статичні характеристики розподілу параметрів оптичного волокна по довжині (показник заломлення), спектральні смуги напівпровідникового лазеру та характеристики засобів перехоплення мають флуктуації і призводить до того, що різниця між виведеними та введеними рівнями оптичного сигналу носить ймовірний характер.

Список літератури

1. *Каток В.Б.* Волоконно-оптичні системи зв'язку. – К. 1999. – 481с.
2. *Каток В.Б., Руденко И.Э., Тарасенко А.П.* Прокладка и монтаж оптических кабелей связи – К.: ИВЦ МС Украины, 1993. – 19с.
3. *Каток В.Б., Руденко І.Е.* Аналіз втрат що виникають в процесі монтажу оптичних кабелів зв'язку – Зв'язок 1996, № 2.

Надійшла 14. 03.2008р.

УДК.681.192:004.281

В.А.Хорошко, Е.О.Тискина

РОЛЬ ОРГАНИЗАЦИИ ПАМЯТИ В ПОВЫШЕНИИ ЭФФЕКТИВНОСТИ ВЫЧИСЛИТЕЛЬНЫХ ПРОЦЕССОВ В СИСТЕМАХ ЗАЩИТЫ ИНФОРМАЦИИ

Важнейшими обеспечивающими подсистемами, определяющими эффективность вычислительного процесса, являються подсистемы информационного и математического обеспечения систем защиты информации (СЗИ). На разных етапах развития средств вычислительной техники и СЗИ каждой из них отводилась своя роль. На ранней стадии, когда преобладали математические задачи с относительно небольшим обьемом информации, главная роль отводилась математическому обеспечению. Информационному же обеспечению доставалась пасивная роль получения, хранения информации. Такой поход обусловил типовую структуру вычислительного модуля, в котором центральное место занимает устройство управления с арифметико-логическими блоками, производящими активне преобразования над информацией хранящейся в памяти. Повышение производительности и надежности вычислительных систем (ВС) СЗИ идет по двум направлениям : первое — совершенствование аппаратного обеспечения, главным образом за счет повышения быстродействия и надежности элементной базы; второе — реализация новых архитектур и принципов организации вычислений.

Дальнейшие совершенствования элементной базы основывается на развитии полупроводниковой технологии, которая почти приблизилась к своим физическим возможностям.

Учитывая это, второе направление представляется перспективным и актуальным в деле повышения производительности и надежности ВС СЗИ.

Если вначале главной задачей этого направления была оптимизация организации только вычислительного процесса, то в настоящее время важнейшей проблемой является оптимизация структуры информационных ресурсов, оптимизация информационных потоков между элементами системы. Примером появления новых архитектурных решений и принципов организации вычислений являются многомашинная ВС (ММВС) и мультипроцессорная ВС (МПВС). В основу их построения заложены три принципа: параллельность выполнения операций, переменность структуры и конструктивная однородность. [1].

Создание МПВС связано с решением двух важнейших проблем: организация связей между функциональными блоками и организация вычислительного процесса в системе.

Различные пути решения этих проблем обусловили различные структуры построения МПВС и различные системы организации вычислительных процессов.

Организация вычислительного процесса в МПВС наиболее совершенны, если все ресурсы системы, и аппаратные, и программные, используются с наибольшей эффективностью, а производительность системы приближается к максимально возможной. Однако такая организация требует больших усилий для реализации, и с целью сокращения таких усилий нередко идут на некоторые упрощения.

Говоря о производительности МПВС и ее зависимости от количества процессов, входящих в состав системы, следует определить два режима работы. [1].

В первом случае МПВС решает большой поток небольших задач, и общая производительность МПВС близка к сумме производительностей процессоров, входящих в ее состав. В другом случае, который является наиболее важным с точки зрения эффективности МПВС, система решает одну большую задачу; при этом каждый из процессоров решает какую-то часть ее, и между ними происходят необходимые обмены информации с целью увязки всего процесса обработки. В этом случае появляются большие потери системы на работу операционной системы.

