

Надежность любой системы криптографической защиты информации (СКЗИ) в значительной степени определяется качеством используемых генераторов случайных и псевдослучайных последовательностей. Генератор, используемый в СКЗИ, должен порождать выходную последовательность, неотличимую от равномерно распределенной случайной последовательности (РРСП) [1]. Для обнаружения отклонения от модели РРСП используются статистические тесты. Статистические свойства последовательностей определяются числовыми характеристиками. На основе оценочных критериев делаются заключения о степени близости свойств анализируемой случайной последовательности и РРСП.

Для выявления зависимостей высокого порядка и выявления скрытых зависимостей требуются дополнительные исследования. Основными математическими моделями, используемыми в таких исследованиях, являются марковские модели. В НИИ ППМИ БГУ были разработаны методы и алгоритмы статистического тестирования выходных последовательностей, основанные на цепи Маркова порядка s с r частичными связями (ЦМ(s, r)) и цепи Маркова условного порядка (ЦМУП).

Данный доклад посвящен разработке программного комплекса, реализующий эффективные алгоритмы статистического анализа выходных последовательностей, основанные на оценивании таких марковских моделей, как однородная цепь Маркова, однородная цепь Маркова порядка s , скрытая марковская модель, двойная марковская модель.

Литература

1. Криптология / Ю.С Харин [и др.]. Минск: БГУ, 2013. 511 с.

СВЕТОДИОДНЫЕ СИСТЕМЫ ВЫСОКОЙ МОЩНОСТИ НА АЛЮМИНИЕВОЙ ПЛАТЕ С КОМБИНИРОВАННЫМ ДИЭЛЕКТРИКОМ

Т.Х. Динь, И.А. Врублевский, К.В. Чернякова, А.К. Тучковский

Обеспечение оптимальных температурных режимов работы активных радиоэлектронных элементов является одной из наиболее важных задач при разработке конструкций плат с высоким тепловыделением. Это особенно актуально для светодиодных модулей освещения высокой мощности. Теплота, выделяемая при $p-n$ переходе светодиода, проходит от корпуса элемента к теплоотводу, а затем рассеивается в окружающем пространстве. При перегреве светодиода значительно уменьшается эффективность его светоотдачи: падает световой поток, изменяется цветовая температура, и срок службы светодиода сокращается в несколько раз. Поэтому в случае плат с высоким тепловыделением очень важно обеспечить максимальное рассеивание выделяемой теплоты. Решение этой задачи зависит от характеристик печатной платы, которые определяются как конструктивными особенностями платы, так и материалом, из которого она изготовлена. Один из способов снижения уровня тепловой нагруженности плат и эффективного отвода тепла от электронных компонентов является использование печатных плат с алюминиевым основанием.

В данной работе в качестве диэлектрического покрытия плат с алюминиевым основанием использовался комбинированный диэлектрик, состоящий из слоя пористого анодного оксида алюминия и слоя препрега, стеклоткани, пропитанной эпоксидными смолами. С целью повышения теплопроводности в слой препрега вводился керамический наполнитель. Для этого были использованы различные керамические наполнители с высокой теплопроводностью – порошки оксида алюминия, нитрида бора, оксида магния, оксида цинка и оксида титана. Тепловые характеристики печатных плат на алюминиевом основании с диэлектрическим покрытием на основе комбинированного диэлектрика исследовались с помощью термограмм поверхности, получаемых с использованием тепловизионных измерений.

ПРЕДСКАЗАНИЕ ОЦЕНОК CVE УЯЗВИМОСТЕЙ НА ОСНОВЕ ИХ ТЕКСТОВОГО ОПИСАНИЯ

А.К. Доронин, В.А. Липницкий

В мире с каждым днем появляются все новые уязвимости компьютерных систем. Американская национальная база данных уязвимостей CVE содержит около 100000 записей