денные оценки показали, что погрешность измерений температуры не превышает 0,2 °С при времени измерения 1 с, при этом максимальная измеряемая температура составляет +400 °С для длины волоконно-оптического измерительного преобразователя в несколько километров при использовании многомодовых градиентных волоконных световодов с металлическим покрытием.

1. Бурже Ж., Сурио П., Комбарну М. Термические методы повышения нефтеотдачи пластов М.: Недра. – 1989. – 422 с.
2. Bolognini Gabriele et. al. Analysis of distributed temperature sensing based on Raman scattering using OTDR coding and discrete Raman amplification // Meas. Sci. Technol. – 2007. – Vol. 18. – № 10. – P.3211-3218.
3. Kwang Suh, Chung Lee Auto-correction method for differential attenuation in a fiber-optic distributed-temperature sensor // O ptics Letters. – 2008. – Vol. 33. – №16. – P. 1845-1847.
4. Culshaw Brian Fiber-Optic Sensors: Applications and Advances // Optics and Photonics News. – 2005. – Vol. 16. – № 11. – P. 24-29.
5. Zou L., Bao X., Afshar S., and Chen L. Dependence of the Brillouin frequency shift on strain and temperature in a photonic crystal fiber // Optics Letters. – 2004. – Vol. 29. – № 13. – P. 1485-1487.
6. Aldo Minardo, Romeo Bernini, Luigi Zeni Stimulated Brillouin scattering modeling for high-resolution, time-domain distributed sensing // Optics Express.– 2007.– Vol. 15, № 16. – P. 10397-10407.
7. Jihong Geng, Sean Staines, Mike Blake, Shibin Jiang Distributed fiber temperature and strain sensor using coherent radio-frequency detection of spontaneous Brillouin scattering // Applied Optics.– 2007.–Vol. 46. – № 23.– P. 5928-5932.
8. Feng Wang, Xiaoyi Bao, Liang Chen, Yun Li, Jeffrey Snoddy, and Xuping Zhang Using pulse with a dark base to achieve high spatial and frequency resolution for the distributed Brillouin sensor // Opt. Lett. – 2008. – Vol.33. – № 22. – P. 2707-2709.

УДК 681

АППАРАТНО-ПРОГРАММНЫЙ КОМПЛЕКС ПОДГОТОВКИ СПЕЦИАЛИСТОВ В ОБЛАСТИ КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ

Кучинский П.В., Ращеня Н.А., Труханович А.Л., Циолта О.Н.
Институт прикладных физических проблем им. А.Н.Севченко» БГУ
Минск, Республика Беларусь

Для подготовки специалистов в области информационной безопасности разработан и изготовлен аппаратно-программный комплекс, позволяющий организовать эффективный процесс изучения основных принципов создания аппаратно-программных устройств защиты информации, способов генерации ключевой информации, изучения алгоритмов криптографического преобразования данных.

Защита информации в современных информационно-коммуникационных системах обеспечивается комплексом организационно-технических мероприятий, включающих разработку, изготовление и применение сложных технических средств и систем защиты от несанкционированного доступа (НСД), в том числе криптографическими методами. Для корректной реализации на практике криптографических методов защиты информации требуются специалисты, владеющие знаниями о существующих криптографических алгоритмах и протоколах, об основных принципах построения надежных систем и комплексов криптографической защиты информации, имеющие практические навыки работы с ними, способные самостоятельно разрабатывать и внедрять современные эффективные программные и аппа-ратно-программные решения защиты от НСД.

Для подготовки грамотных и квалифицированных специалистов в области защиты информации криптографическими методами разработан и создан аппаратно-программный комплекс (АПК) «Крипто-Лаб».

АПК «Крипто-Лаб» выполнен на базе ПЭВМ и включает аппаратно-программное устройство и программное обеспечение.

Аппаратно-программное устройство (АПУ) АПК «Крипто-Лаб» выполнено в виде платы, устанавливаемой в ПЭВМ, и обеспечивает следующие основные технические характеристики и функциональные возможности:

– *PCI*-интерфейс для питания и взаимодействия с ПЭВМ;

– цифровой процессор, память программ и энергонезависимое ОЗУ для обеспечения решения задач пользователя;

– модуль генерации случайной числовой последовательности (СЧП) на физическом источнике шума (полупроводниковый диод).

