ТЕХНИЧЕСКАЯ ДИАГНОСТИКА ЭЛЕКТРОННЫХ СРЕДСТВ

ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ УНПК

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ
УЧРЕЖДЕНИЕ ВЫСШЕГО ПРОФЕССИОНАЛЬНОГО ОБРАЗОВАНИЯ
«ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ - УЧЕБНО-НАУЧНО-
ПРОИЗВОДСТВЕННЫЙ КОМПЛЕКС»

В.Т. Ерёменко, А.А. Рабочий, И.И. Невров,
О.А. Воронина, А.Е. Георгиевский, В.М. Донцов

ТЕХНИЧЕСКАЯ ДИАГНОСТИКА ЭЛЕКТРОННЫХ СРЕДСТВ

Рекомендовано ФГБОУ ВПО «Госуниверситет - УНПК»
для использования в учебном процессе в качестве учебника
для высшего профессионального образования

Орел 2012

УДК 621.396.6(075)
ББК 32.84я7
Т38

Рецензенты:

доктор технических наук, профессор, заведующий кафедрой
«Компьютерные технологии и системы»
Государственного образовательного учреждения
высшего профессионального образования
«Брянский государственный технический университет»
В.И. Аверченков,

доктор технических наук, профессор кафедры «Радиотехника и электроника»
Академии Федеральной службы охраны Российской Федерации
Б.Р. Иванов,

кандидат технических наук, доцент кафедры
«Электроника, вычислительная техника и информационная безопасность»
Федерального государственного бюджетного образовательного
учреждения высшего профессионального образования
«Государственный университет - учебно-научно-
производственный комплекс»
А.В. Тютякин

Т38 **Техническая диагностика электронных средств**: учебник для высшего профессионального образования / В.Т. Ерёменко [и др.]. – Орел: ФГБОУ ВПО «Госуниверситет - УНПК», 2012. – 157 с.

ISBN 978-5-93932-424-3

В учебнике изложены основные понятия и методы контроля и диагностики электронных средств, широко используемых в системах электронной техники. Особое внимание уделено диагностике цифровых вычислительных средств и элементов цифровой электроники.

Предназначен для студентов, продолжающих обучение по магистерским программам 210200.68 «Информационные технологии проектирования электронных средств», 211000.68 «Конструирование и технология электронных средств», и первого года обучения по направлению 210200.62 «Проектирование и технология электронных средств», изучающих дисциплину «Техническая диагностика электронных средств».

Может быть полезен студентам, обучающимся по техническим специальностям, связанным с использованием, разработкой и эксплуатацией информационных управляющих систем и электронных средств в любых отраслях народного хозяйства.

УДК 621.396.6(075)
ББК 32.84я7

ISBN 978-5-93932-424-3

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

Расширение областей автоматизированного управления производственными и интеллектуальными сферами деятельности современного общества сопровождается бурным развитием электронных систем и существенным усложнением этих систем. Вместе с тем непрерывно возрастают требования к надежности действия сложных систем, от правильной работы которых зависят в конечном счёте здоровье и жизнь людей и состояние окружающей среды.

Любой объект, созданный руками человека, не может иметь абсолютную (стопроцентную) надежность. Чтобы приблизиться к ней, человеческая мысль развивается в самых разных направлениях по пути повышения этой надежности. Одним из способов повышения надежности действия технических систем является техническая диагностика, в частности диагностика электронных средств.

Техническая диагностика (ТД) – это отрасль научно-технических знаний, сущность которой составляют теория, методы и средства обнаружения и поиска дефектов объектов технической природы. Под дефектом следует понимать любое несоответствие свойств объекта заданным, требуемым или ожидаемым свойствам. Использование технической диагностики расширяется и совершенствуется, так как она всё ощутимее становится гарантией качества и надежности любых технических, в том числе и электронных систем.

Диагностика в буквальном смысле – это распознавание, определение существа и особенностей на основе всестороннего исследования, способность распознавать, учение о методах и принципах распознавания свойств объекта.

Техническая диагностика является разновидностью технического контроля. Основная задача ТД электронных средств состоит в организации контроля исправности, работоспособности и правильности функционирования изделий электронной техники (ИЭТ). ТД позволяет определять некачественные или потенциально негодные ИЭТ. Результатом ТД является заключение о техническом состоянии электронных приборов – технический диагноз.

Структура учебника построена таким образом, чтобы понимание материала было наилучшим. В первой главе рассмотрены общие вопросы технического контроля, освещены вопросы измерения и погрешностей, так как измерения – это основа контроля и диагностики.

Во второй главе особое внимание уделено частотным измерениям и преобразованиям, как наиболее современным и точным в цифровой технике.

В главе 3 даются понятия об автоматических системах контроля и диагностики электронных средств и видах функционального и тестового диагностирования.

Глава 4 посвящена описанию современных методов контроля и диагностирования процессов передачи и преобразования двоичной информации. В главе 5 рассмотрены вопросы моделирования неисправностей и алгоритмические методы диагностирования, в частности, для запоминающих устройств. В главе 6 дана краткая характеристика аппаратных и программно-аппаратных средств, используемых при диагностировании электронных систем.

В главе 7 рассмотрены особенности диагностики микропроцессорных систем, даны понятия о самодиагностике в этих системах, краткий обзор современных программных средств для диагностики.

Материал учебника выстроен таким образом, чтобы у студента выработалось представление по предлагаемой тематике, достаточное для разработки общей процедуры по осуществлению контроля функционирования и диагностики электронных устройств разного вида. Это представление реализуется и углубляется в ходе выполнения курсовой работы по диагностике конкретного устройства.

1. ОБЩИЕ СВЕДЕНИЯ О ТЕХНИЧЕСКОМ КОНТРОЛЕ И ИЗМЕРЕНИЯХ В ЭЛЕКТРОНИКЕ

1.1. Виды и назначение технического контроля

Технический контроль (ТК) – это проверка соответствия технических характеристик изделий, материалов или процессов требованиям нормативно-технической документации (НТД), осуществляемая в ходе производственного процесса [1]. ТК может быть сплошным и выборочным. В зависимости от стадии производства различают входной, операционный и выходной контроль.

Операционный контроль осуществляется в ходе выполнения или после завершения какой-либо технологической операции. Операционный контроль позволяет своевременно обнаружить брак в изделии (материале) или нарушение технологии, установить причину нарушения, изъять бракованные изделия из дальнейшей обработки, своевременно производить подналадку и настройку оборудования и технологической оснастки.

Выходной контроль готовых изделий электронной техники (ИЭТ) и материалов проводится после выполнения последней операции технологического процесса для выявления некондиционной или потенциально негодной продукции. К выходному контролю часто относят различные испытания изделий на надежность, испытания для определения допустимых границ изменения условий и режимов эксплуатации ИЭТ, для отнесения изделий к той или иной группе по точности, идентичности параметров и т.п.

В электронном приборостроении выходному контролю подвергаются практически все виды ИЭТ – от простых элементов (резисторы, конденсаторы, полупроводниковые элементы и т.п.) до сложных электронных узлов [большие интегральные схемы (БИС), сверхбольшие интегральные схемы (СБИС), микропроцессоры (МП) и др.]. Выходной контроль осуществляется с помощью системы контрольно-измерительных устройств, обеспечивающих измерение параметров ИЭТ и проверку их работоспособности в различных режимах. В интегральной электронике используются различные виды контроля.

Встроенный контроль (ВК) электронных средств (на примере БИС) – это проверка работоспособности электронных устройств (ЭУ), выполняемая с помощью специальных средств контроля и обнаружения

неисправностей (НИ), например, схем сравнения, генераторов сигналов, входящих в состав данного устройства и конструктивно объединенных с ним в единое целое. ВК используется в микроЭВМ, микроконтроллерах, выполненных в виде БИС и СБИС.

Различают встроенный контроль *технологический* (ВКТ) и *функциональный* (ВКФ). Первый используют при создании БИС на разных стадиях их изготовления, а второй – при приемосдаточных испытаниях и в процессе эксплуатации устройства.

По полноте проверки функционирования БИС различают ВК *полный* и *локальный*. В первом виде проверяются все функциональные возможности БИС, во втором – работа отдельных элементов. Кроме того, различают ВК: тест-ориентированный, процедурно-ориентированный и проблемно-ориентированный.

При тест-ориентированном встроенном контроле используется определенная группа тестов.

Процедурно-ориентированный ВК – это проверка работы устройства по результатам решения заданного набора задач.

Проблемно-ориентированный контроль состоит в проверке внутреннего физического или логического состояния БИС при изготовлении, испытаниях или эксплуатации.

Достоинства ВК заключаются в том, что он:

– обеспечивает проверку функционирования БИС в реальном масштабе времени;

– повышает качество контроля.

БИС с ВК имеют обычно один-два вывода для подачи опросных сигналов и получения контрольной информации. Такие БИС или устройства позволяют создавать микроэлектронную аппаратуру с достаточно простой контрольно-диагностической системой, не требующей сложной измерительной аппаратуры.

Входной контроль (ВхК) – это контроль поступающих на предприятие комплектующих изделий, материалов и контрольно-измерительных приборов в целях их выбраковки до запуска в производство.

ВхК материалов и полуфабрикатов предусматривает проверку химического состава, механических, физических свойств материала, геометрических размеров заготовок, наличия в них видимых и скрытых дефектов. Этот контроль осуществляется с помощью:

– микроскопов;

– дефектоскопов;

– лупы;

– мерительных инструментов;
– поверочных плит;
– разрывных машин;
– термостатов;
– анализаторов состава веществ и т.д.

Входной контроль комплектующих имеет целью проверку их соответствия требованиям нормативно-технической документации. Он выполняется с помощью стандартных электро- и радиоизмерительных приборов и устройств, специализированных контрольно-измерительных средств.

ВхК измерительных приборов проводится для подтверждения их соответствия паспортным данным. Такой вид контроля осуществляется с помощью высокоточной электро- и радиоизмерительной аппаратуры: микроамперметров, универсальных вольтметров, омметров и т.п. В состав аппаратуры могут дополнительно входить измерительные генераторы, осциллографы, образцовые меры ЭДС. Все используемые при входном контроле оборудование, аппаратура и инструменты должны подвергаться периодическим межведомственным поверкам.

Неразрушающий контроль (НК) – это совокупность методов измерения и контроля показателей качества изделия без изменения его свойств, параметров и характеристик. НК позволяет:

– получать дополнительную информацию, прямо или косвенно характеризующую поведение этого изделия во времени;

– отбраковывать на стадии изготовления потенциально ненадежные изделия со скрытыми дефектами;

– отбирать наиболее стойкие изделия для работы в особо сложных условиях;

– определять причины возникновения скрытых дефектов.

За счет этого повышается вероятность безотказной работы изделия, уменьшается вероятность отказа изделия во время эксплуатации. Для изделий электронной техники разработаны и широко используются оптические, тепловые, акустические, радиоволновые, радиационные и другие методы НК. Они основаны на анализе взаимодействия электромагнитного излучения с объектом контроля, регистрации тепловых полей, исследовании распространения упругих колебаний в контролируемом объекте, изучении структуры материалов при помощи обычных и электронных микроскопов, спектрометров, эллипсометров и других средств.

С помощью НК решают такие задачи, как проверка качества соединений элементов из разнородных материалов, проверка оптимальности схемно-топологических решений полупроводниковых структур, оценка качества сборки и герметизации электронных приборов, плат; определение электрических параметров испытуемой электронной техники [1]. Состав и назначение технических средств НК определяются задачами в системе контроля качества продукции. Например, для отбора электронных приборов и устройств с пониженным уровнем шума применяют измерители шумов, измерители нелинейных искажений, анализаторы вольт-амперных характеристик.

При разработке или производстве ИЭТ, особенно при анализе причин их отказов, используют комплексы оборудования, где НК может осуществляться различными методами. Например, универсальный лазерный сканирующий микроскоп позволяет получать изображение объекта или его части (оптический метод), регистрировать индуцируемый ток (электрофизический метод), возбуждать в объекте гиперзвуковые колебания (акустический метод). Такие комплексы снабжаются мини- и микроЭВМ для обработки и фиксации результатов контроля или исследования.

Между обычным и неразрушающим контролем нет четкой границы, за исключением случаев контроля механической прочности (испытания на разрыв), растворимости, термостойкости и т.п.

Методы и технические средства НК, используемые для выявления дефектов структуры (поры, трещины, загрязнения, инородные включения), называются *дефектоскопией*.

Визуальный контроль – метод обнаружения и анализа внешних дефектов ИЭТ, возникающих на разных этапах производства, осуществляемый оператором с использованием оптических средств. Это один из видов контроля качества электронных приборов. Наиболее трудоемким считается визуальный контроль монолитных и гибридных ИС, особенно кристаллов с биполярными или МДП-структурами. При визуальном контроле выявляют дефекты полупроводниковых пластин, коррозию и отслаивание металлических пленок, нестравленные участки, смещение слоев, дефекты напыления резиста и т. п. При определении дефектов пользуются эталонными образцами ИЭТ, чертежами, фотографиями, операционными картами технологического процесса, применяя метод сравнения. Основное техническое средство визуального контроля – микроскоп, например металлографический микроскоп ММУ-3. Разработаны автоматизированные установки ви-

зуального контроля, оснащенные микропроцессорной системой с экраном, с автоматизированной подачей контролируемого объекта под окуляр микроскопа [2].

1.2. Измерения – основа диагностики

Один из этапов диагностики – изучение (исследование) объекта, а изучение невозможно без измерения. По мнению Т. Кельвина, «каждая вещь известна лишь в той степени, в какой ее можно измерить» [3]. В электронике используются различные виды измерений: электрические, магнитные, радиоизмерения.

Измерение – это нахождение значений физических величин опытным путем с помощью специальных технических средств. *Значение физической величины* – это количественная характеристика свойств физического объекта, его состояния и происходящих в нём процессов. Физические величины материализуются в специальных средствах измерений – *эталонах и мерах.*

В системе СИ (международная система единиц) определены семь основных единиц, через которые выражаются остальные, называемые производными (ГОСТ 9867-61) (табл. 1.1). Выбраны следующие основные единицы физических величин:

1) масса – килограмм (кг);
2) длина – метр (м);
3) время – секунда (с);
4) сила тока – ампер (А);
5) термодинамическая температура – кельвин (К);
6) сила света – кандела (кд);
7) количество вещества – моль (моль).

Средства измерений – это технические средства, используемые при измерениях и имеющие нормируемые метрологические свойства. Различают следующие виды средств измерений:

– меры;
– измерительные приборы;
– измерительные установки;
– измерительные системы.

Мера – средство измерения, предназначенное для воспроизведения физической величины заданного размера. Мера может быть однозначной, многозначной и в виде набора. Например, конденсатор постоянной емкости, нормальный элемент (НЭ), гиря – это *однозначные* меры.

Нормальный элемент – это специальный гальванический элемент, ЭДС которого точно известна. Есть два вида НЭ:

– *насыщенный НЭ*, имеющий четыре класса точности: 0,0005; 0,001; 0,002; 0,005. Значение ЭДС насыщенного элемента, например, класса 0,0005 при температуре 20 ^{o}C должно быть в пределах (1,0185 – 1,0187) В (допустимое изменение за год ≤ 5мкВ, ток – не более 1 мкА);

Таблица 1.1

Производные единицы некоторых распространенных величин

Физическая величина	Наименование единицы	Обозначение		Выражение
		русское	междунар.	
Работа, энергия, количество теплоты	джоуль	Дж	J	н.м
Мощность	ватт	Вт	W	Дж/с
Количество электричества	кулон	Кл	C	А·с
Электрическое напряжение, разность потенциалов, ЭДС	вольт	В	V	Вт/А
Напряженность электрического поля	вольт на метр	В/м	V/m	-
Электрическое сопротивление	ом	Ом	Ω	В/А
Электрическая емкость	фарада	Ф	F	Кл/В
Поток магнитной индукции	вебер	Вб	Wb	В·С
Индуктивность и взаимная индуктивность	генри	Гн	H	Вб/А
Магнитная индукция	тесла	Тл	T	Вб/м^2
Напряженность магнитного поля	ампер на метр	А/м	A/m	-
Магнитодвижущая сила	ампер	А	A	-
Частота	герц	Гц	Hz	с$^{-1}$

– *ненасыщенный НЭ* (класс точности – не более 0,002, ЭДС – в пределах (1,0186 – 1,0196) В при допустимом изменении за год ≤ 20 мкВ).

Ненасыщенный НЭ имеет меньшее внутреннее сопротивление, чем насыщенный (около 300 Ом).

НЭ – это *образцовая* мера. Его нельзя переворачивать, трясти, нагревать, облучать светом. В качестве *рабочей* меры часто используется прецизионный стабилизатор постоянного напряжения. Он может

обеспечить постоянство выходного напряжения до тысячных долей процента при температурном коэффициенте напряжения около 0,001%/^{o}C и значительных токах нагрузки.

Линейка с миллиметровыми делениями, конденсатор переменной емкости, вариометр индуктивности являются *многозначными* мерами.

Набор мер – набор гирь, магазин сопротивлений, емкостей.

Измерительный прибор – средство измерения, предназначенное для выработки сигналов измерительной информации, т.е. информации о значениях измеряемой величины в форме, доступной для непосредственного восприятия наблюдателя. Измерительные приборы могут быть:

– аналоговые,
– цифровые,
– показывающие,
– регистрирующие,
– самопишущие,
– печатающие.

Для получения результата измерения физической величины в процессе измерения обязательно должна участвовать мера. В измерительных *приборах прямого действия* входная величина преобразуется от входа до указателя, а роль меры выполняет специальное устройство, откалиброванное с помощью меры при изготовлении прибора. В *приборах сравнения* производится непосредственное сравнение входной величины с мерой.

По роду измеряемой электрической величины измерительные приборы подразделяют на амперметры, вольтметры, омметры, особая группа – мультиметры.

По характеру применения различают измерительные приборы стационарные (щитовые) и переносные, а по исполнению – обыкновенные, пыле-, водо-, брызгозащищенные, герметичные и т.д.

1.3. Измерительные преобразователи и физические эффекты, используемые при измерениях

Измерительные преобразователи – это средства измерения, предназначенные для выработки сигналов измерительной информации в форме, удобной для передачи, дальнейшего преобразования, обработки и (или) хранения, но не поддающейся непосредственному восприятию наблюдателя. Измерительный преобразователь имеет вход,

на который подается преобразуемая *входная величина*, и выход, на котором образуется *выходная величина* преобразователя. Выходная величина связана с входной зависимостью вида $y = Ф(x)$, называемой *функцией преобразования*.

Существуют также преобразователи с несколькими входами, реализующие зависимость выходной величины либо от всех входных, либо от одной какой-либо входной величины при неизменных остальных.

Функция преобразования отображает связь между входной и выходной величинами качественно. Для отражения количественной связи между ними вводят *градуировочную характеристику* (ГХ), которая представляет собой зависимость между входной и выходной величинами измерительного преобразователя, составленную в виде таблицы, графика или формулы. *Измерительная цепь* может иметь несколько преобразователей, включенных последовательно. В этом случае первый измерительный преобразователь, к которому непосредственно подводится измеряемая величина, называют *первичным измерительным преобразователем* (ПИП).

Электрические измерительные преобразователи можно различать по характеру преобразуемых величин:

– электрических в электрические;

– неэлектрических в электрические (датчики);

– магнитных в электрические;

– электрических в неэлектрические.

По назначению выделяют:

– *масштабные* измерительные преобразователи: шунты, делители напряжения, измерительные усилители и трансформаторы;

– преобразователи рода величины.

К измерительным преобразователям электрических величин в электрические относятся:

- электрическая величина – цифровой код;
- напряжение – частота;
- напряжение – период электрических колебаний;
- активная мощность – напряжение и т.д.

Примерами преобразователей неэлектрических величин в электрические могут быть:

– термоэлектрические преобразователи;

– термисторы;

– тензорезисторы;

– индуктивные и ёмкостные преобразователи и т. п.

С их помощью в электрический сигнал преобразуются такие неэлектрические величины, как температура, деформация, давление, скорость и т.п.

Примером преобразования электрической величины в неэлектрическую служит измерительный механизм электромеханического прибора.

Для преобразования магнитных величин в электрические используют индукционные, квантовые, гальваномагнитные преобразователи, использующие эффект Холла (открыт в 1879 г.).

Эффект Холла представляет собой явление возникновения в проводнике с током, помещенном в магнитное поле, электрического поля с вектором напряженности, перпендикулярным к направлению тока и направлению вектора магнитной индукции (рис. 1.1) [2].

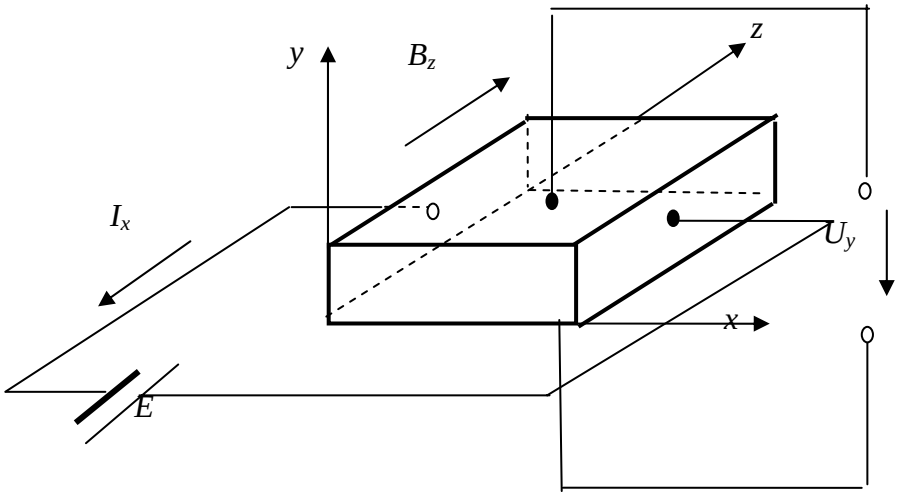


Рис. 1.1. Иллюстрация к принципу возникновения эффекта Холла

Напряжение, создаваемое на гранях элемента Холла:

$$U_y = R \cdot B_z \cdot I_x / L_z ,$$

где R – постоянная Холла (для металлов $R \sim 10^{-3}$ см^3/Кл, для полупроводников $R \sim 10^5$ см^3/Кл, в слабых магнитных полях $R = \mu / \delta$, где μ – подвижность носителей заряда, δ – удельная электропроводимость);

B_z – вектор магнитной индукции внешнего магнитного поля;

I_x – ток в проводнике, создаваемый источником ЭДС E;

L_z – размер пластины по оси z.

Свойства преобразователя Холла (ПХ) – датчика Холла. ПХ преобразует индукцию магнитного поля в электрическое напряжение. Он

представляет собой пленку из полупроводника (Se, Ge, GaAs, InSb), напыленную на прочную подложку из диэлектрика (слюда, керамика, феррит) с четырьмя электродами. Преобразователи Холла могут быть измерительные и индикаторные. Применяются они как первичные преобразователи в магнитометрах, установках для контроля параметров магнитных материалов, бесконтактных амперметрах, аналоговых перемножающих устройствах, измерителях линейных и угловых перемещений, бесконтактных преобразователях постоянного тока в переменный и др. Индикаторные ПХ служат для установления факта наличия или отсутствия магнитного поля в данной точке пространства.

Основными характеристиками ПХ являются следующие:

1. Чувствительность: $K_ч = R_x / B$, где R_x – холловское сопротивление; B – магнитная индукция.
2. Остаточное напряжение при $B = 0$.
3. Температурные коэффициенты чувствительности и остаточного напряжения.
4. Коэффициент нелинейности.
5. Коэффициент расходимости (изменение чувствительности при изменении вектора магнитной индукции).

Помимо эффекта Холла, в технике измерений находят применение и другие эффекты.

Эффект Керра:

– *электроопический* – возникновение двойного лучепреломления в оптически изотропной среде (жидкость, стекло, кристалл с центром симметрии) под действием однородного электрического поля;

– *оптический* – возникновение постоянной составляющей двойного лучепреломления в изотропной среде под действием лазерного излучения;

– *магнитооптический* – изменение характера поляризации света при его отражении от немагнитной среды (линейно поляризованный свет становится эллиптически поляризованным, причем большая ось эллипса оказывается повернутой на некоторый угол по отношению к плоскости поляризации падающего света). Используется при исследовании магнитных материалов.

Эффект Фарадея – эффект магнитооптики, заключающийся во вращении плоскости поляризации света при его распространении в немагнитном веществе. Эффект Фарадея максимален, если свет распространяется параллельно или антипараллельно вектору намагниченности среды.

Эффект Фарадея, разный в диа- и парамагнетиках, используется в оптоэлектронных и СВЧ-устройствах. В оптическом диапазоне наибольший вклад в эффект дает разница диэлектрической проницаемости (ε_- и ε_+). Диэлектрическая проницаемость – это способность диэлектрика поляризоваться в электрическом поле. Для вакуума ε_o = 8,854·10^{-12} Ф/м. Обычно используется относительная проницаемость $\varepsilon_r = \varepsilon / \varepsilon_o$ или диэлектрическая восприимчивость χ, причем $\chi = \varepsilon_r - 1$.

Диамагнетик намагничивается в направлении, противоположном магнитному полю, при отсутствии последнего – немагнитен. Таковыми являются ртуть, графит, золото, цинк, висмут, нафталин, глицерин, азот, водород, инертный газ.

Парамагнетик – слабомагнитное вещество, намагничивающееся во внешнем магнитном поле вдоль направления поля. При отсутствии внешнего поля намагниченность отсутствует. К парамагнетикам относятся ферро-, ферри- и антиферромагнетики при температурах, бóльших температуры точки Кюри.

Магниторезистивный эффект (МРЭ) – изменение электрического сопротивления твердых проводников под действием внешнего магнитного поля. У всех полупроводников и металлов, кроме ферромагнитных, удельное электрическое сопротивление ρ увеличивается с ростом напряженности H магнитного поля (рис. 1.2).

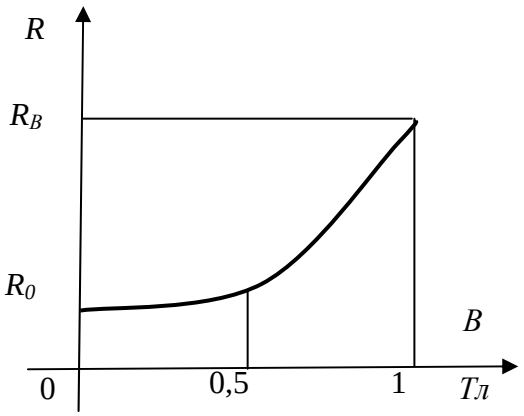


Рис. 1.2. Зависимость сопротивления магниторезистора от индукции магнитного поля:
$R_B / R_0 \sim 1{,}5$; $P_{рас} < 0{,}25$ Вт;
R_0 = (5 – 1000) Ом, материал – ZnSb,
температурный коэффициент
сопротивления – от 0,02 до 2 % К$^{-1}$.

В обычных металлах при комнатной температуре ρ изменяется на десятые доли процента в полях с напряженностью $H = 10^6$ А/м. В полупроводниках МРЭ выражен сильнее и зависит в большей степени от концентрации примесей и температуры. МРЭ лежит в основе работы некоторых магнитометров, детекторов напряжения и др.

Магниторезистивный способ воспроизведения информации применяют в накопителях с подвижными носителями записи (магнитные ленты, диски, барабаны), устройствах памяти на ЦМД, системах звуко-, видео- и цифровой записи (магниторезистивные магнитные головки).

Отличительная особенность магниторезистивного способа состоит в том, что при записи и воспроизведении информации амплитуда сигнала не зависит от скорости движения носителя. Магниторезистор используется как переменный бесконтактный резистор (нет движка), как датчик магнитного поля, потенциометр, переключающий элемент в бесконтактной коммутационной аппаратуре.

По роду выходной величины измерительные преобразователи неэлектрических величин в электрические подразделяются:

– на генераторные – входная величина преобразуется в ЭДС или ток;

– параметрические – входная величина преобразуется в один из параметров электрической цепи *R*, *L*, *C* или *M*.

Генераторные преобразователи не требуют постороннего источника энергии, кроме воздействия преобразуемой величины, а параметрические – нуждаются в постороннем источнике энергии. Например, термоэлектрический преобразователь выполняет свою функцию без постороннего источника энергии, а термоанемометр (нагреваемая проволока) преобразует скорость газа в приращение сопротивления только при помощи постороннего источника тока.

1.4. Основные характеристики процесса измерения

К общим характеристикам процесса измерения относятся:

– погрешности;

– вариации показаний;

– чувствительность к входной величине;

– мощность, потребляемая от объекта измерения;

– быстродействие;

– время установления показаний;

– диапазон измерения;

– надежность.

Первые семь характеристик являются еще и метрологическими характеристиками, которые влияют на результаты измерения.

Погрешность – это характеристика, связанная с понятием об истинном значении физической величины X_u, под которым подразумевается значение физической величины, идеальным образом отражающее в качественном и количественном отношениях соответствующее свойство объекта. *Погрешность измерения* – это отклонение результата измерения от истинного значения входной величины. Различают две составляющие погрешности измерения:

– инструментальную (она зависит от погрешности средств измерений);

– методическую, которая зависит от методики измерения.

Эти составляющие используют для измерительного преобразователя.

Кроме того, различают абсолютную, относительную и приведенную погрешности.

Абсолютная погрешность (Δ) выражается в единицах входной величины. Для прибора $\Delta = X - X_u$, где X – показание прибора.

Для измерительного преобразователя абсолютная погрешность по входу – это разность между значением величины на входе, определяемым по истинному значению на его выходе с помощью градуировочной характеристики преобразователя, и истинным значением величины на входе преобразователя. Абсолютная погрешность, взятая с обратным знаком, называется *поправкой*.

Относительная погрешность определяется выражением

$$\delta = \Delta / X_u \cdot 100\ \%.$$

Для приборов и преобразователей на практике допустимо относить абсолютную погрешность к значению входной величины, найденному с помощью данного средства измерения.

Истинное значение X_u остается неизвестным, поэтому на практике пользуются «действительным» значением величины, которое может быть определено экспериментально при помощи образцовых средств измерения.

Для приборов и преобразователей используют понятие *приведенной погрешности* γ:

$$\gamma = \Delta / X_N \cdot 100\ \%,$$

где X_N – нормирующее значение измеряемой величины, которое принимается равным:

1) для средств измерения с квазиравномерной шкалой:

– конечному значению шкалы, если нулевая отметка на краю или вне шкалы;

– арифметической сумме конечных значений диапазона измерений, если нулевая отметка находится внутри диапазона измерений;

2) для средств измерения с установленным номинальным значением – этому номинальному значению. Например, частотомер с диапазоном 45 – 55 Гц имеет номинальное значение 50 Гц, тогда X_N = 50 Гц;

3) для средств измерения с существенно неравномерной шкалой – всей длине шкалы (или ее части, соответствующей диапазону измерений). В этом случае абсолютную погрешность, как и длину шкалы, выражают в единицах длины.

В зависимости от изменения во времени входной величины различают следующие погрешности средств измерений:

– *статическую погрешность* при измерении постоянной по времени величины;

– *динамическую погрешность* – разность между погрешностью при измерении переменной во времени величины и статической погрешностью в данный момент времени.

В зависимости от характера изменения погрешности различают:

• *систематические погрешности* – составляющие погрешности, остающиеся постоянными или закономерно изменяющиеся при повторном измерении одной и той же величины;

• *случайные погрешности* – составляющие погрешности, изменяющиеся случайным образом при повторных измерениях.

По условиям возникновения различают:

– *основную погрешность* – погрешность средства измерения при нормальных условиях;

– *дополнительную погрешность* – погрешность средства измерения, вызванную отклонением одной или более влияющих величин от нормального значения или выходом за пределы областей нормальных значений.

Зависимость абсолютной погрешности Δ от входной величины характеризуется *аддитивной и мультипликативной* погрешностями (рис. 1.3):

$$|\Delta_{MAX}| = |a| + |вX|,$$

где a – предельное значение аддитивной погрешности;

$вX$ – предельное значение мультипликативной погрешности.

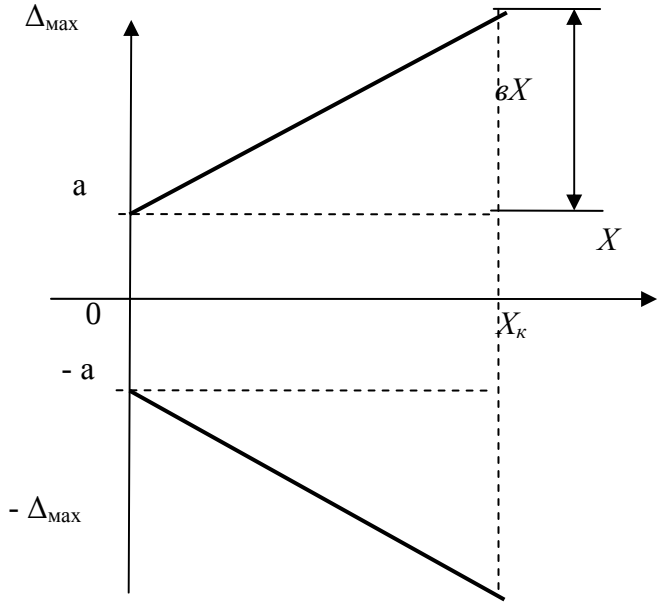


Рис. 1.3. Зависимости погрешностей от входной величины

Аддитивные погрешности не зависят от значений измеряемой величины X, а мультипликативные – пропорциональны значению X. Источники аддитивной погрешности – трение в опорах стрелочных приборов, неточность отсчета по шкале, дрейф, наводки, вибрации и т. п. Аддитивная погрешность по сути определяет то наименьшее значение величины, которое можно измерить.

Источники мультипликативной погрешности – действия влияющих величин на параметры узлов и элементов средств измерения.

Предельное значение относительной погрешности средства измерения δ'_{max} (в процентах) связано с предельным значением абсолютной погрешности Δ_{max} зависимостью

$$\delta'_{max} = \left(|\Delta|_{max} / X\right) \cdot 100\ \% = \left(a / X + |в|\right) \cdot 100\ \%.$$

По ГОСТ 8.401-80 средствам измерения присваиваются определенные классы точности. *Класс точности* – это обобщенная характеристика, определяемая пределами допускаемых основной погрешно-

сти и погрешностей, вызванных изменением значений влияющих величин. У приборов аддитивная составляющая преобладает над мультипликативной, поэтому абсолютная и приведенная погрешности оказываются постоянными в любой точке шкалы. У таких приборов класс точности выражается одним числом, выбираемым из ряда: $1 \cdot 10^n$; $1{,}5 \cdot 10^n$; $2 \cdot 10^n$; $2{,}5 \cdot 10^n$; $4 \cdot 10^n$; $5 \cdot 10^n$; $6 \cdot 10^n$, где n = 1; 0; -1; -2 и т.д.

Основная приведенная погрешность, выраженная в процентах, не должна превышать значение класса точности (к таким приборам относятся регистрирующие и аналоговые показывающие приборы). Для тех приборов, у которых аддитивная и мультипликативная погрешности соизмеримы, класс точности обозначается двумя цифрами через косую черту, например: 0,1/0,05. Погрешность при этом определяется по формуле

$$\delta_{\text{мах}} = \pm [C + d (\left| X_k / X \right| - 1)],$$

где C и d – числа, разделяемые косой чертой (класс точности средства измерения);

X_k – больший (по модулю) из пределов измерений (конечное значение диапазона измерений).

Обозначение класса точности C/d должно быть больше единицы. Это характерно для цифровых показывающих приборов и приборов сравнения с ручным или автоматическим уравновешиванием.

Вариация показаний – это наибольшая разность показаний прибора при одном и том же значении измеряемой величины и неизменных внешних условиях. Причина вариации в стрелочных приборах – трение в опорах подвижной части.

Чувствительность прибора и преобразователя – это производная выходной величины по входной:

$$S = \varphi (X) = dl / dX,$$

где l – перемещение указателя;

X – измеряемая величина.

$S = l / X$, если S не зависит от измеряемой величины и шкала прибора равномерна.

Величина $C = 1 / S$ называется *постоянной прибора*. Например, если S = 10 делений /В, то C = 0,1 В/деление.

Параметр, эквивалентный чувствительности, называют *крутизной*:

$$S(x) = dF(x) / dx.$$

Используют также термины: *чувствительность измерительного преобразователя, коэффициент преобразования, коэффициент передачи, коэффициент усиления,* под которыми подразумевают отношение значения сигнала на выходе измерителя преобразователя к значению вызывающего его сигнала на входе преобразователя.

Порог чувствительноти – это изменение измеряемой величины, вызывающее наименьшее изменение показаний, обнаруживаемое наблюдателем (при нормальном для данного прибора способе отсчета).

Потребляемая мощность – мощность, потребляемая при включении прибора в цепь, в которой делается измерение.

Быстродействие – число измерений (преобразований) в единицу времени. Параметр важен в том случае, когда одним прибором с помощью коммутирующего устройства нужно измерить несколько медленно меняющихся величин.

Время установки показаний (время успокоения) – промежуток времени, который проходит с момента изменения измеряемой величины до момента, когда указатель займет положение, соответствующее новому значению измеряемой величины, а отклонение указателя от установленного значения не превышает 1% длины шкалы (обычно время успокоения – не более 4 с).

Диапазон измерений – область значений между нижним и верхним пределами измерений. Пределы измерений – это наибольшее и наименьшее значения величин, которые могут быть измерены с нормированной погрешностью. В диапазоне измерений следует отмечать *диапазон показаний* – область значений входной величины, ограниченную конечным и начальным значениями шкалы прибора.

Надежность средств измерений – это способность сохранять заданные характеристики при определенных условиях работы в течение заданного промежутка времени. Количественная мера надежности – вероятность безотказной работы в заданном промежутке времени и заданных условиях работы.

Отказ – событие, при котором значение одной или нескольких характеристик средств измерений выходит из заданных предельных значений.

Вероятность безотказной работы – это вероятность того, что в течение определенного времени T непрерывной работы не произой-

дет ни одного отказа. Время безотказной работы указывается в технической документации.

Часто используется приближенное значение вероятности как отношение числа средств измерений, продолжающих после времени T безотказно работать, к общему числу испытываемых средств измерений.

К показателям надежности относят также *среднее время* безотказной работы средства измерения, определяемое как среднеарифметическое времени исправной работы.

1.5. Классификация видов и методов измерений

Наглядно классификацию видов и методов измерений можно представить в виде схем (рис. 1.4 и 1.5).

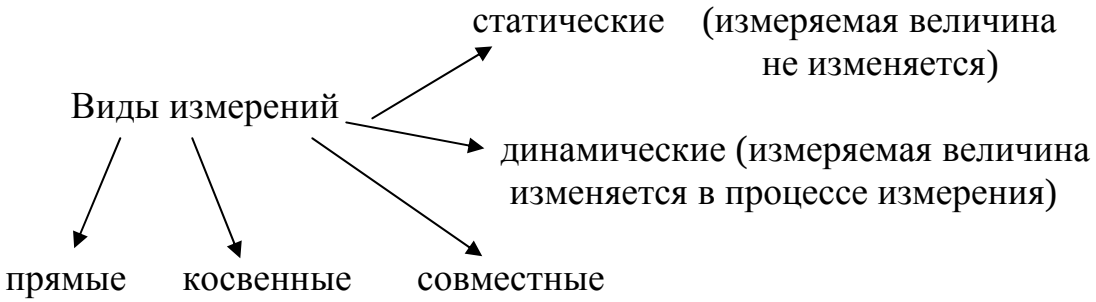


Рис. 1.4. Классификация видов измерений

Прямыми называют измерения, при которых искомое значение измеряемой величины находят непосредственно из опытных данных. *Косвенными* следует называть измерения, при которых искомое значение находят на основании известной функциональной зависимости между величинами:

$$Y = F\,(x_1, x_2 \ldots x_n),$$

где Y – искомое значение;

$(x_1 \ldots x_n)$ – аргументы функции F.

Совместными называют одновременные измерения двух или нескольких разноимённых величин для нахождения зависимости между ними. Одним из примеров совместных измерений является измерение ЭДС термопары для определения коэффициентов аппроксимации характеристики этой термопары:

$$E = At + Bt^2 + Ct^3,$$

где A, B, C – искомые коэффициенты;

t – температура.

Измерив ЭДС E при разных значениях температуры, получим систему уравнений, которая дает возможность определить коэффициенты A, B, C:

$$\left.\begin{aligned} E_1 &= At_1 + Bt_1^{\,2} + Ct_1^{\,3} \\ E_2 &= At_2 + Bt_2^{\,2} + Ct_2^{\,3} \\ E_3 &= At_3 + Bt_3^{\,2} + Ct_3^{\,3} \end{aligned}\right\}$$

Методы измерений весьма многочисленны. Основные из них можно условно разбить на две большие группы: метод непосредственной оценки и метод сравнения с мерой. В диаграмме (рис. 1.5), определяющей классификацию, поясняется смысл этих методов.

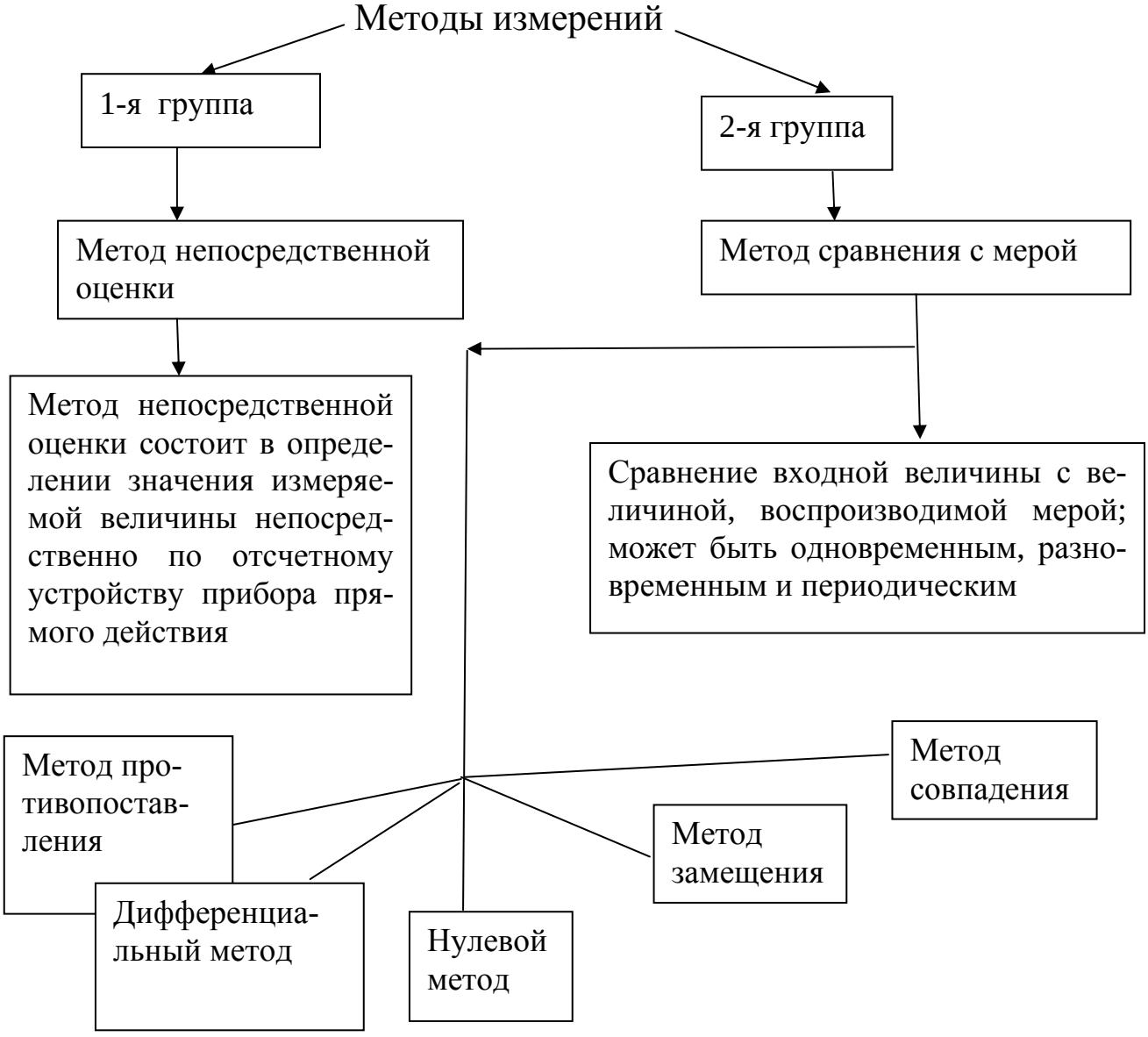


Рис. 1.5. Классификация методов измерений

Метод сравнения с мерой, позволяющий автоматизировать процессы измерения и контроля, имеет множество разновидностей:

• *метод противопоставления* – метод, при котором входная величина, воспроизводимая мерой, одновременно воздействует на устройство сравнения;

• *дифференциальный метод* – метод сравнения с мерой, в котором прибор показывает разность между измеряемой величиной и известной величиной, воспроизводимой мерой;

• *нулевой метод* – метод одновременного или периодического сравнения измеряемой величины с мерой, при которой результирующий эффект воздействия величины на индикатор равновесия доводится до нуля;

• *метод совпадения* – метод одновременного или периодического сравнения, при котором разность между измеряемой величиной и мерой измеряют, используя совпадение отметок шкал или периодических сигналов (например, штангенциркуль, стробоскопический метод измерения частоты вращения механизма);

• *метод замещения* – метод разновременного и периодического сравнения с мерой, в котором измеряемая величина замещается известной величиной, воспроизводимой мерой.

Процесс измерения осуществляется в два этапа. Например, при измерении электрического сопротивления при помощи образцового магазина сопротивлений (регулируемая мера) и моста постоянного тока (электроизмерительный прибор) на первом этапе на вход электроизмерительного прибора подается сигнал x_1 и запоминается значение y_1. На втором этапе сигнал x_1' подается на прибор от регулируемой меры, которая изменяется до тех пор, пока на выходе установится значение y_1. При этом окажется, что $x_1' \sim x_1$.

1.6. Оценка погрешностей измерения

Любое измерение преследует две цели:

1) получить результат измерения, т.е. значение физической величины в виде некоторого числа принятых для этой величины единиц;

2) определить степень достоверности результата измерения.

Результат измерения – случайная величина. Для доказательства достаточно измерить одну и ту же физическую величину с помощью прибора с высокой чувствительностью.

Количественно оценить степень достоверности – значит ввести количественную меру близости между случайным результатом измерения X и неизвестным истинным значением X_u измеряемой величины. Если заданы значения Δ_1 и Δ_2, существенно меньшие, чем X, то интервал $[(X - \Delta_2),(X + \Delta_1)]$ называют доверительным интервалом (рис. 1.6).

