

ПОДГОТОВКА КАДРОВ В ОБЛАСТИ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В РОССИИ

РЕКТОР ФГОБУ
ВПО «МОСКОВСКИЙ
ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ
СВЯЗИ И ИНФОРМАТИКИ»
Артем Сергеевич Аджемов



Интенсивное развитие и использование современных информационных технологий привели в настоящее время к серьезным качественным изменениям в экономической, социально-политической и духовной сфере общественной жизни. Человечество фактически переживает этап формирования нового информационного общества. Вместе с тем это приводит и к росту угроз национальной безопасности, связанных с нарушением установленных режимов использования информационных и коммуникационных систем, ущемлением конституционных прав граждан, распространением вредоносных программ, а также с использованием возможностей современных информационных технологий для осуществления враждебных, террористических и других преступных действий. Поэтому особую остроту сегодня приобретает проблема обеспечения информационной безопасности (ИБ).

Доктрина информационной безопасности Российской Федерации, утвержденная президентом страны 9 сентября 2000 года, констатирует, что информационная сфера, являясь системообразующим фактором жизни общества, активно влияет на состояние политической, экономической, оборонной и других составляющих безопасности России. При этом в качестве одного из приоритетных направлений государственной политики в области обеспечения ИБ определяется совершенствование подготовки кадров, развитие образования в этой сфере.

Если рассматривать сегодняшнее состояние кадрового обеспечения ИБ, то следует отметить, что данный вопрос к настоящему времени применительно к защите информации имеет в стране достаточно серьезную практическую реализацию и некоторые теоретико-методологические обобщения. На сегодняшний день уже около 20 лет функционирует организованная система подготовки молодых и повышения квалификации работающих специалистов по защите информации.

Дальнейшая задача в этой области заключается в создании четкой государственной системы прогнозирования потребности в специалистах, разработке методологии формирования государственного заказа на их подготовку, развитии новых направлений и образовательных программ подготовки кадров, учитывающих принципиально междисциплинарный характер данной области деятельности. Более того, обучение основам ИБ и защиты информации должно стать инвариантной составляющей информационной подготовки в рамках всех без исключения специальностей и направлений профессионального образования, служащей формированию информационной культуры личности на этапе перехода к постиндустриальному обществу. Решение всех этих задач должно быть основано на системном подходе, учитывающем методологические, организационные, содержательные, дидактические и технологические аспекты.

Некоторые подходы к решению наиболее острых проблем, стоящих сегодня перед системой кадрового обеспечения ИБ, и являются предметом настоящей статьи.

ИЗ ИСТОРИИ ВОПРОСА

Исторически можно выделить четыре этапа развития системы подготовки кадров по проблемам ИБ в Российской Федерации:

– 1-й этап (1991–2005 годы) хронологически совпадает с формированием государственных стандартов высшего профессионального образования первого и второго поколения. Основой этого эта-

на явились результаты работы по формированию в 1990-х годах нового направления подготовки кадров в области обеспечения ИБ. На данном этапе были разработаны квалификационные характеристики специалистов по защите информации, учебные планы и программы для различных специальностей, прогноз потребности в подготовке специалистов на период до 2010 года. В результате были сформированы все предпосылки к созданию в стране единой межведомственной системы подготовки, повышения квалификации и переподготовки специалистов на основе концепции непрерывного обучения.

– 2-й этап (2005–2010 годы) был посвящен формированию содержания образовательных программ подготовки специалистов различных квалификационных уровней на основе компетентностного подхода, разработке моделей методической системы обучения на основе комплексной информационно-образовательной среды. Были разработаны также основные подходы к формированию рабочих программ общепрофессиональных и специальных дисциплин в рамках направления «Информационная безопасность» для студентов вузов, содержание лекций, практических и лабораторных занятий на основе комплексной информационно-образовательной среды.