Создание МПВС — одно из важных и актуальных направлений повышения производительности вычислительных средств в системе контроля и защиты на новом уровне.

Реализация этого процесса требует решения ряда сложных проблем. Первое – это создание архитектурно-идеологической базы системы нового поколения. Здесь следует выделить два момента. Первый — разработка и решение проблемы искусственного интеллекта и связанных с ней вопросов создания качественно новых языков общения.

Второй важный момент—это намек новых архитектурных решений. Разработка новых структур на базе МПВС с появлением однокристальных микро ЭВМ (ОМ ЭВМ) и на базе ММВС позволяет создавать новые архитектурные построения систем и принципы организации вычислений в них. Разработанные архитектурные принципы синтеза МПВС позволяют добиваться существенных результатов в деле повышения производительности систем, обеспечивают простоту и эффективность их управления и функционирования. И все же архитектура многих систем обладает рядом недостатком, обусловленных снижением эффективности ее работы при изменении входных условий.

Для преодоления этих недостатков и трудностей разработана концепция МПВС с программируемой архитектурой, у которой программируются не только вычисления, проводимые в каждом процессоре (ОМ ЭВМ), но и пути передачи данных между ними. У систем с такими свойствами возможна эффективная адаптация под конкретную область применения. Развитием этого направления являются системы с перепрограммируемой структурой (СПС).

Программирование структуры системы должно обеспечивать неограниченное наращивание числа микропроцессоров и машин в ВС СЗИ и развитие их на самостоятельно функционирующие подсистемы с произвольным числом вычислений.

Важной проблемой при синтезе СПС является организация памяти. Так же как и МПВС, может быть организована сосредоточенная (СП), распределенная память (РП) или сосредоточенно-распределенная память. [1].

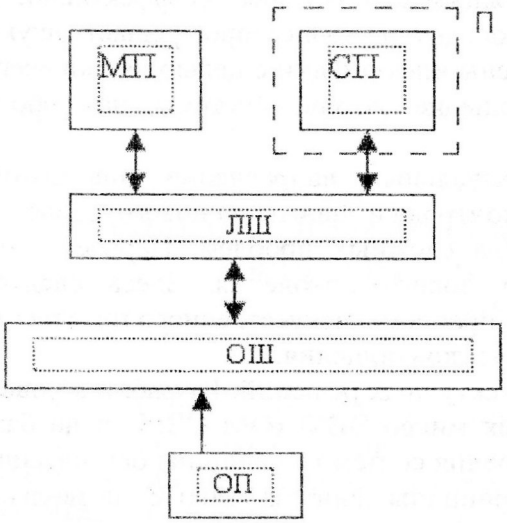
Мультипроцессорная система с программируемой коммутацией и СП отличается тем, что в ней с помощью коммутирующих структур (КС) могут быть запрограммированы любые прямые каналы связи между МП. Но применение СП приводит к тому, что в системе оказывается возможным обмен информацией между МП и памятью лишь на основе материального принципа.

Наиболее быстродействующими и гибкими, имеющими наибольшую перспективу являются многопроцессорные системы с РП и универсальной коммуникацией. В системах могут использоваться как линейные, так и пространственные структуры. [2].

В системах с программируемой коммутацией не обязательно предусматривать жесткие прямые каналы связей межу МП и элементами РП. Можно вместо этого подключить элементы РП и КС, и образовывать в последней по мере необходимости прямые каналы связи между МП и элементами РП программным путем. Это делает систему более гибкой. А массовая перестройка каналов связи качественно изменяет структуру СПС, позволяет осуществлять программированные структуры устройства и таким образом непосредственно оказывает существенное влияние не только на процесс и результаты обработки информации, но и на архитектуру системы.

Вычислительный модуль для СЗИ можно реализовать на большой интегральной схеме, причем в зависимости от задач, реализуемых модулем, его архитектура может изменяться.

Так как в модуль (М) входят несколько процессоров и различные виды памяти, то такой модуль можно оценивать как ВС коллективного пользования.



Рассмотрим два варианта архитектуры вычислительного модуля.

