

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. *Гильеурт 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).

Анализ последних достижений и публикаций показал, что, несмотря на обилие информации о существующем программном обеспечении для реконфигурируемых вычислителей, отсутствуют работы, в которых бы говорилось об анализе ПО с единых позиций, что облегчило бы проведение вычислений с применением РУВ.

Целью настоящей статьи является исследование и разработка принципов построения пакета программ, предназначенного для проведения экспериментов с реконфигурируемыми унифицированными вычислителями.

Все программное обеспечение, имеющее отношение к реконфигурируемым вычислителям, можно условно разделить на четыре группы (рис. 1):

- средства разработки вычислительных структур, загружаемых в ПЛИС;
- прикладное программное обеспечение, использующее вычислительные ресурсы реконфигурируемого вычислителя;
- интерфейс взаимодействия ПЭВМ и РУВ;
- тестирующее программное обеспечение.

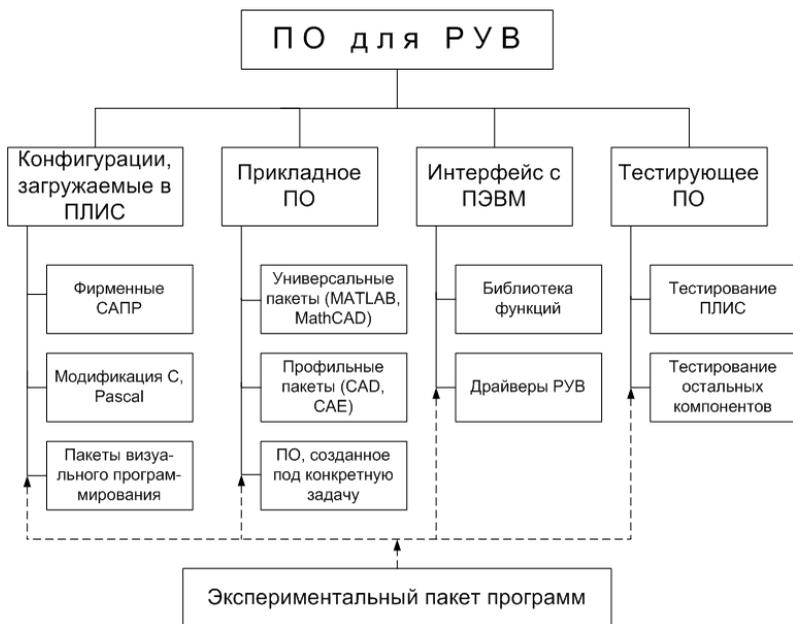


Рис. 1. Программное обеспечение для РУВ

Разнообразие программного обеспечения требует создание единого пакета программ для работы с реконфигурируемыми вычислителями. Такие пакеты должны давать возможность проводить эксперименты по использованию РУВ в различных предметных областях, проверять корректность аппаратной реализации задач на ПЛИС, иметь модульную структуру.

Из требований, сформулированных выше, следует набор функций, которые должен выполнять ЭПП. Поскольку пакет программ является экспериментальным, то в нем должны быть заложены следующие возможности:

- задания тестового набора данных;
- изменения набора данных с минимальными затратами;
- хранения и представления результатов в удобной для анализа форме.

Из специфики применения РУВ следует необходимость выполнения проверок:

- наличия, правильности установки и функционирования системного драйвера РУВ;
- работоспособности процедуры загрузки конфигурации в ПЛИС;
- корректности обмена данными между ПЭВМ и вычислителем.

Из требований, предъявляемых данному пакету программ, и набора функций вытекает структура экспериментального пакета. Он должен включать:

- сервис работ с профилем данных, который содержит информацию об эксперименте;
- поддержку программной проверки аппаратной реализации;
- поддержку вывода информации о реконфигурируемом вычислителе;
- интерфейс взаимодействия ПЭВМ и РУВ;
- поддержку загрузки конфигурации в ПЛИС, входящей в состав вычислителя.

