Н. Г. Милославская (к. т. н., доцент)
Московский инженерно-физический институт (государственный университет)

ПОДГОТОВКА СПЕЦИАЛИСТОВ ПО ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ: МЕЖДУНАРОДНЫЙ ОПЫТ

Введение

Проблемы обеспечения информационной безопасности (ИБ) в сетевых средах — сначала Интернете, а затем и на уровне корпораций в интранете — в настоящее время стали интернациональными. Каждая страна, поддерживая национальную безопасность, решает вопросы борьбы с киберпреступниками своими средствами. В то же время ощущается потребность в выработке единых подходов к обучению безопасной работе в современных сетях, строящихся на основе Интернет-технологий. В современных условиях комплексный подход к решению задач обеспечения ИБ в различных организациях требует наличия как самих технологий, методов, средств и систем защиты, включая процесс обеспечения ИБ и управление им, так и специалистов с соответствующими знаниями и навыками. Известные в мире ИБ консорциум (ISC)2 и аналитическая организация IDC еще четыре года назад составили прогноз, согласно которому в 2008 г. потребность в высококвалифицированных специалистах в области ИБ в мировом масштабе возрастет до 2,1 млн. (прирост около 60 % по сравнению с 2004 г.). В этих целях интересно использование передового опыта, накопленного учебными заведениями мира в области подготовки кадров по проблемам ИБ. Многое зависит от уровня подготовленности преподавательского состава, работающего в данном направлении. Также немаловажно взаимодействие высшей школы с теми, кто является непосредственными потребителями специалистов указанного профиля, т. е. с различными государственными и коммерческими структурами. Все перечисленное неоценимо для совершенствования учебного процесса, поскольку оно позволит расширить учебно-методическую и лабораторную базу и готовить специалистов, отвечающих мировым стандартам.

1998 стал годом, с которого началось активное участие факультета «Информационная безопасность» МИФИ в международной деятельности в области подготовки кадров по ИБ. Здесь можно выделить несколько направлений, имеющих отношение к учебной и научной деятельности:

1) обучение различным аспектам обеспечения ИБ и обмен опытом в этой сфере;

2) участие в конференциях по фундаментальным исследованиям в области защиты информационных и сетевых технологий;

3) применение передовых дистанционных технологий обучения и тестирования знаний;

4) сотрудничество с иностранными фирмами, имеющими свои представительства в Москве (сегодня в числе наших партнеров фирмы Microsoft, Sun Microsystems, Cisco, Informix, Oracle, Computer Associates, Sybase и Digital Security).

Остановимся подробнее на первых двух направлениях.

1. Международные конференции по обучению ИБ

С 1999 г. мировое сообщество осознало необходимость координации усилий в области подготовки кадров по ИБ и провело в Швеции первую международную конференцию по обучению ИБ WISE1 (World Conference on Information Security Education), которая теперь стала традиционной и организуется каждые два года. После этого принимали участников WISE Австралия, США и Россия. Сравнительная таблица по участникам из различных стран и докладов, представленных на конференциях, приведена на рис. 1.

Сотрудники факультета «Информационная безопасность» с 2001 г. входят в состав программных комитетов всех конференций WISE и рабочей группы WG 11.8 Международной федерации по обработке информации IFIP («Образование в области информационной безопасности»), образованной в 1960 г.

под патронажем ЮНЕСКО (http://www.ifip.or.at). С 2003 г. по настоящее время автор настоящей статьи является заместителем председателя WG 11.8.

В 2005 г. МИФИ был основным организатором WISE4. Это важное событие было поддержано Министерством образования и науки РФ и Фондом поддержки и развития образования РФ. Кроме России, были представлены 15 стран мира: Австралия, Белоруссия, Великобритания, Германия, Греция, Ирландия, Корея, Словения, Швейцария, Швеция, США, Танзания, Франция, Чехия и Южно-африканская республика. Были заслушаны 39 докладов, 13 из них были подготовлены учебными заведениями Москвы, Санкт-Петербурга, Таганрога и Воронежа. Также в работе конференции приняли участие представители аппарата Совет Безопасности РФ, Федеральной службы по техническому и экспортному контролю, Ассоциации российских банков и организаций, известных на рынке продуктов и услуг в области обеспечения ИБ (МАСКОМ, Информзащита, ВНИИПВТИ, Элвис+, Computer Associates).

