Одним из таких показателей является шероховатость поверхности.

Шероховатость поверхности замеряют чаще всего в направлении подачи. В направлении скорости практически не измеряют. Для цилиндрических деталей (в наиболее ответственных случаях) снимают круглограмму, которая дает четкое представление лишь о волнистости и макроотклонениях поверхности. Неоднородность шероховатости остается неотмеченной, хотя она в некоторых случаях может достигать 50% и более. Такая неоднородность может вызывать развитие отклонения формы в процессе эксплуатации из-за разной величины износа приработки для разных шероховатостей.

При алмазном выглаживании цилиндрических поверхностей из цветных сплавов наблюдается неоднородность шероховатости в направлении скорости. Причем наблюдается явная зависимость величины неоднородности от радиального биения.

Согласно рекомендациям при выглаживании, допускается обработка при радиальном биении вплоть до 0,2 мм, но с ограничением скорости, исходя из неразрывности контакта.

Однако, результаты замеров шероховатости по образующей в разных сечениях, показывают, что таких рекомендаций недостаточно. Чем больше радиальное биение, тем выше неравномерность шероховатости. Таким образом, искажается истинное значение параметров шероховатости.

Подводя итоги, можно утверждать, что алмазное выглаживание относится к точным видам обработки. Оно должно выполняться на более точном оборудовании с соблюдением норм точности исходной заготовки и точности установки детали в приспособление.

ОСНОВНЫЕ ПРИНЦИПЫ ПАРАЛЛЕЛЬНЫХ ВЫЧИСЛЕНИЙ

Свиридов В.И.

Воронежский институт высоких технологий, Воронеж, e-mail: kitaevakseniyavivt@yandex.ru

В общем плане под параллельными вычислениями понимаются процессы обработки данных, в которых одновременно могут выполняться нескольких машинных операций. Достижение параллелизма возможно только при выполнимости следующих требований к архитектурным принципам построения вычислительной системы:

– независимость функционирования отдельных устройств ЭВМ;

– избыточность элементов вычислительной системы – организация избыточности может осуществляться в следующих основных формах:

– использование специализированных устройств таких, например, как отдельных процессоров для целочисленной и вещественной арифметики, устройств многоуровневой памяти (регистры, кэш);

– дублирование устройств ЭВМ путем использования, например, нескольких однотипных обрабатывающих процессоров или нескольких устройств оперативной памяти.

При рассмотрении проблемы организации параллельных вычислений следует различать следующие возможные режимы выполнения независимых частей программы:

– многозадачный режим (режим разделения времени), при котором для выполнения процессов используется единственный процессор;

– параллельное выполнение, когда в один и тот же момент времени может выполняться несколько команд обработки данных; данный режим вычислений может быть обеспечен не только при наличии нескольких процессоров, но реализуем и при помощи конвейерных и векторных обрабатывающих устройств;

– распределенные вычисления; данный термин обычно используют для указания параллельной обработки данных, при которой используется несколько обрабатывающих устройств, достаточно удаленных друг от друга и в которых передача данных по линиям связи приводит к существенным временным задержкам; как результат, эффективная обработка данных при таком способе организации вычислений возможна только для параллельных алгоритмов с низкой интенсивностью потоков межпроцессорных передач данных.

ЦИФРОВОЙ МОДЕМ ДЛЯ СЕТИ ISDN

Секретова Л.В., Чернышев Н.И.

ГОУ ВПО «Пензенская государственная технологическая академия», Пенза, e-mail: los@pgta.ru

Тенденция к объединению компьютеров в сети обусловлена требованием быстрого обмена информацией между пользователями, получением и передачей сообщений не отходя от рабочего места, возможностью быстрого получения информации из любой точки земного шара. Наиболее трудным является объединение в сеть компьютеров, расположенных на большом расстоянии друг от друга. Прокладка новых линий связи требует привлечения больших средств и продолжительного времени. Для передачи информации в условиях интенсивных помех и наводок требуются дорогостоящие кабели, например такие, как волоконно-оптические.

