

Анатолий МАЛЮК

Кадровое обеспечение информационной безопасности

Развитие информационного общества в России предполагает решение новых задач в области обеспечения доступности, целостности и конфиденциальности государственных информационных ресурсов или, в более общей трактовке, информационной безопасности (ИБ) Российской Федерации.

Известно, что уязвимость любой системы оценивается по наиболее слабому ее звену. В глобальном исследовании по информационной безопасности крупнейшей аудиторской компании «Ernst & Young» отмечается, что человек остается самым слабым местом в обеспечении ИБ [1]. Основные силы направляются на решение технологических вопросов, а о «человеческой» составляющей часто забывают. Между тем различные технические средства можно применять лишь в качестве инструментов для проведения той или иной организационной политики. Они будут сменяться, совершенствоваться, но вопросы управления безопасностью все равно останутся за человеком, от которого в конечном счете и будет зависеть принимаемое решение.



Анатолий МАЛЮК – заведующий кафедрой защиты информации Национального исследовательского ядерного университета «МИФИ», кандидат технических наук, профессор, Заслуженный работник высшей школы РФ

Примечательно, что большинство злоумышленников используют не столько недостатки оборудования и программного обеспечения, сколько отсутствие должной дисциплины, контроля на рабочих местах пользователей, «необучаемость» и неадекватность персонала. Поэтому исключительное значение приобретает кадровое обеспечение развития информационных технологий вообще и информационной безопасности в частности.

Этот вопрос наряду с гуманитарными и научно-техническими проблемами информационной безопасности выделены Советом Безопасности РФ в качестве приоритетных направлений научных исследований. Первое место занимает определение прогнозируемой потребности в специалистах в области защиты информации и информационной безопасности различного уровня и профиля [2]. Чтобы вникнуть в суть данной

проблемы, рассмотрим современное состояние рынка средств обеспечения ИБ.

Российский рынок имеет свои характерные особенности. Во-первых, государство постоянно усиливает здесь свое регулирование, в частности контроль за соблюдением стандартов в области методов и порядка обработки информации, строгим выполнением лицензионных требований к распространению и использованию продуктов в области защиты информации. Во-вторых, рынок перешел из стадии формирования в стадию зрелости. Прослеживается тренд от конкуренции «с кем-то» к конкуренции «за что-то», а именно – за внимание клиентов. Существенно изменилось законодательство, возросло качество бизнеса, в связи с чем изменилась и структура спроса [3]. Можно выделить следующие тенденции развития рынка ИБ.

Усиление государственного присутствия. Прежде всего это новые нормативные требования в области защиты информации (персональных данных, критически важных объектов, в том числе ключевых систем информационной инфраструктуры). Следует отметить и попытки постепенного вытеснения господства западных производителей программного обеспечения из многих сфер экономики, в первую очередь из органов государственного управления и критически важных объектов; ужесточение контроля ввоза оборудования и программного обеспечения, содержащего функции шифрования, на территорию России, а также контроль за деятельностью пользователей в сети Интернет.

Формирование «электронного гражданина». Все больше и больше операций в общественной, политической, бытовой сферах совершается при помощи новых информационных технологий, что требует комплексных решений в области обеспечения ИБ, гражданина и личности.

Техническое регулирование. С 2009 г. вносятся изменения в Федеральный закон «О техническом регулировании». Речь идет о признании западных стандартов и гармонизации их с российскими нормативными требованиями. Пока не совсем ясно, как это скажется на всей области ИБ, но, безусловно, в результате такого изменения закона существенно упростится деятельность потребителей средств ИБ, которые не будут тратить силы и финансовые ресурсы на повторную сертификацию средств защиты (не рассматривая критические области национальной безопасности).

Нехватка квалифицированных кадров. Эта проблема преследует на только нашу страну, но и весь мир. Даже если попытаться быстро укомплектовать область обеспечения ИБ необходимым числом специалистов, то сразу встает вопрос о качестве их знаний, опыте работы и пр.

Отраслевая стандартизация. Банк России стал первым, кто выпустил свой стандарт по ИБ для банковского сообщества, а Федеральный закон «О персональных данных» стал катализатором и для других областей. Планируется выпуск стандартов операторами связи, страховщиками и другими отраслями экономики [4].