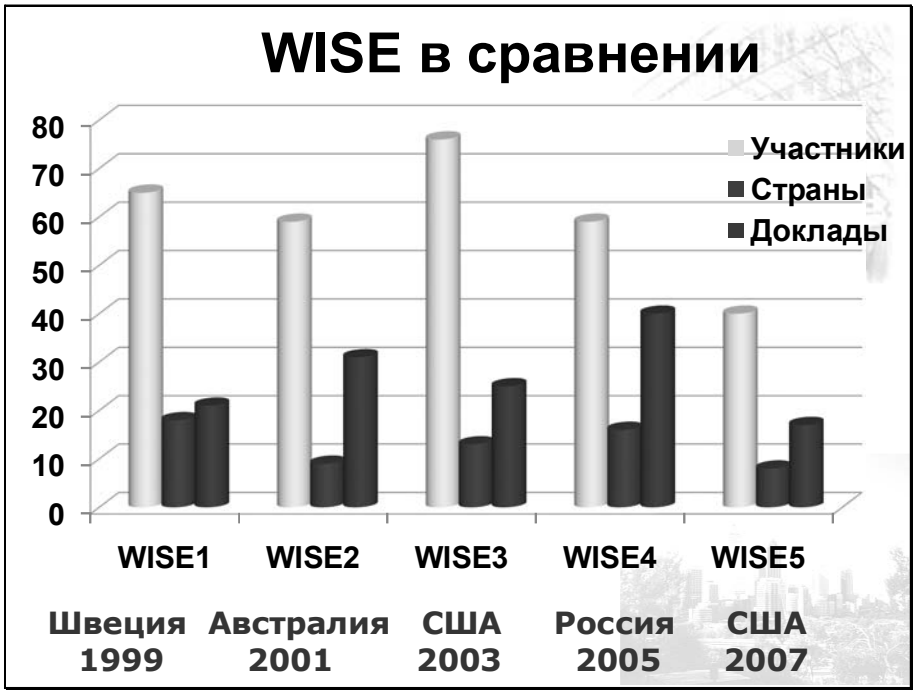

Рис. 1. Конференции WISE в сравнении

Очередная конференция WISE5 прошла в США в июне 2007 г. на базе Военной академии West Point. Участниками были представители Австралии, Великобритании, Греции, Норвегии, России, США, Швеции и ЮАР. Были опробованы три формы проведения заседаний: пленарные заседания (на них было представлено 17 докладов), заседания рабочих групп по секциям и доклады приглашенных выступающих (их было 3).

Выступления на всех конференциях сводятся к следующим общим темам:

· международные стандарты в области обучения ИБ;

· учебные планы и программы академического уровня;

· практические подходы к обучению ИБ;

· связь образования и промышленности, вовлечение практиков в процесс обучения;

· учебно-методическое обеспечение обучения;

· обучение отдельным вопросам (криптографии, компьютерной этике, форензике, правовым аспектам, аудиту безопасности, культуре безопасности и т. п.);

· применение дистанционного обучения и обучения с применением Web-технологий;

· оценка качества обучения.

Следующую конференцию WISE6 планируется провести в рамках ежегодного компьютерного конгресса IFIP в 2009 г. в Бразилии.

Основные выводы, которые можно сделать на основе опыта WISE:

1) созданы условия для обмена опытом по подготовке кадров в области ИБ. Базой для этого является деятельность рабочей группы WG 11.8 федерации IFIP, в частности международные конференции WISE;

2) среди стран, преуспевших в подготовке кадров по ИБ, можно выделить Австралию, государства Европейского сообщества, Россию и США;

3) процесс подготовки кадров по ИБ находится под пристальным вниманием международных и государственных организаций.

2. Сотрудничество при обучении ИБ

Примеры сотрудничества стран-участников ЕС по обучению ИБ — это проекты TEMPUS (Трансъевропейская программа мобильности в сфере высшего образования), ERASMUS/SOCRATES (программа действий ЕС по реализации политики ЕС в области образования и поддержке мобильности студентов университетов) и LEONARDO (программа действий по реализации политики ЕС в области профессиональной подготовки). Например, в программу ERASMUS/SOCRATES вовлечены 25 стран — участников ЕС плюс Исландия, Норвегия, Лихтенштейн, Румыния, Болгария, Турция. Основная ее цель — улучшить качество обучения на базе высшего образования за счет широкого обмена студентами и преподавателями; совместной разработки учебных программ; «языковых» курсов; разработки специализированных тематических сетей; подготовительных визитов; системы кредитов (European Credit Transfer System) и применения дистанционных форм обучения. В качестве основной цели на период 2000—2010 г. определено создание единого европейского образовательного пространства.