– 3-й этап (2011–2013 годы) был посвящен в основном решению вопросов развития информационной культуры общества, и прежде всего культуры информационной безопасности. Были исследованы вопросы этики в сфере информационных технологий, разработаны содержательные основы курса «Гуманитарные проблемы информационной безопасности», сформирована концепция общеобразовательного курса «Основы информационной культуры», рассматривающая ее как ключевой элемент в становлении и развитии умений и навыков членов нового информационного общества, в обеспечении безопасного функционирования информационной среды и инфраструктуры. Работы в этом направлении продолжаются и сегодня. Таким образом, можно говорить, что третий этап развития системы кадрового сопровождения проблемы ИБ еще не завершен.

СОВРЕМЕННОЕ СОСТОЯНИЕ ПОДГОТОВКИ КАДРОВ В ОБЛАСТИ ИБ

Сегодня подготовка кадров в области ИБ имеет существенные особенности, поскольку выступает не только как реакция на спрос рынка в отношении таких специалистов, но и как важная составляющая комплекса мероприятий государства по противодействию угрозам в информационной сфере. Этими особенностями определяются и содержание подготовки указанных специалистов, и особые требования, предъявляемые к об-

разовательным учреждениям при организации такой подготовки.

В общей системе обеспечения ИБ государства кадровое сопровождение является самостоятельной подсистемой, а сама система подготовки специалистов выступает в качестве основы такого сопровождения. Поэтому под подготовкой кадров в области ИБ будем понимать систему, включающую все уровни профессионального образования, переподготовки и повышения квалификации специалистов.

Можно отметить следующие принципы развития системы подготовки кадров в области ИБ, которые дополняют общие принципы функционирования и совершенствования профессионального образования:

- строгое соблюдение законодательства Российской Федерации в области национальной безопасности, общепризнанных норм международного права при подготовке кадров в области ИБ;
- тщательный подбор кадров (это относится как к обучаемым, так и к тем, кто ведет подготовку по образовательным программам в сфере ИБ);
- гармоничное сочетание интересов личности, общества и государства (в виде государственного заказа) при подготовке кадров в области ИБ;
- рациональное ограничение числа вузов, осуществляющих подготовку специалистов в области ИБ;
- государственная поддержка ведущих вузов страны, научно-педагогических коллективов, осуществляющих подготовку специалистов в области ИБ для государственного сектора экономики и системы государственного и муниципального управления;
- комплексное и гармоничное развитие специальностей и содержания подготовки в различных областях наук, включая естественно-научные, технические и гуманитарные;
- самостоятельность группы специальностей и направлений подготовки в области ИБ;
- единство систем подготовки кадров в области ИБ и информационных технологий;
- системность в подготовке кадров, предусматривающую учет междисциплинарного характера проблемы ИБ, изучение влияния на ИБ как внутренних, так и внешних возмущающих факторов, а также использование всей совокупности алгоритмических, криптографических, программно-аппаратных, инженерно-технических, физических, организационных, правовых и морально-этических методов защиты информации;
- преемственность содержания образовательных программ различных поколений;
- сопряженность образовательных программ различных уровней и ступеней профессионального образования (среднее, высшее, послевузовское, дополнительное).

Стоит отметить, что к настоящему времени в России сложились основы дееспособной системы подготовки и повышения квалификации специалистов, способных решать задачи обеспечения ИБ страны. Немаловажно и то, что российская система подготовки кадров в облас-



ти ИБ занимает по ряду позиций ведущее положение, по крайней мере среди европейских стран, о чем свидетельствуют материалы регулярно проводимой Международной конференции по образованию в области информационной безопасности (World Conference Information Security Education). На сегодняшний день эта система включает в себя следующие составляющие:

