Министерство образования и науки Российской Федерации

Федеральное учебно-методическое объединение
в системе высшего образования по укрупненной группе
специальностей и направлений подготовки
10.00.00 «Информационная безопасность»

Институт криптографии, связи и информатики Академии ФСБ России

Самарский национальный исследовательский университет
имени академика С.П. Королева

САМАРСКИЙ УНИВЕРСИТЕТ
SAMARA UNIVERSITY

ТРУДЫ МЕЖВУЗОВСКОЙ НАУЧНО-ПРАКТИЧЕСКОЙ КОНФЕРЕНЦИИ «АКТУАЛЬНЫЕ ПРОБЛЕМЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ»

Инсома - пресс
Самара, 2017

УДК 681.324
ББК 73
Т 78

Федеральное учебно-методическое объединение в системе высшего образования по укрупненной группе специальностей и направлений подготовки 10.00.00 «Информационная безопасность» (ФУМО ВО ИБ)

Самарский национальный исследовательский университет имени академика С.П. Королева (Самарский университет)

Т 78 Труды Межвузовской научно-практической конференции «Актуальные проблемы обеспечения информационной безопасности». – Самара: Изд-во Инсома-пресс, 2017. – 266 с.

Ответственные за выпуск: Сергеев В.В., Чичева М.А.

ISBN 978-5-4317-0246-4

В настоящий сборник вошли материалы Межвузовской научно-практической конференции «Актуальные проблемы обеспечения информационной безопасности», проводимой в рамках XXI Пленума Федерального учебно-методического объединения в системе высшего образования по укрупненной группе специальностей и направлений подготовки 10.00.00 «Информационная безопасность».

УДК 681.324
ББК 73

ISBN 978-5-4317-0246-4

Межвузовская научно-практическая конференция «Актуальные проблемы обеспечения информационной безопасности» проводится в рамках XXI Пленума Федерального учебно-методического объединения в системе высшего образования по укрупненной группе специальностей и направлений подготовки 10.00.00 «Информационная безопасность» с 20 по 24 мая 2017 года на базе Самарского университета, других образовательных организаций городов Самара, Саратов, Волгоград.

Основные тематические направления конференции:

– концептуальные и прикладные вопросы информационной безопасности;

– профессиональное образование в области информационной безопасности.

Организаторы

Министерство образования и науки Российской Федерации

Федеральное учебно-методическое объединение в системе высшего образования по укрупненной группе специальностей и направлений подготовки 10.00.00 «Информационная безопасность» (ФУМО ВО ИБ)

Институт криптографии, связи и информатики Академии ФСБ России

Региональное отделение ФУМО ВО ИБ по Приволжскому федеральному округу

Управление ФСТЭК России по Приволжскому федеральному округу

Департамент информационных технологий и связи Самарской области

Самарский национальный исследовательский университет имени академика С.П.Королева (Самарский университет)

УДК 004.85

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

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

РЕАЛИЗАЦИЯ МАГИСТЕРСКОЙ ПРОГРАММЫ «МЕНЕДЖМЕНТ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ РЕГИОНА» ПО НАПРАВЛЕНИЮ ПОДГОТОВКИ 10.04.01

Ключевыми задачами в области обеспечения информационной безопасности всегда рассматривались вопросы подготовки кадров. Усложнение задач по информационной безопасности требуют новых подходов по формирования профессионалов в этой области. Появление актуального направления подготовки магистров информационной безопасности обуславливает необходимость обсуждения особенности реализации этого образовательного процесса. В данной статье освещены отдельные особенности подготовки магистров на основе имеющегося опыта их обучения на базе Технологического университета (г. Королев) с частичным использованием интеллектуальных методов. Показаны целевые направленности образовательного процесса в тесном взаимодействии с работодателями региона.

Ключевые слова: информационная безопасность, магистерская программа, менеджмент, регион, интеллектуальные методы, выпускные квалификационные работы, образовательный процесс.

