УДК 378.02 (082)

В.Н. Соляной, А.И. Сухотерин, Т.Ш. Шихнабиева

Россия, г. Королев, Государственное бюджетное образовательное учреждение высшего образования Московской области «Технологический университет»

СЕРТИФИКАЦИЯ БАКАЛАВРОВ И МАГИСТРОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПО ТРЕБОВАНИЯМ ПРОФЕССИОНАЛЬНЫХ СТАНДАРТОВ С ИСПОЛЬЗОВАНИЕМ СИСТЕМЫ ДОПОЛНИТЕЛЬНОГО ОБРАЗОВАНИЯ

Практическая реализация проведение независимой оценки квалификации выпускников вузов в области информационной безопасности остается проблемной задачей и требует серьезной теоретической проработки. В статье представлен возможный вариант разрешения данной проблемы на основе формирования федеральных, региональных и ведомственных специализированных центров информационной безопасности на базе ведущих вузов, осуществляющих подготовку профессионалов по информационной безопасности (защиты информации).

Ключевые слова: информационная безопасность, профессиональные стандарты, специалист, сертификация, компетенции, методологический подход.

В 2016 году в Российской федерации утвержден Минтрудом России и опубликован пакет профессиональных стандартов специалистов по информационной безопасности (ИБ):

– «Специалист по автоматизации информационно-аналитической деятельности в сфере безопасности»;

– «Специалист по безопасности компьютерных систем и сетей»;

– «Специалист по защите информации автоматизированных систем»;

– «Специалист по защите информации в телекоммуникационных системах и сетях»;

– «Специалист по технической защите информации».

В пределах указанных в стандартах профессиональных областях по ИБ, документы Минтруда РФ, требуют от специалиста по ИБ специальных знаний, теории алгоритмов, кодов, математической логики и законов об информации и т.д. Помимо прочего, специалист должен уметь обнаруживать,

197нновсифицировать и противодействовать информационным угрозам, выявлять уязвимости, восстанавливать информационную систему после информационных атак, самостоятельно проводить тестовые задачи и расследования инцидентов по ИБ [1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12].

В тоже время, специалист должен пройти курсы повышения квалификации и получить соответствующий сертификат. При этом сертификат станет обязательным при найме сотрудников во всех министерствах и федеральных службах. Причем его наличие будет обязательным условием как для соискателей на должность, так и для действующих сотрудников.

Вопрос подготовки и переподготовки специалистов в области защиты информации (ИБ) будет решаться в первую очередь силами учебных учреждений и учебных центров на их базе, имеющих государственную лицензию на подготовку профессионалов по направлению ИБ.

Постановление Правительства РФ № 584 предусматривает поэтапное введение и применение введенных профессиональных стандартов с завершением этого процесса процесс до 1 января 2020 г.

В тоже время самостоятельных профессиональных стандартов по направлениям «Информационная безопасность», бакалавр (10.03.01) и магистр (10.04.01) не разрабатывались. Профессиональные требования к таким специалистам сформированы в виде отдельных положений, которые отдельными фрагментами прописаны в веденных профессиональных стандартов специалистов по защите информации. С учетом такой специфики просматривается проблема ***определения содержания и реализация сертификационных направлений для профессионалов по ИБ в лице бакалавров и магистров.***

Учитывая приобретенный опыт подготовки бакалавров и магистров в области ИБ в «Технологическом университете» (г. Королев, МО) разрешение указанной проблемы можно реализовать в виде рекомендаций по нескольким вариантам [1,7,8,9,10,11,12].

Первое сертификационное направление (первый сертификационный уровень иерархии) должно охватывать содержание требований (в полном объеме) основной цели вида профессиональной деятельности. Для каждого принятого профессионального стандарта эти требования должны сертифицироваться в пределах прописанных уровней квалификации: для бакалавра – уровень 6; 197нгистра – уровень 7. Такие сертификационные испытания, на наш взгляд, должны проводиться в специализированных федеральных центрах оценки квалификации, развернутых на базе ведущих высших учебных организациях, осуществляющих подготовку специалистов по ЗИ, соответствующих направлению

рассматриваемого профессионального стандарта. При этом сертификация должны быть реализовываться по совокупности всех обобщенных трудовых функций, которые прописаны для каждого рассматриваемого уровня квалификации (бакалавр или магистр по информационной безопасности).

