СЕКЦИЯ 6
ОБУЧЕНИЕ В ОБЛАСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

ОБУЧАЮЩИЕ СИСТЕМЫ НА ОСНОВЕ ИНТЕРАКТИВНЫХ МУЛЬТИМЕДИЙНЫХ МОДУЛЕЙ

Л.А. Конюх, Н.И. Кобринец, С.Е. Карпович

Современные информационные технологии позволяют разрабатывать и эффективно применять различные средства обучения, моделирования и интерактивного исследования. Современный уровень персональных компьютеров и их программного обеспечения дают возможность разрабатывать алгоритмы и программное обеспечение обучающих систем, в том числе и в области технических средств защиты информации.

Научные исследования в этом направлении в последние годы ведутся в учебно-научной лаборатории «Математическое моделирование технических систем и информационные технологии» БГУИР [1]. Анимация, интерактивность и средства мультимедиа, применяемые в наших разработках, позволили создать программные средства – мультимедийные модули – для интерактивного исследования колебательных механических систем, пневматических элементов и систем и других технических объектов. Интерактивные мультимедийные модули разрабатываются как вполне законченные информационные страницы, содержащие запрограммированные математические алгоритмы физических законов или технических принципов. При этом алгоритм имитационного моделирования является сегментированным, то есть, каждый элемент, вводимый интерактивно на рабочее поле монитора, имеет алгоритмический интерфейс, согласованный с основным алгоритмом, описывающим объект визуализации. То же относится и к исключению элементов из рабочего поля. Исключенный элемент как сегмент алгоритма, не нарушает функциональность и достоверность расчета по основному алгоритму, обеспечивающему моделирование и визуализацию.

В настоящей работе рассматривается возможность приложения полученных результатов к разработке интерактивных мультимедийных модулей для технических средств защиты информации.

Литература

1. Интерактивный мультимедийный модуль исследования в реальном режиме времени колебательных систем / С.Е. Карпович [и др.] // Теоретическая и прикладная механика. – 2017. – № 32. – С. 117–123.

ОСОБЕННОСТИ ПОДГОТОВКИ СПЕЦИАЛИСТОВ ПО ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В УСЛОВИЯХ НОВЫХ ВЫЗОВОВ И УГРОЗ КИБЕРНЕТИЧЕСКОГО И ИНФОРМАЦИОННО-ПСИХОЛОГИЧЕСКОГО ХАРАКТЕРА

В.Е. Макаров

В современных условиях одним из важнейших и решающих направлений совершенствования и повышения эффективности организации системы информационной безопасности отдельных организационных структур, общества и государства является подготовка профессиональных кадров, обучающихся в системе высшего профессионального образования по решению не только технических и технологических задач обеспечения технической защиты информации, но и вопросов прогнозирования, выявления, анализу и оценке угроз информационной безопасности; определению основных направлений государственной политики и стратегическое планирование в области обеспечения информационной безопасности; разработке и применению комплекса оперативных и долговременных мер по выявлению, предупреждению и устранению угроз информационной безопасности, локализации и нейтрализации последствий их проявления.

По нашему мнению, многообразие политических и социальных фактов обеспечения информационной безопасности по большому счету, сводится к двум важнейшим проблемам

современности: защите информации и защите от информации, т.е. противодействию информационно-кибернетических операций и информационно-психологических операций. Все это обусловило не только чисто теоретический интерес, но и практическую значимость изучения и исследований информационных операций в контексте реализации управления социальными системами, которое с каждым днем становится все более информационным.

При разработке и реализации учебного плана на кафедре «Информационной безопасности» НИУ МИЭТ г. Москва реализован новый подход в обучении студентов по изучению влияния политических и социальных аспектов на обеспечение информационной безопасности личности, социальных групп, общества и государства в современных условиях усилившегося информационного воздействия со стороны США и некоторых стран Западной Европы. С системных позиций изучаются сведения об эволюции информационного противоборства и о современных технологиях информационного воздействия в социальных системах, анализируется система социальных и политических отношений современного информационного общества как среда организации и проведения тайных операций информационной войны. С современных позиций рассматриваются основные направления противодействия информационной агрессии вероятного противника в современных условиях развития Российской Федерации.

Реализация компетентностного подхода предусматривает широкое использование в учебном процессе активных и интерактивных форм проведения занятий (семинаров в диалоговом режиме, дискуссий, компьютерных симуляций, деловых и ролевых игр, разбора конкретных ситуаций, психологических и иных тренингов, групповых дискуссий, результатов работы студенческих исследовательских групп, вузовских и межвузовских исследовательских групп, вузовских и межвузовских телеконференций) в сочетании с внеаудиторной работой с целью формирования и развития профессиональных навыков обучающихся.

Литература

1. Макаров, В.Е. Политические и социальные аспекты информационной безопасности / В.Е. Макаров. – Таганрог: С.А. Ступин, 2015. – 352 с.

2. Основы информационной безопасности / Е.Б. Белов [и др.]. – М.: Горячая линия–Телеком, 2006. – 544 с.

3. Брусницын, Н.А. Информационная война и безопасность / Н.А. Брусницын. – М.: Вита-Пресс, 2015.– 280 с.

4. Панарин, И.Н. Информационная война и коммуникации / И.Н. Панарин. – М.: Горячая линия–Телеком, 2014. – 236 с.

ОБУЧАЮЩЕЕ ПРОГРАММНОЕ СРЕДСТВО ПО ДИСЦИПЛИНЕ «ЗАЩИТА КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ»

В.И. Пачинин, А.В. Яковлев

Рассматривается задача проектирования обучающего программного средства по дисциплине «Защита компьютерной информации» для специальности «Программное обеспечение информационных технологий» 2-40 01 01. Для реализации задачи используется несколько алгоритмов шифрования, начиная от простых (алгоритм Цезаря), заканчивая симметричными и асимметричными алгоритмами шифрования. Язык разработки Java. В качестве входных данных используется: ФИО пользователя, алгоритм шифрования, способы защиты информации личной и коммерческой. Программное средство демонстрирует детальное описание способов защиты информации с набором пошаговых действий, начиная от защиты помещений и правил поведения, заканчивая алгоритмами шифрования. На знание правил и способов защиты информации проводится тестирование, где студенту предлагается выбрать правильное действие. Используется несколько этапов изучения шифров. Первый подразумевает пошаговую демонстрацию шифрования данных с указанием вариантов программной реализации. На втором этапе изучения алгоритма, программа предлагает варианты шагов шифрования на выбор, необходимо указать их в нужной последовательности и исключить лишние. Третий этап исключает часть описания, чтобы студент сам его реализовал, после чего