Программное обеспечение обеспечивает следующие основные функциональные возможности:

– реализацию криптографических преобразований данных по ГОСТ 28147-89, СТБ 34.101.31-2011, СТБ 1176.1-99, СТБ 1176.2-99 в АПУ и ПЭВМ;

– функционирование АПУ под управлением операционной системы *Windows XP/7*;

– выполнение в ПЭВМ криптографических функций, реализованных в АПУ;

– выгрузку СЧП из АПУ;

– генерацию СЧП на системном (состояние, процессы и события операционной системы ПЭВМ) источнике шума;

– генерацию псевдослучайных числовых последовательностей;

– статистическую обработку числовых последовательностей с визуализацией результатов;

– пошаговое выполнение в ПЭВМ криптографических преобразований данных по ГОСТ 28147-89, СТБ 34.101.31-2011, СТБ 1176.1-99, СТБ 1176.2-99 позволяющее анализировать ошибки в реализации преобразований;

– интерфейс пользователя для работы с АПК «Крипто-Лаб» и визуализации результатов статистической обработки числовых последовательностей и пошагового выполнения криптографических преобразований.

АПК «Крипто-Лаб» позволяет выполнять следующие практические лабораторные работы:

1. Изучение основных принципов создания аппаратно-программных устройств криптографической защиты информации.

Цель работы – изучить основные функциональные и конструктивные особенности построения аппаратно-программных устройств криптографической защиты информации на примере АПК «Крипто-Лаб», включая выделение приоритетных частей функционирования устройства, способы выделения и разделения памяти для использования программного кода, вспомогательной и ключевой информации, способы построения регистров для устройства и способы управления устройством через доступные программные регистры.

2. Изучение способов и анализа качества случайных числовых последовательностей.

Цель работы – изучить физические основы генерации СЧП, основные методы получения и проверки качества случайных последовательностей, получить практические навыки самостоятельной работы по статистической обработке данных для оценки качества СЧП. В комплексе предусмот-рено формирование последовательности при помощи алгоритмов (псевдослучайная последователь-ность), с использованием шумовых диодов и на основе внутреннего ресурса ПЭВМ. Так же реализованы и описаны основные тесты качества СЧП.

3. Изучение способов управления ключевой информацией.

Цель работы – изучить способы генерации ключевой информации, виды ключей, методы установки и расположения ключей в комплексе защиты информации, способы защиты ключей от НСД. Рассматриваются способы контроля целостности ключевой информации посредством получения имитовставки, введением контрольной суммы. Анализируются варианты хранения ключевой информации, пути исследования надежности хранения ключей в разных областях памяти устройства, и предоставляется возможность сделать выводы, где наиболее эффективно хранить ключ. Рассмотрены варианты установки и способы контроля ключевой информации. Также приведены способы уничтожения критической информации при НСД.

4. Изучение алгоритма криптографического преобразования данных ГОСТ28147-89.

Цель работы – изучить способы реализации алгоритма криптографического преобразования по ГОСТ 28147-89, наиболее распространенного и сертифицированного в Республике Беларусь. Комплекс позволяет детально изучить алгоритм в разных режимах работы (режим простой замены, режим гаммирования, режим гаммирования с обратной связью, режим выработки имитовставки), получить визуальное отображение всех шагов ре-ализации алгоритма, понять смысл преобразования. Комплекс предоставляет возможность непосредствен-ного использования алгоритма как в аппаратной, так и в программной реализации.

5. Изучение алгоритма криптографи-ческого преобразования данных СТБ 34.101.31-2011.

Цель работы – изучить способы реализации алгоритма криптографического преобразования по СТБ 34.101.31-2011, режимы работы алгоритма: режим простой замены, режим сцепления блоков, режим гаммирования с обратной связью, режим счетчика, выработка имито-вставки, режим хеширования.

6. Изучение алгоритма криптографи-ческого преобразования данных СТБ 1176.1-99 (функция хеширования).

Цель работы – изучить способы реализации алгоритма криптографического преобразования по СТБ 1176.1-99.

7. Изучение алгоритма криптографического преобразования данных СТБ 1176.2-99 (электронная цифровая подпись).

Цель работы – изучить способы реализации алгоритма криптографического преобразования по СТБ 1176.2-99.

Разработанный аппаратно-программный комплекс АПК «Крипто-Лаб» позволяет при его использовании в учебном процессе получить базовые знания и навыки, необходимые для разра-

ботки и создания программно-аппаратных комплексов защиты от НСД криптографическими методами. В процессе выполнения лабораторных работ обучающийся на практике изучит и освоит основные принципы работы криптографических алгоритмов в различных режимах их использования. Эти навыки позволят в дальнейшем более качественно и эффективно использовать отечественные алгоритмы при создании высоконадежных систем защиты информации.

