Список литературы

1. Aukeman, Mark. Cohort Analysis – understanding your customers / edwblog.com | EDW+ Delivering on the Big Data promise [Электронный ресурс]. URL: http://edwblog.com/adhoc/cohort-analysis-%E2%80%94-understanding-customer-behavior/32 (дата доступа: 09.05.2019).

БЕЗОПАСНОСТЬ СИСТЕМЫ И СИСТЕМА ОТКАЗОУСТОЙЧИВОСТИ

Камил Ихаб Абдулджаббар Камил, М.Б. Абросимов

Отказоустойчивость компьютерной системы – это способность системы продолжать сохранять свою работоспособность после отказа одного или нескольких составных компонентов. Начиная с середины 90-х годов быстрое развитие вычислительных программных приложений, работающих в режиме реального времени, особенно спроса на интеллектуальные устройства, встроенные в программное обеспечение, породило насущную проблему, связанную с отказоустойчивостью программного обеспечения. Неизбежность появления проблемы заключается в том, что синтез системы выполняется лицом, не являющимся специалистом этой системы. Большинство людей, регулярно пользующиеся компьютерами, сталкиваются с проблемой сбоя системы либо сбоев программного обеспечения, работы диска, потери питания, либо в результате ошибки шины. В некоторых случаях эти сбои не более чем мелкая неприятность; в других же случаях они приводят к значительным потерям. Второй вывод, вероятно, станет более распространенным, нежели предыдущий, поскольку зависимость общества от автоматизированных систем возрастает. Отказоустойчивая система должна быть в состоянии устранять неисправности отдельных аппаратных или программных компонентов, устранять сбои питания или другие виды неожиданных аварий и по-прежнему соответствовать своей спецификации. Отказоустойчивость необходима еще и потому, что без нее практически невозможно создать идеальную систему.Надежность системы – это вероятность того, что она будет оставаться работоспособной (потенциально, несмотря на сбои) в течение всего периода работы. Наличие у системы очень высокого уровня надежности наиболее значимо в критически важных приложениях, связанных с управлением космическими кораблями многоразового использования или промышленными объектами, в работе которых любой сбой может повлечь гибель людей [1]. Безопасность и надежность системы – это те вопросы, которые становятся все более важными в сегодняшнем развивающемся мире. Безопасность, гарантирующая выполнение системой требуемой работы, идет рука об руку с надежностью, гарантирующей правильность работы системы. Взаимодействие безопасности и надежности является краеугольным камнем бесперебойной работы функциональной системы на долгие годы. Безотказность работы системы является одним из аспектов ее надежности; однако она по своей природе более сложна, чем безопасность системы, поскольку она содержит атрибуты триады информационной безопасности (CIA) («конфиденциальность, целостность и доступность»). При этом к трем указанным атрибутам необходимо добавить три других: защищенность (безопасность), эксплуатационная технологичность и надежность. Защищенность (безопасность) системы характеризуется «отсутствием аварийных последствий для пользователей и окружающей среды». Эксплуатационная технологичность означает способность системы производить текущий ремонт, техническое обслуживание и вносить другие изменения, такие как исправления и обновления системы. Поскольку безопасность и надежность системы направлены на решение одной и той же цели, способствующей ее доступности, надежность системы тесно взаимосвязана с ее безопасностью. В большинстве случаев мы можем утверждать, что более надежная система должна быть безопасной. Меры безопасности применяются к системе с целью обеспечения ее надежности; но, если вследствие атаки будет нанесен ущерб безопасности системы, то тогда доступ к ней будет прекращен в тех случаях, когда надежность системы гарантирует ее доступность[2].

Список литературы

1. Basic Concepts and Taxonomy of Dependable Secure Computing / Avizienis Algirdas [et al.] // Process for developing common vocabulary in the information security area. 2007. № 1. P. 10–51.

2. Comparing reliability and security: Concepts, requirements, and techniques / R.S. Hanmer [et al.] // Bell Labs Technical Journal. 2007. № 3. P. 65–78.

ИСПОЛНИТЕЛЬНЫЕ МЕХАНИЗМЫ МЕХАТРОННЫХ СИСТЕМ НА МНОГОКООРДИНАТНОМ КОЛЬЦЕВОМ ПРИВОДЕ

С.Е. Карпович, Г.Й. Салманзадех, М.М. Форутан

На сегодняшний день весьма актуальной является задача построения и исследования исполнительных механизмов параллельной кинематики для мехатронных систем координатных перемещений широкого спектра применений, в том числе и в технических средствах защиты информации. Они должны обеспечивать возможность структурного реконфигурирования в зависимости от требуемой реализации пространственных перемещений системы, в которую встраивается эта мехатронная система. Среди кинематических характеристик, в первую очередь, необходимо учитывать способность реализации программируемых движений с заданным числом степеней свободы, поскольку влияние данного параметра на выбор структуры, конструкции и остальные характеристики является определяющим.

Решение этой задачи нами было выполнено на структурно-топологическом уровне [1, 2], что позволило разработать концепцию построения управляемого движения в трехмерном пространстве на базе композиционного использования многокоординатного привода прямого действия и реконфигурируемых механизмов параллельной кинематики. В соответствие с этой концепцией в настоящей работе исследованы две системы перемещений, полученные нами путем реконфигурирования механизма параллельной кинематики на гибридном кольцевом приводе прямого действия.

Список литературы

1. Системы многокоординатных перемещений и исполни-тельные механизмы для прецизионного технологического оборудования / В.В. Жарский [и др.]. Минск: Бестпринт, 2013. 208 с.

2. Литвинов Е.А., Жарский В.В., Ареби М.А. Построение многокоординатной системы перемещений на базе механизма параллельной кинематики // Доклады БГУИР. 2009. № 8 (46). С. 79–84.

ВЫСОКОПРОИЗВОДИТЕЛЬНАЯ РЕАЛИЗАЦИЯ АЛГОРИТМА DES НА БАЗЕ FPGA

М.В. Качинский, А.В. Станкевич, А.И. Шемаров

Быстрое развитие систем связи и расширение использования Интернета привели к возросшей потребности в эффективной безопасности и надежности передачи, обработки и хранения данных. Алгоритмы шифрования являются одним из механизмов обеспечения этой безопасности, при этом выполнение этих алгоритмов для шифрования данных должно осуществляться в режиме реального времени. Кроме того, защищенным системам связи часто требуется способность шифровать сообщения несколькими различными алгоритмами с возможностью регулярной смены ключей. В докладе рассматривается модифицированный подход к формированию раундовых ключей, который можно использовать в различных конвейерных алгоритмах шифрования с закрытым ключом [1]. Подход поддерживает использование различных ключей в каждом такте, что повышает общую безопасность, поскольку пользователи не ограничены использованием одного и того же ключа во время любого сеанса передачи данных. Для иллюстрации способа формирования раундовых ключей используется алгоритм шифрования данных стандарта DES, который хорошо пригоден для конвейерной обработки.

В отличии от традиционного способа реализации генератора ключей алгоритма DES, который использует операции логического циклического сдвига на каждой ступени 16-ступенчатого конвейера для формирования раундовых ключей, рассматриваемый в докладе метод использует заранее сформированные для каждого раунда алгоритма DES перестановки входного ключа. Однако в отличии от [1], в модифицированном способе для правильного