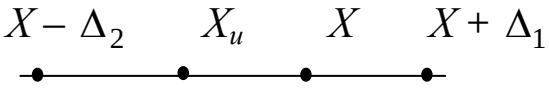


Рис. 1.6. Доверительный интервал измерения

Вероятность того, что доверительный интервал накроет значение X_u измеряемой величины, называют доверительной вероятностью P_g:

$$P_g = P[(X - \Delta_2) \le X_u \le (X + \Delta_1)], \qquad (1)$$

где P – вероятность выполнения соответствующих неравенств.

Исходя из такого представления результата измерения, можно утверждать, что определение достоверности результата измерения – это определение доверительной вероятности P_g при заданных значениях Δ_1, Δ_2, т.е. в результате измерения необходимо получить величины X и P_g при заданных Δ_1, Δ_2.

Ранее было определено правило определения абсолютной погрешности результата измерения:

$$\Delta = X - X_u. \qquad (2)$$

Так как X – случайная величина, то Δ тоже случайная величина.

Тогда, учитывая (1) и (2), можно записать $P_g = P[-\Delta_1 \le \Delta \le \Delta_2]$.

ГОСТ 8.011-72 предусматривает ряд форм представления результата измерения. Одна их них:

$$X, -\Delta_1 \ge \Delta \le \Delta_2, P_g.$$

Например, результат измерения напряжения представлен в виде: $U = 101\,\text{В}$; $1\text{В} \ge \Delta U \le 2\,\text{В}$; $P_g = 0{,}95$.

Это значит, что измеренное значение равно $101\,\text{В}$, погрешность заключена между +1В и -2В с вероятностью 0,95. Тогда можно утверждать, что измеренное напряжение лежит в интервале от 99 до 102 В с вероятностью 0,95.

Погрешность измерения – случайная величина, поэтому для решения вопроса о погрешности пользуются математическим аппаратом теории вероятностей.

Из теории вероятностей известно, что наиболее полной характеристикой случайной величины является её закон распределения, а при оценке погрешностей измерения часто пользуются дифференциальным законом распределения вероятностей [3].

Плотность распределения вероятностей функции $f(\Delta)$ обладает следующими свойствами:

$$f(\Delta) \geq 0, \qquad \int_{-\infty}^{\infty} f(\Delta) d\Delta = 1; \tag{3}$$

$$\int_{-\Delta_1}^{\Delta_2} f(\Delta) d\Delta = \mathrm{P}\left[-\Delta_1 \leq \Delta \leq \Delta_2\right] = P_g. \tag{4}$$

Из выражений (3) и (4) следует, что вероятность появления какого-либо конкретного значения погрешности Δ не может быть отрицательной, а вероятность появления погрешности, заключенной в пределах $-\infty$, ∞, равна единице. Искомая величина P_g может быть определена по выражению (4). Решение обратной задачи (по заданному значению P_g найти Δ_1, Δ_2) возможно лишь, если Δ_1 и Δ_2 связаны между собой определенным образом, например равны.

Другой характеристикой случайной величины Δ [часто этим символом обозначают и случайную величину погрешности и возможное значение, которое может принимать случайная величина (погрешность)] являются так называемые числовые характеристики закона распределения. Наиболее важными из них считаются систематическая погрешность и среднеквадратическое отклонение погрешности. Систематическая погрешность определяется по выражению

$$\Delta_c = \int_{-\infty}^{\infty} \Delta f(\Delta) d\Delta,$$

где $f(\Delta)$ – некоторая функция погрешности;

Δ_c – абсцисса центра тяжести фигуры, заключенной между кривой $f(\Delta)$ и осью Δ (рис. 1.7).

Величину Δ_c принято называть в теории вероятностей математическим ожиданием или средним значением случайной величины Δ, а в метрологии (когда Δ – погрешность) – систематической погрешностью.

Среднеквадратическое отклонение погрешности определяют по выражению

$$\sigma = \sqrt{\int_{-\infty}^{\infty} (\Delta - \Delta_c)^2 f(\Delta) d\Delta},$$

где σ – мера рассеяния (разброса) погрешностей вокруг Δ_c.

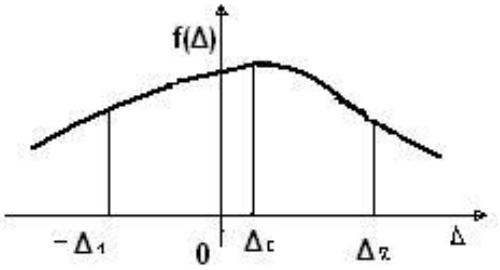


Рис. 1.7. Иллюстрация к понятию систематической погрешности

Видно, что σ – неотрицательная величина. Размерность σ и Δ_c равна размерности погрешности Δ (в этом их удобство).

На практике часто используется так называемый нормальный закон распределения погрешностей, в соответствии с которым функция *f*(Δ) зависит от величины σ согласно выражению (5) (рис. 1.8):

$$f(\Delta) = \frac{1}{\sqrt{2\pi}\sigma} e^{-(\Delta-\Delta_c)^2/(2\sigma^2)}. \qquad (5)$$

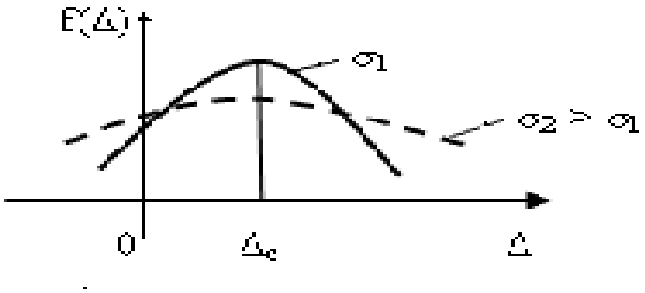


Рис. 1.8. Вид зависимостей *f*(Δ) при разных значениях σ

Зная σ и Δ_c, можно найти $f(\Delta)$, причем, чем больше σ, тем более пологой будет $f(\Delta)$ и тем меньше её максимум.

Для нормального закона распределения погрешностей [3]

$$P_g = \frac{1}{2}[\Phi\left(\frac{\Delta_2 - \Delta_c}{\sigma}\right) + \Phi\left(\frac{\Delta_1 + \Delta_c}{\sigma}\right)],$$

где Φ – вспомогательная функция Лапласа;

$$\Phi(z) = \frac{2}{\sqrt{2\pi}}\int_0^z e^{-t^2/2}dt, \text{ причём } \Phi(-z) = -\Phi(z).$$

В случае если $\Delta_1 = \Delta_2$, а $\Delta_c = 0$,

$$P_g = P[\ |\Delta| \le \Delta_1\ ] = \Phi\ (\Delta_1/\sigma),$$

где $\Phi(z)$ – функция Лапласа (или интеграл вероятностей) – находится по специальным таблицам [3].

2. ЧАСТОТНЫЕ ИЗМЕРЕНИЯ И ИЗМЕРИТЕЛЬНЫЕ СИСТЕМЫ

2.1. Основные свойства частотных измерений

В устройствах контроля и диагностики цифровых устройств практически всегда приходится работать с частотными сигналами того или иного вида. Измерение и контроль частотных сигналов представляют определенную проблему с увеличением частоты и расширением диапазона её изменения. В технике измерения частотных сигналов используются два основных понятия: частота f – количество колебаний в единицу времени и период T – наименьший интервал времени, удовлетворяющий уравнению

$$u(t+iT) = u(t),$$

где i – любое целое число;

$u(t)$ – произвольно выбранное мгновенное значение величины, изменяющейся во времени t.

Соотношение между значениями частоты и периода определяется формулой

$$f = 1/T.$$

Отношение числа периодов n_T периодического сигнала к интервалу времени Δt, за который сосчитано это число, дает среднее (за интервал Δt) значение частоты, называемое средней частотой периодического сигнала (в отличие от частоты):

$$\frac{n_{\text{T}}}{\Delta t} = f_{\text{ср}}.$$

Методы измерения частоты многообразны. В настоящее время наиболее распространен *метод дискретного счета*, на основе которого строят цифровые частотомеры [4]. Этот метод позволяет:

– иметь широкий диапазон измерения одним прибором (от 10 Гц до 32 ГГц);

– гарантировать высокую точность измерения;

– обеспечить возможность обработки результатов наблюдений с помощью микропроцессорных систем;

– относительно просто включать прибор в состав измерительно-вычислительного комплекса;

– строить многофункциональные и многорежимные программируемые приборы, используемые в автоматизированных системах контроля и диагностики ЭВС.

На основе метода дискретного счета получили развитие частотно-временные преобразователи информационных сигналов.

Частотно-временные преобразователи. Причины интенсивного развития частотно-временных преобразователей заключаются в следующем:

1. При передаче информации с различными законами модуляции частотные сигналы обладают наибольшей (наивысшей) помехозащищенностью.

2. В многоканальных измерительных системах коммутация аналоговых сигналов приводит к погрешности из-за переходных процессов, нестабильности, взаимного влияния. Чтобы их ослабить, нужно увеличить уровни сигналов, что усложняет коммутаторы. Коммутация же частотных сигналов может быть осуществлена простым коммутатором без погрешности и потери информации.

3. Частотно-временные преобразования дают возможность получить лучшие метрологические характеристики, так как измерение частоты сводится к счету либо периодов самого сигнала, либо опорной частоты в течение определенного времени – эти операции по простоте и точности превосходят все другие методы аналого-цифрового преобразования.

4. Частотно-временные сигналы – одна из разновидностей цифрового кода (унитарного), т.е. для приема, передачи и преобразования можно использовать обычные элементы и методы цифровой техники. Например, интегрирующее устройство, выполненное на основе счетчика импульсов, имеет передаточную функцию идеального интегратора.

5. Простота преобразования частотно-временного сигнала в код (цифровой эквивалент) и обратно позволяет рационально строить системы преобразования, что облегчает применение микропроцессорных устройств и частотно-цифровых узлов.

Для преобразования сигналов частотно-временных преобразователей в цифровую форму используют частотно-цифровое преобразование двух видов:

а) преобразование циклического действия;

б) преобразование со следящим уравновешиванием.

Частотно-цифровые преобразователи циклического действия реализуют счетные методы измерения двух видов:

– с непосредственным отсчетом частоты – цифровые частотомеры;

– с непосредственным отсчетом периода – цифровые периодомеры.

Принципы измерения частоты и периода. В методе дискретного счета частоты производится прямое сравнение измеряемого значения частоты $f_{\text{х}}$ со значением образцовой частоты $f_{\text{обр}}$, т.е. нужно найти число *n*, показывающее, во сколько раз $f_{\text{х}}$ больше $f_{\text{обр}}$. В этом случае

$$f_{\text{х}} = n\, f_{\text{обр}}.$$

Пусть имеется исследуемая последовательность импульсов с частотой f_x (период T_x) (рис. 2.1). Для измерения нужно выработать частоту f_o с периодом T_o и взять за время измерения отрезок времени, равный периоду образцовой частоты. При этом $f_x / f_o = T_o / T_x = n$, число n покажет, сколько периодов T_x укладывается в интервал T_o.

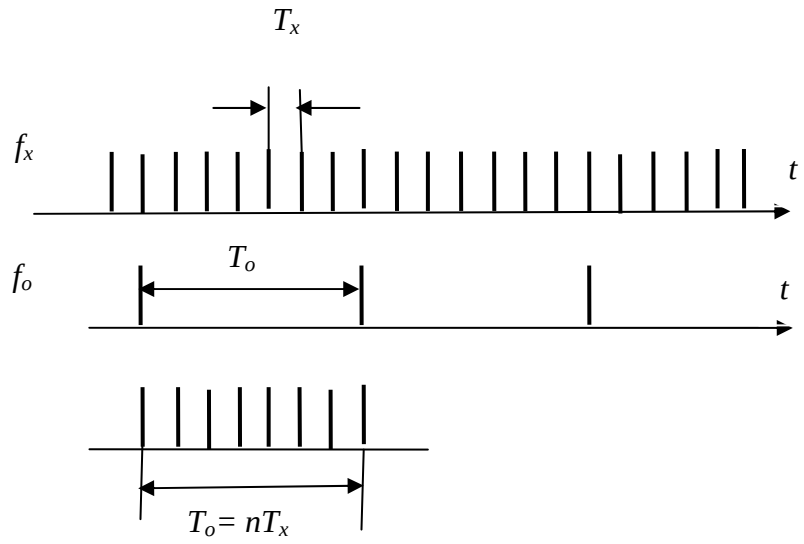


Рис. 2.1. Иллюстрация способа измерения частоты

Алгоритм измерения частоты будет следующим:

1. Сформировать стробирующий импульс – «временные ворота», длительность которых равна периоду сигнала образцовой частоты.

2. Заполнить «временные ворота» импульсами частоты f_x, сосчитать число импульсов n, попавших в ворота.

3. Вычислить отношение $f_x = n/T_o$.

Если, например, нужно измерить частоту непрерывного периодического сигнала (обычно синусоидального), то для измерения следует преобразовать сигнал в периодическую последовательность коротких импульсов, моменты появления которых соответствуют моментам перехода сигнала через нуль с производной одного знака. В этом случае среднее значение частоты за интервал времени, соответствующий двум соседним импульсам, определяется описанным выше способом.

В частотомерах устанавливают время измерения, т. е. длительность «временных ворот»: $T_o = 10^{\,p}$ с, где $p = 0, \pm 1, \pm 2, \ldots$.

Принцип измерения периода поясняется диаграммой (рис. 2.2).

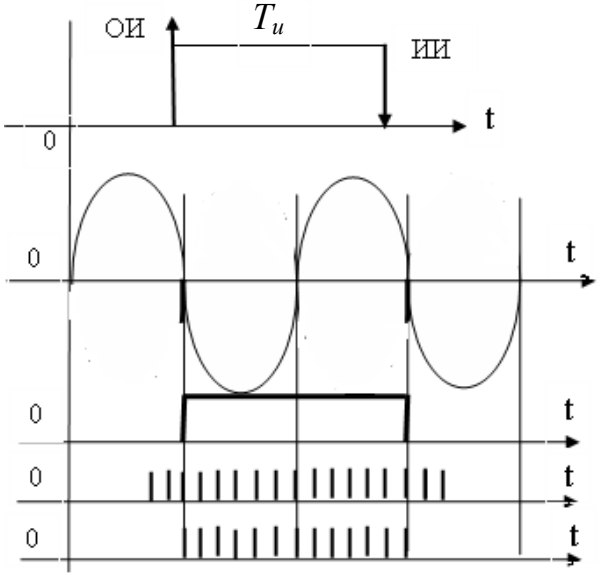


Рис. 2.2. Диаграмма к методу измерения временного промежутка $T_и$ и периода синусоидального сигнала

Измерение периода периодического сигнала – это частный случай общей задачи измерения интервалов времени. Чаще всего измеряемый интервал задается двумя импульсами: опорным и интервальным. Если определяется длительность прямоугольного импульса, то за опорный импульс можно принять фронт, а за интервальный – срез этого импульса.

Для периода периодического сигнала моменты появления опорного и интервального импульсов – это моменты двух соседних переходов сигнала через нулевой уровень с производной одинакового знака.

Сущность метода измерения периода заключается в сравнении измеряемого интервала времени с дискретным интервалом, воспроизводящим единицу времени. Это достигается заполнением измеряемого интервала импульсами с известным (образцовым) периодом.

Число импульсов подсчитывается, и это число будет соответствовать измеряемому интервалу. Импульсы, заполняющие интервал, называют счетными импульсами, они имеют период $T_{сч}$.

Значение измеряемого периода

$$T_{и} = n \cdot T_{сч},$$

где n – число счётных импульсов, уместившихся в промежутке $T_{и}$ (см. рис. 2.2).

Процедура вычисления будет следующая: исследуемый интервал преобразуют в прямоугольный импульс, заполняют его счетными импульсами, подсчитывают число импульсов, уместившихся в измеряемом промежутке.

На основе рассмотренного способа измерения частоты и периода последовательности импульсов можно представить структурную схему измерителя частоты (рис. 2.3).

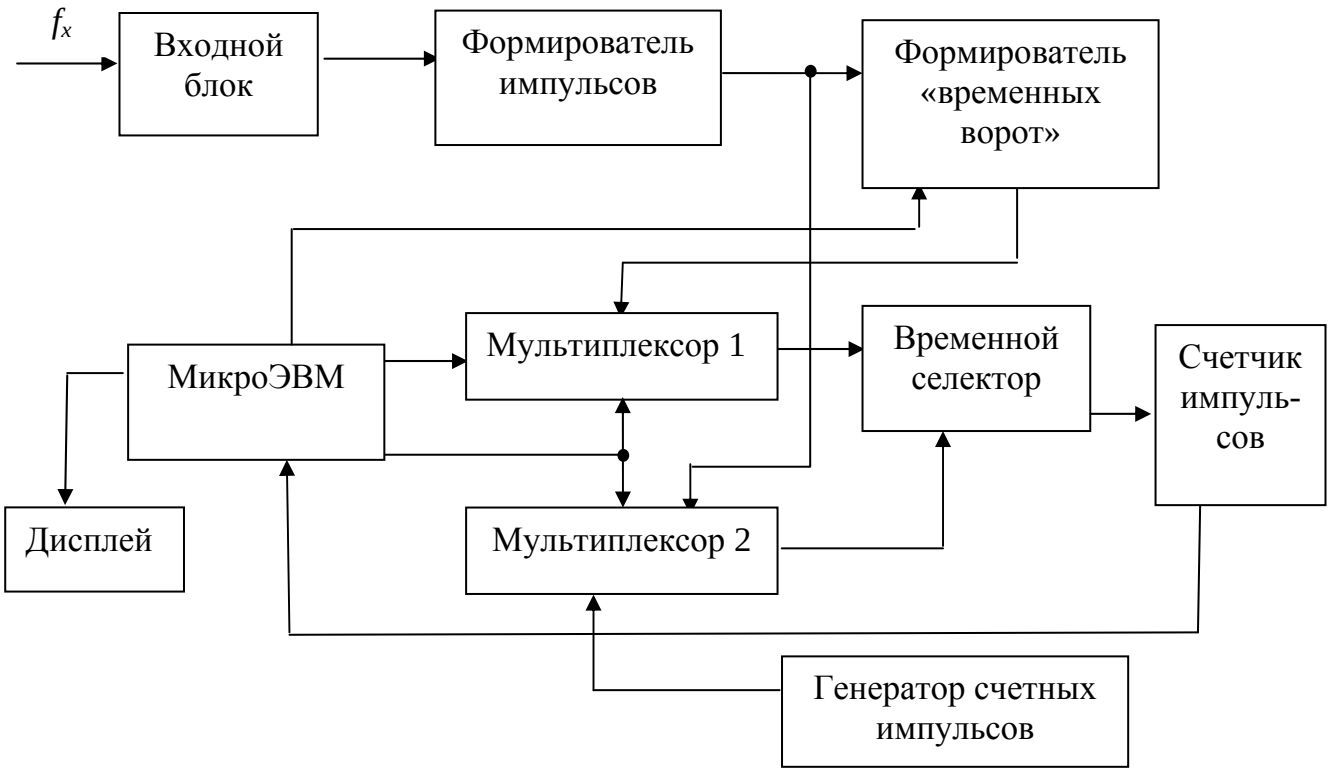


Рис. 2.3. Упрощенная структурная схема измерителя частоты

Счетные импульсы, непрерывно поступающие на один вход временного селектора, могут проходить в счетчик только тогда, когда на втором входе селектора действует прямоугольный (селекторный) импульс, образующий «временные ворота». Он формируется из исследуемого сигнала с помощью специальной схемы (например, триггера Шмитта), содержащейся в блоке формирования импульсов.

Функции формирователя «временных ворот», временного селектора и счетчика импульсов можно реализовать, например, с помощью БИС КР580ВИ53 (КР1810ВИ54), программируя режим ее работы.

В качестве генератора импульсов применяется тактовый генератор микроконтроллера.

Метод дискретного счета успешно используется для измерения не только периода и частоты, но и напряжения, силы тока, параметров цепей. В основу работы многих цифровых средств контроля и измерения положен принцип преобразования измеряемой электрической величины в частоту с ее последующим измерением счетным способом (рис. 2.4).

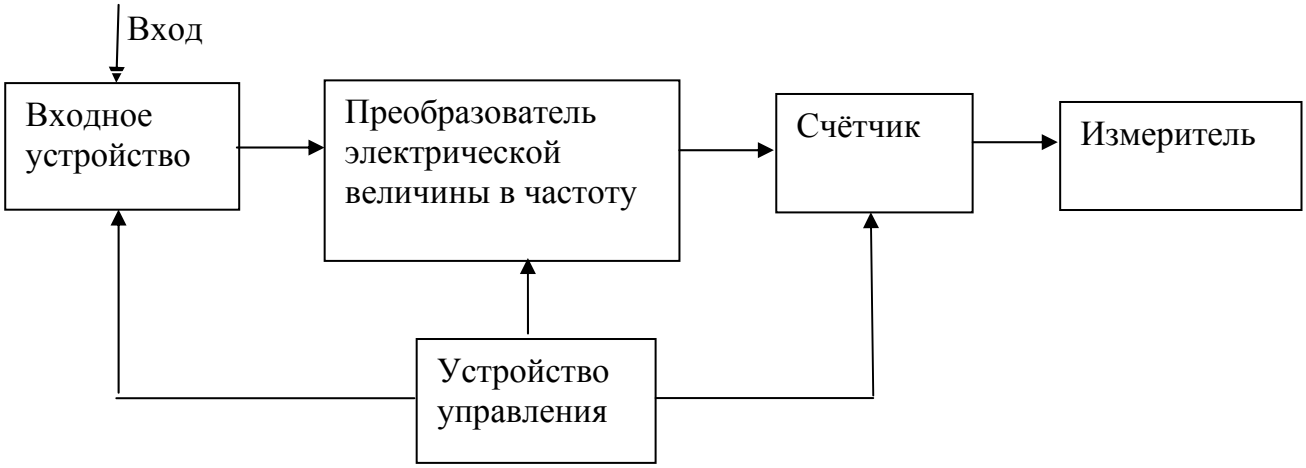


Рис. 2.4. Структурная схема частотно-цифрового преобразователя

Частотомер для измерения частоты можно представить структурной схемой (рис. 2.5).

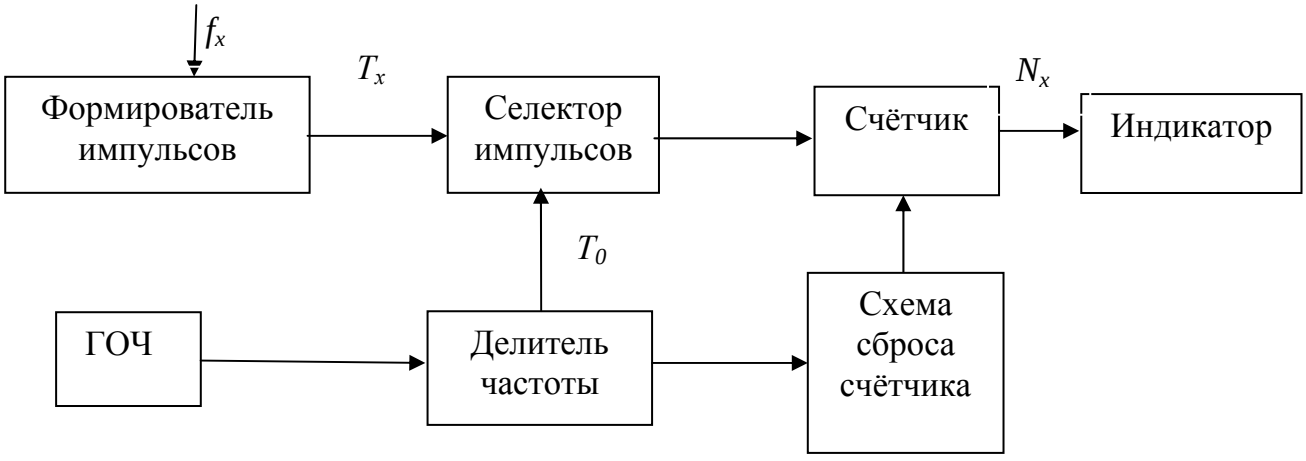


Рис. 2.5. Упрощенная структурная схема частотомера:
ГОЧ – генератор образцовой частоты

Измеряемая частота f_x (период T_x) рассчитывается по выражению

$$f_x = N_x / T_0,$$

где N_x – число импульсов, зафиксированное счётчиком за промежуток времени T_0;

$T_0 = m/f_0$, где m – коэффициент деления частоты f_0 генератора образцовой частоты.

В этом случае $f_x = (f_0 \cdot N_x)/m$.

2.2. Контроль электрических величин и параметров элементов электрической цепи частотными методами

Измерение напряжения. Измерение напряжения U, силы тока J, емкости конденсатора C и сопротивления резистора R сводится к преобразованию этих величин в последовательность импульсов, длительность или частоту которых измеряют частотомером. При измерении постоянного напряжения часто используют преобразователи напряжения в частоту (ПНЧ). Основная идея преобразования напряжения в частоту поясняется диаграммами сигналов (рис. 2.6). На диаграммах показан процесс образования частотного сигнала, характеризующего численное значение измеряемого постоянного напряжения.

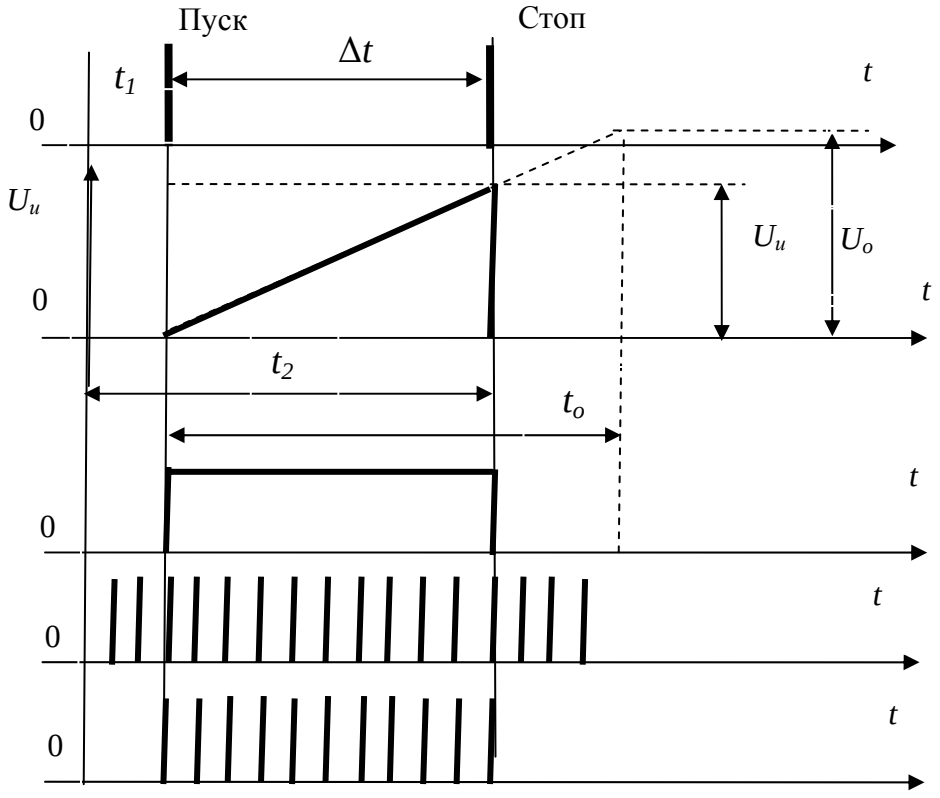


Рис. 2.6. Диаграмма процесса измерения напряжения частотным способом

В момент времени t_1 сбрасываются в нуль показания счетчика цифрового измерителя, запускаются компаратор и генератор линейно изменяющегося напряжения. Измеряемое напряжение U_u, подводимое к одному входу компаратора, сравнивается с линейно изменяющимся (опорным) напряжением U_o, подаваемым на второй вход компаратора от генератора линейно изменяющегося напряжения (ГЛИН). На выходе компаратора формируется прямоугольный импульс длительностью $\Delta t = t_2 - t_1$, формирующий «временные ворота» для пропуска счетных импульсов на счетчик. В этом случае измеренное напряжение будет определяться по показаниям счётчика, запоминающего число калиброванных (счётных) импульсов, попавших во «временные ворота»:

$$U_u = m \cdot v \cdot T_k,$$

где m – число подсчитанных импульсов;

v – скорость нарастания линейного напряжения; $v = U_o / t_o$, где U_o – опорное напряжение генератора ГЛИН, t_o – время нарастания опорного напряжения;

T_k – период счётных импульсов.

При измерении синусоидального напряжения его выпрямляют и измеряют таким же способом.

Подобный способ применяется во многих устройствах. Одно из них – генератор, управляемый напряжением (ГУН) (рис. 2.7).

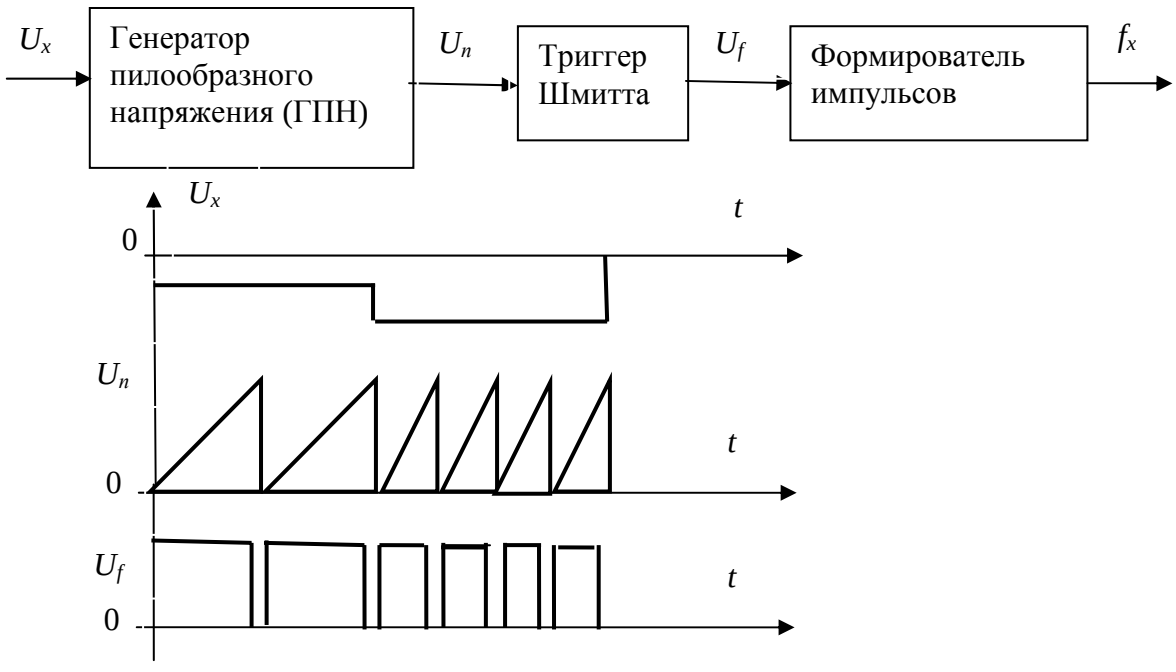


Рис. 2.7. Структурная схема преобразователя напряжения в частоту (ГУН) и диаграммы сигналов в нём

В его состав входят генератор пилообразного напряжения (ГПН), триггер Шмитта и формирователь импульсов. ГПН формирует импульсы, ширина которых зависит от значения измеряемого напряжения, подаваемого на вход ГПН. Триггер Шмитта и формирователь импульсов придают импульсам форму, удобную для дальнейшей обработки и счёта.

Измерение напряжения производится с промежуточным преобразованием.

При аппаратной реализации преобразователей часто используют преобразование с «обратной пилой», т. е. с линейно уменьшающимся опорным напряжением. Принцип получения частотного эквивалента измеряемого напряжения поясняется временной диаграммой (рис. 2.8).

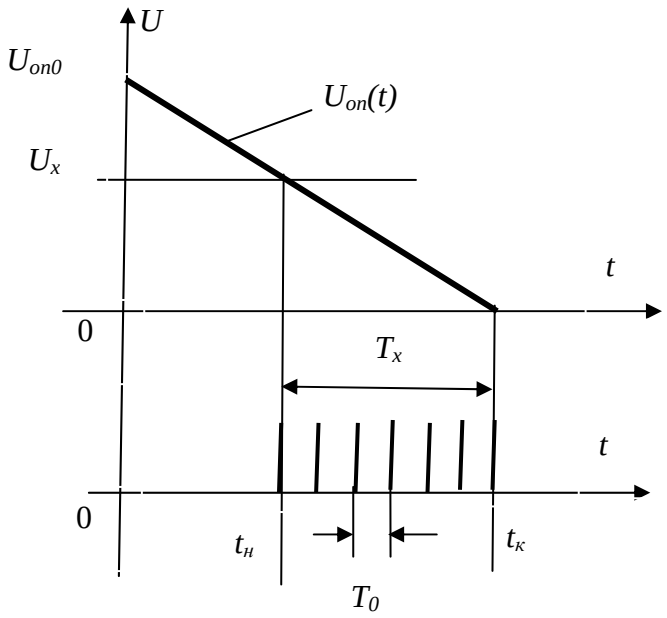


Рис. 2.8. Диаграмма частотного преобразования постоянного напряжения:
$U_{оп0}$ – начальное значение опорного напряжения;
U_x – измеряемое постоянное напряжение;
T_x – фиксируемый отрезок времени;
T_0 – период калиброванных импульсов

Фиксируются два момента: $t_н$ – момент начала, $t_к$ – момент достижения опорным напряжением нулевого значения; $(t_к\text{-}t_н)=T_x$ – промежуток времени, в котором происходит накопление числа импульсов $N_{изм}$ с периодом T_0, т.е. $T_x = N_{изм}\cdot T_0$.

Уравнение прямой, проведенной через две точки в координатах U, t, можно записать в виде $U = U_{оп0}\cdot(1 - t/t_к)$.

В момент начала измерения $U = U_x = U_{оп0}\ (1 - t_н/t_к)$. Для конкретного измерителя известны значения $U_{оп0}$, T_0 и $t_к$, поэтому измеренное значение напряжения U_x будет определено как $U_x = K_п \cdot N_{изм}$, где $K_п$ – постоянная измерительного прибора. Структурная схема такого измерителя показана на рис. 2.9.

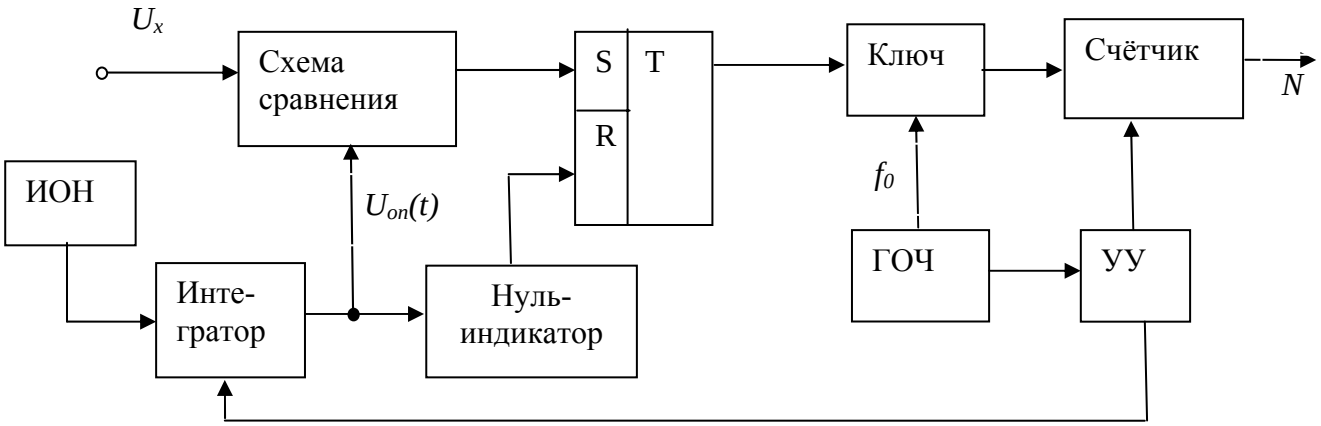


Рис. 2.9. Структурная схема частотного измерителя напряжения:
ИОН – источник опорного напряжения; ГОЧ – генератор образцовой частоты;
УУ – управляющее устройство

На точность работы преобразователя основное влияние оказывают точность задания опорного напряжения и стабильность частоты ГОЧ.

С целью уменьшения требуемой емкости счетчика и уменьшения погрешности от нестабильности образцовой частоты используют схемы с преобразователями напряжения в частоту (ПНЧ) (рис. 2.10).

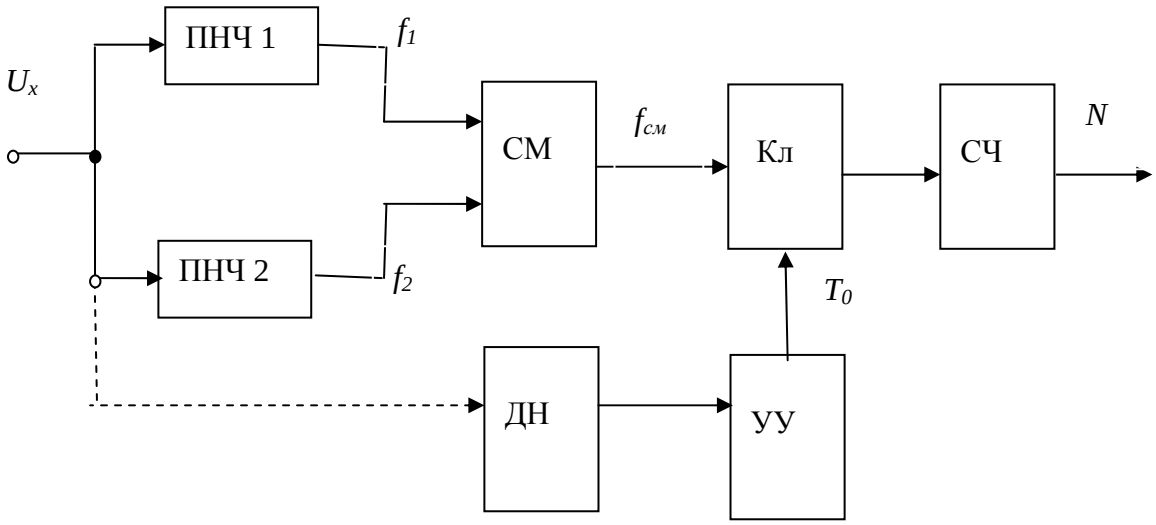


Рис. 2.10. Упрощенная структурная схема измерителя напряжения с ПНЧ:
ПНЧ 1, ПНЧ 2 – преобразователи напряжения в частоту; СМ – смеситель частот;
ДН – детектор нуля; Кл – ключ; УУ – устройство управления;
СЧ – счётчик импульсов

Измеряемая величина U_x подается на входы двух преобразователей частоты в напряжение одновременно.

На выходах ПНЧ образуются частоты $f_1 = f_0 + \Delta f_x$, $f_2 = f_0 - \Delta f_x$. На выходе СМ образуется разностная частота $f_{см} = f_1 - f_2 = 2 \cdot \Delta f_x$, которая затем известным способом преобразуется в число импульсов N.

Если измеряется постоянное напряжение, то УУ работает в режиме выработки образцового периода измерения T_0. Для измерения переменного напряжения необходим детектор нуля, который формирует импульсы в моменты перехода U_x через нулевое значение. УУ в этом режиме формирует образцовый период $T_0 = n \cdot T_x$, где n – число периодов измеряемого напряжения, T_x – период переменного измеряемого напряжения.

Рассмотренные выше способы измерения частоты, периода, постоянного напряжения приборами с цифровым отсчетом применимы также к измерению отношения двух частот, силы тока, емкости конденсаторов и сопротивления резисторов.

Измерение *R, C, L*-параметров. Измерение *R, C, L*-параметров основано на определении постоянной времени разряда *RC*- или *RL*-цепи, один из элементов которой принят за эталон. Постоянная времени процесса определяется как $RC = \tau_1$ либо $\tau_2 = \dfrac{L}{R}$.

Структурная схема измерителя сопротивления R показана на рис. 2.11.

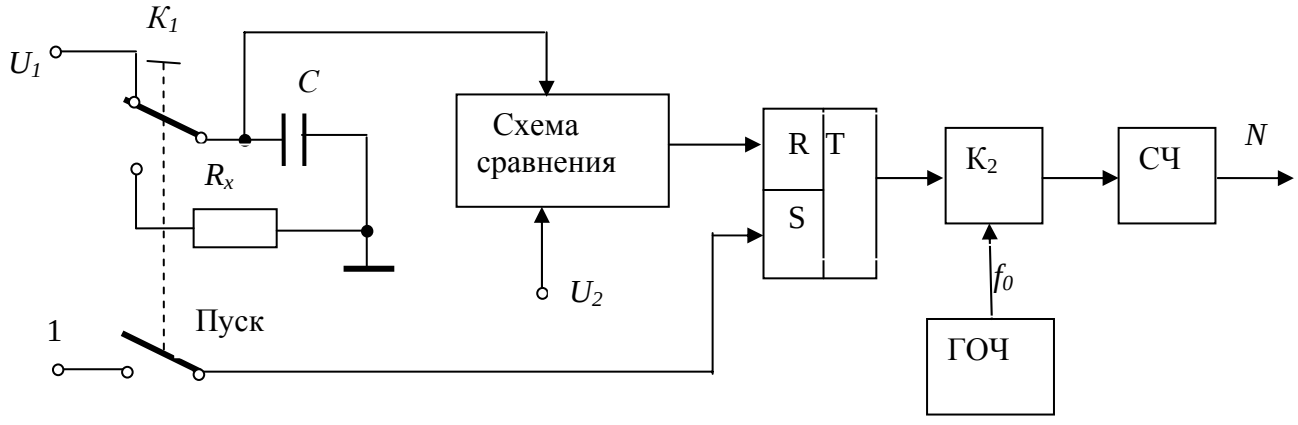


Рис. 2.11. Упрощённая структурная схема измерителя сопротивления резистора: U_1 – напряжение заряда конденсатора; K_1 – пусковой ключ; U_2 – напряжение фиксируемого уровня; K_2 – селектор импульсов, заполняющих измерительный интервал времени, образованный на выходе триггера RST; СЧ – счётчик импульсов, фиксируемых на выходе числом N

В исходном состоянии конденсатор C заряжен до напряжения U_1. В момент t_0 включается ключ K_1 (в нижнее положение на схеме), и конденсатор разряжается на резистор R_x с постоянной времени $\tau = R_x \cdot C$ от начального уровня напряжения U_1 до заданного уровня U_2 (рис. 2.12).

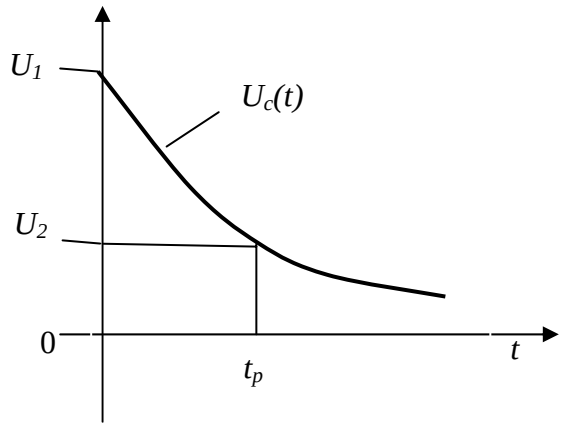


Рис. 2.12. Диаграмма разряда конденсатора

При известных (заданных) значениях напряжений время разряда t_p определяется из уравнения разряда конденсатора $U_2 = U_1 \exp(-t_p/\tau)$, откуда следует $t_p = -\tau \cdot \ln(U_2/U_1)$.

Время разряда t_p фиксируется в момент достижения напряжением $U_c(t)$ значения U_2, задаваемого с большой точностью. Одновременно с началом разряда пускается ключ K_2, и счетчик отсчитывает импульсы, пропускаемые от генератора ГОЧ на вход счетчика. В момент t_p, когда $U_c(t) = U_2$, ключ K_2 закрывается, и код, накопленный в счетчике, будет пропорционален значению R_x. При этом $t_p = N \cdot T_0$, а $R_x = N \cdot T_0 / (C_0 \cdot |\ln U_2/U_1|)$, где $T_0 = 1/f_0$ – период импульсов ГОЧ; C_0 – известная величина ёмкости конденсатора С.

Аналогично можно измерить ёмкость конденсатора, только в этом случае образцовым элементом будет резистор R_0. Тогда

$$C_x = N \cdot T_0 / (R_0 \cdot |\ln U_2/U_1|).$$

Измерение фазовых соотношений. Измерение фазовых соотношений (сдвига фаз между двумя переменными напряжениями или двумя импульсными последовательностями) осуществляется предварительным преобразованием фазовых сдвигов во временной интервал с его последующим измерением с помощью частотно-временного преобразователя (ЧВП).

Сдвиг по фазе Δφ определяется количеством импульсов, попавших в счётчик за время Δ*t*, ограниченное двумя соседними короткими импульсами одной полярности (рис. 2.13):

$$\Delta\varphi = N \cdot T_0 \cdot 2\pi f,$$

где N – число импульсов, фиксируемое счётчиком;

T_0 – период счётных импульсов ГОЧ; $T_0 = 1/f_0$.

