

Федеральное агентство по образованию Российской Федерации.  
Российский Государственный Университет нефти и газа им. И. М.  
Губкина

Кафедра информационно-измерительных систем

**Ю.А.ДАДАЯН**  
**ПОМЕХОУСТОЙЧИВОЕ КОДИРОВАНИЕ**

Учебное пособие для студентов специальности  
«Информационно-измерительная техника и технологии»  
по курсу  
«Преобразование измерительных сигналов»

Москва, 2009 г

Содержание:

1. Помехи и помехоустойчивость. Общее описание.....	3
2. Методы передачи цифровой информации .....	11
3. Помехоустойчивое кодирование .....	32
4. Циклический код.....	44
5. Принципы построения кодирующих и декодирующих устройств.....	56
6. Код Хэмминга .....	67

## 1. Помехи и помехоустойчивость.

### Общее описание

В современных информационно-измерительных системах для объектов нефтегазовых отраслей важное значение имеет надежность и достоверность передачи измерительной информации от объектов в виду их значительной удаленности друг от друга и наличии промышленных помех больших уровней.

Известно, что каналы связи, по которым передается измерительная информация, практически никогда не бывают идеальными. В них могут всегда присутствовать помехи. Отличие лишь в уровне помех и в их спектральном составе. Помехи в каналах связи образуются по различным причинам, но результат воздействия их на передаваемую информацию всегда один – информация искажается.

Помехой называется стороннее возмущение, действующее в системе и препятствующее правильному приему сигналов. Помехи бывают промышленные и атмосферные, закономерные и случайные, внутренние и внешние. Промышленные помехи возникают при работе двигателей станков, лифтов и кранов, сварочных аппаратов, рентгеновских установок. К промышленным относятся так же помехи, создаваемые городским электротранспортом. Атмосферные помехи – молнии, пыльные и снежные бури, северное сияние, иней на антенне и даже солнечное излучение (в УКВ диапазоне).

Если помеха регулярная, то не трудно найти ей противодействие. Например, фон можно устранить компенсацией, помеху от соседней радиостанции – применив соответствующий фильтр.

Если помеха случайная, то бороться с ней сложнее. Случайные помехи подразделяются на аддитивные и мультипликативные.

Аддитивной называется помеха, которая суммируется с сигналом. Аддитивная помеха существует независимо от сигнала и может наблюдаться как при наличии сигнала, так и при его отсутствии. Действие аддитивной помехи характеризуется величиной

$$U_a(t) = U_c(t) + U_\zeta(t)$$

Где  $U_c$  и  $U_\zeta$  – напряжения соответственно сигнала и помехи.

Наиболее универсальная причина аддитивной помехи – флуктуации, т. е. колебания случайных величин около их среднего значения. Примером флуктуации может быть броуновское движение молекул, дробовый эффект в электронных лампах и др. Флуктуационная помеха принципиально неустранима. Бороться с ней можно, применяя сложные схемы и режимы, но полностью ее устранить нельзя.

Мультипликативная помеха проявляется только при передаче сигналов, и действие ее заключается в многократном их усилении или ослаблении. Природа мультипликативной помехи состоит в случайном изменении параметров канала связи. Например, суточное и сезонное распространение коротких волн и пр. Действие мультипликативной помехи может характеризоваться величиной

$$U_m(t) = \gamma \cdot U_c(t),$$

где  $\gamma$  – некоторый коэффициент, учитывающий изменение параметров связи.

Перечисленные помехи являются внешними.

Помехоустойчивостью называется способность системы осуществлять прием информации в условиях наличия помех в линии связи.

При анализе информационных систем различают помехоустойчивость системы к ложным срабатываниям от помех в линии связи в тот момент, когда информация не передается (статическая помехоустойчивость) и способность системы выделять полезные сигналы из шумов (динамическая помехоустойчивость). Статическую помехоустойчивость оценивают средним числом ложных сигналов, образуемых из помех за единицу времени, а динамическую – средним числом ложных команд, образуемых из переданных за единицу времени (включая непринятые сигналы).

Количественно помехоустойчивость характеризуют степенью соответствия принятого сообщения переданному. Эту величину называют критерием верности (достоверности) передачи информации.

При передаче дискретных сообщений влияние помех проявляется в том, что вместо того или иного передаваемого символа принимается другой. Такое случайное событие называют ошибкой. Простейшим критерием верности при передаче дискретных сообщений является вероятность появления ошибки при передаче одного символа или одного бита информации.

При передаче непрерывных аналоговых сообщений степень соответствия переданного и принятого сигналов характеризует случайная величина отклонения принятого сигнала  $y(t)$  от переданного  $x(t)$ . Мерой отклонения обычно служит расстояние  $\varepsilon$

между  $y(t)$  и  $x(t)$ . Критерием верности в этом случае является вероятность  $P_0$  того, что наблюдаемое отклонение будет меньше некоторого заданного  $\varepsilon_0$ :

$$p_0 = p(\varepsilon < \varepsilon_0)$$

Основы теории помехоустойчивости были заложены академиком В. А. Котельниковым в работе «Теория потенциальной помехоустойчивости».

Потенциальной помехоустойчивостью В.А. Котельников называл предельно достижимую помехоустойчивость передачи информации при заданной помехе.

Основными задачами теории помехоустойчивости является выбор и обоснование критериев верности для различных условий передачи информации, анализ помехоустойчивости методов и алгоритмов передачи информации, техническая реализация оптимальных методов и алгоритмов передачи информации.

Общими методами борьбы с регулярными помехами являются: превышение уровня сигнала над уровнем шумов (помех), методы накопления сигналов, построение кодов с обнаружением и исправлением ошибок и т. д.

Рассмотрим некоторые из них.

#### 1. Увеличение отношения сигнал/помеха

Вероятность правильного приема зависит от интенсивности помехи по сравнению с интенсивностью сигнала. Интенсивности сигнала и помехи принято выражать их средними мощностями. Для краткости эта величина называется отношением сигнал/помеха.

Самый простой и очевидный способ увеличения отношения сигнал/помеха состоит в увеличении мощности сигнала. Увеличение мощности сигнала приводит соответственно к увеличению мощности источника питания, габариты и вес всей системы.

## 2. Метод накопления

Рассмотрим этот метод на примере сигнала в виде прямоугольных импульсов (рис 1).

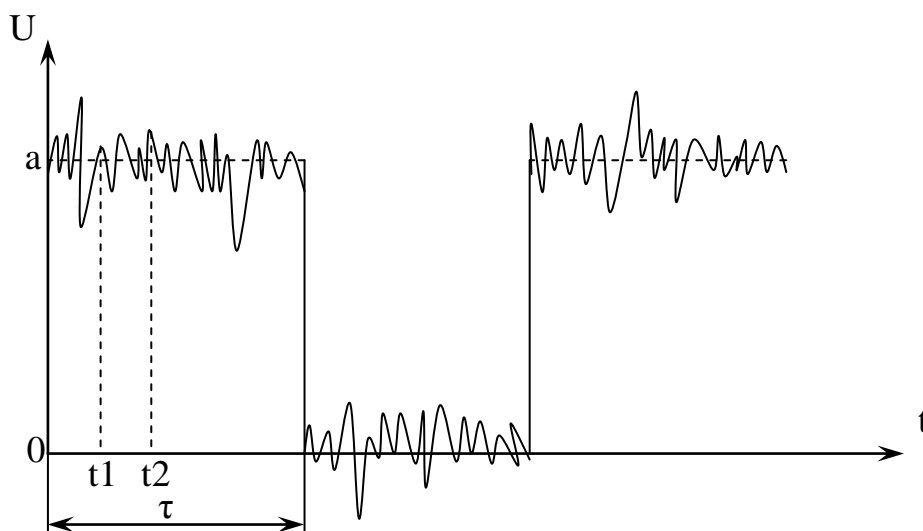


Рис.1.

На передаваемый сигнал в виде прямоугольных импульсов накладывается случайная помеха со средним значением, равным нулю. Если производить прием методом пробы, т. е. брать отсчет принимаемого сигнала в некоторый момент на протяжении действия импульса, то получим

$$y = a + \xi,$$

где  $\xi$  – случайная величина, выражающая мгновенное значение помехи в момент отсчета.

Отношение сигнал/помеха можно в этом случае выразить как

$$\rho_0 = \frac{a^2}{\overline{\xi^2}}$$

Где  $\overline{\xi^2}$  – средний квадрат помехи.

Если взять на протяжении действия импульса не один, а несколько отсчетов в разные моменты времени, то получим:

$$\begin{aligned}y_1 &= a + \xi_1 \\y_2 &= a + \xi_2 \\&\vdots \\y_n &= a + \xi_n\end{aligned}$$

Составив сумму этих отсчетов:

$$y = \sum_{k=1}^n y_k = n \cdot a + \sum_{k=1}^n \xi_k$$

Первый член выражает полезный сигнал, второй помеху. Беря средние квадраты обоих членов, составим отношение сигнал/помеха.

$$\rho = \frac{n^2 \cdot a^2}{(\sum \xi_k^2)}$$

Если случайные величины  $\xi_k$  независимы, то имеем:

$$\rho = \frac{n^2 \cdot a^2}{n \cdot \overline{\xi^2}} = n \cdot \rho_0$$

т. е. при n-кратном повторении отсчетов отношение сигнал/помеха возрастает в n раз.



Вместо суммирования отдельных отсчетов можно выполнить интегрирование смеси сигнала с помехой на протяжении времени действия импульса.

$$y = \int_0^{\tau} [a + \xi(t)] dt = a \cdot \tau + \int_0^{\tau} \zeta(t) dt$$

Второе слагаемое в уравнении значительно меньше первого, так как помеха имеет знакопеременный характер.

### 3. Метод фильтрации.

Для увеличения отношения сигнал/помеха можно использовать различие в спектрах сигнала и помехи. Если бы спектры сигнала и помехи располагались в неперекрывающихся полосах, то сигнал мог бы быть полностью очищен от помех. Для этого достаточно было бы пропустить смесь сигнала и помехи через полосовой фильтр с соответствующей полосой пропускания.

В действительности спектры сигнала и помехи практически всегда перекрываются. И тем не менее, применение фильтров может значительно увеличить отношение сигнал/помеха.

Предположим, исходные спектры сигнала и помехи имеют ширины одного порядка, но оба неоднородны (рис 2).

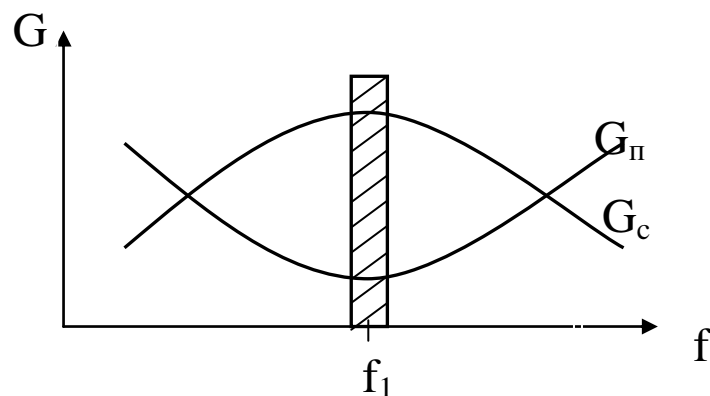


Рис.2

Для получения наибольшего отношения сигнал/помеха нужно найти то значение частоты  $f_1$ , при котором имеется наибольшее

отношение  $G_C / G_{\Pi}$  и применить полосовой фильтр, пропускающий узкую полосу частот около  $f_1$ .

В этом случае форма входного сигнала не сохраняется: на выходе узкополосного фильтра будет сигнал, близкий по форме к синусоиде с частотой  $f_1$ , т. е. можно «обнаружить» сигнал.

Таким образом увеличение отношения сигнал/помеха может быть получен либо за счет увеличения мощности сигнала, либо за счет увеличения длительности сигнала, либо за счет расширения его спектра.

Разделение спектров помех и сигнала возможно при использовании различных видов модуляции (манипуляции) сигналов при передаче по каналам связи.

#### Контрольные вопросы.

1. Укажите признаки классификации помех.
2. Как определяют помехоустойчивость передачи информации?
3. Что такое критерий верности?
4. Что понимают под потенциальной устойчивостью?
5. Опишите методы борьбы с регулярными помехами: метод накопления, метод фильтрации и другие.

## 2. Методы передачи цифровой информации.

Все больший практический интерес приобретают дискретные системы связи. Передаваемые в этих системах дискретные сообщения подвергаются кодированию.

Кодирование – это преобразование сообщений в определенное сочетание элементарных дискретных символов, называемые кодовыми комбинациями.

Коды – это система соответствий между сообщениями и сочетаниями символов (сигналов). Элементарные символы, из которых формируются кодовые комбинации, называются элементами кода.

Число  $m$  различных типов элементов, используемых при построении кода, называется основанием кода.

Число  $N$  различных кодовых комбинаций называется объемом кода.

Число  $n$  элементов, образующих кодовую комбинацию, называется значностью кода. Если значность одинакова для всех элементов сообщений, то код называется равномерным.

При рассмотрении взаимодействия источника информации и канала связи возникают важные понятия производительности источника, пропускной способности канала и скорости передачи информации.

Под производительностью источника понимается скорость создания информации, т. е. количество информации, создаваемое источником в единицу времени (обычно в секунду).

Для дискретного источника создающего  $N_1$  элементов в секунду, производительность

$$J_1 = H(x) \cdot N_1 \frac{\text{бит}}{\text{с}},$$

где  $H(x)$  – энтропия, равная количеству информации на один элемент в среднем.

Под скоростью передачи информации по каналу понимается количество информации, получаемой единицу времени. Для дискретного источника скорость передачи информации

$$R = \frac{1}{T} [H(C) - H(C/D)],$$

где  $H(C)$  – энтропия отправленных последовательностей  $C$  элементов  $X_i$  общей продолжительностью в  $T$  с;

$H(C/D)$  – условная энтропия отправленных последовательностей с учетом полученных последовательностей  $D$  элементов  $Y_k$ .

Под пропускной способностью канала понимается максимально возможная скорость передачи информации, которую можно достигнуть выбором кодирования,

$$C = \max_{\text{по кодам}} \cdot \frac{1}{T} [H(C) - H(C/D)].$$

Если скорость создания информации  $J_1$  меньше пропускаемой способности, то имеется правило кодирования, при котором вероятность ошибок может быть сделана сколь угодно малой. При тех же условиях скорость передачи информации  $R$  может сколь угодно приближаться к пропускной способности канала.

