Слободин Руслан Сергеевич

аспирант

ФГБОУ ВО «Юго-Западный государственный университет»

г. Курск, Курская область

ФУНКЦИОНАЛЬНЫЕ ВОЗМОЖНОСТИ КОНТРОЛЛЕРА ЗАЩИТЫ ИНФОРМАЦИИ НА БАЗЕ ПРОГРАММИРУЕМЫХ ЛОГИЧЕСКИХ ИНТЕГРАЛЬНЫХ СХЕМ (ПЛИС)

Аннотация: *в статье описываются функциональные возможности контроллеров защиты информации на базе программируемых логических интегральных схем. Рассматривается проектирование вычислительных систем с использованием гибридных процессоров.*

Ключевые слова: *гибридные системы, программируемая интегральная схема, контроллер защиты информации, система на кристалле, прошивка, Intel, Altera.*

В современном мире информация становится одним из важнейших факторов жизни человечества. Информация приобрела свою стоимость. Обладание, какой-либо информацией, может быть очень полезно для человека, равно как и потеря времени при обработке какой-либо информации может нанести человеку непоправимый ущерб. Именно поэтому при разработке и проектировании информационных систем так важно уделить большое значение вопросам защиты данных обрабатываемых в данной системе. В тоже время не стоит забывать и о необходимости быстрой обработки информации. Никому не нужна хорошо защищенная информационная система, если скорость ее работы при этом ничтожно мала.

Выполнение функций защиты информации, таких как, криптографическое преобразование информации, фильтрация потоков данных, генерация псевдослучайных последовательностей, формирование и проверки электронной цифровой подписи, контроль целостности информации требуют больших вычислительных мощностей. В основном эти функции выполняются программными

средствами, а при таком подходе обработка выполнение функций защиты информации занимает значительную часть времени центрального процессора (CPU), не позволяя ему эффективно выполнять остальные задачи. Наиболее эффективным методом уменьшения временных задержек на обработку является обход ядра ОС и аппаратная обработка данных.

Таким образом, при проектировании защищенной информационной системы предлагается строить систему с использованием специализированных контроллеров защиты информации, основывающих свою работу на микросхемах перепрограммируемой логики.

Такие контроллеры можно разделить на два типа. Первый тип контроллеров представляет из себя плату с интерфейсом PCI Express. На борту таких устройств размещаются микросхемы ПЛИС, микросхемы оперативной памяти, микросхемы для генерации случайных последовательностей. В микросхеме ПЛИС будет развернута система на кристалле (СнК). Система представляет собой набор готовых и выполняющих конкретную функцию IP-ядер, таких как процессор, ядра шифрования, контроллеры для работы с жесткими дисками, ядра, реализующие обработку сетевого трафика, фильтрацию пакетов. Такая плата может работать как самостоятельно, то есть при подаче питания, загружается рабочая прошивка и плата начинает работать. Так же существует возможность загрузки готовых прошивок в плату с использованием приложения высокого уровня. К примеру, в микросхемах от компании Altera предусмотрена конфигурация микросхемы через протокол PCI Express (CvP – Configuration via Protocol). Это означает, что необходимая для выполнения конкретной задачи конфигурация будет загружена, в работающую плату, без выключения компьютера. Такая быстрая смена конфигурации контроллера защиты информации позволит быстро реагировать на вновь появляющиеся угрозы или на изменения в системе.

Второй тип контроллеров используется в системах с использованием центрального процессора на борту, которого располагается микросхема ПЛИС. О начале поставки двух чиповой платформы для разработки, состоящей из процессора Xeon E5–2600 v4 и FPGA Altera Arria 10 заявила корпорация Intel. Такие

процессоры будут иметь высокоскоростной интерфейс для взаимодействия с микросхемой ПЛИС. В этом случае контроллер защиты информации будет выглядеть как ускоритель для процессора. Внутри такого ускорителя будет находиться система на кристалле, внутри которой будут располагаться IP-ядра, способные осуществлять всевозможную предобработку информационных потоков, и выполняющие функции, связанные с защитой информации.

Создание защищенных информационных систем с использованием контроллеров защиты информации с реконфигурируемой логикой на базе ПЛИС позволяет выполнять задачи защиты информации без уменьшения временных задержек в центральном процессоре. Так же одним из достоинств такой системы – перестраиваемая архитектура позволяющая подстраивать контроллер защиты информации под конкретную задачу.

Список литературы

1. Симонов А.М. Гибридная архитектура параллельных вычислительных систем / А.М. Симонов, А.М. Кориков // Доклады ТУСУРа. – 2012. – №2 (26). – Ч. 1. – С. 178–183.

2. Архангельский А.В. Опыт аппаратной реализации функциональных модулей средств защиты информации на интегральных схемах программируемой логики // Программные продукты и системы. – 2013. – №2. – С. 108–113.