не готовит).

Работы, связанные с аудитом информационной безопасности и аттестационными испытаниями объектов информатизации, носят исследовательский характер и требуют высокого уровня подготовки специалистов во многих предметных областях. Поэтому подготовку таких специалистов целесообразно организовать именно в рамках магистратуры.

По предварительным оценкам ФСТЭК России, потребность в магистрах по данному направлению подготовки в государственных и коммерческих организациях и учреждениях составляет более 100 человек в год.

Проведенный анализ показал, что в организациях и фирмах, занимающихся аудитом информационной безопасности и аттестацией объектов информатизации, численность сотрудников

структурных подразделений данного профиля составляет от 3 до 15 человек. При этом потребность в магистрах по предлагаемой программе подготовки составляет 1—2 человека в год.

Следовательно, открытие подготовки магистров по программе «Аудит информационной безопасности автоматизированных систем» является весьма актуальным.

С целью формирования основной образовательной программы магистратуры по данной программе подготовки проведен анализ целей и задач аудита безопасности информационных автоматизированных систем (ИАС).

Главными целями проведения аудита безопасности ИАС являются:

- анализ рисков, связанных с возможностью осуществления угроз безопасности в отношении защищаемых ресурсов ИАС;
- оценка текущего уровня защищенности ИАС;
- оценка соответствия ИАС существующим стандартам в области информационной безопасности и защиты информации;
- выработка рекомендаций по внедрению новых и повышению эффективности существующих механизмов обеспечения безопасности ИАС.

В число дополнительных задач аудита могут также входить:

- разработка документов политики безопасности организации (концепции обеспечения безопасности информации, регламенты обеспечения безопасности информации, инструкции и другие организационно-распорядительные документы по вопросам обеспечения безопасности информации);
- участие в обучении пользователей и обслуживающего персонала ИАС вопросам обеспечения информационной безопасности;
- участие в разборе инцидентов, связанных с нарушением информационной безопасности, и другие.

В соответствии с ФГОС ВПО, выпускник по направлению подготовки 090900 «Информационная безопасность» с квалификацией (степенью) «магистр» должен обладать следующими профессиональными компетенциями [1]:

в области проектной деятельности способностью:

• понимать и анализировать направления развития информационно-коммуникационных технологий объекта защиты, прогнозировать эффективность функционирования систем информационной безопасности, оценивать затраты и риски, формировать стратегию создания систем информационной безопасности в соответствии со стратегией развития организации (ПК-1);

• проектировать сложные системы и комплексы управления информационной безопасностью с учетом особенностей объектов защиты (ПК-2);

• произвести и детально обосновать выбор структуры, принципов организации, комплекса средств и технологий обеспечения информационной безопасности объектов защиты (ПК-3);

• самостоятельно осваивать и адаптировать к защищаемым объектам современные методы обеспечения информационной безопасности, вновь вводимые отечественные и международные стандарты (ПК-4);

• разработать программы и методики испытаний, организовать тестирование и отладку программно-аппаратных, криптографических и технических систем и средств обеспечения информационной безопасности (ПК-5);

в области научно-исследовательской деятельности способностью:

• анализировать фундаментальные и прикладные проблемы информационной безопасности в условиях становления современного информационного общества (ПК-6);

• анализировать угрозы информационной безопасности объектов и разрабатывать методы противодействия им (ПК-7);

• осуществлять сбор, обработку, анализ и систематизацию научно-технической информации по теме исследования, выбор методик и средств решения задачи, разрабатывать планы и программы проведения научных исследований и технических разработок (ПК-8);

• проводить экспериментальные исследования защищенности объектов с применением современных математических методов, технических и программных средств обработки результатов эксперимента (ПК-9);

• оформлять научно-технические отчеты, обзоры, готовить публикации по результатам выполненных исследований, научные доклады (ПК-10);

в области научно-педагогической деятельности способностью:

• выполнять педагогическую работу в средних специальных и высших учебных заведениях в должностях преподавателя и ассистента под руководством ведущего преподавателя и профессора (доцента) по дисциплинам направления (ПК-11);

• разрабатывать методические материалы, используемые студентами в учебном процессе (ПК-12);

в области организационно-управленческой деятельности способностью:

• организовать работу коллектива исполнителей, принимать управленческие решения в условиях спектра мнений, определять порядок выполнения работ (ПК-13);

• организовать работу по совершенствованию, модернизации, унификации систем, средств и технологий обеспечения информационной безопасности в соответствии с правовыми нормативными актами и методическими документами ФСБ России, ФСТЭК России (ПК-14);

• разрабатывать проекты методических и нормативных документов, технической документации, а также предложения и мероприятия по реализации разработанных проектов и программ (ПК-15);

• организовать и выполнить работы по изготовлению, монтажу, наладке, испытанию и сдаче в эксплуатацию систем и средств обеспечения информационной безопасности (ПК-16).