В то же время уже существует телефонная сеть, охватывающая весь земной шар. Телефонная сеть есть в большинстве домов. На предприятиях используется внутренняя телефонная сеть для связи подразделений. Однако коммутируемая телефонная сеть общего пользования (КТСОП) позволяет передавать только аналоговый сигнал. Поэтому для преобразования дискретных цифровых сигналов в аналоговую форму и обратно были разработаны специальные устройства – модемы. У современных модемных подключений максимальная теоретическая скорость передачи составляет 56 кбит/сек, хотя на практике средняя скорость передачи достигает лишь 40-50 кбит/сек. Подключение по КТСОП обладает рядом недостатков: возможная занятость телефона абонента, низкая скорость и невысокое качество передачи. Однако преимущества КТСОП также очевидны – связь через модем не требует прокладки новых линий связи, поскольку используется существующая телефонная сеть и невысокая стоимость оборудования. Основные проблемы КТСОП удалось решить благодаря построению цифровых сетей с интеграцией служб. Такая сеть получила название *ISDN* (*Integrated Services Digital Network*).

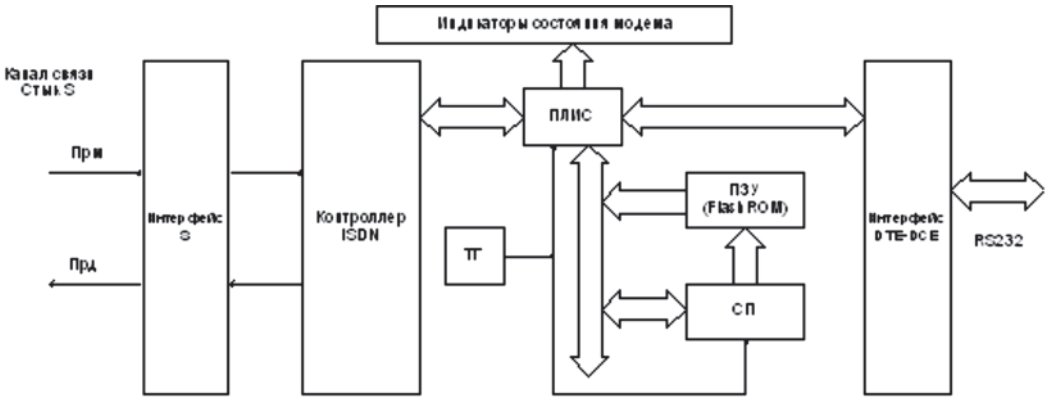
ISDN – это оригинальная концепция построения цифровой сети с интеграцией услуг, специфицированная еще в середине семидесятых годов Международным консультативным комитетом по телефонии и телеграфии (МККТТ). Однако данная технология получила развитие лишь в начале 90-х годов.

Авторами разработано устройство для подключения оборудования общего доступа (ООД) к цифровой сети интегрального обслуживания по интерфейсу базового доступа *ISDN S0* (или *S*). В качестве ООД используется персональный компьютер оператора, который, используя внутреннюю цифровую сеть *ISDN* на предприятии, может осуществлять удаленный доступ или терминальный доступ к объектам управления.

Предлагаемые в настоящее время на Российском рынке изделия этого сегмента обеспечивают большие функциональные возможности, а именно: широкий набор используемых интерфейсов и поддерживаемых протоколов. Это приводит их к аппаратурной и программной избыточности и, как следствие, и к высокой стоимости. В то же время, для осуществления

удаленного и терминального доступа на предприятиях с использованием внутренней цифровой сети *ISDN*, универсальность не является непременным атрибутом оборудования. Поэтому при проектировании цифрового модема были установлены параметры устройства с жестко заданными характеристиками, благодаря чему общая схема устройства значительно упрощается и, как следствие, уменьшится и его стоимость.