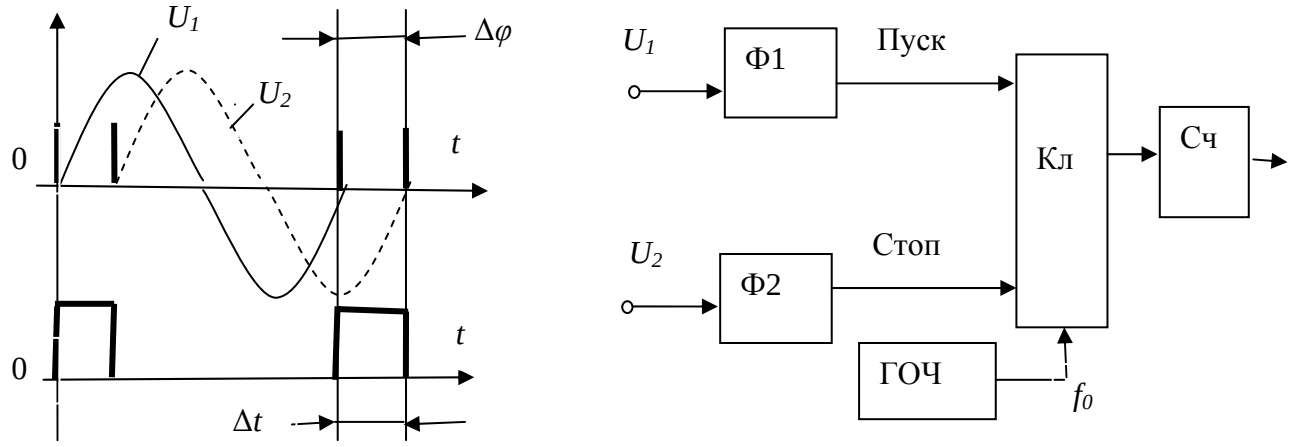


Рис. 2.13. Диаграммы сигналов и упрощенная структурная схема измерителя фазового сдвига между двумя переменными напряжениями:
U_1, U_2 – напряжения одинаковой частоты, имеющие сдвиг по фазе Δφ;
Ф1, Ф2 – формирователи коротких импульсов в моменты переходов сигналов через нулевые значения; ГОЧ – генератор образцовой частоты f_0;
Сч – счётчик импульсов, возникающих на выходе ключевой схемы Кл

Погрешность измерения фазового сдвига Δφ будет зависеть напрямую от частоты самих сигналов.

Второй способ измерения сдвига фаз может быть осуществлен с применением вычислительного устройства (ВУ) (рис. 2.14).

Основная идея состоит в том, что на счетчик непрерывно поступают импульсы частоты f_0 от ГОЧ, а ФИ1 формирует короткие импульсы, которые дают команду ВУ записать число N_2 и сбросить счетчик импульсов ГОЧ, образовавшихся в промежутке между импульсами, соответствующими нулям $U_1(t)$. Импульсы с выхода ФИ2 управляют процессом записи кода счетчика в регистр РГ. В момент возникновения импульса от ФИ2 в счетчике находится число $N_1 \equiv \Delta t_x$, где Δt_x – промежуток времени, соответствующий сдвигу фаз $\Delta\varphi_x$. Таким образом, в вычислитель поступает

два числа: N_2 и N_1. Вычислитель определяет $\frac{N_1}{N_2} \cdot \frac{1}{2\pi} = \Delta\varphi_x$, где N_2 – код счетчика, пропорциональный T_x; N_1 – код счетчика, пропорциональный Δt_x.

Операция деления в ВУ может быть выполнена с помощью PIC-контроллера либо специальными схемами преобразования кода в частоту.

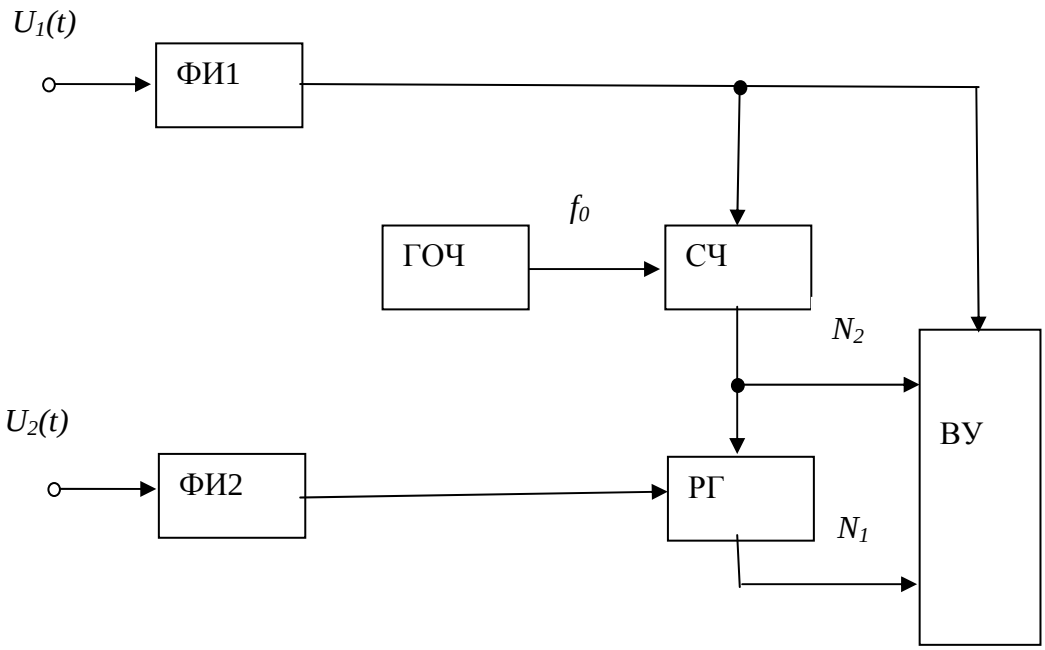


Рис. 2.14. Упрощённая структурная схема измерителя сдвига фаз с вычислительным устройством:
ФИ1, ФИ2 – формирователи импульсов; СЧ – счётчик импульсов; РГ – регистр, фиксирующий код числа поступающих на его входы импульсов; ВУ – вычислительное устройство

Измерение силы тока. Частотное измерение силы тока основано на измерении падения напряжения на образцовом резисторе R_0, по которому протекает измеряемый ток I_x, с последующим преобразованием падения напряжения в частоту. Очень малые по величине токи измеряют с помощью операционных усилителей (ОУ).

Минимальное значение измеряемого с заданной точностью тока I_x определяется соотношением $I_{xmin} = (I_{вх}/\delta)\cdot 100$ %, где δ – заданная точность измерения, %; $I_{вх}$ – входной ток ОУ. На выходе операционного усилителя при подаче на его вход измеряемого тока формируется напряжение, пропорциональное этому току: $U_x = R_{ос}\cdot I_x$ (рис. 2.15).

Используя принцип измерения силы тока, можно измерить значение сопротивления резистора R_x, если применить генератор стабильного тока. В качестве последнего часто используют схему на полевом транзисторе.

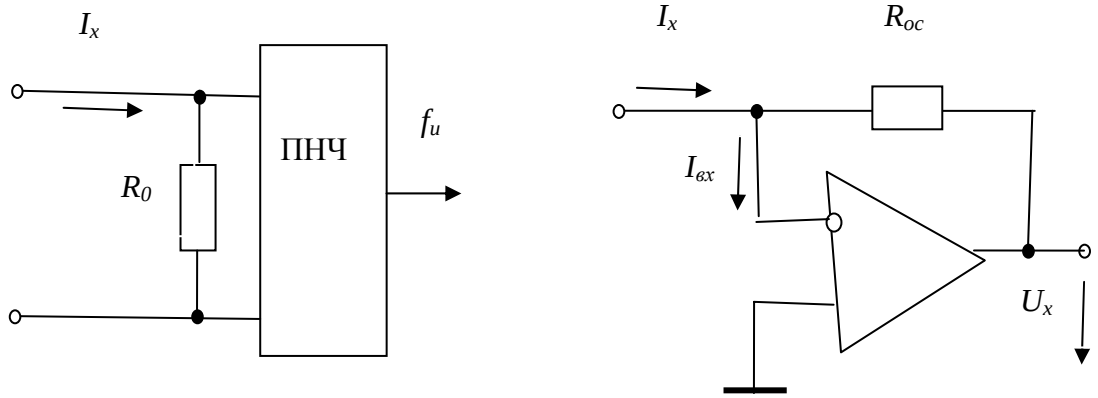


Рис. 2.15. Структурные схемы преобразователей измеряемого тока в частоту и в напряжение (при малых значениях измеряемого тока)

Включив измеряемый резистор на вход операционного усилителя, на его выходе получим напряжение, пропорциональное величине сопротивления этого резистора (рис. 2.16).

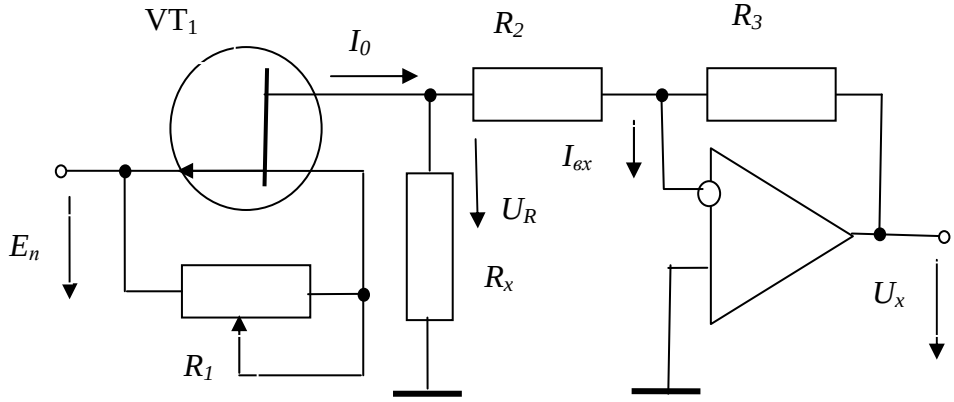


Рис. 2.16. Схема преобразования сопротивления резистора в напряжение

Подстроечный резистор R_1 служит для установки тока I_0, а усиление напряжения происходит на ОУ. На резисторе R_x стабильным током I_0 создаётся падение напряжения $U_R = I_0 \cdot R_x$. На выходе ОУ образуется напряжение, величина которого пропорциональна сопротивлению резистора R_x:

$$U_x = I_0 \cdot R_3 \cdot R_x / R_2.$$

Условия высокой точности измерения:

1) $R_x << R_2, R_3$;

2) $I_0 >> I_{вх}$ (в несколько десятков раз) (рис. 2.16);

3) $U_R \le 0{,}1E_n$, где E_n – напряжение источника питания.

Например, при $I_0 = 1$ мА и $E_n = 10$ В $R_x \le 1000$ Ом.

При использовании полевого транзистора $R_1 = U_{отс}/I_0$, где $U_{отс}$ – напряжение отсечки транзистора VT_1.

Генераторные частотные преобразователи. Широко используются также генераторные схемы, преобразующие значения параметров в частоту. С этой целью применяются схемы автогенераторов, у которых генерируемая частота напрямую зависит от измеряемых параметров. Использование таких преобразователей при построении датчиков позволяет организовать связь между датчиком и удаленным вычислительным терминалом по частотным каналам. Например, в качестве преобразователя можно использовать мультивибратор, собранный на основе операционного усилителя (рис. 2.17).

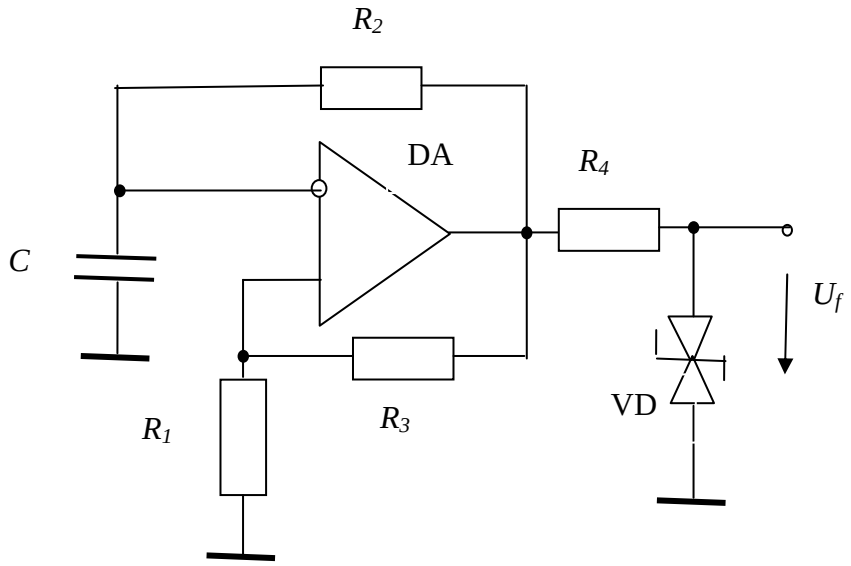


Рис. 2.17. Схема мультивибратора – преобразователя параметров конденсатора и резисторов в частоту выходного сигнала

Включая на место C или R_2 измеряемые элементы, получим преобразователь *(C – f)* либо *(R – f)*. При этом период выходных колебаний

$$T = 2C_1 \cdot R_2 \cdot \ln (1 + 2R_1/R_3).$$

Так как колебания на выходе ОУ двухполярные, то необходимо устанавливать дополнительно двухсторонний диодный ограничитель амплитуды (резистор R_4 и диодная пара VD) (см. рис. 2.17).

2.3. Информационно-измерительные системы

Измерительные системы (ИС) – это совокупность средств измерений и вспомогательных устройств, соединенных между собой каналами связи. При большом объеме получаемой информации множество измерительных приборов может оказаться бесполезным из-за физиолого-психологических ограничений наблюдателя либо при необходимости математической обработки ряда предварительных данных. В этих случаях используют измерительные системы.

Измерительные системы предназначены для автоматического получения измерительной информации от ряда источников и её передачи, обработки и представления в той или иной форме. Если *ИС* обслуживает объект, находящийся от нее на значительном расстоянии, ее называют *телеизмерительной*. В подобных системах информация передается либо по проводам, либо по радиоканалам.

Измерительная система, в которой предусмотрена возможность представления информации оператору, называют информационно-измерительной (ГОСТ 8.437-81) или измерительной информационной. Система, снабженная ЭВМ, называется измерительно-вычислительным комплексом (ИВК).

Информационно-измерительные системы используются в тех случаях, когда в системе требуется организация большого массива измерений различных физических величин. Например, турбогенератор мощностью 1200 Мвт при испытаниях контролируется с помощью 1500 первичных измерительных преобразователей. На Саяно-Шушенской ГЭС контроль за состоянием сооружений и работой агрегатов осуществлялся посредством 3000 первичных измерительных преобразователей. В этих условиях невозможно оператору отслеживать показания непосредственно. Кроме того, если преобразователей немного, но процессы – быстропротекающие, оперативный контроль тоже практически невозможен.

Для сбора, обработки и представления информации оператору в удобной форме используются специальные виды средств измерений – измерительно-информационные системы (ИИС) [1].

ИИС подразделяются:

1) на системы сбора измерительной информации, их называют измерительными системами;

2) системы автоматического контроля, предназначенные для контроля за работой разного рода машин, агрегатов или технологических процессов;

3) системы технической диагностики, служащие для выявления технической неисправности различных изделий;

4) телеизмерительные системы, предназначенные для сбора измерительной информации с удаленных на большие расстояния объектов.

Важной разновидностью ИИС являются измерительно-вычислительные комплексы. Так же как и ИИС, ИВК представляют собой автоматизированные средства измерения и обработки измерительной информации, предназначенные для применения на сложных объектах. Их отличительная черта – наличие в системе свободно программируемой ЭВМ, используемой не только для обработки результатов измерения, но и для управления самим процессом измерения, а также для диагностики и управления воздействиями на объект.

Современные ИИС строятся на основе агрегатного принципа, т.е. на основе выпускаемых функциональных узлов, объединенных общим алгоритмом функционирования. Унифицированные функциональные узлы (блоки и модули), предназначенные для построения ИИС, образуют агрегатные комплексы Государственной системы промышленных приборов и средств автоматизации (ГСП). В СССР к 1985 году было создано около 20 агрегатных комплексов (АСЭТ, АСВТ, АСКР и др.).

Изделия, входящие в агрегатный комплекс, должны легко сопрягаться друг с другом без дополнительных устройств, т. е. обладать так называемой совместимостью. Различают шесть видов совместимости:

1. Энергетическая совместимость по трём видам используемой энергии: электрической, пневматической, гидравлической.

2. Функциональная. Изделия должны быть взаимоувязаны для совместной работы.

3. Метрологическая, т.е. должна быть обеспечена сопоставимость метрологических характеристик в измерительном тракте, составленном из нескольких приборов.

4. Конструктивная. Должны быть обеспечены единая форма и стиль конструктива и механических соединений.

5. Эксплуатационная. Должны быть сопоставимы характеристики надёжности, стабильности, степени влияния внешних факторов.

6. Информационная. Должна быть обеспечена согласованность входных и выходных сигналов по виду, диапазону изменения, порядку обмена сигналами между узлами и внешней средой.

Информационная совместимость достигается унификацией измерительных сигналов, применением стандартных интерфейсов. Например, для измерительных преобразователей с токовым выходом стандарт ГСП нормирует диапазон изменения выходного тока от 0 до 5 мА или от 4 до 20 мА, а для преобразователей с выходом по напряжению – от 0 до 10 В.

Понятие «интерфейс» охватывает электрические, логические и конструктивные условия, устанавливающие требования к соединяемым функциональным узлам и связям между ними.

Электрические условия определяют требования к параметрам сигналов взаимодействия и способу их передачи, а логические условия – номенклатуру сигналов, пространственные и временные соотношения между ними.

Конструктивные условия устанавливают конкретные требования к элементам интерфейса: вид разъема, его месторасположение, порядок распайки контактов (цоколевка) и т.д.

Для ИИС и ИВК были распространены (1985 г.) интерфейс КАМАК (CAMAC – Computer Application for Measurement Automation and Control) и приборный интерфейс, рекомендованный МЭК. Изделия агрегатных комплексов позволяют строить ИИС методом проектной компоновки, что сокращает сроки создания систем.

Основные структуры ИИС. Один из признаков классификации структур – способ обмена сигналами взаимодействия (согласованное преобразование информации всеми функциональными узлами системы).

Структура ИИС зависит от способа управления – децентрализованного или централизованного, а также определяется способом соединения узлов между собой и с управляющим устройством. Различают три основных вида соединений: цепочечное, радиальное, магистральное соединение (рис. 2.18 – 2.20).

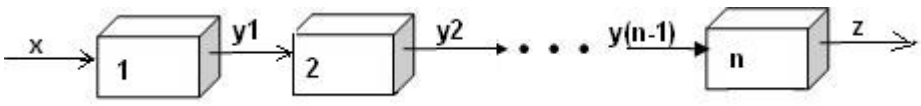


Рис. 2.18. Цепочечное соединение функциональных узлов в системе

Могут быть комбинации рассмотренных структур: радиально-цепочечные, радиально-магистральные.

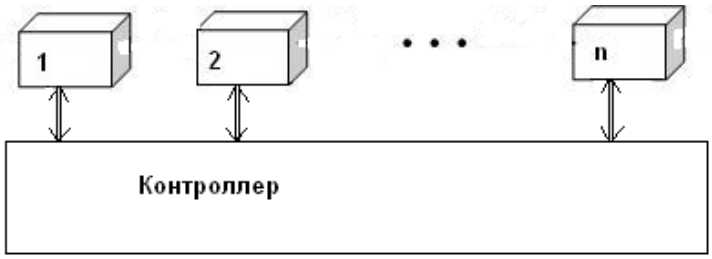


Рис. 2.19. Радиальная структура системы контроля и управления

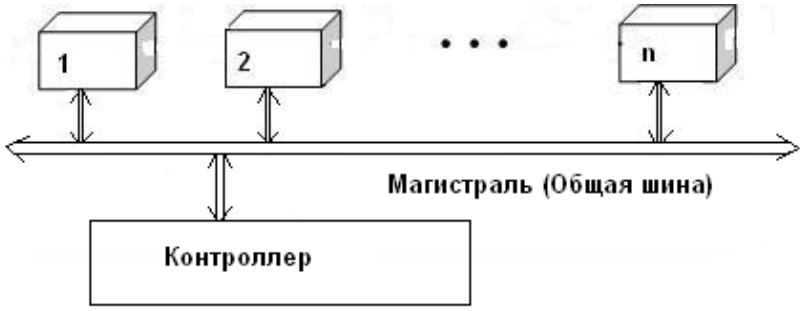


Рис. 2.20. Магистральная структура системы контроля и управления

В схеме обобщенной структуры ИИС (рис. 2.21) обозначено:

1 – средства измерения и преобразования информации;

2 – средства обработки и хранения информации;

3 – средства отображения, индикации или регистрации информации;

4 – устройство управления потоками информации;

5 – устройство формирования управляющих воздействий;

6 – исполнительные устройства;

7 – управляемый объект;

8 – первичные измерительные преобразователи.

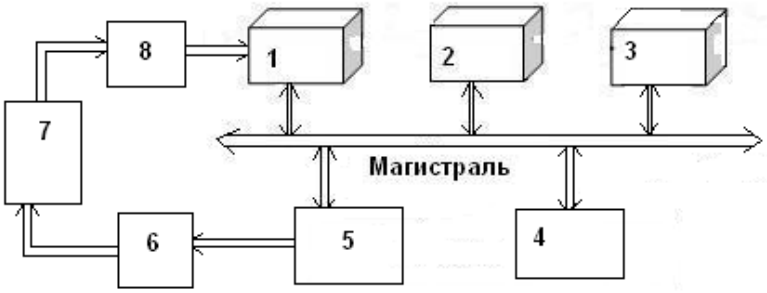


Рис. 2.21. Обобщённая структура ИИС

Информация о состоянии объекта 7 с помощью первичных измерительных преобразователей 8 попадает в средства измерения и преобразования 1, где выходные сигналы первичных преобразователей подвергаются таким операциям, как: фильтрация, масштабирование, линеаризация, аналого-цифровое преобразование.

Затем сигналы в цифровой форме передаются через магистраль на цифровые средства обработки и хранения информации для обработки по определенным программам или накопления, а также на средства отображения информации (СОИ) для индикации и регистрации.

Устройство формирования управляющих воздействий 5 через исполнительные устройства 6 воздействует на объект 7 для регулирования, контроля, тестирования и т.п.

В качестве средства измерения и преобразования информации в ИИС применяются различные устройства: специализированные вычислительные устройства, микропроцессоры, универсальные ЭВМ. В последнем случае на ЭВМ возлагаются и функции устройства управления.

Основные виды преобразования измерительных сигналов в ИИС. К таковым относятся:

– дискретизация;
– коммутация;
– фильтрация;
– масштабирование;
– линеаризация;
– выборка и хранение аналоговой информации;
– аналого-цифровое преобразование.

Дискретизация – это способ преобразования непрерывной функции, заключающийся в замене зависимости вида $X(t)$, характеризующей функцию (или процесс), некоторой дискретной во времени последовательностью чисел X_1, X_2, $\ldots X_n$ (результатов измерений), отражающих значения $X(t)$ в фиксированные моменты времени t_1, t_2, $\ldots$ t_n (рис. 2.22). Последовательность чисел должна быть такой, чтобы по ней можно было восстановить исходный процесс с заданной погрешностью.

Дискретизация может быть основана на измерении значений *X(T)* различными способами:

1) в заранее назначенные моменты времени, например через равные промежутки времени (циклическая дискретизация);

2) в моменты времени, которые определяются развитием процесса *X(T)* (спорадическая и адаптивная дискретизация);

3) в случайные моменты времени, не связанные с ходом процесса, например по вызову оператора.

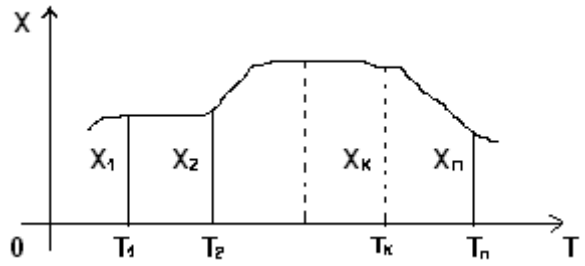


Рис. 2.22. Дискретизация функции

Наиболее просто реализуется циклическая дискретизация. При её использовании возникает задача выбора периода (частоты) дискретизации. Применительно к каналам связи эта задача была впервые решена В.А. Котельниковым в 1933 г. путем доказательств следующих теорем:

Теорема 1. Любую функцию $U(t)$, состоящую из сигналов с частотой от нуля до некоторого предельного значения частоты $f(n)$, можно представить в виде

$$U(t)=\sum_{k=-\infty}^{\infty}U(k\Delta t)\frac{\sin\omega_{\text{n}}\left[t-k/(2f_n)\right]}{\omega_{\text{n}}\left[t-k/(2f_n)\right]}, \qquad (1)$$

где k – целое число;

$\omega_{\text{n}}=2\pi f_n$;

$U(k\Delta t)$ – мгновенные значения функции $U(t_k)$ в момент отсчета, т.е. через промежуток времени Δt.

Любая функция, представленная формулой (1), содержит лишь сигналы с частотой от нуля до f_n.

Теорема 2. Любую функцию $F(t)$, состоящую из частот от нуля до f_n, можно передать с любой точностью при помощи чисел, следующих друг за другом через равные промежутки времени:

$$\Delta t=1/(2f_n).$$

В теоремах речь идет о непрерывной функции с ограниченным спектром, т.е. о функции, неограниченной во времени.

Теоремы В.А. Котельникова дают возможность определить оптимальный способ восстановления аналогового сигнала на приёмном конце линии связи.

В качестве восстанавливающих функций $Z(t)$ обычно выбирают простые функции, например степенные полиномы (методы Лагранжа, Ньютона). Критерием точности восстановления часто служат следующие условия:

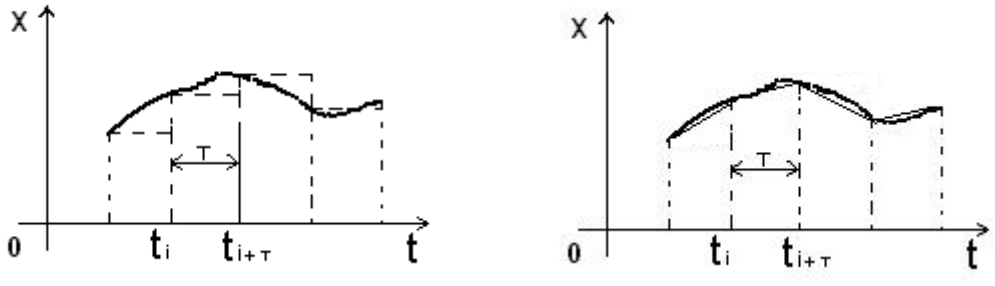
1) Условие совпадения восстанавливающей функции $Z(t)$ с исходным процессом *X(t)* в узлах интерполяции (в моменты отсчетов):

$$X(t_i) - Z(t_i) = 0;\ i = 1, 2 \ldots.$$

2) Условие минимума среднеквадратической ошибки приближения:

$$\min \int_0^T \left| X(t) - Z(t) \right|^2 dt.$$

Вид восстанавливающих функций зависит от конкретных условий (может быть ступенчатая, линейная, параболическая). Если критично время преобразования, например при формировании управляющих сигналов, применяется ступенчатая интерполяция. В других случаях возможна линейная или параболическая интерполяция. Виды интерполяции можно представить графически (рис. 2.23).



а *б*

Рис. 2.23. Виды интерполяции: *а* – ступенчатая; *б* – линейная

Значение периода дискретизации зависит от максимально допустимой погрешности восстановления $|\Delta|_{\max}$ исходного процесса и вида исходной и восстанавливающей функций. Например, если функция $X(t)$ дважды дифференцируема и известны максимальные значе-

ния её первой и второй производных $\left[X'(t)_{\max},\ X''(t)_{\max}\right]$, то для ступенчатой интерполяции можно определить период дискретизации:

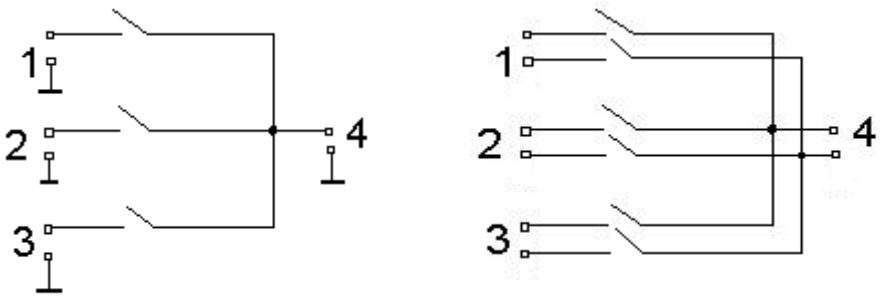
$$T_{cm} \le |\Delta|_{\max} / |X'(t)|_{\max},$$

а для линейной интерполяции

$$T_{\min} \le \sqrt{8|\Delta|_{\max} / |X''(t)|_{\max}}.$$

Если процесс $X(t)$ представлен случайной функцией, то период дискретизации выбирается по заданному значению $|\Delta|_{\max}$ и виду функции $X(t)$ (автокорреляционный метод).

Коммутация – процесс, при котором источники измерительной информации в определенной последовательности подключаются ко входу измерительного канала (рис. 2.24).



а *б*

Рис. 2.24. Примеры ключей для коммутации измерительных сигналов:
а – система однополюсных ключей; *б* – система двухполюсных ключей; 1, 2, 3 – входы ключей; 4 – выход

Основной элемент коммутатора – ключ (он может быть электромеханическим или полупроводниковым). В качестве электромеханического ключа часто используют герконы. Время срабатывания геркона ≈ 1мс, он может выполнить до 10^8 срабатываний, имеет в замкнутом состоянии сопротивление – сотые доли Ома, в разомкнутом – 10^8 Ом. Применяется геркон для коммутации очень малых напряжений (несколько микровольт).

Там, где требуется быстродействие около 1мкс, применяют полупроводниковые ключи на основе МОП-структур. Недостаток таких ключей – заметное сопротивление в замкнутом состоя-

нии (100–200 Ом) и малое (относительно геркона) значение максимально допустимого напряжения (≈10 В) на выводах разомкнутого ключа (серия ключей К590КН1-14).

Фильтрация сигналов предназначена для отделения полезного сигнала от помех. Сигналы от датчиков часто имеют низкие уровни (особенно от термопар, тензодатчиков) – несколько милливольт, причем уровень помех обычно высок.

Спектр полезного сигнала многих датчиков лежит в диапазоне частот от 0 до 1Гц, а среди помех наиболее заметны наводки промышленных частот 50 Гц. Выделение полезного сигнала (фильтрация) осуществляется с помощью устройств, называемых фильтрами. Простейшие фильтры могут быть типа RC, RL, RLC, пассивные (рис. 2.25) и активные (активные выполняются на базе ОУ).

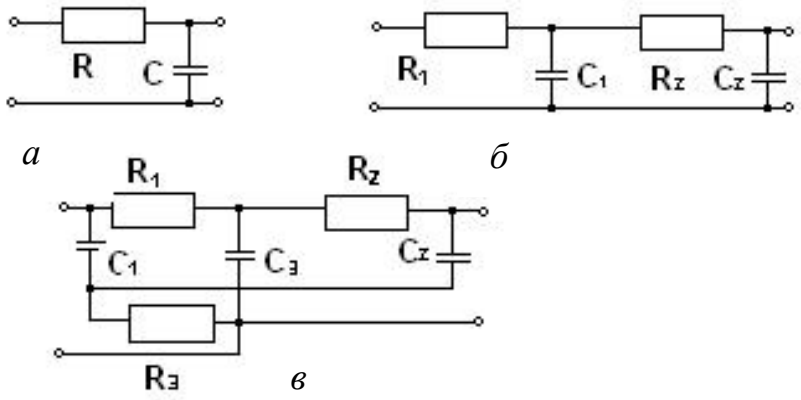


Рис. 2.25. Пассивные RC-фильтры:
а – однозвенный; *б* – двухзвенный; *в* – полосовой

В радиотехнике широко используются пьезокерамические фильтры для формирования АЧХ тракта промежуточной частоты в супергетеродинных полупроводниковых приемниках частотно-модулирован-ных сигналов. В сочетании с интегральными схемами они позволяют создавать радиоприемные устройства с хорошими параметрами,
например фильтр ФП1П8-3 (Радио. № 5. 1984 г. С. 60).

Для полосового фильтра (см. рис. 2.25, *в*) обычно выбирают:

$$R_1 = R_2 = R; \quad R_3 = 0{,}5R; \quad C_1 = C_2 = C; \quad C_3 = 2C.$$

В этом случае центральная частота фильтра $\omega_0 = 1/RC$.

Активные фильтры позволяют улучшить фильтрующие свойства и получать фильтры с лучшими характеристиками на основе пассивных RC-цепей.

Масштабирование – операция, с помощью которой входной сигнал приводится к определенному (нормированному) диапазону измерений. В процессе масштабирования входной сигнал умножается на постоянное число (масштабирующий коэффициент K). Как правило, это делитель напряжения или ОУ, охваченный обратными связями. В делителях напряжения резисторы R_2, R_3 делаются проволочными из манганина, имеющего стабильное сопротивление (рис. 2.26).

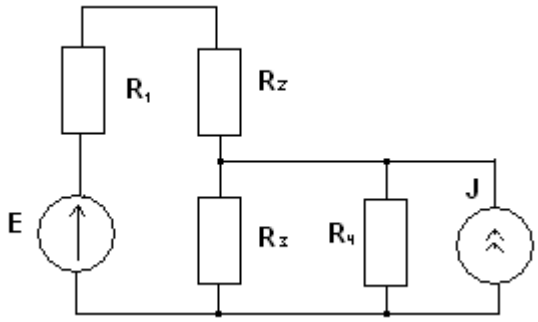


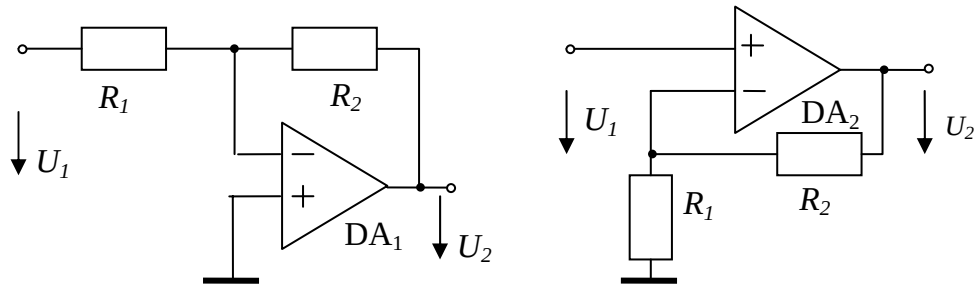
Рис. 2.26. Масштабирующий делитель напряжения в измерительном канале

Входное сопротивление делителя должно быть высоким, выходное – минимальным, чтобы уменьшить методическую погрешность от внутреннего сопротивления R_1 источника сигнала и ослабления действия на сигнал входного сопротивления приемника R_4. Если входная цепь приемника сигнала содержит активные элементы (транзисторы и ОУ), то требуется, чтобы входной ток приемника J не создавал на выходном сопротивлении делителя R_3 заметного падения напряжения, которое представляет собой аддитивную (по отношению к входному сигналу) погрешность.

В масштабных преобразователях на основе ОУ (рис. 2.27) масштабные коэффициенты определяются следующим образом:

– для инвертирующего преобразователя $K_u = U_2/U_1 = R_2/R_1$;

– для неинвертирующего – $K_{ни} = 1 + R_2/R_1 = U_2/U_1$.



а *б*

Рис. 2.27. Масштабные преобразователи на основе ОУ:
а – инвертирующий; *б* – неинвертирующий

Линеаризация – это преобразование сигнала для получения линейной зависимости между выходным сигналом измерительного канала и значением измеряемой величины. Линеаризация требуется, когда измерительный преобразователь обладает нелинейной функцией преобразования (например, термоэлектрические преобразователи), а по технологическим требованиям нужен сигнал, пропорциональный значению измеряемой величины.

Линеаризация предполагает, что в составе измерительного канала имеется измерительный преобразователь, обладающий обратной функцией преобразования. Процесс линеаризации можно осуществлять либо в аналоговой, либо в цифровой форме.

В аналоговом виде линеаризацию осуществляют, используя нелинейный элемент с функцией F^{-1}, в цифровом – с помощью функционального аналого-цифрового преобразования (ФАЦП). В результате измеряемая величина X преобразуется в пропорциональное значение кода $N = X / q$, где q – шаг квантования величины X (рис. 2.28).

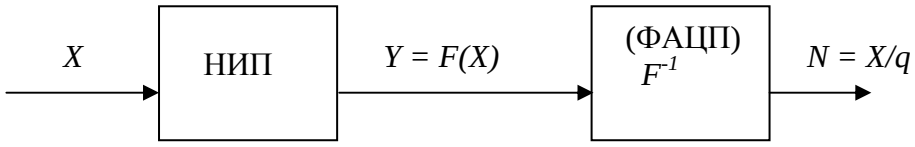


Рис. 2.28. Линеаризация нелинейного измерительного преобразователя

Выборка и хранение аналоговой измерительной информации. При контроле быстропротекающих процессов аналоговую информацию в виде напряжения можно хранить несколько миллисекунд с помощью схемы УВХ (рис. 2.29).

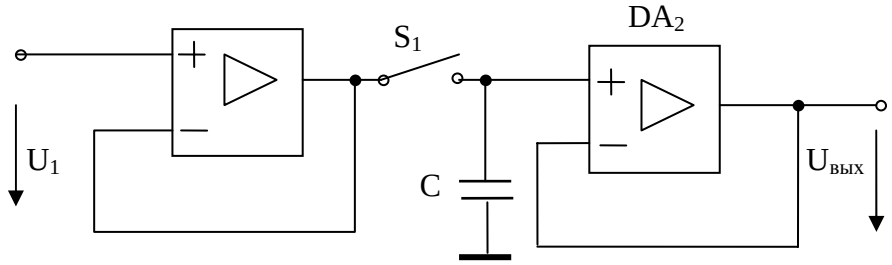


Рис. 2.29. Структурная схема УВХ аналоговой информации

В современных системах используют АЦП и ЗУ, управляемые микроконтроллерами.

Аналого-цифровое преобразование (АЦП) позволяет использовать всю мощь вычислительной техники для обработки измерительной информации в реальном масштабе времени. В ИИС наиболее часто используют АЦП интегрирующего и число-импульсного преобразования.

Доказано, что приемник интегрирующего типа является оптимальным приемником сигналов постоянного напряжения с точки зрения помехоустойчивости. Наиболее часто применяются АЦП двукратного интегрирования.

3. ОБЩИЕ ВОПРОСЫ КОНТРОЛЯ ФУНКЦИОНИРОВАНИЯ И ДИАГНОСТИКИ ЭЛЕКТРОННЫХ СРЕДСТВ

3.1. Уровни и характеристики системы автоматического контроля ЭВМ

Так как ЭВМ – это преобразователь информации, то любые выполняемые ею операции можно разделить на три класса: передача информации, логические преобразования, арифметические преобразования [6].

Передача информации: кодовое (машинное) слово передается в пространстве (из одного места в другое) или во времени (запоминание и хранение слов в ЗУ). Передача информации в пространстве и хранение должны быть выполнены так, чтобы входное слово, поступающее на вход устройства или схемы, совпадало с выходящим словом, фиксируемым на выходе.

Логическое преобразование состоит в формировании по некоторым правилам из K входных слов длиной n одного выходного слова той же длины. При этом двоичный символ в i-м разряде выходного слова зависит только от значений символов в i-х разрядах и не зависит от значений символов в других разрядах входных слов. Чаще всего $K = 2$ или $K = 1$ [операции И, ИЛИ, НЕ (инверсия)].

Арифметические преобразования (операции): из двух входных слов, задающих числовые операнды, вырабатывается регулирующее выходное слово, причем значение двоичного символа в i-м разряде выходного слова зависит от значений символов как в i-м, так и в других разрядах входных слов.

Таким образом, для построения системы автоматического контроля (САК) нужно иметь схемы контроля правильности передачи (и хранения) информации, контроля правильности логических и арифметических преобразований. Чаще всего в САК включают и средства автоматической коррекции обнаруживаемых ошибок.

В основе системы контроля функционирования ЭВМ лежит *принцип избыточности*, предполагающий использование какого-либо вида избыточности (временной, информационной, аппаратурной, алгоритмической).

Временная избыточность – это применение дополнительных затрат времени на выполнение контрольных операций (например, использование двойного счета задачи).

Информационная избыточность – представление команд и данных в ЭВМ кодами с дополнительными разрядами, используемыми в процедурах контроля и коррекции ошибок.

Аппаратурная избыточность – применение дополнительной аппаратуры для реализации контроля и коррекции ошибок (например, два арифметико-логических устройства (АЛУ), работающих параллельно со сравнением результатов).

Алгоритмическая избыточность – решение задачи по разным алгоритмам (программам) с проверкой результатов на совпадение.

Чаще всего используется комбинация последних двух видов избыточности. Использование САК порождает проблему контроля правильности работы самих САК. Решение этой проблемы – самоконтроль.

Основными характеристиками САК являются:

– доля оборудования ЭВМ, охваченного этой системой;

– степень детализации, с которой САК указывает место возникновения ошибки (детальное распознавание места неисправности – задача системы САД);

– отношение объема оборудования САК к общему оборудованию ЭВМ;

– время реакции САК на ошибку.

Классификация средств контроля. Различают следующие уровни представления ЭВМ [10]: логический (Л), функциональный (Ф), системный (С), пользовательский (П) (рис. 3.1). Каждому уровню соответствуют средства контроля, условно показанные в виде незамкнутых колец. Замкнутость кольца определяется вероятностью обнаружения ошибок средствами контроля соответствующего уровня. Часть ошибок может проникать на следующий уровень и попасть в результат вычисления.

На *логическом* уровне используются различные виды специальных кодов: коды с проверкой на четность/нечетность, корректирующие коды Хэмминга, циклические коды (например, код Грэя), остаточные и арифметические коды, контроль дублированием со сравнением результатов и др. На логическом уровне обнаружение ошибок производится непрерывно, поэтому можно совмещать выполнение основных

и контрольных операций во времени (с помощью быстродействующих аппаратных средств), что мало влияет на снижение быстродействия машины в целом.

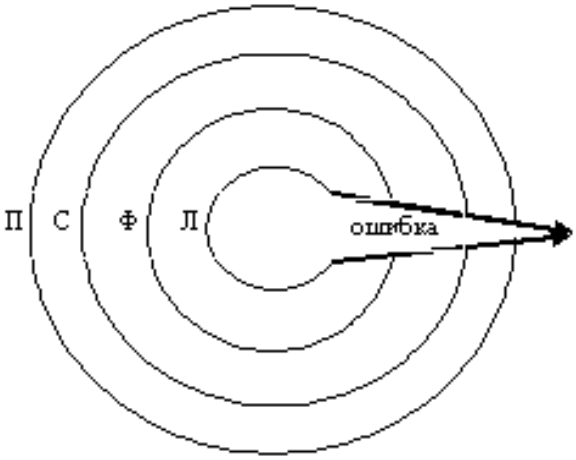


Рис. 3.1. Условное изображение уровней представления средств контроля

На *функциональном* уровне используются:

- контроль с помощью таймеров простоя;
- периодическое тестирование;
- контроль корректности протоколов обмена.

Контроль с помощью таймеров простоя, в котором применяются охранные таймеры (watchdog timers), – наиболее простой способ. Охранный таймер работает следующим образом: при нормальной работе процессор периодически (через время тайм-аута) запускает внешний по отношению к нему таймер-счетчик обратного счета. Последний начинает отсчитывать условное время простоя, признаком окончания которого является нулевое состояние счетчика. Если работа идет нормально, таймер не заканчивает счет, так как его повторный запуск происходит до окончания счета. Если за время тайм-аута процессор не запустит таймер, он выдает сигнал на прерывание (и на запуск восстановительных процедур). Например, в ЭВМ ЕС-1046 время таймера составляло 30 с. Развитие этого метода – применение охранных сервисных процессоров, которые могут отслеживать активность основного процессора.

Периодическое тестирование (микропрограммное или программное) используется в тех случаях, когда средства контроля на логическом уровне не охватывают все узлы ЭВМ. Периодическое тестиро-

вание ведет к непроизвольным затратам машинного времени, поэтому разработчики рекомендуют определять оптимальную периодичность тестирования

$$T_{опт} = \sqrt{\frac{2t}{\lambda}},$$

где λ – интенсивность потока отказов в аппаратуре, охваченной тестовым контролем;

t – длительность тестирования.

Например, t = 0,1 ч; $\lambda = 10^{-2}$ ч$^{-1}$; $T_{опт}$ = 4,5 ч.

Часто применяют периодическое самотестирование на программном уровне со сбросом охранного таймера при успешном завершении теста (например, процессор делает вычисления со стандартными данными и сравнивает результат с эталоном). Если результат совпадает, таймер сбрасывается.

Контроль корректности протоколов осуществляется путем контроля обмена между внутренними регистрами, процессором и регистрами и т.д.

На *системном* уровне используются:

- контроль по неверному ходу программы, обращению к неиспользуемой или несуществующей области памяти, к несуществующему коду операции;
- контроль корректности форматов данных и команд;
- контроль форматов и протоколов обмена с внешними устройствами и т.д.

В ЭВМ общего назначения контроль на логическом, функциональном и системном уровнях обеспечивает обнаружение более 80 % ошибок, обусловленных неисправностями.

На *пользовательском* уровне используются:

- контроль с помощью двойного счета;
- проверка на допустимость входных и выходных параметров программы;
- реверсивный контроль.

Проверка на допустимость входных и выходных параметров программы основана на проверке принадлежности параметров определенному диапазону значений.

Реверсивный контроль основан на том, что по результатам рабочей программы определяются соответствующие входные параметры, которые сравниваются с реальными, представленными в документации.

3.2. Общая модель процесса обнаружения ошибок

Ошибка – это проявление неисправности. Неисправность приводит к ошибке в том случае, если изменяет значение сигнала на противоположное. До тех пор, пока это не произойдет, неисправность остается скрытой.

Неисправности классифицируют по различным признакам (табл. 3.1).

Таблица 3.1

Классификация неисправностей

По источнику происхождения	По уровню детерминированности	По степени распространения	По длительности
Внутренние и внешние	Детерминированные (соответствуют уровню 0 и 1) и недетерминированные (могут восприниматься как 0 и 1)	Локальные (одиночные) и распространенные (кратные)	Постоянные, случайные, перемежающиеся

Неисправности *внутренние* – это неисправности электронных компонентов, *внешние* – возникающие от наводки, помехи, электромагнитной радиации.

Локальные (одиночные) неисправности затрагивают одну переменную, а *распространенные* (кратные) – несколько цепей или ячеек памяти (например, в БИС, СБИС).

Случайные неисправности возникают при кратковременном изменении параметров из-за колебаний температуры, магнитной радиации, изменения задержек, помехи по питанию, воздействия α-частиц на полупроводниковые элементы.

Перемежающиеся неисправности являются следствием постоянных неисправностей, например: нарушения контактов в разъемах, критическая (по задержкам) временная диаграмма и т.п. Перемежающиеся неисправности характеризуются периодами активности и пассивности. Интервал времени между моментами возникновения неисправности и появления ошибки называют периодом скрытости неисправности.

Задача САК состоит в обнаружении ошибки с минимальной задержкой во времени и минимальным «расстоянием» к месту ее воз-

никновения, т.е. по возможности с большей временной и пространственной разрешающей способностью. Типичный процесс обнаружения ошибки можно представить в виде схемы (рис. 3.2).

