

безопасности является актуальной, поскольку надёжность технических систем представляет такое свойство, которое проявляется в течение длительного времени.

В докладе сообщается о разработке шести виртуальных лабораторных работ:

1. Определение надёжности электронных устройств моделированием на ЭВМ отказов элементов.

2. Проверка правильности выбора элементов электронного каскада по коэффициентам электрической нагрузки.

3. Оценка надёжности электронной системы безопасности методом прямого перебора её работоспособных состояний.

4. Определение надёжности электронной системы безопасности методом построения дерева её отказов.

5. Исследование эффективности функционирования электронной системы безопасности с учётом работоспособности технических устройств и вероятностей правильного восприятия и/или обработки сигналов об угрозах.

6. Отбор компонентов технических систем требуемого уровня надёжности методом индивидуального прогнозирования.

Разработчики компьютерных лабораторных работ по учебной дисциплине НТС будут признательны специалистам за критические замечания по уточнению сценариев и советы по программной реализации лабораторных работ (bsm@bsuir.by).

## **ПОДГОТОВКА СПЕЦИАЛИСТОВ В ОБЛАСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПО ЗАОЧНОЙ ФОРМЕ ОБУЧЕНИЯ**

С.А. БУРЛЯЕВ

Одним из государственных приоритетов в Республике Беларусь провозглашена ориентация на современное информационное общество и развитие рынка информационных услуг [1]. В связи с этим, подготовка высококвалифицированных специалистов в области информационных технологий является одними из важнейших направлений деятельности государства на современном этапе.

На фоне этого, в последнее время, всё чаще появляется информация о том, что в Беларуси будет сокращаться система заочного образования, аргументируя это тем, что качество обучения на заочном отделении недостаточное. Есть мнение, что при получении образования по заочной форме невозможно получить достаточно полноценные знания. Все это глубокое заблуждение.

Заочное образование сначала появилось как форма обучения для тех, кто не имеет физической возможности присутствовать в учебном заведении. Сейчас заочно учатся те, кто не может себе позволить тратить время на очное обучение или не имеет денег для этого. Заочное образование позволяет сочетать учёбу с работой и для многих является единственным способом получения диплома.

Безусловно, программа очного обучения охватывает гораздо больший объём знаний, но, в основном, это пустая теория, которая, как известно, мертва без практики.

Для специалистов, занимающихся информационной безопасностью особенно важны именно практические навыки, которые возможно получить, лишь работая в данной области, и здесь заочное образование подходит, как нельзя кстати. Другое дело, получит ли студент достаточный объём теоретических знаний, и какой опыт приобретет, зависит только от самого студента.

Заочное отделение предполагает серьёзную самостоятельную подготовку и требует от студента высокой личной самоорганизации, упорства, усидчивости и реальной заинтересованности в достижении поставленных целей. Без личного интереса к специальности, без мотивации и стремления любая форма обучения будет бесполезной.

## Список литературы

1. О Стратегии развития информационного общества в Республике Беларусь на период до 2015 года и плане первоочередных мер по реализации Стратегии развития информационного общества в Республике Беларусь на 2010 год / Постановление Совета Министров Республики Беларусь 9 августа 2010 г. № 1174. — [Электронный ресурс]. — <http://pravo.by/webnpa/text.asp?RN=C21001174>. — Доступ 29.04.2014.

## **СИСТЕМА ДЛЯ ИЗУЧЕНИЯ И ОТЛАДКИ МИКРОПРОЦЕССОРНЫХ УСТРОЙСТВ**

А.И. ГУЛЬКОВ, А.А. ДЕРЮШЕВ

С каждым годом уровень технических систем в области информационной безопасности развивается стремительными темпами. Это вызывает необходимость подготовки квалифицированных специалистов, работающих в этой области, при этом большое значение необходимо уделить изучению микропроцессорных устройств, являющихся основой систем безопасности, уделив внимание как теоретической подготовке, так и развитию практических навыков.

Существующие на сегодня системы изучения и отладки микроконтроллеров, доступные на белорусском рынке, являются узкоспециализированными, ориентированными на изучение одного типа микроконтроллеров без возможности в дальнейшем заменить его на более современный, что не отвечает требованиями времени. Кроме того, цена данных систем, по нашим оценкам, завышена как минимум в пять раз. Сказанное послужило причиной разработки нашей собственной системы.

Разработанная система построена по модульному принципу и включает в себя блок микропроцессора с программатором, блок управления и коммутации, блоки периферийных устройств (матричный сегментный светодиодный индикаторы, знакосинтезирующий и графический ЖК индикаторы, светодиоды, кнопки, матричную клавиатуру, считыватель iButton, часы реального времени PCF8583, приемник инфракрасного сигнала и ряд других), блок питания. В настоящее время в системе для изучения и отладки используются микроконтроллеры ATmega128A и PIC16F727, однако, при необходимости, тип микроконтроллера может быть легко изменен на любой другой. Электронный блок управления и коммутации позволяет с помощью меню выбирать набор периферийных устройств, подключенных в данный момент к микроконтроллеру; зарезервированные свободные порты блока коммутации позволяют легко изменять и дополнять этот набор. Отладка и программирование микроконтроллера осуществляются с персонального компьютера через интерфейс USB.

Считаем, что разработанная система найдет широкое применение не только при изучении систем безопасности, но и в других курсах, связанных с применением микроконтроллерных устройств.

## **ПРОБЛЕМНЫЕ ВОПРОСЫ, СВЯЗАННЫЕ С НАЗНАЧЕНИЕМ ВНЕШТАТНЫХ СПЕЦИАЛИСТОВ ПО ЗАЩИТЕ ИНФОРМАЦИИ**

Л.Л. УТИН, Р.А. ДИДКОВСКИЙ

В современных условиях защита информации стала сложной организационно-технической проблемой, решение которой возможно путем создания системы защиты информации. В Инструкции по обеспечению режима секретности в Республике Беларусь для организации обеспечения защиты информации могут создаваться подразделения технической защиты информации (далее — ТЗИ). Слово «могут создаваться» понимается как «могут создаваться, а могут не создаваться», и руководители организаций, что бы не