Важно отметить и предоставление ЕС финансовой поддержки развитию сотрудничества в области высшего образования и науки как между странами ЕС, так и в более широком европейском контексте.

Конкретным результатом осуществления программы межуниверситетской кооперации по обучению ИБ, кроме грантов и подготовки кадров высшей квалификации, являются летние и зимние школы под названием «Европейская интенсивная программа “Безопасность информационных и коммуникационных технологий”» (European Intensive Programme on Information and Communication Technologies Security, IPICS).

Первая летняя школа IPICS состоялась в 1998 г. в Вене, после чего она проходила в Греции, Швеции, Испании, Австрии, Бельгии и Великобритании. В 2008 г. планируется проведение IPICS в Германии, а на следующий год — опять в Австрии.

Зимние школы IPICS с 2000 г. проходят в Финляндия в апреле, что не позволяет российским студентам участвовать в них — они заняты в своем учебном процессе.

По программе IPICS обучаются студенты и аспиранты из ЕС, занимающиеся тематикой, связанной с ИБ. К сожалению, Россия пока не участвует полноправно в этом процессе. Но благодаря установленным связям с 2002 г. российские студенты стали участвовать в летних школах. В рамках каждой школы обучается порядка 30—40 слушателей из Австрии, Великобритании, Германии, Греции, Испании, Ирландии, Финляндии, Швеции, а с 2005 г. даже ЮАР. В летней школе в 2002 г. впервые приняли участие двое студентов МИФИ, в 2005 г. — один студент МИФИ и трое — из Северо-Кавказского государственного технического университета (г. Ставрополь). Нужно отметить, что иностранные слушатели IPICS высоко оценивают как профессиональные знания, так и владение английским языком российских ребят.

Лекции слушателям читаются ведущими преподавателями университетов стран Европы. Общий объем занятий по программе IPICS составляет 60 часов (10 дней по 6 часов). По окончании школы слушатели получают задание для написания эссе. При положительной оценке предоставленных

материалов преподавателем, представлявшим данную тему на лекции, слушатель получает определенное количество «кредитов», учитываемых при его дальнейшем обучении в основном университете.

Таким образом, сотрудничество стран-участников ЕС отличается крепкими связями (интеграцией) университетов и педагогических колледжей в Центральной и Восточной Европе. Предварительная подготовка для обучения ИБ — это бакалавриат по вычислительной технике, информатике или информационным системам/математике/инженерным дисциплинам/экономическим наукам. Осуществляется подготовка магистров — пока MS in Computer Science, далее переход к Information Systems Security и Computer and Communication Systems Security.

3. Конференции по проблемам ИБ

Другие международные мероприятия, где происходит обмен опытом по обучению в области ИБ, — это конференции по информационным и сетевым технологиям с секциями по ИБ и специализированные конференции и совещания по ИБ и безопасности в сетях. Подготовка высококвалифицированных специалистов по ИБ невозможна без проведения учебно-исследовательской и научной работы. Для этого нужно осознавать современный мировой уровня развития теории и практики обеспечения ИБ. Такие знания можно почерпнуть из открытых иностранных публикаций и из непосредственного общения с учеными разных стран во время международных конференций и семинаров. Поэтому факультет активно участвует в мероприятиях по фундаментальным исследованиям в области защиты информационных и сетевых технологий. Вот лишь некоторые примеры такого участия:

· 4-я международная конференция по сетям (Англия, 2004 г.);

· 19-я международная конференция по безопасности (Франция, 2004 г.);

· первая международная конференция по Интернет-технологиям и приложениям (Великобритания, 2005 г.);

· ежегодная конференция по безопасности SEC2006 (Швеция, 2006 г.);

· международная конференция «Еврокрипт» (Санкт-Петербург, 2006 г.);

· восьмая международная конференция по страхованию информации IEEE IAW (Военная академия Вест-Поинт США, 2007 г.) и т. п.