Обязательная сертификация должна реализовываться как для выпускников вузов, так и для лиц окончивших переподготовки кадров ИБ по планам дополнительного образования в виде специализируемых курсов. Содержание и наименование таких специализируемых курсов должны соответствовать аналогам одноименных профилей, реализуемых вузами по направлениям подготовки ИБ (10.03.01- бакалавр и 10.04.01- магистр). В среднем целесообразный объем данных курсов должен составлять в среднем 500 учебных часов. Студенты выпускники курсов имеют возможность параллельно получить дополнительное высшее образование и сертификат, подтверждающий это образование.

Пример реализации указанных предложений (первый сертификационный уровень) для профессионального стандарта «Специалист по безопасности компьютерных систем и сетей».

Название спецкурса для бакалавра ИБ (10.03.01): Защита информации в компьютерных системах и сетях (Администрирование средств защиты информации в компьютерных системах и сетях);

Тематика модулей курса (областей сертификационного тестирования):

– Администрирование подсистем защиты информации в операционных системах;

– Администрирование программно-аппаратных средств защиты информации в компьютерных сетях;

– Администрирование средств защиты информации прикладного и системного программного обеспечения.

Второе сертификационное направление (второй сертификационный уровень иерархии) должно предусматривать определение (оценку) степени реализации требований профессиональных стандартов на уровне отдельных обобщенных трудовых функций, соответствующих для каждого рассматриваемого уровня квалификации (бакалавр или магистр по информационной безопасности).

Обязательная сертификация для данного направления должна реализовываться, прежде всего, для лиц окончивших курсы переподготовки или повышения квалификации кадров ИБ по планам дополнительного образования в виде специализируемых курсов. Содержание и наименование таких специализируемых курсов должны соответствовать аналогам одноименных названий

обобщенных трудовых функций. В среднем целесообразный объем таких курсов должен составлять в среднем порядка 250 учебных часов.

Сертификационные испытания в данном подходе целесообразно проводить по каждой трудовой функции рассматриваемой обобщенной трудовой функции, которые закреплены за рассматриваемыми уровнями квалификации (бакалавр или магистр по информационной безопасности).

Такие сертификационные испытания (второе сертификационное направление) должны проводиться в специализированных региональных (ведомственных) центрах оценки квалификации, развернутых на базе региональных ведущих высших учебных организациях, осуществляющих подготовку специалистов по ЗИ, соответствующих направлению рассматриваемого профессионального стандарта.

Применительно к вузам, имеющие направления подготовки ИБ (10.03.01-бакалавр и 10.04.01- магистр), студенты, обучаясь в рамках утвержденных профилей по ИБ (ЗИ), будут иметь возможность реализовать дополнительное образование и получить подтверждающий сертификат по отдельным обобщенным трудовым функциям (в пределах отдельных (нескольких) изучаемых профилей по ИБ) [1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12].

Пример реализации указанных предложений для профессионального стандарта «Специалист по безопасности компьютерных систем и сетей» для бакалавра ИБ (10.03.01):

– название первого учебного спецкурса (тематики сертификационных тестов): Администрирование подсистем защиты информации в операционных системах;

– название второго учебного спецкурса (тематики сертификационных тестов): Администрирование программно-аппаратных средств защиты информации в компьютерных сетях;

– название третьего учебного спецкурса (тематики сертификационных тестов): Администрирование средств защиты информации прикладного и системного программного обеспечения.

Третье сертификационное направление должно предусматривать определение (оценку) степени реализации требований профессиональных стандартов. Сертификации подлежит практическая реализация отдельных трудовых функций, соответствующих для каждого рассматриваемого уровня квалификации (бакалавр или магистр по информационной безопасности) в виде совокупности потребных мер: трудовых действий; необходимых умений; необходимых знаний и других характеристик.