Пакет программ, поддерживающий перечисленные выше функции и предназначенный для проведения экспериментов в области блочного симметричного шифрования, был разработан в Отделе теории моделирования ИПМЭ им. Г.Е.Пухова НАНУ. Данный пакет разработан для решения задач шифрования блочными алгоритмами (ГОСТ 28147, AES), в том числе с применением методов усиления [4]. ЭПП разработан в среде программирования Delphi 7. Конфигурации, необходимые для загрузки в ПЛИС, были созданы с использованием фирменного САПР ISE 10.1 фирмы Xilinx. Более подробно вопросы разработки вычислительных структур в области блочного симметричного шифрования рассмотрены в работе [5].

В пакете программ предусмотрено создание, редактирование и сохранение профиля шифрования (рис. 2), про который говорилось выше.

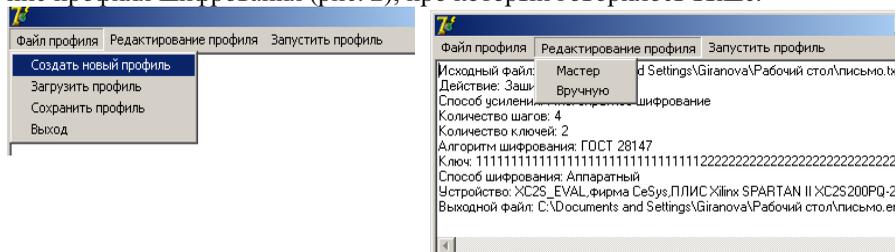


Рис. 2 Сервис работ с профилем шифрования.

1. Гильгурт С.Я. Обзор современных реконфигурируемых унифицированных вычислителей // Моделювання та інформаційні технології. Зб. наук. пр. ІПМЕ НАН України. – Вип. 49. – Київ: 2008. – С. 17-24.
2. Гильгурт С.Я., Гиранова А.К. Некоторые вопросы обмена данными между персональным компьютером и реконфигурируемым устройством // Моделювання та інформаційні технології. Зб. наук. пр. ІПМЕ НАН України. – Вип. 43. – Київ: 2007. – С. 86–94.
3. Гиранова А.К. Анализ программного обеспечения реконфигурируемых вычислителей // Моделювання та інформаційні технології. Зб. наук. пр. ІПМЕ НАН України. – Київ – 2007. Вип. 41. – С. 43–48.
4. Гиранова А.К. Анализ подходов к повышению эффективности закрытия информации и вопросы их реализации на унифицированных вычислителях // Зб. наук. праць ІПМЕ НАН України. – Київ, 2009. – Вип. 52. – С. 78-83.
5. Гиранова А.К. Обобщенная структура реконфигурируемого процессора, реализующего симметричные алгоритмы закрытия информации // Зб. наук. пр. ІПМЕ НАН України. – Київ, 2010. – Вип. 57.

Поступила 24.02.2011р.

УДК 519.6

Б.Б. Любінський¹, Р.А. Бунь^{1,2},

СПЕЦІАЛІЗОВАНЕ ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ ДЛЯ ГЕОГРАФІЧНОГО АНАЛІЗУ ТА ІНВЕНТАРИЗАЦІЇ ПАРНИКОВИХ ГАЗІВ

Summary. An approach to building specialized software for spatial inventory of greenhouse gases is presented. Architecture of software is carried out and the main requirements for this software are established. The specifics of used data formats are analyzed.

Keywords: software, architecture, geoinformation technology, greenhouse gas, inventory, spatial analysis.

Анотація. Представлено підхід до реалізації спеціалізованого програмного забезпечення для просторової інвентаризації парникових газів. Розроблено архітектуру та встановлено основні вимоги до програмного забезпечення, проаналізовано специфіку форматів використовуваних даних.

Ключові слова: програмне забезпечення, архітектура, геоінформаційна технологія, парниковий газ, інвентаризація, просторовий аналіз.

¹ Національний університет "Львівська політехніка"

² Академія бізнесу м.Домброва Гурніча Польща