Помехоустойчивое кодирование базируется на теореме Шеннона: «Для дискретного канала с шумом при скорости передачи

двоичных символов, меньшей чем пропускная способность канала, существует такой код, при котором вероятность ошибочного декодирования будет сколь угодно мала».

В процессе передачи по каналам связи кодовых комбинаций может осуществляться модуляция переносчика сигнала.

Модуляцией называется изменение параметра переносчика сигнала в соответствии с функцией, отображающей передаваемое сообщение. В качестве переносчика используются постоянный ток, переменный ток низкой или высокой частоты, периодическая последовательность коротких импульсов (например, многоканальные системы связи с временным разделением каналов). Параметрами переносчика, подлежащими модуляции, могут быть амплитуда, частота и фаза.

От вида модуляции в значительной степени зависят помехоустойчивость и пропускная способность системы связи.

В случае передачи дискретных сообщений каждый элемент кода (кодированный символ) передается отрезком сигнала длительностью  $T$ .

На рис. 3 приведены примеры эпюры двоичных сигналов при различных видах манипуляции для кодовой комбинации 10110.

Если в качестве переносчика используется постоянный ток, то манипуляция может быть осуществлена изменением величины тока (рис. 3а) либо его направления (рис. 3б). Наибольшее применение нашли в настоящее время дискретные системы связи, в которых элементы сигнала представляют собой ограниченные на конечном отрезке времени (от 0 до  $T$ ) гармонические колебания (рис. 3, в, г, д). К ним относятся системы с амплитудной, частотной или фазовой манипуляцией.

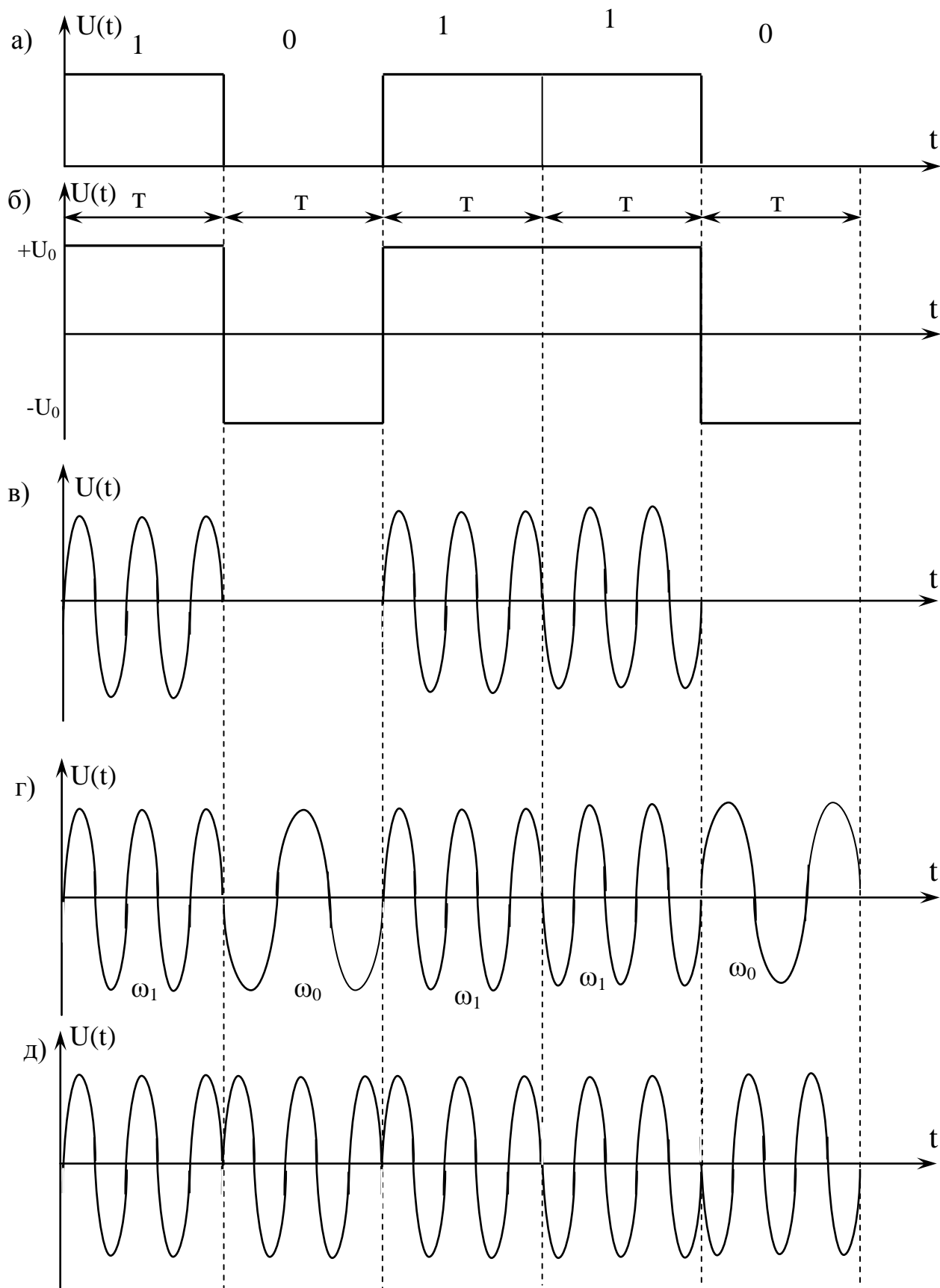


Рис.3

При амплитудной манипуляции (рис. 3в) передаче «1» соответствует наличие единичного элемента переменного тока длительностью  $T$ , передаче «0» – пауза, т. е.

$$U_{c1}(t) = U_{mc} \cdot \cos \omega t; \quad U_{c0}(t) = 0.$$

При частотной манипуляции (рис. 3г) передаче «1» соответствует элемент с несущей частотой  $\omega_1$ , передаче «0» – элемент с несущей частотой  $\omega_0$ , т. е.

$$U_{c1}(t) = U_{mc} \cdot \cos \omega_1 t; \quad U_{c0}(t) = U_{mc} \cdot \cos \omega_0 t.$$

При фазовой манипуляции (рис. 3д) передаче «1» соответствует определенная фаза несущего колебания элемента, передаче «0» – другая (обычно противоположная) фаза, то есть

$$U_{c1}(t) = U_{mc} \cdot \cos \omega t; \quad U_{c0}(t) = -U_{mc} \cdot \cos \omega t.$$

При амплитудной манипуляции огибающая повторяет форму первичного сигнала, т. е. получаются гармонические колебания, амплитуда которых имеет только два значения  $U_{mc}$  и  $0$ .

Если спектр модулирующего сигнала известен, то нетрудно построить спектр сигнала после амплитудной манипуляции по общему правилу; сместить спектр модулирующего сигнала на интервал частот, равный несущей частоте  $\omega_1$ , и зеркально отобразить относительно спектральной линии на несущей частоте.

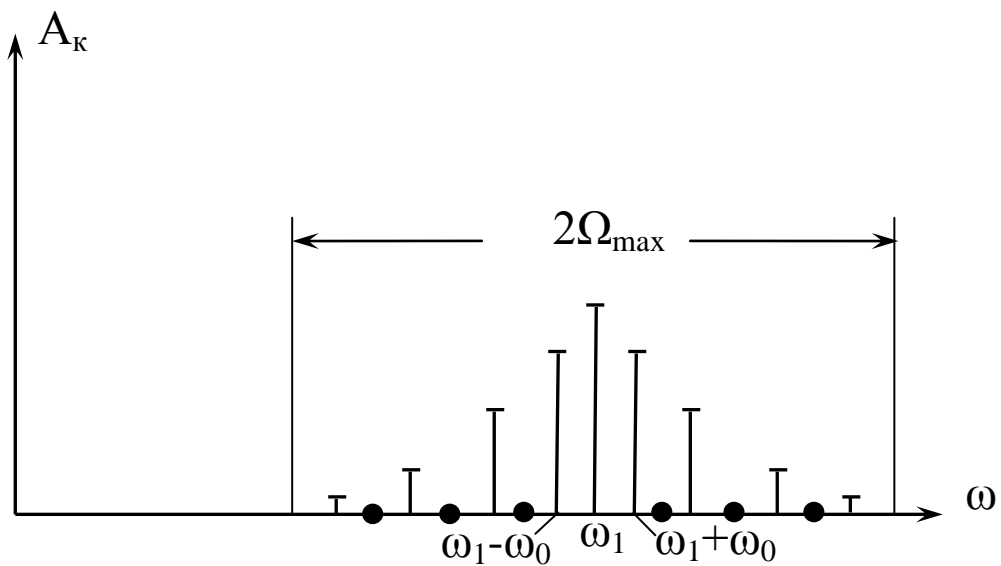


Рис. 4

На рис. 4. показан спектр сигнала после амплитудной манипуляции для случая, когда единичные элементы переменного тока чередуются с паузой. Амплитуды боковых частот постепенно уменьшаются в той же мере, как и амплитуды высших гармоник первичного сигнала.

Если спектр модулирующего сигнала ограничить при помощи фильтров частотой  $\Omega_{\max}$ , то ширина спектра сигнала после манипуляции составит  $2 \Omega_{\max}$ . Таким образом, в результате амплитудных манипуляций ширина спектра увеличилась вдвое. Спектр сигнала можно ограничивать полосовым фильтром с полосой пропускания  $2 \Omega_{\max}$ .

Ограничение полосы пропускания приводит к искажениям прямоугольной формы огибающей и тем самым восстановленного первичного сигнала после демодуляции. Но довольно часто практически достаточно полоса



$$2\Omega_{\max} = 2 \cdot 3\omega_0 = 6\omega_0 \quad (\omega_0 = \frac{2\pi}{T}),$$

где  $\Omega$  – полоса частоты спектра манипулированных сигналов (рис. 3а).

Сигнал после частотной манипуляции должен иметь два граничных значения частоты:

$$\omega_0 = \omega_{\min} \quad \text{И} \quad \omega_1 = \omega_{\max}$$

В общем случае при уменьшении частоты фаза сигнала может так же изменяться скачком. Спектр такого сигнала представлен на рис. 5.

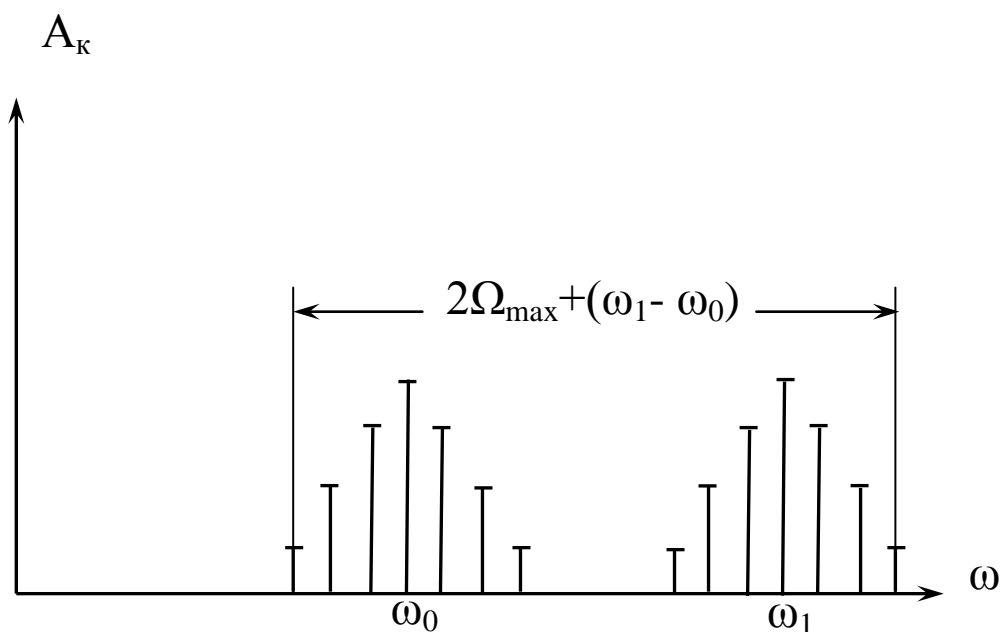


Рис.5

Необходимая ширина спектра равна  $2\Omega_{\max} + (\omega_1 - \omega_0)$ , т.е. больше чем при амплитудной манипуляции на величину  $\omega_1 - \omega_0$ .

Обычно для частотной манипуляции изменяют скачкообразно один из параметров генератора несущих колебаний. При таком

изменении параметра частота генерируемых колебаний так же изменяется скачком (рис. 3,г), т.е. отсутствует скачкообразное изменение фазы напряжения. Спектр такого частотно манипулированного сигнала состоит из колебаний на несущей частоте  $\omega_1$  и на боковых частотах  $\omega_1 \pm k\omega_0$ , как и в случае гармонического модулирующего сигнала, но амплитуды колебаний другие.

В последнее время все большее значение для передачи дискретной информации приобретает фазовая манипуляция.

В простейшем случае передачи сигналов двоичным кодом фазы несущего колебания, соответствующего посылке и паузе или положительному и отрицательному импульсам (рис. 3, а, б), отличаются на  $180^\circ$  (рис. 3д). Зная спектр сигнала при амплитудной манипуляции последовательностью прямоугольных импульсов нетрудно найти спектр при манипуляции по фазе на  $180^\circ$ . Спектр сигнала при манипуляции по фазе можно получить из спектра последовательности прямоугольных импульсов, увеличив вдвое амплитуду всех боковых составляющих и исключив колебания несущей частоты (рис. 6).