- пять федеральных государственных образовательных стандартов (ФГОС) высшего профессионального образования и разработанных на их базе основных образовательных программ подготовки специалистов в области ИБ по специальностям: «Компьютерная безопасность», «Информационная безопасность автоматизированных систем», «Информационная безопасность телекоммуникационных систем», «Информационно-аналитические системы безопасности», «Безопасность информационных технологий в правоохранительной сфере»;
- два ФГОС высшего профессионального образования по направлению «Информационная безопасность» (подготовка бакалавров и магистров);
- три ГОС среднего профессионального образования по специальностям: «Информационная безопасность телекоммуникационных систем», «Информационная безопасность автоматизированных систем», «Организация и технология защиты информации»;
- образовательные программы дополнительного образования и соответствующие курсы переподготовки и повышения квалификации;
- образовательные программы послевузовского профессионального образования в данной области (подготовка кадров высшей квалификации по специальности «Методы и системы защиты информации, информационная безопасность»);
- учебно-методическое объединение вузов России по образованию в области ИБ;
- более 150 вузов России (государственных и негосударственных), которые готовят специалистов по указанным специальностям;
- 29 региональных учебно-научных центров по проблемам ИБ в системе высшей школы.

На российском ИТ-рынке специализированную подготовку в области обеспечения ИБ осуществляют также учебные центры повышения квалификации, для которых это направление является приоритетным (АНО ДПО «Информзащита», АНО «Эшелон», Domina Security и др.), а также образовательные центры в области ИТ и телекоммуникаций (НОУ ДПО «Институт «АйТи», школа информационных технологий CNews, НОУ ДПО «ЦПК «АИС», ОЧУ «Специалист», НОУ УЦ «Сетевая академия» и др.).

Анализ стандартов, образовательных программ и траекторий для специальностей и направлений подготовки группы «Информационная безопасность» позволяет сформулировать следующие общие выводы:

- Для специальностей группы (далее – специальности ИБ) явно выражена общность структур общепрофессионального цикла дисциплин, что под-

тверждает их общую идеологию, необходимость их дальнейшего развития в рамках единой организационной структуры. Это основной принцип формирования специальностей ИБ. Он отличается от используемых при формировании других групп.

- Характерным для специальностей ИБ является наличие в блоке общепрофессиональных дисциплин групп дисциплин, ориентированных на изучение тех или иных методов и средств обеспечения ИБ. Общий объем указанных дисциплин для различных специальностей ИБ составляет до 1,5 тыс. часов, а в среднем 32% от объема блока общепрофессиональных дисциплин.
- Цикл общепрофессиональных дисциплин специальностей ИБ базируется на достаточно специализированном естественно-научном цикле. Так, по сравнению с родственными ГОС в области техники и технологии естественно-научный цикл для специальностей, закрепленных за УМО ИБ, отличается большим объемом (на 300–800 часов) и существенной дискретно-математической составляющей, включающей дополнительно две дисциплины объемом 300–500 часов.
- В каждом ГОС в общепрофессиональном и естественно-научном циклах имеется блок дисциплин, отражающих специфику предметной области подготовки специалистов, соответствующей профилю их профессиональной деятельности. Это отличие в содержании образовательной программы для различных специальностей ИБ составляет 1–1,6 тыс. часов, или примерно 25–35% от объема блоков общепрофессиональных естественно-научных дисциплин.
- ГОС каждой специальности ИБ предполагает специализацию в объеме 0,7–1,5 тыс. часов.
- В качестве траектории образования реализуется как подготовка дипломированных специалистов, так и подготовка бакалавров и магистров по направлению «Информационная безопасность».