4. Опыт обучения ИБ США и Австралии

В США серьезное внимание уделяется подготовке кадров для защиты национальных информационных структур и сильное влияние на обучение оказывает государство и фонд поддержки развития науки (National Science Foundation). С 1991 г. выполняется программа National Security Education Program. Обучение осуществляется в основном на базе военных учреждений (Naval Postgraduate School, US Military Academy) и некоторых университетов (например, штатов Айдахо, Айова, Джорджии). Причем учебный процесс включает не только освоение теоретических знаний, но и их закрепление на практике в специально создаваемых для этих целей учебно-лабораторных комплексах (они впервые появились в выше названных военных учреждениях). В 1998 г. был создан Национальный центр защиты инфраструктуры (NIPC), объединяющий представителей органов власти, военных и частного сектора. Также функционирует и Национальный союз кибербезопасности, одной из своих целей имеющий повышение уровня образования в сфере ИБ. Для совершенствования методов обучения в Министерстве обороны создано специальное подразделение Information Assurance Program Office (Управление программ по ИБ).

Обучение в США проводится в виде дополнительного образования и сосредоточено на подготовке и переподготовке кадров по техническим аспектам защиты информации. Есть опыт National Center of Academic Excellence (при поддержке Агентства национальной безопасности с 1998 г.) подготовки бакалавров (BS in Computer Security) по программе «National Colloquium for Information Systems Security Education» (www.ncisse.org).

Из опыта США следует очень важный вывод: только активное участие государства и промышленности в программах обучения удовлетворяет потребности общества в специалистах по ИБ.

Поддержка обучения ИБ со стороны правительства может осуществляться в следующей форме:

· предоставления на конкурентной основе грантов по особо важным проблемам ИБ;

· предоставления оборудования, необходимого для исследований и обучения;

· выделения межведомственных ссуд учебным заведениям;

· организации интернатуры для приобретения практического опыта;

· повышения квалификации преподавателей;

· поддержки перспективных в ближайшие 3—5 лет областей фундаментальных исследований;

· помощи в развитии ИБ как признанной дисциплины;

· выделения грантов для учебных заведений-участников (в том числе из разных стран);

· привлечения квалифицированного персонала из государственных учреждений для преподавания и размещение филиалов факультетов в государственных учреждениях.

Основные направления сотрудничества науки и промышленности в гражданских вузах таковы:

· безвозмездная передача учебным заведениям нового оборудования и средств защиты;

· краткосрочные ссуды на оборудование и экспертизу для поддержки обучения и исследований;

· предоставление достаточного финансирования студентам, аспирантам и вузам для их развития;

· наем квалифицированного персонала из промышленности для преподавания и размещение факультетов на базе промышленных предприятий;

· руководство научно-исследовательскими работами;

· совместная разработка учебных программ.

Обучение ИБ в Австралии осуществляется под контролем и на базе государства и военных учреждений. В процессе активно участвует Australian Computer Society. Требуемый уровень предварительной подготовки — это бакалавр. Обучение проводится в университетах (например, University of South Australia и Edith Cowan University) и на базе сертификационных курсов (типа «Improved Communication Skills»). Характерно привлечение дистанционных средств обучения из-за особенностей населенности страны, поскольку современное обучение ИБ может быть качественным лишь в случае грамотного использования новых образовательных технологий, которые базируются на современных достижениях информационных технологий. Речь идет о создании образовательной среды, в которой каждый обучаемый получает всю необходимую информацию в удобной форме, должном объеме, в желаемое время и в желаемом месте. При этом оптимально решается проблема контроля и сертификации знаний.

5. Обобщенный опыт подготовки специалистов по ИБ

Особо остановимся на вопросах обобщенного зарубежного опыта в области подготовки специалистов по ИБ. Такое обучение осуществляется по трем основным направлениям:

1) обучение очное в высших учебных заведениях (гражданских и военных): подготовка бакалавров (Bachelor of Science, BoS) и магистров (Master of Science, MoS);

2) обучение дистанционное (бакалавров и магистров);

3) обучение на краткосрочных курсах: очное и дистанционное (Post Graduate Certificate — PgC).