Кафедра информационной безопасности Технологического университета Московской области на протяжении ряда лет готовит магистров в области информационной безопасности по направлению 10.04.01 [1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16]. Актуальность реализации программы подготовки магистров в области информационной безопасности обусловлена следующими факторами:

– существенной потребностью специалистов, обладающих знаниями, умениями и навыками в области информационной безопасности в связи с интенсивным ростом объемов данных, размещаемых и обрабатываемых в информационных ресурсах в облачной среде и веб-приложениях;

– ростом бессистемности и чрезмерности информации в сети Интернет, который не учитывает возрастные и психологические особенности детей;

– сложившейся обстановкой в обществе и мире, где возросла информационная безопасность личности;

– реализацией программы "Национальная технологическая инициатива" [2], направленной на формирование принципиально новых рынков по созданию условий для глобального технологического лидерства нашей страны к 2035 году и перехода к передовым производствам и технологиям, приводящим к росту информационного сегмента производства, безопасность которого необходимо обеспечить.

Как известно, в настоящее время наблюдается повсеместное усиление зависимости успешной деятельности компаний в бизнесе от организационных мер и технических средств контроля и уменьшения рисков в области информационной безопасности.

Реализация магистерской программы по направлению "Менеджмент информационной безопасности региона" также обусловлена спецификой региона (г. Королёв, Московская й область), в котором непосредственно функционирует наш вуз - государственное бюджетное образовательное учреждение высшего образования Московской области «Технологический университет» [1, 2, 3, 5, 6, 7, 8, 10, 14, 15, 16].

Известно, что г. Королёв является одним из крупных научно-производственных центров Московской области, где в довоенные годы был центром развития артиллерии, с 50-х годов прошлого столетия началось создание ряда НИИ, конструкторских бюро, заводов, ставших основой ракетно-космической отрасли страны.

В настоящее время градообразующими являются предприятия:

– РКК "Энергия" им. С.П.Королёва – ведущее предприятие российской космической отрасли;

– ЦНИИМАШ, включающий в себя Центр управления полётами;

– КБ химического машиностроения им. А.М.Исаева (филиал ГКНЦП им. Хруничева) – одно из ведущих КБ в области разработки и испытаний жидкостных ракетных двигателей, двигательных установок и их компонентов;

– НИИ Космических систем им. А.А.Максимова (филиал ГКНЦП им. Хруничева), занимающийся исследованиями и экспериментальными разработками по созданию новой техники и прогрессивных технологий, и в частности: космических, энергосберегающих;

11. Соляной В.Н., Сухотерин А.И. Практика применения иновационного 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

УДК 378.02 (082)

А.И. Сухотерин, В.Н. Соляной, А.Н. Воронов

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

СТАНОВЛЕНИЕ СПЕЦИАЛЬНОСТИ «ИНФОРМАЦИОННО-АНАЛИТИЧЕСКИЕ СИСТЕМЫ БЕЗОПАСНОСТИ» НА ОСНОВЕ РАЗВИТИЯ ПРОФИЛЯ «ИНФОРМАЦИОННО-АНАЛИТИЧЕСКИЕ СИСТЕМЫ ФИНАНСОВОГО МОНИТОРИНГА» – БАКАЛАВР ИБ

Совершенствуя модель высшего профессионального образования, которая предполагает формирование у обучаемых базовых и профильно-специализированных компетенций необходимо ориентироваться на конечный результат подготовки профессионалов по информационной безопасности. Новой специальностью в этой области рассматривается «Информационно-аналитические системы безопасности». Наиболее рациональным путем развертывания данной специальности в вузе следует рассматривать предварительное открытие по направлению 10.03.01 «Информационная безопасность» профиль « Информационно-аналитические системы финансового мониторинга». Данный подход и предложен в статье.

Ключевые слова: информационная безопасность, аналитические системы, финансовый мониторинг, специальность, вуз.

В настоящее время, в век интенсивно развивающихся современных информационных технологий и, в особенности сетевых технологий, создаются все предпосылки для овладения информацией посторонними лицами. В этих условиях существующие проблемы по информационной безопасности постоянно усугубляются во всех сферах современного общества процессами внедрения новых информационных технологий [1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16].