УДК 621.317.799:621.382

МЕТОДИКА ОПРЕДЕЛЕНИЯ ВАХ ОБЪЕКТА ТЕСТИРОВАНИЯ ЭЛЕКТРИЧЕСКИ СВЯЗАННОГО С ДОПОЛНИТЕЛЬНЫМ ЭЛЕМЕНТОМ

Лисенков Б.Н., Грицев Н.В, Бруек А.А.
ОАО «МНИПИ»
Минск, Республика Беларусь

Разработана методика определения вольтамперной характеристики (ВАХ) объекта тестирования (ОТ) при наличии электрически связанного с ним (последовательно или параллельно) дополнительного элемента (вспомогательного или паразитного).

Методика основана на том, что при последовательном включении через ОТ и дополнительный элемент течет общий ток *I*, а при параллельном – к ним приложено общее напряжение *U*. Согласно методике, вначале измеряют, визуально оценивают и запоминают по команде оператора ВАХ дополнительного элемента. Для этого, при последовательном включении дополнительного элемента и ОТ, объект тестирования закорачивают, а при параллельном – исключают.

Затем приступают к определению, путем несложных расчетов, искомой ВАХ ОТ, для чего измеряют суммарную ВАХ, отражающую свойства электрически связанных ОТ и дополнительного элемента.

Рисунки 1 и 2 иллюстрируют предлагаемую методику определения ВАХ ОТ электрически связанного с дополнительным элементом, при по-следовательном и при параллельном включении дополнительного элемента, соответственно.

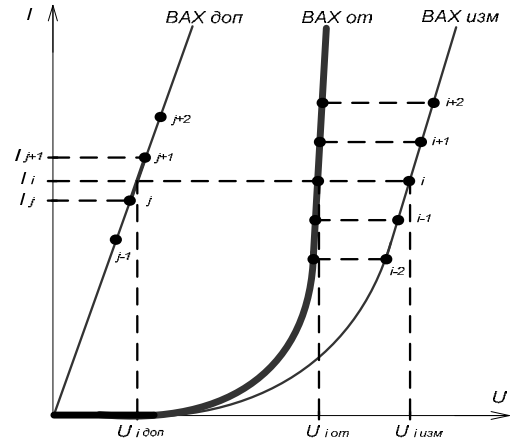

Рисунок 1 – определение ВАХ ОТ при последовательном включении

Значения общего параметра (*I* или *U*, в зависимости от схемы включения) в измеренных точках суммарной вольтамперной характеристики используют как реперные (опорные). Каждому реперному значению общего параметра ставят в со-ответствие две соседние точки запомненной ранее ВАХ дополнительного элемента, в одной из которых значение общего параметра меньше, а в другой – больше рассматриваемого реперного значе-ния. В качестве общего параметра каждой из точек искомой ВАХ ОТ используют его значения, выбранные в качестве реперных, при этом, противоположный параметр каждой из точек искомой ВАХ находят на пересечении прямой, соединяющей две упомянутые соседние точки на ВАХ дополнительного элемента соответствующие данному реперному значению, с линией, соответствующей этому значению.

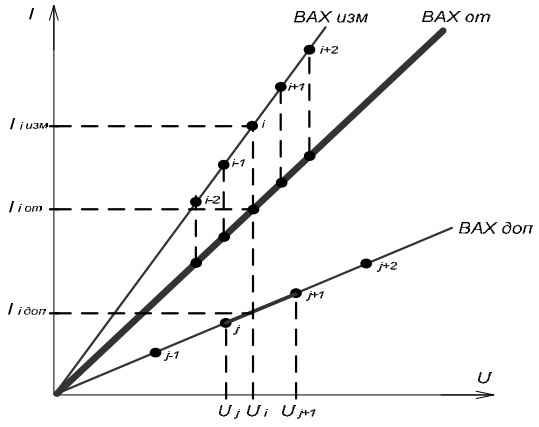

Рисунок 2 – определение ВАХ ОТ при параллельном включении

Таким образом, при использовании в измерительной схеме одного и того же дополнительного элемента, достаточно однократного измерения его ВАХ, чтобы затем определить ВАХ множества ОТ поочередно подключаемых к данной схеме.

ВАХдоп, ВАХот и ВАХизм – характеристики дополнительного элемента, объекта тестирова-