Очное обучение бакалавров осуществляется с выдачей по завершении обучения следующих дипломов:

· Bachelor of Information Systems Security — изучаемая область защиты ИС охватывает как администрирование, так и технические аспекты; выпускники становятся важной частью ИТ-команды и могут использовать концепции и принципы обеспечения безопасности и защиты информации и активов компании;

· Bachelor of Information Technology: Cyber Security — учебная программа дает практические и теоретические знания, необходимые для того, чтобы выпускники могли обнаружить и остановить киберпреступления и взломы защиты ИС; их знаний достаточно для защиты активов компании от

нелегального использования; знание киберпространства позволяет выпускникам правильно проектировать архитектуру защиты ИС от угроз ИБ;

· BoS in Information Technology: Computer Networking & Security — учебная программа фокусируется на защите компьютерных сетей и отдельных компьютеров от хакеров, вредоносного кода, вирусов и червей и готовит специалистов, способных администрировать, планировать и координировать такую деятельность, как установка и обновление АО и ПО, используемого для защиты сетей;

· BoS in Electronics and Information Security — учебная программа рассчитана на подготовку специалистов по ИБ.

При *дистанционном обучении подготовка бакалавров* ведется по двум направлениям:

· BoS in Information Technology / Information System Security (University of Phoenix, США) — степень дает необходимые знания для успешного применения теории и принципов информационных технологий для решения реальных задач защиты бизнеса;

· BoS in Organizational Security and Management (University of Phoenix, США) — степень предназначена для решения возрастающих национальных и международных потребностей в профессионалах с расширенной технической подготовкой для индустрии безопасности.

Очная подготовка магистров осуществляется, например, в США (Johns Hopkins University) с присвоением степени MoS in Security Informatics и Норвегии (Høgskolen i Gjøvik University) с присвоением степени MoS in Information Security.

В Johns Hopkins University обучение ведется по четырем группам дисциплин, включающих 10 курсов (из них ряд по выбору), соответствующих 30 кредитам, и защиту дипломного проекта. Группы обязательных учебных дисциплин таковы:

· «Технологии» (минимум 4 курса из следующего перечня: «Безопасность Java», «Разработка защищенных систем», «Исследование защищенных систем», «Безопасность сетей», «Криптография и защита сетей», «Безопасность и собственность», «Криптографические протоколы», «Компьютерная безопасность», «Создание защищенного ПО», «Статистические методы в предотвращении вторжений» + «Компьютерная форензика», «Интернет-протоколы», «Криптология»);

· «Политики» (минимум 4 курса из перечня: «Страхование информации», «Права в цифровом веке», «Моральные и правовые основы собственности», «Информационная революция и мировые политики», «Электронная коммерция», «Управление внутренней безопасностью»);

· «Здоровье» («Управление защитой здравоохранения», «Информатика для здравоохранения», «Приложения для здравоохранения»);

· «Управление» («Финансовые вопросы управления защитой операций», «Внедрение программ защиты информации», «Принципы защиты корпораций и собственности», «Безопасность WWW», «Безопасность электронной коммерции», «ИОК и безопасность»).

В Норвегии подготовка магистров рассчитана на 2 года (4 семестра). В течение первого года необходимо изучить 7 обязательных курсов по технологиям и менеджменту — «Криптология», «ИБ и архитектура безопасности», «Управление безопасностью», «Безопасность сетей», «Научная методология», «Информационное общество и безопасность», «Правовые аспекты ИБ». На втором году нужно выбрать 3 курса из перечня: «Системное администрирование», «Расследование инцидентов и компьютерная форензика», «Аутентификация», «Защита периметра», «Обнаружение и предотвращение вторжений», «Защита беспроводной связи», «Информационная война». Степень присваивается после защиты дипломного проекта.

Существует большой выбор программ *дистанционного обучения магистров*.

· MoS in Information Security (InfoSec) (James Madison University, с 1997 г. — одна из первых в США; выпускники получают два сертификата National Security Agency: Information Systems Security Professionals (NSTISSI № 4011) и Information Systems Security Officers (CNSSI № 4014); на первом семестре изучаются «Операционные системы» и «Формальные методы в ИБ», на летней школе «Этика,

право и политика в киберпространстве», на втором семестре — «Проектирование защищенного ПО» и «Сети и безопасность сетей», на третьем семестре — «Проектирование защищенного ПО (углубленный курс)» и «Криптография: алгоритмы и приложения»; на четвертом семестре — «Безопасность сетей (углубленный курс)», на пятом семестре — «Мониторинг ИБ», по завершении обучения возможна защита диплома или сдача двух альтернативных экзаменов — «Компьютерная форензика» и «Распределенные вычисления и безопасность»;