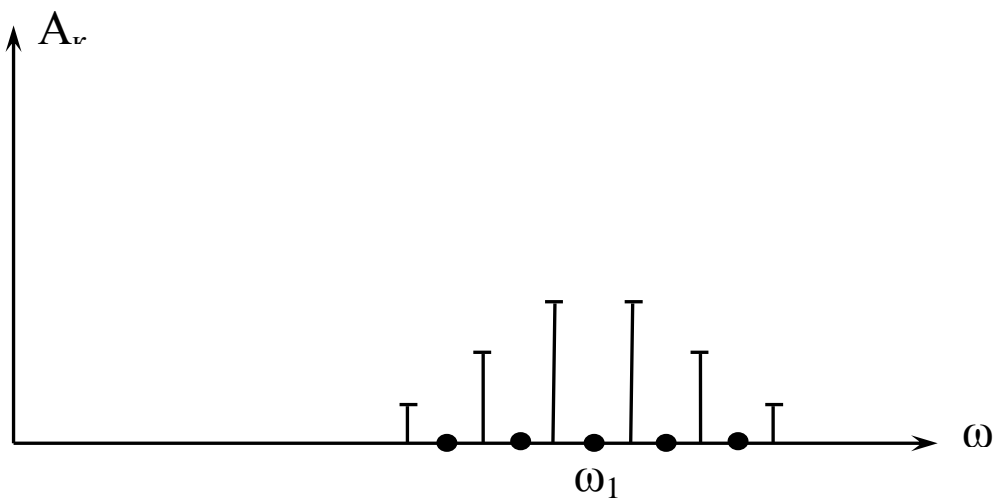


Рис.6

Оценим приведенные выше методы манипуляции сигналов с точки зрения помехоустойчивости.

При амплитудной манипуляции в случае некогерентного приема, т. е. когда сведения о фазе сигнала отсутствуют, единственным критерием, позволяющим отличить элемент, соответствующий «1» от паузы, является величина амплитуды колебаний. Если напряжение на выходе приемного устройства превышает некоторый пороговый уровень  $E_0$ , то фиксируется сигнал «0». В соответствии с этим приемное устройство должно содержать полосовой фильтр, обеспечивающий защиту от сосредоточенных помех соответствующего частотного диапазона и снижения уровня флуктуационных помех, а так же пороговое устройство разделяющего, «1» и «0».

Ошибки при приеме возникают если:

а) при передаче «1» суммарное напряжение сигнала и флуктуационной помехи на выходе приемника  $U_{с.п.}$  будет ниже порогового  $E_0$ , т. е.

$$U_{с.п.} < E_0$$

б) при передаче «0» напряжении помех  $U_{п.}$  окажется больше  $E_0$ , т. е.

$$U_{п.} > E_0$$

Для флуктуационных помех вероятность ложного приема зависит как от превышения сигнала над помехой, так и от величины порогового напряжения.

Вероятность ошибочного приема возникающего под влиянием флуктуационных помех, можно ориентировочно подсчитать по формуле:

$$P_{\text{ош. А. М.}} \approx \frac{1}{2} \cdot e^{-\frac{1}{4} \cdot \left( \frac{U_{\text{сэф}}}{\sigma_{\text{п}}} \right)^2}$$

где  $U_{\text{сэф}}$  – эффективное значение огибающей сигнал;

$\sigma_{\text{п}}$  – с.к.о. напряжения помехи.

Приемное устройство для частотно манипулированных сигналов должно содержать два канала с фильтрами на частоты  $f_0$  и  $f_1$ , амплитудные детекторы выпрямляющие напряжение  $U_{f_0}$  и  $U_{f_1}$  и схему сравнения со встречным включением выпрямительных напряжений. Полярность выходного напряжения на выходе дифференциального детектора зависит от того как, какое из сравнительных напряжений больше  $U_{f_0}$  или  $U_{f_1}$  (рис. 7).

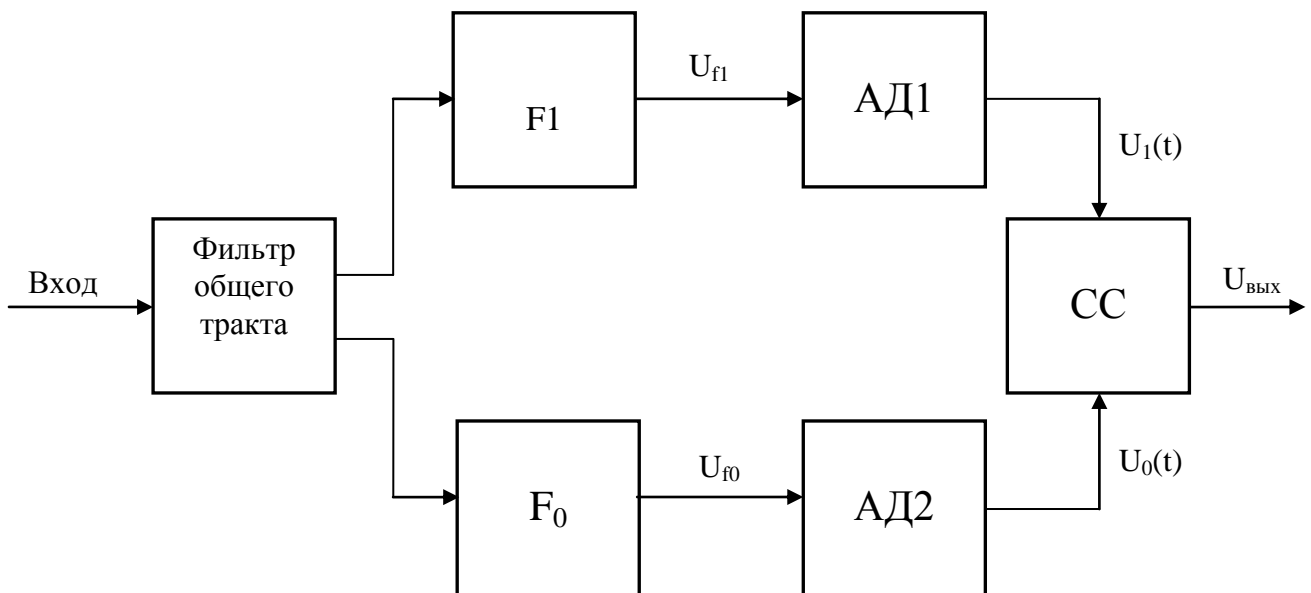


Рис.7

В отсутствие помех принятому элементу «1» соответствует неравенство  $U_{f_1} > U_{f_0}$  и  $U_{\text{вых}} > 0$ , элементу «0» соответствует неравенство  $U_{f_0} > U_{f_1}$  и  $U_{\text{вых}} < 0$ .

Ошибки при приеме возникают в том случае, если значение огибающей помехи  $U_{\text{п}}$  на выходе фильтра, через который в данный момент сигнал не проходит, превышает значение огибающей суммы сигнала и помехи  $U_{\text{с.п.}}$  на выходе другого фильтра, через который в данный момент проходит сигнал т. е.

$$P_{\text{ош}} = p\{U_{\text{п}} > U_{\text{с.п.}}\}$$

Принципиальное отличие от рассмотренного ранее случая амплитудной манипуляции состоит в том, что здесь нет порога ограничения  $E_0$ , превышение которого значения огибающей напряжения помех приводит к ошибке. Огибающая напряжения помех сравнивается здесь с величиной огибающей напряжения смеси сигнала и помехи  $U_{\text{с.п.}}$ , которая может принимать различные текущие значения. Каждому текущему значению  $U_{\text{с.п.}}$  соответствует определенная вероятность  $p_1$  его превышения значения огибающей напряжения помех  $U_{\text{п}}$ .

Рассмотрим метод фазовой манипуляции. Наибольшая ширина спектра соответствует передаче сигнала, представляющего собой последовательность чередующихся манипулированных по фазе на  $180^\circ$  элементов одинаковой амплитуды. Элементам «0» и «1» соответствуют сигналы:

$$U_1(t) = U_{mc} \cdot \cos \omega t;$$

$$U_0(t) = -U_{mc} \cdot \cos \omega t.$$

Спектр двоичных фазоманипулированных сигналов практически отличается от спектра амплитудноманипулированных сигналов лишь тем, что у него частично либо полностью подавлены колебания несущей частоты. Степень этого подавления зависит от характера модулирующей функции.

При фазовой манипуляции информация заключается в фазе принимаемого сигнала. В приемном устройстве фаза принятых колебаний сравнивается в синхронном детекторе с фазой синхронного неманипулированного (опорного) напряжения, синфазного либо противофазного с принимаемым сигналом.

В случае наличия флуктационных помех на вход фазового детектора воздействуют сигнал  $U_c = \pm U_{mc} \cdot \cos \omega t$  и флуктационные помехи. Напряжение флуктационной помехи можно представить виде двух гармонических частот  $\Omega$ : синфазной с сигналом и квадратурной (смещенной по фазе относительно сигнала на  $90^\circ$ ):

$$U_n(t) = x(t) \cos \omega t + y(t) \sin \omega t$$

Амплитуды этих составляющих являются случайными величинами, имеющими нормальное распределение вероятностей и одинаковые дисперсии.

Поскольку действующее в фазовом детекторе опорное напряжение синфазно с сигналом, квадратурная составляющая напряжения помех эффекта на выходе детектора не создает; этим

обуславливается повышенной помехоустойчивостью при когерентном приеме.

Задача разделения фазоманипулированного сигнала сводится к определению фазы суммарного сигнала – помехи и полезного.

Ошибка возникает, если фаза суммарного сигнала окажется противоположной фазе напряжения передаваемого сигнала

$$(+U_{mc} \cdot \cos \omega t \text{ или } -U_{mc} \cdot \cos \omega t).$$

### Помехоустойчивость модулированных сигналов.

Воздействие помехи на носитель приводит к паразитной модуляции его параметров. При этом модуляции подвергаются, как правило, все информационные параметры, в результате получается сложный сигнал. Покажем это на примере действия простейшей аддитивной гармонической помехи:

$$u_{\xi} = U_{\xi m} \cos \omega t$$

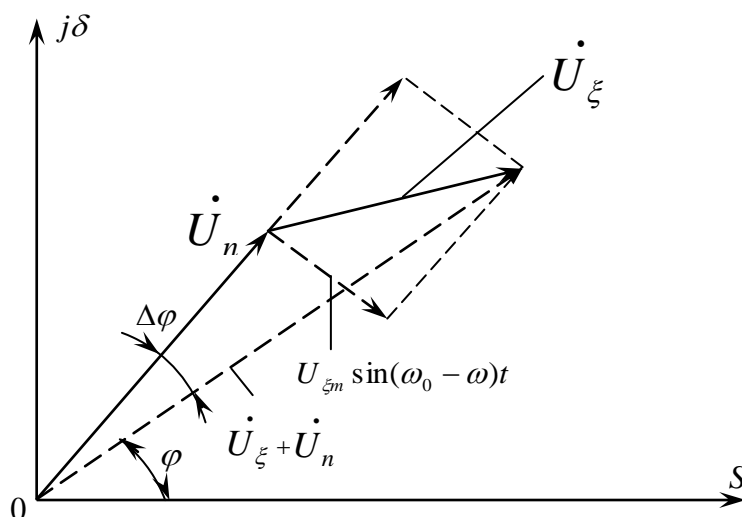
на носитель в виде колебания:

$$u_n = U_0 \cos \omega_0 t$$

с параметрами  $U_0$  и  $\omega_0$ . Выражение для носителя с наложенной на него

помехой в векторной форме имеет вид суммы:  $\dot{U}_H + \dot{U}_{\xi}$

Поскольку вектор  $U_H$  вращается со скоростью  $\omega_0$ , то при его фиксации система координат  $(s, j\sigma)$  станет вращаться в обратном направлении со скоростью  $\omega_0$ , а вектор  $U_{\xi}$  – со скоростью  $\omega_0 - \omega$ . Проекция вектора  $U_{\xi}$  на вектор  $U_H$  порождает амплитудную модуляцию.



Векторная диаграмма гармонического носителя  
с наложенной на него помехой

Эта проекция равна

$$U_0 + U_{\zeta m} \cos(\omega_0 - \omega)t$$

Изменение угла  $\Delta\varphi(t)$  приводит к частотной модуляции. Угол

$$\Delta\varphi \approx \operatorname{tg} \Delta\varphi = \frac{U_{\zeta m} \sin(\omega_0 - \omega)}{U_0 + U_{\zeta m} \cos(\omega_0 - \omega)t}$$

При  $U_{\zeta m} \leq U_0$

$$\Delta\varphi \approx \frac{U_{\zeta m} \sin(\omega_0 - \omega)t}{U_0}$$

Т.о. помеха вызывает как амплитудную, так и частотную модуляцию, т.е. воздействует на оба информационных параметра  $U_0$  и  $\omega_0$ .

Очевидно, что более сложный аддитивный сигнал также вызывает паразитную модуляцию обоих параметров. К таким же последствиям приводят и другие виды помех. В процессе паразитной модуляции помеха оказывает различное влияние на разные параметры носителя.



Это позволяет путем выбора для передачи полезной информации таких параметров, которые наименее подвергаются воздействию помехи, повысить помехоустойчивость передачи. При демодуляции независимо от природы выбранного параметра  $a_i$  полезная  $\Delta a_i(t)$  и вредная  $\delta a_i(t)$  модулирующие составляющие могут быть приведены к сигналу единого типа, например, в виде интенсивности. Сравним различные виды модуляции по соотношению интенсивности полезного сигнала и помех. Интенсивность помех характеризуется мощностью  $P_{\xi_i}$ , которая при нулевом среднем значении равна дисперсии  $D_{\xi_i}$

$$P_{\xi_i} = |\delta a_i(t)|^2 = D_{\xi_i}$$

Соответственно интенсивность полезного сигнала определяет его средняя мощность

$$P_{x_i} = |\Delta a_i(t)|^2.$$

Помехоустойчивость модуляции по  $i$ -му параметру оценивается соотношением этих мощностей:

$$\rho = \frac{P_{x_i}}{P_{\xi_i}}$$

Это соотношение для различных параметров  $a_i$  оказывается различным. Из двух видов модуляции, связанных с параметрами  $a_i$  и  $a_j$  более помехоустойчивым можно считать тот, для которого это соотношение больше. Сигналы с большим отношением  $\rho_i$ , обладают большими информационными возможностями.

Используя данный критерий, проведем сравнение по помехоустойчивости двух видов модуляции – амплитудной и частотной с носителем в виде колебания  $u_n = U_0 \cos(\omega_0 t + \varphi_0)$ .

Для других видов модуляции сравнения можно провести аналогичным способом.

