

УДК 004.001

ПОВЫШЕНИЕ КАЧЕСТВА ПОДГОТОВКИ СПЕЦИАЛИСТОВ В ОБЛАСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

© И.А. Зауголков, Е.М. Михайлова

Ключевые слова: информационная безопасность; комплексные меры по защите информации; способы и средства защиты информации.

Статья посвящена необходимости повышения квалификации сотрудников предприятий, занимающихся вопросами обеспечения информационной безопасности предприятий и организаций.

Резкий скачок информатизации российского общества на современном этапе развития значительно повысил внимание к проблеме информационной безопасности. Можно выделить несколько факторов, способствующих дальнейшему развитию российского рынка информационной безопасности. В первую очередь, к таким факторам относится необходимость соблюдать требования обязательных стандартов и законов, затрагивающих вопросы информационной безопасности. Например, согласно Федеральному закону «О персональных данных», все информационные системы компаний должны быть приведены в соответствие с его требованиями не позднее 1 января 2010 г. Нарушение требований Закона при обработке персональных данных влечет за собой гражданскую, уголовную, административную, дисциплинарную ответственность.

Для кредитно-финансовых организаций обязательным является выполнение стандарта PCI DSS. Такая ситуация характерна не только для России, но и для Европы и США, где достаточно давно основным движущим фактором развития рынка информационной безопасности стала необходимость соблюдения требований по защите информации, определенных в локальных нормативных документах, таких как SOX, HIPAA и т. д.

Еще одним фактором, способствующим развитию сферы информационной безопасности в условиях кризиса, является необходимость устранения критических уязвимостей, из-за которых в компании происходят или могут произойти инциденты, приводящие к значительному ущербу для бизнеса.

В настоящее время большинство российских компаний становятся более зрелыми и компетентными участниками как внутреннего торгового рынка, так и внешнего. К определяющим факторам таких изменений можно отнести процедуру постепенного вхождения России во Всемирную торговую организацию и желание крупных компаний выйти на фондовые рынки. Поэтому становится все более очевидно, что сегодня утечка конфиденциальной информации не просто подорвет конкурентоспособность компании, но может привести и к ее банкротству. Поэтому проблема защиты информации резко обострилась с развитием конкуренции в среде свободного предпринимательства [1].

Эффективная система управления информационной безопасностью, во-первых, обеспечивает необходимый уровень защиты всех информационных активов компании, т. е. существенно снижается риск нанесения ущерба компании, и, во-вторых, гарантирует, что меры и средства защиты информации являются адекватными и пропорциональными возможному ущербу. Кроме этого, позволяет самой компании, а также ее партнерам убедиться в том, что система управления ИБ внедрена в общую систему управления бизнес-процессами компании, что она работает правильно и эффективно. Это особенность важна в том случае, если компания работает с большими объемами ценной информации или если компания обрабатывает или хранит ценную информацию своих клиентов.

Однако даже новейшие системы информационной безопасности не в состоянии работать без участия и контроля со стороны человека. Человек становится носителем огромного количества конфиденциальной и секретной информации, что одновременно с несомненными плюсами имеет и свои недостатки, т. к. он становится потенциальным источником угроз безопасности информации.

В настоящее время лидирующие позиции среди основных угроз занимает внутренний нарушитель. Это связано, прежде всего, с тем, что внешний периметр в большинстве компаний защищен достаточно надежно, а сотрудникам компании необходимо иметь доступ к конфиденциальной информации компании для выполнения своих должностных обязанностей. Следовательно, средства защиты в гораздо меньшей степени обеспечивают безопасность информации от внутреннего нарушителя.

Поэтому эффективность защиты информации во многом определяется, прежде всего, человеческим фактором, в качестве одной из характеристик которого выступает уровень профессиональной подготовки. Все вышесказанное привело к возрастанию потребностей в специалистах в области информационной безопасности, обладающих высокой информационной культурой, владеющих новейшими информационными технологиями и умеющих применять в своей профессиональной деятельности приобретенные знания и навыки.

Именно поэтому в Доктрине информационной безопасности Российской Федерации развитие системы обучения кадров, работающих в области обеспечения информационной безопасности, отнесено к числу первоочередных мероприятий по реализации государственной политики в рассматриваемое среде.

Для большинства руководителей предприятий найти высокопрофессиональных специалистов в области защиты информации становится большой проблемой, т. к. наличие таковых на современном рынке труда весьма ограничено. В основном, руководители организаций видят два пути разрешения данной проблемы: одни – направляют на переподготовку своих штатных сотрудников, основу которых составляют профессионалы спецслужб, силовых ведомств, ушедшие в отставку в связи с их многократными реорганизациями, по выслуге лет и т. п.; другие – привлекают молодых перспективных специалистов с недостаточным опытом работы и организуют для них программы обучения и развития. Но во время обучения специалисты по защите информации, с одной стороны, отрываются от своих основных обязанностей и тем самым наносят компании немалый ущерб, а с другой стороны, процесс обучения не должен носить одноразовый характер, что требует дополнительных затрат от руководства. Сфера информационной безопасности остается исключительно востребованной в условиях кризиса.

Поэтому в последнее время большинство работодателей все-таки предпочитают искать опытные и квалифицированные кадры, способные обеспечивать максимальную эффективность реализуемых мер по защите информации.

Все вышеизложенное активизирует деятельность образовательных учреждений к представлению более качественных образовательных услуг на рынке труда в сфере информационной безопасности.

В связи с этим, во многих образовательных учреждениях уже функционируют курсы повышения квалификации для специалистов в данной области. Исходя из опыта организация и проведение курсов по программам повышения квалификации сотрудников служб безопасности предприятий и организаций на базе региональных образовательных учреждений позволит:

1. повысить эффективность подготовки специалистов в сфере информационной безопасности;
2. сократить сроки и уменьшить расходы на обучение;
3. систематизировать работу по подготовке руководителей хозяйствующих субъектов и работников режимно-секретных органов.

ЛИТЕРАТУРА

1. Чибрикин И. Информационная безопасность для организаций с высоким уровнем риска: новые угрозы и возможные подходы к их нейтрализации // Jet Info. 2007. № 1.

Поступила в редакцию 11 апреля 2009 г.

Zaugolkov I.A., Mihailova E.M. Improvement of the informational safety field experts' preparation quality. Article is devoted to the necessity of improvement of professional skill of the employees of enterprises providing the informational safety of firms and the organizations.

Key words: informational safety; complex measures on information protection; ways and information protection frames.