

ПРИМЕНЕНИЕ СПЕЦИАЛИЗИРОВАННЫХ ВЫЧИСЛИТЕЛЕЙ НА ОСНОВЕ ПЛИС ДЛЯ РЕШЕНИЯ ЗАДАЧ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Лобов В.А.

Научный руководитель – асс. Заворотная М.Г.

Харьковский национальный университет радиоэлектроники, кафедра микропроцессорных технологий и систем, e-mail: viktor.lobov@nure.ua

Modern society can not be imagined in all spheres of human activity. Comprehensive implementation, on the one hand, noticeably helps in many work and everyday tasks. The introduction of new information technologies in the management and communications system is accompanied by the development and wide dissemination of new ways to ensure the security of information transmission and data protection. Formed two main areas in which in recent years, developing cryptographic tools to ensure secure transmission of information. The first is the improvement of traditional encryption systems. The second is the introduction of fundamentally new means of closing information.

В настоящее время существует несколько подходов к построению вычислителей для суперкомпьютеров: первый – традиционный, применяется при проектировании суперЭВМ; второй – для построения специализированных вычислителей на базе ПЛИС.

Современное общество невозможно представить без информационных технологий, они присутствуют во всех сферах человеческой деятельности. Повсеместное их внедрение, с одной стороны, заметно помогает в решении многих рабочих и повседневных задач, а с другой стороны – таит в себе множество угроз. Поэтому внедрение новых информационных технологий в системы управления и связи сопровождается разработкой и широким распространением новых способов обеспечения безопасности передачи информации и защиты данных.

Анализ развития средств защиты данных в информационных сетях показывает, что в настоящее время наблюдается тенденция к резкому расширению использования криптографических средств в информационных инфраструктурах многих государств. Сформировалось два основных направления, по которым в последние годы развиваются криптографические средства обеспечения безопасной передачи информации. Первое – совершенствование традиционных систем шифрования. Второй – внедрение принципиально новых средств закрытия информации.

Традиционно широкое применение ПЛИС нашли в системах цифровой обработки сигналов (ЦОС), что определяется большим удельным весом ресурсов, пригодных для ЦОС. При этом практически все производители ПЛИС сегодня располагают умножителями в виде

аппаратных модулей на кристалле (который полностью аналогичен умножителю в сигнальном процессоре или микроконтроллере). В то же время ПЛИС обладают не только максимальными абсолютными показателями производительности в задачах цифровой обработки, но и лучшим соотношением производительности и цены, чем современные сигнальные процессоры, выполненные по аналогичной ПЛИС и инструментальные средства разработки проектов на их основе, представляют собой надежную платформу для создания реконфигурируемых высокопроизводительных вычислительных систем. Расширение сферы ПЛИС определяется растущим спросом на устройства с быстрой перестройкой выполняемых функций, сокращением проектно-технологического цикла новых или модифицируемых изделий, востребованностью режимов изменения внутренней структуры в реальном масштабе времени, повышением быстродействия, снижения потребляемой мощности, а также снижением цен на эти устройства. Рассматривая опыт использования ПЛИС в вычислительных системах, в частности, в распределенных, многопроцессорных и других подобных системах, где ПЛИС нашли наиболее широкое применение, обратимся к использованию ПЛИС в суперкомпьютерах, в том числе для решения графовых задач. Как отмечается в работе, сегодня обработка графов является одним из быстро развивающихся направлений, что связано, в первую очередь, с необходимостью решения новых задач – анализа социальных сетей.

Область применения БВР (блок реконфигурированный) – это задача линейной алгебры, цифровой обработки сигналов, математической физики, символьной обработки. Вычислитель может быть использован во многих встраиваемых решениях. Главные его особенности - возможность конфигурирования собственной структуры и возможность объединения с другими аналогичными устройствами для создания кластерных структур с выполнением функции основного вычислительного элемента.

В настоящее время общество уязвимо перед угрозами, исходящих из этой сферы, более чем, когда либо, так же уязвимо от надлежащего функционирования информационных и коммуникативных технологий. Новые подходы и технологии в области защиты информации ныне настолько актуальны и востребованы, так-как они решают самую насущную задачу по реализации безопасного мира. Индустрия спецвычислителей адекватно и своевременно реагирует на запросы информационного общества и за последние годы прошла большой путь перед тем, как найти своё место в решении задач обеспечения информационной безопасности.

СПИСОК ИСТОЧНИКОВ: 1. КиберЛенинка [Электронный ресурс]. – Режим доступа: <https://cyberleninka.ru/article/n/primenenie-plis-dlya-posroeniya-vychislitelnyh-sistem-i-ih-komponentov>. 2. Применение специализированных вычислителей на основе ПЛИС для решения задач ИБ [Электронный ресурс]. – Режим доступа: <https://issuu.com/cta-mag/docs/20134076>