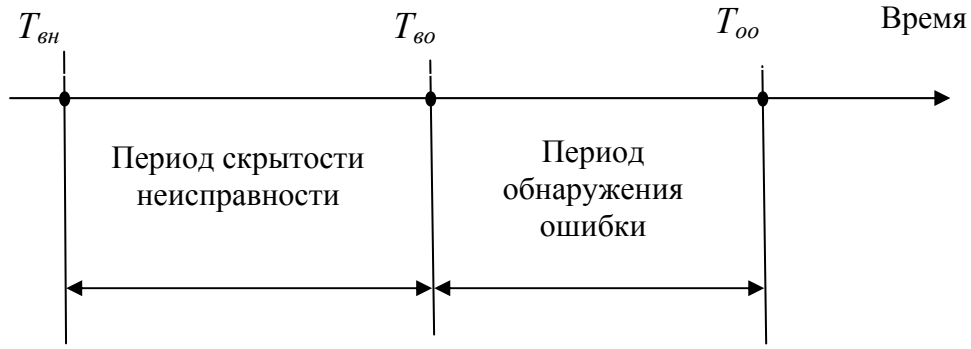


Рис. 3.2. Условное представление на оси времени процесса обнаружения ошибки после возникновения неисправности:
$T_{вн}$ – момент возникновения неисправности;
$T_{во}$ – момент возникновения ошибки; $T_{оо}$ – момент обнаружения ошибки

Можно выделить следующие состояния контролируемого вычислительного устройства:

1. Устройство исправно ($И$).
2. В устройстве имеется активная неисправность, но ошибка не проявилась ($Н$).
3. В устройстве имеется неисправность, перешедшая в пассивное состояние ($ПН$).
4. В устройстве имеется хотя бы одна необнаруженная ошибка, и вызвавшая ее неисправность сохраняется ($НО$).
5. Перемежающаяся неисправность перешла в пассивное состояние, или случайная неисправность самоустранилась после того, как она вызвала ошибку ($СО$).
6. Ошибка обнаружена ($ОО$).

Если изобразить состояния контролируемого вычислительного устройства кружками с обозначениями внутри, а дугами – переходы из одного состояния в другое с соответствующими интенсивностями λ, то процесс обнаружения ошибки может характеризоваться графом состояний. Учитывая, что ошибка может быть обнаружена до и после искажения информации в системе, следует различать два соответствующих вида состояний: $ОО_1$ и $ОО_2$ (рис. 3.3) [6].

С появлением неисправности устройство из состояния $И$ (исправно) может перейти в состояние $Н$ (неисправно) с вероятностью λ_{12}.

Если неисправность – случайная, она может самоустраниться, и устройство вновь перейдет в состояние *И* (с вероятностью λ_{21}). Если неисправность – перемежающаяся, то возникают переходы $И \to ПН(\lambda_{13})$ (*ПН* – перемежающаяся неисправность) и $ПН \to И(\lambda_{31})$, $ПН \to Н(\lambda_{32})$, $Н \to ПН(\lambda_{23})$. На логическом уровне период обнаружения ошибки очень мал, и ошибка может не вызвать искажения информации, поэтому возможен переход $Н \to ОО_1$, когда ошибка обнаружена до искажения информации.

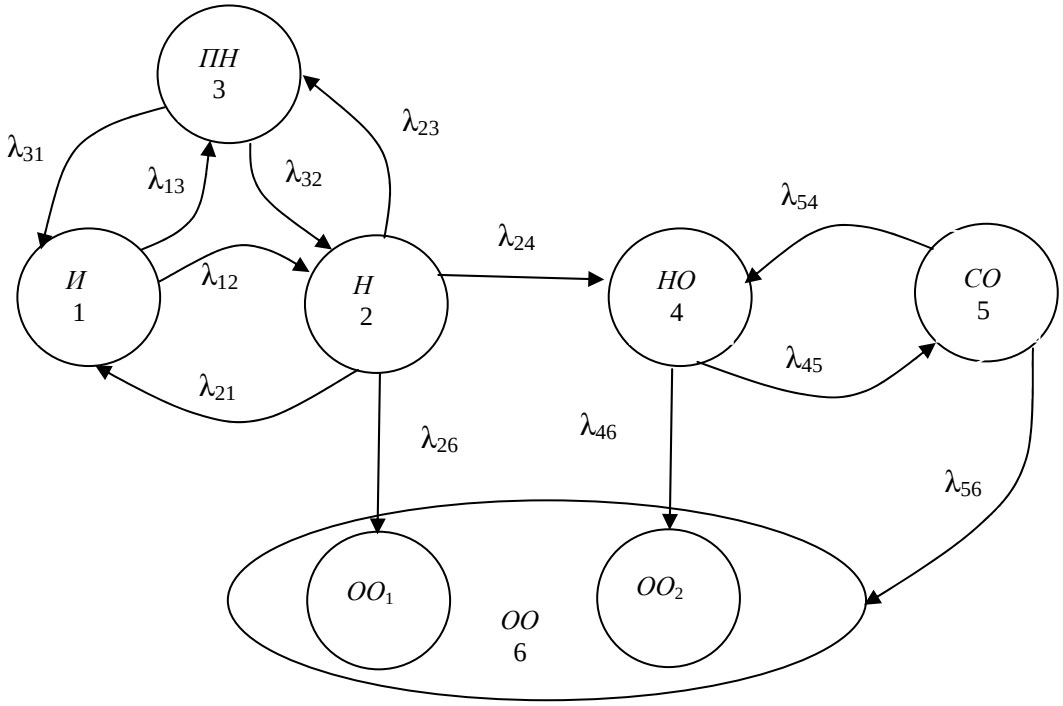


Рис. 3.3. Модель процесса обнаружения ошибки

Если ошибка не обнаруживается средствами контроля логического уровня, она остается скрытой до обнаружения ее средствами контроля других уровней, т.е. устройство переходит в состояние $Н \to НО$ (необнаруженная ошибка). В этом состоянии ошибка вызывает искажение информации до ее обнаружения ($НО \to ОО_2$). При обнаружении ошибки (если это удалось) состояние устройства можно характеризовать состоянием $ОО_2$. Из состояния *НО* устройство может также перейти в состояние *СО* (самоустраняющаяся ошибка), если имела место случайная или перемежающаяся неисправность, которая самоустранилась или стала пассивной, когда она уже испортила информацию.

Считается, что вычислительный процесс заканчивается недостоверным результатом, если в момент его окончания в устройстве имеется необнаруженная ошибка. Вероятность обнаружения ошибок на логическом уровне меньше единицы, часть ошибок может вызывать искажение информации, что может иметь два последствия:

– выдачу неверного результата до того, как система обнаружит ошибку;

– необходимость сложных и длительных процедур по восстановлению информации.

Задача выбора оптимального соотношения средств контроля различных уровней является одной из основных задач при проектировании вычислительных устройств. При этом необходимо в первую очередь обеспечить контролепригодность устройства.

3.3. Контролепригодность цифровых устройств

Контролепригодность (КПГ) – это свойство устройства, обусловленное приспособленностью к проведению контроля его технического состояния в процессе изготовления и эксплуатации. КПГ определяется возможностью генерации тестовых сигналов, их обработки и выдачи результатов контроля, объемом тестов, методикой тестирования (диагностирования). Таким образом, контролепригодность в значительной мере определяется тестируемостью.

Тестируемость цифрового устройства (ЦУ) – это наличие для любой неисправности заданного класса вход-выходной последовательности битов конечной длины, обнаруживающей эту неисправность. Условиями тестируемости являются управляемость и наблюдаемость.

Управляемость – это возможность установки ЦУ в заданное состояние путем подачи на его входы некоторых входных кодов; *наблюдаемость* – это возможность выявления того, в каком состоянии находилось устройство по анализу его вход-выходной последовательности за конечное число тактов.

КПГ оценивается рядом показателей, зависящих от показателей надежности, способов восстановления и т.п. При этом должен быть четко ограничен класс обнаруживаемых неисправностей.

Выделяют следующие *принципы построения контролепригодных устройств:*

- установление заданной полноты контроля и глубины поиска неисправности;
- определение необходимого числа контрольных точек для обнаружения заданного класса неисправностей;
- выбор структурных построений устройств, облегчающих их тестирование;
- рациональное разбиение аппаратуры на составные части (модули), определяющие глубину диагностирования;
- организация межмодульного интерфейса, позволяющего электрически разделять отдельные модули друг от друга в режиме диагностирования;
- создание высоконадежного диагностического ядра, на основе которого возможно построение иерархической системы диагностирования. Функцией диагностического ядра является генерирование тестовых последовательностей и анализ результатов тестирования.

3.4. Системы автоматического диагностирования

Цель диагностирования – обнаружение и локализация неисправностей. *Системы автоматического диагностирования* (САД) призваны облегчить обслуживание и ремонт электронных средств, в частности они повышают готовность и обслуживаемость ЭВМ [6].

САД – это комплекс программных и аппаратурных средств и справочной документации (тесты, инструкции, диагностические справочники) (рис. 3.4).

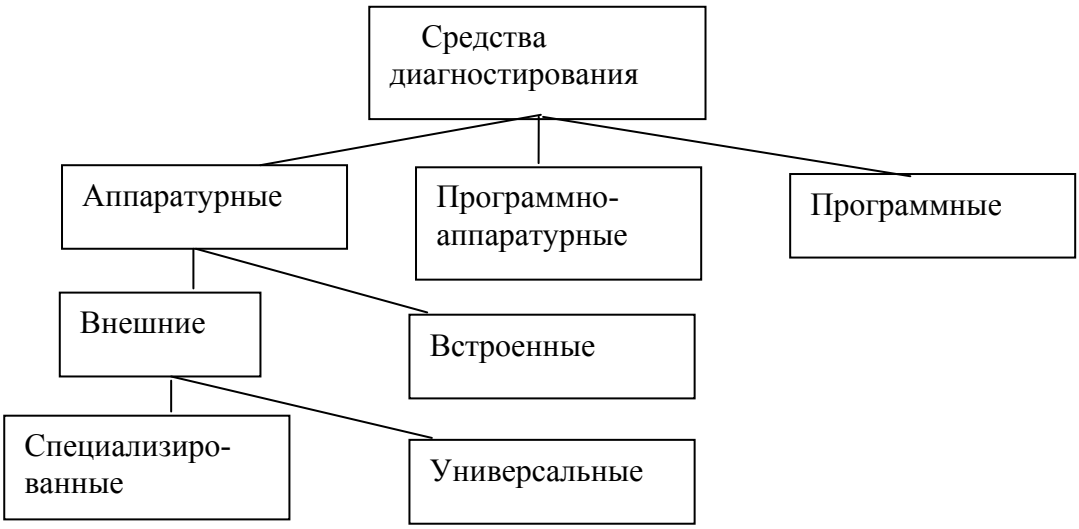


Рис. 3.4. Общая классификация средств диагностирования

САД разделяют на системы тестового и функционального диагностирования. *Тест* – это задача с известным решением, предназначенная для проверки правильности работы устройства или программы. *Тестовое диагностирование* применяют для оценки исправности или поиска дефектов чаще всего при изготовлении изделий электронной техники, при хранении перед эксплуатацией и после неё. *Функциональное диагностирование* чаще используют в процессе эксплуатации устройств для проверки правильности их функционирования и определения дефектов, ведущих к отказу (нарушению работоспособности).

Систему тестового диагностирования можно представить структурной схемой (рис. 3.5).

Рис. 3.5. Структурная схема системы тестового диагностирования

В системе тестового диагностирования воздействия на диагностируемое устройство (ДУ) поступают от средств системы диагностирования (СД). *Тествоздействие* – это совокупность кодов, воздействующих на диагностируемое устройство с целью локализации места неисправности.

В системах функционального диагностирования воздействия, поступающие на ДУ, задаются рабочим алгоритмом функционирования устройства (рис. 3.6).

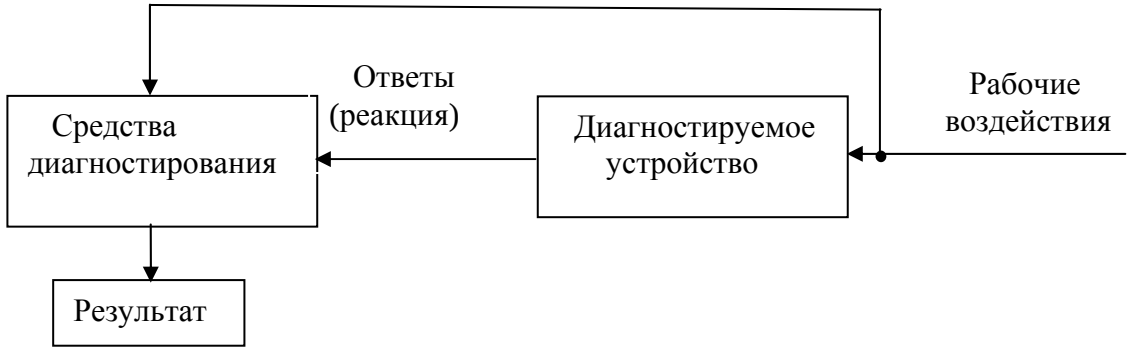


Рис. 3.6. Структурная схема системы функционального диагностирования

Внешние средства диагностирования применяют для средних и больших ЭВМ. В микроЭВМ чаще используются встроенные и внешние универсальные средства.

Процесс диагностирования состоит из элементарных проверок, каждая из которых характеризуется подаваемым тестовым или рабочим воздействием и снимаемым ответом. Эти ответы (значения сигналов в контрольных точках) являются результатом элементарной проверки.

Объект элементарной проверки – часть ДУ, на проверку которого рассчитано диагностическое воздействие (тестовое или рабочее).

Алгоритм диагностирования – совокупность (последовательность) элементарных проверок и правил обработки результатов. Алгоритм может быть безусловным и условным. В безусловном алгоритме используется одна фиксированная последовательность; в условном – задано несколько различных последовательностей реализации элементарных проверок.

Диагностическое ядро – та часть аппаратуры, которая должна быть заведомо работоспособной до начала процесса диагностирования.

При диагностировании ЭВМ широко используется *принцип раскрутки* (принцип расширяющихся областей). Он заключается в том, что на каждом этапе диагностирования ядро и аппаратура уже проверенных исправных областей устройства образуют теперь средство тестового диагностирования, а аппаратура очередной проверяемой области является объектом диагностирования (рис. 3.7).

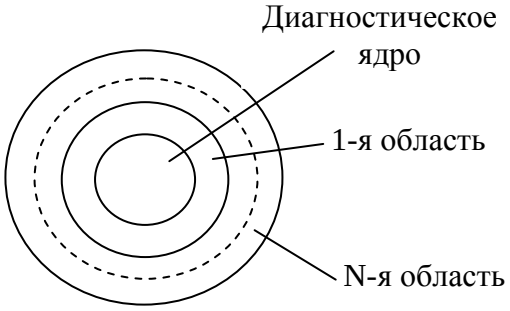


Рис. 3.7. Принцип раскрутки

Средства тестового диагностирования (СТД) выполняют такие функции, как:

– загрузка тестовой информации;

– подача тестовых воздействий на вход проверяемого устройства (блока);

– опрос ответов с выхода проверяемого блока;

– сравнение полученных ответов с ожидаемыми (эталонными);

– анализ и индикация результатов.

В соответствии с этим внешние СТД можно представить в виде структурной схемы (рис. 3.8).

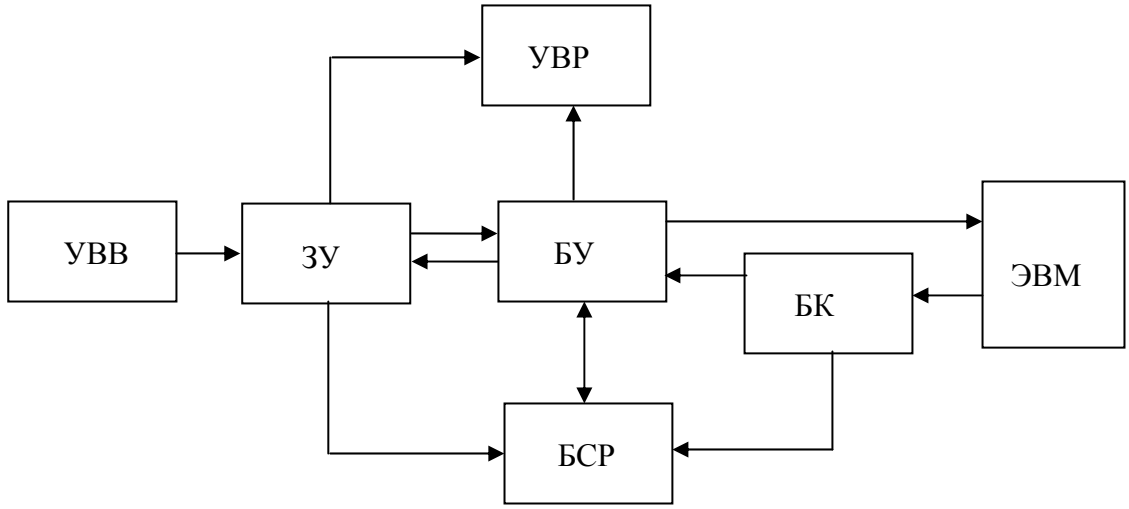


Рис. 3.8. Упрощенная структурная схема системы тестового диагностирования:
БУ – блок управления чтением и выдачей тестовых воздействий, снятием сигналов ответа, распределением потоков информации;
БК – блок коммутации, переключает потоки информации; УВВ – устройство ввода внешней информации; ЗУ – запоминающее устройство (накопитель);
БСР – блок сравнения потоков информации; УВР – устройство выдачи результата

Если в эту структуру добавить клавиатуру и дисплей, то получится структура так называемого сервисного процессора, предназначенного для обслуживания и диагностирования ЭВМ.

Классификация и характеристики методов диагностирования электронных средств. Методы диагностирования характеризуются объектом элементарной проверки, способами подачи воздействия и снятия ответов. Совокупность методов можно классифицировать в соответствии с описанными ранее средствами диагностирования (рис. 3.9).

Процесс разработки системы диагностирования включает следующие этапы:

а) выбор метода диагностирования;

б) определение способов интерпретации результатов диагностирования;

в) выбор аппаратурных средств диагностирования;
г) разработка диагностических тестов;
д) составление диагностических справочников;
е) проверка качества системы диагностирования.

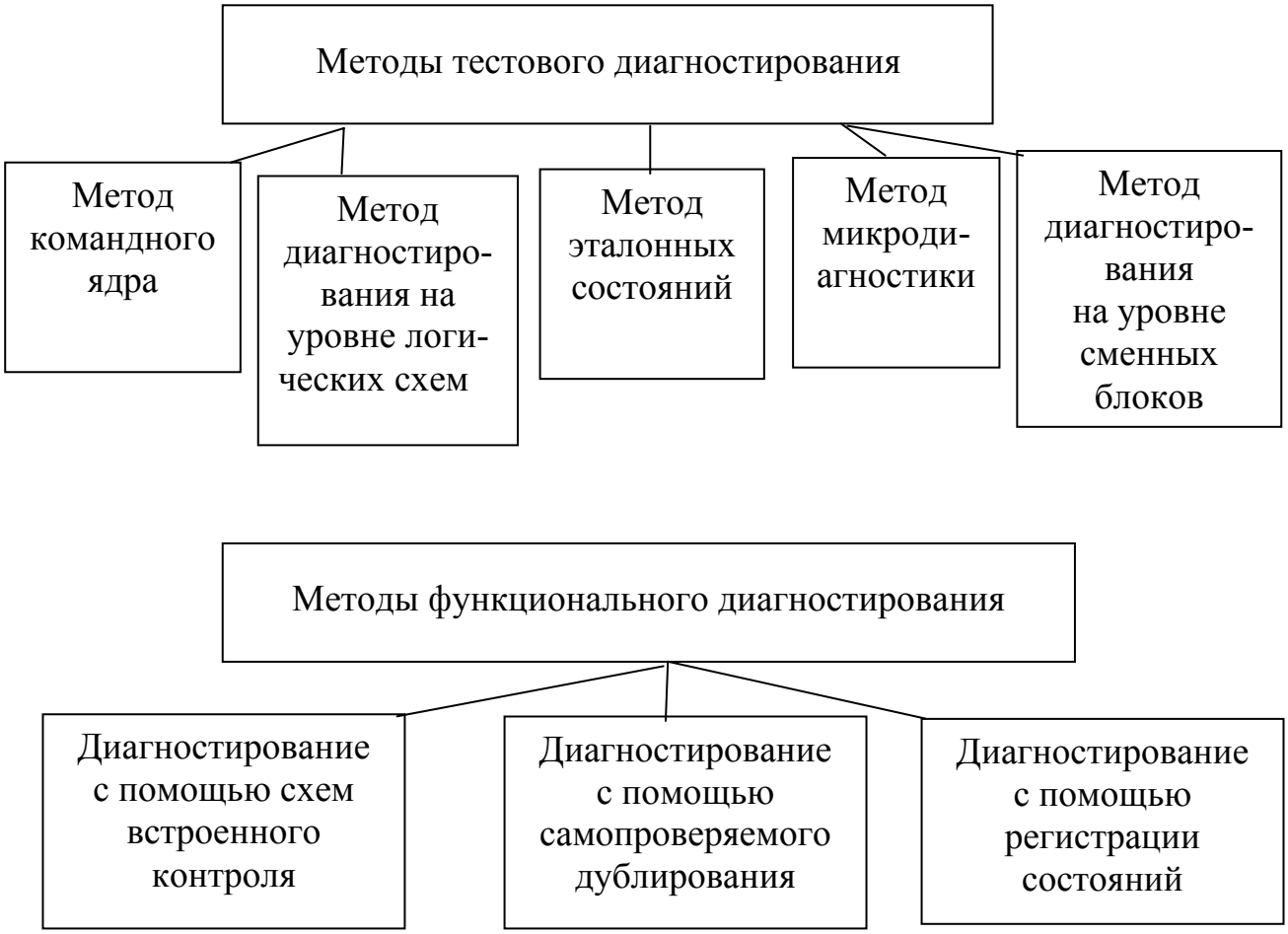


Рис. 3.9. Классификация методов диагностирования

Сравнение различных систем диагностирования можно производить по ряду показателей:

1. Вероятность обнаружения неисправности F.
2. Вероятность правильного диагностирования D.

Удовлетворительными считаются показатели $F \geq 0{,}95$; $D \geq 0{,}9$.

Правильное диагностирование – это такое, при котором неисправный блок идентифицирован кодом, отмечен в разделе диагностического справочника, код которого соответствует коду остановки. Если этого нет, то неисправность считается обнаруженной, но не локализованной. В этом случае потребуются дополнительные меры по локализации неисправности.

3. Средняя продолжительность однократного диагностирования τ_D либо коэффициент продолжительности диагностирования $K_д$:

$$K_д = 1 - \tau_D / T_в ,$$

где $T_в$ – время восстановления.

4. Глубина поиска дефектов L, которая указывает составную часть диагностируемого устройства (ДУ), с точностью до которой определяется место дефекта (до модуля, до микросхемы и т.д.). В качестве показателя глубины поиска используется выражение

$$L = \sum n_i / N,$$

где n_i – число предполагаемых неисправных сменных блоков (ТЭЗ) при i-й неисправности;

N – общее число неисправностей.

5. Объем диагностического ядра. Это доля аппаратуры, которая должна быть заведомо исправна до начала процесса диагностирования.

Краткая характеристика методов тестового диагностирования. *Метод командного (диагностического) ядра* основан на использовании программных средств диагностирования. В системе команд ЭВМ выделяется перечень (ядро) команд, необходимых для загрузки тестов, сравнения результатов с эталонными, ветвления по несовпадению результатов и выдачи сообщений персоналу. Объектом элементарной проверки при этом методе является аппаратура, использованная при выполнении команд. Недостаток метода – требуется большой объем диагностического ядра.

Метод диагностирования на уровне логических схем. Объектами элементарных проверок являются логические схемы, при этом используются раздельная проверка схем с памятью (где есть регистры, триггеры) и проверка комбинационных схем. Известны две реализации этого метода:

1) Двухэтапное диагностирование.

В этой реализации метода используется так называемый формат ТЛН (тест локализации неисправностей).

Содержание (структура) ТЛН:

– *установочная информация* – для микропрограммы установки регистров процессора в требуемые для теста состояния;

– *управляющее слово* – задает адрес микрокоманды, содержащей проверяемую микрооперацию и число выполняемых микрокоманд.

– *адрес результата* – задаёт адрес диагностической области оперативной памяти, в которую в результате опроса записывается состояние проверяемого регистра;

– *маска* – выделяет (маскирует) проверяемые биты;

– *эталон* – содержит ожидаемые результаты;

– *адрес перехода по удаче* – задает начальный адрес следующего теста (адрес первого слова) при совпадении результата с эталоном;

– *адрес перехода по неудаче* – для конечных тестов задает номер теста.

В процессе диагностирования выполняются диагностические операции, которые могут быть реализованы аппаратурно или с помощью микропрограмм. Диагностирование выполняется в два этапа: на первом этапе проверяются все регистры и триггеры, которые могли быть установлены с помощью операции «установка» и опрошены с помощью операции «опрос»; на втором этапе – все комбинационные схемы.

2) Последовательное сканирование. В данной реализации схемы с памятью в режиме диагностирования превращают в один сдвигающий регистр с возможностью установки в произвольное состояние и опроса с помощью операции «сдвиг».

Диагностирование выполняется также в два этапа: на первом этапе устанавливается режим сдвигающего регистра; осуществляется проверка сдвигающего регистра и, следовательно, всех схем с памятью путем последовательного сдвига по нему нулей и единиц; на втором – производится диагностирование комбинационных схем.

Метод эталонных состояний. Процесс диагностирования заключается в потактовом выполнении рабочих алгоритмов работы ДУ, опросе состояния ДУ в каждом такте, сравнении состояния ДУ с эталонным и ветвлении (переходе) в зависимости от исхода сравнения: к выполнению следующего такта или сообщению о неисправности.

Процедура диагностирования методом эталонных состояний представляется в виде структурной схемы алгоритма. Эталонной последовательностью состояний считается последовательность состояний S_{ij}, $j = 0...n,$ имеющих место при отсутствии ошибок, где i – путь из множества N путей, каждому из которых соответствует последовательность состояний ЭВМ в каждом такте $S_{i0}, S_{i1}...S_{ij}... S_{in}$, n – число тактов выполнения операции с конкретными условиями.

Метод микродиагностирования. Объектом элементарной проверки является аппаратура, участвующая в выполнении микроопераций.

Микродиагностика – это совокупность процедур, диагностических микропрограмм и специальных схем, обеспечивающих транспортировку тестового набора на вход ДУ, выполнение проверяемой микрооперации, транспортировку результатов проверки к схемам анализа и сравнения с эталоном, ветвления по результатам сравнения.

Различают два типа микродиагностики: встроенную и загружаемую. Первая предполагает размещение диагностических микропрограмм в ПЗУ программ ЭВМ. Вторая размещается на внешнем носителе данных.

Глубина поиска дефекта при микродиагностике зависит от числа схем, для которых предусмотрена возможность непосредственного опроса состояния. В современных ЭВМ – это почти все триггеры и регистры.

Метод диагностирования, ориентированный на проверку сменных блоков. Объект элементарных проверок – сменные блоки, в качестве которых чаще всего используют типовые элементы замены (ТЭЗ). Есть два варианта реализации данного метода:

1. В каждый сменный блок вводится дополнительная аппаратура, обеспечивающая подачу на вход сменного блока тестового воздействия от средства тестового диагностирования (СТД) и передачу ответов к точкам опроса. Диагностирование заключается в настройке схем управления на проверку сменного блока, подаче тестовых воздействий на его вход, опросе результатов на выходе и сравнении их с эталонными.

2. Селекторы устанавливают в тех сменных блоках, которые соединены с первичными входами ДУ, и на обратных связях, обеспечивая их разрыв в режиме диагностирования. Выходы каждого сменного блока соединяют со средствами тестового диагностирования. СТД имеют информационные выходы, соединяемые с дополнительными входами всех селекторов. Они служат для выдачи тестовых воздействий на блоки устройства.

Характеристика методов функционального диагностирования. *Метод диагностирования с помощью схем встроенного контроля.* Объектом элементарной проверки является сменный блок. В этом методе средства функционального диагностирования – это схемы встроенного контроля (СВК), конструктивно совмещенные с каждым сменным блоком (рис. 3.10).

К достоинствам метода диагностирования с помощью схем встроенного контроля относятся: быстрое диагностирование сбоев и отказов; сокращение затрат на локализацию перемежающихся отказов и на разработку диагностических тестов.

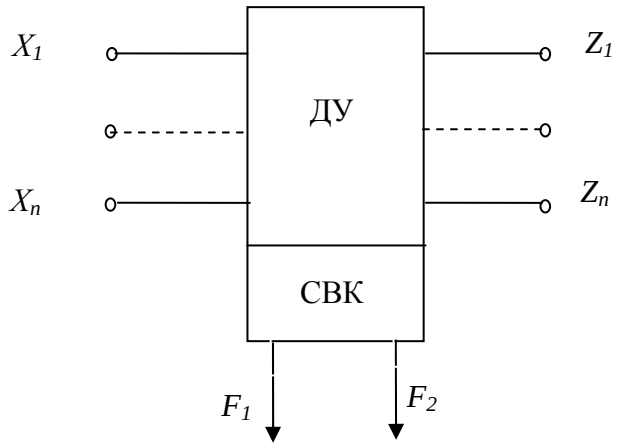


Рис. 3.10. Совмещение СВК
и диагностируемого устройства:
$X_1 \ldots X_n$, $Z_1 \ldots Z_n$ – соответственно входные
и выходные линии диагностируемого устройства;
F_1, F_2 – выходы СВК («исправен, неисправен»)

Метод диагностирования с помощью самопроверяемого дублирования (рис. 3.11). В схеме имеются дублирующее диагностируемое устройство и самопроверяемые схемы сжатия информации. Эти схемы обеспечивают получение сводного сигнала ошибки, свидетельствующего о неисправности диагностируемого блока.

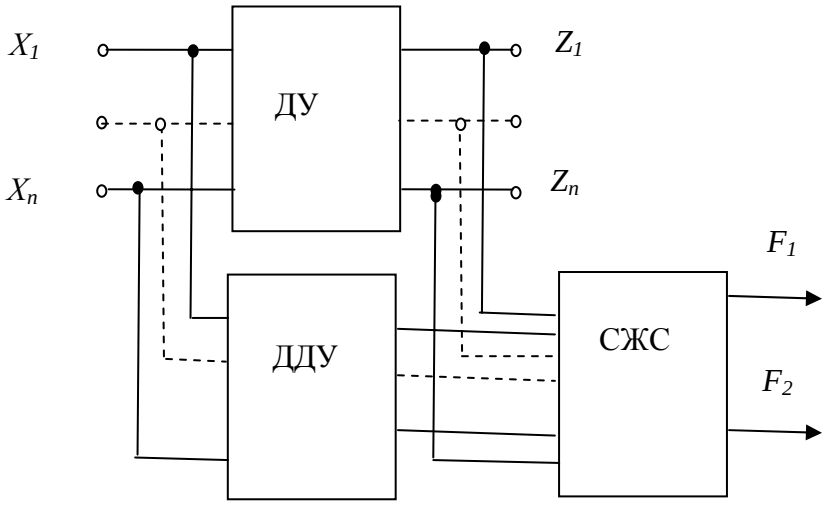


Рис. 3.11. Схема метода диагностирования
с дублированием проверяемого блока:
ДДУ – дублирующее диагностируемое устройство;
СЖС – схема сжатия и сравнения информации

Метод диагностирования с помощью регистрации состояния. Этот метод характеризуется тем, что неисправность или сбой локализуется по состоянию ЭВМ, зарегистрированному в момент проявления ошибки и содержащему информацию о состоянии схем контроля, регистров, адресов микрокоманд в моменты, предшествующие моменту ошибки. Место возникновения ошибки определяется путем прослеживания трассы ошибки от места ее проявления до момента ее возникновения. Метод осуществляется системами прогнозирования отказов.

3.5. Тестопригодность электронных средств

С учетом большого разнообразия методов тестового диагностирования электронные средства должны обладать такой приспособленностью к тестированию (тестопригодностью), чтобы минимизировать затраты на тестирование. Тестопригодными можно назвать схемы со сравнительно небольшой трудоемкостью вычисления тестов, несложной интерпретацией результатов тестирования, с достаточной полнотой проверки и глубиной поиска дефектов. Полнота проверки – это доля обнаруживаемых дефектов при тестировании.

Тестопригодность достигается структурной модификацией исходных схем, введением дополнительных средств и линий управления.

Показателями тестируемости, как и контролепригодности, могут быть управляемость и наблюдаемость.

Например, *управляемость* по уровню сигнала «1» или «0» на линии N определяется минимальным числом линий схемы, которые необходимо установить в конкретные состояния для установки единицы (нуля) в этой линии.

Наблюдаемость линии – это число линий схемы, которые необходимо установить в требуемое состояние для того, чтобы обеспечить возможность наблюдения состояния линии N на выходе схемы.

Если обозначить управляемость и наблюдаемость линии N через $C_0(N)$, $C_1(N)$, $C_2(N)$, то суммарное значение управляемости и наблюдаемости определится выражением

$$S_N = \sum C_i(N),$$

где $i = 0, 1, 2$.

Чем больше S_N, тем хуже управляемость и наблюдаемость.

Тестопригодность схемы можно определить суммарной величиной

$$S = \sum K_i \cdot S_N,$$

где K_i – весовые коэффициенты управляемости и наблюдаемости.

Правила обеспечения тестопригодности:

1. Нужно обеспечить управляемость извне цепей сброса триггеров и регистров, для чего использовать либо незадействованные линии сброса, либо дополнительные линии управления, имеющие соединения с внешними контактами.

2. Необходимо обеспечить наблюдаемость состояния триггеров со стороны внешних контактов.

3. При наличии трудноуправляемых участков схем можно использовать линии блокировки и дополнительные входы.

4. Для улучшения тестируемости участка В, заключенного между участками А и С, можно применять дополнительные мультиплексоры, обеспечивающие управляемость и наблюдаемость участка В извне.

5. Для лучшей наблюдаемости нужно использовать дополнительные контрольные точки, при этом стремиться к тому, чтобы эти точки можно было использовать как дополнительные входы управления.

6. Необходимо избегать схем с неуправляемыми петлями обратной связи, так как они затрудняют вычисление тестов и снижают полноту проверки. Управление этими цепями можно обеспечить либо выводом во внешнюю цепь, либо введением дополнительного блокировочного узла.

7. Следует избегать использования избыточных схем, так как избыточность маскирует некоторые неисправности и ухудшает тестопригодность. В случае если избыточность используется, например, для устранения состязаний, в схему надо вводить дополнительные линии управления, позволяющие при тестировании исключить избыточность.

8. В связи с тем что методика и аппаратура проверки аналоговых и цифровых элементов различны, желательно размещать их на разных платах.

9. Целесообразно при разработке устройств и ТЭЗ учитывать характеристики тестовой аппаратуры.

10. Если в схеме имеется внутренний тактовый генератор, нужно предусмотреть возможность его отключения и подачи внешних тактовых импульсов.

11. Если в схеме есть ИС ОЗУ, необходимо обеспечить их управляемость и наблюдаемость с помощью внешних контактов.

12. С целью улучшения тестопригодности многоразрядных счетчиков следует использовать управляемые контрольные точки, делящие его на части.

13. Желательно унифицировать номера внешних контактов, предназначенных для одной и той же функции (например, интерфейс).

14. Для облегчения снятия и тестирования ТЭЗ с БИС (в частности, микропроцессорных БИС) нужно использовать разъемные колодки для установки БИС, особенно в опытных образцах изделий.

4. МЕТОДЫ И СРЕДСТВА КОНТРОЛЯ ПЕРЕДАЧИ И ОБРАБОТКИ ДВОИЧНОЙ ИНФОРМАЦИИ

Контроль передачи двоичной информации осуществляется преимущественно на основе кодов с *информационной избыточностью*. Чаще всего используются коды с обнаружением и коррекцией ошибок [7].

Если длина кода – n разрядов, то таким кодом можно представить 2^n различных слов. В случае если все разряды слова используются для представления информации, код называется *простым (неизбыточным).* Если для представления информации используется только часть кодового слова, код называется *избыточным*. Часть слов в избыточных кодах можно условно считать запрещенными, и если они появляются у приемника при передаче информации, то это свидетельствует о наличии ошибки передачи. Принадлежность слова к разрешенным или запрещенным определяется правилами кодирования, и эти правила различны для разных кодов.

Различают *равномерные и неравномерные* коды. Первые содержат слова, имеющие одинаковое число разрядов. В ЭВМ используются преимущественно равномерные коды. В свою очередь, равномерные избыточные коды могут быть *разделимыми и неразделимыми*. Разделимые коды всегда содержат постоянное число информационных и избыточных разрядов, причем избыточные разряды занимают одни и те же позиции в кодовом слове. В неразделимых кодах нельзя указать, где располагаются информационные, а где избыточные разряды.

При оценке способности кода обнаруживать и исправлять ошибки используется понятие кодового расстояния. *Кодовое расстояние* (КР) – это число разрядов, в которых символы слов не совпадают. Если длина слова – n, то кодовое расстояние может принимать значение от 1 до n.

Способность кода обнаруживать или исправлять ошибки оценивается *минимальным кодовым расстоянием* (*МКР*). Это минимальное расстояние между двумя любыми словами в этом коде (данной кодовой совокупности). Если имеется хотя бы одна пара слов, отличающихся друг от друга только в одном разряде, то $МКР = 1$. Для разделимых избыточных кодов $МКР > 1$. Например, если $МКР \geq 2$, то любые два слова в этом коде различаются не менее чем в двух разрядах.

В этом случае появление одиночной ошибки приведет к появлению запрещенного слова, и это может быть обнаружено, если разрешенными считать слова, имеющие $МКР \geq 2$.

В общем случае, чтобы избыточный код позволял обнаруживать ошибки кратности r, должно выполняться условие $МКР \geq (r+1)$.

Действительно, ошибка в r разрядах слова создает новое слово, отстоящее от первого на расстоянии r. Чтобы оно не совпало с каким-либо другим разрешенным словом, минимальное расстояние между двумя любыми разрешенными словами должно быть хотя бы на единицу больше, чем r. Итак, от правильного слова новое отстоит на расстоянии r. От любого другого разрешенного слова оно должно отстоять не менее чем на $(r+1)$, а минимальное кодовое расстояние должно быть не меньше суммы этих величин. Для исправления r-кратной ошибки должно быть

$$МКР \geq 2r+1 \quad [7].$$

Кодовое расстояние между двумя комбинациями двоичного кода определяется очень просто: суммируются эти комбинации по модулю 2, и подсчитывается число единиц в полученной комбинации.

Кодовое расстояние хорошо определяется при построении геометрической модели кодов. В вершинах n-угольников (n – значность кода) расположены кодовые комбинации, а количество ребер n-угольника, отделяющих одну комбинацию от другой, равно кодовому расстоянию.

Пример. Необходимо определить кодовое расстояние между комбинациями:

$$\begin{array}{r} 0001 \\ \oplus\ 0001 \\ \hline 0000 \end{array} \qquad\qquad \begin{array}{r} 11000111001 \\ \oplus\ 10000011101 \\ \hline 01000100100 \end{array}$$

В первом примере кодовое расстояние d = 0, во втором – d = 3. Знак «$\oplus$» обозначает логическую операцию «ИСКЛЮЧАЮЩЕЕ ИЛИ».

Для иллюстрации метода определения кодового расстояния нужно построить геометрическую модель трехэлементного кода (рис. 4.1). Принцип присвоения кодовой комбинации: если проекция на ось равна нулю, то ставится нуль, и наоборот. Порядок проекции должен быть одним для всех: сначала на ось 1, потом на ось 2, затем на ось 3. Следует обозначить углы и расположить грани таким образом, чтобы соседние коды различались только в одной позиции.

Геометрическое представление кода позволяет очень просто определять коды, способные обнаруживать и исправлять ошибки. Для этого используется правило, согласно которому коды, обнаруживающие ошибку, должны иметь кодовое расстояние, равное двум, т.е. отличаются друг от друга в двух символах. Например, комбинации, обнаруживающие ошибку в комбинации 011, будут выглядеть так: 101, 100, 000, 110.

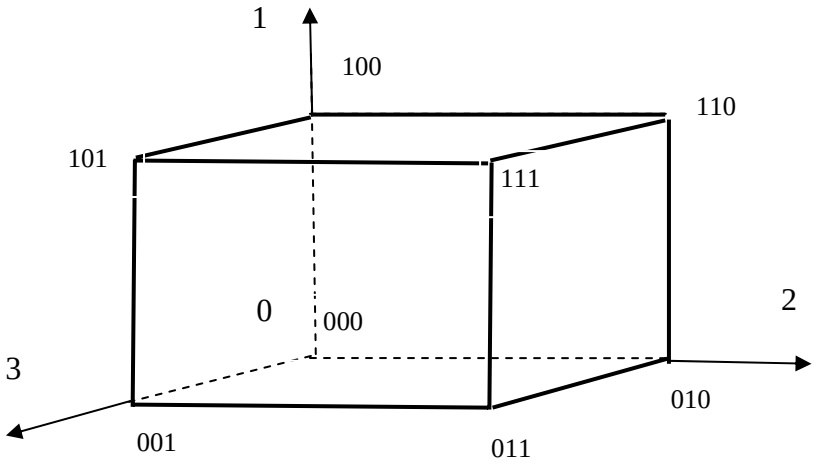


Рис. 4.1. Геометрическое представление трёхэлементного кода

Исправлять ошибку могут только те комбинации, которые имеют кодовое расстояние не менее трех, т.е. отстоящие друг от друга на расстоянии трех ребер (см. рис. 4.1), поэтому они расположены на противоположных вершинах куба: это коды-спутники 000–111, 010–101, 001–110, 011–100.

4.1. Коды с проверкой четности (нечетности)

Коды с проверкой четности образуются путем добавления к группе информационных разрядов, представляющих собой простой (неизбыточный) код, одного избыточного (контрольного) разряда. При этом в контрольный разряд записывается 0 или 1 таким образом, чтобы сумма единиц в слове, включая избыточный разряд, была четной (при контроле по четности) или нечетной (при контроле по нечетности). В дальнейшем при всех передачах (включая запись в память и считывание) слово передается вместе со своим контрольным разрядом или словом. Приемник (приемное устройство) при приеме кон-

тролирует соответствие четности суммы единиц слова значению контрольного разряда. Несоответствие интерпретируется как наличие ошибки при передаче.

Минимальное расстояние кода $МКР = 2$, поэтому код с проверкой четности обнаруживает все одиночные ошибки и случаи нечетного числа ошибок (3, 5 и т. д.). При возникновении одновременно двух или четного числа ошибок код их не обнаруживает.

При контроле по нечетности проверяется полное пропадание информации, так как кодовое слово, состоящее из нулей, относится к запрещенным.

Код с проверкой четности обладает малой избыточностью – не требует больших аппаратурных затрат. Он применяется в ЭВМ для контроля передач информации между регистрами и для контроля считываемой информации в ОЗУ. Интересна связь кодирования при контроле по четности и логической операции «ИСКЛЮЧАЮЩЕЕ ИЛИ» (сложение по модулю 2). Если число единиц в слове, сформированном для передачи, должно быть четным, то в контрольный разряд записывается прямой код суммы по модулю 2 всех информационных разрядов слова. При контроле на нечетность в контрольный разряд заносится обратный код суммы по модулю 2. Например, кодируемое слово имеет шесть разрядов: 011010. Для контроля по четности оно должно быть представлено в виде 0110101, а для контроля по нечётности – в виде 0110100.

4.2. Организация контроля передачи информации с контролем по модулю 2

В этом способе каждое слово дополняется контрольным разрядом, значение которого выбирается так, чтобы сделать четным (или нечетным) вес каждой комбинации (вес – это количество единиц в слове). Контроль по нечетности позволяет фиксировать обрыв всех проводов линий передачи сигналов. Контроль по четности не обнаруживает такую неисправность.

В табл. 4.1 показан принцип образования контрольных битов для четырёхразрядных слов по правилу, согласно которому

$$C_{чет} = a_3 \oplus a_2 \oplus a_1 \oplus a_0, \quad C_{нечет} = \overline{a_3 \oplus a_2 \oplus a_1 \oplus a_0}.$$

Применяется этот метод там, где наиболее вероятны одиночные ошибки (групповые ошибки фиксироваться не будут). Например, в основной памяти МК каждый бит слова хранится в своей собственной ячейке, поэтому наиболее вероятны одиночные ошибки.

Таблица 4.1

Принцип образования контрольных битов

Информационные биты				Контрольные биты	
a_3	a_2	a_1	a_0	$C_{чет}$	$C_{нечет}$
0	0	0	0	0	1
0	0	0	1	1	0
0	0	1	0	1	0
0	0	1	1	0	1
.	.	.	.	.	.
.	.	.	.	.	.
1	1	0	1	1	0
.	.	.	.	.	.
1	1	1	1	0	1

Для памяти на магнитных дисках этот метод неэффективен, так как на них портится несколько соседних ячеек (например, из-за царапины).

Контроль по модулю 2 реализуется с помощью схем свертки. Например, можно использовать схему свертки байта. При этом число логических элементов в свёртываемой схеме определяется по выражению $N = 2^n - 1$, где n – целое число, равное 3 для одного байта и 2 – для полубайта (рис. 4.2).

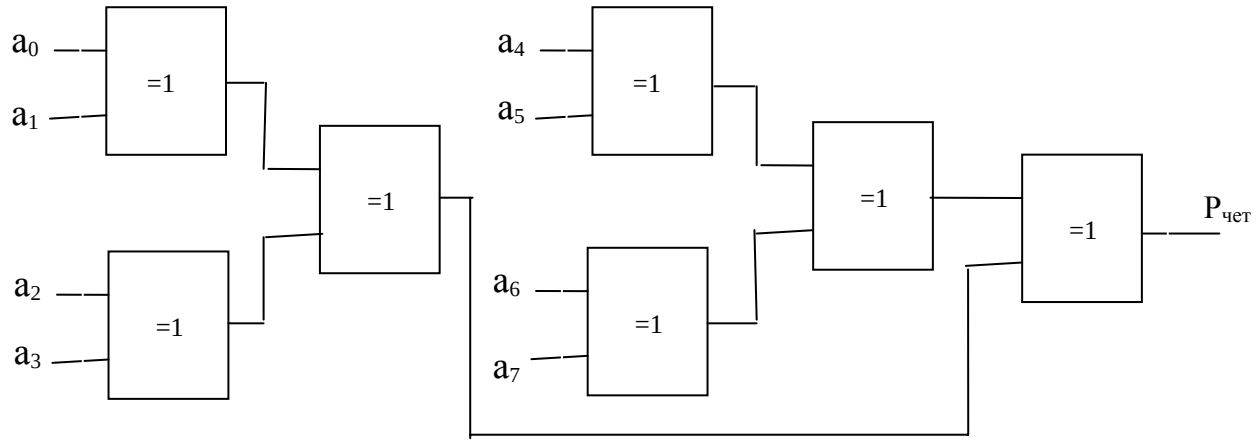


Рис. 4.2. Пирамидальная (параллельная) схема свёртки байта данных

Если слово передается в последовательном коде, то используется схема свёртки последовательного типа (рис. 4.3). В схеме нельзя менять передаваемое слово, пока не закончится цикл свёртки.