Носитель  $u_n = U_0 \cos(\omega_0 t + \varphi_0)$  имеет три информационных параметра:  $a_1=U_0$ ,  $a_2=\omega_0$ ,  $a_3=\varphi_0$ . При АМ и ЧМ начальная фаза  $\varphi_0$  информации не несет, поэтому и в дальнейшем будем полагать  $\varphi_0=0$ . Модулированный сигнал при АМ и ЧМ описывается соответственно функциями.

$$u_{x(t)} = [U_0 + \Delta u(t)] \cos \omega_0 t$$

$$u_{x(t)} = U_0 \cos \int_0^t [\omega_0 + \Delta \omega(t)] dt$$

определим  $p_i$  при модуляции синусоидальным колебанием

$$x(t) = x_m \sin \Omega t$$

в предположении наличия аддитивной помехи типа реального “белого шума”, имеющего равномерный энергетический спектр  $S_{\xi\xi}$  в полосе  $2\Omega$  (от  $\omega_0-\Omega$  до  $\omega_0+\Omega$ ), т.е. в пределах ширины спектра модулированного по амплитуде полезного сигнала.

Модулирующая составляющая при АМ

$$\Delta a_1(t) = \Delta u(t) = Kx(t) = \Delta U_m \sin \Omega t \quad \text{где } \Delta U_m = Kx_m$$

Ее средняя мощность

$$P_{xa} = |\Delta u(t)|^2 = |\Delta U_m \sin \Omega t|^2 = \frac{2}{T} \int_0^{T/2} (\Delta U_m)^2 \sin^2 \Omega t dt = \frac{(\Delta U_m)^2}{2}$$

где  $T = 2\pi/\Omega$

Отношение сигнала к помехе имеет наибольшее значение в случае стопроцентной модуляции, при которой  $\Delta U_m = U_0$  и, следовательно,

$$P_{xa} = U_0^2/2$$

Средняя мощность помехи:

$$P_{\xi a} = D_{\xi} = \frac{1}{\pi} \int_0^{\infty} S_{\xi\xi}(\omega) d\omega = \frac{1}{\pi} \int_0^{2\Omega} S_{\xi\xi} d\omega = \frac{2}{\pi} S_{\xi\xi} \Omega$$

Помехоустойчивость при амплитудной модуляции

$$\rho_a = \frac{P_{xa}}{P_{\xi a}} = \frac{\pi U_0^2}{4\Omega S_{\xi\xi}}$$

Для частотной модуляции имеем:

$$\Delta a_2(t) = \Delta\omega(t) = Kx(t) = \Delta\omega_m \sin \Omega t, \text{ где } \Delta\omega_m = Kx_m$$

Средняя мощность частотного сигнала

$$P_{xa} = |\Delta\omega(t)|^2 = \frac{2}{T} \int_0^{T/2} (\Delta\omega_m)^2 \sin^2 \Omega t dt = \frac{(\Delta\omega_m)^2}{2}$$

Определим теперь среднюю мощность  $P_{\xi\omega}$  при частотной модуляции. Так как случайную помеху можно рассматривать как бесконечную сумму бесконечно малых гармоник со случайной амплитудой  $dA_m$  и случайной фазой, но с детерминированным значением средней мощности.

Однако как было сказано в начале, гармоническое колебание с частотой  $\omega$  и амплитудой  $dA_m$  при наложении на носитель приводит к модуляции последнего с модулирующей функцией.

$$\delta\omega(t) = \left(\frac{dA_m}{U_0}\right)(\omega_0 - \omega)\cos(\omega_0 - \omega)t$$

Мощность этого колебания, усредненная во времени,

$$dP_{\xi\omega}^I = \frac{1}{2} \frac{dA_m^2}{U_0^2} (\omega_0 - \omega)^2$$

Рассмотрим теперь  $\delta\omega(t)$  как функцию со случайной амплитудой, после усреднения  $dP_{\xi\omega}^I$  по множеству реализаций получим среднюю мощность помехи  $\delta\omega(t)$ , представляющую собой элементарную составляющую  $dP_{\xi\omega}$ , приходящуюся на диапазон частот  $d\omega$

$$dP_{\xi\omega} = \frac{1}{2} \frac{M|dA_m^2|}{U_0^2} (\omega_0 - \omega)^2$$

Учитывая, что:

$$\frac{M|dA_m^2|}{2} = \frac{1}{\pi} S_{\xi}(\omega)d\omega$$

Элемент мощности модулирующей функции можно представить в виде

$$dP_{\xi\omega} = \frac{(\omega_0 - \omega)^2}{U_0^2} \frac{1}{\pi} S_{\xi}(\omega)d\omega$$

По условию энергетический спектр помехи равномерен в диапазоне от  $\omega_0 - \Omega$  до  $\omega_0 + \Omega$  и равен нулю вне этого диапазона. Поэтому

$$P_{\xi\omega} = \frac{1}{\pi} S_{\xi\xi} \frac{1}{U_0^2} \int_{\omega_0-\Omega}^{\omega_0+\Omega} (\omega_0 - \omega)^2 d\omega$$

Сделав замену переменных

$$\omega_1 = \omega - \omega_0$$

получим:

$$P_{\xi\omega} = \frac{2}{\pi} S_{\xi\xi} \frac{1}{U_0^2} \int_0^{\Omega} \omega_1^2 d\omega_1 = \frac{2S_{\xi\xi}}{3\pi U_0^2} \Omega^3$$

Помехоустойчивость при частотной модуляции

$$\rho_a = \frac{P_{xa}}{P_{\xi a}} = \frac{3nU_0^2}{4\Omega} \cdot \frac{\Delta\omega_m^2}{S_{\xi\xi}}$$

Сравнивая  $\rho_\omega$  с  $\rho_a$ , получаем:

$$\rho_\omega = 3\left(\frac{\Delta\omega_m}{\Omega}\right)^2$$

$$\rho_a = 3m^2 \rho_\omega$$

Из полученного соотношения следует, что помехоустойчивость частотной модуляции намного превышает помехоустойчивость амплитудной модуляции (в  $3m^2$  раз).

Выигрыш в помехоустойчивости получается благодаря расширению спектра сигнала, который при частотной модуляции занимает значительно большую полосу (ориентировочно в  $m$  раз).

На рис. 8 приведен график зависимости вероятности ошибок  $P_{\text{ош}}$  от соотношения мощностей сигнал/помеха ( $I^2$ ) для различных видов манипуляции.

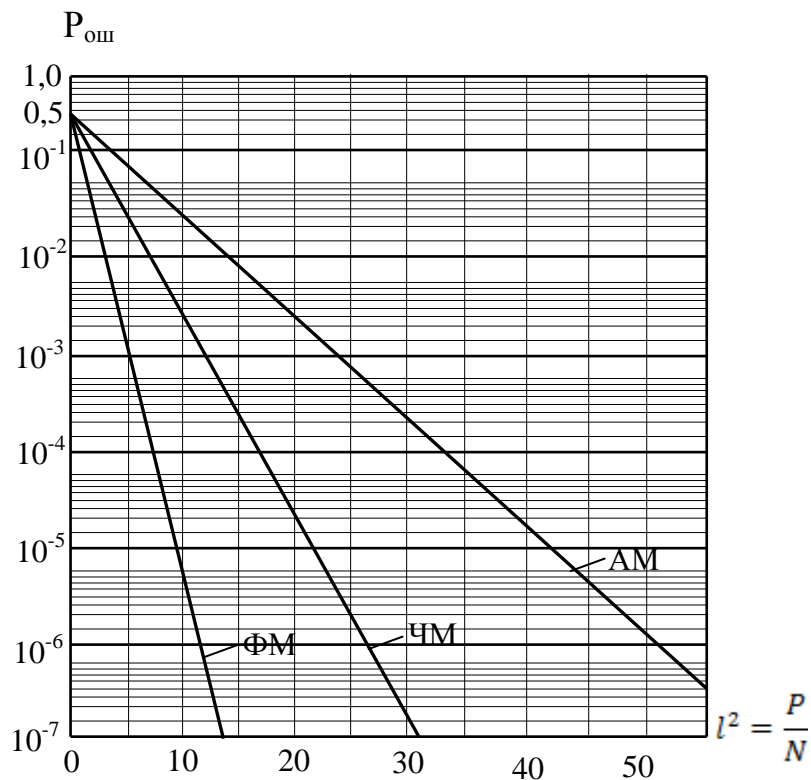


Рис. 8.

Как видно из приведенного графика вероятность ошибки при некогерентном приеме двоичных амплитудноманипулированных и частотноманипулируемых сигналов в условиях воздействия флуктационных помех, помехоустойчивость при частотной манипуляции оказывается значительно выше. Однако при этом следует учитывать, что при одинаковой амплитуде сигнала средняя мощность передатчика при частотной манипуляции должна быть вдвое больше, чем при амплитудной манипуляции. Из этого же графика видно, что помехоустойчивость при фазовой манипуляции значительно выше, чем при частотной и особенно амплитудой.

### Контрольные вопросы.

1. Дайте определения кодирования, кода, кодовой комбинации, значности кода.
2. Что такое производительность источника дискретного сообщения?
3. Что такое скорость передачи информации и пропускная способность канала связи?
4. Сформулируйте теорему Шеннона о передаче информации по каналу с шумами.
5. Виды манипуляции двоичных сигналов.
6. Спектры различных видов манипулированных сигналов.
7. Сравнительная оценка манипулированных сигналов с точки зрения помехоустойчивости.

### 3. Помехоустойчивое кодирование

При технической реализации кода каждому элементу кода сопоставляется физический элемент – импульс напряжения, тока или другой величины.

Задачи кодирования при отсутствии помех и при наличии помех в канале связи существенно различны. В первом случае ставится задача добиться представления элементов сообщений при минимальной средней значимости кода, т.е. минимальным числом элементов кода в среднем на одно сообщение. Это достигается путем по возможности полной ликвидации избыточности сообщения. Во втором случае ставится задача снижения вероятности ошибок в передаче элементов сообщений. Это достигается, наоборот, введением избыточности в кодовые сообщения. Такой код называется помехоустойчивым.

Помехоустойчивый код отличается от обычного кода тем, что в канал связи передается не все кодовые комбинации, которые можно сформировать из имеющегося количества разрядов, а лишь некоторые из них, обладающие определенным свойством и называемые разрешенными. Остальные неиспользуемые кодовые комбинации называют запрещенными. Таким образом, все множество  $N=2^n$  кодовых комбинаций ( $n$ - число разрядов в кодовой комбинации) разбивается на два подмножества.

Для равнодоступного кода все комбинации кода отличаются друг от друга одним разрядом, и поэтому искажение даже одного разряда нельзя обнаружить.



Коды, позволяющие только определить наличие ошибок, но не указывающие номер искаженных разрядов, называют кодами с обнаружением ошибок.

Коды, которые не только обнаруживают ошибку, но и указывают номер искаженной позиции, называются кодами с исправлением ошибок.

При использовании помехоустойчивого кода в канал связи передаются только разрешенные кодовые комбинации.

Обнаружение и исправление возникающих в каналах связи ошибок достигается за счет введения в передаваемые кодовые комбинации избыточных разрядов.

Рассмотрим, каким образом может быть обнаружена ошибка. Предположим, что информация передается  $m$ -разрядным двоичным кодом. Следовательно, число всех возможных кодовых комбинаций будет равно  $N_0=2^m$ . К каждой кодовой комбинации добавим один разряд  $n=m+1$ . Значение этого разряда выберем так, чтобы сумма единиц в кодовой комбинации была всегда четной (либо всегда нечетной). В результате этого каждая из  $N_0$  кодовых комбинаций будет отличаться друг от друга не менее чем двумя разрядами. При таком коде одиночная (либо любая нечетная) ошибка, изменяющая число единиц на нечетное (либо на четное), будет обнаружена.

Если же в кодовую комбинацию ввести большее количество дополнительных разрядов, то можно не только обнаруживать, но и исправлять ошибки. Например, если любые две разрешенные кодовые комбинации отличаются друг от друга не менее чем тремя разрядами, то одиночная ошибка исказит информацию так, что ошибочная комбинация будет отличаться от истинной только одним разрядом и

остаётся в области, относящейся к передаваемой кодовой комбинации, и поэтому может быть исправлена.

Простейшие геометрические представления, введенные Хеммингом, наглядно объясняют свойства корректирующих кодов. Изобразим кодовую группу в  $m$ - мерном пространстве в виде  $m$ - мерного “куба”, причем ребро “куба” направим по осям координат, каждая из которых отвечает позиции (разряду) двоичного знака в кодовой группе. При этом вершины “куба” будут соответствовать всем возможным комбинациям чисел данной кодовой группы. Эти вершины называются кодовыми точками. Так, например, в случае трехзначного кода, когда  $m=3$ , кодовая группа изобразится в трехмерном пространстве в виде куба с кодовыми точками: 000; 001; 010; 011; 100; 101; 110; 111.

На рис.9 оси пронумерованы согласно обычной разрядности двоичных чисел, т.е. справа налево.

Хэмминг ввел метрику пространства, в котором изображается кодовая группа, задав расстояние  $D(x;y)$ . Это расстояние принимается равным числу координат, на которое кодовая точка  $Y$  отличается от кодовой точки  $X$ . В геометрической интерпретации оно по существу равно наименьшему числу ребер  $m$ -мерного куба, которое нужно пройти, чтобы попасть из  $X$  в  $Y$ . Так, например, расстояние между точками 010 и 111 (рис.8) равно двум, так как попасть из одной точки в другую можно по пунктирной стрелочке.

