автоматизированных систем обработки информации» показывает, что изучаемые в рамках лекционных, семинарских и особенно практических занятий вопросы осваиваются с большим интересом. Это способствует подготовке курсантов к правильной организации мероприятий по обеспечению безопасности АСОИ и самостоятельной эксплуатации комплексных систем обеспечения безопасности АСОИ, выработке практических навыков работы с основными средствами защиты информации, формирования политики информационной безопасности.

Современный этап развития общества характеризуется возрастающей ролью информационной сферы. Информационная сфера активно влияет на состояние политической, экономической, оборонной и других составляющих национальной безопасности. Поэтому развитие и расширение дисциплины «Методы и средства обеспечения безопасности автоматизированных систем обработки информации» представляется весьма вероятной.

Литература

1. Концепция национальной безопасности Республики Беларусь. Утверждена Указом Президента РБ № 390 от 17.07.2001.

2. Жук А.П. Защита информации: учебное пособие. М., 2017. 359 с.

ПРОГРАММА СТАТИСТИЧЕСКОГО ТЕСТИРОВАНИЯ БИТОВЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ

И.В. Дайняк, Н.Г. Киевец, А.М. Ярук

Программа статистического тестирования битовых последовательностей предназначена для исследования сгенерированной каким-либо способом последовательности битов, в том числе полученной от физического генератора случайных чисел, на предмет пригодности к применению в криптографических системах. В основе программы лежат алгоритмы частотных тестов, тестов подпоследовательностей, тестов аппроксимированной энтропии и других тестов, основанных на статистических характеристиках.

Программа статистического тестирования реализована в виде Windows-приложения на языке Си в среде Bloodshed Dev-C++ версии 4.9.9.2. Основными требованиями при реализации программы были: 1) реализация каждого теста в виде отдельной функции с целью возможности его запуска в отдельности; 2) возможность запуска серии тестов с отслеживанием времени, затраченного на каждый тест и тестирование в целом; 3) получение отчета о тестировании, содержащего для каждого задействованного теста описание критерия прохождения и полученных при этом значений вероятности. В программе реализованы 14 основных тестов входной битовой последовательности и 7 двухуровневых тестов подпоследовательностей.

Интерфейс программы реализован на Windows API в виде простого окна с горизонтальным меню, так как на текущем этапе разработки и отладки повышенных требований к программе не предъявляется. Меню содержит набор стандартных операций по работе с файлами (загрузка битовой последовательности из файла и формирование файла отчета с результатами тестирования), группу основных тестов и группу двухуровневых тестов, обеспечивая тем самым двухуровневое тестирование битовой последовательности [1] с отображением результатов непосредственно в окне программы.

Литература

1. Киевец Н. Г. Статистическое тестирование генераторов случайных чисел электронных пластиковых карт // Математические методы в технике и технологиях : сб. тр. Междунар. науч. конф., Санкт-Петербург, Минск, Самара, окт.–нояб. 2017 г. Ч. 2. С. 19–22.

РАЗРАБОТКА ПРОГРАММНОГО КОМПЛЕКСА СТАТИСТИЧЕСКОГО ТЕСТИРОВАНИЯ КРИПТОГРАФИЧЕСКИХ ГЕНЕРАТОРОВ НА ОСНОВЕ МАРКОВСКИХ МОДЕЛЕЙ

М.Ю. Деркач, Ю.С. Харин

Проблема защиты информации затрагивает практически все сферы деятельности человека. Среди способов защиты информации важнейшим считается криптографический [1].

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 последовательностей 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