представителями ЕК, подтвердили возможность включения проекта в программу сотрудничества с ЕК в 2011 году.

Независимо от окончательного решения о включении проекта в программу сотрудничества, автор намерен продолжать работу в области совершенствования аварийной готовности и радиационной защиты АЭС, о результатах которой можно будет узнать на страницах данного и иных периодических специализированных изданий.

9. НП 306.2.141-2008. Общие положения безопасности атомных станций – ГКЯРУ. 2008. – 36 с.
10. ГСТУ 95.1.01.03.024-97. Автоматизированные системы контроля радиационной обстановки для атомных станций. Основные положения. – ГНИЦСКАР. 1997. – 21 с.
11. GS-R-2. Готовность и реагирование в случае ядерной и радиационной аварийной ситуации – МАГАТЭ. 2004. – 104 с.
12. *J. Ehrhardt.* The RODOS system: decision support for off-site emergency management in Europe / Nuclear Technology Publishing – 1997. - №1-4. P. 35-40.
13. 00.РБ.XQ.Pr.01.A. Регламент радиационного контроля при эксплуатации объектов ОП ЗАЭС – ОП ЗАЭС. 2010. – 267 с.

Поступила 3.02.2011р.

УДК 004.274:004.056

С.Я. Гильгурт, к.т.н., ИПМЭ им. Г.Е. Пухова НАНУ, г. Киев
Б.В.Дурняк, д.т.н., УАД, г. Львов
Ю.М. Коростиль, д.т.н., ИПМЭ им. Г.Е. Пухова НАНУ, г. Киев

ПРИМЕНЕНИЕ РЕКОНФИГУРИРУЕМЫХ УСТРОЙСТВ ДЛЯ КОНТРОЛЯ ЦЕЛОСТНОСТИ ДАННЫХ В РАСПРЕДЕЛЕННЫХ ИНФОРМАЦИОННЫХ СИСТЕМАХ

Аннотация. В статье исследованы возможности применения реконфигурируемых устройств на базе ПЛИС для решения задач контроля целостности файлов данных и программ пользователей в распределенных компьютерных сетях.

Библиогр.: 12 наим.

Ключевые слова: реконфигурируемый вычислитель, распределенные вычисления, грид, контроль целостности информации.

Необходимость дополнительной защиты собственных данных и программ пользователей в распределенных компьютерных сетях является известной проблемой [1]. Актуальными являются также некоторые смежные вопросы защиты информации, возникающие при запуске заданий на удаленных вычислительных ресурсах. Одним из них является контроль

целостности файлов пользователей.

С другой стороны, часто оказывается, что задача, решаемая в распределенной среде, помимо повышенной ресурсоемкости оперирует с большими объемами данных, которые необходимо удаленно хранить и обрабатывать, что затрудняет контроль целостности известными средствами.

В этой связи представляют интерес реконфигурируемые устройства на базе программируемых логических интегральных схем (ПЛИС). В ряде исследований, проводимых в настоящее время, рассматривается возможность применения таких устройств в целях компьютерной безопасности [2], в частности, для закрытия информации пользователей грид-среды [3].

В настоящей работе исследуются вопросы применения программируемой логики для решения задач контроля целостности данных пользователей в распределенных вычислительных сетях.

Анализ последних достижений и публикаций свидетельствует о наличии большого количества информации по смежной тематике, в частности, по методам и средствам контроля целостности, по реализации на ПЛИС различных криптографических процедур, включая вычисление хэш-функций, симметричное и асимметричное шифрование, а также по штатным средствам обеспечения безопасности информации в грид-сетях.

В то же время, информация по вопросам, являющимся предметом настоящего исследования, фактически, отсутствуют.

Целью настоящей работы является исследование возможностей применения реконфигурируемых устройств для решения задач контроля целостности файлов данных и программ пользователей в сложных, в том числе распределенных компьютерных системах.

Рассмотрим сначала, как решаются задачи, близкие по характеру к поставленной в настоящей работе проблеме, и в чем заключается ее специфика, затрудняющая применение известных решений.

Существующие системы контроля целостности (СКЦ) используют пассивные методы проверки таких объектов, как исполняемые программные модули, динамические библиотеки, драйверы, конфигурационные файлы, базы данных, записи системного реестра, а также их атрибутов, например, время последней модификации. Для каждого контролируемого объекта СКЦ периодически, либо по запросу, вычисляют по определенному алгоритму некоторый аутентификатор, который затем сравнивается с эталонным значением, найденным заранее, что позволяет выявлять изменения.