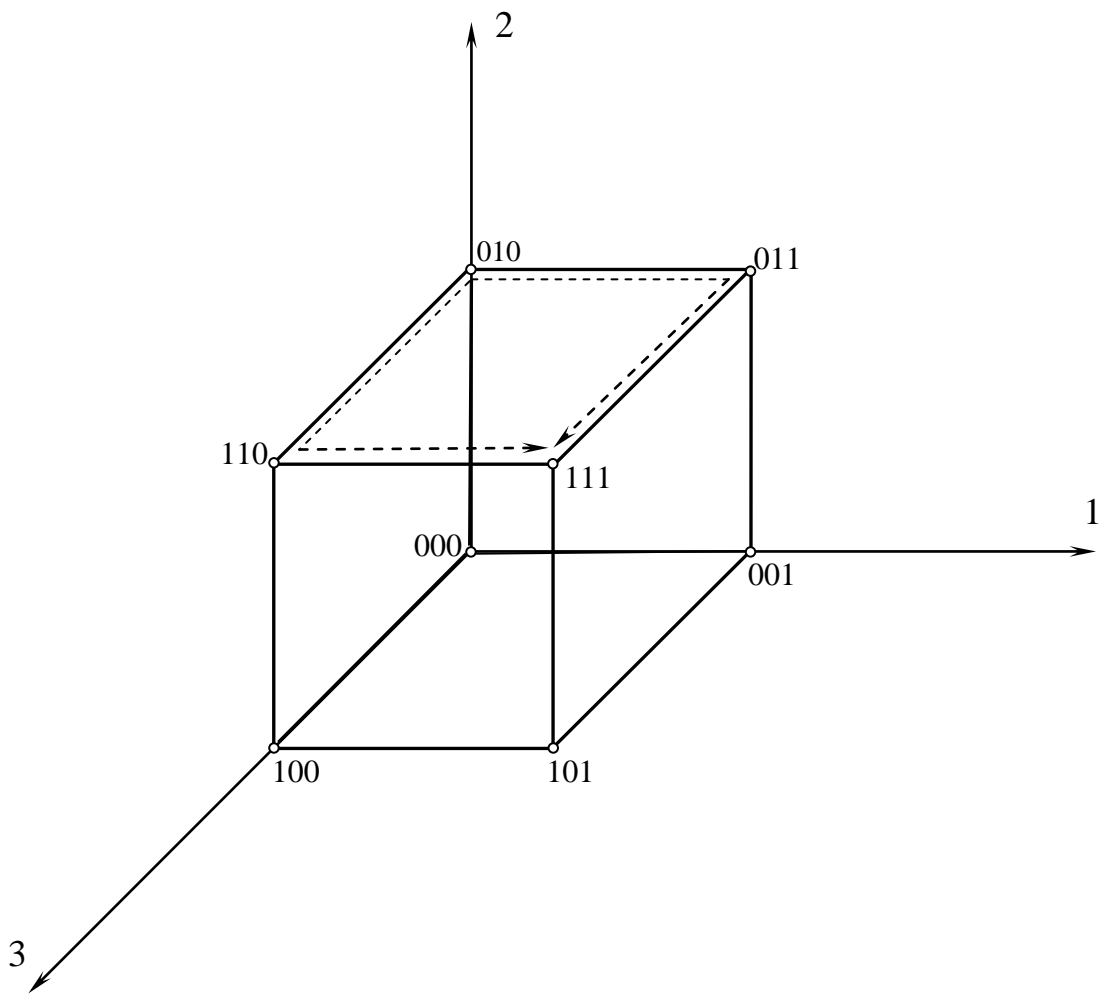


Рис.9

Геометрическая модель четырехзначного кода представляет собой фигуру четырехмерного пространства и может быть построена путем смещения вершин трехмерного куба в новом направлении (рис.10).

В общем случае  $m$ - мерный куб должен иметь  $2m$ - вершин,  $m \cdot 2^{m-1}$  ребер,  $m(m-1) \cdot 2^{m-3}$  граней, а наиболее удаленная от данной вершины его точка должна находиться на расстоянии  $m$  ребер.

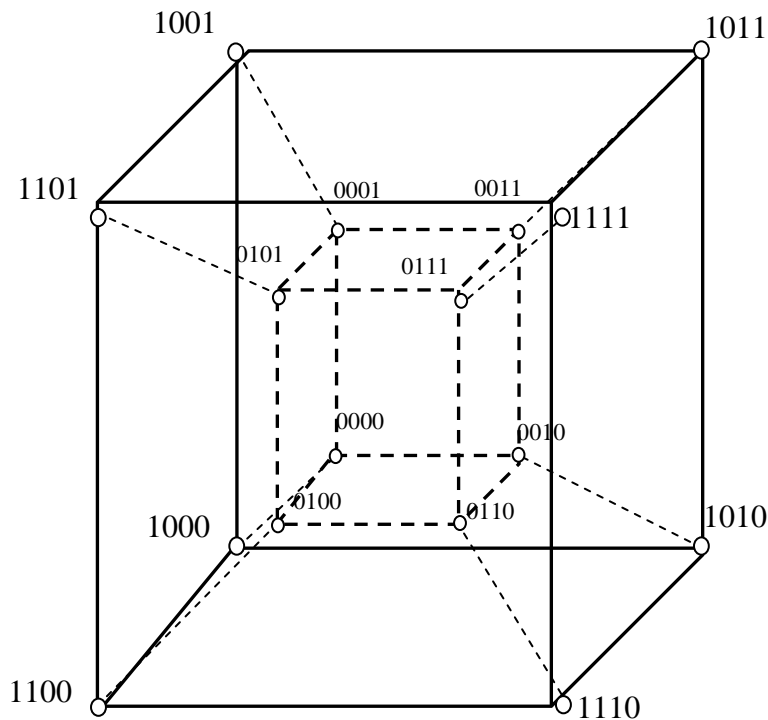


Рис.10.

Представление кодов в виде геометрической модели производят для наглядности изображения и облегчения анализа их свойств. Однако с ростом числа элементов кода  $n$  геометрические модели становятся громоздкими, теряют наглядность, а их построение вызывает большие трудности.

Для построения помехозащищенных кодов вводится понятие кодového расстояния. Под кодovým или под хэмминговым расстоянием понимают минимальное число позиций, на которых символы одной комбинации данного кода отличаются от символов другой кодовой комбинации. Например, кодовое расстояние между комбинациями 10101 и 11111 равно двум. В общем случае кодовое расстояние между  $i$  комбинацией и  $j$  комбинацией выражается формулой:

$$d_{ij} = \sum_{k=1}^n (x_{ik} \oplus x_{jk}),$$

где  $x_{ik}$ - символ на  $K^{ой}$  позиции  $i$ -й кодовой комбинации;

$\oplus$  - знак суммирования по модулю 2.

Определим, как связана величина  $d$  с кратностью обнаруживаемых и исправляемых ошибок. Ошибка не обнаруживается, если одна разрешенная кодовая комбинация в результате искажений преобразуется в другую разрешенную. Например, если у нас  $m=3$ , то можно отобрать кодовые комбинации, где обнаруживается одиночная (нечетная) ошибка: 000, 101, 110 и 011.

Любая одиночная (нечетная) ошибка переведет разрешенную комбинацию в запрещенную: 100, 001, 010, 111.

Следовательно, для обеспечения возможности обнаружения всех ошибок кратности до  $z$  включительно необходимо, чтобы кодовое расстояние было равно:

$$d_{\min} \geq r+1.$$

Для исправления одиночной ошибки разобьем все множество комбинаций на две области (рис. 11) и будем исправлять только две кодовые комбинации: 110 и 001.

В этом случае одиночная ошибка оставляет кодовую комбинацию в области, относящейся к передаваемой кодовой комбинации. Так, при искажении одного разряда в комбинации 001 она превратится в 000, или в 011, или в 101. Все эти комбинации находятся в той же области, что и комбинация 001.

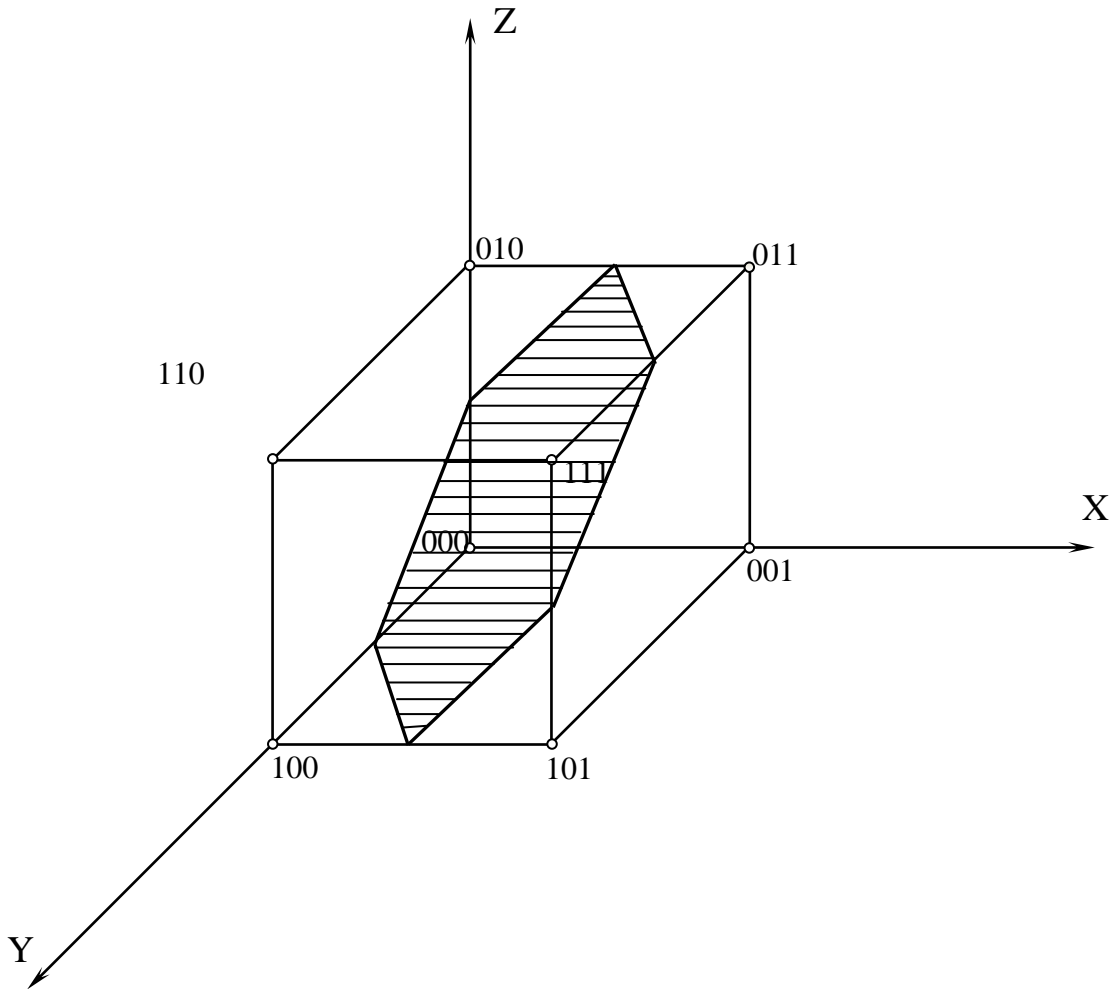


Рис.11

Введением определенного количества дополнительных разрядов устанавливается нужное кодовое расстояние между комбинациями. Например, для обнаружения одиночных ошибок расстояние между кодовыми комбинациями должно быть не менее двух, для исправления одиночной ошибки расстояние должно быть не менее трех разрядов.

$$d_{\min} \geq 2r + 1$$

Необходимое кодовое расстояние  $d$  и помехоустойчивость кода определяется избыточностью кода, под которым понимают отношение

$$R = \frac{n - m}{n} = \frac{k}{n},$$

где  $k$  – число проверочных (избыточных) разрядов;

$n$  – общее число разрядов в кодовой комбинации;

$m$  – число информационных разрядов;

Количество проверочных разрядов  $k$ , необходимое для исправления ошибок кратности  $r$  и менее, определяется из неравенства:

$$2^k \geq \sum_{i=0}^r C_n^i$$

Для исправления одиночной ошибки необходимо пользоваться неравенством

$$2^k - 1 \geq n \text{ или}$$

$$2^{n-m} - 1 \geq n.$$

Каждый проверочный разряд является функцией определенных информационных разрядов. Конкретно, какие информационные разряды участвуют в формировании данного проверочного и по какому закону он формируется, определяется алгоритмом построения данного кода. Наиболее часто значение каждого проверочного разряда (“0” или “1”) выбирается так, что сумма по модулю два определенных информационных и данного проверочного разрядов было равно 0. Проверочные разряды могут располагаться в кодовой комбинации на любом месте.

Из большого многообразия помехоустойчивых кодов заслуживают внимание коды, обеспечивающие высокую

достоверность при малой величине избыточности и простоте схемных реализаций корректирующих и декодирующих устройств.

Все коды, в принципе, могут быть использованы как в качестве обнаруживающих, так и в качестве исправляющих ошибки кодов. На практике одни коды находят наибольшее применение как обнаруживающие, другие – как коды с исправлением ошибок. Рассмотрим некоторые из них.

Коды с проверкой на четность. При построении таких кодов передаваемая последовательность разрядов разбивается на группы. В наиболее простом случае проверка на четность производится в каждом кодовом сообщении, в результате чего число единиц доводится до четного. Так, кодовая комбинация 01110 в результате кодирования преобразуется в комбинацию 011101. Основным недостатком кода является необнаружение ошибок четной кратности. Поэтому такие коды находят применение в тех звеньях информационно - измерительных систем, где наиболее вероятно одиночные ошибки. Проверка на четность легко реализуется в простейшем случае для этого достаточно иметь один триггер со счетным входом.

Коды с постоянством веса. Под кодом с постоянным весом понимают двоичный равномерный код, в котором все разрешенные комбинации содержат одинаковое число единиц. Такой код обеспечивает обнаружение всех ошибок, за исключением тех случаев, когда несколько единиц превратятся в нули, а столько же нулей – в единицы. Эти ошибки называют ошибками смещения.

В настоящее время широкое распространение получили коды: “2 из 5”, “3 из 6”, “3 из 7”, “4 из 8”, “3 из 8”.



Для двоичных кодов число кодовых комбинаций в кодах с постоянным весом длиной в  $n$  символов равно

$$N = C_n^l = \frac{n!}{l!(n-l)!},$$

где  $l$  - число единиц в кодовом слове. Если бы не существовало условия “постоянного” веса, то число комбинаций кода могло бы быть гораздо большим, а именно  $2^n$ .

В общей классификации помехоустойчивых кодов следует выделить разделимые коды, в которых разряды могут быть принципиально разделены на проверочные и информационные. При этом место проверочных и информационных разрядов в кодовой комбинации вполне определено. В неразделимых кодах (например, коды с постоянным весом) деление на информационные и проверочные разряды отсутствуют. В свою очередь разделимые коды подразделяются на систематические и несистематические.

Систематическими кодами называют такие, у которых сумма по модулю два двух разрешенных комбинаций кода дает комбинацию того же кода. Кроме того, в систематических кодах проверочные символы могут образовываться путем различных линейных комбинаций информационных символов. Декодирование систематических кодов также основано на проверке линейных соотношений между символами, стоящими на определенных проверочных позициях. В случае двоичных кодов этот процесс сводится к проверке на четность.

