локальным освещением рабочего места этими типами ламп необходимо всегда использовать и общее освещение.

АСПЕКТЫ ПРИМЕНЕНИЯ НОВЫХ ТЕХНИЧЕСКИХ РЕШЕНИЙ В ОБРАЗОВАНИИ

Г.А. Власова

Быстрое развитие технических и программных средств для систем передачи, хранения и обработки информации требует постоянного обучения персонала. Поэтому значительная часть экспозиции выставки «ТИБО 2015» была посвящена техническим решениям для образования. Среди них можно выделить:

1) аудио- и видеосистемы для образования (аудиторные акустические системы с излучением на 360°, обеспечивающие высокую равномерность звукового давления по всей площади аудитории, с бесшнуровым микрофоном-пультом дистанционного управления и возможностью изменения режима звучания; интерактивные сенсорные системы с экраном multi-touch производства HORIZONT с диагональю 42´´ либо 65´´ и Panasonic с диагональю 50´´, 65´´ либо 80´´;

2) цифровые лаборатории и компьютерное моделирование процессов и устройств в учреждениях образования;

3) системы видео-конференц-связи для дистанционного обучения и корпоративных коммуникаций (Cisco, Yealink).

Подобные системы позволяют повысить качество образовательного процесса и сократить затраты на обучение. Так, устраняется необходимость использования в учебном процессе дорогостоящего оборудования и материалов. Кроме того, программа обучения становиться гибкой, легко масштабируемой, позволяет отслеживать тенденции развития техники и технологии. Это расширяет компетенцию обучаемых специалистов, позволяет им создавать актуальные решения для различных информационных систем.

Важно и то, что снижается нагрузка на главный инструмент лектора - голос. Имеются данные, что преподаватели страдают от заболеваний голосовых связок в 32 раза чаще, чем остальные люди.

ИСПОЛЬЗОВАНИЕ DLP-СИСТЕМЫ В ПОДГОТОВКЕ СПЕЦИАЛИСТОВ ПО ЗАЩИТЕ ИНФОРМАЦИИ

А.М. Кадан, М.К. Рудь, П.С. Французов, В.И. Цидик

При обучении студентов современным высокотехнологичным специальностям, к которым можно отнести область защиты информации, учебные заведения часто не располагают современной программно-технической инфраструктурой, которая позволила бы вести современное практико-ориентированное обучение. В связи с этим важную роль приобретает сотрудничество вузов с ИТ-компаниями, разработчиками популярных продуктов и специализированных программных систем.

Так для обеспечения подготовки студентов специальностей «Компьютерная безопасность» (специализация «Защищенные информационные системы») и «Управление информационными ресурсами» в рамках договора о сотрудничестве ГрГУ им. Я.Купалы и компании «ИнфоВотч» создан учебный стенд продукта «InfoWatch Traffic Monitor».

Стенд представляет собой DLP-систему систему (DLP - Data Leak Protection, защита от утечек информации), адаптированную к использованию в условиях вуза. Программное обеспечение стенда допускает контроль таких каналов утечки, как передача данных по протоколам SMTP, HTTP, HTTPS, копирование файлов на сменные носители, печать документов на локальных и сетевых принтерах, службы обмена сообщениями Skype, Jabber, ICQ, хранение документов на рабочих станциях и сетевых папках.

Стенд позволяет демонстрировать технологии решения целого класса учебных задач из области защиты информации: предотвращения утечек и контроля перемещения конфиденциальной информации за пределы организации; предотвращения утечек

персональных данных и клиентских баз; защиты интеллектуальной собственности; применения целевых политик контроля персонала, входящего в т.н. «группы риска»; расследования инцидентов информационной безопасности и пр.

Выполнена настройка конфигурации его баз контекстной фильтрации, шаблонов, цифровых отпечатков в соответствии с требованиями системы менеджмента университета, ведется формирование и отслеживание учебной базы данных инцидентов.

О ПОДГОТОВКЕ СПЕЦИАЛИСТОВ В ОБЛАСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ВОЕННОМ ВУЗЕ

Л. В. Михайловская, Е. В. Валаханович

Современные тенденции развития инженерных технологий требуют адекватной корректировки содержания процесса преподавания дисциплин, изучающих средства и методы информационной безопасности, формирующих высокий уровень подготовки будущего специалиста.

В военно-инженерном вузе в большей степени, чем в гражданском вузе, необходимо создание особой педагогической технологии, позволяющей по возможности снизить неблагоприятное влияние факторов, связанных с особенностями обучения курсантов, таких как: объективной необходимости пропуска занятий курсантами, ограничением времени на самостоятельную подготовку, приоритетом физической подготовки по отношению к общеобразовательной.

В целях уменьшения влияния вышеперечисленных факторов на процесс обучения в области информационной безопасности в Военной академии Республики Беларусь на кафедре высшей математики разработан электронный учебно-методический комплекс (ЭУМК) по дисциплинам «Прикладная математика» и «Защита информации».

В частности, ЭУМК содержит цикл лабораторных работ, позволяющий курсантам закрепить теоретический курс и самостоятельно совершенствовать свои силы по взлому современных криптографических систем различной степени сложности. ЭУМК является сетевым ресурсом, доступным в полном объеме для обучаемых, позволяющий курсантам самостоятельно изучить учебные вопросы, следуя подсказкам и пояснениям. Данный комплекс, кроме того, служит действенным инструментом для углубленного изучения предмета. Следует отметить возможности оперативной модификации учебного материала в ЭУМК и построения индивидуальной траектории обучения для каждого курсанта, что позволяет осуществлять качественную подготовку военных инженерных кадров адекватно требованиям времени и современным тенденциям развития технологий.

СТАНДАРТ ШИФРОВАНИЯ AES В УЧЕБНОМ ПРОЦЕССЕ

В. А. Липницкий, Л. В. Михайловская

В 2001 году в западном мире стандарт шифрования DES канул в лету и был заменен новым стандартом AES (Advanced Encription Standart). Почти пятнадцатилетний практический опыт работы с этим стандартом демонстрирует его полную надежность и криптографическую стойкость.

DES и AES относятся к одному классу систем шифрования с закрытыми ключами. Это - поточные шифры, применяемые в быстрых системах передачи информации. В отличие от DES, который работает с небольшими блоками информации в 32 бит, AES за один такт обрабатывает в 4 раза больший блок двоичной информации. Основу DES составляют комбинаторные преобразователи, в криптосистеме AES задействованы методы, ориентированные на применение современной вычислительной техники. Обрабатываемый блок разбивается в матрицу 4x4, элементы которой в процессе работы алгоритма представляются в виде двоичных байт, двузначных шестнадцатеричных чисел, полиномами с коэффициентами из Z/2Z – элементами поля Галуа из Z/2Z. Каждая форма соответствует своему классу криптографических преобразований. Сильное рассеивание и