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

программа проверяет предложенный вариант. За каждый этап выполнения выставляются баллы, после чего они суммируются. Программа учитывает время выполнения задания. Также проводится анализ ошибок с указанием неверных действий.

Программное средство может применяться на практических и лабораторных занятиях. Оно моделирует различные ситуации, при которых полезная информация может подвергнуться угрозе раскрытия или повреждения. Также в разделе «Законодательство» указаны все законодательные акты Республики Беларусь в сфере защиты информации. Использование данного обучающего программного средства позволит сократить время на проверку знаний по итогам изучения алгоритмов шифрования и способов защиты информации.

Примечание редколлегии. Тексты тезисов докладов, вошедших в настоящий сборник, представлены в авторской редакции.