По мнению работодателей, эти профессиональные компетенции не в полной мере отражают тот уровень знаний и умений, которыми должен обладать специалист в области аудита информационной безопасности автоматизированных систем.

Поэтому вузом введены новые профильные компетенции (ПКДВ), дополняющие профессиональные компетенции ПК-1, ПК-3, ПК-5, ПК-7, ПК-9, ПК-13, ПК-15:

– способен проводить экспертный анализ уровня защищенности автоматизированных систем обработки информации ограниченного доступа от различного вида угроз и оценку соответствия автоматизированных систем международным и отечественным стандартам и нормативно-методическим документам ФСБ России и ФСТЭК России в области информационной безопасности и защиты информации (ПКДВ-1);

– способен разрабатывать модели угроз информационной безопасности, проводить анализ рисков угроз информационной безопасности, разрабатывать документы политики информационной безопасности (ПКДВ-2);

– способен разрабатывать программы и методики аттестационных испытаний по оценке защищенности информации от утечки по техническим каналам и несанкционированного доступа к информации, проводить аттестационные испытания с использованием технических и программных средств, оформлять заключения по результатам аттестационных испытаний (ПКДВ-3).

Разработанные дополнительные профильные компетенции более понятны работодателям и отражают требования к уровню подготовки специалиста в области аудита информационной безопасности автоматизированных систем.

Сформированность каждой из дополнительных компетенций предполагает наличие у выпускника совокупности ряда взаимосвязанных знаний, умений и навыков.

Сформированность компетенции **ПКДВ-1** у магистра предполагает наличие:

- **знаний** систем и средств обработки информации ограниченного доступа, технических каналов утечки информации, способов и средств несанкционированного доступа к информации, способов и средств защиты информации от утечки по техническим каналам, способов и средств защиты информации от несанкционированного доступа, организации защиты информации на объектах информатизации, нормативных правовых актов, организационно-распорядительных и нормативно-методических документов по информационной безопасности и защите информации;
- **умений** провести оценку угроз информационной безопасности, оценку рисков информационной безопасности, оценку уровня защищенности автоматизированной системы от угроз безопасности информации;
- **владения навыками** проведения экспертного анализа уровня защищенности автоматизированной системы от угроз безопасности информации и экспертной оценки соответствия автоматизированной системы международным и отечественным стандартам и нормативно-методическим документам ФСБ России и ФСТЭК России в области информационной безопасности и защиты информации.

Сформированность компетенции **ПКДВ-2** у магистра предполагает наличие:

- **знаний** систем и средств обработки информации ограниченного доступа, технических каналов утечки информации, способов и средств несанкционированного доступа к информации, способов и средств защиты информации от утечки по техническим каналам, способов и средств защиты информации от несанкционированного доступа, организации защиты информации на объектах информатизации, нормативных правовых актов, организационно-распорядительных и нормативно-методических документов по информационной безопасности и защите информации;
- **умений** провести оценку угроз информационной безопасности, разработать модели угроз информационной безопасности, провести анализ рисков угроз информационной безопасности, разработать документы политики информационной безопасности (концепцию обеспечения безопасности информации, регламенты обеспечения безопасности информации, инструкции и другие организационно-распорядительные документы по вопросам обеспечения безопасности информации);
- **владения навыками** разработки модели угроз информационной безопасности, анализа рисков угроз информационной безопасности, разработки документов политики информационной безопасности.

Сформированность компетенции **ПКДВ-3** у магистра предполагает наличие:

- **знаний** систем и средств обработки информации ограниченного доступа, технических каналов утечки информации, способов и средств несанкционированного доступа к информации, способов и средств защиты информации от утечки по техническим каналам и несанкционированного доступа к информации, методов и средств контроля эффективности защиты информации от утечки по техническим каналам и защиты информации от несанкционированного доступа, организации защиты информации на объектах информатизации, организации аттестации объектов информатизации по требованиям безопасности информации;
- **умений** по организации аттестационных испытаний, по оценке защищенности информации от утечки по техническим каналам и несанкционированного доступа к информации, проведению аттестационных испытаний с использованием технических и программных средств, оформлению заключения по результатам аттестационных испытаний;

▪ **владения навыками** проведения аттестационных испытаний и оценки защищенности информации от утечки по техническим каналам и несанкционированного доступа к информации с использованием технических и программных средств.