Мы обозначили лишь незначительную часть направлений развития рынка ИБ. Нарисовать общую картину в настоящий момент затруднительно. Тому есть несколько причин:

- не учитывается доля проектов по ИБ в общей стоимости ИТ-проектов;
- в аналитические отчеты, как правило, не включается информация от вендоров в области ИБ;
- иностранные вендоры в области ИБ стремятся закрыть информацию о выручке от продаж в нашей стране;
- вендоры не разделяют выручки от продаж в корпоративном и розничном сегментах;
- отсутствуют единая классификация рынка ИБ, сведения о методах сбора и обработки данных (это позволяет компаниям заявлять выручку по ИТ-проектам как выручку по направлению ИБ, что искажает реальную картину расстановки сил в сегменте ИБ) [5].

Перечисленные выше причины усложняют процесс сбора информации, связанной не только с рынком ИБ, но и с вопросами кадрового обеспечения этой сферы деятельности. Чтобы получить примерную оценку численности занятых специалистов, работающих в области обеспечения ИБ, можно воспользоваться результатами исследования, проведенного по инициативе Ассоциации предприятий компьютерных и информационных технологий (http://www.apkit.ru) в 2007 г. [6]. В нем представлено общее число занятых в российской экономике ИТ-специалистов, обозначена текущая потребность в них, а также предлагается прогноз этих величин на пять ближайших лет. Взяв за основу эти данные и учитывая то, что число отделов ИБ в структуре информационного обеспечения деятельности обычно составляет до 30%, можно сделать следующие выводы. Численность ИТ-персонала в российской экономике, согласно данным исследования [6], в 2011 г. должна составлять около 1,7 млн человек. Следовательно, необходимый объем кадров в области ИБ достигнет приблизительно 500 тыс. человек. При этом надо иметь в виду, что в упомянутом исследовании за основу прогнозирования был взят сценарный подход, по которому требуется движение к экономике знаний, повышению конкурентоспособности экономики в целом и рынка услуг в частности [7].

При таком сценарии развития, очевидно, никогда не удастся достичь полного баланса прогнозируемой потребности и масштабов подготовки кадров. Всегда будет не хватать квалифицированных ИТ-специалистов. Это связано как с довольно длительным сроком подготовки, так и с повышенной мобильностью специалистов.

Рассмотрим, как решается проблема подготовки кадров в области обеспечения ИБ в других странах, прежде всего в США. Здесь на протяжении последних

10-15 лет чрезвычайно большое значение придается привлечению к проблеме ИБ широкого общественного внимания. В 1998 г. был создан Национальный центр защиты инфраструктуры (National Infrastructure Protection Center), задача которого – предотвращение, сдерживание, реагирование и расследование преступлений, направленных против стабильности национальной информационной инфраструктуры [8]. 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 (http://www.iacis.com/). В конце 2009 г. 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 центра занимаются мониторингом и предупреждением различного рода компьютерных атак [9, 10].

Отдельно отметим компании, проводящие обучение в области обеспечения ИБ. Это 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 NAVAL 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) [11]. Агентством национальной безопасности (NSA) около десяти 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 11 сентября 2001 г. во многих городах США начали проводиться семинары, конференции, встречи по проблемам киберпреступности и кибертерроризма [12].

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, ощущается нехватка квалифицированных специалистов данного профиля.

Используют США и подготовку кадров через международные консорциумы. Мировым лидером по сертификации специалистов по ИБ является Международный консорциум по сертификации в области безопасности информационных систем (International Information Systems Security Certification Consortium, Inc.). Для получения сертификата Certified Information Systems Security Professional (CISSP) необходимо иметь опыт работы по специальности не менее четырех лет (или три года и степень бакалавра), сдать непростой экзамен, следовать «Кодексу этики» и постоянно поддерживать свою квалификацию. Для подтверждения сертификации CISSP достаточно каждые три года проходить обучение на авторизованных курсах по ИБ, а также принимать участие в конференциях по этой теме.

Отметим 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.