Современное развитие мировой экономики характеризуется всё большей зависимостью рынка от значительного объёма информационных потоков. Несмотря на всё возрастающие усилия по созданию технологий защиты данных (информации), их уязвимость не только не уменьшается, но и постоянно возрастает. Поэтому актуальность проблем, связанных с защитой потоков информационных данных и обеспечением информационной безопасности их

УДК 004.85

В.Н. Соляной, А.И. Сухотерин, Е.Д. Беленко

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

ЭНЕРГОИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ИНФОРМАЦИОННЫХ ОБЪЕКТОВ КАК НЕОБХОДИМАЯ ОБЛАСТЬ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Усложнение задач по обеспечению информационной безопасности в современных условиях является неоспоримым фактом действительности. Принципиально новой задачей в области информационной безопасности (ИБ) следует рассматривать обеспечение безопасности функционирования информационных объектов от скрытых деструктивных энергоинформационных воздействий (излучений) малой интенсивности, исходящих от субъектов (людей), техники и природы. При проявлении резонансных условий данные излучения могут приводить к серьезным нарушениям функционировании современных социотехнических систем. Выявление и разрешение данной проблемы по ИБ в общем виде представлены в материалах статьи.

Ключевые слова: энергоинформационная безопасность, деструктивные воздействия. модель, решения по ИБ.

В современном информационном обществе, в процессе своего бурного развития, начинают проявляться, с одной стороны, странные и, с другой стороны, достаточные опасные и скрытые явления, которые достаточно трудно объясняются или совсем не объясняются традиционной наукой [1,2,3,4,5,6,7,8,9,10,11]. Такие процессы требуют глубокого изучения и учета при обеспечении информационной безопасности защищаемого информационного ресурса на всех уровнях функционирования информационного общества. Именно данная существующая проблема обеспечения информационной безопасности (ИБ) и является предметом обсуждения в данной статье.

В теоретико-прикладном аспекте все объекты информационной защиты следует представлять как сложные социотехнические системы (СТС), включающие три взаимовлияющих друг на друга ключевых компонентов: человек (социум); техника (технические процессы) и окружающая среда (природа). В

этих условиях можно показать существование трех просматриваемых парадигм обеспечения информационной безопасности.

Во-первых, традиционные задачи обеспечения информационной безопасности СТС, в настоящий период времени, реализуются по хорошо разработанной типовой схемы. Данный подход реализуется на уровне достаточно исследуемого процесса по взаимовлиянию материально-вещественных структур и известными физическими полями. При этом такой алгоритм традиционно включает в себя: обнаружение и выявление угроз, нарушителей и уязвимостей (с использованием различных инструментальных, как правило, технических средств); определение ущерба (рисков); обоснование и реализация целесообразных мер по противодействию угрозам с оценкой функциональной и экономической их эффективности. Защищаемые информационные процессы СТС базируются на основе законов классической физики. С учетом изложенного, условно, данный процесс обеспечения ИБ можно представлять как реализация традиционного «материально-вещественного варианта обеспечения информационной безопасности».

Во-вторых, на атомарно-молекулярном (материальном) уроне окружающий мир, включая и СТС, нужно одновременно рассматривать как материальные объекты (в виде большой совокупности взаимовлияющих друг на друга элементарных частиц, находящихся в постоянном движении), так и в виде совокупности излучающих элементарными частицами известных и неизвестных полей (полевой уровень). При этом указанные полевые излучения в обычных условиях существования, как показывают исследования, обладают очень низкой интенсивностью и фактически не фиксируются существующими техническими инструментальными средствами. Такие полевые излучения обладают скрытыми и достаточно высоко проникающими взаимными информационными воздействиями с положительными и деструктивными итоговыми эффектами. Для понимания процессов по обеспечения ИБ современных сложных СТС на полевом уровне можно использовать существующую и достаточно разработанную теорию электронно-магнитных полей на основе одновременного применения принципов классической и квантовой физики. Возможность создания, при определенных внутренних и внешних условиях, в рассматриваемых материально-вещественных объектах естественных или (и) преднамеренных резонансных полевых проявлений и является причиной возникновения достаточно мощных и глубоко проникающих информационно-полевых (типа «электромагнитных») излучений, оказывающих серьезное воздействие на исследуемые информационные процессы и объекты. Данная

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, классифицировать 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; магистра - 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 рас-

ОГЛАВЛЕНИЕ