Анализ профессиональных знаний, умений и навыков, которыми должен обладать выпускник, позволил объединить их вначале в темы и разделы (модули), а затем сформировать перечень дисциплин учебного плана. Для расчета объема каждой дисциплины учитывалось суммарное время, необходимое для формирования у студента предусмотренных данной дисциплиной представлений, знаний, умений и навыков. При этом использовались следующие нормы расхода времени:

- на формирование представлений, связанных с отдельными сравнительно простыми понятиями, — до 0,5 часа (в среднем 15—20 минут), а связанных с отдельными сложными понятиями или группой взаимосвязанных понятий — до 1 часа (в среднем 30—40 минут);
- на формирование аналогичных знаний (вместе с формированием необходимых представлений) соответственно 1,5—2 и 2,5—4 часа (в среднем от 60 до 120 минут);
- на формирование отдельных умений (вместе с формированием необходимых представлений и знаний) в зависимости от их содержания и сложности — от 4 до 8 часов (в среднем от 160 до 240 минут);
- на привитие отдельных навыков (вместе с формированием необходимых представлений, знаний и умений) в зависимости от их содержания и сложности — от 6 до 12 часов (в среднем от 240 до 320 минут).

Полнокровная тема в дисциплине (т. е. та, которая предусматривает формирование представлений, знаний, умений и навыков) должна иметь объем около 10—12 часов, другие темы могут быть меньшего объема.

Перечень дисциплин разработанной основной образовательной программы магистратуры по программе подготовки «Аудит информационной безопасности автоматизированных систем» приведен в таблице 1.

Для каждой компетенции разработаны структурно-логические схемы формирования профессиональных компетенций, которые легли в основу разработанного учебного плана подготовки магистров по программе «Аудит информационной безопасности автоматизированных систем».

Разработанный учебный план магистерской подготовки прошел экспертизу на факультете информационной безопасности Национального исследовательского ядерного университета «МИФИ», в ФСТЭК России и в УМО по образованию в области информационной безопасности и одобрен ими.

Начало подготовки магистров по программе подготовки «Аудит информационной безопасности автоматизированных систем» планируется с 1 сентября 2012 г.

Таблица 1. Перечень дисциплин основной образовательной программы магистратуры по программе подготовки «Аудит информационной безопасности автоматизированных систем»

Код	**Наименование учебной дисциплины (иной нагрузки)**	**Общая трудоемкость**	
		ЗЕТ	**Часы**
М.1	**Общенаучный цикл**	**23**	**828**
	Базовая часть	**8**	**288**
М.1.1	Специальные главы математики	2	72
М.1.2	Специальные главы физики	3	108
М.1.3	Экономика и управление	3	108
	Вариативная часть	15	540
М.1.4	Иностранный язык	4	144

Код	Наименование учебной дисциплины (иной нагрузки)	Общая трудоемкость	
		ЗЕТ	Часы
М.1.5	Педагогика высшей школы	3	108
	Дисциплины по выбору студента (2 из 4)	8	288
М.1.6.1	Современная философия и методология науки	3	108
М.1.6.2	Психологическая диагностика	3	108
М.1.7.1	Теория игр и исследование операций	5	180
М.1.7.2	Теоретические основы управления	5	180
М.2	**Профессиональный цикл**	**37**	**1332**
	Базовая часть	**10**	**360**
М.2.1	Защищенные информационные системы	5	180
М.2.2	Управление информационной безопасностью	5	180
	Вариативная часть	**27**	**972**
М.2.3	Технологии обеспечения информационной безопасности объектов	5	180
М.2.4	Организация аудита информационной безопасности автоматизированных систем	5	180
М.2.5	Аттестация объектов информатизации	5	180
М.2.6	Деловая игра	2	72
	Дисциплины по выбору студента (2 из 4)	**10**	**360**
М.2.7.1	Правовые основы аудита информационной безопасности	5	180
М.2.7.2	Отечественные и зарубежные стандарты в области информационной безопасности	5	180
М.2.8.1	Теоретические основы защиты информации от утечки по техническим каналам	5	180
М.2.8.2	Теоретические основы компьютерной безопасности	5	180
М.3	**Практика и научно-исследовательская работа**	**48**	**1728**
М.4	**Итоговая государственная аттестация**	**12**	**432**
	Общая трудоемкость основной образовательной программы	**120**	**4320**

СПИСОК ЛИТЕРАТУРЫ:

1. Федеральный государственный образовательный стандарт высшего профессионального образования по направлению подготовки 090900 «Информационная безопасность». Квалификация (степень) магистр. Утвержден приказом Министерства образования и науки Российской Федерации от 28 октября 2009 г. № 497. URL: http://www.edu.ru/db-mon/mo/Data/d_09/prm497-1.pdf.