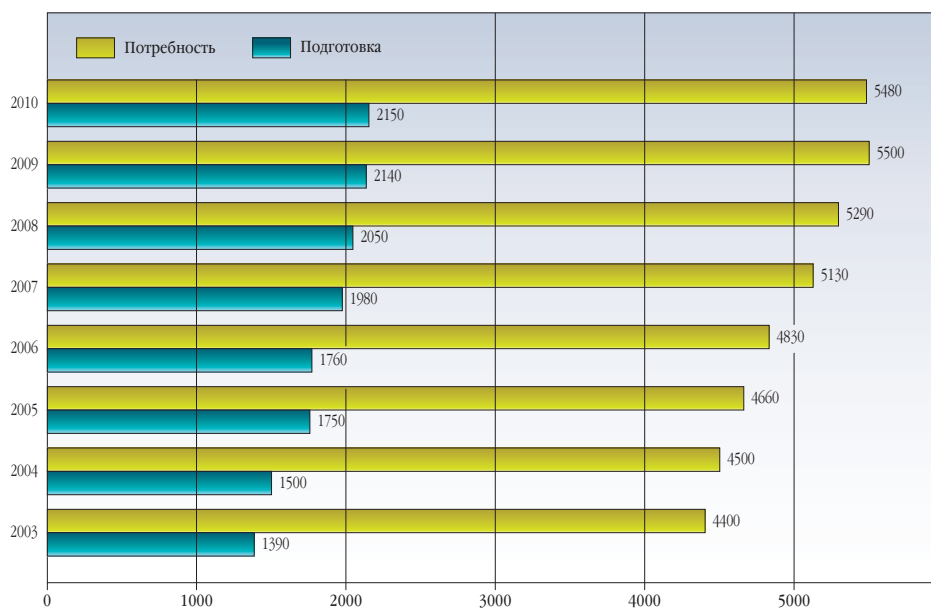
Таким образом, из анализа приведенной информации можно заключить, что задача кадрового обеспечения области ИБ решается в двух основных направлениях:

- подготовка специалистов с высшим и средним профессиональным образованием;
- дополнительное образование – повышение квалификации и переподготовка кадров.

Зададимся далее вопросом: сколько же специалистов такого профиля необходимо для эффективного функционирования отраслей экономики? Здесь следует отметить, что как в России, так и за рубежом потребители высказывают неудовлетворенность количеством подготавливаемых специалистов. Действительно, анализ различных оценок потребности в специалистах, сравнение их с прогнозами развития систем подготовки кадров ясно показывают, что реальная и прогнозируемая ежегодная дополнительная потребность в таких специалистах значительно превосходит суммарный выпуск всех вузов, осуществляющих данную подготовку. Иллюстрацией этого может служить прогноз потребности и выпуска



1



ПРОГНОЗИРУЕМАЯ ПОДГОТОВКА СПЕЦИАЛИСТОВ ПО ГРУППЕ СПЕЦИАЛЬНОСТЕЙ «ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ» И ПОТРЕБНОСТЬ В НИХ

специалистов, проводившийся по заданию Министерства образования Российской Федерации в 2003 году. Его результаты представлены на рисунке 1.

Интересные результаты дает анализ распределения этой потребности. Так, если в 2001 году она составляла 2550 человек, то соответствующий показатель на 2003 год возрос до 4400, то есть более чем в 1,7 раза. Это свидетельствует, что в ближайшей перспективе сфера информационной безопасности будет испытывать жесточайший кадровый голод, что является сегодня сильнейшим стимулятором развития подготовки специалистов по защите информации.

Приведенные тенденции сохраняются и в более поздних прогнозах, что подтверждается, например, результатами прогнозирования потребности, проводившегося в 2010 году. Так, при прогнозируемой дополнительной потребности в специалистах по специальности «Информационная безопасность автоматизированных систем» в 2015 году примерно в 1,5 тыс. человек ожидаемый суммарный выпуск из вузов не превышает 700 человек.

Совершенно очевидно, что решить проблему нехватки специалистов по ИБ с помощью только подготовки новых кадров с высшим и средним профессиональным образованием практически невозможно. Основные причины этого:

- большой временной интервал процесса подготовки;
- явно недостаточное количество выпускаемых специалистов (среднее количество специалистов в области ИБ, выпускаемых в год высшими учебными заведениями страны, оценивается примерно в 1,7 тыс. человек, тогда как лишь государственным учреждениям ежегодно требуется порядка 1,5 тыс. человек);
- инерционность обучения, связанная с долговременной (в пределах одного цикла обучения) ста-

бильностью учебных программ и планов (за это время требования к содержанию обучения существенно изменяются);

- сложность организации целевой подготовки специалистов в интересах конкретного предприятия (к сожалению, в настоящее время не каждая организация может сформулировать требования к уровню знаний и умений специалиста в области ИБ);
- сложности с профессиональной ориентацией поступающих на обучение из-за проблем с реализацией принципа тщательного отбора кадров, обучающихся по специальностям и направлениям подготовки в области ИБ.

