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;

– ОАО Корпорация “Тактическое ракетное вооружение” - разрабатывает и производит широкий спектр боевых ракетных комплексов и авиационных систем;

– ОАО НПО “Композит” – важнейшая организация в области материаловедения ракетно – космической техники;

– НПО Измерительной техники, которое проводит разработку и исследование информационно – измерительных комплексов и систем, информационно – телеметрического обеспечения, средств диагностики, контроля управления, датчиков и преобразующей аппаратуры.

Кроме приведенных выше предприятий, в Московской области находится ряд объектов стратегического назначения, компании, государственные и частные фирмы, которые нуждаются в специалистах в области информационной безопасности.

Все выше перечисленные предприятия обладают секретной и конфиденциальной информацией, которую необходимо защитить и, естественно, в них функционируют подразделения по защите информации или обеспечению информационной безопасности.

Кафедра информационной безопасности Технологического университета готовит магистров в области информационной безопасности, как для региона, так и для компаний федерального назначения. Для учёта специфики региона дисциплины (модули), относящиеся к вариативной части блока 1 учебного плана дополнены рядом разделов указанной направленности.

Следует отметить, что мировой экономике наносится колоссальный ущерб от компьютерных атак в связи с тем, что применяемые в современных информационных системах традиционные комплексы системы защиты информации практически не позволяют обеспечивать выполнение требований по ее защите.

Ситуация ещё усугубляется в связи с появлением неизвестных ранее типов информационных воздействий и использованием глобальной сети интернет для бизнеса. В системах защиты необходимо управление в реальном 254нноштабе времени – оперативное реагирование на аномальные события и предотвращение возможных неизвестных типов воздействий. Поэтому перспективным направлением обеспечения информационной безопасности является использование интеллектуальных методов и моделей [3] при разработке систем защиты информации [1, 2, 3, 4, 5, 6, 7, 8, 9].

Современные методы и технологии обеспечения информационной безопасности позволяют оценить существующий уровень остаточных информаци-

онных рисков, что особенно важно в тех случаях, когда к корпоративной информационной системе предъявляются повышенные требования в области защиты информации и непрерывности бизнеса. Качественно выполненный анализ информационных рисков позволяет провести сравнительный анализ различных вариантов защиты информации, выбрать адекватные контрмеры и средства контроля, оценить уровень остаточных информационных рисков.

Известно, что инструментальные средства анализа рисков, основанные на нейросетях, методах нечёткой логики и процедурах логического вывода позволяют строить объектно-ориентированные модели активов компаний, модели угроз и рисков, и выделить риск, неприемлемый для компании.

При обнаружении угроз и атак нечеткая логика часто используется совместно с нейронными сетями или экспертными системами, так как сама нечеткая система позволяет лишь выносить предположения о возможной угрозе [10, 11, 12, 13, 14, 15, 16]. В оценке рисков информационной безопасности, оценка показателей риска не имеет четких свойств и неопределенностей. Данный метод количественно оценивает риски информационной безопасности с нечетким подходом к оценке, в частности, осуществляет:

1) анализ активов, уязвимостей, угроз и отношения угрозы и уязвимости к выявлению риска информационной безопасности;

2) на основе нечеткого подхода к оценке, факторы риска создают множество U = {u1,u2,u3..};

3) создаёт набор оценок риска конфиденциальности, степени уязвимости и т. д. V = {v1,v2,v3..};

4) система устанавливает уровень риска для каждого объекта анализа и на этом основании выносит заключение о факторе риска, предлагающемся к набору оценок;

5) на основе полученных данных выносится решение о степени уязвимости системы либо о существовании угрозы.

Преимущества систем обеспечения информационной безопасности (СОИБ) на основе интеллектуальных методов и моделей показаны в таблице 1.

На практике разные методы и модели комбинируются, дополняя друг друга по функционалу. Методы искусственного интеллекта могут браться за основу при построении целостной системы информационной безопасности или же могут быть реализованы отдельно, для поиска уязвимостей или оптимизации процесса управления рисками.

