

СПОСОБ ИЗУЧЕНИЯ СВОЙСТВ СИГНАЛОВ В ИНФО-ТЕЛЕКОММУНИКАЦИОННЫХ СЕТЯХ ПРИ ВЫБОРЕ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ

И.И. ЧЕРНАЯ, Я.В. РОЩУПКИН

Современный этап развития инфо-телекоммуникационных сетей выдвигает на первый план решение задачи надежной защиты передаваемой информации, в том числе, и с помощью технических средств.

Однако, чтобы грамотно и эффективно разрабатывать и использовать такие средства необходимо изучить и проанализировать свойства и особенности сигналов, передаваемых по инфо-телекоммуникационным сетям.

В докладе представлен способ и программа такого экспресс-анализа, который позволяет исследователям, а также студентам и магистрантам быстро получить сведения о таких параметрах, как спектры сигналов различного вида и формы, виды модуляции; амплитуда, частота, фаза, период и длительность импульсов и др. Возможно проведение анализа как аналоговых, так и цифровых сигналов.

Кроме того способ позволяет задавать различные параметры сигналов и изменять их по мере необходимости в соответствии с предложенным заданием.

Способ и программа успешно опробованы при проведении лабораторных занятий со студентами.

ПРАКТИЧЕСКАЯ ПОДГОТОВКА СТУДЕНТОВ ПО ДИСЦИПЛИНЕ «НАДЁЖНОСТЬ ТЕХНИЧЕСКИХ СИСТЕМ» СПЕЦИАЛЬНОСТИ «ЭЛЕКТРОННЫЕ СИСТЕМЫ БЕЗОПАСНОСТИ»

С.М. БОРОВИКОВ, Е.Н. ШНЕЙДЕРОВ, Р.П. ГРИШЕЛЬ,
Н.А. ЖАГОРА, В.Е. МАТЮШКОВ

Одной из важнейших учебных дисциплин профессиональной подготовки по специальности «Электронные системы безопасности» является дисциплина «Надёжность технических систем». Для формирования и развития у студентов навыков практической подготовки по этой дисциплине служат лабораторные занятия. Возникает вопрос, что должен представлять собою лабораторный практикум по дисциплине «Надёжность технических систем»?

Для проведения лабораторных работ нужны испытания на надёжность отдельных частей системы. Организация и проведение работ с использованием классических, пусть даже ускоренных форсированных испытаний практически невозможна. Объясняется это тем, что надёжность электронных устройств и систем является свойством, которое проявляется с течением длительного времени работы (наработки) технических устройств: тысячи и даже десятки тысяч часов.

Анализ показывает, что выходом из положения является математическое моделирование наработки технических частей системы безопасности на основе достижений информационных технологий. Сам практикум в этом случае должен представлять виртуальные лабораторные работы. Слово «виртуальные» подчёркивает то, что исследуемые элементы, устройства, системы и их функционирование (длительная наработка, возникновение отказов, определение состояния работоспособности или неработоспособности) будут моделироваться в памяти ЭВМ. Интересующие закономерности и итоговые показатели надёжности устройств и системы в целом можно будет определить, выполняя обработку результатов моделирования.

Работы, проведённые авторами, показали, что наиболее сложным этапом создания виртуального лабораторного практикума является написание удачных сценариев к лабораторным работам. Авторы будут благодарны за советы, предложения и рекомендации

по подготовке новых сценариев к лабораторным работам. Справки и предложения по e-mail: bsm@bsuir.by.

ПОДГОТОВКА СТУДЕНТОВ ПО УЧЕБНОЙ ДИСЦИПЛИНЕ «ИНТЕЛЛЕКТУАЛЬНЫЕ ЭЛЕКТРОННЫЕ СИСТЕМЫ БЕЗОПАСНОСТИ»

С.М. БОРОВИКОВ, Е.Н. ШНЕЙДЕРОВ, И.Н. ЦЫРЕЛЬЧУК, В.А. КОВАЛЕНКО

Реалии сегодняшнего рынка электронных систем безопасности (ЭСБ) требуют нового подхода к подготовке специалистов в области обеспечения безопасности объектов и физических лиц. Многофункциональные интеллектуальные системы безопасности, построенные на IP и IT-технологиях, становятся наиболее востребованными, вытесняя традиционные системы. Например, такие высокотехнологичные решения, как «Умный дом», «Безопасный город», отвечают критериям самых требовательных заказчиков по безопасности объектов жизненно важной инфраструктуры. Этим объясняется введение в специальность «Электронные системы безопасности» новой учебной дисциплины «Интеллектуальные электронные системы безопасности», основной задачей которой является внедрение достижений компьютерной техники и её программного обеспечения в процессы функционирования электронных систем безопасности.

В докладе сообщается о содержании учебной дисциплины, указываются знания, которые получит студент и рассматриваются навыки и умения, которые будут сформированы в результате изучения дисциплины и выполнения курсового проекта. В частности, в результате изучения дисциплины студент должен научиться выбирать структуру и разрабатывать алгоритмы функционирования интеллектуальных электронных систем безопасности (ИЭСБ) в зависимости от особенностей объекта и задач, возлагаемых на систему безопасности; обоснованно выбирать аппаратно-программную платформу для объединения аппаратных частей системы безопасности в автоматизированную систему управления; обеспечивать аппаратно-программную реализацию алгоритмов функционирования подсистем автоматизации, работающих в составе ИЭСБ; программировать микропроцессорную технику и ЭВМ, встраиваемые в ИЭСБ.

Указанные профессиональные умения позволят проектировать современные интеллектуальные электронные системы безопасности, в том числе системы, обеспечивающие информационную безопасность.