Имитационную модель получают один раз с помощью предварительных экспериментальных исследований обучающей выборки. Обучающая выборка – это некая выборка, случайным образом сформированная из более крупной выборки или партии ИЭТ, параметрической надежностью экземпляров которой интересуются специалисты. Экспериментальные исследования включают получение математических выражений (моделей), показывающих, как выбранный функциональный параметр ИЭТ рассматриваемого типа изменяется от уровня имитационного фактора и от значения наработки.

Индивидуальное прогнозирование выполняют применительно к той выборке или партии ИЭТ, из которой была взята обучающая выборка. Причем прогноз получают для тех экземпляров, которые не принимали участия в обучающем эксперименте.

Рассмотренный метод имитационных воздействий был положен в основу разработки методики индивидуального прогнозирования параметрической надежности биполярных транзисторов. В качестве имитационного фактора рассматривалось напряжение, прикладываемое к *p*-*n*-переходу транзисторов. С методикой можно ознакомиться на кафедре ПИКС БГУИР (обращаться в ауд. 37 1-го учебного корпуса университета).

Список литературы

1. Боровиков С.М. Статистическое прогнозирование для отбраковки потенциально ненадежных изделий электронной техники. М.: Новое знание, 2013. 343 с.

ДИФФЕРЕНЦИАЛЬНЫЙ МЕТОД АНАЛИЗА АНАЛОГОВОЙ СХЕМОТЕХНИКИ

И.А. Богод

В работе исследованы свойства дифференциального метода анализа аналоговой схемотехники. Данный метод отличается от классического тем, что с его помощью за счет использования дифференциальных параметров можно добиться гораздо меньшей погрешности по сравнению с результатами расчетов классическим методом. В работе исследованы несколько относительно простых схем, и в результате сравнения их расчетных погрешностей было установлено, что дифференциальный метод обладает наибольшей точностью в схемах с цепями отрицательной обратной связи. Данный метод позволяет получить более точные результаты и может оказать положительное влияние на способности и возможности нынешних и будущих специалистов в области криптографии и защиты информации.

Список литературы

1. Свирид В.Л. Аналоговая микросхемотехника. В 3 ч. Ч. 1: Интегральные микросхемы. Системотехническое проектирование радиоэлектронной аппаратуры. Минск: БГУИР, 2003. 232 с.

2. Свирид В. Л. Дифференциальный метод анализа аналоговой схемотехники // Доклады БГУИР. 2016. № 8 (102). С. 39–45.

АВТОМАТИЗАЦИЯ ПРОЦЕДУРЫ ИНДИВИДУАЛЬНОГО ПРОГНОЗИРОВАНИЯ НАДЕЖНОСТИ ПОЛУПРОВОДНИКОВЫХ ПРИБОРОВ

С.М. Боровиков, А.В. Будник, В.О. Казючиц

Для аппаратных частей технических систем, в том числе систем обеспечения информационной безопасности, во многих случаях предъявляются повышенные требования к надежности. Для обеспечения требуемого уровня надежности необходимо при изготовлении аппаратных частей использовать комплектующие элементы повышенного уровня качества. Полупроводниковые приборы (ППП) составляют заметную часть в составе устройств, используемых в электронных системах безопасности. Совершенствование технологии изготовления ППП привело к снижению доли внезапных отказов. Постепенные отказы, отражающие внутренне присущие материалам ППП свойства, в частности старение, в принципе исключить невозможно. Примерно в 80 % случаев отказы ППП проявляются в виде

постепенных (деградационных) отказов. Этим вызван растущий интерес к постепенным отказам ППП. В работе [1] приведена методика индивидуального прогнозирования надежности ППП по постепенным отказам, позволяющая из партий однотипных приборов отобрать экземпляры, отвечающие требованию по надежности. Для повышения эффективности процедуры индивидуального прогнозирования актуальна ее автоматизация. При участии авторов разработано программное средство, включенное в систему автоматизированного расчета надежности электронных устройств АРИОН-плюс [2]. С программным средством автоматизации индивидуального прогнозирования надежности ППП по постепенным отказам и системой АРИОН-плюс можно ознакомиться на кафедре ПИКС БГУИР, обращаться по e-mail: bsm@bsuir.by или в ауд. 37 1-го учебного корпуса университета.

Список литературы

1. Боровиков С.М. Статистическое прогнозирование для отбраковки потенциально ненадежных изделий электронной техники. М. : Новое знание, 2013. 343 с.

2. Разработка программного комплекса автоматизированной оценки надежности электронных устройств и систем: отчет о НИР (заключительный). Рук. С.М. Боровиков. Минск, 2016. 46 с. № госрегистрации 20121425.

ОБ ИЗУЧЕНИИ ВИДОВ И ОСОБЕННОСТЕЙ УГРОЗ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРИ ПОДГОТОВКЕ ВОЕННЫХ СПЕЦИАЛИСТОВ

Е.В. Валаханович, Л.В. Михайловская

В настоящее время военному специалисту необходимо соответствовать современным профессиональным требованиям в области защиты информации. Вследствие этого на кафедре высшей математики учреждения образования «Военная академия Республики Беларусь» разработаны и внедрены факультативный курс «Защита информации» и дисциплина «Прикладная математика». Одной из начальных тем вышеназванных курсов является тема «Классификация угроз информационной безопасности».

Авторы считают необходимым уточнение разработанной ранее, например, в [1], классификации угроз. Угрозы информационной безопасности в зависимости от характера ущерба, который они могут нанести, целесообразно систематизировать исходя из двух основополагающих критериев: происхождения и категорий безопасности. Предлагается угрозы по происхождению подразделить на два направления: стихийные (природного характера) и созданные людьми. Источники угроз информационной безопасности, созданные людьми, можно разделить на три типа: преднамеренные, техногенные и случайные. Угрозы по категориям безопасности соответственно делятся на три направления: угрозы нарушения целостности, конфиденциальности и доступности.

Так как средства и методы обработки, передачи и защиты информации постоянно совершенствуются, то перечень и классификация угроз информационной безопасности могут изменяться и приводить к появлению принципиально новых видов угроз и способов преодоления систем безопасности.

Таким образом, непрерывная и надежная работа по защите информации в сфере военной деятельности обусловлена разработкой классификации угроз информационной безопасности, как первого шага в алгоритме работы по их предотвращению и предупреждению.

Список литературы

1. Mehrhoff M. IT-Grundschutzhandbuch. Standard – Sicherheitsmapnahmen. Bundesamt fur Sicherheit in der Informationstechnik. DBUS-Jahrestagung, 2004.