Последнее имеет очень важное значение. В то же время при существующей системе подготовки предполагается обучение молодых людей в возрасте 17–18 лет. Даже если кроме проверки знаний устраивать проверку психофизиологических характеристик (возможность практической реализации этого весьма сомнительна), то это вряд ли обеспечит эффективность отбора, так как за длительное время обучения данные параметры могут кардинально поменяться. Кроме того, выпускники могут пойти работать не по специальности или, что еще хуже, будут выполнять функции, противоположные защите.

В этой связи представляется, что приоритетное развитие в области кадрового обеспечения ИБ в ближайшей перспективе должно получить дополнительное образование. Среди несомненных достоинств этой формы обучения можно отметить малую длительность подготовки, гибкость учебных программ, простоту реализации целевой подготовки в интересах конкретного предприятия, возможность наиболее полного удовлетворения потребности в специалистах различного уровня квалификации. Однако здесь требуется дифференцированный подход



к обучению, учитывающий различные категории обучаемых. Следует также соблюдать принцип, заключающийся в том, что специалист должен знать и уметь только то, что ему положено знать и уметь. Если не следовать этому принципу, то знания и умения могут привести к возникновению у специалиста амбиций, влекущих несанкционированные действия по собственному желанию или под влиянием внешних факторов. Учитывая характер знаний и навыков у специалистов в области ИБ, можно сделать вывод, что знания в этой области должны получать только те, кому это необходимо, а круг обучаемых определяется исключительно предприятием, тем самым и реализуется целевой характер дополнительного образования. И, естественно, необходимо обеспечить информационную безопасность самой системы обучения (в первую очередь содержания подготовки).

Из изложенного выше становится совершенно очевидной первостепенная роль государственного регулирования подготовки, переподготовки и повышения квалификации кадров в области ИБ. Нельзя не отметить, что механизмы такого регулирования в полной мере еще не выработаны. Особенно это относится к механизму формирования государственного заказа на подготовку.

Следовательно, система подготовки кадров в области ИБ должна выглядеть как корпоративная система обучения, решающая задачу подготовки специалистов при соблюдении определенных ограничений, что должно быть учтено при управлении такой системой.

На наш взгляд, механизм государственного регулирования должен включать следующие элементы:

- определение контрольных цифр приема и формирование государственного кадрового заказа, особенно в интересах федеральных органов исполнительной власти;
- поддержку функционирования и дальнейшее развитие группы направлений и специальностей в области ИБ;
- разработку ГОС и образовательных программ при активном участии потребителей этих специалистов;
- мониторинг использования специалистов в области ИБ;
- финансовое и материально-техническое обеспечение подготовки специалистов;
- издание и использование в образовательном процессе учебно-методической литературы, прошедшей экспертизу в соответствующих ведомствах;
- совершенствование порядка лицензирования и контроля образовательной деятельности в области ИБ;
- аттестацию и подготовку соответствующих педагогических кадров.

ДОПОЛНИТЕЛЬНОЕ ОБРАЗОВАНИЕ

Из предыдущего изложения становится ясной чрезвычайно важная роль дополнительного образования в удовлетворении потребности в специалистах по защите информации. Однако в области повышения квалификации и переподготовки кадров в настоящее время

явно недооценивается роль государства в координации образовательной деятельности. Многие ниши в системе дополнительного образования сегодня в значительной степени заняты коммерческими фирмами, программы обучения которых преимущественно направлены на первичную подготовку пользователей конкретных продуктов и зачастую носят откровенно рекламный характер. Определенные результаты достигнуты в обеспечении единства требований и контроля качества обучения в системе переподготовки в области защиты государственной тайны. Распространить сформированный при этом нормативный механизм на систему переподготовки по общим вопросам ИБ представляется не только возможным, но и наиболее рациональным. Наибольший интерес в этой области представляет опыт региональных учебно-научных центров по проблемам ИБ в системе высшей школы. Они работают уже достаточно долго, провели обучение по множеству разнообразных программ.