Обязательная сертификация для данного направления должна реализовываться, прежде всего, для лиц окончивших курсы повышения квалификации кадров ИБ по планам дополнительного образования в виде специализируемых курсов. Содержание и наименование таких специализируемых курсов должны соответствовать аналогам одноименных названий трудовых функций. В среднем целесообразный объем таких курсов должен составлять в среднем порядка 75 учебных часов.

Сертификационные испытания в данном подходе целесообразно проводить по каждой трудовой функции, которые закреплены за рассматриваемыми уровнями квалификации (бакалавр или магистр по информационной безопасности).

Такие сертификационные испытания (третье сертификационное направление) должны проводиться в специализированных центрах информационной безопасности, развернутых на базе высших учебных организациях, осуществляющих подготовку специалистов по ЗИ, соответствующих направлению рассматриваемого профессионального стандарта.

Применительно к таким вузам, имеющие направления подготовки ИБ (10.03.01- бакалавр и 10.04.01- магистр), студенты, обучаясь в рамках утвержденных профилей по ИБ (ЗИ), должны иметь возможность реализовать дополнительное образование и получить подтверждающий сертификат по отдельным трудовым функциям (в пределах изучаемого одного профиля по ИБ) [1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12].

Пример реализации указанных предложений для профессионального стандарта «Специалист по безопасности компьютерных систем и сетей» для бакалавра ИБ (10.03.01):

Название первого спецкурса: «Администрирование подсистем защиты информации в операционных системах»;

Тематика групп учебных вопросов (сертификационных тестов):

– архитектура и принципы построения операционных систем;

– программные интерфейсы операционных систем;

– виды политик управления доступом и информационными потоками применительно к операционным системам;

– архитектура подсистем защиты информации в операционных системах;

– принципы функционирования средств защиты информации в 200нновационных системах, в том числе использующих криптографические алгоритмы;

– состав типовых конфигураций программно-аппаратных средств защиты информации;

– требования по составу и характеристикам подсистем защиты информации применительно к операционным системам;

– порядок реализации методов и средств антивирусной защиты в операционных системах;

– программно-аппаратные средства и методы защиты информации в операционных системах;

– принципы работы и правила эксплуатации программно-аппаратных средств защиты информации;

– нормативные правовые акты в области защиты информации;

– руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации;

– организационные меры по защите информации.

Название второго спецкурса: «Администрирование программно-аппаратных средств защиты информации в компьютерных сетях».

Тематика групп учебных вопросов (сертификационных тестов):

– принципы построения компьютерных сетей;

– стек сетевых протоколов операционных систем;

– стек протоколов сетевого оборудования;

– порядок реализации методов и средств межсетевого экранирования;

– принципы функционирования сетевых протоколов, включающих криптографические алгоритмы;

– виды политик управления доступом и информационными потоками в компьютерных сетях;

– источники угроз информационной безопасности в компьютерных сетях и меры по их предотвращению;

– состав типовых конфигураций программно-аппаратных средств защиты информации и их режимов функционирования в компьютерных сетях;

– методы измерений, контроля и технических расчетов характеристик программно-аппаратных средств защиты информации;

– принципы работы и правила эксплуатации эксплуатируемых программно-аппаратных средств защиты информации;

– программно-аппаратные средства и методы защиты информации в компьютерных сетях;

– нормативные правовые акты в области защиты информации;

– руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации;

– организационные меры по защите информации.

Название третьего спецкурса: «Администрирование средств защиты информации прикладного и системного программного обеспечения».

Рекомендуемая тематика групп учебных вопросов (сертификационных тестов):

– архитектура подсистем защиты информации в операционных системах;

– принципы построения систем управления базами данных;

– основные средства и методы анализа программных реализаций;

– принципы построения антивирусного программного обеспечения;

– виды политик управления доступом и информационными потоками применительно к прикладному программному обеспечению;

– источники угроз информационной безопасности программного обеспечения и меры по их предотвращению;

– уязвимости используемого программного обеспечения и методы их эксплуатации;

– виды и формы функционирования вредоносного программного обеспечения;

– характерные признаки наличия вредоносного программного обеспечения;

– средства и методы обнаружения ранее неизвестного вредоносного программного обеспечения;

– принципы функционирования технологий криптографической защиты информации;

– порядок обеспечения безопасности информации при эксплуатации программного обеспечения;

– нормативные правовые акты в области защиты информации;

– руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации;

– организационные меры по защите информации.