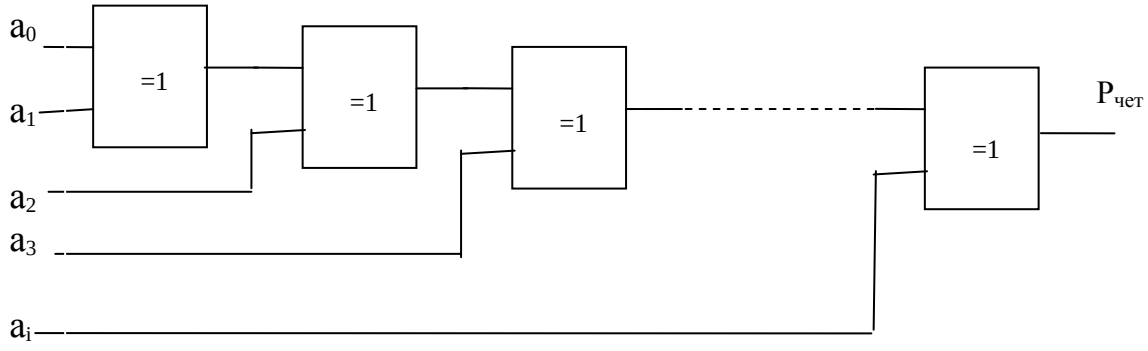


Рис. 4.3. Схема свёртки последовательного типа

Серийно выпускаются специальные микросхемы, например КР1533ИП5, предназначенные для получения свертки по модулю 2 одного байта данных (рис. 4.4).

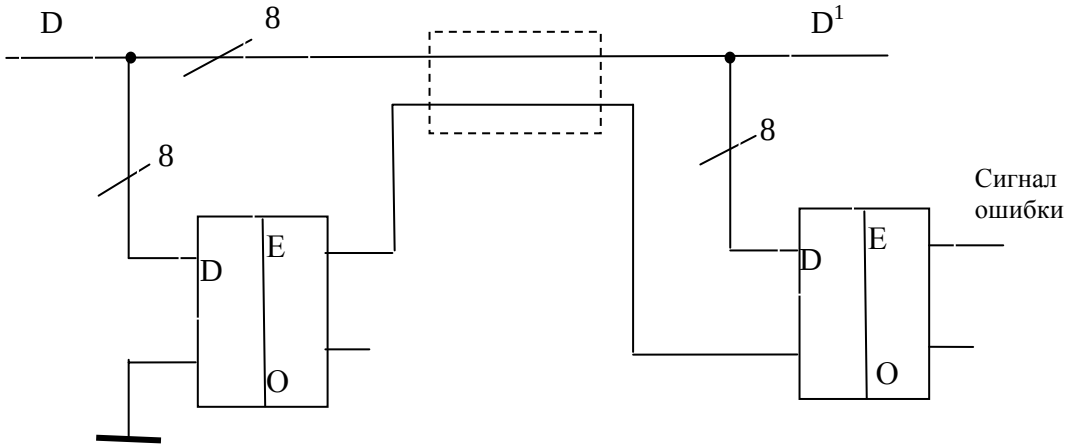


Рис. 4.4. Структурная схема использования микросхемы КР1533ИП5 для контроля пересылки байта данных по многопроводной линии передачи

Схема свёртки используется следующим образом. Если на входе слово имеет четное число единиц, то у передатчика на выходе Е формируется сигнал «1». В этом случае приемник будет ощущать правильное (нечетное) число единиц, при этом на выходе приемника Е будет присутствовать сигнал «0», сигнализирующий о том, что ошибки нет.

Используя свёртку по модулю 2, возможно организовать контроль работы логического преобразовательного элемента (рис. 4.5).

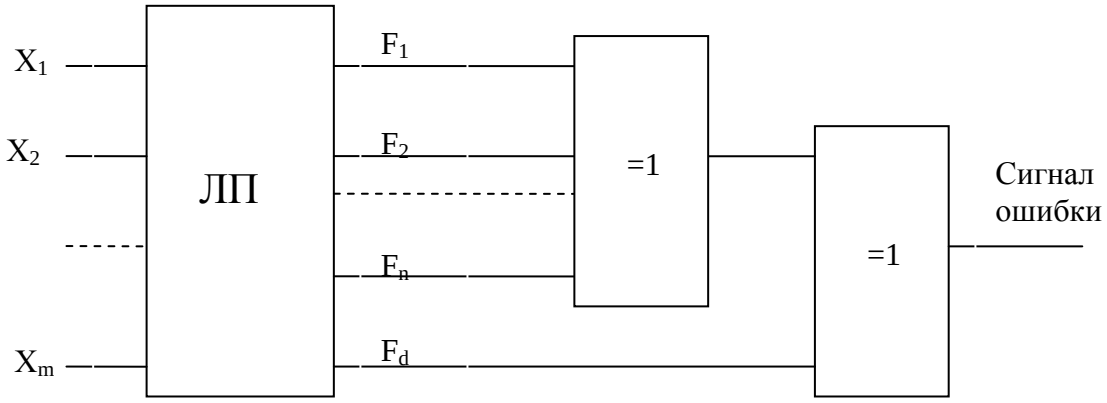


Рис. 4.5. Структурная схема контроля работы логического преобразователя с использованием схемы свёртки по модулю 2

Контроль логического преобразователя (ЛП) осуществляется проверкой соотношения $F_d = F_1 \oplus F_2 \oplus \ldots \oplus F_n$.

Принцип использования проверки на четность при передаче многоразрядного двоичного слова. Пусть сообщение имеет вид 12-разрядной последовательности 0 и 1. Сообщение разбивается на три 4-разрядных слова, и между каждыми двумя словами помещается блок из трех контрольных разрядов, полученных из 4-разрядного информационного слова (рис. 4.6). В результате будут образованы три 7-разрядных слова, которые и будут переданы адресату. Правило образования контрольного числа основано на использовании сложения по модулю 2. Для этого в третий разряд 7-разрядного слова записывается сумма по модулю 2, образованная 7, 6 и 5-м разрядами этого слова.

Во второй разряд записывается сумма по модулю 2, образованная 7, 6 и 4-м разрядами, в первый разряд – сумма, образованная 7, 5 и 4-м разрядами.

При проверке принятого слова, состоящего из трёх 7-разрядных блоков, для каждой группы из четырех информационных разрядов вновь образуют 7-разрядные слова с тремя контрольными разрядами. В каждом 7-разрядном слове подсчитывается число единиц. Если оно окажется нечётным, фиксируется ошибка. Таким образом, если в результате действия шумов и помех в канале передачи последователь-

ность воспроизводимых приемником чисел содержит ошибки, то они обнаруживаются после проведения операций суммирования по модулю 2 (рис. 4.6).

Используется правило: сумма двоичных чисел по модулю 2 равна нулю при четном количестве единиц и единице – при нечетном.

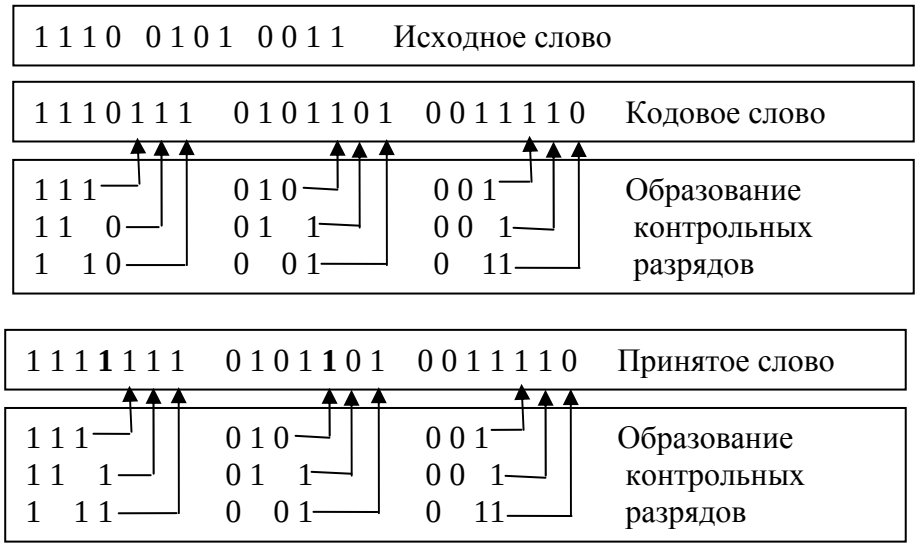


Рис. 4.6. Условное изображение процедуры обнаружения ошибок при передаче информационного слова методом проверки на чётность

Проблема кодирования в теории информации состоит в разработке способа, при котором каждому слову исходного сообщения длиной N ставится в соответствие кодовое слово длиной $M > N$, последнее используется для передачи данных. Из теоремы Шеннона следует, что если отношение N/M меньше некоторой критической неотрицательной величины, называемой пропускной способностью канала, то влияние ошибок в канале можно сделать сколь угодно малым. При достаточно большой длине слов M и N возникают проблемы объема памяти, задержки, усложняются вычисления, поэтому выбор размера слов требует компромиссных решений.

4.3. Контроль по совпадению

После передачи информации из одного канала в другой правильность передачи можно проверить путем поразрядного сравнения прямого и инверсного значений содержимого всех разрядов регистра.

В этом случае не нужно формирование дополнительных (контрольных) разрядов, т.е. способ контроля требует только аппаратурной (схемной) избыточности.

После передачи информации из регистра $РГ_А$ в регистр $РГ_Б$ через время, чуть большее времени установления переходных процессов в триггерах регистров, на выходе схемы сравнения появляется сигнал ошибки при любом несовпадении кодовых комбинаций на выходах передающего и принимающего регистров (рис. 4.7).

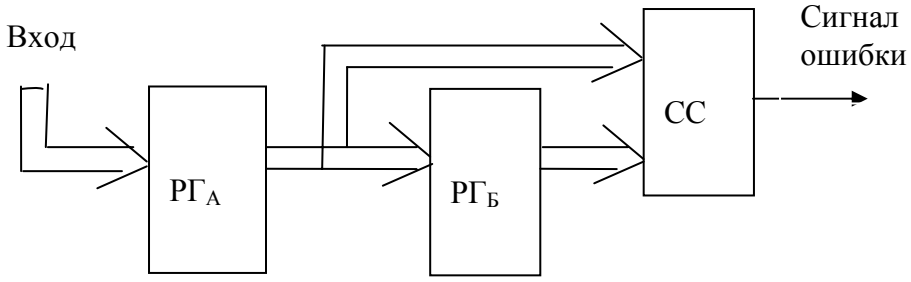


Рис. 4.7. Структурная схема контроля ошибки
при регистровых передачах:
СС – схема сравнения кодовых комбинаций

Главное достоинство метода заключается в том, что обнаруживаются ошибки любой кратности (одиночные и *r*-кратные). К недостатку метода относится то, что он позволяет проверить правильность передачи числа в регистр и отсутствие сбоев при хранении только до тех пор, пока не изменится информация в передающем регистре.

4.4. Корректирующие коды (коды с исправлением ошибок)

Процесс квантования (дискретизации) непрерывного сигнала обязательно сопровождается ошибкой квантования (шум квантования), которая не может быть устранена полностью. Если в исходном сообщении имеются лишь последовательности дискретных сигналов, то при передаче таких сообщений можно в ряде случаев существенно уменьшить или вообще устранить ошибки передачи.

В ЭВМ применяют корректирующие коды, позволяющие не только обнаруживать, но и исправлять ошибки. Примером такого кода является *код Хэмминга*. Он строится таким образом, что к имеющимся информационным разрядам слова добавляется определенное число

контрольных разрядов, которые формируются перед передачей информационного слова путем подсчета четности суммы единиц для определённых групп информационных разрядов.

Контрольная аппаратура на приёмном конце линии передачи образует из принятых информационных и контрольных разрядов путём аналогичных подсчётов чётности корректирующее число, которое равно нулю при отсутствии ошибки либо указывает место ошибки. Ошибочный разряд корректируется путём инверсии его значения.

Требуемое число контрольных разрядов (разрядность корректирующего числа) определяется из следующих соображений. Пусть кодовое слово имеет m информационных разрядов при общем числе разрядов n. Число контрольных разрядов должно быть

$$K = n - m.$$

Двоичное число длиной K разрядов позволяет образовать 2^K состояний, при которых ошибка может присутствовать либо отсутствовать в любом i-м разряде. Соотношение между числами информационных и контрольных разрядов имеет вид

$$2^K \geq (n+1) \quad \text{или} \quad (2^K - K - 1) \geq m.$$

Например, числа контрольных разрядов 2, 3, 4, 5 позволяют в коде Хэмминга передать соответственно 1, 4, 11, 26 информационных разрядов, так как

$$K = 2 \rightarrow m \leq 1, \quad K = 3 \rightarrow m \leq 4, \quad K = 4 \rightarrow m \leq 11,$$
$$K = 5 \rightarrow m \leq 26.$$

Видно, что избыточность кода Хэмминга значительно больше избыточности кода с проверкой четности.

Структура комбинаций кода Хэмминга:

Например, для $m = 4$ $n = 7$, $K = 3$, так как $4 \leq (2^3 - 3 - 1)$:

номера разрядов	7	6	5	4	3	2	1
кодовое слово	a_7	a_6	a_5	$к_4$	a_3	$к_2$	$к_1$

В кодовом слове a_7, a_6, a_5, a_3 – места разрядов информационного 4-разрядного слова; $к_4$, $к_2$, $к_1$ – места контрольных разрядов. Их значения образуются по следующим правилам:

$$к_1 = a_7 \oplus a_5 \oplus a_3,$$
$$к_2 = a_7 \oplus a_6 \oplus a_3,$$
$$к_4 = a_7 \oplus a_6 \oplus a_5.$$

Например, информационное слово 1011 после кодирования будет иметь вид 1010101.

Проверка и обнаружение ошибки при передачах осуществляется путем образования на приемном конце корректирующих (проверочных) чисел, образованных по следующим правилам:

$$к_1 \oplus a_7 \oplus a_5 \oplus a_3 = B_1,$$
$$к_2 \oplus a_7 \oplus a_6 \oplus a_3 = B_2,$$
$$к_4 \oplus a_7 \oplus a_6 \oplus a_5 = B_4.$$

Для определения ошибочного разряда анализируется контрольное слово $B_4B_2B_1$. Например, слово 000 говорит о том, что ошибки нет; слово 011– ошибка в третьем бите; слово 110 – ошибка в шестом бите и т. д.

Ошибка устраняется простым инвертированием найденного разряда. Аппаратная реализация указанных операций осуществляется с помощью логических схем «ИСКЛЮЧАЮЩЕЕ ИЛИ».

Циклические (полиномиальные) коды. Наряду с корректирующими кодами Хэмминга широко используются циклические коды (ЦК). Свое название они получили потому, что большинство кодовых комбинаций в них получают циклическим сдвигом, т. е. таким сдвигом, при котором крайний по направлению сдвига разряд перемещается за один шаг на место 1-го и соответственно сдвигаются на одну позицию остальные разряды. Сдвиг может быть справа налево либо слева направо. При этом с каждым шагом получается новая (другая) кодовая комбинация.

Например, сдвиг слева направо: 1011 1101 1110 0111 1011;
сдвиг справа налево: 1011 0111 1110 1101 1011.

Циклические коды относятся, в основном, к систематическим кодам, т. е. кодам, в которых места информационных и контрольных битов определены однозначно. Свойства ЦК обнаруживать и исправлять ошибки при передаче двоичной информации основаны на алгебраических свойствах многочленов, которыми можно представлять двоичные числа.

Пример. Число $A(x)$ может быть представлено в общем случае в следующем виде:

$$A(x) = a_m x^{m-1} + a_{m-1} x^{m-2} + \ldots a_3 x^2 + a_2 x^1 + a_1 x^0.$$

Пусть $A = 1011_2 = 1\cdot2^3 + 0\cdot2^2 + 1\cdot2^1 + 1\cdot2^0$. Представление двоичного числа A в виде многочлена (полинома) будет иметь вид

$$A(x) = x^3 + x + 1.$$

При этих условиях многочлен $x^3 + x + 1$ следует интерпретировать как двоичное число 1011. Видно, что степень полинома на единицу меньше числа разрядов. Для систем двоичного исчисления при работе с полиномами приняты дополнительные условия: сложение делается только по модулю 2; вычитание заменяется сложением.

В теории ЦК различают следующие виды полиномов:

а) информационный $G(x)$ [имеет степень $(m-1)$];

б) образующий (порождающий) полином $P(x)$ (имеет степень K_0);

в) кодовый полином $F(x)$ [будет иметь степень $n = (m + K_0)$].

Если слово имеет m информационных битов, то кодовый полином будет иметь степень $n = (m + K_0)$, где K_0 – степень образующего полинома, а $(m-1)$ – степень информационного полинома (степень полинома на единицу меньше числа битов в слове).

ЦК используются преимущественно при последовательной передаче данных между ЭВМ и ЗУ, а также при передаче данных по каналам связи.

Принцип обнаружения и коррекции ошибок циклическим кодом. Контроль передачи данных с помощью ЦК основан на следующих положениях. Если информационный полином умножить на образующий полином и полученный при этом полином $F(x)$ (кодовый полином) передать приемнику информации и там выполнить обратное действие, т. е. деление принятого полинома на образующий, и проанализировать остаток от деления, то нулевой остаток говорит о том, что ошибка отсутствует (или не обнаружена).

Ненулевой остаток говорит о том, что произошла ошибка. В качестве образующих (порождающих) полиномов выбирают так называемые неприводимые полиномы – те, которые не могут быть представлены произведением полиномов низших степеней.

Например:

$$P(x) = x + 1; \qquad P(x) = x^2 + x + 1; \qquad P(x) = x^3 + x^2 + 1;$$
$$P(x) = x^3 + x + 1; \quad P(x) = x^4 + x^3 + 1 \qquad \text{и т. д.}$$

Выбор степени K_0 образующего полинома определяется возможностью обнаружения и исправления ошибок. Для нахождения K_0 ис-

пользуется выражение $(2^{K_O} - K_0 - 1) \geq m$, причем $n = m + K_0$, как и прежде, – степень кодового полинома, определяемая в зависимости от минимального кодового расстояния $d_{\text{мин}} = 2r + 1$, где r – кратность ошибки. Из числа образующих полиномов, удовлетворяющих первому условию, следует выбирать как можно более короткие, степени не ниже K_0, но число ненулевых членов должно быть больше или равно минимальному кодовому расстоянию.

Например, при $d_{\text{мин}} = 5$ для кодов, обнаруживающих и исправляющих две ошибки, число контрольных разрядов

$K_0 =]\log_2 [(n^2 + n + 1)/ 2][.$

Для кодов, исправляющих r ошибок, причём $d_{\text{мин}} = 2r + 1$, K_r определяется по выражению $K_r =]\log_2 [(n^r + n^{r-1} \ldots + n + 1)/2][.$

Примечание: обратные квадратные скобки в приведённых выражениях указывают на округление в большую сторону.

Используя приведённые формулы, можно получить соотношения между числами информационных (m) и контрольных (K) разрядов в зависимости от числа исправляемых ошибок r:

r	1	1	2	3	5
m	4	11	7	5	11
K	3	4	8	10	20
n	7	15	15	15	31

Рассмотрим процедуру (методику) формирования циклического кода и его декодирования. Целесообразно вспомнить свойства логической функции «ИСКЛЮЧАЮЩЕЕ ИЛИ», которая широко используется в теории и практике построения кодов и контроля различных операций.

Основные теоремы для функции «ИСКЛЮЧАЮЩЕЕ ИЛИ»:

1) $a \oplus 0 = a$; 2) $a \oplus a = 0$; 3) $a \oplus b = b \oplus a$;
$a \oplus 1 = \overline{a}$; $a \oplus \overline{a} = 1$; $a \oplus b \oplus c = a \oplus (b \oplus c) = (a \oplus b) \oplus c$;

4) $a \oplus b = \overline{b} \oplus \overline{a}$; 5) $a \oplus b = b*\overline{a} + a*\overline{b}$; 6) $a \oplus a*b = a*\overline{b}$;
$\overline{a \oplus b} = b \oplus \overline{a} = a \oplus \overline{b}$; $\overline{a \oplus b} = b*a + \overline{a}*\overline{b}$; $a \oplus \overline{a}*b = a + b$.

В приведённых соотношениях знак «+» обозначает логическое сложение, знак «*» – логическое умножение, знак «$\oplus$» – сложение по модулю 2.

В процессах формирования и декодирования циклического кода используется следующий прием: информационный полином $G(x)$

степени $(m-1)$, который надо закодировать, умножается на X^k, что соответствует сдвигу на k разрядов влево. Полученный таким образом полином $X^k \cdot G(x)$ делится на порождающий полином $P(x)$ для определения остатка $R(x)$, который будет иметь степень меньше k:

$$x^k * G(x) / P(x) = Q(x) \oplus [R(x) / P(x)].$$

Из этого выражения следует

$$x^k * G(x) = Q(x) * P(x) \oplus R(x)$$

или $F(x) = Q(x) * P(x) = x^k * G(x) \oplus R(x)$.

Полином $F(x)$ делится на $P(x)$ без остатка и поэтому является кодовым полиномом.

Остаток $R(x)$ имеет степень не больше k, а $X^k \cdot G(x)$ имеет нулевые коэффициенты в k младших членах. При этом m старших разрядов кода $F(x)$ равны коэффициентам информационного полинома $G(x)$ и представляют собой кодируемое сообщение, а младшие k коэффициентов кодового полинома $F(x)$ представляют собой коэффициенты остатка $R(x)$, т.е. контрольные биты. Из вышеизложенного следует, что кодовый полином можно получить путем сдвига информационного полинома на k бит, деления его на порождающий полином $P(x)$ и записи остатка в младшие k битов кодового полинома.

Процедура кодирования, соответствующая этому алгоритму, реализуется с помощью сдвигового регистра с обратными связями, соответствующими виду порождающего полинома $P(x)$.

Если полином, полученный при передаче сообщения, содержит ошибки, то он может быть представлен в виде $H(x) = F(x) \oplus E(x)$. Это выражение означает, что если полином принятого сообщения $H(x)$ не делится на $P(x)$, то при передаче произошла ошибка $E(x)$.

Выбор порождающего полинома $P(x)$ зависит от характера ошибок при передаче.

Алгоритм исправления ошибок в принятой кодовой комбинации $F(x)$ состоит в следующем. Принятую кодовую комбинацию делим на образующий полином, затем анализируем остаток. Если вес остатка (число единиц в коде остатка) равен 0, считается, что комбинация принята верно.

Если вес (количество единиц) остатка $W \neq 0$, делаем циклический сдвиг принятой комбинации влево на один разряд, снова делим

на $P(x)$ и анализируем остаток. Если $W > S$, где S – число исправляемых ошибок, снова делаем сдвиг влево на один шаг, делим на $P(x)$ и вновь анализируем остаток. Если $W > S$, продолжим сдвиг и анализ до тех пор, пока не получим $W \leq S$, при этом нужно считать число сдвигов. Пусть это было q сдвигов.

Последнее делимое (при котором было получено $W \leq S$) складываем с остатком, а затем полученную кодовую комбинацию подвергаем циклическому сдвигу вправо на q разрядов. Полученная кодовая комбинация будет точно соответствовать переданной, т.е. ошибка будет исправлена: $[F(x) = H(x)]$.

Пример. Пусть передаётся сообщение в виде полинома $F(x) = 1101001$, а адресат получает сообщение $F_1(x) = 1100001$. Образующий полином $P(x) = 1011$, число исправляемых ошибок $S = 1$.

Адресат при получении сообщения включает процедуру проверки, производя деление полинома F_1 на образующий полином $P(x)$:

$$1100001/1011 = 1111 + 1000/1011.$$

Анализ показывает, что остаток от деления не равен нулю и имеет вес, равный единице (в данном случае $W = S$).

Для исправления ошибки включается процедура исправления, согласно которой при $W = S = 1$ нужно делимое сложить с остатком (сложение делается по модулю 2) и получить исправленную комбинацию:

$$1100001 \oplus 1000 = 1101001.$$

Эффективность ЦК зависит от правильного выбора образующего кода. Существуют рекомендации по выбору числа корректирующих разрядов k.

Рекомендации по образованию циклических кодов:

1) В качестве образующих рекомендуется использовать следующие неприводимые полиномы от аргумента X :

$P(x) = x + 1$ соответствует двоичному коду 11;
$P(x) = x^2 + x + 1$ – двоичному коду 111;
$P(x) = x^3 + x^2 + 1$ – двоичному коду 1101;
$P(x) = x^3 + x + 1$ – двоичному коду 1011;
$P(x) = x^4 + x^3 + 1$ – двоичному коду 11001;
$P(x) = x^4 + x^2 + 1$ – двоичному коду 10101 и т.д.,

причём степень полинома должна быть на единицу меньше числа разрядов представляемого кода.

2) Выбор степени K образующего полинома определяется возможностью обнаружения и исправления ошибок. Например, если надо обнаружить и исправить одну ошибку (S = 1), то необходимо иметь код с минимальным кодовым расстоянием $d_o = 2S + 1 = 3$.

Если число информационных разрядов – m, то число контрольных разрядов k определяется из выражения

$$(2^k - k) \geq (m+1).$$

Кодовая комбинация, для которой выбирается образующий полином, будет содержать общее число разрядов n, равное сумме чисел информационных и контрольных разрядов: $n = m+k$, при этом $2^m \leq [2^n/(n+1)]$.

Из числа образующих полиномов следует выбирать по возможности более короткий, со степенью не менее K ($K = k - 1$) и числом ненулевых членов не менее d_0.

Пример. Пусть требуется закодировать одну из комбинаций 4-разрядного двоичного кода 1101, которому соответствует информационный полином $G(x)=x^3+x^2+1$. В качестве образующего выберем полином $P(x)=x^3+x+1$, которому соответствует двоичный код 1011. Согласно процедуре образования кодового полинома, умножаем информационный полином на x^K, где K – степень образующего полинома:

$$G(x)*x^K=(x^3+x^2+1)*x^3=x^6+x^5+x^3,$$

что соответствует двоичному коду 1101000. Теперь надо найти значения корректирующих разрядов. Для этого выполняем деление: $G(x)*x^K / P(x)$, или в двоичных кодах

$$1101000/\ 1011 = 1111 + (001/1011).$$

Остаток в виде 3-разрядного двоичного числа (001) записываем на место трёх младших разрядов кода 1101000, полученного ранее. В результате искомый кодовый полином будет иметь вид $F(x)$ = 1101001. Циклические коды эффективно используют матричные методы расчетов, что, в свою очередь, хорошо выполняется в вычислительной технике. В этих расчётах используют информационные, образующие, единичные матрицы [8].

В матричной форме построение образующей матрицы сводится к составлению единичной транспонированной матрицы и дополни-

тельной матрицы, элементы которой представляют собой остатки от деления единицы с нулями на образующий полином $P(x)$. При этом используются те остатки, вес которых $W \geq (d_o - 1)$. Длина остатков должна быть равна k, а число – m.

4.5. Контроль арифметических операций

Арифметические операции можно представить в виде таких действий, как передача слова, преобразование содержимого регистров: сдвиг, взятие обратного кода (инверсия), сложение.

В операции сдвига значение i-го разряда регистра передается в регистр с номером $(i + m)$ или $(i - m)$ в зависимости от направления сдвига (m – число разрядов, на которое делается сдвиг). Поэтому для контроля операции сдвига можно использовать те же методы, что и для контроля передачи информации (например, контроль четности количества единиц). При этом кроме схемы определения общей четности содержимого регистра необходимы схемы, устанавливающие четность разности между числом единиц, выдвигаемых из регистра и вдвигаемых в регистр.

Операция взятия обратного кода может быть также проконтролирована путем использования кодов с проверкой четности. Здесь используется следующее правило: если число информационных разрядов в слове четно, то число единиц в слове четно при четном числе нулей и нечетно при нечетном числе нулей. В этом случае после образования обратного кода четность числа единиц в слове сохраняется. Тогда, проверив сохранение четности суммы единиц в слове (включая контрольный разряд), можно сделать вывод о правильности взятия обратного кода.

Если число информационных разрядов в слове нечетно, то четному числу единиц в слове соответствует нечетное число нулей, а нечетному числу единиц – четное число нулей. В данном случае после образования обратного кода четность числа единиц изменится на обратную. Далее необходимо взять обратный код от содержимого контрольного разряда и проверить сохранение четности суммы единиц в слове (с учетом инвертированного контрольного разряда).

Способ сложения, использующий проверку четности. При сложении чисел a и b разряды суммы S образуются следующим образом:

$$S_1 = a_1 \oplus b_1 \oplus p_1;$$
$$S_2 = a_2 \oplus b_2 \oplus p_2;$$
$$\ldots\ldots\ldots\ldots\ldots$$
$$S_n = a_n \oplus b_n \oplus p_n ,$$

где S_i, a_i, b_i, p_i $(i = 1\ldots.n)$ – значения разрядов суммы, слагаемых и переноса, поступающего в i-й разряд. В этом случае результат сложения имеет вид:

$$S_1 \oplus S_2 \oplus \ldots \oplus S_n = (a_1 \oplus a_2 \oplus \ldots \oplus a_n) \oplus (b_1 \oplus b_2 \oplus \ldots \oplus b_n) \oplus (p_1 \oplus p_2 \oplus \ldots \oplus p_n).$$

Так как сумма по модулю 2 всех разрядов слова выражает четность суммы единиц слова, то *четность* S = *четность* a $\oplus$ *четность* b $\oplus$ *четность* p.

Следовательно, при правильном образовании суммы четность суммы единиц должна удовлетворять этому выражению. Однако при этом не будет обнаружено четное число ошибок. Распространение ошибки по многим разрядам суммы произойдет, если сбой имеет место в схеме формирования переноса. В связи с этим для полноты контроля необходимо проверять правильность образования переносов P_i. Это делается с помощью схемы, которая проверяет, что в каждом разряде существует либо перенос в прямом коде, либо инверсия переноса, но не существует одновременно и то и другое.

Другой способ контроля заключается в дублировании схем формирования переносов и сравнении переносов основной и дублирующей схем (рис. 4.8).

Оба слагаемых поступают на схемы формирования переносов и затем, после них – на схему контроля совпадения. Алгоритм проверки выполняется с помощью формирователей четности и переносов с последующей проверкой условия: *чётность* S = *четность* a $\oplus$ *четность* b $\oplus$ *четность p.*

Другой способ контроля выполнения арифметических операций (сложение, вычитание, умножение) осуществляется с помощью контрольных кодов, представляющих собой остатки от деления чисел на некоторое заданное число, называемое модулем q (*контроль по модулю q*).

Если в качестве контролируемого кода используется остаток R по модулю q, то в качестве контрольной операции над остатками может

быть выбрана та же арифметическая операция, которая производится над числами. Это основано на том, что для сложения, вычитания и умножения действительно соотношение

$$R_q(A \mathbin{@} B) = R_q\,[\,R_q(A) \mathbin{@} R_q(B)],$$

где $R_q(X)$ – остаток от деления числа X на число (модуль) q (кратко: остаток по модулю q);

@ – знак арифметической операции сложения, вычитания или умножения.

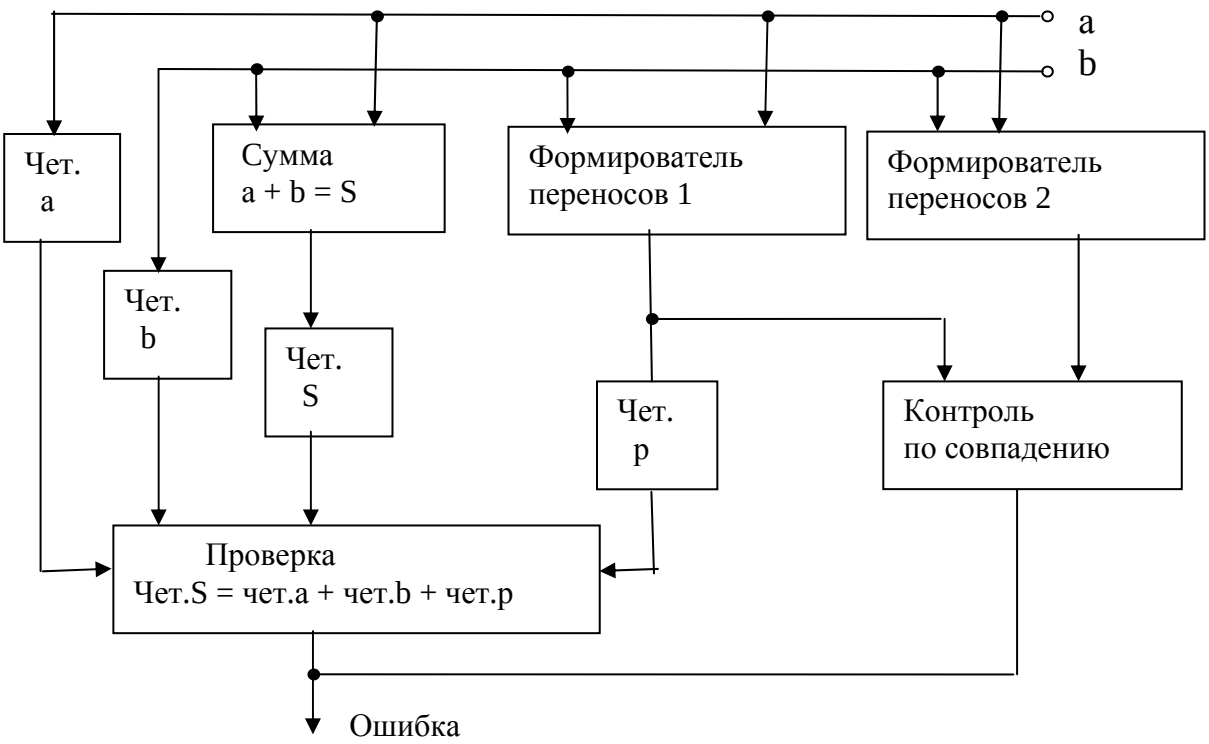


Рис. 4.8. Структурная схема контроля сумматора

Контроль арифметической операции по модулю организуется следующим образом. Каждому числу X, участвующему в операции, ставится в соответствие контрольный код – остаток $R_q(X)$. Одновременно с выполнением основной операции та же операция производится над их контрольными кодами, и контрольный код результата основной операции сравнивается с результатом операции над контрольными кодами исходных чисел. При несовпадении фиксируется ошибка. При этом чем меньше модуль q, тем меньше разрядность контрольного кода R и проще аппаратная реализация. Для двоичных чисел $q_{мин}$= 3, поэтому в ЭВМ часто используют контроль по модулю 3. Можно доказать, что при контроле по модулю 3 обнаруживаются любые оди-

ночные ошибки. Известно, что одиночная ошибка в каком-либо *i*-м разряде двоичного числа соответствует изменению числа на $\pm 2^i$. Для обнаружения ошибки необходимо, чтобы контрольные коды, образованные от чисел a и a $\pm$ 2^i, не совпадали. Действительно, $R_q(a) \neq R_q(a \pm 2^i) = R_q(a) \pm R_q(2^i)$ или $R_q(2^i) \neq 0$. Но 2^i – чётное число и не делится на 3 без остатка, следовательно, требуемое условие выполняется. Кроме одиночных ошибок при контроле по модулю 3 обнаруживается и часть двойных ошибок – те, при которых правильный и ошибочный результаты имеют несовпадающие остатки R_q от деления на $q = 3$. Структурная схема сумматора с контролем по модулю 3 показана на рис. 4.9.

Может применяться контроль по модулю с бóльшим основанием, чем 3.

Значение модуля выбирается из следующих соображений:

1) любая одиночная ошибка должна приводить к нарушению условия

$$R_q(A \mathbin{@} B) = R_q [\, R_q(A) \mathbin{@} R_q(B)];$$

2) операция деления на q для определения остатка $R_q(X)$ должна осуществляться сравнительно несложными средствами.

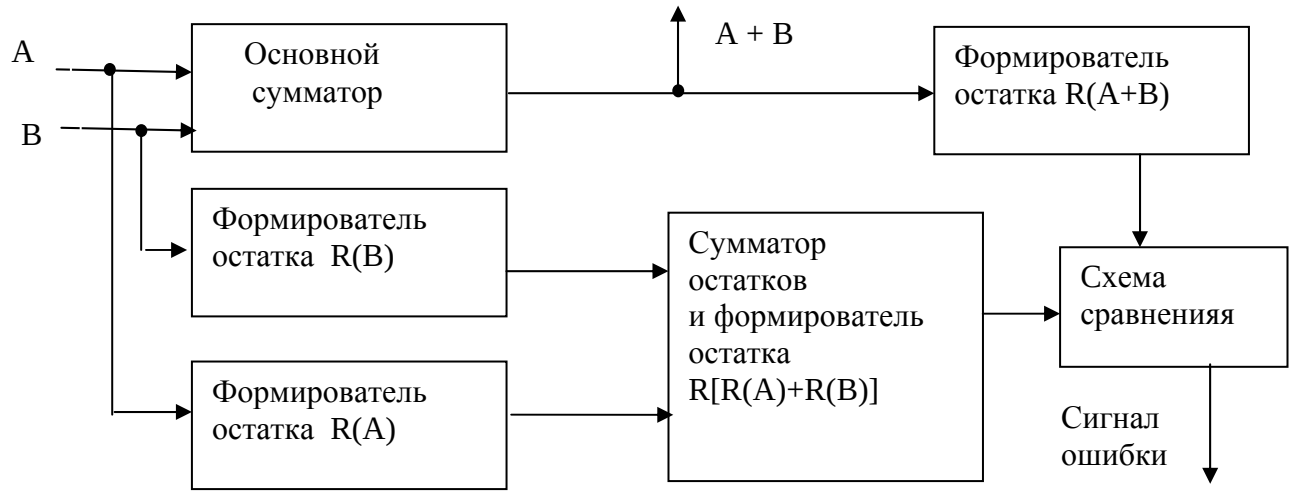


Рис. 4.9. Структурная схема контроля арифметического сумматора

Первому условию удовлетворяют модули $q = 2^S - 1$, где S – показатель степени (S = 1, 2, 3…) – целое число.

По второму условию нужно брать S как можно меньше, так как чем меньше модуль q, тем меньше разрядность контрольного кода и проще аппаратура. Метод нахождения остатков по модулю q от

двоичных чисел осуществляется разбиением информационного слова на группы по S разрядов с последующим арифметическим суммированием и определением остатка по модулю q. Если S = 2, то исходное слово разбивается на диады, S = 3 – на триады, S = 4 – на тетрады и т.д.

Пример. Необходимо определить двоичный код остатка по модулю 3 4-разрядного слова 1011.

Решение:

$R_3(1011) = R_3(10 + 11) = R_3(2+3) = R_3(5) = 2$, что соответствует двоичному коду 010. Здесь $R_3(X)$ обозначает операцию нахождения остатков от деления чисел на модуль 3. Число было разбито на диады, так как $3 = 2^2 - 1$. Диады были заменены их десятичными значениями, их сумма поделена на 3, и остаток от деления получен в десятичном исчислении.

4.6. Некоторые способы контроля комбинационных схем

Контроль с помощью дублирующей схемы. Контроль дублированием состоит в побитном сравнении выходных сигналов основной и дублирующей комбинационных схем (КС) с последующим объединением одноимённых выходных сигналов в один сигнал ошибки с помощью схем сложения по модулю 2 (рис. 4.10).

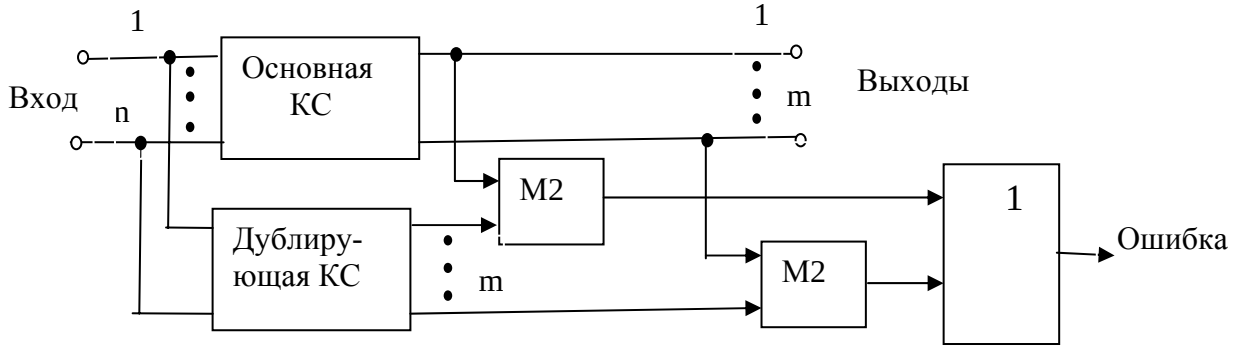


Рис. 4.10. Схема контроля комбинационной схемы дублированием

Формулы для определения сигнала ошибки будут иметь следующий вид:

$$F_{ош} = (x_i \oplus y_i) \vee (x_{i+1} \oplus y_{i+1});$$

$$F_{ош} = (x_i \oplus y_i)(x_1 \oplus y_1) \vee (x_2 \oplus y_2) \vee ...(x_m \oplus y_m).$$

Используется основное свойство логической функции «ИСКЛЮЧАЮЩЕЕ ИЛИ», согласно которому $a \oplus a = 0$.

Недостаток такого способа контроля состоит в том, что нужно иметь дублирующую схему.

Контроль путем проверки особенностей выходных сигналов. Этот метод эффективен для дешифраторов. Для реализации метода выходы дешифратора делятся на четную и нечетную группы, объединяемые в своих группах через элементы ИЛИ, выходы которых подключены к входам схемы сложения по модулю 2 (рис. 4.11). Используется тот факт, что по принципу действия дешифратора сигнал «1» должен быть только на его одном выходе.

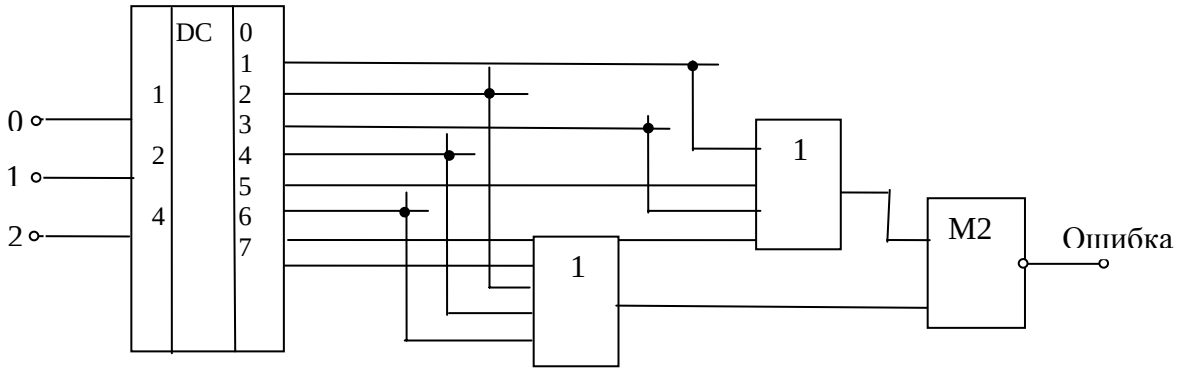


Рис. 4.11. Схема контроля дешифратора

Недостаток состоит в том, что не будут обнаружены ошибки, приводящие к появлению сигналов на двух и более выходах, относящихся к одной и той же группе (четной или нечетной), так как ошибка зафиксируется как одиночная.

4.7. Понятие о самопроверяемых схемах контроля

Необходимость проверки самих схем контроля очевидна. Для этого применяют самопроверяемые схемы контроля – диагностические средства проверки схем контроля. Схема контроля (СК) называется самопроверяемой, если она обнаруживает не только неисправности контролируемого устройства (КУ), но и свои собственные [9]. Схема контроля с двумя выходами (f_1, f_2) является полностью самопроверяемой, если она обладает свойствами:

– самотестируемости. Все неисправности СК из заданного класса проявляются на выходах f_1, f_2 в виде пары сигналов со значениями 00 и 11;

– защищенности от неисправности. Каждая неисправность из заданного класса проявляется на выходах f_1, f_2 только в виде пары сигналов со значениями 00 и 11 [9].

При построении самопроверяемой схемы контроля следует учесть требование раздельной реализации функций f_1, f_2; это гарантирует, что любая одиночная константная неисправность на входах и выходах СК не приведет к инвертированию сигналов на обоих выходах схемы. Значение сигналов 01, 10 на выходах f_1, f_2 свидетельствует о правильном функционировании КУ и СК, а значения 00, 11 – о наличии одиночной неисправности в КУ или СК.

Пример. Рассмотрим схему контроля по нечетности байтового регистра, имеющего восемь информационных и один контрольный бит (рис. 4.12). Схема с самоконтролем состоит из двух отдельных СК, реализующих следующие функции:

$$f_1 = X_1 + X_2 + X_3 + X_4; \qquad f_2 = X_5 + X_6 + X_7 + X_8 + C_k.$$

Рис. 4.12. Пример самопроверяемой схемы

Поскольку любая входная информация должна иметь нечетное число единиц (контроль по нечетности), то одна из групп обязательно будет содержать четное число единиц, а другая – нечетное. Следовательно, выходной сигнал f_1 f_2 должен иметь значение 01 или 10.

При появлении одиночной ошибки на входе общее число единиц станет четным (нечетным) и обе группы создадут на выходе выходной сигнал 00 или 11 (табл. 4.2).

Другим примером использования самопроверяемой схемы является схема контроля дешифратора (рис. 4.13).

