химическим травлением в растворе CrO_3:H_3PO_4:H_2O при температуре 85 °С удаляли выращенный Al_2O_3 с образованием микрорельефа. Затем осуществляли вторую стадию анодирования в том же электролите, снимали слабозадубленные фоторезистивные маски с мест формируемых встроенных проводников и проводили двухстороннее сквозное анодирование уже всей открытой поверхности оснований. Так как толщина Al в местах, соответствующих будущим зонам межэлементного разделения меньше, то они анодировались полностью до смыкания встречнорастущих Al_2O_3-слоев, а на других участках анодирование прекращалось с образованием встроенных внутри оксида проводников. Причем, какой величины был сделан уступ микрорельефа, такой же толщины формировались Al-проводники внутри Al_2O_3-пластин. Таким образом, получены встроеннные коммутационные элементы с толщиной Al от 5 до 100 мкм и различной глубиной их залегания в объеме Al_2O_3-пластин.

Список литературы

1. Сокол В.А., Шиманович Д.Л., Литвинович Г.В. Технологические приемы формирования Al–Al_2O_3 микроструктур для мощных электромеханических систем // Доклады БГУИР. 2012. № 8 (70). С. 44–49.

ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ ДЛЯ ПОСТРОЕНИЯ ЗАЩИЩЕННЫХ ВИРТУАЛЬНЫХ СРЕД

А.Н. Шляхтич, А.С. Шилов

На сегодняшний день виртуализация является одним из основных направлений развития информационных технологий. Это обусловлено тем, что путем применения указанной технологии можно значительно сократить затраты на создание информационных систем и сетей. Одной из основных задач, решаемых в ходе создания информационной системы или сети на основе технологии виртуализации (виртуальной среды) является разработка подходов по защите этих сред от угроз информационной безопасности. Один из таких подходов связан с выбором программного обеспечения для организации функционирования виртуальных сред.

Авторами проведен анализ уязвимостей программного обеспечения, используемого в настоящее время для организации функционирования виртуальных сред. На основе проведенного анализа определено, что наибольший уровень защищенности виртуальных сред может быть обеспечен в том случае, если для организации их функционирования применяется следующее программное обеспечение:

– платформа виртуализации VMware vSphere в составе гипервизора VMware ESXi и сервера управления VMware vCenter Server 5.1;

– платформа виртуализации и обеспечения безопасности сети VMware NSX версии 6.3;

– многофункциональное виртуальное устройство защиты информации FortiGate-VM под управлением программного обеспечения FortiOS v.5.6 для установки в среде виртуализации VMware.

Указанные программные продукты сертифицированы на территории Республики Беларусь.

РАСЧЕТ ЭКСПЛУАТАЦИОННОЙ ИНТЕНСИВНОСТИ ОТКАЗОВ ПЕЧАТНЫХ ПЛАТ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ

Н.С. Шматко

Надежность – одно из важнейших свойств изделий, в том числе электронных устройств, которое определяет их эксплуатационную пригодность. Особенно важно оценить эксплуатационную интенсивность отказов электронной аппаратуры в сфере защиты информации, так как преждевременный и незапланированный отказ средства защиты информации может привести к потере или утечке информации. Данные в компьютерных системах подвержены риску утраты из-за неисправности или уничтожения оборудования.

Для прогнозирования отказов аппаратуры защиты информации необходимо предварительно оценить ее надежность. Способы защиты информации включают использование аппаратных средств и устройств, а также внедрение специализированных технических средств, которые в большинстве случаев разработаны на основе печатных плат. В связи с этим необходимо определить методику для расчета надежности печатных плат обеспечивает получение более достоверных результатов. В работе рассмотрены подходы и методы определения эксплуатационной интенсивности отказов печатных плат, включенные в справочники или стандарты по расчету надежности электронного оборудования следующих стран: Россия, США, Франция. На основе анализа установлено, что в большей степени учет условий эксплуатации, конструкторско-технологических и других особенностей печатных плат обеспечивает модель расчета эксплуатационной надежности, включенная в справочник «RDF 2000 : Reliability Data Handbook. A universal model for reliability prediction of Electronics components, PCBs and equipment» [1]. Эта модель учитывает следующие важнейшие факторы: температуру окружающей среды, количество слоев печатной платы, количество отверстий для установки элементов, площадь печатной платы, количество токопроводящих дорожек, значение преобладающей ширины токопроводящих дорожек, возможные тепловые изменения при использовании печатной платы на объекте в составе аппаратуры.

Список литературы

1. A universal model for reliability prediction of Electronics components, PCBs and equipment. RDF 2000 : reliability data handbook. Paris : UTE C 80-810, 2000. 99 p.

ФИЛЬТРАЦИЯ HTTP-ТРАФИКА СИСТЕМ ВЕБ-АНАЛИТИКИ

Е.А. Юхо, Т.В. Борботько

Веб-аналитика (web-analytics) – система для измерения, сбора, анализа информации о посетителях веб-сайтов для улучшения и оптимизации работы ресурса. Главным назначением веб-аналитики является мониторинг посещений веб-страниц. На основе полученных данных изучается поведение пользователей сайта, принимаются решения о развитии и расширении возможностей ресурса.

Типовой алгоритм работы систем веб-аналитики:

– при загрузке страницы обрабатывается JS код;

– в браузер записываются, или считываются cookies;

– GIF хит отправляется на сервер системы веб-аналитики;

– данные обрабатываются на сервере и передаются в интерфейс системы в виде отчетов;

– доступ к полученным системой данным реализуется через API.

Чтобы изменить или скрыть данные от веб-аналитики, пользователю потребуется внести изменения в настройки своей операционной системы, браузера, или использовать средства фильтрации, такие как анонимайзер (веб-прокси) HideMe.nameVPN.

Для оценки эффективности известных способов защиты от сбора данных системами веб-аналитики проведен эксперимент, в ходе которого использовался тестовый стенд, выполненный на основе персонального компьютера с операционной системой Windows и браузером Firefox. В качестве средства оценки применяемых методов и средств защиты использовалась система веб-аналитики Яндекс Метрика. Показано, что достаточно использовать настройки указанного браузера для блокирования запросов Яндекс Метрики, дополнительных программных средств не требуется.