В Российской Федерации сегодня функционирует достаточно развитая система подготовки специалистов в области ИБ, занимающая по ряду позиций ведущее положение среди европейских стран, о чем свидетельствуют материалы регулярно проводимой международной конференции по образованию в области информационной безопасности (World Conference Information Security Education). Как система, такая подготовка стала складываться в нашей стране в начале 90-х годов, чему способствовало несколько обстоятельств: переход общества на новые информационные и телекоммуникационные технологии, повсеместное использование этих технологий, реформа высшего образования и др.

За прошедшие годы была развернута подготовка кадров в естественно-научном и техническом направлениях. Существенно меньшими были успехи в гуманитарной области и на стыке указанных дисциплин, т. е. в комплексной подготовке специалистов, владеющих всем арсеналом средств и методов обеспечения ИБ. Но необходимость в такой деятельности ощущается все острее.

Созданные в России основы государственной системы подготовки кадров в области ИБ включают в себя следующие элементы:

- *объекты системы* (высшие и средние специальные учебные заведения, региональные учебно-научные центры, учебные центры дополнительного образования;
- *субъекты системы* (студенты, учащиеся, преподаватели, административный персонал);

- *учебно-методическое обеспечение системы* (государственные образовательные стандарты высшего и среднего профессионального образования по группе специальностей и направлению «Информационная безопасность», учебные планы, программы, учебники и информационные материалы);
- *подсистема управления* (Министерство образования и науки РФ, органы исполнительной власти на региональном уровне, учебно-методическое объединение по образованию в области информационной безопасности).

На российском рынке ИТ специализированную подготовку в области обеспечения информационной безопасности осуществляют также учебные центры повышения квалификации, для которых это направление является приоритетным (учебный центр «Информзащита», «Эшелон», Domina Security и др.), и образовательные центры в области ИТ и телекоммуникаций («Академия АйТи», школа CNews, АИС, «Специалист», сетевая академия «Ланит» и др.).

В нашей стране существует довольно широкая номенклатура направлений и специальностей подготовки и переподготовки кадров в области обеспечения ИБ. Отличительными чертами действующих и вводимых вновь государственных образовательных стандартов в этой области являются углубленное изучение теоретических основ, акцент на практическую направленность обучения, высокая мобильность содержания читаемых курсов, проведение учебных курсов по нормативно-правовой базе и гуманитарным аспектам защиты информации. Российские учебные заведения, как правило, имеют тесные контакты с ведущими западными центрами.

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.

Анализ различных оценок потребности в специалистах по ИБ, полученных как у нас в стране, так и за рубежом, сравнение их с прогнозами развития систем подготовки специалистов ясно показывают, что решить поставленные задачи с помощью только подготовки новых кадров с высшим и средним профессиональным образованием практически невозможно. Основные причины этого:

- большой временной интервал процесса подготовки (при этом, если говорить о Российской Федерации, то надо иметь в виду, что созданная система подготовки кадров только набирает обороты);
- явно недостаточное количество выпускаемых специалистов; так, среднее количество специалистов в области ИБ, выпускаемых в год высшими учебными заведениями страны, оценивается примерно в 1700 человек, тогда как лишь государственным учреждениям ежегодно требуется порядка 1500 человек;
- инерционность обучения, связанная с долговременной (в пределах одного цикла обучения) стабильностью учебных программ и планов (за это время требования к содержанию обучения существенно изменяются);
- сложность организации целевой подготовки специалистов в интересах конкретного предприятия (к сожалению, сегодня 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 в области ИБ.

Последнее имеет очень важное значение. 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 требует отдельного изучения), это вряд ли обеспечит эффективность отбора, поскольку за длительное время обучения 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 данной формы обучения – малая длительность подготовки, гибкость учебных программ, простота 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. В этом и реализуется целевой характер дополнительного образования. И, естественно, необходимо обеспечить ИБ самой системы обучения (в первую очередь по содержанию обучения).

Из изложенного выше становится 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. Прежде всего это относится к механизму формирования государственного заказа на подготовку.