Поэтому при подборе тематики выпускных квалификационных работ 255нгистров преподаватели кафедры большое внимание уделяют использова-

нию перспективных методов, в частности, разработке систем обеспечения информационной безопасности корпоративных информационных систем на основе интеллектуальных методов и моделей.

Таблица 1 – Сравнительная характеристика интеллектуальных СОИБ и традиционных

Традиционные методы	***Интеллектуальные методы***
Осуществляют проверку подлинности субъекта, например по паролю, PIN-коду, криптографическому ключу и т.д.	Осуществляют проверку подлинности субъекта, не только по паролю, PIN-коду, криптографическому ключу и т.д., но и по биометрическим признакам или интеллектуальным смарт-картам
Обеспечивает защиту от известных вирусов и другого вредоносного программного обеспечения	Обеспечивает защиту от известных вирусов и другого вредоносного программного обеспечения, а также 256ннолиз файлов и выявление новых видов вредоносного программного обеспечения
Обеспечивает защиту от известных видов атак, попыток несанкционированного доступа, их блокировка	Проводит анализ трафика и выявление новых, неизвестных ранее видов угроз и уязвимостей
Позволяет зашифровывать данные для более безопасной передачи по каналам связи	Позволяет автоматизировать периодическую смену криптографических ключей

Кроме того, при подборе комиссии Государственной итоговой аттестации магистров обращают внимание на тот факт, чтобы в её состав обязательно вошли представители работодателей.

Основными направленностями подготовки магистров по информационной безопасности с учетом требований работодателей, являются:

– по масштабности объектов информационной защите – это, прежде всего, региональные корпоративные (распределенные) информационные объекты (предприятия, организации, учреждения, фирмы и т.п.), функционирующие с использованием современных Интернет – систем;

– по областям информационной безопасности региона – это, в порядке их приоритетности, исследовательски-аналитическая деятельность, 256нноваци-

оннонно-управленческая сфера, проектно-эксплуатационная область и образовательно-педагогическая деятельность.

Примерная тематика выпускных квалификационных работ по рассматриваемой магистерской программы «Менеджмент информационной безопасности региона» [14, 15, 16]:

– совершенствование системы информационной безопасности регионального научно-исследовательского учреждения на основе разработки интеллектуальной подсистемы управления электронным документооборотом;

– совершенствование системы информационной безопасности регионального холдинга на основе внедрения корпоративной технологии электронной подписи;

– разработка концептуальных основ построения проактивной системы физической защиты информационных объектов региона;

– региональный анализ применения современных технологии по информационной безопасности в образовательном процессе;

– бизнес-план по обеспечению информационной безопасности на корпоративных предприятиях;

– создание информационной системы мониторинга региональной информационной безопасности;

– построение информационной системы анализа и прогнозирования информационной безопасности в региональных финансовых структурах;

– разработка информационной системы экспресс-анализа состояния информационной безопасности на корпоративных информационных объектах;

– создание информационной системы безопасности региональных объектов малого и среднего бизнеса;

– контроль и оценка информационной безопасности в современных корпоративных информационных системах;

– методика определения экономической эффективности систем информационной безопасности регионального предприятии;

– построение системы информационной безопасности геоинформационных систем в регионе;

– разработка системы управления информационной безопасностью на региональном предприятии;

– создание региональной мультимедийной системы контроля эффективности обеспечения информационной безопасностью;

– разработка программы стандартизации в области обеспечения информационной безопасностью IT технологий для региональных предприятий;

– создание информационной системы защищенного электронного документооборота на корпоративном предприятии;

– разработка информационной системы планирования деятельности регионального предприятия по обеспечению информационной безопасностью.

Другой особенностью проведения обучения магистров в Технологическом университете следует рассматривать возможность студентам одновременно работать (по выбранной направленности информационной безопасности) на предприятиях (организациях и учреждениях) региона и получать образования. При этом учебные занятия проводятся вечером два раза в течение рабочей недели и в ходе одного выходного дня (суббота или воскресенье).