· MoS: Information Security (AIU Online, DeVry University's Keller Graduate School of Management, University of Phoenix, Strayer University Online, Strayer University, Colorado Technical University, Jones International University, Virginia College Online, The University of Liverpool, Villanova University) — учебная программа включает изучение следующих дисциплин: «Технические системы связи», «Разработка систем», «Обзор корпоративных приложений», «Управление проектами», «Тестирование корпоративных приложений», «Обеспечение качества», «Основы бизнеса», «Сетевые технологии», «Безопасность корпоративных систем», «Операционные системы», «Управление рисками для проектов», «Практика управления безопасностью», «Криптология», «Безопасность сетей»;

· MoS in Information Security Policy & Management (Carnegie Mellon University);

· MoS in Information Assurance (Norwich University);

· MoS in Information Security and Assurance (George Mason University);

· MoS in Management: Information Systems Security (Computer Sciences -> Information Technology Management ->…) (AIU Online, DeVry University's Keller Graduate School of Management, University of Phoenix, Strayer University Online, Strayer University, Colorado Technical University, Jones International University, Virginia College Online, The University of Liverpool, Villanova University, ITT Technical Institute, Gibbs College) — учебная программа включает изучение следующих дисциплин: «Языки программирования», «Управление информационными системами (ИС)», «Управление проектами для ИС», «Технология клиент-сервер и распределенные вычисления», «Системы управления базами данных», «Хранилища данных», «Телекоммуникации и компьютерные сети», «Электронная коммерция в Интернете», «Системные анализ и проектирование», «Системы поддержки принятия решений»; выпускники способны как планировать и реализовывать меры защиты, так и разрабатывать и внедрять политики ИБ для ИС; они являются техническими лидерами (обладают техническими навыками) в администрировании систем защиты, включая методы противодействия угрозам ИБ корпоративным техническим ресурсам.

Очные краткосрочные курсы подготовки магистров имеются, например, в Великобритании (University of Glamorgan) — учебная программа «Penetration Testing and Information Security» (тесты на проникновении и ИБ).

Дистанционные краткосрочные курсы при подготовке магистров (Graduate Certificate in Information Security: Online Certificate) осуществляют AIU Online, University of Phoenix, Strayer University Online, Jones International University, Virginia College Online, The University of Liverpool, Villanova University, Utica College, Regis University, Champlain College. При этом изучаются следующие дисциплины: «Основы ИБ», «Теория защиты сетей», «Практические вопросы защиты сетей», «Восстановление после прерываний и резервирование». Получаемые навыки: студенты учатся защищать сети, данные и интеллектуальную собственность, а также выявлять угрозы инфраструктуре корпорации и понимать стратегические перспективы внедрения комплексных систем защиты. Выпускники способны управлять сервисами, защищающими людей и собственность. Они могут работать по направлениям «Системный анализ», «Компьютерная безопасность» или «Проектирование защищенных систем».

Знакомство с мировым опытом образовательной деятельности в учебных центрах различных стран позволяет сделать следующие выводы:

1) нужны специализированные единые программы для студентов — специалистов 1-го уровня (бакалавров) и выпускников — исследователей и преподавателей (магистров и кандидатов наук) и различные программы для специалистов по ИТ и по ИБ;

2) существующая во многих странах образовательная система не справляется с растущей потребностью в расширении подготовки кадров по ИБ различного уровня и профиля;

3) требуется дополнительное профессиональное обучение и курсы повышения квалификации для работающих специалистов;

4) теория и практика обеспечения ИБ динамично развивается — появляются новые разделы (например, компьютерная форензика, культура безопасности), которые нужно оперативно включать в процесс обучения;

5) для получения практических навыков в области различных аспектов обеспечения ИБ в учебном процессе необходимо использовать учебно-лабораторные комплексы, которые могут быть предназначены для проведения исследований сетевого аппаратного обеспечения, компьютеров, операционных систем, хранилищ данных, программного обеспечения и различных программно-аппаратных и технических средств защиты сетей, а также отработки моделей новых информационных и сетевых технологий на различных платформах.

6. Международный опыт сертификации специалистов по ИБ

Сегодня крайне важно проводить правильную кадровую политику, осуществляя подбор кадров на основе единого подхода к *независимой, объективной оценке их квалификации*.