Большинство систематических кодов отображаются при помощи производящей и проверочной матриц.

Производящей (образующей, порождающей) называется матрица, при помощи которой производится построение кода.

Примерами систематических кодов являются циклические коды и коды Хэмминга. Для систематического кода применяется обозначение  $(n,m)$  –код, где  $n$  – число всех разрядов в кодовой комбинации,  $m$  – число информационных разрядов.

## Контрольные вопросы

1. Дайте определение помехоустойчивого кодирования; коды обнаруживающие ошибки и коды исправляющие ошибки.
2. Геометрическая модель корректирующего кода.
3. Как определяют расстояние между кодовыми комбинациями?
4. Как определить минимальное кодовое расстояние для обнаружения и исправления  $r$ - кратной ошибки?
5. Как определить число контрольных разрядов для  $m$  информационных разрядов?
6. Коды с проверкой на четность и коды с постоянным весом.
7. Разделимые и неразделимые коды, систематические и несистематические коды.

## Циклический код

Из известных помехоустойчивых кодов циклические коды отличаются высокой эффективностью обнаружения ошибок и сравнительно простой реализации кодирующих и декодирующих устройств. Название этого класса кодов произошло от основного их свойства, заключающегося в том, что если кодовая комбинация  $a_0, a_1, a_2, \dots, a_{n-1}, a_n$  принадлежит коду  $A$ , то комбинация  $a_n, a_0, a_1, a_2, \dots, a_{n-1}$ , полученная циклической перестановкой элементов, также принадлежит коду  $A$ . Циклические коды достаточно часто описываются с использованием многочленов переменной  $x$ .

Цифры двоичного кода можно рассматривать как коэффициенты многочлена переменной  $x$ . Например, записанное в двоичном коде сообщение 1 0 0 1 1 0 1 может быть представлено многочленом вида  $1*x^6+0*x^5+0*x^4+1*x^3+1*x^2+0*x+1=x^6+x^3+x^2+1$ . При таком представлении кодов математические операции с полученными многочленами производятся в соответствии с законами обычной алгебры, за исключением того, что сложение осуществляется по модулю 2:  $x^a+0=x^a$ ,  $0+0=0$ . Принцип обнаружения ошибок при помощи циклического кода заключается в том, что в качестве разрешенных кодовых комбинаций принимаются такие комбинации, которые делятся без остатка на некоторый заранее выбранный исходный (образующий) многочлен  $P(x)$ . Если принятая комбинация искажена, то это условие на приемной стороне не будет выполнено, в результате чего формируется сигнал, указывающий на наличие ошибки.

В процессе кодирования сообщения многочлен  $G(x)$ , отображающий двоичный код передаваемого сообщения, умножается на  $x^k$ . При этом длина кодовой комбинации увеличивается на  $k$  разрядов, которые предназначены для проверочных разрядов. Произведение  $G(x)x^k$  делят на так называемый исходный (образующий) многочлен  $P(x)$ , и остаток от этого деления  $R(x)$  суммируют с произведением  $G(x)x^k$ . Полученная кодовая комбинация, описываемая кодовым многочленом  $F(x) = G(x)x^k + R(x)$ , делится без остатка на исходный многочлен  $P(x)$ . Это можно показать следующим образом. Если обозначить  $f(x)$  частное от деления  $G(x)x^k$  на  $P(x)$ , то будет справедливо равенство  $G(x)x^k = f(x)P(x) + R(x)$ . Переносим  $R(x)$  за знак равенства, получим  $G(x)x^k + R(x) = f(x)P(x)$ .

При таком методе построения коэффициенты при высших степенях  $x$  являются обозначениями информационных разрядов, а коэффициенты при степенях порядка  $k-1$  и ниже – проверочными.

**Пример.** Дано:  $n=7$ ,  $m=4$ ,  $k=3$  и  $P(x) = x^3 + x^2 + 1$ . Требуется закодировать сообщение 1 0 1 1. Для кодирования сообщения 1 0 1 1, соответствующего многочлену  $G(x) = x^3 + x + 1$ , разделим  $G(x)x^3$  на  $P(x)$ :

$$\begin{array}{r|l} x^6 + x^4 + x^3 & x^3 + x^2 + 1 \\ \hline x^6 + x^5 + x^3 & x^3 + x^2 \\ \hline x^5 + x^4 & \\ \hline x^5 + x^4 + x^2 & \\ \hline R(x) = x^2 & \end{array}$$

В итоге этой операции получим остаток  $R(x) = x^2$ .

Суммируя произведение  $G(x)x^3$  с полученным остатком, получим кодовый многочлен

$$F(x) = G(x)x^3 + R(x) = x^6 + x^4 + x^3 + x^2.$$

В двоичном коде этому многочлену соответствует кодовая комбинация 1 0 1 1 1 0 0, в которой проверочные разряды занимают три последние позиции.

Принятое сообщение, которое обозначим  $F'(x)$ , можно представить в виде суммы двух слагаемых: многочлена, сформированного на передающей стороне  $F(x)$ , и многочлена ошибки  $E(x)$ :  $F'(x)=F(x)+E(x)$ . Этот многочлен подвергается делению на  $P(x)$ . Если деление производится без остатка, то принимается решение, что информация искажена.

В случае применения циклического кода в качестве кода с исправлением ошибок места искаженных разрядов определяются путем анализа остатка, получившегося после деления принятой кодовой комбинации на исходный многочлен.

По заданному объему информационного кода однозначно определяется число информационных разрядов  $K$ . Далее необходимо найти наименьшее  $n$ , обеспечивающее обнаружение или исправление ошибок заданной кратности. Для циклического кода эта проблема сводится к нахождению образующего многочлена  $P(x)$ . Образующие многочлены иногда называются “неприводимыми”, так как эти многочлены делятся без остатка только на себя или на единицы (по аналогии с простыми числами). Образующий многочлен следует выбирать как можно более коротким: наибольшая степень его должна быть равна числу контрольных разрядов, а число ненулевых членов должно быть не меньше минимального кодового расстояния.

Например:  $x^3+x^2+1$  и  $x^3+x+1$  – подобны друг другу и обладают равноценными корректирующими способностями.

Достоинство циклического кода в том, что он используется для обнаружения как взаимонезависимых ошибок, так и групповых.

Циклические коды обладают двумя важными свойствами:

1. Если в разрешенной кодовой комбинации осуществить циклический сдвиг на один элемент, т.е. переставить элемент комбинации, занимающий последнюю позицию на первое место, а остальные сдвинуть на один шаг, то получим другую разрешенную кодовую комбинацию данного циклического кода.
2. Сумма по модулю два любых двух разрешенных комбинаций циклического кода является разрешенной комбинацией данного циклического кода.

Циклические коды относятся к блоковым кодам. Последовательность кодовых комбинаций в циклическом коде разбивается на отдельные блоки, состоящие из информационных и проверочных разрядов и в пределах этих блоков производится исправление ошибок.

Блок состоит из:

- $m$  – информационных элементов (разрядов);
- $k$  – контрольных элементов (разрядов);
- $n=m+k$  – общее число разрядов циклического кода.

В кодовой комбинации циклического в начале идут информационные элементы, а потом проверочные.

Пример. Число информационных разрядов  $m=11$ . Кодовая комбинация 10110100111. Рассмотрим циклический код, обнаруживающий и исправляющий все одиночные ошибки.

1. Общее число символов в кодовой комбинации  $n$  находим из неравенства

$$2^{n-m} - 1 \geq C_n^1 = n$$

$$n - m = k = 4$$

2. Из таблицы выбираем образующий многочлен четвертой степени

$$x^4 + x^3 + 1$$

или в двоичном коде 11001.

Число ненулевых членов равно 3 ( $d_{\min} = 2r + 1$ )

3. Исходный многочлен (100110100111) умножаем на  $x^k$  ( $x^4$ ), что фактически означает по отношению к комбинации кода необходимость приписать со стороны младших разрядов  $k$  нулей, т.е.

$$101101001110000.$$

4. Полученный многочлен делится на образующий полином.

1011010011	0000	11001
11001		
11111		
11001		
11000		
11001		
11110		
11001		
11100		
11001		
1010		

Найденный остаток 1010 записывается на месте контрольных разрядов.



Окончательная запись циклического кода исходной комбинации будет выглядеть так:

101101001111010

### Матричная запись циклического кода

При построении циклического кода удобно использовать матричную запись:

$$A_{n,m} = (A_m, A_{k,m}),$$

где  $A_{n,m}$ - матрица циклического кода;

$A_m$ - единичная транспонированная матрица;

$A_{k,m}$ - матрица контрольных элементов. Она получается из остатков от деления единицы с нулями (общее число разрядов  $n$ ) на образующий многочлен  $P(x)$ , выраженный в двоичном эквиваленте. Число остатков равно числу информационных символов.

В нашем примере:

$$\begin{array}{r}
 1000000000000000 \quad | \quad 11001 \\
 \oplus \quad 11001 \\
 \hline
 1^{\text{ый}} \text{ остаток} \quad 10010 \\
 \oplus \quad 11001 \\
 \hline
 2^{\text{ый}} \text{ остаток} \quad 10110 \\
 \oplus \quad 11001 \\
 \hline
 3^{\text{ий}} \text{ остаток} \quad 11110 \\
 \frown \quad 11001 \\
 \hline
 4^{\text{ый}} \text{ и } 5^{\text{ый}} \text{ остатки} \quad 0111 \\
 \oplus \quad 11100 \\
 \oplus \quad 11001 \\
 \hline
 6^{\text{ой}} \text{ и } 7^{\text{ой}} \text{ остатки} \quad 01010 \\
 \oplus \quad 10100 \\
 \oplus \quad 11001 \\
 \hline
 8^{\text{ой}} \text{ остаток} \quad 11010 \\
 \oplus \quad 11001 \\
 \hline
 9,10 \text{ и } 11^{\text{ый}} \text{ остатки} \quad 0011 \\
 \quad \quad \quad 0110 \\
 \quad \quad \quad 1100
 \end{array}$$

Если в остатке при делении первый разряд равен нулю, то последующие остатки получаются путем циклического переноса. Таким образом получены 5, 7, 10 и 11 остатки. Эти остатки записываются в строки матрицы контрольных элементов. Окончательно матрица циклического кода для рассматриваемого

примера (одиннадцать информационных разрядов и образующий полином  $P(x) = 11001$ ) будет иметь вид:

$$A_{15, 11} = \left| \begin{array}{cc} 000000000001 & 1001 \\ 00000000010 & 1011 \\ 00000000100 & 1111 \\ 00000001000 & 0111 \\ 00000010000 & 1110 \\ 00000100000 & 0101 \\ 00001000000 & 1010 \\ 00010000000 & 1101 \\ 00100000000 & 0011 \\ 01000000000 & 0110 \\ 10000000000 & 1100 \end{array} \right|$$

Легко показать, что при суммировании соответствующих строк по модулю два можно получить с помощью матрицы любую кодовую комбинацию циклического кода. В рассматриваемой кодовой комбинации необходимо просуммировать 1, 2, 3, 6, 8, 9 и 11 строки.

В случае возникновения ошибки в одном из информационных разрядов циклического кода по виду остатка от деления полученной кодовой комбинации на образующий полином можно определить номер разряда, где произошла ошибка.

Предположим, ошибка произошла в 9<sup>ом</sup> информационном разряде:

$$\begin{array}{r}
 \oplus \begin{array}{r} 100101001111010 \\ \hline 11001 \end{array} \quad | \quad 11001 \\
 \oplus \begin{array}{r} 10111 \\ \hline 11001 \end{array} \\
 \oplus \begin{array}{r} 11100 \\ \hline 11001 \end{array} \\
 \oplus \begin{array}{r} 10101 \\ \hline 11001 \end{array} \\
 \oplus \begin{array}{r} 11001 \\ \hline 11001 \end{array} \\
 \oplus \begin{array}{r} 11010 \\ \hline 11011 \end{array} \\
 \text{Остаток} \longrightarrow \boxed{0011}
 \end{array}$$

В матрице циклического кода этот остаток указывает на то, что ошибка произошла в девятом разряде.

Если ошибка (одиночная) произошла в контрольных разрядах, то обычно в остатке одна единица, а остальные – нули.

### Обнаружение и исправление одиночных ошибок

Обнаружению и исправлению одиночных ошибок в циклическом коде производится на основе анализа веса остатка (количество единиц).

Если в результате деления полинома циклического кода на образующий полином в остатке будет больше, чем одна единица, то осуществляется циклический сдвиг кодовой комбинации, и вновь образованный полином делится на тот же образующий многочлен. Циклический сдвиг и деление продолжается до тех пор, пока в остатке вес не будет равен единице. Как только  $W=1$ , суммируем остаток с последним разрядом и производим сдвиг в обратную сторону.

Рассмотрим тот же пример с ошибкой в девятом информационном разряде.

Исходный код: 101101001111010  
 Ошибочный код: 1001101001111010

После деления на образующий полином 11001 в остатке была получена комбинация 0011, т.е.  $W=2$ . Реализуем первый циклический сдвиг и делим на образующий полином:

$$\begin{array}{r|l}
 001101001111010 & 11001 \\
 \oplus 11001 & \\
 \hline
 \oplus 11011 & \\
 \oplus 1100 & \\
 \hline
 \oplus 11001 & \\
 \oplus 1100 & \\
 \oplus 11001 & \\
 \oplus 10110 & \\
 \oplus 11001 & \\
 \oplus 11111 & \\
 \oplus 11001 & \\
 \hline
 00110 & W=3
 \end{array}$$

Второй циклический сдвиг:

$$\begin{array}{r}
 \boxed{0}10100111101010 \quad | \quad 11001 \\
 \oplus 11001 \\
 \hline
 11011 \\
 \oplus 1100 \\
 \hline
 11001 \\
 \oplus 11001 \\
 \hline
 11100 \\
 \oplus 11001 \\
 \hline
 10110 \\
 \oplus 1100 \\
 \hline
 11111 \\
 \oplus 11001 \\
 \hline
 1100 \qquad W=2
 \end{array}$$

Третий циклический сдвиг:

$$\begin{array}{r}
 \oplus 10100111101010\boxed{0} \quad | \quad 11001 \\
 \oplus 11001 \\
 \hline
 11011 \\
 \oplus 11001 \\
 \hline
 10111 \\
 \oplus 11001 \\
 \hline
 11100 \\
 \oplus 11001 \\
 \hline
 10110 \\
 \oplus 11001 \\
 \hline
 11111 \\
 \oplus 11001 \\
 \hline
 11000 \\
 11001 \\
 \hline
 1 \qquad W=1
 \end{array}$$

Полученную в остатке единицу суммируем с последним разрядом (где произошла ошибка) и сдвигаем кодовую комбинацию в обратную сторону.