Важным является вопрос о послевузовском образовании, в частности о взаимосвязи научных специальностей с приоритетными направлениями научных исследований в области обеспечения ИБ Российской Федерации.

В настоящее время послевузовское образование в области ИБ осуществляется в рамках нескольких научных специальностей, имеющих различное, иногда достаточно поверхностное отношение к этой тематике. Единственная специальность «Методы и системы защиты информации, информационная безопасность» охватывает все важнейшие проблемы этой сферы деятельности и предусматривает защиту докторских и кандидатских диссертаций в рамках двух отраслей наук – физико-математических и технических. Все специальности высшего профессионального образования направления «Информационная безопасность» имеют сопряжение с данной научной специальностью. По ней имеется несколько утвержденных паспортов. Большая часть из них посвящена техническим вопросам обеспечения ИБ.

СРЕДНЕЕ ПРОФЕССИОНАЛЬНОЕ ОБРАЗОВАНИЕ

Опыт рассмотрения заявок на лицензирование специальностей группы «Информационная безопасность», обоснований, представляемых вузами и местными органами власти, обращение к опыту разработки и эксплуатации государственных защищенных информационных систем показывают, что очень многие задачи, упоминаемые в обоснованиях необходимости подготовки специалистов по защите информации, могут решать сотрудники среднего технического звена. Обеспечение защиты информации как объект профессиональной деятельности, наряду с организационно-управленческими, проектными и аналитическими составляющими, разработкой математических методов и алгоритмов, созданием программных и аппаратных средств защиты, построением сложных комплексных систем, включает в себя и технологическую деятельность, для которой во многих случаях не требуется высшее профессиональное образование, но в то же время необходимы профессиональные знания и умения. При этом объем такой деятельности



значительно превышает объем организационно-управленческой, проектно-конструкторской и аналитической деятельности, а также объем работы по созданию математической и аппаратной базы.

В связи с этим в качестве первого шага в решении проблемы формирования образовательной области «Информационная безопасность» в рамках среднего профессионального образования, как указывалось выше, разработано три стандарта, предусматривающих следующие направления профессиональной деятельности:

- «Организационное обеспечение защиты информации» (место работы выпускника – подразделения обеспечения ИБ предприятий и организаций различных профилей и форм собственности);
- «Эксплуатация и обслуживание технических средств защиты информации» (место работы выпускника – подразделения, обеспечивающие развертывание и эксплуатацию компьютерных систем, обрабатывающих конфиденциальную информацию);
- «Эксплуатация защищенных автоматизированных систем» (место работы выпускника – подразделения обеспечения ИБ, а также любые структуры, связанные с использованием технических средств обработки, хранения и передачи конфиденциальной информации);
- «Защищенные телекоммуникационные системы» (место работы выпускника – подразделения, обеспечивающие развертывание и эксплуатацию сложных телекоммуникационных систем, в которых циркулирует конфиденциальная информация).

Таким образом, данные стандарты предусматривают подготовку специалистов для профессиональной деятельности по защите информации, обслуживанию и эксплуатации систем и средств обеспечения ИБ в качестве техника в организациях (на предприятиях) различной отраслевой направленности независимо от их организационно-правовых форм. Нормативный срок обучения при очной форме подготовки на базе среднего (полного) общего образования составляет 2 года 10 месяцев. Внедрение данных стандартов, вместе со стандартами высшего и дополнительного профессионального образования, создает необходимые условия для формирования полноценной системы непрерывного образования в области обеспечения информационной безопасности.