На отечественном рынке труда квалификация специалиста подтверждается, как правило, документом об успешном окончании определенного учебного центра (в рамках систем высшего, среднего или дополнительного профессионального образования). Такой подход отличается субъективизмом и отсутствием реальной достоверности об уровне квалификации конкретного специалиста. При этом для профессиональных областей, которые имеют высокую динамику развития и обновления, выделенные недостатки только усиливаются. Единственным выходом из создавшегося положения является создание и использование отечественной независимой системы сертификации, включающей согласованные программы сертификации, процедуры ее прохождения и доверенные уровни документального подтверждения уровня квалификации. Пока такой системы в России нет. Дефицит потребности восполняется различными международными системами сертификации. В данном случае представляется целесообразным проанализировать опыт, накопленный за рубежом и в России по использованию таких систем с целью определения их возможностей и перспективности.

Подготовкой и сертификацией специалистов в области ИБ за рубежом занимается значительное число известных организаций. Их учебные программы все больше базируются на таких международных стандартах, как ISO/IEC 27002/27001, «Общие критерии», ITSEC и некоторых других, рекомендуемых организациями — мировыми лидерами в сфере ИБ.

Сертификаты практиков в области защиты систем (SSCP — Systems Security Certified Practitioner) и общепризнанный «золотой стандарт» (без привязки к конкретным продуктам) профессионалов в области защиты информационных систем (CISSP — Certified Information Systems Security Professional) выдаются консорциумом (ISC)I. Сертификационный экзамен по CISSP включает 10 предметных областей, которые должен знать профессионал. Сертификацию по данным программам можно пройти в России.

Ассоциация ISACA (Information Systems Audit and Control Association) имеет два сертификата: аудитор информационных систем (CISA — Certified Information Systems Auditor) и менеджер информационных систем (CISM — Certified Information Security Manager), который специализируется только в вопросах управления ИБ.

Сертификационный экзамен Security+ компании CompTIA включает такие разделы, как защита коммуникаций, инфраструктура безопасности, криптография, контроль доступа, аутентификация, внешние атаки и практические и организационные вопросы обеспечения ИБ.

Производитель программных средств защиты компания Check Point выдает сертификаты как в области защиты, так и управления безопасностью, но применительно к работе с их продуктами: сотрудник отдела безопасности (CCSPA — Check Point Certified Security Principles Associate), эксперт по защите (CCSE — Check Point Certified Security Expert), эксперт по управлению безопасностью (CCMSE — Check Point Certified Managed Security Expert).

В большом количестве сертификатов, предлагаемых фирмой CISCO, есть несколько, относящихся как к специализированным областям защиты, например, специалист по межсетевым экранам (Cisco Firewall Specialist) и специалист по системам обнаружения вторжений (Cisco IDS Specialist), так и к общим — профессионал по безопасности (CCSP — Cisco Certified Security Professional) и эксперт по межсетевому взаимодействию (CCIE — Cisco Certified Internetworking Expert).

Специальный центр анализа инцидентов (GIAC — Global Incident Analysis Center), созданный в 1999 г. при институте SANS (System Administration, Networking and Security Institute), признает одной из своих основных целей удостоверение того, что специалист имеет представление, знания и практические навыки в ключевых областях обеспечения ИБ сетей, компьютеров и ПО. Приоритетными областями выделяются аудит, обнаружение вторжений (GCIA — GIAC Certified Intrusion Analyst), расследование инцидентов ИБ (GCIH — GIAC Certified Incident Handling), межсетевые экраны (GCFA — GIAC Certified Firewall Analyst) и защита периметра, компьютерная форензика (сбор информации для последующего расследования компьютерных преступлений), хакерские методы, защита ОС Windows (GCWN — GIAC Certified Windows Security) и UNIX (GCUX — GIAC Certified Unix Security). Есть у GIAC и очень специфичный сертификат — специалист по ISO 17799 (G7799 — GIAC Certified ISO-17799 Specialist), предполагающий, что его обладатель как демонстрирует глубокое понимание стандарта, так и умеет применять его на практике.

Среди еще не названных организаций можно указать (в алфавитном порядке) следующие, перечислением которых список выдающих признанные мировые сертификаты специалистов ИБ практически исчерпан. Это Ascendant Learning (SCNP — Security Certified Network Professional и SCNA — Security Certified Network Architect); EC-Council (CEH — Certified Ethical Hacker); Microsoft (MCSA: Security — Microsoft Certified Systems Administrator: Security и MCSE: Security — Microsoft Certified Systems Engineer: Security); Planet3 Wireless (CWSP — Certified Wireless Security Professional); ProsoftTraining (Certified Internet Webmaster (CIW) Security Analyst); RSA Security (RSA Certified Systems Engineer и RSA Certified Administrator); Sun (Sun Certified Security Administrator); Symantec (SCSE — Symantec Certified Security Engineer и SCSP — Symantec Certified Security Practitioner); TruSecure (TICSA — TruSecure ICSA Certified Security Associate).