Структурная схема цифрового модема приведена на рисунке. Модем представляет собой устройство, имеющее цифровой интерфейс с компьютером (последовательный порт *RS*-232) и интерфейс с каналом связи – разъем для телефонного кабеля (*RJ*-45). В цифровых модемах не используется модуляция и демодуляция сигнала, поэтому его структура проще аналогового. Модем состоит из следующих основных блоков: интерфейс DTE-DCE; интерфейс S; сигнальный процессор (СП); флэш-ПЗУ; программируемая логическая интегральная схема (ПЛИС); тактовый генератор (ТГ); индикаторы состояния модема; узел питания.



Структурная схема модема

Реализация модема в соответствии с приведённой структурной схемой позволяет снизить габариты и стоимость устройства.

КРИПТОСИСТЕМЫ И ВИДЫ АТАК

Секретова Л. В., Борисова С.Н.

ГОУ ВПО «Пензенская государственная технологическая академия», Пенза, e-mail: iis@pgta.ru

Теоретически, приложив достаточно усилий, можно взломать любую криптографическую систему. Вопрос заключается в том, сколько работы необходимо проделать, чтобы информация была расшифрована. Существует множество типов атак, каждый из которых обладает той или иной степенью сложности. Рассмотрим некоторые из них.

Только шифрованный текст. Говоря о взломе системы шифрования, многие имеют в виду атаку с использованием только шифрованного текста. В этом случае пользователи А и Б зашифровывают свои данные, а злоумышленник видит только шифрованный текст. Попытка расшифровать сообщения только при наличии шифрованного текста и называется атакой с использованием только шифрованного текста. Это наиболее трудный тип атаки, поскольку злоумышленник обладает наименьшим объемом информации.

Известный открытый текст. При атаке с известным открытым текстом известен и открытый и шифрованный текст. Цель такой атаки состоит в том, чтобы найти ключ.

На практике существует множество ситуаций, откуда можно узнать открытый текст сообщения. Иногда содержимое сообщения легко отгадать.

При наличии известного открытого текста у злоумышленника оказывается больше информации, чем при наличии только шифрованного текста, а вся дополнительная информация только увеличивает шанс расшифрования.

Существует два вида атак с избранным открытым текстом:

Автономный (offline). Открытый текст, который должен подвергнуться шифрованию, подготавливается заранее, еще до получения шифрованного текста.

*Оперативный (online).*Набор каждого последующего открытого текста осуществляется, исходя из уже полученных шифрованных текстов. Данный вид является более результативным.

Криптосистемы и виды атак на них. Рассмотренные выше виды атак применимы ко всем видам криптосистем. Но каждая из них имеет свои индивидуальные особенности, в результате чего имеются и специфические атаки характерные только для определенных видов криптосистем.

Атаки на блочные шифры. *Блочный шифр* – это функция шифрования, которая применяется к блокам текста фиксированной длины. Текущее поколение блочных шифров работает с блоками текста длиной 128 бит.

Функции шифрования построены на основе многократного применения 32-битовых операций. Применяя такие операции, довольно сложно получить нечетную перестановку. В результате практически все известные блочные шифры генерируют только четную перестановку. Упомянутый факт позволяет злоумышленнику построить простой *различитель* (на основе *различающей атаки*). Так называемый *атака с проверкой четности*. Для заданного значения ключа строится перестановку, зашифровав по порядку все возможные варианты открытого текста. Если перестановка является нечетной, значит, перед нами идеальный блочный шифр, так как реальный блочный шифр никогда не генерирует нечетную перестановку.

Атака с помощью решения уравнений. Основная идея этого метода заключается в том, чтобы представить блочное шифрование в виде системы линейных и квадратных уравнений над некоторым конечным полем, а затем решить эти уравнения, используя новые методы наподобие *XL*, *FXL* и *XSL*.

Атаки на асимметричные шифры. Алгоритм *RSA* обеспечивает как цифровое подписывание, так и шифрование, что делает его весьма универсальным средством.

Алгоритм *RSA* основан на использовании односторонней функции с лазейкой. N – это открытый ключ, который формируется как $n = p \cdot q$. Разложение числа n на множители и есть та самая «лазейка». Значения p и q – это два разных больших простых числа,