

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

БЕЗОПАСНОСТЬ ИНФОРМАЦИИ И ОБЕСПЕЧЕНИЕ НАДЕЖНОСТИ 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 запароленных 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.

В то же время, практически каждый студент имеет в своем распоряжении как минимум один сотовый телефон. Технический уровень этих телефонов различен, однако все позволяют отправлять SMS, что и послужило отправным пунктом для разработки системы.

Созданная система состоит из двух модулей. Первый модуль включает сотовый телефон преподавателя с ОС Android и разработанной программой, содержащей базу данных. Второй модуль выполнен в виде сайта и предназначен для организации удобного доступа студентов к результатам опроса. Работа системы начинается с заполнения таблицы сведений о студентах, для чего каждый из них должен прислать SMS, содержащее специальный символ, ФИО и номер группы. В таблице предусмотрены поля для трех различных телефонов для каждого студента. Заполнение таблицы происходит в автоматическом режиме; при необходимости она может быть подкорректирована вручную. Другая таблица содержит набор возможных вариантов ответов на каждый вопрос и баллы за каждый вариант ответа для данного теста. Процесс опроса заключается в демонстрации студентам мультимедиа слайдов с вопросами и вариантами ответов. Каждый вопрос предполагает возможность нескольких ответов, которые разделяются запятой. После ответа на один вопрос, студент ставит точку с запятой и отвечает на следующий. После ответа на все вопросы SMS отправляется на номер преподавателя, после чего производится его разбор с подсчетом набранных баллов. Затем информация из телефона передается в серверную базу данных.

ПОВЫШЕНИЕ ЭФФЕКТИВНОСТИ ПОДГОТОВКИ СПЕЦИАЛИСТОВ ПО НАПРАВЛЕНИЮ КОМПЛЕКСНОЙ БЕЗОПАСНОСТИ

В.В. МАЛИКОВ

Для повышения эффективности самостоятельного получения новых знаний в режиме 24*7*365, предлагается построение процесса обучения на основе адаптированного алгоритма широко вещания источник-получатель: multicast.

Основные этапы для эффективной адаптации алгоритма multicast к процессу обучения:

- путем проведения/участия в разноплановых on-line/off-line семинарах/конференциях, проработке типовых групп/профилей социальных сетей, форумах сформированных сообществ, выделить среди всего профессионального сообщества наиболее мотивированную его часть по определенным критериям: профессионализм, инициативность, стремление к постоянному профессиональному развитию;
- в рамках выделенного подмножества сообщества сформировать инициативную группу из представителей: регуляторов отрасли, академического образования, производителей/интеграторов современных информационных систем;
- детально изучить конкретные потребности регуляторов отрасли, академического образования, производителей/интеграторов современных информационных систем, а также других членов профессионального сообщества;
- создать единый специализированный on-line ресурс доступа к актуальной информации по современным информационным технологиям;
- анонсировать и проводить тематические off-line семинары/конференции с участием компетентных специалистов регуляторов отрасли, академического образования, производителей/интеграторов современных информационных систем, а также лидеров профессионального сообщества;