Технологический университет проводит мероприятия по гарантии обеспечение качества подготовки магистров на основе разработки и реализации:

– стратегии по обеспечению качества подготовки выпускников с привлечением представителей работодателей;

– мониторинга, периодического рецензирования, образовательных программ;

– объективных процедур оценки уровня знаний и умений обучающихся, компетенций выпускников;

– обеспечения компетентности преподавательского состава;

– регулярного проведения само обследования по согласованным критериям для оценки деятельности (стратегии) и сопоставления с другими образовательными учреждениями с привлечением представителей работодателей;

– информирования общественности о результатах своей деятельности, планах, инновациях.

Реализация компетентностного подхода в процессе подготовки магистров в университете предусматривает широкое использование в учебном процессе активных и интерактивных форм проведения занятий (компьютерных симуляций, деловых и ролевых игр, разбора конкретных ситуаций, психологических и иных тренингов) в сочетании с внеаудиторной работой с целью формирования и развития профессиональных компетенций обучающихся. В процессе обучения предусматриваются встречи с представителями российских и зарубежных компаний, государственных и общественных организаций, мастер-классы экспертов и специалистов, посещение специализированных выставок по информационной безопасности.

Научно-исследовательская работа магистрантов рассматривается, как обязательный этап подготовки и направлена на формирование как общекультурных, так и профессиональных компетенций. Выпускающая кафедра ин-

формационной безопасности университета предусматривает следующие виды, этапы выполнения и контроля научно-исследовательской работы магистрантов:

– планирование научно-исследовательской работы, включающее ознакомление с тематикой исследовательских работ в данной области и выбор темы исследования, написание реферата по избранной теме;

– проведение научно-исследовательской работы;

– составление отчета о научно-исследовательской работе;

– публичная защита выполненной работы;

– авторская публикация полученных результатов исследований.

В процессе выполнения научно-исследовательской работы и в ходе защиты ее результатов проводиться широкое обсуждение в учебных и научных структурах университета с привлечением работодателей и ведущих исследователей региона, позволяющее оценить уровень приобретенных компетенций обучающихся. При этом широко используется студентами метод группового проектирования по задачам, формируемыми работодателями и совместно с ними реализуемыми на всех этапах исследований [1,2,10,11,12,13,14,15,16].

Непосредственное научное руководство подготовкой магистрантов осуществляется высоко подготовленными преподавателями, имеющими ученую степень доктор наук и ученое звание профессор.

Руководство кафедры информационной безопасности тщательно проводит отбор контингента для обучения в магистратуре. Так, набор в магистратуру формируется из бакалавров – выпускников соответствующего и других направления подготовки в области информационной безопасности, а также ведётся целевой набор бакалавров и специалистов с предприятий, федеральных и региональных организационных структур и выпускников вузов на основании конкурсного отбора.

Литература

1. Федеральный государственный образовательный стандарт высшего образования по направлению подготовки 10.04.01 Информационная безопасность (уровень магистратуры)//Приказ Министерства и образования РФ. Регистрационный №44823 от 20 декабря 2016 г.

2. Национальная технологическая инициатива. Агентство стратегических инициатив [Электронный ресурс] //URL: http://asi.ru/nti (дата обращения: 19.09.2016 г.)

3. Шихнабиева Т.Ш. Использование интеллектуальных методов и моделей в системе обучения и контроля знаний при подготовке специалистов в области информационной безопасности// Сборник трудов по материалам II Международной научно-практической интернет – конференции “Инновационные технологии в современном образовании”, Королёв, 2015. С. 437- 443.

4. Брюхомицкий Ю.А. Нейросетевые модели для систем информационной безопасности. Учебное пособие // Таганрог, 2005.

5. Степанушко И.В., Трегубенко И.Б. Интеллектуальные средства для решения задач классификации в системах защиты информации// Черкасский государственный технологический университет, 2010. Доктрина 260нновационной безопасности РФ, утверждена Указом Президента Российской Федерации № 646 от 05.12.2016 г.

6. 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.

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

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

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

10. 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.

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

12. 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.

13. 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.

14. 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 261нновационной безопасности» г. Таганрог, Рост. обл.: Изд-во Южн.фед.унив., 2015.-332 с. ISSN 2219-8792.

15. Соляной В.Н., Сухотерин А.И. Практика применения 261нновационного 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.

16. 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