Таблица 4.2

Процесс обнаружения неисправности

Состояние входов $M2_1$	Состояние входов $M2_2$		f_1	f_2
	Инф.	$C_к$		
1	2	3	4	5
Чет.	Чет.	1	0	1
Чет.	Нечет.	0	0	1
Нечет.	Чет.	0	1	0

Окончание табл. 4.2

1	2	3	4	5
Нечет.	Нечет.	1	1	0
Нечет.	Чет.	1	1	1
Нечет.	Нечет.	0	1	1
Чет.	Чет.	0	0	0
Чет.	Нечет.	1	0	0

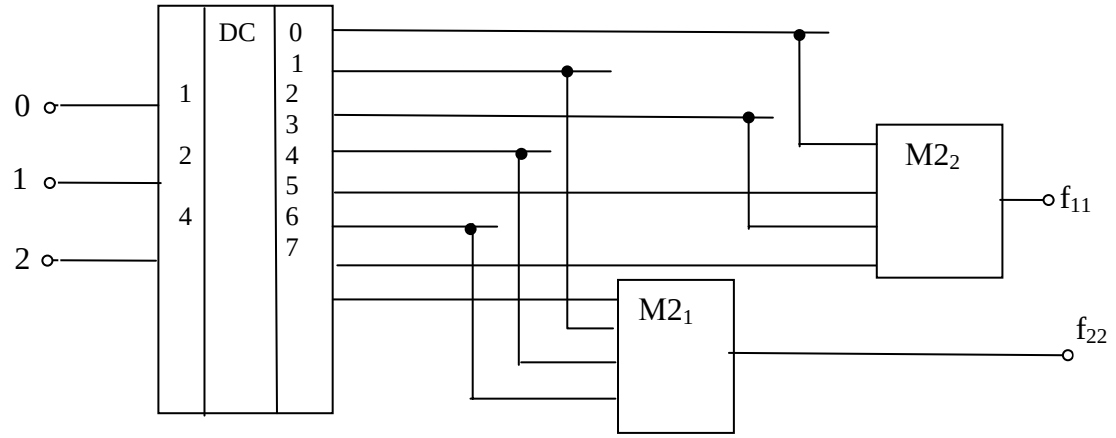


Рис. 4.13. Использование самопроверяемой схемы для контроля работы дешифратора

Для объединения сигналов с выходов схем контроля с целью формирования общего сигнала ошибки применяют самопроверяемые схемы сжатия (СЖ). Например, сигналы от двух самопроверяемых СК с помощью схемы логики можно объединить в один сдвоенный выходной сигнал (табл. 4.3 и рис. 4.14).

Если на одном из входов схемы сжатия сигналы f_1, f_2 принимают значения 00 или 11, то сигнал на её выходе также будет свидетельствовать о наличии ошибки.

Таблица 4.3

Сигналы на входах и выходе СЖ

f_{11}	f_{12}	f_{21}	f_{22}	f_{31}	f_{32}
0	0	0	0	0	0
0	0	0	1	0	0
0	0	1	0	0	0
0	0	1	1	0	0
0	1	0	0	0	0
0	1	0	1	1	0
0	1	1	0	0	1
0	1	1	1	1	1
1	0	0	0	0	0

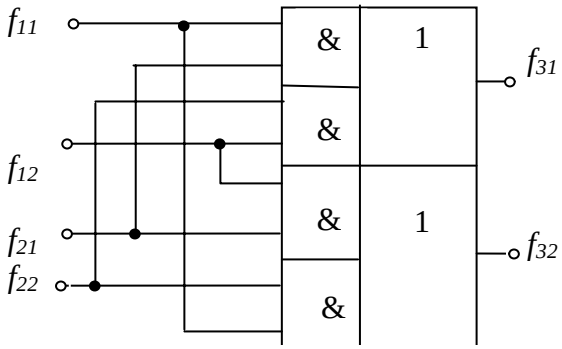


Рис. 4.14. Схема сжатия выходной информации от двух самопроверяемых схем

Прерывания от схем контроля. В ЭВМ предусматривается регистр ошибок, который служит для фиксации ошибок, обнаруженных средствами контроля логического и функционального уровней. После фиксации ошибки должен производиться анализ типа ошибки, по которому формируют условия прерывания от схемы контроля.

В зависимости от вида ошибки условия прерывания разделяют на *подавляемые* и *неотложные*. Прерывание от средств контроля дает сигнал операционной системе о сбоях и отказах в аппаратуре, месте и степени повреждения. Прерывание от СК, вызванное подавляемым условием, не прекращает выполнения текущей команды и осуществляется после того, как нормально закончится выполнение и обработка более приоритетных прерываний.

При неотложных условиях прерывания от СК выполнение текущей команды прекращается и отменяются другие прерывания.

Код прерывания должен содержать тип ошибки и степень повреждения.

Прерывание от СК запускает программы обработки ошибки, входящие в состав операционной системы, которые на основании полученной информации пытаются восстановить вычислительный процесс.

Некоторые способы независимой проверки схем контроля. Существуют следующие способы проверки СК:

- введение информации с заведомо неправильной четностью в информационные каналы;
- имитация ошибок в самих схемах контроля четности;
- имитация ошибок в схемах контроля путем дублирования;
- имитация одиночных и двойных ошибок в ОЗУ;
- имитация ошибок в общем регистре ошибок.

5. МОДЕЛИ НЕИСПРАВНОСТЕЙ И АЛГОРИТМИЧЕСКИЕ МЕТОДЫ ДИАГНОСТИРОВАНИЯ

5.1. Уровни описания объектов и моделирование неисправностей

Тестирование лежит в основе процессов диагностирования и профилактических испытаний. Тестирование делается во время испытаний, которые могут быть статическими и динамическими. Статические – это испытания, при которых частота тестовых воздействий значительно меньше частот реальных воздействий при работе устройства. При динамических испытаниях обе частоты соответствуют друг другу.

Испытания могут быть функциональными и параметрическими. Функциональные испытания предусматривают проверку соответствия функционирования устройства заданному алгоритму. Параметрические испытания связаны с контролем токов, напряжений, формы и длительности импульсов, сопротивлений резисторов, ёмкостей конденсаторов и т.п. Объектами тестирования могут быть четыре вида (уровня) объектов [10]:

– отдельные логические схемы;

– устройства, такие как ЦП, ОЗУ, ПЗУ;

– архитектурные свойства вычислительных устройств;

– системные свойства изделия, т.е. совокупное функционирование всех устройств как единого целого.

При вычислении тестов каждого уровня используются модели (описания) устройств – объектов тестирования. *Уровни описания* могут быть разные: *схемный, функциональный* (микрооперационный или регистровых передач), *алгоритмический*, или *архитектурный*, *системный*. Каждый уровень описания имеет свой язык описания.

Большинство неисправностей, возникающих при эксплуатации электронных средств, представляют собой *замыкание линий* на землю или на линию напряжения питания, *короткое замыкание* между сигнальными линиями, *обрывы*, *отсутствие резисторов*, *пробои* транзисторов, *низкий коэффициент* усиления, чрезмерное *увеличение задержек*. Неисправности могут быть *одиночными* или *кратными*.

Для разработки и вычисления тестов физические неисправности могут быть представлены их логическими моделями на уровне логических схем.

Используются следующие модели неисправностей:

1) *константные неисправности*. Для них моделируют постоянные 0 или 1 на входах или выходах логических схем, обозначая соответственно К0 (константа 0) и К1 (константа 1). Например, в линии «а» неисправности К0 и К1 обозначают следующим образом: a/0, a/1;

2) *короткие замыкания* (КЗ). Обычно моделируют КЗ между сигнальными проводниками схем. При этом приходится в модели вводить дополнительную схему.

Например, исходная схема содержит два логических элемента с тремя входными линиями каждый (рис. 5.1). Составим моделирующую схему, позволяющую однозначно определить замыкание входных линий.

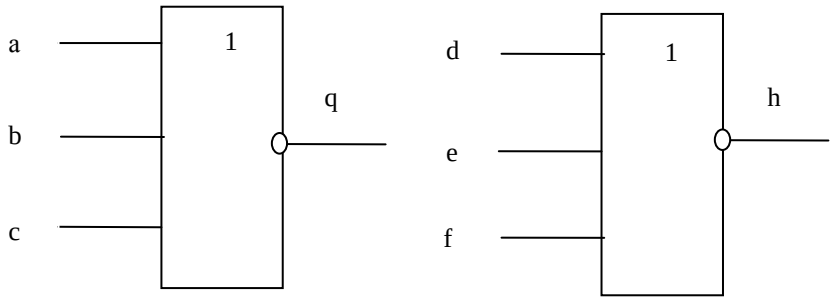


Рис. 5.1. Исходная схема для моделирования замыкания линий

Если замыкают между собой, например, c и d, то схему моделирования можно представить в ином виде (рис. 5.2).

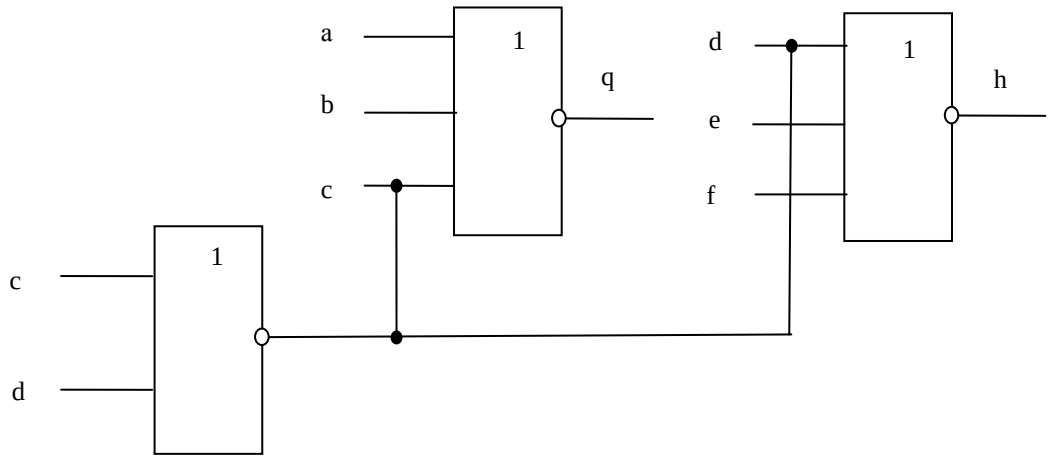


Рис. 5.2. Моделирование замыкания введением дополнительной схемы

Таблицы сигналов имеют следующий вид:

	Входы						Выходы	
	a	b	c	d	e	f	q	h
Исправная схема	0	0	1	0	0	0	0	1
Неисправная схема	0	0	0	0	0	0	1	1

Сравнение таблиц показывает, что неисправность вида КЗ обнаруживается с помощью моделирующей схемы.

Константные неисправности и короткие замыкания называют статическими, они обнаруживаются при статическом тестировании. Для уровня логических схем чаще всего используют простейшие модели (КЗ, К0, К1).

Описание схем на уровне логических вентилей часто оказывается сложным и громоздким. По мере роста степени интеграции резко увеличивается машинное время для вычисления тестов и моделирования неисправностей. Машинное время $t = kn^3$, где n – число вентилей (логических элементов). Кроме того, с ростом числа вентилей уменьшается полнота проверки (при числе вентилей 1000 полнота проверки становится равной примерно 90 %). Еще один недостаток описания на уровне логических схем – это то, что детали структуры БИС чаще всего неизвестны для разработчика тестов.

Чтобы преодолеть эти недостатки (обойти их), используют другой (более высокий) уровень описания, в котором в качестве элемента описания используют не вентили, а функциональный узел. Этот уровень называют *функциональным* (микрооперационным или уровнем регистровых передач). При этом используется графовая модель процессоров и других устройств. В ней модель устройства представляет собой граф, вершины которого соответствуют регистрам, сумматорам, функциональным преобразователям, информационным входам и выходам, а ребра определяют пути передачи информации. Модели неисправностей функционального уровня описания определяют множество *функциональных неисправностей*, идентичных по своим свойствам множеству константных неисправностей.

Модели неисправностей на функциональном уровне могут быть обозначены, например, следующим образом:

- в дешифраторе выборки регистра:

- функция $f(R_i / 0)$ – регистр R_i не выбирается;
- функция $f(R_i / R_j)$ – вместо регистра R_i выбирается R_j;
- функция $f(R_i / R_i + R_j)$ – кроме R_i, выбирается ещё и R_j;

- для дешифратора микроопераций:

• функция $f(m_i / 0)$ – микрооперация не активируется;

• функция $f(m_i / m_j)$ – вместо m_i активируется m_j;

• функция $f(m_i / m_i + m_j)$ – кроме m_i, активируется ещё и m_j;

- для регистров и трактов передачи данных:

• неисправность типа К0 и К1 у триггеров и К1, К0, КЗ для линии передачи данных.

Следующий уровень описания – *архитектурный*, или алгоритмический. Описание задается на языке высокого уровня либо граф-схемой алгоритма (ГСА), либо граф-схемой команд. Моделями неисправностей в этом случае являются неисправности аппаратуры и ошибки разработки, приводящие к неверному результату выполнения команд.

Системный уровень описания характеризует совокупное поведение всех устройств, их взаимодействие во времени.

На алгоритмическом и системном уровнях описание вычисления тестов используется чаще всего не для обнаружения конкретных неисправностей или их сочетаний, а для проверки правильности функционирования алгоритма или системы при возможных сочетаниях операндов.

5.2. Методы генерации тестовых воздействий при тестировании и виды сжатых эталонов

В процессе тестирования используются различные методы генерации тестовых воздействий.

Детерминированный метод генерации – это вычисление совокупности тестовых наборов для определения какой-либо неисправности из общего списка, моделирование схемы на этом наборе для выявления подмножества неисправностей и повторение этой процедуры до исчерпания списка неисправностей.

Исчерпывающая генерация – подача на входы устройства всех возможных тестовых наборов.

Вероятностная генерация – формируются случайные тестовые наборы, например от датчика случайных чисел.

Процесс тестирования может быть организован в виде одной из двух процедур:

- *компактное тестирование*, т.е. тестирование со *сжатием* результатов;

- *исчерпывающее тестирование*, которое позволяет обойтись без моделей неисправностей и не требует сложных методов вычисления тестов. Недостаток – при большом числе входов время на перебор комбинаций становится продолжительным.

При компактном тестировании результаты сжимаются и сравниваются со сжатым эталоном. Основные виды *сжатых эталонов*: функции счета, контрольные суммы, синдром и сигнатура.

1. *Функции счета (ФС).*

Использование ФС можно пояснить схемой детерминированного компактного тестирования дискретного устройства (ДУ) с использованием этих функций (рис. 5.3).

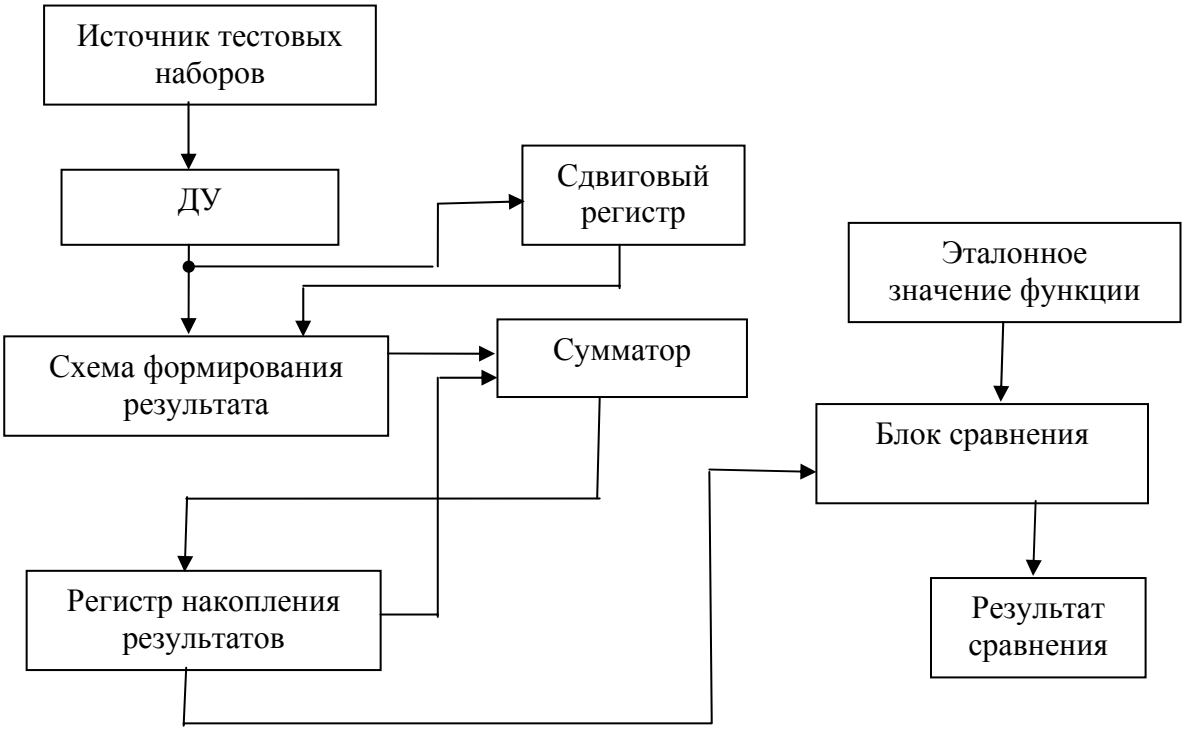


Рис. 5.3. Структурная схема процесса тестирования дискретного устройства

Тестируемое устройство имеет один выход. На вход ДУ подается последовательность тестовых наборов. Сдвиговой регистр, имеющий m разрядов, хранит m последних результатов $R_i = [r_i, r_{i+1},\ldots r_{i+m-1}]$. Значение m – число последовательных результатов, подвергаемых анализу с целью определения наличия и числа интересующих признаков в последовательности. Этот анализ делает схема формирования результата, на выходе которой формируется текущее значение $C_m(R_i)$ соответствующей функции счета. Сумматор далее

вычисляет $S_m(R_i) = C_m(R_i) + S_m(R_{i-1})$, где $S_m(R_{i-1})$ – предыдущее суммарное значение функции счета, накопленное в регистре накопления. Окончательное значение функции счета сравнивается с эталонным значением этой суммы.

Разновидности функций счета:

- ФС единичных значений результата;
- ФС числа переходов (изменений значений) результатов от 0 к 1 и от 1 к 0;
- ФС числа повторений значений результатов;
- ФС числа фронтов (изменений от 0 к 1);
- ФС числа срезов (изменений от 1 к 0).

Эффективность компактного тестирования с помощью ФС зависит как от выбора вида ФС, так и от тестовой последовательности.

2. *Контрольные суммы (КС).*

Использование контрольных сумм предполагает рассмотрение совокупности результатов тестирования как массива чисел, над которым выполняется операция поразрядного или арифметического суммирования.

Пусть есть упорядоченное множество n m-разрядных чисел {Ui}, где i = 1, 2,..n – число, соответствующее выходной последовательности ДУ. Можно использовать следующие способы суммирования:

а) поразрядное суммирование по mod 2;

б) арифметическое суммирование по различным модулям, причём $M = n\,(\,2^m - 1\,)$ – полная арифметическая сумма; $M = 2^m$ – арифметическая сумма без учета переноса из старшего разряда; $M = 2^m - 1$ – арифметическая сумма с циклическим переносом в младший разряд.

Полученная в результате тестирования сумма сравнивается с эталонной, определённой (вычисленной) заранее для заведомо исправной схемы.

3. Синдром.

Синдром булевой функции – это число, связанное с числом входов и минтермов функции $S = K / 2^n$, где K – где число минтермов функции; n – число входов проверяемой схемы. Минтермы – это произведения логических переменных, отличающиеся хотя бы одним сомножителем. Синдром используется для тестирования комбинационных схем и требует полного перебора комбинаций логических переменных на входах схемы.

По формуле $S = K / 2^n$ можно определить синдром только для простых одновыходных схем (рис. 5.4).

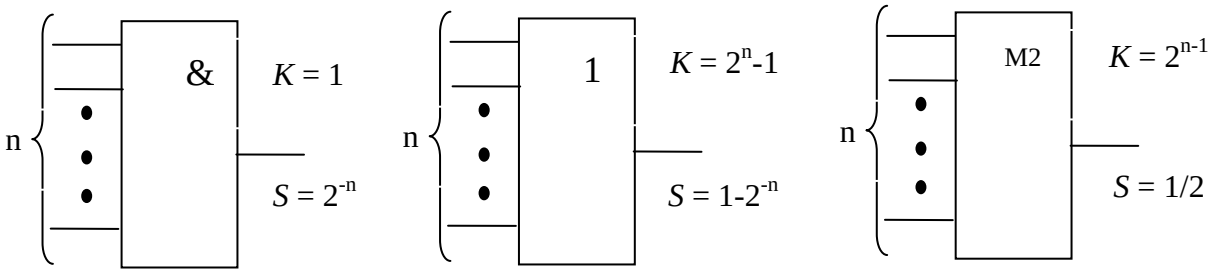


Рис. 5.4. Примеры вычисления синдромов для логических элементов

Пример вычисления синдрома булевой функции, реализуемой схемой с несколькими логическими элементами, приведён на рис. 5.5.

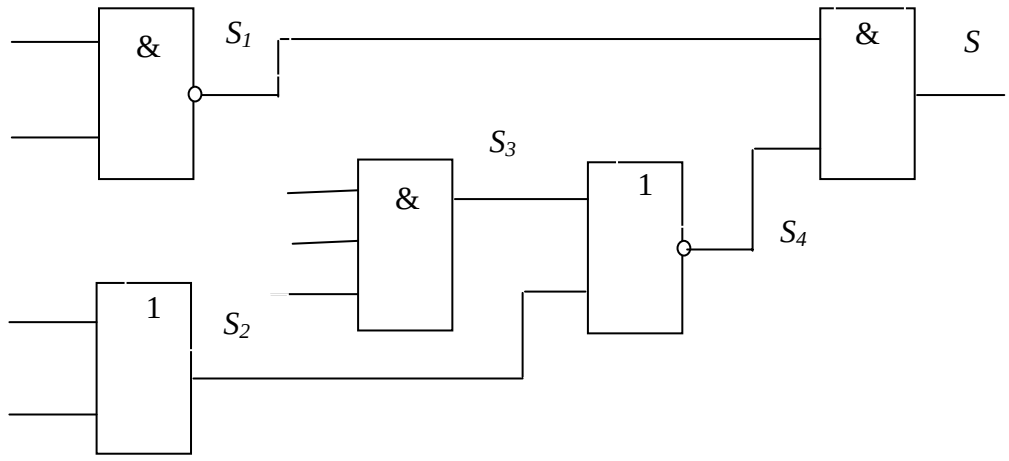


Рис. 5.5. Схема, для которой вычисляется синдром *S*

Синдромы рассчитываются по следующим выражениям:
$S_1 = 1 – 2^{-2}$; $S_2 = 1 – 2^{-2}$; $S_3 = 2^{-3}$; $S_4 = 1 – (S_2 + S_3 – S_2S_3)$;
$S = S_1S_4 = 21 / 128$.

Согласно определению синдрома, из численного значения синдрома рассматриваемой схемы *S* получаем значения $K = 21$, $2^n = 128$ или $n = 7$.

Синдромное тестирование комбинационных схем может быть представлено в виде функциональной схемы (рис. 5.6).

Счетчик синдрома подсчитывает число единиц на выходе проверяемой схемы, так как число *K* (число минтермов) – это число единичных результатов на выходе схемы при подаче на вход полного набора переменных.

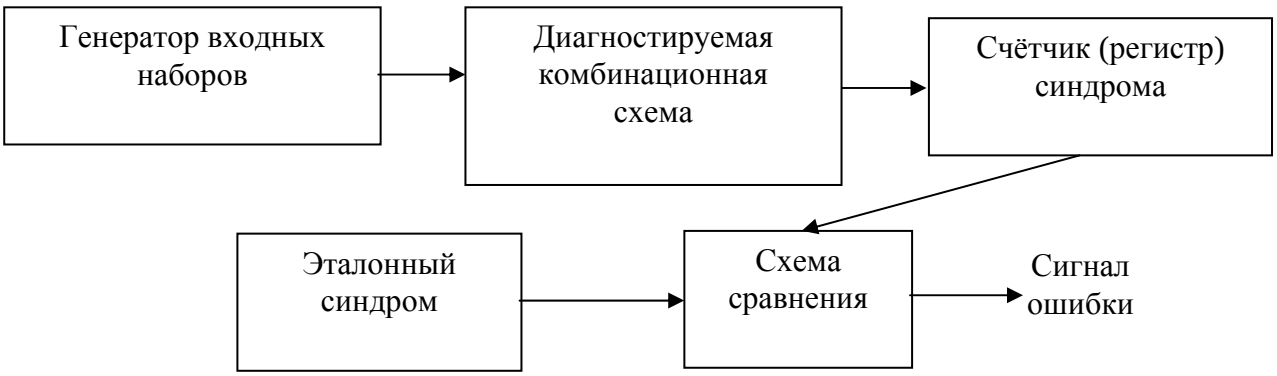


Рис. 5.6. Функциональная схема синдромного тестирования

Комбинационная схема должна быть спроектирована так, чтобы синдром исправной схемы отличался от синдрома неисправной. Для уменьшения длины тестов, равной 2^n, комбинационная схема разбивается на подсхемы, каждая из которых должна иметь свой синдром. Синдромное тестирование используется при исчерпывающем компактном тестировании.

4. Сигнатура.

Сигнатура, как один из видов сжатых эталонов, используется для диагностики сложных устройств в процессе контроля с помощью сигнатурного анализа.

Сигнатурный анализ предполагает использование циклических избыточных кодов для сжатия длинных двоичных кодов (реакций цифровых устройств (ЦУ) на тестовые последовательности) в короткий (4-5) разрядный шестнадцатеричный код, который индицируется и сравнивается с указанным в документации контрольным кодом для каждой контролируемой точки. Этот контрольный код называют *сигнатурой*.

При сигнатурном анализе применяется принцип сжатия информации с использованием характеристических полиномов.

Исчерпывающее тестирование ЦУ методом сигнатурного анализа. В основе метода лежит использование циклических кодов для сжатия двоичных длинных кодов (являющихся реакциями ЦУ на тестирование) в более короткий шестнадцатеричный код, который

индицируется и сравнивается с кодом, указанным в документации. Код, указанный в документации, является эталонным (*эталонная сигнатура*).

Циклический код строится следующим образом. Информационная комбинация *A(x)* делится на образующий полином *G(x).* Операция *A(x)/G(x)* выполняется на сдвиговом регистре с обратными связями. Остаток (содержимое регистра сдвига) и есть сжатый результат тестирования, т.е. сигнатура. Сравнивая ее с эталонной (расчетной), делают вывод об исправности ЦУ.

Пример. Необходимо определить сигнатуру для исправного ЦУ при выдаче с него результатов тестирования в виде 20-битной последовательности FC1FF, т.е. *A(x)*= 1111 1100 0001 1111 1111.

В качестве регистра сдвига используется 16-разрядный регистр с обратными связями (рис. 5.7).

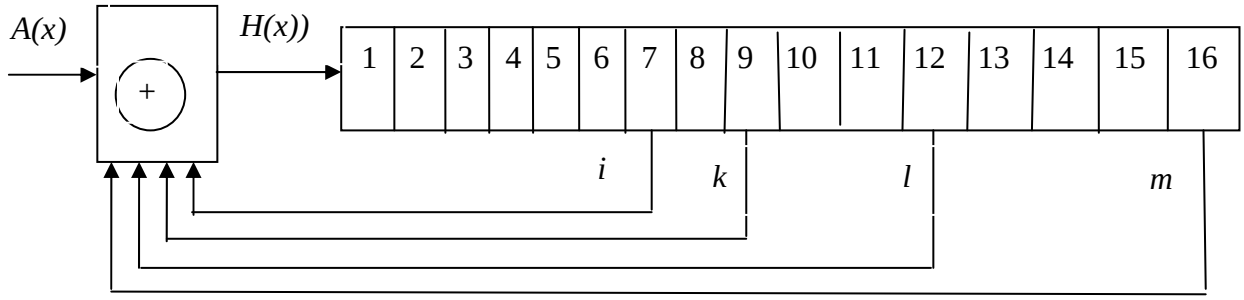


Рис. 5.7. Упрощенная функциональная схема деления полиномов *A(x)/G(x)*

На схеме *H(x)* – промежуточный результат, образующийся на выходе сумматора по модулю 2. Это последовательность битов, подаваемых с каждым тактом на вход первого триггера сдвигового регистра.

Отводы обратных связей регистра сдвига, соответствующие ненулевым коэффициентам при степенях *x* многочлена *G(x),* через сумматор по mod 2 подаются на входной регистр вместе с контролируемой функцией.

В регистре сдвига обеспечивается деление $A(x)/G(x) = X^m + X^l + X^k + X^i + 1$, где *m, l, k, i* – соответственно старший и промежуточные разряды.

Для образования сигнатуры потребуется *n* тактов (*n* = 20). Число разрядов *N* в регистре сигнатурного анализатора выбирается из соотношения

$$N = J \cdot] \log_2 K [,$$

где *J* – ожидаемая кратность ошибки в контролируемой последовательности;

K – число битов в этой последовательности.

Алгоритм использования сигнатуры при диагностике устройств может иметь следующий вид (рис. 5.8).

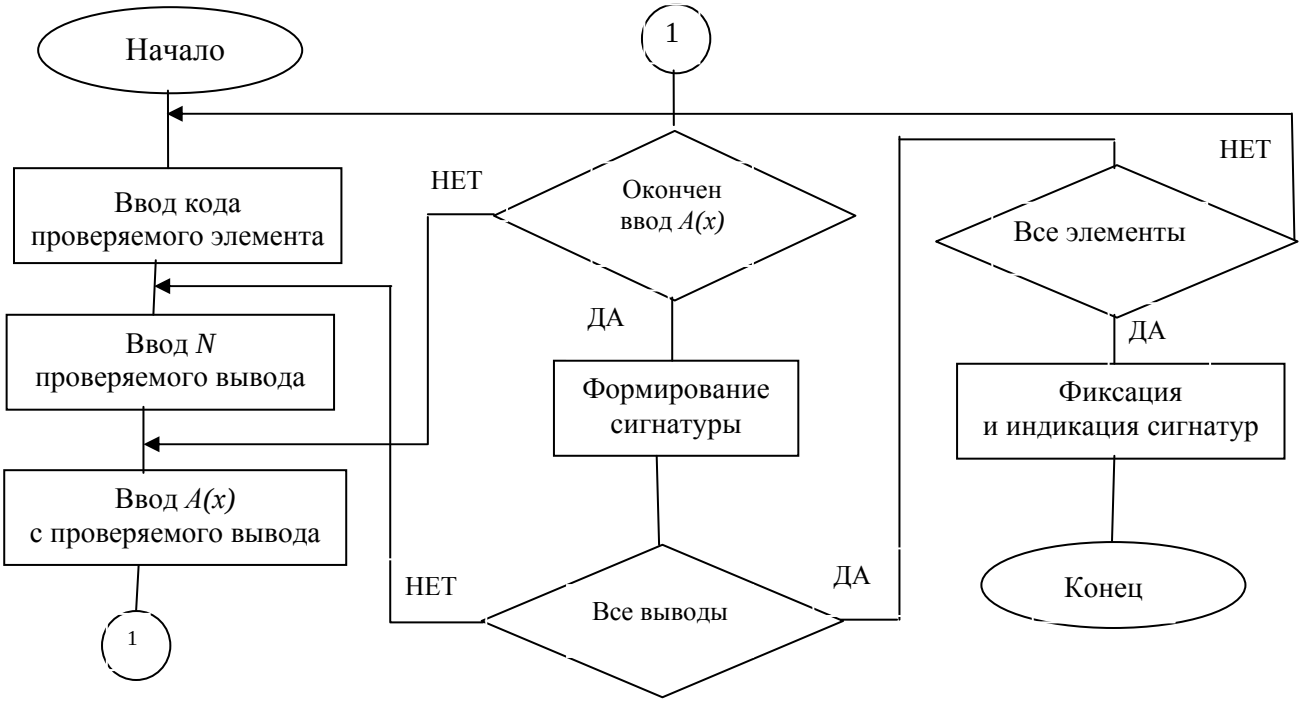


Рис. 5.8. Алгоритм процесса образования сигнатур при диагностике

Сигнатурный анализ основан на следующих алгебраических соотношениях:

1) если $f(x)$ – входная последовательность, $q(x)$ – образующий полином, а $R(x)$ – остаток, то $f(x)/q(x) = A(x) + R(x)/q(x)$, откуда $f(x) = A(x) \cdot q(x) + R(x)$;

2) образующий полином $q(x)$ (степени n) должен иметь число ненулевых членов, большее или равное $(2J + 1)$.

Например, для $n = 16$ можно образовать семь полиномов с минимальным числом членов, равным 5, при $J = 2$.

Вероятностное тестирование. Функциональная схема вероятностного тестирования сравнивает в режиме реального времени реакции диагностируемого и эталонного устройств на тестовые наборы, подаваемые одновременно на их входы (рис. 5.9).

Вероятностное компактное тестирование, как и обычное, выполняется за два или три шага в зависимости от того, какая схема – комбинационная или с памятью. Для схем с памятью на первом шаге производится инициализация, т.е. установка схемы в исходное состо-

яние путем подачи на вход последовательности заданных чисел. Следующие два шага – накопление результатов и сравнение со сжатым эталоном.

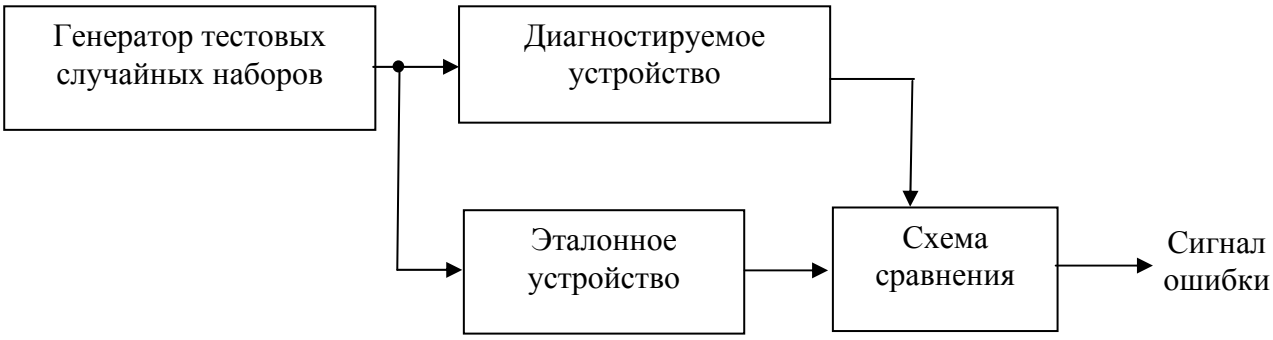


Рис. 5.9. Функциональная схема вероятностного тестирования

При вероятностном тестировании проверяемая схема считается исправной, если результат отличается от эталона на заданную величину Δ, называемую допустимым отклонением (рис. 5.10). Отклонение может возникать из-за сжатия результатов и неодинакового начального состояния тестируемых схем.

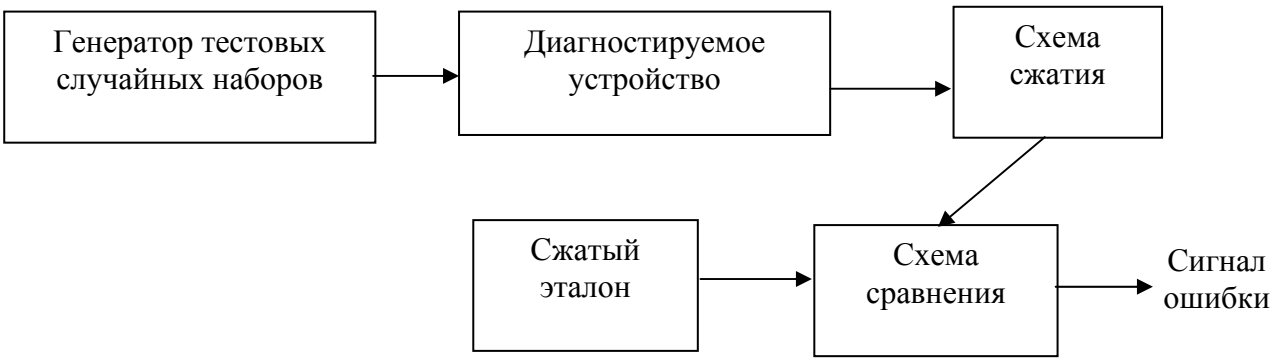


Рис. 5.10. Функциональная схема вероятностного тестирования со сжатым эталоном

Одним из наиболее распространенных способов сжатия результата является функция счета числа единиц. В данном случае для комбинационной схемы в качестве среднестатистического эталона используется вероятность появления единичного логического уровня на выходе схемы. Эта вероятность зависит от вероятностей появления единичных сигналов на входах схемы и определяется параметрами генератора случайных наборов.

5.3. Тестирование запоминающих устройств

Контроль функционирования ОЗУ. Около половины интенсивности потока ошибок ЭВМ приходится на долю оперативных запоминающих устройств (ОЗУ). ОЗУ большой емкости – это динамические полупроводниковые ОЗУ, имеющие в несколько раз бóльшую емкость, чем статические. Причиной постоянных неисправностей в ОЗУ являются отказы интегральных схем (ИС), а случайных – изменение содержимого ОЗУ, например, из-за скачков напряжения питания, помех, воздействия α-частиц. Неисправности ОЗУ проявляются как неисправность одного разряда (бита), неисправность шины выборки разряда, неисправность шины выборки слова, неисправность обеих шин, неисправность всей ИС.

Повышение надежности ОЗУ достигается использованием алгоритмов проверки с помощью корректирующих кодов. Широко распространены коды с коррекцией одиночной и обнаружением двойной ошибки. Наиболее известным среди этих кодов является код Хэмминга.

Общие методы контроля и диагностики запоминающих устройств. Функциональный контроль ЗУ решает две задачи диагностики:

- установление факта наличия неисправности;
- определение места неисправности.

Основную функцию выполняет генератор тестов, который должен формировать последовательности тестирующих и опорных сигналов по заданному закону (рис. 5.11). Тест – последовательность этих сигналов.

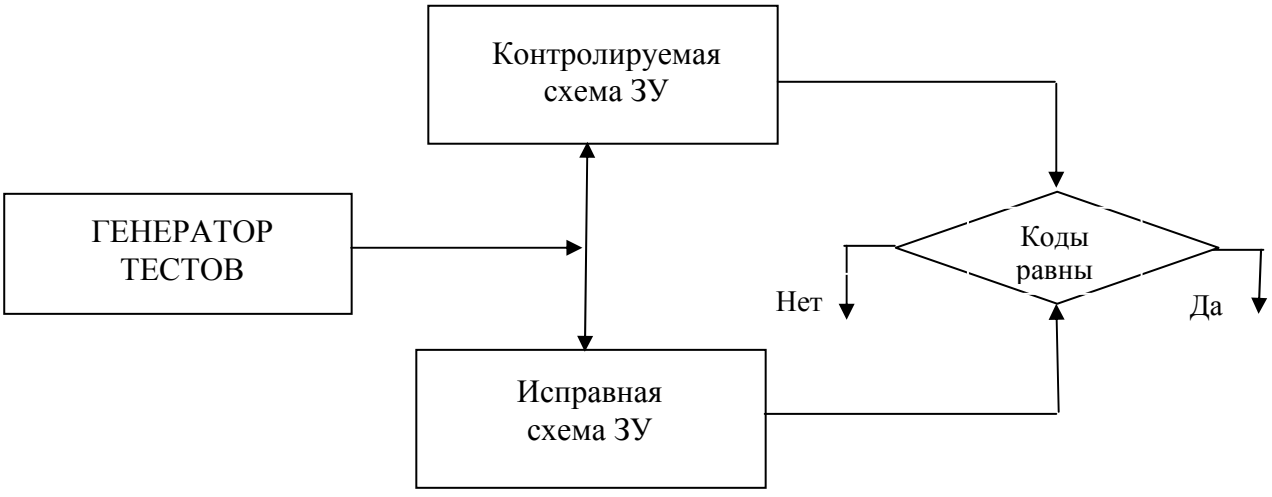


Рис. 5.11. Структурная схема функционального контроля ЗУ

Наборы входных сигналов (машинные слова – коды) будут определять порядок обращения к элементам памяти и последовательность выполняемых операций. При этом следует иметь в виду, что математические адреса элементов памяти в общем случае могут не совпадать с их физическими координатами. Это важно при анализе отказов БИС ЗУ.

Эквивалентность выходных и эталонных сигналов устанавливается путем логического сравнения: если сигналы эквивалентны, можно считать, что функционирование правильно.

Эффективность ФК решающим образом определяется построением теста, поэтому используются различные способы генерации тестовых последовательностей. Наиболее эффективными, но самыми затратными являются тесты «Пинг-Понг» и «Галопирующий».

Алгоритмические методы тестирования микросхем ОЗУ и ПЗУ. При диагностировании ОЗУ применяются разнообразные виды тестов [11]:

«*Все нули (все единицы)*». Во все ячейки ОЗУ производится запись нулей (единиц), после чего осуществляется последовательное считывание и проверка этой информации.

Тест «Адресный». В каждую ячейку ОЗУ записывается код собственного адреса, затем осуществляется последовательное считывание
и проверка этой информации. Этот тест обеспечивает проверку адресных дешифраторов ОЗУ.

Тест «Шахматный». В ОЗУ записывается информация, имеющая шахматное распределение, затем производится последовательное считывание и проверка этой информации. Шахматный тест используется для проверки взаимовлияния ячеек, содержащих информацию, записанную в обратном коде.

Тест «Сканирующий». Производится запись нулей (единиц) во все ячейки ОЗУ, затем выполняется последовательное считывание и проверка. После этого процесс повторяется с единицами (нулями). Сканирующий тест используется для проверки ОЗУ в условиях максимальной статической помехи, вызванной суммарным током утечки всех ячеек ОЗУ, находящихся в одном состоянии.

«*Чередующиеся строки 0 и 1*». В смежные ячейки ОЗУ записывается информация в обратном коде, затем осуществляется последовательное считывание и проверка. Этот тест применяется для проверки взаимовлияния адресных шин по строкам.

«*Чередующиеся столбцы 0 и 1*». Данный тест используется для проверки взаимовлияния адресных шин по столбцам.

«*Запись и запись/считывание вперед и назад*». По всем адресам записываются нули, затем выполняется считывание и проверка. После проверки каждой очередной ячейки в нее записывается информация в обратном коде. После проверки последней ячейки и записи в нее единиц процедура повторяется от старшего адреса к младшему с чтением единиц, их проверкой и записью нулей. Тест используется для проверки взаимовлияния соседних ячеек при смене в них информации.

Тест «*Марширующий*». Во все ячейки записывается «1» и последовательно считывается с проверкой и заменой их на «0». Затем процедура повторяется в обратном коде, т.е. последовательное считывание «0» начиная с 1-й ячейки с проверкой и заменой на «1». После обращения к последнему адресу проверка повторяется с данными в обратном коде, т. е. с нулями, и в обратном направлении – от последней ячейки к первой.

После обращения к первой ячейке процедура повторяется, считываются «0», и на их место записываются «1». После обращения к последнему адресу выполняется чтение с проверкой «1» всех ячеек ОЗУ – от первой до последней.

«*Дополнительная адресация*». Во все ячейки ОЗУ записывается фоновый набор единиц (нулей), затем производится считывание ячейки начиная с первой, с последующей проверкой и записью в нее противоположной информации. Каждое следующее обращение выполняется по адресу, код которого является дополнением к предыдущему.

Этот тест предназначен для проверки адресных цепей, информация которых в этом месте подвергается максимальному изменению.

«*Долбление*». Во все ячейки ОЗУ записывается тестовая информация, после чего производится многократное считывание по каждому адресу с последующей проверкой по всем адресам. Процедура повторяется при замене информации в каждой ячейке на информацию в обратном коде.

Тест служит для проверки способности ячеек выдерживать многократное считывание.

«*Крест*». В каждую ячейку ОЗУ записывается тестовое слово (нули и единицы), а в каждую из четырёх соседних ячеек – фоновое слово (нули и единицы). Затем информация в соседних ячейках изменяется, и исследуется влияние этого изменения на проверяемую ячейку.

Определяется чувствительность ячейки к крестообразно расположенным соседним ячейкам.

«*Разрушение считыванием*». Во все ячейки ОЗУ записывается, считывается и проверяется тестовое слово (все – единицы). Выполняется приращение адреса, и тестовое слово записывается во вторую ячейку. После этого информация из первой и второй ячеек считывается и проверяется. Процедура продолжается до тех пор, пока во все ячейки ОЗУ не будет записано тестовое слово. К нулевой ячейке делается n обращений, к первой – $(n – 1)$, к последней – одно.

Тест используется для проверки взаимовлияния ячеек ОЗУ при записи в них одной и той же информации.

Тест «*Бегущий*». В первую ячейку ОЗУ записываются единицы (нули), а во все остальные – фоновые нули (единицы). Затем все адреса последовательно считываются с проверкой. Последней считывается первая ячейка с последующей записью в неё нулей (единиц). Последовательность операций повторяется для второй, третьей и далее вплоть до последней ячейки.

Тест предназначен для обнаружения сбоев в ОЗУ, вызванных переходными процессами в различных цепях, так как перемещение «1» на фоне «0» (или наоборот) создает наихудшие условия для усилителей считывания.

«*Пинг-понг*». В первую ячейку ОЗУ записывается «1», во все остальные – «0». Последовательно считываются и проверяются ячейки 2, 1, затем 3, 1; 4, 1 и т. д., пока все пары переходов, включающие ячейку 1, не будут проверены. После этого в ячейку записывается «0», а во все остальные – «1». В такой же последовательности операции повторяются для ячейки 2 и т. д. Цикл повторяется для инверсной информации.

С помощью данного теста проверяется функционирование накопительной части ОЗУ, дешифратора, влияние записи на сохранность информации.

Тест «*Галопирующий*». В первую ячейку ОЗУ записывается «1», а в остальные – «0». Потом последовательно считываются и проверяются ячейки 2, 1, 2, затем 3, 1, 3 и т. д., пока все пары переходов, включая ячейку 1, не будут проверены.

После этого в ячейку 1 записывается «0», и информация считывается и проверяется. Затем это повторяется для ячеек 2, 3, вплоть

до последней. По эффективности этот тест эквивалентен тесту «Пинг-понг».

Вышеперечисленные тесты обнаруживают различные отказы (табл. 5.1).

Таблица 5.1

Виды отказов

Тест	Обнаруживаемые отказы					
	В матрице			В дешифраторе		
	Отсутствие записи	Ложная запись	Ложное считывание	Отсутствие выборки	Многократная выборка	Неоднозначная выборка
Сканирующий	-	0	0	0	0	0
Шахматный	+	-	0	-	0	0
Запись и запись / считывание вперед и назад	+	+	-	-	-	-
Марширующий	+	+	-	-	-	-
Дополнительная адресация	+	-	-	+	-	+
Крест	+	+	-	-	-	0
Бегущий	+	+	+	-	-	-
Пинг-понг	+	+	+	+	+	+
Галопирующий	+	+	+	+	+	+
Примечание: + – обнаруживает, - – не обнаруживает, 0 – неполное обнаружение.						

