УДК 004.056.53

В.А. Атрощенко, Р.А. Дьяченко, В.А. Кучер

Россия, Краснодар, ФГБОУ ВО КубГТУ

НОВЫЕ ТРЕБОВАНИЯ К ПОДГОТОВКЕ СПЕЦИАЛИСТОВ В ОБЛАСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

В статье рассмотрены новые задачи, которые необходимо решать в учебном процессе вузов, связанные с появлением новых уязвимостей информационных систем критически важных объектов. Описывается организация подготовки специалистов по информационной безопасности для организаций, использующих системы на основе технологии BigData, а также методы и средства проектирования систем, средств и технологий обеспечения и управления информационной безопасностью бизнес-процессов.

Ключевые слова: информационная безопасность, технология BigData, профессиональные стандарты, информационная безопасность бизнес-процессов

Уровень профессиональной подготовки в области защищенных информационных технологий и информационной безопасности в настоящее время выступают как важная составляющая в комплексе мероприятий по противодействию угрозам жизненно важным интересам общества, государства и личности в информационной сфере.

Так, в Доктрине информационной безопасности Российской Федерации, утвержденной Указом Президента Российской Федерации от 05.12.2016 г. № 646 и определяющей стратегические цели и основные направления обеспечения информационной безопасности с учетом национальных приоритетов России, отмечается, что основными направлениями обеспечения 20нновационной безопасности в области науки, технологий и образования являются [1]:

– достижение конкурентоспособности российских информационных технологий и развитие научно-технического потенциала в области обеспечения информационной безопасности;

– создание и внедрение информационных технологий, изначально устойчивых к различным видам воздействия;

– проведение научных исследований и осуществление опытных разработок в целях создания перспективных информационных технологий и средств обеспечения информационной безопасности;

– развитие кадрового потенциала в области обеспечения информационной безопасности и применения информационных технологий;

– обеспечение защищенности граждан от информационных угроз, в том числе за счет формирования культуры личной информационной безопасности.

Задачи поставлены очень серьезные, сложные и затратные, требующие больших усилий, но другой альтернативы не существует. Это наглядно демонстрируют регулярные атаки на информационные активы органов государственной власти и управления, коммерческих структур, а также отдельных граждан.

В таких условиях выполнение поставленных Доктриной информационной безопасности задач предполагает эффективную разработку и внедрение инновационных технологий, проведение научных исследований и совершенствование подготовки специалистов в области защищенных информационных технологий и информационной безопасности, повышение осведомленности различных категорий граждан в области защиты информации. Причем 21ннновазация всего комплекса работ предполагает четкое взаимодействие различных структур, как государственных, так и коммерческих, в том числе научно-исследовательских, производственных и учебных организаций под руководством соответствующих регуляторов этой деятельности.

Высокая динамика развития информационных технологий, наблюдаемая в настоящее время, дает не только новые преимущества для развития экономики России, но и влечет за собой многократный рост числа уязвимостей информационных систем.

Существует класс информационных систем, обеспечение безопасности которых является одним из основных требований. К ним можно отнести, например, системы управления опасными технологическими производствами, транспортом, объектами управления инфраструктурой, энергетикой и другие. Такие информационные системы называют критическими.

Безопасность критических информационных систем во многом зависит от безопасности сетей связи, хранилищ информации, составляющих основу информационной инфраструктуры страны или компании. На разных этапах процесса обеспечения безопасности критической информационной инфраструктуры или информационной системы необходимо иметь достоверную оценку безопасности информационной архитектуры.

Это, в свою очередь, обуславливает развитие существующих и появление новых технологий, методов и средств их защиты. В результате возрастает потребность в квалифицированных и компетентных специалистах по 22нновационной безопасности с различным уровнем подготовки и наличия опыта работы.

Научно-технический прогресс, развитие производств и технологий, а также динамично изменяющийся рынок труда требуют постоянного развития профессиональных навыков и компетенций работника. Квалификационные справочники, в свою очередь, постепенно устаревают: либо в них вообще нет новых профессий, либо их описание не соответствует действительности. Именно этим и обусловлена потребность изменения действующей системы квалификаций, а точнее, замена Единого тарифно-квалификационного справочника работ и профессий рабочих (ЕТКС) и Единого квалификационного справочника должностей руководителей, специалистов и служащих (ЕКС) системой профессиональных стандартов.

Понятия «квалификация работника» и «профессиональный стандарт» определены в ст. 195.1 Трудового кодекса Российской Федерации. Согласно указанной статье квалификация работника – это уровень знаний, умений, профессиональных навыков и опыта работы работника.

В свою очередь, профессиональный стандарт – это характеристика квалификации, необходимой работнику для осуществления определенного вида профессиональной деятельности. Профессиональные стандарты в области информационной безопасности – это новое слово, как в образовании, так и в сфере современного труда в данной области.

Отметим, что ранее в законодательстве отсутствовало понятие профессионального стандарта, и это затрудняло разработку и реализацию профессиональных стандартов на практике.

Для работодателей профессиональный стандарт будет являться основой для установления более конкретных требований при выполнении трудовой функции работника с учетом специфики деятельности организации.

Положения соответствующих профессиональных стандартов должны будут учитываться при формировании федеральных государственных образовательных стандартов профессионального образования поколения 3++. Таким образом, должна решиться появившаяся в последние годы проблема, когда выпускник учебного заведения обладает одними профессиональными навыками, а работодателю требуются совсем другие.

Специалисты в области информационной безопасности испытывают потребность в знаниях о новых технологиях и решениях, в приобретении навы-

ков применения новых средств защиты. Связано это, прежде всего, с практически ежедневным появлением новых уязвимостей и угроз безопасности компьютерных сетей, и, соответственно, методов, продуктов и решений в области защиты информации.