## 5. Принципы построения кодирующих и декодирующих устройств

Кодирующие и декодирующие устройства циклического кода строятся на основе регистров с обратными связями. При кодировании и декодировании циклических кодов получаемый остаток  $R(x)$  содержит число разрядов, равное показателю степени образующего многочлена  $P(x)$ . Поэтому регистр с обратными связями (ОС) должен содержать  $k$  ячеек памяти.

Регистры с обратными связями в соответствии с выбранным образующим многочленом строятся по следующим правилам:

1. Число каскадов регистра выбирают равным степени образующего многочлена.
2. Количество сумматоров по модулю 2 берется на единицу меньше числа ненулевых членов образующего многочлена.
3. Входы всех ячеек (триггеров) регистра обозначают  $X^i$  ( $i=0,1,2$ ). Выход последней ячейки (триггера) обозначается  $X^k$ , а вход первой –  $X^0=1$ .
4. Сумматоры по модулю 2 устанавливаются на входе тех ячеек, для которых в формуле образующего многочлена  $X^i$  имеет ненулевое значение.  
Например, для  $P(x)=x^3+x+1$  сумматоры устанавливаются на входах триггеров 1 и 2(рис.11)
5. Выход последнего триггера соединяется с одним из входов сумматоров.



6. Выходы предыдущих триггеров соединяются со входами последующих через сумматоры или без них, в зависимости от того, установлены они между ячейками или нет.

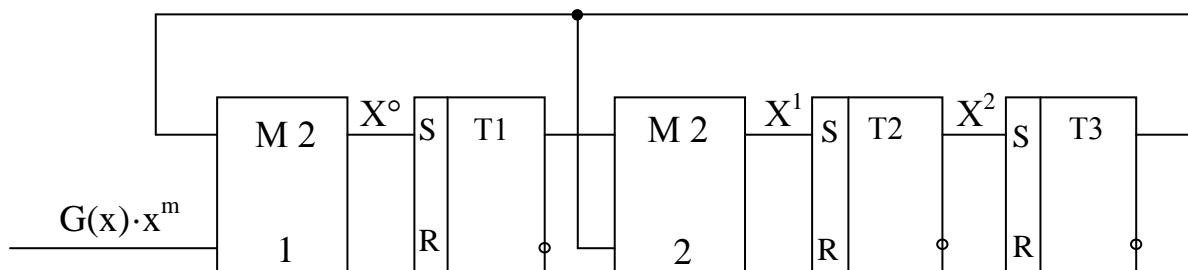


Рис.12

Сдвиг информации в регистре осуществляется импульсами, поступающими от генератора импульсов, который на схеме рис.12 не показан. На вход устройства поступают только коэффициенты многочленов, начиная с коэффициента при переменной в старшей степени.

За первые  $(n-m)$  тактов коэффициенты многочлена – делимого заполняют регистр, причем коэффициент при  $X$  в старшей степени достигает крайней правой ячейки. На следующем такте “единица” делимого, выходящая из крайней ячейки регистра, по цепи обратной связи подается к сумматорам по модулю 2, что равносильно вычитанию – делителя из многочлена – делимого. Если в результате предыдущей операции коэффициент при старшей степени  $X$  у остатка оказался равным нулю, то на следующем такте делитель не вычитается. Коэффициенты делимого только сдвигаются вперед по

регистру на один разряд, что находится в полном соответствии с тем, как это делается при делении многочленов столбиком.

Деление заканчивается с приходом последнего символа многочлена – делимого. При этом разность будет иметь более низкую степень, чем делитель. Эта разность и есть остаток.

Рассмотрим процесс деления многочлена 1001 на образующий многочлен  $P(x)=x^3+x+1$  (рис.13). Работа схемы поясняется таблицей 1.

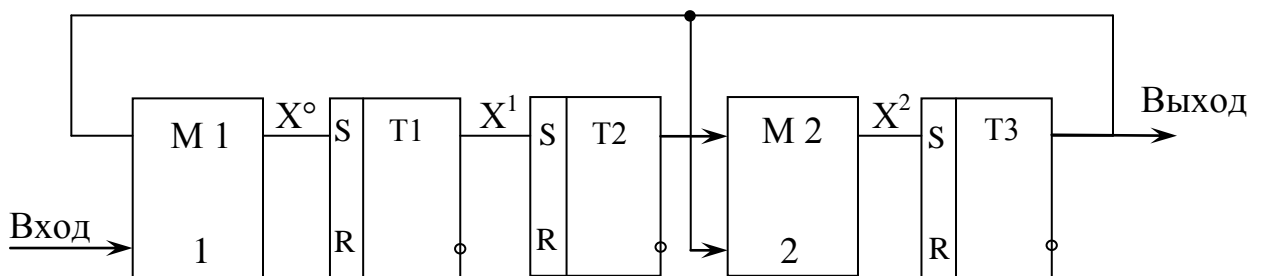


Рис.13

Таблица 1

№ тактов	Вход	Состояние ячеек регистра		
		T1	T2	T3
1	1	1	0	0
2	0	0	1	0
3	0	0	0	1
4	1	0	0	1
5	0	1	0	1
6	0	1	1	1
7	0	1	1	0
8	-	0	1	1
9	-	1	0	0
10	-	0	1	0
11	-	0	0	1
12	-	1	0	1
13	-	1	1	1
14	-	1	1	0

Вычисление остатка начинается с четвертого такта и заканчивается после седьмого такта.

### Кодирующие устройства

На практике кодирующие устройства строятся таким образом, что коэффициенты кодируемого многочлена участвуют в обратной связи не через  $n-m$  сдвигов, а сразу с первого такта. Это позволяет устранить разрыв между информационными и проверочными символами. Для рассматривавшегося ранее случая схема кодирующего устройства приведена на рис.14.

Сумматор, который ставится перед первым триггером (вход  $X^0$ ), подключается в этой схеме через ключ  $K2$ .

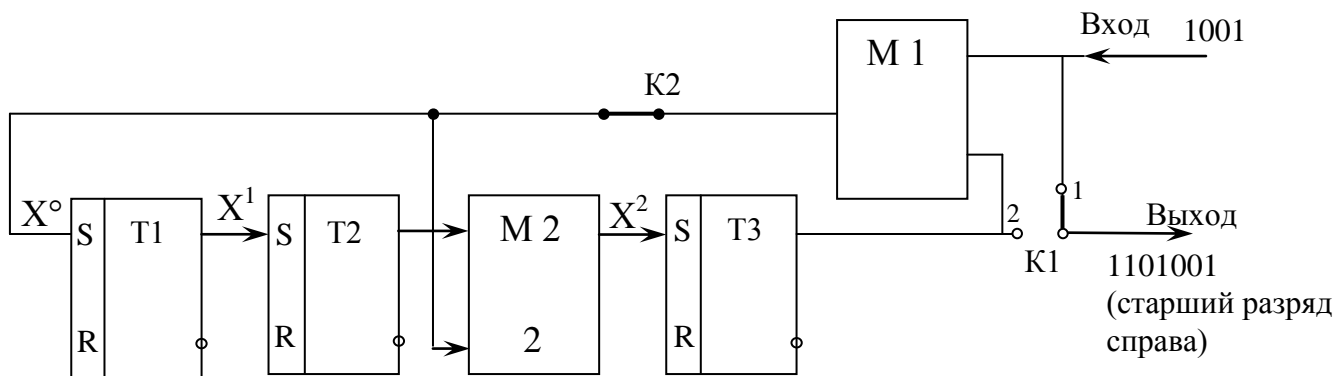



Рис.14

В исходном состоянии ключ  $K1$  находится в состоянии 1, а ключ  $K2$  замкнут. Информационные символы одновременно поступают как в линию связи, так и в регистр сдвига, где за  $m$  тактов образуется остаток. Затем ключ  $K2$  размыкается, ключ  $K1$  переходит в положение 2 и остаток поступает в линию связи. Процесс формирования кодовой

комбинации шаг за шагом приведен в таблице 2, где черточками отмечены освобождающиеся ячейки, занимаемые новыми информационными символами.

Таблица 2

№ тактов	Вход	Состояние ячеек			Выход
		1	2	3	
1	1	1	0	1	1
2	0	1	1	1	01
3	0	1	1	0	001
4	1	1	1	0	1001
5	0	-	1	1	01001
6	0	-	-	1	101001
7	0	-	-	-	1101001


 контрольные разряды      исходная информация

Декодирующее устройство.

В этих устройствах для обнаружения и исправления ошибок производится деление принятой кодовой комбинации на тот же образующий многочлен, который использовался при формировании комбинации данного циклического кода.

Декодирующие устройства в принципе мало отличаются от кодирующих устройств. В случае исправления ошибок схема несколько усложняется, так как информацию о разрядах, в которых

произошла ошибка, несет остаток. Схема декодирующего устройства для образующего полинома  $x^3+x^2+1$  представлена на рис.15.

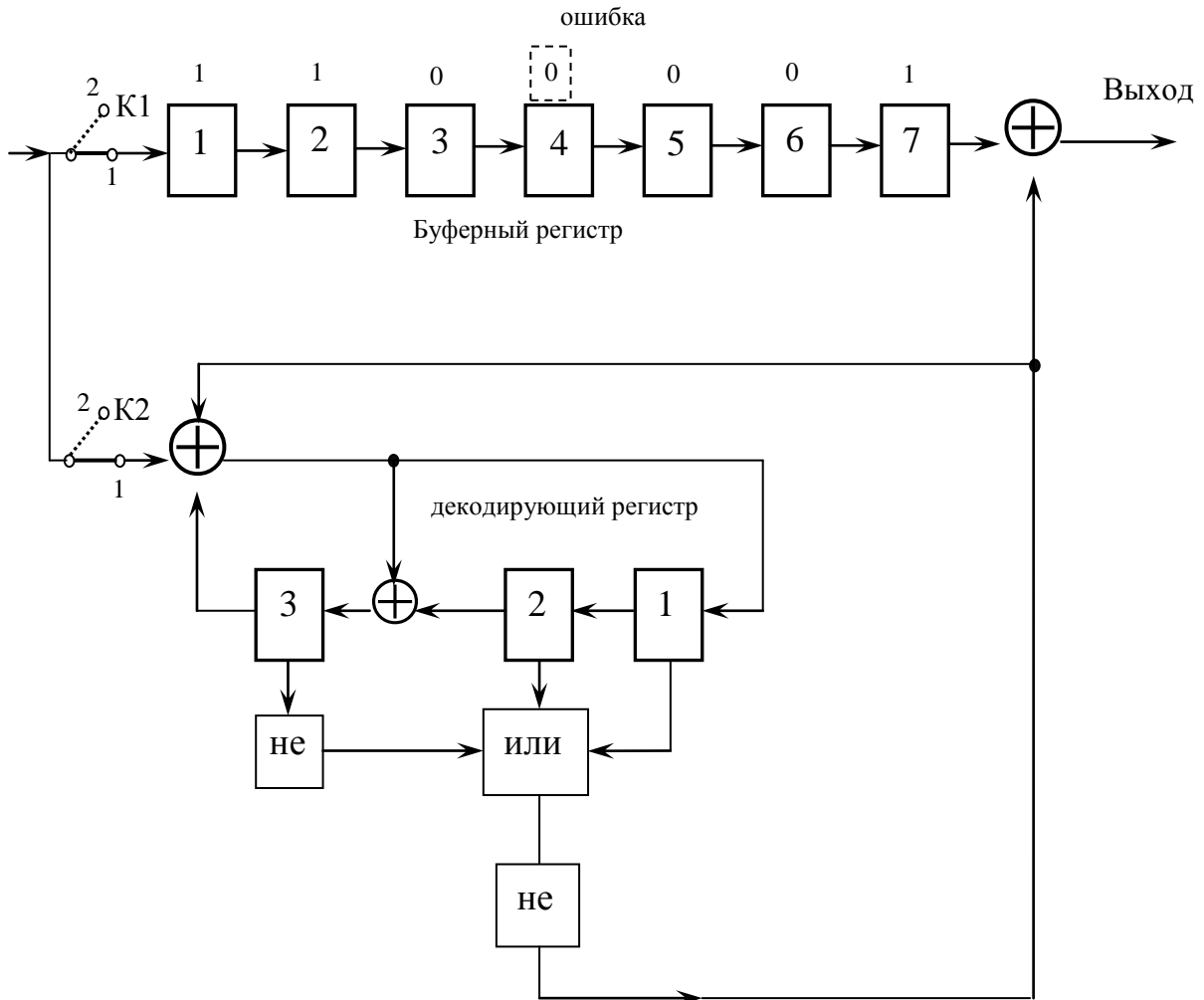


Рис.15

Символы подлежащей декодированию кодовой комбинации, возможно содержащей ошибку, последовательно, начиная со старшего разряда, вводятся в n-разрядный буферный регистр сдвига и одновременно в (n-m)-разрядный декодирующий регистр. В нашем случае  $n=7$  и  $(n-m)=3$ .

Электронный ключ К1 пропускает в буферный регистр только  $m$  информационных символов. В декодирующем регистре за  $n$  тактов определяется остаток, после чего вход регистра отключается (ключом К2) и в нем производится еще  $n$  сдвигов. С каждым сдвигом буферный регистр покидает один символ, а в декодирующем регистре появляется новый остаток. На выходы декодирующего регистра подключена комбинаторно-логическая схема, построенная таким образом, чтобы она отмечала все те остатки, которые появляются в декодирующем регистре, когда каждый из ошибочных символов занимает крайнюю правую ячейку в буферном регистре. При следующем сдвиге на выходе комбинаторно-логической схемы образуется единица, которая, воздействуя на сумматор коррекции, исправляет искаженный символ. Декодирование длится  $2n$  тактов.