ЗАРУБЕЖНЫЙ ОПЫТ ПОДГОТОВКИ КАДРОВ

Учитывая международный характер проблем обеспечения ИБ, полезно будет также использовать при дальнейшем развитии российской системы подготовки соответствующих кадров имеющийся мировой опыт в этой области.

Кратко рассмотрим, как решается проблема подготовки кадров в области обеспечения ИБ в других странах, и прежде всего в США. Важно отметить, что в этой стране на протяжении последних

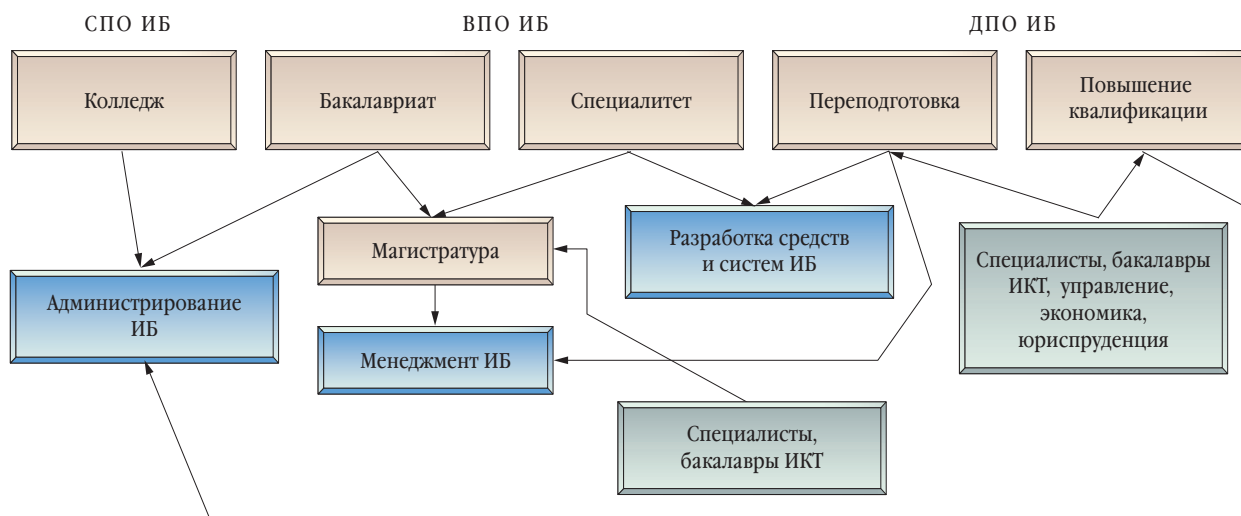
10–15 лет чрезвычайно большое значение придается привлечению к проблеме ИБ широкого общественного внимания. В 1998 году здесь был создан Национальный центр защиты инфраструктуры (National Infrastructure Protection Center), задачей которого является предотвращение, сдерживание, реагирование и расследование преступлений, направленных против стабильности национальной информационной инфраструктуры. Примерно в тот же период была создана Международная ассоциация специалистов по компьютерным исследованиям (The International Association of Computer Investigative Specialists), которая занимается обучением в области компьютерно-технической экспертизы. В конце 2009 года был создан Национальный центр кибербезопасности (National Cybersecurity and Communications Integration Center), призванный помочь государству в разработке подходов к решению проблем обеспечения ИБ, повысить уровень образования в этой сфере, а также координировать все национальные системы сетевой защиты. Сотрудники данного центра занимаются мониторингом и предупреждением различного рода компьютерных атак.