Совершенствование системы подготовки кадров в области ИБ проходило в последнее время в рамках реализации Федеральной целевой программы развития образования на 2006-2010 гг. Она основана на принципиально новых подходах – формировании кадрового потенциала и «приоритетности современных образовательных и информационных технологий» [13]. В ходе ее реализации осуществлена система мер по совершенствованию нормативно-правовой базы, кадровому, информационному и материально-техническому обеспечению сферы образования. Управление современной системой подготовки кадров в области ИБ учитывает: единство учебно-методического обеспечения; сложившуюся структуру объектов системы; использование в этой системе современных информационных и образовательных технологий; существование в России трехуровневой системы управления образованием (Министерство образования и науки или региональный орган управления – учебно-методическое объединение – учебное заведение или учебный центр); требования по защите информации, предъявляемые к содержанию обучения.

В завершенной форме система подготовки кадров в области ИБ должна выглядеть как корпоративная система обучения, позволяющая готовить специалистов при определенных ограничениях, например, в условиях необходимости обеспечения безопасности информации, что должно быть учтено при управлении такой системой.

С точки зрения государственного регулирования процесса подготовки специалистов в области ИБ следует отметить кадровое обеспечение системы защиты государственной тайны, являющейся составной частью системы обеспечения ИБ. Понятно, что здесь государственное регулирование является важнейшим аспектом всего процесса.

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

- определение 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 государственных образовательных стандартов и образовательных программ при активном участии министерств и ведомств, занятых в этой сфере;
- 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.

Представляется, что исключительное значение проблемы ИБ в реализации Стратегии национальной безопасности Российской Федерации до 2020 г., требует разработки специальной Федеральной целевой программы развития системы подготовки кадров в области обеспечения информационной безопасности Российской Федерации на долгосрочную перспективу, предусматривающей многоступенчатость профессионального образования, формирование новых направлений и специальностей, приоритетное развитие системы дополнительного образования, в первую очередь повышения квалификации.

Литература

1. Ernst & Young's 2008 Global Information Security Survey, 2008. URL: http://www.ey.com/Publication/vwLUAssets/GISS_2008_EN/$FILE/GISS_2008_EN.pdf
2. Приоритетные проблемы научных исследований в области обеспечения информационной безопасности Российской Федерации. URL: http://www.scrf.gov.ru/documents/93.html
3. *Гайкович В.* Рынок ИБ находится в фазе ожидания очень сильного роста // Журнал «Information Security». URL: http://www.itsec.ru/newstext.php?news_id=48690
4. *Лукацкий А.* Что готовит нам 2010 год? // Портал «Компьютера-Онлайн». URL: http://www.computerra.ru/blogs/cisco/491459/
5. *Гайкович В.* Что представляет собой современный российский рынок ИБ 2009? URL: http://www.infosec.ru/experts/301/
6. Аналитическое исследование «ИТ кадры в российской экономике» URL: http://www.apkit.ru/files/ITstaff_demant_2007.pdf
7. Прогноз социально-экономического развития Российской Федерации на 2010 год и плановый период 2011 и 2012 годов: Министерство экономического развития Российской Федерации. URL: http://www.economy.gov.ru/wps/wcm/connect/economylib4/mer/resources/14ad420040ac73d9b63efe87b4cd4b14/prognoz.doc
8. National Infrastructure Protection and Computer Intrusion Program (NIPS). URL: http://memphis.fbi.gov/menipc.htm
9. US government opens $9m cyber security center, TG-daily. URL: http://www.tgdaily.com/security-features/44495-us-government-jpens-9m-cyber-security-center
10. Американский центр борьбы с киберпреступностью стоит $9 млн. // Журнал «Information security». URL: http://www.itsec.ru/newstext.php?news_id=62428
11. DoD Directive 8579.1 URL: http://www.isc2.org/dodmandate/default.aspx
12. *Маклаков Г.* Научно-методологические аспекты подготовки специалистов в области информационной безопасности. URL: http://www.crime-research.ru/articles/maklakov0105/
13. Концепция Федеральной целевой программы развития образования на 2006-2010 годы: Федеральное агентство по образованию. URL: http://ed.gov.ru/files/materials/1799/RPR1340.doc