По характеру зависимости длительности выполнения тестов от числа ячеек ОЗУ тесты можно разделить на две группы: пропорциональные n, пропорциональные n^2, где n – емкость ОЗУ (табл. 5.2).

Таблица 5.2

Длительность выполнения тестов

Наименование теста	Зависимость длительности от n
1	2
Все нули (единицы)	$2n$
Адресный	$2n$
Шахматный	$4n$
Сканирующий	$4n$
Чередующиеся строки 0 и 1	$4n$
Чередующиеся столбцы 0 и 1	$4n$
Запись и запись/считывание вперёд и назад	$5n$
Марширующий	$10n$

Окончание табл. 5.2

1	2
Дополнительная адресация	$10n$
Крест	$128n$
Разрушение считыванием	n^2
Бегущий	$2(n^2+2n)$
Пинг-понг	$2(2n^2+2n)$
Галопирующий	$2(3n^2+3n)$

Аппаратный контроль запоминающих устройств. В запоминающем устройстве необходимо проверять адресную и накопительную части. Если считываемый из ЗУ код содержит информацию об адресе, то контроль функционирования адресной части может быть осуществлен за счет увеличения разрядности ЗУ и схемы сравнения кодов.

По коду адреса, хранящемуся в регистре адреса Рег.А, с помощью кодирующего узла К вычисляется контрольный код, который поступает в дополнительные разряды регистра числа Рег.Ч при записи числа в накопитель Н, а при считывании – на схему сравнения (рис. 5.12) [12]. Адресная информация кодируется арифметическим кодом, порождаемым одним модулем (контроль по модулю, например по модулю 3).

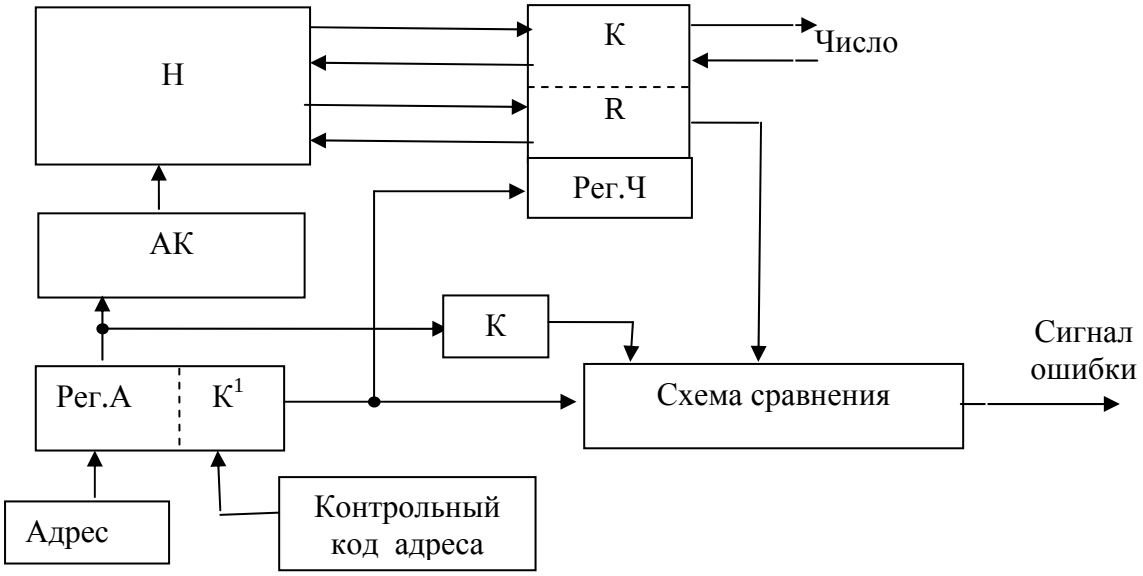


Рис. 5.12. Структурная схема ЗУ с контролем функционирования адресной части

Если адресная информация поступает в ЗУ в закодированном виде, контроль ЗУ может быть организован следующим образом. В ре-

жиме записи информации контрольный код адреса поступает в дополнительные разряды регистра Рег.Ч, затем этот код сравнивается с контрольным кодом, полученным на выходе кодера К. Это обеспечивает контроль правильности выполнения операций приема кода адреса и пересылки контрольного кода из Рег.А в Рег.Ч. В режиме считывания информации из ЗУ считанный контрольный код сравнивается с принятым в Рег.А. Перед выполнением операции сравнения может быть выполнена операция контроля правильности приёма кода адреса в Рег.А так же, как и при записи информации в ЗУ.

При контроле адресной части ПЗУ, информация из которых только считывается, контрольный код адреса записывается (прошивается) вместе с каждым числом. При считывании информации этот код сравнивается с контрольным кодом, сопровождающим адрес, по которому производится обращение в ЗУ. Если регистр адреса не содержит специальных контрольных разрядов, то контрольный код адреса может быть определен с помощью кодера. Сравнение вычисленного и считываемого из ЗУ контрольных кодов дает возможность осуществить контроль адресной части ПЗУ.

6. СРЕДСТВА КОНТРОЛЯ И ДИАГНОСТИРОВАНИЯ

6.1. Средства диагностирования аналоговых и цифровых устройств

При диагностировании и поиске неисправностей широко используются электрические измерительные приборы: вольтметры, омметры, мультиметры, осциллографы. В настоящее время практически все они применяют рассмотренные ранее способы измерения на основе использования микропроцессорной техники. Основой для построения многих видов приборов, служащих для диагностики электронных средств, являются *электронные вольтметры*. По сравнению с обычными вольтметрами эти приборы имеют повышенные точность и чувствительность, лучшую помехоустойчивость, автоматическую коррекцию погрешностей и самодиагностику отказов. Упрощенная структурная схема одного из таких приборов приведена рис. 6.1.

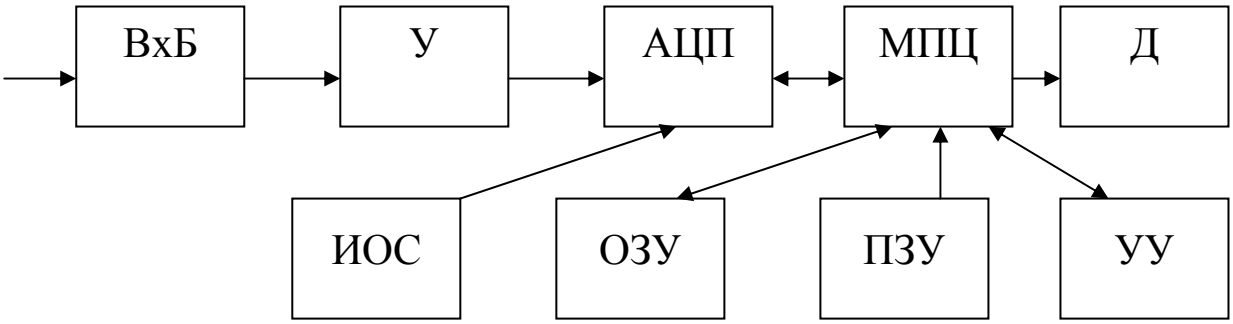


Рис. 6.1. Типичная структурная схема современного мультиметра: ВхБ – входной блок; У – промежуточный усилитель-преобразователь; АЦП – аналого-цифровой преобразователь; ИОС – источник опорного (эталонного) сигнала; МПЦ – микроконтроллер; Д – дисплей; ОЗУ, ПЗУ – соответственно оперативное и постоянное запоминающие устройства; УУ – клавиатура и элементы управления (управляющее устройство)

Входной блок (ВхБ) служит для выбора режима работы и пределов измерения. В нём происходит также преобразование переменных напряжений в постоянные (выпрямление, масштабирование, ограничение, фильтрация и т.п.). Обычно во входном блоке размещаются схемы измерения сопротивлений, емкости, параметров полупроводниковых дискретных элементов. Источник опорного (образцового)

сигнала (ИОС) содержит образцовый делитель напряжения и высокостабильный источник опорного напряжения, которое необходимо для нормальной работы аналого-цифрового преобразователя (АЦП). Сигналы, образованные на выходе АЦП, поступают на входе МПЦ, где обрабатываются по заданному алгоритму. Нужный алгоритм, записанный в ПЗУ, выбирается пользователем с помощью клавиатуры и других элементов в устройстве управления (УУ). Результат измерения отражается на дисплее. Погрешности измерения для современных мультиметров и вольтметров составляют от 0,01 до 0,001 %. Объем ПЗУ обычно не более 8 Кб, а время измерения лежит в пределах 20 – 640 мс, чувствительность – от 1 до 10 мкВ в зависимости от модели МПЦ. В СССР серийно выпускался электронный вольтметр Щ1518 на базе МПУ К580 с чувствительностью 10 мкВ, погрешностью 0,01% и временем измерения около 400 мс. Блок-схема алгоритма работы устройства управления вольтметром представлена на рис. 6.2 [12].

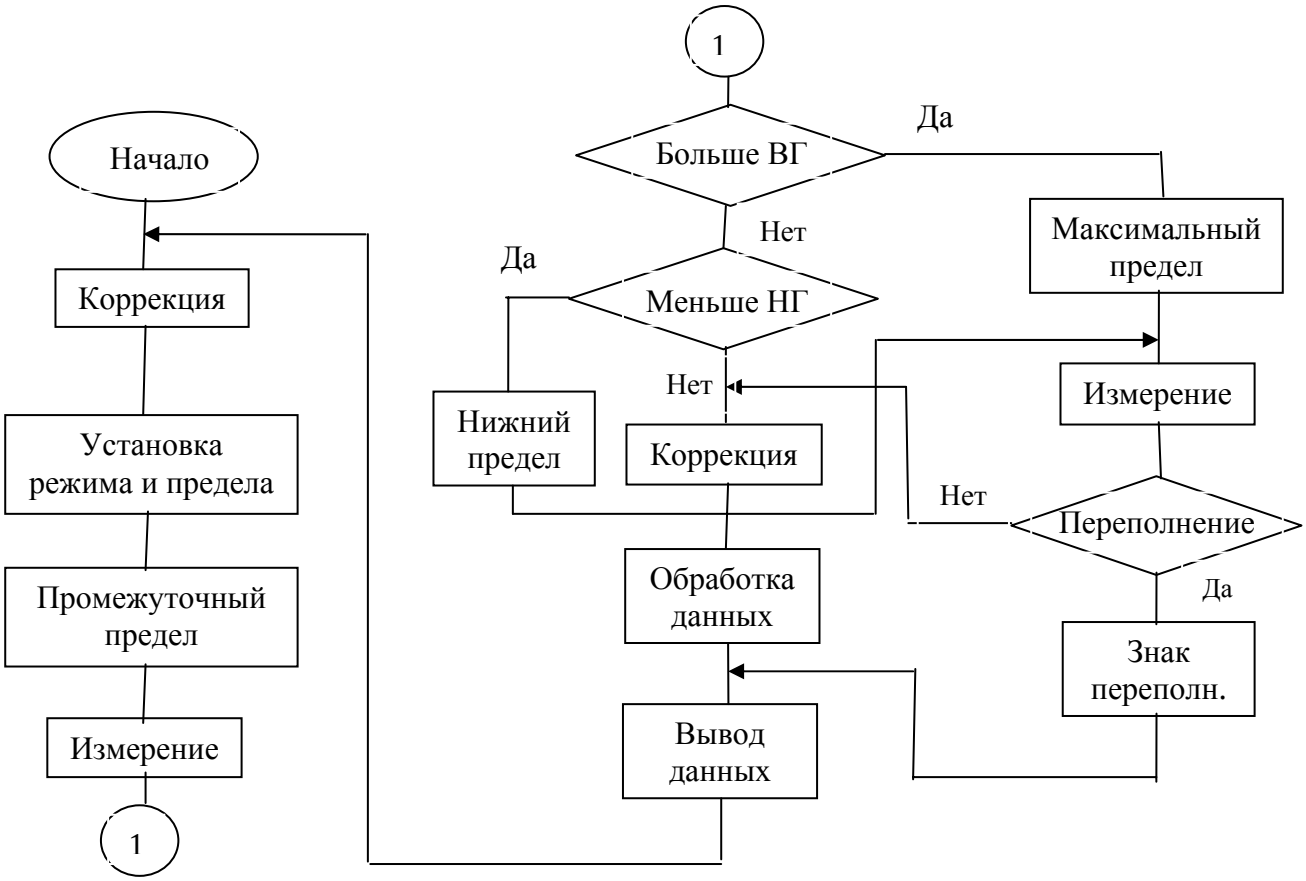


Рис. 6.2. Упрощенная структурная схема алгоритма работы управляющего устройства измерительного прибора

Алгоритм работы прибора можно представить следующим образом. После включения питания проводится процедура коррекции, в результате которой определяются и фиксируются в ОЗУ поправочные величины. Затем осуществляется ввод в ОЗУ сведений о режимах измерения (вид контролируемого параметра, диапазон измерения и т.п.). После этого проводится само измерение: измерительный тракт и выбор диапазона измерения обеспечиваются входным блоком (ВхБ). Входной сигнал преобразуется в АЦП и считывается микроконтроллером. Производится цифровая коррекция результата преобразования. Последним этапом процесса измерения является (при необходимости) обработка результатов измерения. Полученные данные выводятся для индикации на дисплей. Алгоритм работы, записанный в ПЗУ, занимает объем памяти не более 2,5 Кб, программа обработки данных – до 1,5 Кб.

Для обработки данных применяют следующие программы [12]:

Программа 1 *«Умножение R = CX»*. Она используется для пересчета результатов измерения одной физической величины (X) в другую (R). Это требуется, например, в случае измерения выходного сигнала измерительных преобразователей различных физических величин (давление, температура, влажность и т.п.) и восстановления по выходному сигналу этого преобразователя значения искомой величины. Константа C может быть введена с клавиатуры.

Программа 2 *«Процентное соотношение* $R = 100\ (X - X_н)/X_н$*»*. По этой программе каждое измеренное значение X сравнивается с номинальным значением $X_н$, которое предварительно вводится в ОЗУ. Используется обычно при допусковом контроле, например, сопротивления резисторов.

Программа 3 *«Поправка* $R = X - C$*»*. В этом случае константа C вычитается из результата каждого измерения X при вводе положительной величины C и суммируется при вводе отрицательной величины C. Программу можно использовать при градуировке прибора, измеряя «уход» нуля с его последующим исключением из результата измерения.

Программа 4 *«Отношение»*. По данной программе можно выполнить три вида отношений: линейное $R = X/r$, логарифмическое $R = 20 \lg (X/r)$, квадратичное $R = X^2/r$, где r – некоторая величина, введенная в ОЗУ как константа. Линейное отношение можно использовать, например, для вычисления тока, протекающего через резистор, по измеренному значению падения напряжения на нем. Квадратичное

отношение может быть использовано при вычислении уровня мощности в электрической цепи, а логарифмическое отношение – при измерении в децибелах уровня шумов, коэффициентов усиления, потерь в фильтрах и т.д.

Программа 5 *«Максимум/минимум»*. При проведении серии измерений можно получить результат в виде двух значений: $X_{макс}$ и $X_{мин}$ либо в виде их разности.

Программа 6 *«Пределы»*. Она дает возможность, при задании с клавиатуры верхнего $X_в$ и нижнего $X_н$ пределов измеряемой величины, получить результат в серии измерений в виде числа измерений, при которых $X > X_в$; $X < X_н$; $X_н \le X \le X_в$, где X – измеряемая величина.

Программа 7 *«Статистика»*. По окончании обработки результатов измерения по этой программе для заданной выборки измерений можно получить следующую информацию:

- число измерений n;
- выборочное среднее $R_{ср} = \frac{1}{n}\sum_{i=1}^{n}\overline{X}_i = X_{ср}$;
- дисперсию $D_{ср} = \frac{1}{n}\sum_{i=1}^{n}(X_i - X_{ср})^2$;
- стандартное среднее квадратическое отклонение $\sigma_x = \sqrt{\frac{1}{n}\sum_{i=1}^{n}X_i^2}$.

Программа 8 *«Термопара»*. По данной программе можно ввести дополнительную коррекцию результата измерения по показанию встроенной в прибор термопары. Для этого предварительно с помощью образцовых средств определяется зависимость погрешности данного прибора от изменения температуры окружающей среды, и в ПЗУ заносятся поправочные коэффициенты. Характеристика встроенной термопары аппроксимируется кубической полиномной зависимостью $E = a + b\theta + c\theta^2 + d\theta^3$, константы которой записаны в ПЗУ. Для конкретного значения температуры окружающей среды θ вычисляется ЭДС термопары E, и рассчитывается поправка к показаниям вольтметра.

Самодиагностика прибора осуществляется путем диагностики отказов. Обнаружение отказов основано на том, что при нормальной работе поправочные значения должны лежать в заданных (допустимых) пределах. Если они не укладываются в область допустимых значений, на дисплее индицируется сообщение о неисправности прибора.

6.2. Аппаратные средства контроля и диагностирования цифровых устройств

Логический пробник. Простейшим видом аппаратных средств диагностики является одноконтактный логический пробник. Он представляет собой устройство для индикации двоичного состояния элементов дискретных схем [13].

Задача пробника – обеспечить проверку логических схем, возможность наблюдения логических уровней без настройки и калибровки (настройка и калибровка требуется в осциллографах). Состояние контролируемых логических уровней индексируется либо светодиодом, либо миниатюрной лампой накаливания. В пробнике могут быть следующие состояния: есть сигнал «1» в точке контроля – светится индикатор, есть сигнал «0» – индикатор не светится, переключается сигнал – светодиод мигает, светится в половину яркости – отсутствие сигнала («плохой» сигнал).

Логический пробник должен быть сделан так, чтобы обеспечить работу с разными видами микросхем: ТТЛ, ЭСЛ, КМОП. В пробнике обычно имеется схема расширения импульсов, с помощью которой оператор может проверить наличие импульсных сигналов высокой частоты. При наличии импульсов индикатор мигает с определенной (несколько Гц) частотой (рис. 6.3).

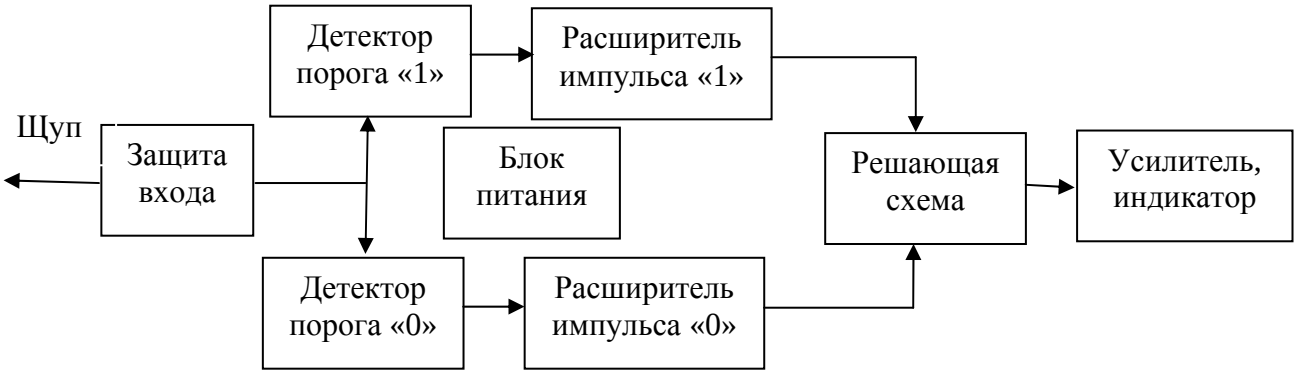


Рис. 6.3. Структурная схема логического пробника

Отдельные логические пробники имеют средства для запоминания на некоторое время одиночных импульсов. Пробник является простым, но надёжным средством для контроля портов ввода-вывода микропроцессора, линий, по которым передаются признаки состояний, и других точек системы, где состояние изменяется сравнительно редко.

Пробник используется для предварительной диагностики работы цифровой системы. Иногда это позволяет в простых схемах достаточно точно локализовать неисправность с малыми затратами времени на поиск отказавшего элемента. Для поиска неисправностей в сложных схемах применяются более сложные приборы, такие, например, как логический и сигнатурный анализаторы.

Логический анализатор. Этот прибор предназначен для сбора данных о поведении дискретных систем, обработки этих данных и представления их оператору в различной форме [14]. Логические анализаторы (ЛА) характеризуются числом каналов, емкостью памяти на канал (глубина записи), частотой записи, способами синхронизации и запуска, формой представления данных. Логический анализатор – это комбинация многоканального регистратора двоичных сигналов, пульта управления и дисплея (рис. 6.4).

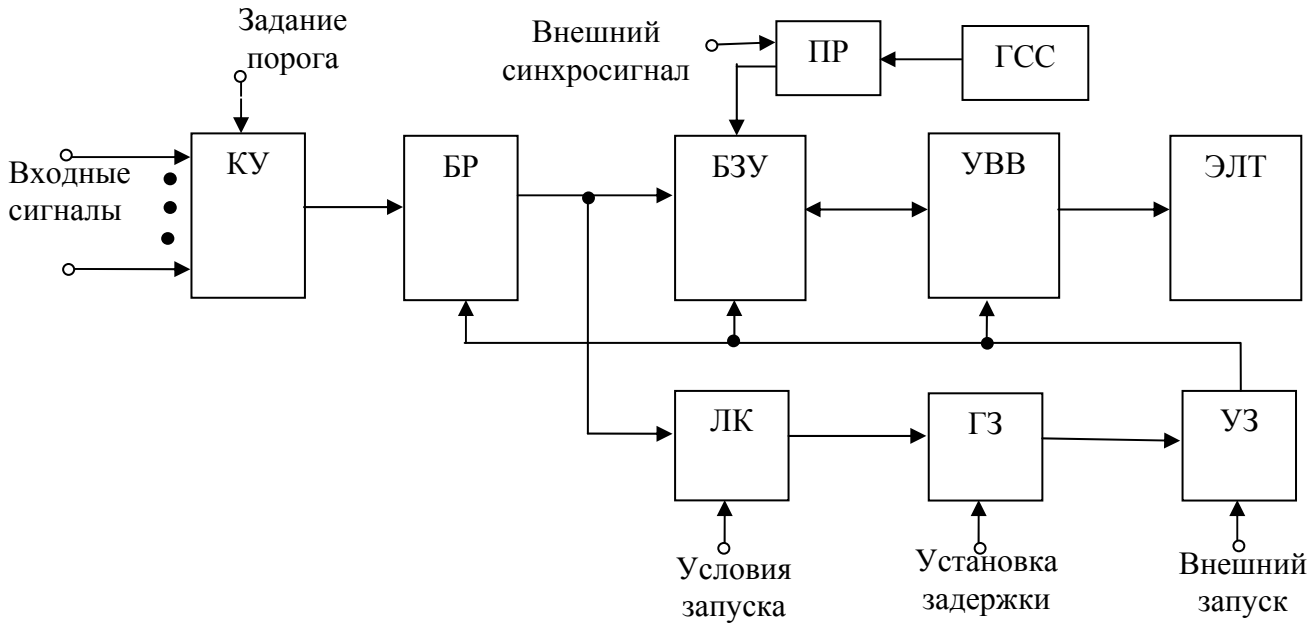


Рис. 6.4. Упрощённая структурная схема логического анализатора:
КУ – компараторы уровней входных сигналов; БР – буферный регистр;
БЗУ – блок запоминающих устройств; ПР – переключатель режимов; ГСС – генератор синхросигналов; ЛК – логический компаратор; ГЗ – генератор временной задержки;
УЗ – устройство запуска; УВВ – устройство управления выводом информации на электронно-лучевой индикатор (ЭЛТ)

На входные каналы логического анализатора поступают сигналы с отлаживаемой или диагностируемой системы. Компараторы уровней (КУ) распределяют их на соответствующие уровни и форми-

руют набор значений этих уровней. Этот набор подается на буферный регистр, в БЗУ и на логический компаратор (ЛК). Последний предварительно настраивается (программируется) на обнаружение определенной последовательности наборов значений сигналов, формирует и опознает условия запуска. После определения условий логический компаратор выдает сигнал генератору задержки.

Генератор задержки по истечении заданного времени выдаёт сигнал на устройство запуска, которое инициирует или запрещает (прекращает) запись значений входных сигналов в ЗУ. Генератор задержки формирует задержки, величина которых зависит от объема памяти на канал. После записи в БЗУ устройство управления визуальным выводом (УВВ) выдает информацию через дисплей в удобном для оператора виде (таблицы состояний, временные диаграммы и т.п.).

Условно различают два типа анализаторов, соответствующих двум режимам записи:

1) анализаторы логических состояний (АЛС), использующие синхронный режим записи анализируемых сигналов;

2) анализаторы временных диаграмм (АВД), использующие асинхронный режим.

АЛС фиксируют состояние контрольных точек проверяемой схемы во время существования (обычно по фронту) тактовых сигналов самой схемы и записывают процесс изменения этих состояний синхронно с работой устройства.

АВД фиксируют состояния контрольных точек в моменты времени, задаваемые независимо работающим внутренним тактовым генератором.

Анализаторы имеют два основных режима работы:

- режим регистрации (фиксации) данных;
- режим отображения (представления) данных.

Регистрация (фиксация) данных. Режим регистрации данных о поведении какой-либо системы предполагает следующие действия:

- подключение ЛА к объекту;
- определение логических значений сигналов, поступивших на объект;
- запись сформированной информации в память ЛА.

Для подключения к точкам контроля в ЛА используют зонды (миниатюрные щупы), позволяющие подключаться к контактам одного ряда выводов корпуса микросхемы со стандартным шагом (например, DIP с шагом 2,5 мм). При определении значений сигналов ЛА отображают нормированные по уровню цифровые сигналы.

Логический анализатор должен обладать обязательным свойством: его входные цепи не должны влиять на функционирование используемого объекта, для чего должно соблюдаться условие: $R_{вх} \geq 1$ Мом, $C_{вх} \leq$ (10-25) пФ.

Как отмечалось выше, различают синхронный и асинхронный режимы записи. Запись информации в виде «0» и «1» производится в тактовые моменты времени. Синхросигналы могут поступать с диагностируемой схемы или от внутреннего генератора. Первый случай – синхронный режим, второй – асинхронный. В синхронном режиме набор значений сигналов записывается в память либо фронтом, либо спадом синхросигнала от объекта. Асинхронный режим используется для нетактируемых информационных сигналов. Достоинство такого способа фиксации сигналов состоит в том, что, выбрав высокую частоту тактирования, можно обеспечить более точную и детальную регистрацию временного изменения входного сигнала (рис. 6.5).

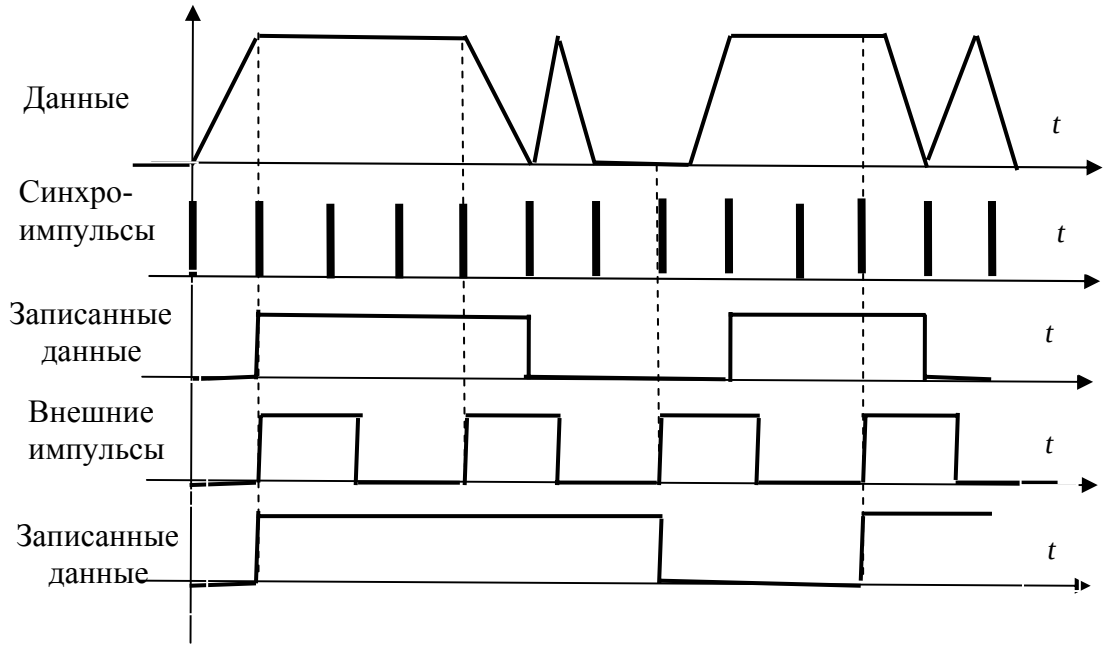


Рис. 6.5. Временные диаграммы сигналов при записи данных с разной частотой тактирования

С целью обеспечения высокой разрешающей способности необходимо, чтобы частота синхронизации анализатора в 5 – 10 раз превышала частоту наблюдаемых событий. Тактовая частота выбирается путем анализа минимальных интервалов времени между двумя событиями, которые могут встретиться в диагностируемой системе. Например, если $t_{мин}$ = 50 нс, то следует иметь тактовую частоту 20 МГц. Если $t_{мин}$ = 10 нс, то $f_{такт}$ = 100 МГц.

При работе с МПУ с тактовой частотой 1 – 4 МГц (например, 580ИК80А) нужно иметь ЛА с тактовой частотой 50 – 100 МГц, так как минимальная длина синхроимпульса может быть 80 нс, что соответствует частоте 6 МГц.

Синхронный режим работы анализатора рационален при исследовании (контроле) выполнения программ, так как интерес представляют состояния элементов (анализаторы логических состояний) системы в определенные моменты времени, когда логические уровни уже установлены с момента синхронизации. В этом режиме поступающие данные воспринимаются ЛА так же, как и используемой системой (синхронизация одна и та же). Для обеспечения этого ЛА должны иметь минимально необходимое время фиксации данных (отрезок времени, в течение которого данные не должны изменяться после прихода фронта синхросигнала) и минимально возможное время установления данных (отрезок времени, в течение которого данные должны иметь стабильные уровни до прихода синхросигнала).

В настоящее время разработаны ЛА, позволяющие обеспечить оба режима работы. Универсальные ЛА имеют от 8 до 48 каналов регистрации, частоту регистрации от 20 до 500 МГц, глубину регистрации от 16 до 2048 бит/канал с возможностью идентификации информации, т.е. различения информации, передаваемой по одной магистрали. Эта проблема возникает для систем МПУ, так как по линиям одной и той же магистрали могут передаваться и данные и адреса (или часть адресной управляющей информации). В этом случае анализатор, имеющий только один источник синхросигналов, не может различить данные, передаваемые по одной магистрали. Необходимым (одним из необходимых) условием разделения данных является наличие режима многофазной синхронизации (трех различных источников синхросигналов). Он реализуется следующим образом: входные каналы ЛА разбиваются на две или три группы. По одной группе каналов записываются адреса, по другой – данные, по третьей – команды управления. Каждая группа каналов записывается по своему синхросигналу и в свой разряд буферного регистра. После прихода всех синхросигналов данные с буферного регистра подаются в ЗУ и на компьютер.

Способы запуска ЛА. В процессе поиска источника ошибки возникает необходимость просматривать отдельные участки потоков данных, характеризующих поведение системы. Для этого нужно иметь возможность в требуемый момент прекратить или инициализировать запись данных в память.

Процесс запуска – это анализ потока данных и обнаружение заданного события. Иногда говорят о положительном или отрицательном запуске: если сигнал запуска инициирует запись данных в память, то это положительный запуск; если сигнал запуска прекращает запись в память – отрицательный запуск. Отрицательный запуск дает возможность «вернуть назад» и проанализировать логические состояния или временные соотношения сигналов от начала отслеживания до прекращения записи.

Реализуются следующие виды запуска:

а) запуск по кодовому слову (по комбинации значений сигналов), т.е. при появлении на входе анализатора определенного, заранее выбранного двоичного слова;

б) запуск по последовательностям слов. Этот вид запуска позволяет выбрать в программе, имеющей множество ветвей, один определяющий путь (рис. 6.6). A, B, C … L – это, например, 16-разрядные адреса. ABEFKL, ADL, ACHKL – разные пути. После запуска в памяти анализатора будет храниться трасса того или иного участка программы (в зависимости от выбранной последовательности слов);

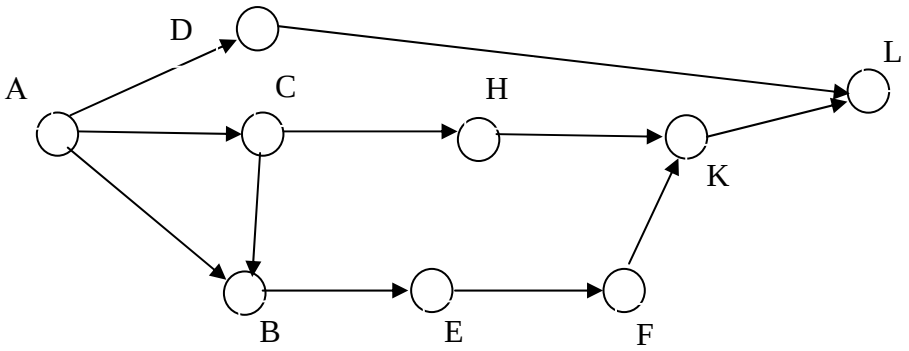


Рис. 6.6. Выбор определяющего пути

в) запуск по несовпадению. Он используется при анализе систем в случае возникновения самых неприятных неисправностей – перемежающихся, т.е. появляющихся случайным образом. Для реализации этого вида запуска нужно иметь дополнительное ЗУ. Анализатор принимает данные из подозреваемой части программы и записывает их в это ЗУ. В процессе реализации режима проверки по несовпадению, когда анализатор вновь проводит проверку, анализируются условия, которые были при записи в первом случае. При обнаружении этих условий он регистрирует данные и сравнивает с данными, хранящи-

мися в эталонном ЗУ. Если данные различны, прибор запускается и фиксирует состояние системы. Если данные не различаются, анализатор снова готовит эталонные данные и ожидает нового прихода данных, соответствующих условиям, при которых производится проверка.

Отображение (представление) данных. Этот режим характеризуется формой представления данных (например, о поведении МП систем). Наиболее распространенными формами отображения являются:

- временные диаграммы;
- таблицы последовательностей данных.

В первом случае момент запуска индицируется на экране вертикальной прерывистой линией – маркером запуска. Тем самым на экране фиксируется раздел между данными, поступившими до и после момента запуска. Процесс индикации временных диаграмм можно осуществить с изменением масштабов по оси времени.

Таблицы последовательностей данных могут отражать таблицы истинности комбинационных устройств, устройств ввода-вывода и состояний устройств с памятью, трассу программы. Данные могут быть представлены в двоичном, восьмеричном, шестнадцатеричном кодах, в коде ASCII. Для удобства представления и возможности отладки программ, написанных на языке ассемблера, в некоторых ЛА данные могут быть представлены на том же языке.

ЛА снабжаются стандартными интерфейсами (например, IEEE-448, ГОСТ 26.003-80), позволяющими программировать анализатор от внешних устройств и обработку результатов с помощью ЭВМ.

Генераторы слов. Это приборы, предназначенные для формирования и подачи входных воздействий на программируемую или диагностируемую дискретную систему. Совместно с логическими анализаторами генераторы слов (ГС) образуют систему подачи внешних сигналов и сбора ответных реакций микропроцессорных модулей и схем произвольной логики. ГС используются для тестирования либо эмуляции (замены) дискретных устройств системы. Упрощённая структурная схема ГС показана на рис. 6.7.

Генераторы слов (генераторы данных, генераторы тестовых последовательностей) характеризуются числом каналов, емкостью памя-

ти, частотой подачи воздействий (тактовая частота), способами подачи данных и формирования входных воздействий.

Входные наборы (их последовательность), которые необходимо подать на систему диагностирования, заносятся в ЗУ через УУ вводом либо с клавиатуры, либо по интерфейсу из памяти ЭВМ (рис. 6.7).

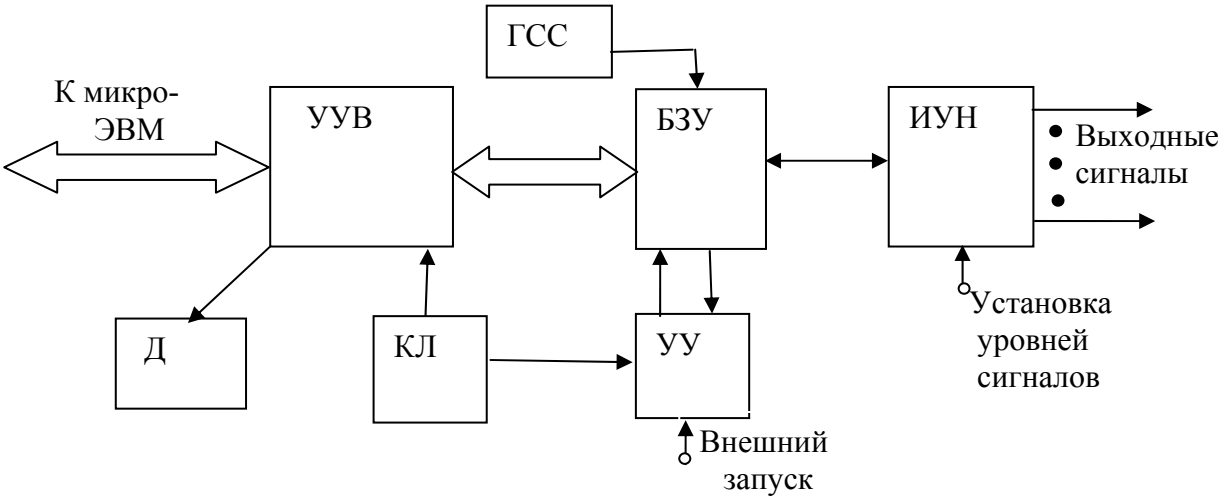


Рис. 6.7. Структурная схема генератора слов:
УУВ – устройство управления и связи с периферией; Д – дисплей;
КЛ – клавиатура; ГСС – внутренний генератор стандартных сигналов;
УУ – управляющий блок; БЗУ – блок запоминания и управления;
ИУН – формирователь выходных сигналов

Входные наборы должны подаваться с определенной частотой тактирования. Уровни «1» или «0» обеспечиваются драйверами – источниками, управляемыми напряжением (ИУН). Объект диагностирования подключается к выходным каналам ГС.

Пуск ГС осуществляется либо с клавиатуры, либо извне, например от ЭВМ, либо от логического анализатора. После команды «Пуск» данные считываются из памяти и через драйверы (ИУН) поступают на выходные каналы с заданной частотой.

Число выходных каналов – важный параметр ГС. В ряде случаев все входы тестируемого устройства удается разбить на группы и организовать подачу воздействий последовательно, отдельно на каждую группу входов. Число выходных каналов колеблется от 2 до 80 (2, 8, 16, 32, 64, 80).

Тактовая частота выбирается высокой, так как ряд неисправностей дискретных систем обнаруживается лишь на высоких частотах функционирования. По этой причине чаще всего желательно вести тестирование на максимально возможной для проверяемой

схемы тактовой частоте. Последняя изменяется от сотен герц до десятков мегагерц (есть 50 МГц).

Емкость памяти в ГС содержит от 16 до 2048 слов и выполняется на быстродействующих ЗУ (время выборки – 25 нс). Драйверы должны иметь третье состояние и позволять подключать объекты, выполненные по различной технологии (ТТЛ, ТТЛШ, КМОП, ЭСЛ).

По способу подачи воздействий различают ГС последовательного и параллельного кодов.

Режим последовательного кода предназначен для тестирования или эмуляции (имитации) систем с последовательной передачей данных. ГС последовательного кода имеют один или два информационных выходных канала, синхровыходы для генерации первого и последнего битов синхросигнала. Некоторые ГС позволяют генерировать псевдослучайную последовательность сигналов (ПСПС).

По способу реализации устройств правления (УУ) выделяют три типа ГС:

1) с буферной памятью. В этих ГС данные из памяти считываются последовательно, начиная от конкретного начального адреса и кончая заданным конечным адресом ЗУ (это наиболее просто);

2) с управляющей памятью. Память делится на две части – данных и команд, имеющих общее управление и общий регистр адреса. Данные и команды считываются одновременно. Команды поступают на дешифратор команд, определяющий, что нужно сделать со считанными данными. Этим достигается быстродействие;

3) с алгоритмическим генерированием последовательностей на основе специализированного микропрограммируемого процессора. Такой ГС должен иметь память данных и память микропрограмм.

ГС имеют возможность организации считывания данных из памяти либо при поступлении сигнала внутреннего генератора, либо извне от объекта контроля. В первом случае обеспечивается режим, при котором очередной входной набор подается на объект диагностирования при поступлении синхросигнала либо от внутреннего генератора, либо от оператора с клавиатуры, либо от внешнего синхрогенератора. При этом последовательность входных наборов не зависит от реакции объекта диагностирования. Во втором случае очередной входной набор может зависеть как от запрограммированного алгоритма тестирования, так и от реакции объекта на последовательность.

Современные ГС имеют в своем программном обеспечении различные средства программирования (трансляторы, редакторы, отладчики).

Представителем семейства ГС является прибор Г5-9-80, выпускавшийся в СССР. У этого ГС обеспечивается два режима работы (последовательный и параллельный), максимальная тактовая частота – 50 МГц. Число выходных каналов – 16. Емкость ЗУ – 2048 бит/канал для работы с ЭСЛ- и ТТЛ-уровнями.

Комплексы диагностирования. Объединяющие возможности логических анализаторов и генераторов слов, комплексы диагностирования (КД) способны подавать входные воздействия на диагностируемую систему, собирать и анализировать ответные реакции системы. КД имеют режим, при котором ГС и ЛА функционируют как единое целое под общим управлением микропроцессора с общим программным обеспечением и сигналами управления.

В состав КД входят микроЭВМ с периферией, устройство ГС, устройство ЛА (рис. 6.8). ГС и ЛА объединяются совместно с микроЭВМ
с помощью периферии и программного обеспечения (рис. 6.8).

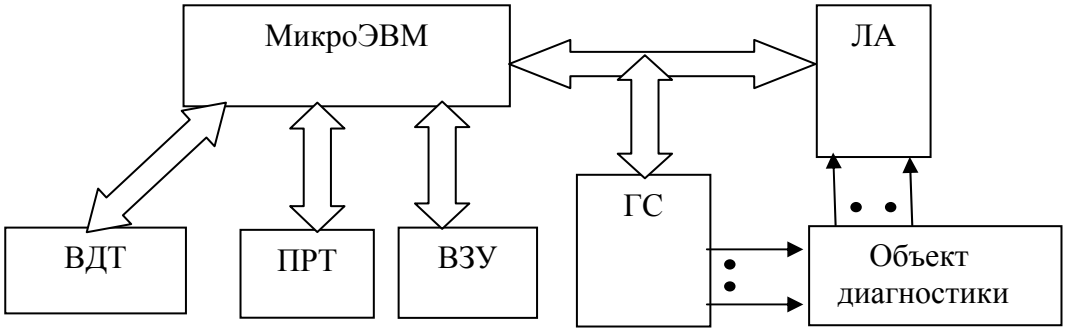


Рис. 6.8. Структурная схема простого диагностического комплекса:
ВДТ – видеотерминал; ПРТ – принтер; ВЗУ – внешняя память;
ГС – генератор сигналов (слов); ЛА – логический анализатор

МикроЭВМ формирует тестовые наборы, загружает и настраивает на определенный режим работы ГС и ЛА, анализирует результаты тестирования, обрабатывает информацию о поведении объекта, осуществляет диалог с оператором.

ЛА позволяет собирать данные о поведении системы в режиме реального времени. Видеотерминал помогает осуществить диалог с опе-

ратором, принтер – документировать результаты. Внешняя память, увеличивая общую емкость памяти, расширяет функции комплекса, позволяет иметь библиотеки тестирующих программ, использовать языки высокого уровня, запоминать процедуры отладки и диагностирования.

6.3. Устройство и применение сигнатурного анализатора

Прибор, в котором используется принцип диагностики, основанный на сравнении сигнатур, получил название сигнатурного анализатора. *Сигнатура* – это двоичное число, полученное в результате преобразования длинных последовательностей двоичных сигналов. Если сравнить логический и сигнатурный анализаторы, то следует отметить два обстоятельства:

- использование логического анализатора требует высокой квалификации оператора и необходимости знания принципов работы диагностируемого устройства;
- для каждой конкретной неисправности при работе с логическим анализатором следует настраивать прибор и исследуемую систему на новый режим работы.

Этих трудностей лишен сигнатурный анализатор, который по принципу действия позволяет достаточно просто и быстро локализовать неисправность в сложных цифровых системах. Первым прибором, предназначенным для сигнатурного анализа, был прибор Hewlett Packard 5004A, выпущенный в 1977 г. (рис. 6.9) [12].