Особенностью архитектуры М1 (рис.1) является наличие сосредоточенной общей памяти (ОП) модуля и локальной памяти (ЛП) каждого МП. Доступ к ОП осуществляется через общую шину (ОШ), которая содержит порты связи. В каждый момент времени только один МП может произвести обращение к памяти. МП выполняет фрагменты программ до момента, когда необходимо обращаться к общей ОП. После выдачи запроса на ОШ может оказаться, что она занята, и тогда МП ожидает пока шина не станет доступной. Так как у нее принято симметричная модель, то обеспечивается (в среднем) баланс между сообщениями, принятыми процессором и выданными им. Активность МП можно записать как

$$Q=2\Psi_{МП}$$

Производительность анализируемой архитектуры может быть описана следующим выражением:

$$П=\frac{\sum_{a=0}^{N} q^a \frac{N!}{(N-a)!}-1}{q\sum_{a=0}^{N} q^a \frac{N!}{(N-a)!}}, \qquad (1)$$

Где N- количество процессов; $\Psi_{МП}$ - скорость генерации сообщений передаваемых между процессорами; q-рабочая перегрузка. Все основные параметры согласно[2].

Как нами ранее отличалось, ОП может быть разбита на маленькие модули для каждого МП (рис.2). Для архитектуры М2 предполагаем, что ЛП разбита на области собственной памяти МП и ОП. Причем каждый процессор соединен со своей собственной памятью локальной шиной (ЛШ). При обращении к ОП МП использует свою собственную ЛШ, ОШ, ЛШ, соединенную с соответствующим модулем ОП, где находится входной порог соответствующего МП.

В этой архитектуре необходим механизм арбитража, так как конфликты могут возникать при использовании каждой из шин, представленных в модуле [3].

Микропроцессор, обращавшийся к ОШ, получает приоритет в использовании любого ресурса и может прерывать обслуживание других МП. Если процессор находится в активном состоянии, то он блокируется, а если был в состоянии ожидания, то сохраняет свое состояние и освобождает свое ЛШ. Эта тактика позволяет устранять тупиковые ситуации и повысить эффективность вычислительного модуля.

Как уже отмечалось, в симметрической модели сохраняется баланс между поступившими и выданными сообщениями. Из этого следует, что средняя длина цикла МП может быть представлена как сумма среднего периода требуемого для формирования сообщения, средней длины периода передачи, требуемого для приема этого сообщения:

$$Q = \frac{y_{МП} t_{пер}}{y_{МП} + t_{пер}}.$$

Из-за блокирующего феномена, когда один МП обращается к ЛШ другого, архитектура М2 может быть промодулирована как простая система массового обслуживания (СМО). При этом модель Марковской цепи может быть сконструирована при условии, что отношение состояний системы - выбрано верно. Для архитектуры М2 состояние системы определяется множеством (S_0m_0; S_1m_1;… S_em_e:…). С учетом симметрии системы может быть использована теория кусочных марковсих цепей для уменьшения числа состояний цепи, так как агрегативные состояния требуют менее детального описания.

Важным свойством этой модели – то, что ее размер растет линейно только от количества МП в системе.

Равные вероятности состояний кусочных марковских цепей легко оцениваются путем решения системы линейных уравнений. Благодаря регулярности структуры цепи нетрудно задать программу, которой автоматически генерирует состояние цепи и оценивает равные вероятности для систем любого размера. Проблемы, связанные с объемом вычислений, возникают для больших систем (порядка сотни МП) при решении систем линейных уравнений. Так, S – множество состояний Марковской цепи, S_t – состояние в данный момент и π(S) – его уравновешенная вероятность, то производительность для архитектуры М2 будет:

$$X = (1 - q) \sum_{sOs_i} N_a(S) p(S) \qquad (2)$$

Фактор $(1 - q)$ введен для учета времени обмена информацией, включенного в цикл МП фактически используемого для формирования результата обработки, и при этом средняя длина цикла для архитектуры М2 будет:

$$Q = t_{пер} q .$$

Сравнивая архитектуры М1 и М2, видим, что М1 при малых нагрузках имеет большую производительность, чем архитектура М2. Это объясняется тем, что при малых нагрузках средняя задержка ожидания очень мала и не создает дополнительных конфликтов в архитектуре М1. В архитектуре М2 каждое обращение к области внешней ОП прерывает МП, вероятность активности которого с собственной ЛП очень велика при малых нагрузках. Точка разрыва между архитектурами М1 и М2 находится при нагрузке 50%. Для более высоких нагрузок архитектура М2 становится более эффективной.