На сегодняшний день разработано большое число систем контроля целостности, как коммерческих, так и свободно распространяемых, различающихся операционными средами, архитектурой и функциональными возможностями. В качестве аутентификатора в них чаще всего используются криптографически стойкие беспарольные хэш-функции. Такие алгоритмы, как функция электронной цифровой подписи, либо блочные симметричные шифры (БСШ) в режиме генерации имитовставки, в современных СКЦ используются реже, поскольку для их выполнения требуется ключевая

информация [4]. Если же функция контроля целостности является составной частью системы дополнительной защиты данных [1], в которой задействуются секретные ключи, вводимые пользователями, то применение хэш-функций с ключами либо имитовставок становится целесообразным.

Следует отметить, что процедуры нахождения как хэш-функций, так и имитовставок в вычислительном плане являются более тесносвязанными операциями по сравнению, например, с БСШ. Так, если симметричный алгоритм шифрования, например, ГОСТ 28147-89 в режиме простой замены, при котором блоки информации обрабатываются полностью независимо, позволяет распараллелить его для выполнения на кластере, то в случае применения того же алгоритма для контроля целостности в режиме вычисления имитовставки требуется строго последовательная обработка всех блоков информации [5]. И тогда становится существенным преимущество реконфигурируемых устройств, в которых можно синтезировать произвольные вычислительные структуры, в том числе конвейерные, эффективные для реализации тесносвязанных алгоритмов.

Цифровые реконфигурируемые устройства, создаваемые чаще всего на базе микросхем программируемой логики типа FPGA, в настоящее время находят все более широкое применение в различных областях, в том числе и для решения задач информационной безопасности, [6].

В публикации [7] проведен подробный сравнительный анализ реализации на ПЛИС типа FPGA различных криптографических задач. Результаты данного исследования часто цитируются в литературе по соответствующей тематике. В этой работе, в частности, говорится о том, что вычисление на ПЛИС беспарольных хэш-функций (например, по таким распространенным алгоритмам, как MD5 и SHA) самих по себе не дает существенного выигрыша в производительности по сравнению с программной реализацией. Более ощутимый эффект от применения программируемой логики достигается либо при их совместном использовании с другими ресурсоемкими криптографическими операциями, в которых задействована ключевая информация (например, как часть алгоритма генерации цифровой подписи), либо когда требуется находить значения хэш-функций от больших массивов данных [8].

Другими словами, эффект от использования ПЛИС тем выше, чем больше размеры файлов, подлежащих контролю целостности. Данный вывод также подтверждается публикацией [9], в которой предлагается структура для ускоренного вычисления хэш-функций по алгоритму MD5, позволяющая достичь производительности более 14 Гбит/сек. Но этот результат достигается лишь для сетевых приложений, то есть для обработки интенсивного потока пакетов относительно небольшого размера. В случае же контроля целостности данных грид-приложений, необходимо обрабатывать файлы, размер которых измеряется многими гигабайтами.

Однако, несмотря на несомненные преимущества реконфигурируемых устройств, при их практическом использовании возникают определенные

технические трудности. О проблемах, сдерживающих широкое распространение программируемой логики говорится, например, в работе [10]. Одна из главных проблем заключается в сложности разработки конфигураций (файлов, описывающих синтезированную вычислительную структуру), загружаемых в микросхемы ПЛИС.

Один из путей решения данной проблемы заключается в разработке методик синтеза, основанных на обобщенных структурах, позволяющих реализовать целый ряд приложений в некоторой предметной области. Такие методики дают возможность снизить требования к разработчику и сократить сроки выполнения проекта. Примером применения данной идеи для реализации широкого класса БСШ может служить работа [11].

Аналогичный подход, но для хэш-функций, описан в публикации [12]. Предложенная в ней универсальная структура позволяет с высокой производительностью вычислять хэш-функции по алгоритмам MD5, SHA-1 и SHA-2.

Выводы. Проведенный в настоящей работе предварительный анализ показал, что при решении задачи контроля целостности файлов данных больших размеров в распределенных вычислительных системах, преимущества реконфигурируемых устройств на базе ПЛИС делают целесообразным их применение.

