за критические замечания по уточнению сценариев и советы по программной реализации лабораторных работ (bsm@bsuir.by).

БЕЗОПАСНОСТЬ ИНФОРМАЦИИ И ОБЕСПЕЧЕНИЕ НАДЁЖНОСТИ КОМПЬЮТЕРНЫХ СЕТЕЙ

В.А. ГАНЖА, О.И. ЧИЧКО

В докладе представлены соображения, мысли и примеры методики обучения защите информации как в информационных системах в общем, так и в компьютерных сетях в частности. Эти материалы апробированы авторами на протяжении ряда лет преподавания в различных вузах и перед различными слушательскими аудиториями.

В силу большой насыщенности литературой как русскоязычной, так и на английском языке по информационной безопасности и по криптографии, построение лекционной части курса, обычно, затруднений не вызывает.

Акцентируется внимание на проведении практических и лабораторных занятий. Рассматривается работа обучаемых с простейшими пакетами и утилитами, создающими хэш-функции по алгоритмам MD5, SHA1. Иллюстрируются возможности простейших пакетов стеганографии.

На занятиях проводится простейший криптоанализ со студентами, на примере взлома запароленых архивов в зависимости от длины ключа и его состава (только цифры, только буквы, и буквы и цифры). Разбираются некоторые аспекты использования пакетов PGP (платформа Microsoft Windows) и GPG (платформа Linux) для практической работы с обучаемыми.

Генерация пары ключей (публичного и приватного) для осуществления и иллюстрации метода асимметричного шифрования. Организация тренинга обучаемых по рассылке и получению электронной почты с использованием приватных и публичных ключей. Методы аутентификации сообщений, создание цифровой подписи в пакете PGP и верификация этой подписи.

Курирование и руководство самостоятельного задания обучаемых по проекту построения небольшой локальной компьютерной сети с привязкой отдельных компонентов оборудования к 7-уровневой модели OSI и реализация функций информационной безопасности конкретными уровнями этой модели.

МОБИЛЬНАЯ СИСТЕМА ЭКСПРЕСС-ОПРОСА СТУДЕНТОВ

А.А. ДЕРЮШЕВ

При преподавании студентам технических предметов большое значение имеет постоянный контроль знаний студентов. Повышение качества данного контроля и его оперативности невозможно без использования вычислительной техники, однако при увеличении числа контролируемых студентов до 100-150 (экспресс-опрос на лекции) человек делает невозможным использование персональных компьютеров. Можно использовать системы электронного голосования типа Hitachi Verdict, состоящие из базового модуля, подключаемого к компьютеру, и персональных пультов студентов. Однако данные системы, как правило, ограничиваются небольшим числом персональных пультов (16-32), а также требуют существенных затрат на свое приобретение.