Однако малые нагрузки в модулях могут рассматриваться, как самые значительные. Поэтому хорошо разработанная система должна работать в области защиты, если проблемная декомпозиция в задачах и распределение задач между процессорами имеет целью снизить затраты на связи.

Разнообразие архитектур не ограничивается рассмотренными вариантами. Их применение более эффективно в специальных ВС СЗИ, где требуется высокая производительность для получения информации в реальном масштабе времени. Это позволит СЗИ быстрее и четче реагировать на различные попытки несанкционированного получения информации.

Список литературы

1. Скорик В.Н., Степанов А.Е., Хорошко В.А. Мультимикропроцессорные системы. – К.: Техныка, 1989.-192с.

2. Егоров Ф.Н. Орленко В.С., Хорошко В.А. Вычислительные модули для системы защиты информации / Збірник наук. праць. Військового інституту КНУ ім. Т. Шевчена. 2008, Вып. №11. – с. 117-124.
3. Капустян М.В., Орленко Т.И., Хорошко В.А. Модели передачи информации с учетом обнаружения, недопущения с учетом обнаружения, недопущения и устранения тупиковых ситуаций / Вісник ДУІКТ, т. 4, №3, 2006. – с. 156-162.

Поступила 14.03.2008г.

УДК 621.3

О.В.Рыбальский

МЕТОД ПРОВЕРКИ ЭФФЕКТИВНОСТИ ЗАЩИТЫ АКУСТИЧЕСКОЙ ИНФОРМАЦИИ

Вступление

Известно, что основным применяемым методом проверки эффективности активной помехи, используемой для зашумления защищаемого помещения, является метод субъективной оценки разборчивости речи, производимой группой слушателей [1].

Вместе с тем данный метод имеет ряд существенных недостатков. Во-первых, он весьма длителен и трудоемок, а также требует привлечения большого количества людей. Во-вторых, качество оценки зависит от уровня подготовки слушателей, что не может обеспечить уверенность в достоверности такой оценки.

Исходя из этого было бы, по нашему мнению, целесообразно разработать метод экспресс-анализа, позволяющий получить объективную и достоверную оценку эффективности уровня зашумления.

Основная часть

Известно, что еще в 70-х годах XX века профессором Пироговым А.А. был предложен метод объективного экспресс-анализа качества трактов передачи речевых сообщений, основанный на использовании критериев, адекватных принципам оценки качества слуховым анализатором человека [2]. Этот метод был развит до реальных методик и средств [3].

Метод основан на сопоставлении фонетической функции речевого сигнала на входе и выходе исследуемого тракта передачи.

Вместе с тем, фонетическая функция речи (ФФР) достаточно широко используется в фоноскопической экспертизе [4], а мы считаем, что все исследования эффективности блокирования технических каналов утечки акустической информации должны строится с учетом возможностей очистки речевых сигналов, используемых в такой экспертизе.

Более того, в процессе разработки методов и средств проведения такой экспертизы было установлено, что ФФР имеет максимумы при произнесении артикулированных звуков и минимумы в моменты, когда артикуляция отсутствует [4]. Рассмотрим особенности ФФР в плане построения систем фоноскопической экспертизы и попытаемся проанализировать ее пригодность для оценки эффективности защищенности акустической информации.

ФФР можно записать как

$$P(\omega,t)=C\int_0^{\infty}e^{-\frac{\tau}{T}}\lg\frac{S(\omega,t)}{S[\omega,(t-\tau)]}d\tau\ , \qquad (1)$$

где

$P(\omega,t)$ – двумерная фонетическая функция речи;

Ω – частота;