1. *Давиденко А.Н., Гильгурт С.Я., Душеба В.В., Гиранова А.К.* Технические средства дополнительной защиты данных пользователей в распределенных информационных системах // III Міжнародна науково-технічна конференція «Комп'ютерні системи та мережні технології» / Тези доп., 15-17 червня 2010 р. – К.: Вид-во Нац.авіац.ун-ту «НАУ-друк», 2010. – С. 29.
2. *Гильгурт С.Я.* Обзор возможностей реконфигурируемых устройств для применения в компьютерной безопасности // Зб. наук. пр. ІПМЕ НАН України. – Київ, 2010. – Вип. 55. – С. 117-123.
3. *Гильгурт С.Я., Гиранова А.К.* О применении реконфигурируемых вычислителей для решения вопросов защиты информации, пересылаемой в грид-среде // Зб. наук. пр. ІПМЕ НАН України. – Київ, 2009. – Вип. 51. – С. 65-72.
4. *Казарин О.В.* Теория и практика защиты программ. – М.: МГУЛ, 2004. – 391 с.
5. *Гіранова А.К.* Деякі питання застосування кластерних обчислювальних систем для вирішення задач закриття інформації // Зб. наук. праць ІПМЕ НАН України «Моделювання та інформаційні технології». – Київ, 2010. – Вип. 56. – С.95-100.
6. *Коростиль Ю.М., Давиденко А.Н, Гильгурт С.Я., Панченко М.М.* Анализ внешних атак на локальную сеть и возможностей защиты реконфигурируемыми устройствами // Моделювання та інформаційні технології. Зб. наук. пр. ІПМЕ НАН України. – Київ, 2010. – Вип. 55. – С. 16-21.
7. *Jarvinen K., Tommiska M., Skytta J.* Comparative survey of high-performance cryptographic algorithm implementations on FPGAs // IEE Proc. Inf. Security, vol. 152, pp. 3-12, Oct. 2005.
8. *Jarvinen K., Tommiska M., Skytta J.* Hardware implementation analysis of the MD5 hash algorithm // Proceedings of the Proceedings of the 38th Annual Hawaii International Conference on System Sciences (HICSS'05) - Track 9, page 298.1, Washington, DC, USA, 2005.

9. *Sedov S* A Fast Parallel Architecture for Hash Codes Computation // PACT '09: Proceedings of the 2009 18th International Conference on Parallel Architectures and Compilation Techniques (September 2009), pp. 29-40.
10. *Гильгурт С.Я.* О применении реконфигурируемых унифицированных вычислителей для решения научно-технических задач / Параллельные вычислительные технологии (ПаВТ'2008) // Труды международной научной конференции (Санкт-Петербург, 28 января – 1 февраля 2008 г.). – Челябинск: Изд. ЮУрГУ, 2008. – С. 358-363.
11. *Гиранова А.К.* Обобщенная структура реконфигурируемого процессора, реализующего симметричные алгоритмы закрытия информации // Зб. наук. пр. ІПМЕ НАН України. – Київ, 2010. –Вип. 57.
12. *Ducloyer S., Vaslin R., Gogniat G., Wanderley E.* Hardware implementation of a multi-mode hash architecture for MD5, SHA-1 and SHA-2 // Proceedings on the Design and Architectures for Signal and Image Processing Workshop (DASIP '07), Grenoble, France, November 2007.

Поступила 21.02.2011р.

УДК 004.056.55:004.272.23:004.274:004.4

А.К. Гиранова, ИПМЭ им. Г.Е.Пухова НАНУ, г. Киев

РАЗРАБОТКА ПАКЕТА ПРОГРАММ ДЛЯ ПРОВЕДЕНИЯ ЭКСПЕРИМЕНТОВ С РЕКОНФИГУРИРУЕМЫМИ ВЫЧИСЛИТЕЛЯМИ

Аннотация. В статье выдвинуты требования и предложена структура пакета программ для проведения экспериментов с реконфигурируемыми вычислителями. Такой пакет программ реализован, применительно к области блочного симметричного шифрования.

Ключевые слова: экспериментальный пакет программ, реконфигурируемый вычислитель, закрытие информации.

В настоящее время для решения ресурсоемких задач все чаще применяются аппаратные ускорители, в том числе и реконфигурируемые унифицированные вычислители (РУВ).

В работах [1, 2] говорилось про сложности, с которыми приходится сталкиваться при использовании реконфигурируемых унифицированных вычислителей. Существует различное программное обеспечение (ПО) для РУВ [3], необходимое для их эффективного использования. Оно является разноплановым и требует от разработчиков решения вопросов системного программирования. Для более глубокого анализа существующего программного обеспечения для РУВ необходим экспериментальный пакет программ (ЭПП).