Анализ программ сертификации перечисленных выше организаций показывает, что их содержание не учитывает специфику нормативной и правовой базы России в области ИБ. Поэтому практическая значимость такой сертификации сомнительна. При отсутствии отечественной системы сертификации полученный специалистом сертификат чаще всего рассматриваются как положительный факт, дающий преимущества перед другим специалистом, не имеющим такого сертификата, но не более.

При сертификации по международным программам обычно выделяют два уровня: первый — администратор, инженер, специалист, и второй — профессионал, эксперт. Хотя, проводя более точное определение знаний и умений, можно определить и более тонкую градацию уровней.

7. Рабочая деятельность сертифицированных специалистов в области ИБ

Все сертификаты специалистов по ИБ разрабатывались в обеспечение конечного числа должностей в современных зарубежных фирмах, относящихся к области обеспечения ИБ. Они таковы:

1) сотрудник отдела безопасности (privacy officer) (разрабатывает и реализует политики и меры защиты информации);

2) архитектор ИБ (IS architect) (направляет всю работу по ИБ в организации);

3) аналитик по вопросам ИБ (IS analyst) (осуществляет аналитическую работу в области ИБ для нужд организации);

4) техник по компьютерным вирусам (virus technician) (анализирует информацию по только что обнаруженным вирусам и предлагает способы борьбы с ними до выхода официальных обновлений производителей антивирусов);

5) тестировщик ИБ («red team» tester) (планирует и по согласованию с руководством осуществляет атаки на компьютерные системы — так называемый «этический хакинг», или проведение тестов на проникновение);

6) криптограф (cryptographer) (защищает информацию посредством криптографических методов);

7) криптоаналитик (cryptanalyst) (анализирует зашифрованную информацию);

8) администратор ИБ (security administrator) (разрабатывает и внедряет системы защиты, которые обнаруживают, предотвращают, изолируют или снижают риски нарушения ИБ; поддерживает в актуальном состоянии средства и меры защиты, а также устанавливают и обеспечивают правила разграничения доступа);

9) сотрудник группы реагирования на инциденты ИБ (IS incident response team member) (работают в группе для подготовки и обеспечения быстрого реагирования в случае возникновения инцидентов ИБ);

10) специалист по восстановлению (disaster recovery specialist) (разрабатывает и внедряет программы по восстановлению данных после инцидентов ИБ);

11) специалист по компьютерным преступлениям/сотрудник отдела компьютерной форензики (computer crime specialists/computer forensic investigator) (сохраняет, идентифицирует, выделяет и документирует свидетельства инцидентов ИБ);

12) аудитор ИБ (IS auditor) (оценивает адекватность и эффективность ИБ информационных систем);

13) руководитель отдела ИБ (chief IS officer) (руководит отделом ИБ в целом и персоналом отдела).

Обратим внимание на то, что градация названных выше должностей не соответствует перечню должностей и квалификаций, принятых в России. Это еще раз подтверждает вывод о невозможности широкого использования в России международных программ сертификации специалистов по ИБ, а также актуализирует проблему создания отечественной системы сертификации. Поэтому из выше изложенного можно сделать два основных вывода:

1) необходимы как национальный, так и единый (интернациональный) подходы к независимой, объективной оценке квалификации специалистов в области ИБ;

2) необходимо установление соответствия между квалификационными требованиями к различным специалистам по ИБ и образовательными программами их подготовки (включая вопросы бакалавриата и магистратуры).

8. Заключительные выводы

Итак, на основе анализа международного опыта в области обучения ИБ можно сделать выводы, что в мире в настоящее время существуют:

· учебные планы и программы для магистров (единичные для бакалавров);

· признание ИБ вопросом многих дисциплин;

· учебно-методическое обеспечение (для обязательных и факультативных предметов, а также для дистанционного обучения);

· учебно-лабораторная база (например, США, Австралия, Греция, Италия);

· требования по предварительной подготовке;

· система кредитов для учебных программ по ИБ;

· практический опыт;

· совместные проекты по обучению.

В то же время пока отсутствуют:

· единые образовательные стандарты;

· требования к специалистам по ИБ;

· определения краткосрочных и долгосрочных приоритетов подготовки специалистов.