Новые задачи и новые технологии породили огромные массивы данных и возможность их обрабатывать. В настоящее время на передний план выходят «облачные технологии», виртуализация, безопасность мобильных устройств и социальных сетей.

Использование больших данных в сфере информационной безопасности в первую очередь позволяет обрабатывать огромные объемы самых различных данных в реальном времени. Например, в SIEM-системах технология BigData позволяет хранить и анализировать большое количество логов разных систем: Web-серверов, серверов приложений, баз данных и др. В результате мы имеем возможность в реальном времени выполнять сложные аналитические запросы.

Системы на основе BigData используются для анализа прогнозирования в таких больших проектах, как «Безопасный город». Разработанный компанией «Ростелеком», этот комплекс решений позволяет полностью контролировать ситуацию в сфере безопасности в регионах: инфраструктуру ЖКХ и городские объекты, экологическую обстановку, наличие аварийных ситуаций, социальную стабильность, а также оперативно реагировать на чрезвычайные происшествия. DLP-системы также смогут внести свой вклад в развитие подобных проектов, предоставляя им различные аналитические данные.

Усиление фундаментальной подготовки студентов посредством реализации многоступенчатой системы организации учебного процесса, ориентированной на формирование компетенций обучающихся и внедрения 23ннноваициоонных образовательных технологий.

Создание и обновление учебной, методической и материально-технической базы для реализации образовательных программ в соответствии с требованиями ФГОС ВО 3+ по специальностям и направлениям подготовки 10.00.00 Информационная безопасность, должно осуществляться также в соответствии с требованиями профессиональных стандартов в области информационной безопасности и с учетом рекомендаций сообщества работодателей в данной области.

Новые задачи и новое содержание требований к их решению, сформулированное в профессиональных стандартах в области информационной безопасности в форме трудовых функций, а также учет мнения работодателей Краснодарского края, потребовали соответствующей реакции вузов. В связи с

этим в программы бакалавриата, специалитета и магистратуры укрупненной группы специальностей и направлений подготовки 10.00.00 Информационная безопасность, реализуемых в Кубанском государственном технологическом университете (КубГТУ) в 2017 году, включена целая группа новых дисциплин:

– »Хранение данных и управление информацией» (10.03.01), 3 з.е.;

– »Технологии хранения больших данных и управления информацией» (10.05.01, 10.05.03), 3 з.е.;

– »Технологии BigData в системах защиты информации» (10.04.01), 3 з.е.;

– »Проектное управление в сфере информационной безопасности» (10.04.01, 10.05.01, 10.05.03), 3 з.е.;

– »Информационная безопасность облачных вычислений и распределенных компьютерных систем» (10.05.01, 10.05.03, 10.04.01), 3 з.е.;

– »Обеспечение информационной безопасности бизнеса», (10.05.01, 10.05.03), 3 з.е.;

– »Деловые коммуникации в обеспечении информационной безопасности» (10.04.01), 3 з.е.;

– »Управление бизнес-процессами обеспечения информационной безопасности» (10.04.01) 3 з.е.;

– »Современные методы анализа и управления рисками непрерывности и информационной безопасности бизнеса» (10.04.01), 3 з.е.;

– »Комплексная оценка рисков непрерывности бизнес-процессов» (10.04.01), 3 з.е.;

– »Методы и средства проектирования систем, средств и технологий обеспечения информационной безопасности бизнес-процессов», (10.04.01), 3 з.е.;

– »Организация работ и принятие управленческих решений в сфере информационной безопасности бизнес-процессов» (10.04.01), 3 з.е.

Для реализации этих задач в КубГТУ планируется в 2017 году закупить оборудование, ввести в эксплуатацию и использовать в учебном процессе и научных исследованиях две новые специализированные лаборатории на базе современного учебного Дата-центра и системы хранения данных:

– »Технологии хранения, обработки и управления информацией в защищенном виде»;

– »Технологии облачных систем, больших данных и защита информации».

В рамках существующего с 2014 года совместного с системным интегратором ЗАО «Сириус» учебно-научного центра проблем информационной безопасности также планируются следующие мероприятия [2].

1. Создание тестового полигона оценки реальной защищенности применяемых в Краснодарском крае государственных информационных систем (ИС) (развертывание клона ИС; развертывание применяемых средств защиты информации, моделирование методов проникновения, оценки защищенности и т.п.).

2. Тестирование нового телекоммуникационного оборудования и программного обеспечения, средств защиты информации, планируемых к внедрению в сетях органов государственной власти и управления Краснодарского края (создание макета инфраструктуры, схожей с реальными сетями региона и исследование уязвимостей системы);

3. Проведение технических семинаров и практических занятий по современным проблемам информационной безопасности.

Вывод. Хорошо подготовленный специалист в области защищенных информационных технологий и информационной безопасности позволяет своей организации не только экономить значительные материальные и финансовые средства, благодаря рациональному выбору методов и средств защиты и полному использованию заложенных в них возможностей, но и, в конечном счете, окупить инвестиции в информационную безопасность за счет предотвращения возможного ущерба.

Литература

1. Доктрина информационной безопасности Российской Федерации, утвержденная Указом Президента Российской Федерации от 05.12.2016 г. № 646/ http://www.kremlin.ru/.

2. Кучер В.А., Зангиев Т.Т., Тарасов Е.С. Применение автоматизированных комплексов и учебно-тренировочных средств для изучения вопросов управления информационной безопасностью. Таганрог, научно-практический журнал «Информационное противодействие угрозам терроризма», № 25, том 1, 2015, с. 240-244.