Данный методологический подход также можно рассмотреть как возможные рекомендации для организации и проведения аналогичных сертификационных испытаний и в системе среднего профессионального образования в области информационной безопасности (с учетом требований профессиональных стандартов).

Литература

1. Доктрина информационной безопасности РФ, утверждена Указом Президента Российской Федерации № 646 от 05.12.2016 г.

2. Профессиональный стандарт «Специалист по безопасности компьютерных систем и сетей». Утвержден приказом Министерства труда и социальной защиты Российской Федерации от 1 ноября 2016 г. N 598н.

3. Родионов Б.Н., Титов В.Б., Ярочкин В.И. Энергоинформационная безопасность человека и государства. М.: Паруса, 1997.

4. Павленко А.Р. Защита населения от негативного влияния геопатогенных зон, мониторов, телевизоров. Киев, 1997.

5. Ханцеверов Ф.Р. Эниология. Чудеса без мистики. Книга научных версий. (Книга 2). М., 1999.

6. Соляной В.Н., Сухотерин А.И. Взаимодействие человека, техники и природы: проблема информационной безопасности. Научный журнал (КИУЭС). Вопросы региональной экономики. №5 г. Королев, ФТА, 2010.

7. Рысин Ю. С. Социально-информационные опасности телерадиовещания и информационных технологий. Учебное пособие. М.: Гелиос АРВ, 2007.

8. Перечень специальностей и направлений подготовки высшего образования, соответствующих приоритетным направлениям модернизации и технологического развития российской экономики. Распоряжение Правительства РФ от 6 января 2015 г. №7-р.

9. Соляной В.Н., Сухотерин А.И. Модульно-ориентированный подход формирования базовых дисциплин ФГОС ВО 3+ как основа реализации профессиональной подготовки бакалавров в области информационной безопасности Научно-практический журнал №25, том 2 2015г. «Информационное противодействие угрозам терроризма. Материалы XIX пленума учебно-методического объединения по образованию в области информационной безопасности «Учебно-методическое обеспечение образовательных программ в области информационной безопасности» г. Таганрог, Рост. обл.: Изд-во Южн.фед.унив., 2015.-332 с. ISSN 2219-8792.

10. Соляной В.Н., Сухотерин А.И. Становление направления «Радиоэлектронная безопасность информационных объектов» в системе дополнительного профессионального по информационной безопасности. Научно-практический журнал №25, том 2 2015г. «Информационное противодействие угрозам терроризма. Материалы XIX пленума учебно-методического объединения по образованию в области информационной безопасности «Учебно-методическое обеспечение образовательных программ в области 20Знновационной безопасности» г. Таганрог, Рост. обл.: Изд-во Южн.фед.унив., 2015.-332 с. ISSN 2219-8792.

11. Соляной В.Н., Сухотерин А.И. Практика применения 204нновационного научно-образовательного комплекса по подготовке бакалавров и магистров в области информационной безопасности Научно-практический журнал №25, том 1 «Информационное противодействие угрозам терроризма. **Материалы** XIX пленума учебно-методического объединения по образованию в области информационной безопасности «Учебно-методическое обеспечение образовательных программ в области информационной безопасности» г. Таганрог, Рост. обл.: Изд-во Южн.фед.унив., 2015.-332 с. ISSN 2219-8792.

12. Соляной В.Н., Сухотерин А.И, Шихнабиева Т.Ш., Сиротский А.А. Некоторые элементы ассоциативности в методиках преподавания дисциплин технической направленности. Организация менеджмента информационной безопасности в финансово-кредитных учреждениях. Информационная безопасность бизнеса и общества. Сборник статей научно – преподавательского состава кафедры информационных систем, сетей и безопасности / Российский Государственный Социальный Университет. – М.: Издательство «Перо», 2016.-111 с. ISBN 978-5-906851-15-4