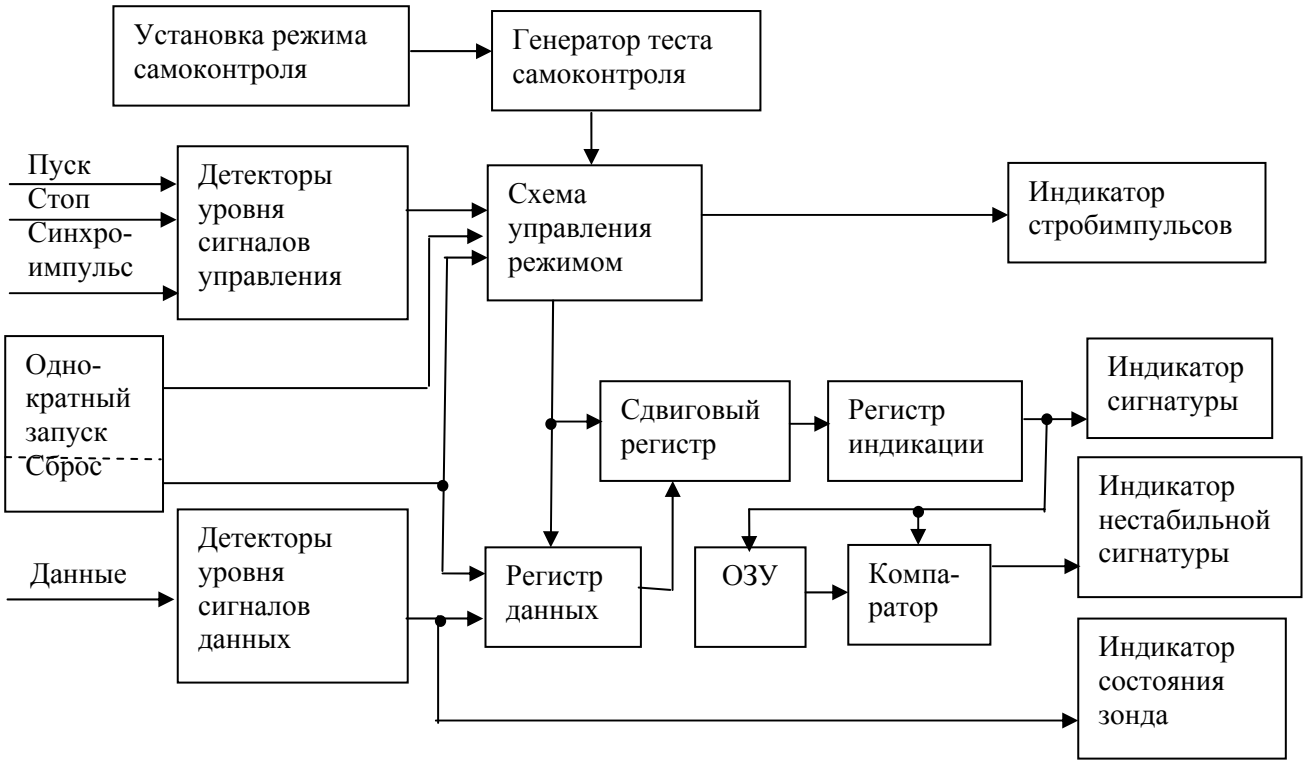


Рис. 6.9. Структурная схема анализатора 5004A

Сигнатурный анализатор снабжается зондами, через которые от испытываемой схемы поступают сигналы данных и управления: сигналы запуска «Пуск» и останова «Стоп», сигнал «Синхронизация». Интервал времени между сигналами «Пуск» и «Стоп» определяет время накопления сигнатуры. Последняя формируется путем синхронного ввода данных в сдвиговый регистр по активному фронту синхроимпульса. Максимальная частота синхроимпульса – 10 МГц, время предустановки данных перед фронтом синхроимпульса – не менее 15 нс. Принцип работы анализатора можно пояснить временными диаграммами (рис. 6.10).

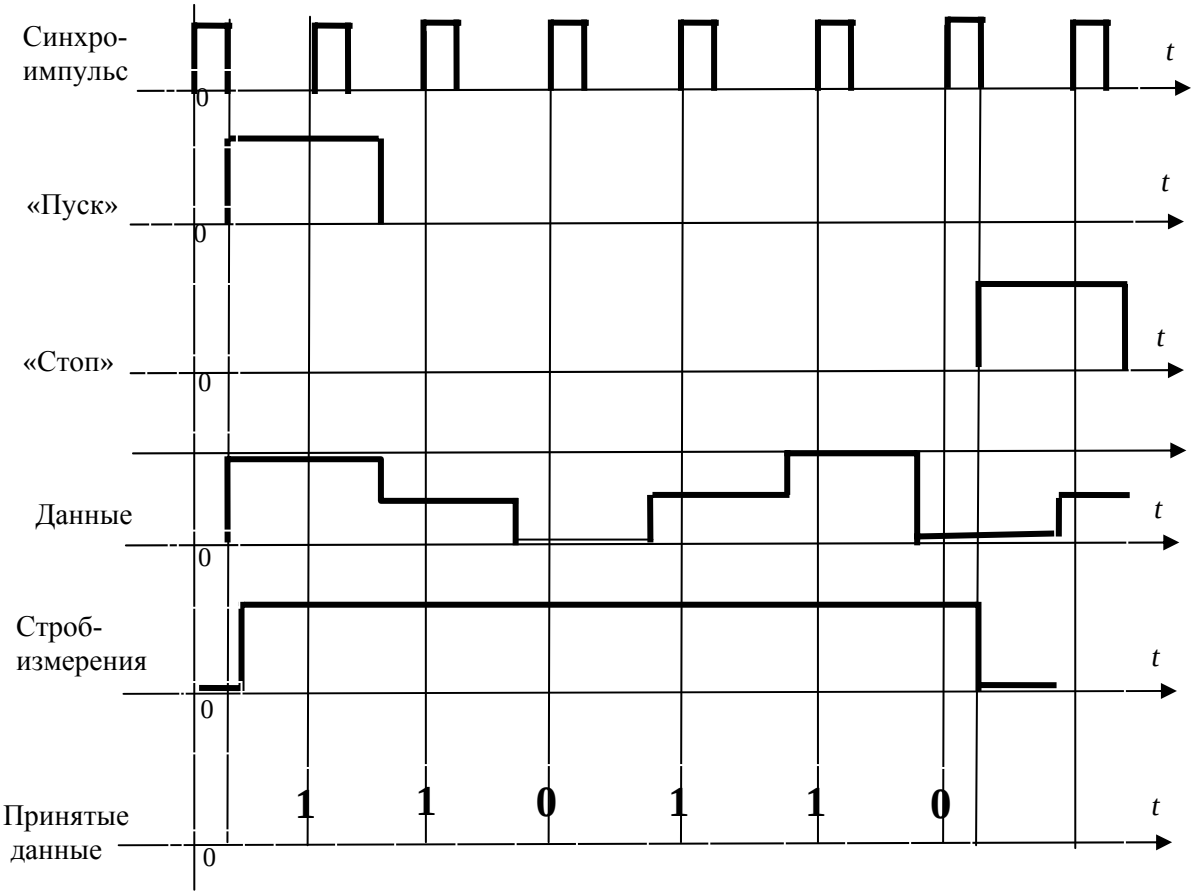


Рис. 6.10. Временные диаграммы работы сигнатурного анализатора

На передней панели сигнатурного анализатора располагаются светодиодные индикаторы, показывающие наличие сигналов строб-импульса накопления сигнатуры, нестабильности сигнатур и состояния зонда. Индикатор нестабильности сигнатур фиксирует неравенство сигнатур, полученных в соседних измерительных интервалах для одной точки измерения. Индикатор состояния зонда отражает наличие импульсов и значение амплитуд контролируемых импульсов (нулевое, единичное или неопределенное).

Предусмотрен режим однократного запуска, при котором прибор фиксирует только одну сигнатуру, соответствующую первому измерительному интервалу, и сохраняет её до нажатия кнопки «Сброс». В приборе задан режим самоконтроля, который может быть установлен оператором.

Все последующие модели сигнатурных анализаторов повторяют структуру рассмотренного прибора. Например, полную принципиальную схему сигнатурного анализатора можно найти в [15].

7. ПРОГРАММНАЯ ДИАГНОСТИКА ЭЛЕКТРОННЫХ СРЕДСТВ

7.1. Особенности микропроцессорных систем при поиске неисправностей и диагностике

В микропроцессорных системах (МПС) поиск неисправностей и наладка осуществляются не так просто, как в других системах. Здесь требуются иные средства и методы, отличающиеся от традиционных [12]. В МПС управляющие функции реализуются микропрограммно, алгоритмы регулирования скрыты в алгоритмах программы, записанной в ПЗУ.

Динамика работы МПС такова, что сигналы появляются и исчезают в течение нескольких микросекунд. В таких системах надо знать не только, что смотреть (контролировать), но и где смотреть.

Кроме того, в МПС обычно шины данных и адресов имеют двунаправленный характер, что затрудняет интерпретацию данных и адресов. Обнаружение источника неисправности осложняется тем, что к шине подключено несколько устройств, а число элементарных операций и шагов программы велико. С учетом этого желательно предусматривать в программном обеспечении МПС программу самопроверки (автодиагностики), которую следует выполнять сразу после включения питания, перед включением в работу управляемого устройства, после его выключения из работы или после сброса (Reset) самой МПС.

Автодиагностика МПС должна осуществляться в фоновом режиме, когда не выполняются другие (управляющие) программы, а также в процессе нормальной работы, например по прерыванию от сигнала таймера или другого сигнала, приостанавливающего работу программы, чтобы выполнить диагностический тест.

Минимальной задачей автодиагностики является обнаружение неисправности (установление факта появления неисправности). В первую очередь устанавливается факт сохранения базы данных в ПЗУ, где хранятся данные, обеспечивающие правильную работу всей системы. Кроме этого автодиагностика должна установить правильность работы устройств ввода-вывода, параметров питания и т. д. Локализация неисправности и её устранение могут быть выполнены по-

сле остановки системы и перевода управления, например, на дублирующую систему (для дорогостоящих или уникальных объектов, отказы которых связаны с большим ущербом).

В настоящее время основным типом промышленных устройств управления стал контроллер, в состав которого входит микроконтроллер – однокорпусная микроЭВМ, имеющая в своем составе процессор, память, ОЗУ и ПЗУ, порты ввода-вывода, внутренний генератор тактовых сигналов, АЦП, ЖКИ-драйверы, таймеры, USB-порты [16]. Особенно широко применяются микроконтроллеры, имеющие сравнительно небольшое число команд (52 вместо 256) (PIC-контроллеры). Например, контроллер PIC16C84 (КР1878ВЕ1 фирмы «Ангстрем»), выполненный по технологии КМОП в корпусе DIP с 18 выводами, имеет память команд 1К×16, ОЗУ 128×8 байт, память данных ЭСППЗУ 64×8, тактовую частоту f_m = 32 кГц ÷ 8 мГц, Wochdog, стек данных и команд, два порта (на 4 и 8 бит).

Напряжение питания – от 4,5 до 5,5 В, максимальный ток потребления – 25 мА, температурный диапазон – от -40 до + 85 °С.

Микропроцессорные системы удачно приспособлены для самоконтроля и диагностики [12]. Это обусловлено свойствами самих систем и принципом их действия. К таким свойствам относятся следующие:

1) способность МПС самостоятельно генерировать тестовые последовательности, заданные программно;

2) возможность логической обработки результатов тестирования без применения дополнительной аппаратуры;

3) программная доступность всех узлов МПС, что позволяет процессору опрашивать состояние этих узлов;

4) возможность закладки тестирующих программ (микропрограмм), написанных на том же языке, что используется в системе;

5) относительно простое включение тестовых программ в общий алгоритм действия.

В МПС достаточно легко организовать диагностику неисправностей на функциональном уровне, т.е. на уровне функциональных узлов системы.

Программа самодиагностики может быть легко «вписана» в адресное пространство рабочих программ МПС (рис. 7.1). Для этого используется либо собственное ПЗУ, либо дополнительное как расширение памяти. Последнее возможно, если для этого приспособлена общая структура МПС. На рис. 7.2 представлена структурная схема

включения в адресное пространство МПС дополнительной схемы ПЗУ, в котором записаны только тестовые программы [14].

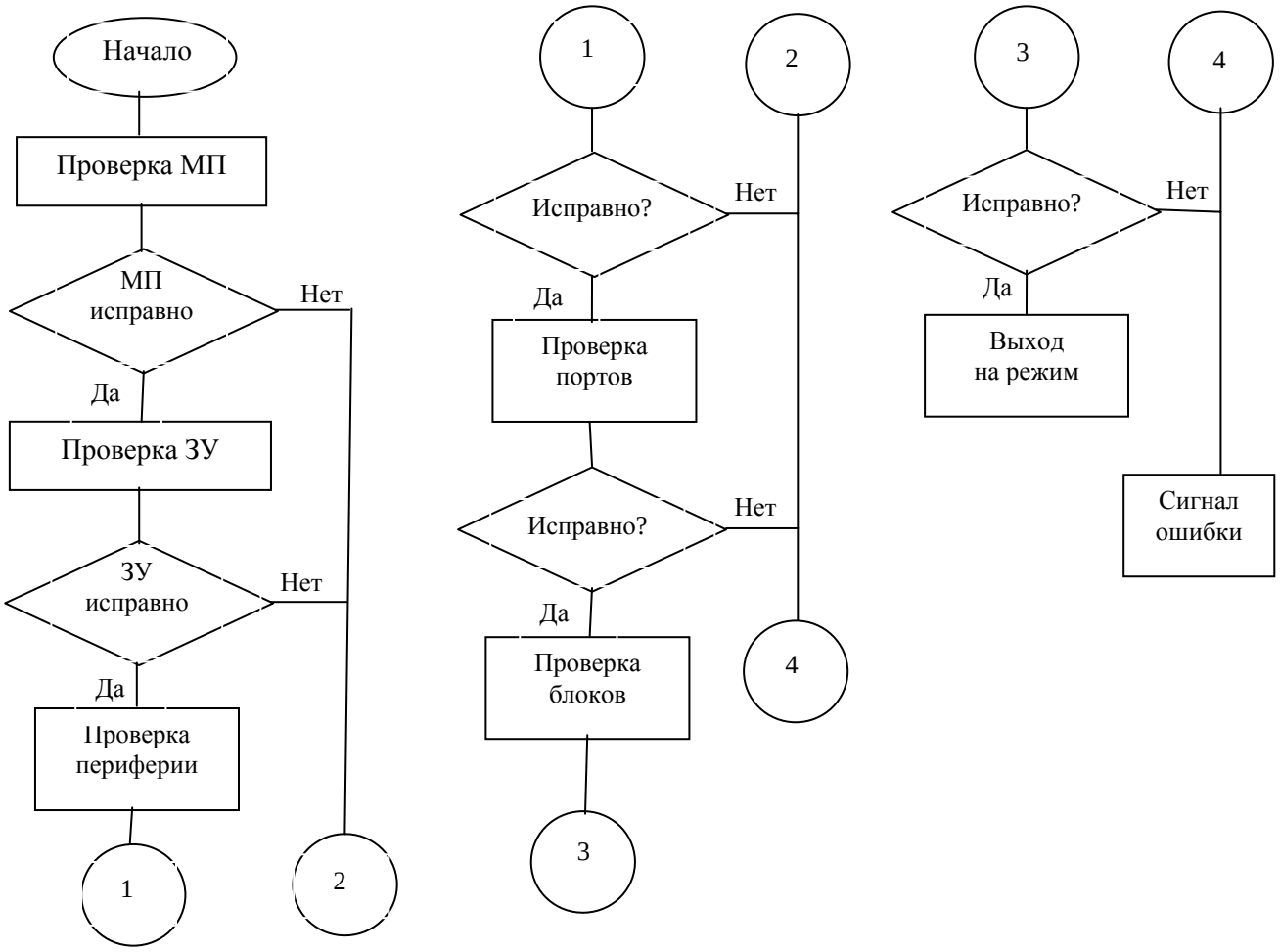


Рис. 7.1. Блок-схема алгоритма самодиагностики МПС

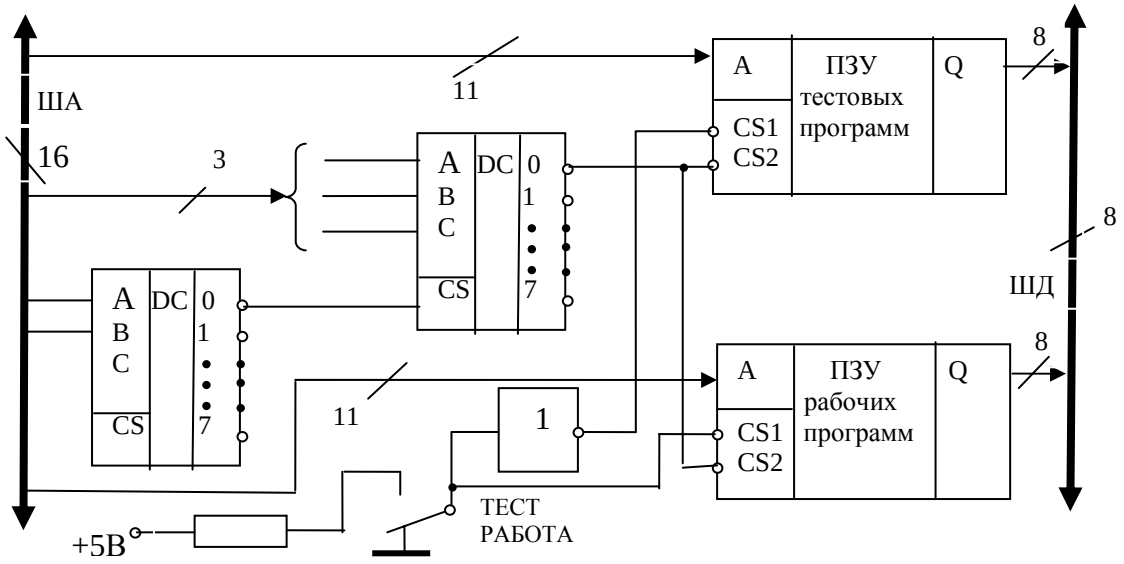


Рис. 7.2. Структурная схема включения тестового ПЗУ в МПС

Для самодиагностики используется принцип последовательной проверки узлов системы. В этом случае следует предположить, что определенные узлы системы заведомо исправны. В первую очередь, это относится к блоку питания и внутреннему генератору синхроимпульсов МП. Кроме того, придется предположить также, что исправны такие узлы, как регистры МП и цепи адресации тестовой программы. Несмотря на такое сужение области действия процесса самодиагностики, последняя позволяет предотвратить неправильную работу МПС и избежать неприятностей от неверных действий системы управления.

Как правило, в управляющих МПС программа самодиагностики выполняется всегда при включении питающего напряжения. Для более точной локализации и устранения неисправностей, как правило, используется дополнительная аппаратура (логический анализатор, осциллограф и т.п.) после того, как программа самодиагностики укажет на существование неисправности. Возможность применения программ самодиагностики в этих случаях следует предусматривать при проектировании МПС.

7.2. Программные средства диагностирования компьютеров

Программные средства диагностирования применяются для сложных систем, диагностика которых только аппаратными средствами либо недостаточна, либо требует сложного диагностического оборудования.

Программное обеспечение (ПО) для диагностирования должно содержать систему автоматизированного синтеза тестов, операционную систему, язык программирования с соответствующими трансляторами. Различают универсальное (УПО) и специализированное (СПО) программное обеспечение. Как правило, УПО используют для организации работы встроенных аппаратных средств диагностирования, СПО позволяет более эффективно решать отдельные задачи диагностирования.

Известны системы подготовки тестов «ФЛЭШ», язык высокого уровня «МЭПС», предназначенный для упрощения и сокращения этапа подготовки тестовых программ, язык тестирования «МЭМтест-IV» для цифровых и аналоговых процедур проверки и многие другие [12].

Программы, используемые в настоящее время, разрабатываются с учетом необходимости обеспечения успеха на рынке. Для этого они должны обладать такими качествами, как:

- функциональность, т.е. программа должна полностью удовлетворять потребности пользователя;
- наглядный, удобный, интуитивно понятный и привычный пользователю интерфейс (способ взаимодействия программы с пользователем);
- простота освоения даже начинающими пользователями, для чего применяются информативные подсказки, встроенные справочники и подробная документация;
- надежность, т.е. устойчивость программы к ошибкам пользователя, отказам оборудования и т.п.

В связи с распространением компьютерной техники особое значение приобретают программы диагностирования компьютерных средств. Крупнейшие производители программных продуктов предлагают широкий спектр специализированных и универсальных программ.

Пакет программ *Norton Utilites* (*NU*). Утилиты пакета позволяют защитить данные на компьютере, в некоторых случаях восстановить информацию, разрушенную при сбоях работы с диском, и т.д.

В составе пакета имеются следующие утилиты:

Norton System Check – комплексная проверка системы, проверяет жесткий диск, сканирует реестр Windows 98, а также выполняет ряд других операций, способствующих увеличению производительности компьютера.

Norton WinDoctor – оптимизатор реестра (базы данных, в которой хранятся различные параметры Windows). Утилита WinDoctor сканирует реестр, обнаруживает в нем ошибки и лишние записи. Утилита контролирует корректность ярлыков программы и «ассоциаций» (принадлежности расширений типу файлов). После завершения работы утилита выводит на экран имеющиеся проблемы и дает возможность оператору их поправить.

Norton DiskDoctor – программа, контролирующая физическое и логическое состояние жесткого диска. Физическое состояние характеризуется наличием (или отсутствием) на диске повреждений носителя информации, например магнитного слоя. Логическое состояние определяется наличием (или отсутствием) различных повреждений файловой системы, например «потерянных» фрагментов данных и других логических ошибок.

Norton Connection Doctor проверяет установленный в компьютере модем и тестирует соединение с Интернетом.

Norton UnErase осуществляет поиск и восстановление удаленных (стертых) файлов и директорий. Программа определяет вероятность восстановления [возможно (good) или невозможно (excellent)].

Norton Speed Disc – утилита оптимизации доступа к жесткому диску. Она позволяет увеличить скорость считывания данных с диска за счет минимизации перемещения считывающих головок. Для этого программа дефрагментирует файлы и перемещает свободное пространство в конец диска на дорожки, которые находятся дальше от считывающих головок.

Norton Optimize Wizard – мастер оптимизации. Главная функция – уменьшить размер реестра, удалив из него «пустые» и лишние записи. Кроме этого программа может оптимизировать расположение на диске Swap-файла (участок диска (КЭШ), который система использует при нехватке оперативной памяти). Следует заметить, что пользоваться этой утилитой надо с осторожностью. Это относится и к следующей утилите.

Norton Space Wizard – программа чистки диска от ненужных файлов, например временных файлов с расширением .tmp, создаваемых Windows, резервных копий документов и системных файлов с расширением .bak, а также лишних копий файлов.

Norton System Doctor. Эта программа после запуска выполняет сразу несколько операций: проверяет диск на наличие вирусов и ошибок; определяет потребность в дефрагментации диска, сканирует Norton Utilites на предмет необходимости обновления. Программа показывает, насколько загружен процессор, сколько оперативной памяти используется, сколько свободного места осталось на диске и т.д. Однако её недостаток состоит в том, что программа сама очень сильно загружает процессор.

Norton Rescue Disc позволяет создать системную загрузочную дискету со всеми необходимыми системными файлами и утилитами для восстановления системы в случае сбоя. Объем резервного комплекта – около 8 Мб.

Norton Wipeinfo позволяет удалять файлы с компьютера таким образом, что их восстановление оказывается невозможным. Программа не просто удаляет файл, а ещё забивает освободившееся место «пустыми» символами по несколько раз.

Norton Recykle Bin – улучшенная, «защищенная» корзина для Windows. Если из стандартной корзины можно восстановить только то, что в ней лежит, то «защищенная» способна осуществлять поиск удаленных файлов по всему диску и возвращать их.

Norton System Information позволяет получить информацию о компьютере: какие комплектующие используются, какие драйверы и программы установлены, какова производительность процессора и других компонентов. Программа может дать более полную и полезную информацию, чем вкладка «Система» в панели управления Windows.

Norton Live Update – программа для обновления Norton Utilites, работает при соединении с Интернетом. Она может соединяться с сервером Symantec, находить обновление антивирусных баз или патчи для программ Norton Utilites, скачать их из сети и выполнить процедуру установки. После этого нужно перезагрузить компьютер, и обновленная программа будет готова к использованию.

Norton Crach Guard и Norton Crach Guard Deluxe. Иногда при работе Windows в системе наблюдается сбой из-за конфликтов программ. При таком сбое может появляться сообщение об ошибке, и происходит аварийный выход из Windows с потерей всех несохраненных данных. Подобная ситуация называется *Crach* (созвучно с «крах»). Это происходит из-за того, что некоторые программы в Windows используют одно и то же адресное пространство в памяти, не будучи изолированными друг от друга. Программы *Crach Guard* и *Crach Guard Deluxe* не только перехватывают «крахи», но и исправляют их. Теперь при «крахе» на экране будет появляться не стандартное окно ошибки Windows, а окно Norton Crach Guard, которое дает возможность попытаться «разморозить» зависшее приложение. При этом пользователь получит время, чтобы сохранить результаты своей работы.

Программа *Norton Crach Guard Deluxe* – это расширенный вариант первой. Она может дополнительно проверить жесткий диск и исправить ошибки на нем, а также проверить реестр. Эти программы совершенно автономны и могут функционировать отдельно, несмотря на то, что входят в состав Norton Utilites.

Программа *Everest Ultimate Editon*. Она служит для диагностики и тестирования аппаратных средств компьютера, представляет информацию об аппаратном и программном обеспечении, тестирует модули ПК и выдает рекомендации по их совершенствованию. Про-

грамма отображает информацию о CPU, материнской плате, жестком диске, системных шинах, температурных сенсорах и установленных программах. Встроенная база данных программы имеет подробную информацию о более чем 22000 компьютерных компонентов. Программа тестирует монитор, память, определяет стабильность работы системы, оценивает производительность CPU. Результатом работы программы является подробный отчет о составе, свойствах и качестве работы всех узлов компьютера.

Ценным свойством программы Everest является возможность её использования практически на любом компьютере без установки на жесткий диск этого компьютера. С помощью программы можно легко определять установленные устройства, быстро получить помощь от технической поддержки, сведения о драйверах для устройств и оптимальном программном обеспечении, доступ к последним обновлениям. Программа Everest позволяет сравнить результаты тестирования компьютера с подобными для других систем. Стабильность работы тестируемой системы программа Everest оценивает по эффективности системы охлаждения, способности компьютера обрабатывать большие программы, по результатам тестирования числа обращений к компонентам системы и их состоянию при большой частоте обращений. Таким образом, программа Everest обнаруживает системную нестабильность и дает рекомендации по её устранению.

Программный диагностический пакет *Fix-It Utilities* (объем ≈ 115Мб). Это разработка компании Ontrack Data Systems (Великобритания), содержащая средства для мониторинга, анализа и оптимизации системы, для коррекции программных проблем. Программа позволяет постоянно отслеживать критические параметры системы, такие как использование памяти, степень загрузки процессора, свободное дисковое пространство.

Fix-It Utilities корректно работает под управлением любой из версий Windows. Полный пакет содержит 28 утилит, сгруппированных в шесть основных разделов:

- *Fix Wizard* – мастер для комплексной проверки и настройки системы;
- *Disk and Files* – комплект утилит для обслуживания дисков и файлов;
- *System Registry* – комплект для обслуживания системного реестра;

• *System Diagnostics* – инструментальные средства диагностики системы;

• *System Protection* – комплект утилит для защиты и поддержания целостности системы;

• *Crisis Center* – утилиты и сервисы для восстановления данных после краха системы.

Fix Wizard позволяет запустить в работу целый ряд утилит из пакета с предварительной настройкой процедур. В число таких процедур входит поиск вирусов, создание резервных копий основных системных файлов, очистка, проверка и дефрагментация жесткого диска, оптимизация системного реестра.

Disk and Files содержит утилиты для проверки жестких дисков и исправления некоторых ошибок. Программа позволяет поддерживать «чистоту» на дисках компьютера путем дефрагментации диска и объединения воедино свободного пространства. Утилита *Disk Snapshot*, входящая в состав Disk and Files, создает копии загрузочных секторов дисков и FAT, которые целесообразно иметь на случай невозможности прочитать поврежденный диск. С большой долей вероятности восстановить потерянные данные можно, используя «свежий» образ системных областей диска.

System Registry позволяет исправлять ошибки в системном реестре Windows. Основной принцип исправления – поиск ошибочных ссылок в базе данных реестра и их удаление. Утилиты, входящие в этот раздел, позволяют выполнить дополнительную настройку Windows, например: изменить внешний вид рабочего стола, настроить клавиатуру и мышь, управлять процессом загрузки системы. Утилита *Reg Defrag*, входящая в состав System Registry, может преобразовать структуру реестра с целью уменьшения времени доступа к нему.

System Diagnostics имеет в своем составе пять утилит, позволяющих тестировать работоспособность практически всех компонентов компьютера. При тестировании выводится на экран изложение всей тестовой процедуры с указанием ориентировочного времени каждого теста, что создает удобство проведения диагностики. Имеется возможность группирования тестов по способу их исполнения и выбора варианта тестирования из трех видов: быстрый, стандартный, глубокий (самый продолжительный, но зато и самый полный).

Утилита *System Explorer*, входящая в состав System Diagnostics, представляет пользователю подробную информацию о текущем состоянии и настройке системы: компоненты, конфигурационные фай-

лы, параметры открытых окон, загруженные драйверы, сведения о носителях информации, работающих программах. По каждому пункту выдается подробный отчет, который можно распечатать.

Утилита *Smart Defender* представляет информацию о работе системы самодиагностики жестких дисков Smart, которая повсеместно используется во всех современных винчестерах. Программа контролирует текущее состояние жесткого диска и по ряду косвенных признаков может предсказать ориентировочный срок его безотказного функционирования.

System Protection позволяет в некоторых случаях разморозить зависшие приложения (утилита *CrachProof*). Утилита *Easy Recovery*, входящая в состав System Protection, считается эффективной при восстановлении информации на жестком диске. Программа восстанавливает файлы, исходя не из таблицы FAT, как чаще всего бывает, а сканируя весь диск, кластер за кластером, и восстанавливает (по мере возможностей) все найденные цепочки данных. При этом восстановленные данные содержатся в памяти компьютера, а не «сбрасываются» на диск. Таким способом сохраняется возможность вернуться к первоначальному состоянию диска в случае неудачной попытки восстановления.

Пакет Fix-It Utilities отличается от других программных продуктов способностью выполнять анализ с исследованием компонентов, что позволяет выявлять проблемы ещё до того, как они приведут к серьезным последствиям.

Пакет тестирующих программ *SiSoft Sandra 2009*. Пакет был разработан как «помощник в проведении анализа и диагностики системы», о чем говорит аббревиатура Sandra (System Analyzer Diagnostic and Reporting Assistant). В состав полной версии пакета входят около 70 модулей для сбора информации обо всех основных компонентах ПК. Главное окно программы напоминает панель управления Windows с большим количеством ярлыков. Пакет поставляется в двух версиях: профессиональной и стандартной. Последняя – бесплатная, но имеет ограничения. Все утилиты, входящие в пакет, можно условно разделить на четыре класса: информационные, утилиты оценки производительности, просмотра системных файлов, тестирования.

Программа позволяет вывести на экран общую информацию о тестируемом компьютере, которая отражается в окне сводной информации (сведения о CPU, системных шинах, чипсете материнской платы, мониторе, дисководах, клавиатуре, установленных портах, звуковой карте, коммуникационных устройствах, версии Windows).

Информационная утилита пакета SiSoft Sandra *CPU & BIOS Information* выводит информацию о центральном процессоре и BIOS, может выдавать некоторые советы по замене этих компонентов.

PCI & AGP Buses Information сообщает сведения о самих шинах и об устройствах, к ним подключенных, представляет также информацию о номерах прерываний устройств. *Video System Information* позволяет получить данные о мониторе и видеоадаптере. *Drives Information* выдает информацию о всех дисководах системы.

Имеются также утилиты, сообщающие сведения о клавиатуре *(Keyboard Information),* звуковой карте (*Sound Card Information),* принтере (*Printer Information*). Информацию об установленных драйверах и связанных с ними устройствах можно получить, используя утилиту *MCI Devices Information*. Утилиты *Windows Information* и *WinSock Information* дают сведения о версии Windows и о встроенных библиотеках подпрограмм, осуществляющих связь с Интернетом.

Утилита *Process Information* выдает сведения о процессах, которые выполняются на компьютере в данный момент. При этом определяется, сколько оперативной памяти занимает данный процесс, какие динамические библиотеки (DLL) он использует, разрядность используемой информации и т.п. Данные о процессе отображаются в окне. Для получения информации утилиту Process Information нужно активизировать после запуска исследуемых программ, а нажав на кнопку *Update*, можно определить изменение состояния того или иного процесса.

Create и Report Wizard – мастер, создающий отчет о результатах тестирования компьютера. Сведения можно распечатать, записать на диск, передать по факсу. Производительность системы оценивается тестированием CPU, дисководов, оперативной памяти. Для этого используются соответствующие утилиты CPU: *Benchmark, Drivers Benchmark, CD-ROM Benchmark, Memory Benchmark* (*Benchmark,* в переводе на русский – отметка уровня). Результаты работы программы представляются в наглядной форме в виде гистограммы. Производительность оценивается, в основном, по быстродействию соответствующих компонентов.

Имеющийся состав утилит пакета SiSoft Sandra позволяет произвести стресс-тестирование компьютера путем запуска утилиты «Тест стабильности», используя набор «Эталонные тесты». При этом нужные модули надо отметить в соответствующем меню и настроить необходимые параметры. Результаты тестирования будут отражены на

экране и в отчете, где будут указаны время тестирования, параметры нагрева компонентов, напряжение питания, скорость вентилятора, загруженность процессора и т.п.

Эффективное использование рассмотренных пакетов программ для диагностирования компьютеров возможно только для тех пользователей, которые достаточно ясно представляют себе аппаратную часть и принцип действия компонентов, входящих в структуру компьютера.

7.3. Диагностика модемов

Модем – это устройство, предназначенное для связи с внешней средой в системе электронных коммуникаций [17]. Важным видом коммуникации являются, например, телефонные аналоговые сети. Компьютер – это цифровое устройство, поэтому для его стыковки с телефонной сетью служит модем, который переводит цифровые сигналы в аналоговые и наоборот. Структура соединения двух вычислительных устройств (ВУ1 и ВУ2) в локальную сеть с помощью модемов МДМ1 и МДМ2 приведена на рис. 7.3.

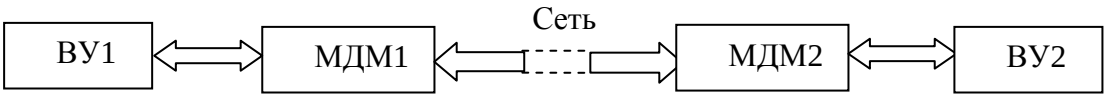


Рис. 7.3. Структурная схема использования модемов для соединения двух вычислительных устройств через телефонную сеть

В конструктивном отношении модем может быть встроенным в компьютер либо представлять собой отдельное устройство настольного типа.

В первом случае модем существует в компьютере как плата расширения. Он может быть предназначен для интерфейса ISA либо интерфейса PSA. Для подобных модемов диагностику целесообразно проводить в составе компьютера, используя либо собственные ресурсы компьютера, либо диагностические программы, устанавливаемые на жесткий диск специально для диагностирования системы, в том числе и встроенного модема.

Внешний модем подключается к компьютеру через COM-порт, а к телефонной линии – через специальный адаптер (сплиттер).

При появлении проблем с модемом, в первую очередь, необходимо проверить соответствующие соединения и убедиться в их исправности и работоспособности. COM-порт компьютера может быть проверен средствами ОС компьютера. В простейшем случае работоспособность COM-порта проверяют, подключив к нему, например, мышь. При необходимости используют специальные программы и переходники-заглушки к разъемам DB9-DB25, распределение сигналов по контактам которых должно соответствовать определенным правилам (табл. 7.1).

Таблица 7.1

Назначение контактов

Сигнал	№ контактов DB9	№ контактов DB25	Направление
DCD	1	8	Вход детектора принимаемого сигнала
RX	2	3	Вход (прием данных)
TX	3	2	Выход (передача данных)
DTR	4	20	Выход (OOD готово)
GND (SG)	5	7	Сигнальная земля
DSR	6	6	Вход (АПД готова)
RTS	7	4	Выход (запрос передачи)
CTS	8	5	Вход (готов к передаче)
R1	9	22	Вход (индикатор вызова)

Если используются заглушки, то схема соединения контактов в них должна соответствовать рекомендациям для COM-портов (рис. 7.4).

Рис. 7.4. Схемы петлевых заглушек для COM-портов

В качестве тестирующих программ можно рекомендовать CheckIt и Norton Diaqnostics (из пакета Norton Utilites). В программе нужно выбрать проверку данного порта с опцией *loop-back*. Будут проверены выходные цепи, регистры, UART, внутренние цепи. После проверки COM-порта следует приступить к диагностике модема.

Большинство проблем модема обусловлены либо неверной настройкой, либо конфликтом с другими устройствами. Эти проблемы могут быть обнаружены не только внешними диагностическими программами, но и средствами ОС Windows 9X и более новых версий. Для проверки, например, в Windows 95 можно воспользоваться панелью списка модемов *(setting /control panel/ modems)* и кнопкой *diaqnostics*. В результате появится панель со списком портов и закрепленных за ними устройств. Выбрав порт, который использует модем, нужно нажать кнопку *more info*, и после тестирования выведется окно результатов. Если тест не проходит, выводится сообщение о том, что модем не отвечает, и дается совет по исправлению ситуации.

Известной программой, осуществляющей диагностику порта компьютера и самого модема, является также программа BitWare, тестирующая все возможности обычного модема.

Наиболее эффективно использование терминального программного обеспечения, позволяющего работать с модемом напрямую через его команды. К таковым относятся Telemate (DOS) и Giper Terminal (Windows 95). С помощью этих программ можно проверить модем на прохождение команд, функцию набора номера, осуществить и проверить режим самодиагностики. Тесты, выполняемые с помощью команд группы &T, осуществляются в трех режимах:

1) при аналоговом шлейфе (аналоговая петля);
2) локальном цифровом шлейфе;
3) удаленном цифровом шлейфе.

Первый вид теста используется для проверки работы передатчика (ПРД) и приемника (ПРМ) модема (МДМ), для чего выход передатчика соединяется с входом приемника, причем оба устройства отсоединяются от интерфейса телефонной линии (ИТФ ТЛ) (рис. 7.5).

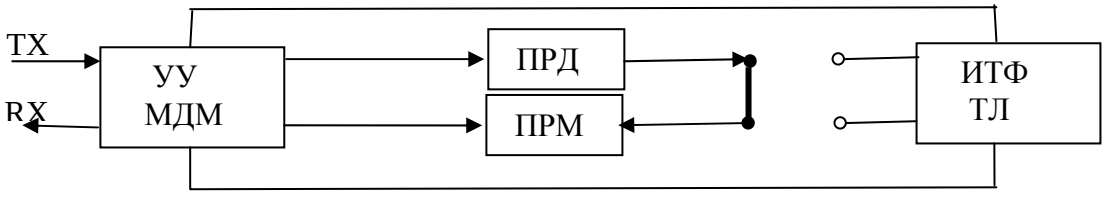


Рис. 7.5. Направление движения потока данных при тестировании с аналоговой петлей

Существуют два варианта тестирования:

- с вводом данных пользователем и сравнением результатов ввода и приема данных на экране;

- в режиме самотестирования, когда модем сам посылает свою тестирующую (эталонную) последовательность на свой передатчик, который возвращает её через шлейф на вход приемника. Внутренний анализатор ошибок зафиксирует все ошибки и по окончании теста выдаст на экран количество ошибок.

После тестирования с помощью аналогового шлейфа нужно тестировать модем в режиме цифрового шлейфа (цифровой петли). Этот тест может помочь обнаружить проблемы, связанные с телефонной линией и с удаленным модемом. В данном случае движение потока данных осуществляется от одного модема к другому и обратно через интерфейсы телефонных линий и приемники/передатчики двух модемов, один из которых уже прошел успешное тестирование с аналоговой петлей.

Тестирование производится со стороны удаленного модема 2 по соглашению с пользователем модема 1. Целостность линии оценивает пользователь модема 2. Он же заодно и тестирует свой модем. Для того, чтобы это мог сделать и пользователь модема 1, по соглашению с пользователем модема 2 нужно установить удаленный цифровой шлейф (рис. 7.6). Это делается по запросу пользователя модема 1. При этом модем проверяется при работе с линией, при заданной скорости передачи и в заданных режимах.

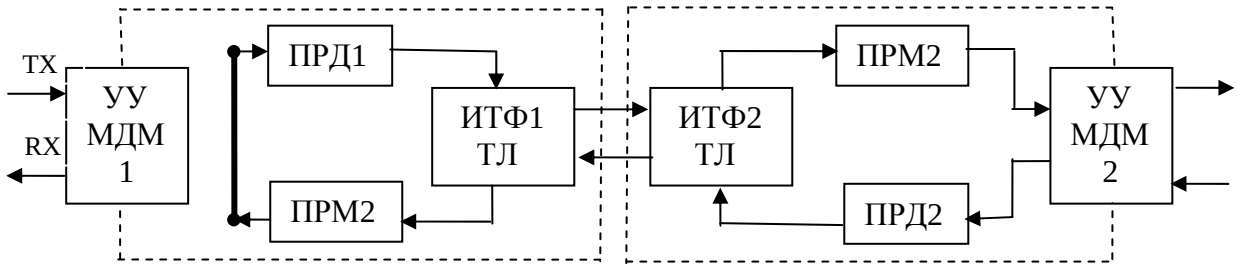


Рис. 7.6. Направление движения потока данных при тестировании с цифровой петлей

Если требуется исключить из тракта один из модемов, можно использовать удаленный шлейф непрерывного канала. Если установлено, что в линии связи имеется неисправность, то для более точной локализации последней необходимо проверить характеристики линии связи, т.е. канала тональной частоты.

Проверка канала тональной частоты. Состояние канала тональной частоты (ТЧ) характеризуется *затуханием*, *частотной*

характеристикой, *уровнем помех*. Затухание сигнала определяется путем замера уровней сигнала эталонной частоты на выходе модема передающей стороны и на входе модема принимающей стороны с помощью измерителей уровня. Если затухание находится в пределах допустимого, проверяют другие характеристики линии. Если затухание велико, то выполняется поиск участка тракта, в котором происходит это затухание.

Второй параметр – частотная характеристика (ЧХ). Канал ТЧ должен иметь ЧХ, удовлетворяющую определенным требованиям, которые задают максимально допустимую разницу (в децибелах) между затуханием на эталонной частоте и других частотах. Сигналы на частотах <300 и >3400 Гц затухают настолько сильно, что непригодны для передачи. Поэтому считается, что полоса пропускания канала ТЧ равна 3100 Гц.

Измерения ЧХ делают специальной аппаратурой, которая позволяет измерять частоту передаваемого сигнала и его затухание на приемном конце линии. Можно также использовать звуковой генератор и измеритель уровня с последующим подсчетом затухания на каждой частоте.

ЛИТЕРАТУРА

1. Технические средства диагностирования: справочник / В.В. Клюев, П.П. Пархоменко, В.Е. Абрамчик и др.; под общей редакцией В.В. Клюева. – М.: Машиностроение, 1989. – 672 с., ил.

2. Электроника: Энциклопедический словарь / гл. ред. В.Г. Колесников. – М.: Советская энциклопедия, 1991. – 688 с.: ил.

3. Электрические измерения: учебное пособие для вузов / Б.Н. Малиновский, Р.М. Демидова-Панферова, Ю.Н. Евланов и др.; под ред. д-ра техн. наук Б.Н. Малиновского. – М.: Энергоатомиздат, 1985. – 416 с., ил.

4. Кончаловский, В.Ю. Цифровые измерительные устройства: учебное пособие для вузов / В.Ю. Кончаловский. – М.: Энергоатомиздат, 1985. – 304 с., ил.

5. Справочник проектировщика АСУТП / Г.Л. Смилянский, Л.З. Амлинский, В.Я. Баранов и др.; под ред. Г.Л. Смилянского. – М.: Машиностроение, 1983. – 527 с., ил.

6. Каган, Б.М. Основы эксплуатации ЭВМ: учебное пособие для вузов / Б.М. Каган, И.Б. Мкртумян. – М.: Энергоатомиздат, 1988. – 432 с.: ил.

7. Справочник по цифровой вычислительной технике / Б.Н. Малиновский, В.Я. Александров, В.П. Боюн и др.; под ред. Б.Н. Малиновского. – К.: Техника, 1980. – 320 с., ил.

8. Цымбал, В.П. Задачник по теории информации и кодированию / В.П. Цымбал. – Киев: Вища школа, 1976. – 276 с.: ил.

9. Согомонян, Е.С. Самопроверяемые устройства и отказоустойчивые системы / Е.С. Согомонян, Е.В. Слабоков. – М.: Радио и связь, 1989. – 208 с.: ил.

10. Каган, Б.М. Электронные вычислительные машины и системы: учебное пособие для вузов / Б.М. Каган. – М.: Энергоатомиздат, 1991. – 592 с.: ил.

11. Полупроводниковые БИС запоминающих устройств: справочник / В.В. Баранов, Н.В. Бекин, А.Ю. Гордонов и др.; под ред. А.Ю. Гордонова и А.Ю. Дьякова. – М.: Радио и связь, 1987. – 360 с.: ил.

12. Микропроцессоры: системы программирования и отладки / В.А. Мясников, М.Б. Игнатьев, А.А. Кочкин, Ю.Е. Шейнин; под ред. В.А. Мясникова, М.Б. Игнатьева. – М.: Энергоатомиздат, 1985. – 272 с., ил.

13. Токхейм, Р. Основы цифровой электроники: [пер. с англ.] / Р. Токхейм. – М.: Мир, 1988. – 392 с.: ил.

14. Микропроцессоры: в 3 кн. Кн. 3. Средства отладки, лабораторный практикум и задачник: учебник для втузов / Н.В. Воробьев, В.Л. Горбунов, А.В. Горячев и др.; под ред. Л.Н. Преснухина. – М.: Высшая школа, 1986. – 351 с.: ил.

15. Ефремов, В.Я. Сигнатурный анализатор / В.Я. Ефремов // Микропроцессорные средства и системы. – 1987. – № 6. – С. 46 – 51.

16. Однокристальные микроконтроллеры PIC12C5X, PIC12C6X, PIC16X8X, PIC14000, M16c/61/62 / пер. с англ. и ред. Б.Я. Прокопенко. – 2-е изд. – М.: Издательский дом «Додэка-XXI», 2001. – 336 с.: ил.

17. Нефедов, В.И. Основы радиоэлектроники и связи: учебник для вузов / В.И. Нефедов. – 3-е изд., испр. – М.: Высш. шк., 2005. – 510 с.: ил.

Учебное издание

Ерёменко Владимир Тарасович
Рабочий Александр Александрович
Невров Иван Иванович
Воронина Оксана Александровна
Георгиевский Александр Евгеньевич
Донцов Венедикт Михайлович

ТЕХНИЧЕСКАЯ ДИАГНОСТИКА ЭЛЕКТРОННЫХ СРЕДСТВ

Учебник

Редактор Т.Д. Васильева
Технический редактор Т.П. Прокудина

Федеральное государственное бюджетное образовательное
учреждение высшего профессионального образования
«Государственный университет - учебно-научно-
производственный комплекс»
Лицензия ИД № 00670 от 05.01.2000 г.

Подписано к печати 17.02.2012 г. Формат 60х84 1/16.
Усл. печ. л. 9,8. Тираж 100 экз.
Заказ №_____

Отпечатано с готового оригинал-макета
на полиграфической базе ФГБОУ ВПО «Госуниверситет - УНПК»,
302030, г. Орел, ул. Московская, 65.