Отдельно отметим компании, проводящие обучение в области обеспечения ИБ. Среди них следует выделить: Check Point Software Technologies, Cisco Systems, Microsoft, IBM Tivoli Systems Global Security Laboratory, International Information Systems Security Certification Consortium, Internet Security Systems, Network Associates, Symantec. Кроме упомянутых частных компаний, подготовку специалистов в области ИБ осуществляют и государственные структуры: аспирантура Военно-морской академии США предлагает 12 различных курсов, Агентство по защите информационных систем (Defense Information Systems Agency, DISA) – 8 курсов. Активно участвует в этой работе и колледж управления информационными ресурсами (Information Resource Management College). Для совершенствования методов обучения в министерстве обороны США создано специальное подразделение по управлению программами в области обеспечения ИБ (Information Assurance Program Office). Агентством национальной безопасности (National Security Agency, NSA) около 10 лет назад был сформирован ряд центров послевузовского образования, к которым позже подключили 14 ведущих университетов США. Одновременно Белый дом приступил к обучению правительственных чиновников (до 10 тыс. человек ежегодно) в рамках федеральной программы обеспечения безопасности ИТ. После трагедии, произошедшей 11 сентября 2001 года, во многих американских городах начали усиленно проводиться семинары, конференции, встречи по проблемам киберпреступности и кибертерроризма.

Не рассматривая подробно структуру подготовки специалистов в области обеспечения ИБ в США, тем не менее можно сделать вывод, что существующая здесь сеть подготовки специалистов достаточно развита. Но даже при таких масштабах, по мнению экспертов, в США ощущается нехватка квалифицированных специалистов данного профиля.



2



СИСТЕМА ПОДГОТОВКИ И ПЕРЕПОДГОТОВКИ КАДРОВ ПО ИБ

Используют США и способ подготовки кадров через международные консорциумы. Мировым лидером сертификации специалистов по ИБ является Международный консорциум по сертификации в области безопасности информационных систем (International Information Systems Security Certification Consortium, Inc., или (ISC)²). Для получения сертификата Certified Information Systems Security Professional (CISSP) необходимо иметь опыт работы по специальности не менее 4 лет (или 3 года и степень бакалавра), сдать непростой экзамен, следовать кодексу этики (ISC)² и постоянно поддерживать свою квалификацию. Для подтверждения сертификации CISSP достаточно каждые 3 года проходить обучение на авторизованных курсах по ИБ, а также принимать участие в конференциях по этой теме. Следует отметить еще решения компании Cisco, создавшей образовательный проект «Сетевая академия Cisco», осуществляемый совместно образовательными учреждениями и компанией. Вначале планировалось выпускать квалифицированных специалистов по обслуживанию сетей, но в дальнейшем академия приобрела известность и как мощный центр по подготовке специалистов в области защиты информации.

НЕКОТОРЫЕ ВЫВОДЫ

Во-первых, совершенно очевидно, что удовлетворить потребность в высококвалифицированных специалистах в области обеспечения ИБ можно только на

основе комплексного использования всех возможностей среднего, высшего и дополнительного профессионального образования. Именно сочетание всех этих форм позволяет построить единую стройную систему подготовки кадров на основе непрерывности образовательного процесса и удовлетворить широкий спектр предъявляемых потребителями требований как в содержательном, так и в квалификационном аспекте. При этом взаимодействие этих систем, по нашему мнению, может выглядеть так, как показано на рисунке 2.

Во-вторых, необходимо отметить, что на сегодняшний день фактически нетронутым остается такой пласт, как подготовка кадров в области второй составляющей ИБ – защиты личности и общества от разрушающего воздействия информации.

Справедливости ради надо сказать, что вторая составляющая ИБ гораздо сложнее, неопределеннее первой, что порождает особые трудности при решении соответствующих задач. Кроме того, обеспечение сколько-нибудь эффективной защиты от негативной информации возможно лишь при наличии развитой законодательной и нормативно-правовой базы, процесс создания которой в России еще далеко не завершен.

Таким образом, в свете реализации положений доктрины информационной безопасности и стратегии развития информационного общества в Российской Федерации стоит достаточно сложная задача – создать образовательные траектории по подготовке специалистов в области ИБ в ее гуманитарной составляющей.