Самый простой детектор получается в том случае, если используется код, рассчитанный на исправление одиночных ошибок. Если исказился символ старшего разряда, занимающий крайнюю правую ячейку буферного регистра, то вектор ошибки равен 001. В зависимости от номера искаженного разряда после первых  $n$  сдвигов будем получать различные остатки. Вследствие этого выделенный остаток будет появляться в декодирующем регистре через различное число последующих сдвигов, обеспечивая исправление искаженного символа.

В рассматриваемом примере после седьмого такта сдвига получена в декодирующем регистре комбинация 011, что указывает на ошибку в четвертом информационном разряде. На девятом такте сдвига в декодирующем регистре образуется кодовая комбинация 001. На этом же такте на выходе буферного регистра появится ошибочный символ. Единица декодирующего регистра, воздействуя на сумматор

коррекции, исправит искаженный символ. В нашем случае “0” будет преобразован в “1”, т.е. будет скорректирована искаженная кодовая комбинация и в результате получена исходная комбинация 1101001.

Одновременно по цепи обратной связи с выхода декодирующего регистра подается на его входной сумматор единица, которая устанавливает ячейки декодирующего регистра в нулевое состояние.

В таблице 3 шаг за шагом представлен процесс исправления ошибки в четвертом разряде кодовой комбинации

1 1 0 1 0 0 1

Таблица 3

№ такта	Вход	Состояние ячеек декодирующего регистра			Выход декодирующего регистра	Выход декодирующего устройства
		1	2	3		
1	1	1	0	1	0	
2	0	1	1	1	0	
3	0	0	1	1	0	
4	ошибка 0	1	1	0	0	
5	0	0	0	1	0	
6	1	0	0	0	0	
7	1	1	1	0	0	
8	0	0	0	<b>1</b>	0	1
9	0	0	<b>1</b>	0	0	01
10	0	<b>1</b>	0	0	Исправление <b>1</b>	001
11	0	0	0	0	0	<b>1001</b>
12	0	0	0	0	0	<b>01001</b>
13	0	0	0	0	0	<b>101001</b>
14	0	0	0	0	0	<b>1101001</b>

В таблице 4 приведены некоторые образующие многочлены циклического кода.

Таблица 4

Код	Многочлен	Код	Многочлен
11	$x+1$	1011111	$x^6+x^4+x^3+x^2+x+1$
101	$x^2+1$	1100001	$x^6+x^5+1$
111	$x^2+x+1$	1100011	$x^6+x^5+x+1$
1001	$x^3+1$	1100101	$x^6+x^5+x^2+1$
1011	$x^3+x+1$	1100111	$x^6+x^5+x^2+x+1$
1101	$x^3+x^2+1$	1101001	$x^6+x^5+x^3+1$
1111	$x^3+x^2+x+1$	1101011	$x^6+x^5+x^3+x+1$
10001	$x^4+1$	1101101	$x^6+x^5+x^3+x^2+1$
10011	$x^4+x+1$	1101111	$x^6+x^5+x^3+x^2+x+1$
10101	$x^4+x^2+1$	1110001	$x^6+x^5+x^4+1$
10111	$x^4+x^2+x+1$	1110011	$x^6+x^5+x^4+x+1$
11001	$x^4+x^3+1$	1110101	$x^6+x^5+x^4+x^2+1$
11011	$x^4+x^3+x+1$	1110111	$x^6+x^5+x^4+x^2+x+1$
11101	$x^4+x^3+x^2+1$	1111001	$x^6+x^5+x^4+x^3+1$
11111	$x^4+x^2+x+1$	1111011	$x^6+x^5+x^4+x^3+x+1$
100001	$x^5+1$	1111101	$x^6+x^5+x^4+x^3+x^2+1$
100011	$x^5+x+1$	1111111	$x^6+x^5+x^4+x^3+x^2+x+1$
100101	$x^5+x^2+1$	10000001	$x^7+1$
100111	$x^5+x^2+x+1$	11100001	$x^7+x^6+x^5+1$
101001	$x^5+x^3+1$	100000001	$x^8+1$
101011	$x^5+x^3+x+1$	100000011	$x^8+x+1$
101101	$x^5+x^3+x^2+1$	1000000001	$x^9+1$
101111	$x^5+x^3+x^2+x+1$	1100000001	$x^9+x^8+1$
110001	$x^5+x^4+1$	10000000001	$x^{10}+1$
110011	$x^5+x^4+x+1$	100000000001	$x^{11}+1$
110101	$x^5+x^4+x^2+1$	100000000011	$x^{11}+x+1$
110111	$x^5+x^4+x^2+x+1$	100000000101	$x^{11}+x^2+1$
111001	$x^5+x^4+x^3+1$	1000000000001	$x^{12}+1$
111011	$x^5+x^4+x^3+x+1$	10000000000001	$x^{13}+1$
111101	$x^5+x^4+x^3+x^2+1$	100000000000001	$x^{14}+1$
111111	$x^5+x^4+x^3+x^2+x+1$	100000000000011	$x^{14}+x+1$
1000001	$x^6+1$	100000000000101	$x^{14}+x^2+1$
1000011	$x^6+x+1$	100000000000111	$x^{14}+x^2+x+1$
1000101	$x^6+x^2+1$	100000000001001	$x^{14}+x^3+1$
1000111	$x^6+x^2+x+1$	100000000000001	$x^{15}+1$



1001001	$x^6+x^3+1$	1000000000000011	$x^{15}+x+1$
1001011	$x^6+x^3+x+1$	1100000000000011	$x^{15}+x^{14}+x+1$
1001101	$x^6+x^3+x^2+1$	10000000000000001	$x^{16}+1$
1001111	$x^6+x^3+x^2+x+1$	10000000000000011	$x^{16}+x+1$
1010001	$x^6+x^4+1$	10000000000000101	$x^{16}+x^2+1$
1010011	$x^6+x^4+x+1$	10000000000000111	$x^{16}+x^2+x+1$
1010101	$x^6+x^4+x^2+1$	10000000000001001	$x^{16}+x^3+1$
1010111	$x^6+x^4+x^2+x+1$	10000000000001011	$x^{16}+x^3+x+1$
1011001	$x^6+x^4+x^3+1$	10000000000001101	$x^{16}+x^3+x^2+1$
1011011	$x^6+x^4+x^3+x+1$	10000000000001111	$x^{16}+x^3+x^2+x+1$
1011101	$x^6+x^4+x^3+x^2+1$	10000000000010001	$x^{16}+x^4+1$
		10000000000010011	$x^{16}+x^4+x+1$

### Контрольные вопросы

1. Как записать  $n$ - разрядное число в виде полинома?
2. Дайте определение основных свойств циклических кодов.
3. Опишите принцип обнаружения ошибок в циклических кодах.
4. Что такое образующий многочлен и как он выбирается?
5. Опишите алгоритм формирования циклического кода.
6. Матричная запись циклического кода.
7. Каким образом с помощью матричной записи циклического кода можно получить любую кодовую комбинацию циклического кода?
8. Как определяется в циклическом коде номер разряда, где произошла ошибка?
9. Алгоритм обнаружения и исправления одиночных ошибок в циклическом коде.
10. Принцип построения кодирующих и декодирующих устройств циклического кода.
11. Что такое сумматор по модулю 2?
12. Как работает регистр сдвига?
13. Как определяется число каскадов регистра сдвига циклического кода?
14. Какое количество сумматоров по модулю 2 выбирается для кодирующего устройства конкретного циклического кода?
15. Где устанавливаются сумматоры по модулю 2 в кодирующем устройстве циклического кода?
16. С какой целью на выходе декодирующего регистра подключена комбинаторно- логическая схема?

## Код Хэмминга

Построение корректирующего кода Хэмминга производится исходя из требуемого объема информационных сообщений и статистических данных о наиболее вероятных векторах ошибок в используемом канале связи. Вектором ошибки будем называть кодовую комбинацию, имеющую единицы в разрядах, подвергшихся искажению, и нули во всех остальных разрядах. Любую искаженную кодовую комбинацию можно рассматривать как сумму по модулю 2 разрешенной кодовой комбинации и вектора ошибки.

В коде Хэмминга необходимое число проверочных разрядов определяется из известного соотношения

$$2^{n-k} - 1 \geq n$$

Значения символов в проверочных разрядах устанавливаются в результате суммирования по модулю 2 значений символов в определенных информационных разрядах.

В коде Хэмминга сопоставляются подлежащие исправлению номера разрядов с ошибками в разрядах, начиная с младшего, в порядке возрастания двоичных чисел. В этом случае каждому вектору ошибки соответствует своя кодовая комбинация, называемая опознавателем. Каждый опознаватель представляет собой двоичное число, в котором произошла ошибка.

Векторы ошибок	Опознаватели
0000001	001
0000010	010
0000100	011
0001000	100
0010000	110
1000000	111

Сущность кода Хэмминга состоит в том, что производятся многократные проверки на четность различных вариантов сумм разрядов полученного кода, в результате которых получается двоичный код номера искаженного разряда.

Пользуясь приведенной выше таблицей, нетрудно определить, символы каких разрядов должны входить в каждую из проверок на четность.

Предположим, что в результате первой проверки на четность для младшего разряда опознавателя будет получена единица. Очевидно, это может быть следствием ошибки в одном из разрядов, опознаватели которых в младшем разряде имеют единицу. Следовательно, первое проверочное равенство должно включать символы 1-го, 3-го, 5-го, 7-го и т.д. разрядов:

$$a_1 \oplus a_3 \oplus a_5 \oplus \dots = 0$$

Единица во втором разряде опознавателя может быть следствием ошибки в разрядах, опознаватели которых имеют единицу во втором разряде. Отсюда второе проверочное равенство должно иметь вид:

$$a_2 \oplus a_3 \oplus a_6 \oplus a_7 = 0$$

Аналогично находим и третье равенство:

$$a_4 \oplus a_5 \oplus a_6 \oplus a_7 = 0$$

Чтобы эти равенства при отсутствии ошибок удовлетворялись для любых значений информационных символов в кодовой комбинации, необходимо использовать в нашем случае три проверочных разряда (всего семь информационных разрядов). Следует выбрать так номера этих разрядов, чтобы каждый из них входил только в одно из равенств. Это обеспечит однозначное определение значений символов в проверочных разрядах при кодировании. Указанному условию удовлетворяют разряды, опознаватели которых имеют по одной единице. Это будет первый, второй, четвертый, восьмой и т.д. разряды.

Таким образом, для кода, например, (7,4), исправляющего одиночные ошибки, искомые соотношения принимают вид:

$$a_1 = a_3 \oplus a_5 \oplus a_7$$

$$a_2 = a_3 \oplus a_6 \oplus a_7$$

$$a_4 = a_5 \oplus a_6 \oplus a_7$$

В принципе, место расположения контрольных разрядов в коде Хэмминга безразлично, но определенные удобства создает такое размещение, при котором контрольные разряды входили бы в возможно меньшее число сумм, получаемых при проверке кода. Это будет, если контрольные размещать в разрядах, номера которых равны целой степени числа 2, т.е. в разрядах: 1,2,4,8,16,32 и т.д.

Проверка на приемной стороне принятой кодовой комбинации осуществляется следующим образом: создаются контрольные суммы  $S_1, S_2, S_3$  и  $S_4$ .

$$S_1 = a_1 \oplus a_3 \oplus a_5 \oplus a_7 \dots$$

$$S_2 = a_2 \oplus a_3 \oplus a_6 \oplus a_7 \dots$$

$$S_3 = a_4 \oplus a_5 \oplus a_6 \oplus a_7 \dots$$

$$S_4 = a_8 \oplus a_9 \oplus a_{10} \oplus a_{11} \dots$$

Правило построения контрольных сумм:

$S_1$  - все нечетные разряды

$S_2$  - начиная со второго разряда по два разряда подряд через два разряда

$S_3$  - начиная с 4<sup>го</sup> разряда по 4 разряда через 4

$S_4$  - начиная с 8<sup>го</sup> разряда по 8 разрядов через 8 разрядов.

Если все суммы равны нулю, то в принятой кодовой комбинации нет ошибки. В случае, когда одна или несколько контрольных сумм равны единице, то эти суммы располагаются слева направо в порядке возрастания индексов и полученная запись в двоичном коде указывает на номер разряда, где произошла ошибка.

Пример. Построить код Хэмминга с исправлением одиночной ошибки при 11 информационных разрядах, т.е.  $m=11$ . Определим число контрольных разрядов.

$$2^{n-m} - 1 = n$$

$$2^{n-11} - 1 \geq 11 + k$$

$$n = 15$$

Число контрольных разрядов – 4.

Предположим, необходимо закодировать сообщение:

10110100111

Представим это информационное сообщение в виде кода Хэмминга, установив контрольные разряды на 1, 2, 4, 8 позициях.

15 14 13 12 11 10 9 8 7 6 5 4 3 2 1  
1 0 1 1 0 1 0  $a_8$  0 1 1  $a_4$  1  $a_2$   $a_1$

Определим значение контрольных разрядов, запишем их в соответствующих местах, и в окончательном виде код Хэмминга без ошибок будет выглядеть так:

1 0 1 1 0 1 0  $0$  0 1 1  $1$  1  $0$   $0$

Если при передаче данного сообщения произошло искажение в каком-либо информационном разряде, например, в третьем:

1 0 1 1 0 1 0  $0$  0 1 1  $1$  0  $0$   $0$

Найдем контрольные суммы:

$$S_1=1$$

$$S_2=1$$

$$S_3=0$$

$$S_4=0$$

По полученному коду

$$\begin{array}{c} S_4 S_3 S_2 S_1 \\ \boxed{0 \ 0 \ 1 \ 1} \end{array}$$

видно, что искажение произошло в третьем разряде.

### Матричная запись кода Хэмминга

Матрица кода Хэмминга состоит из двух частей:

1. Одиночной транспонированной матрицы в канонической форме, соответствующая количеству информационных разрядов;

2. Дополнительной матрицы, дописываемой справа, которая соответствует проверочным разрядам. Эта матрица содержит информацию о способе построения кода.

Каждую строку дополнительной матрицы можно получить, записав на основании найденных уравнений значения проверочных символов для соответствующей строки единичной транспонированной матрицы.

Пример: Матричная запись кода Хэмминга  $M_{(15,11)}$ .

Число информационных разрядов – 11.

Число контрольных разрядов – 4

Общее число разрядов кода Хэмминга – 15.

$$M_{(15,11)} = \begin{array}{c} \begin{array}{c} \text{единичная транспони-} \\ \text{рованная матрица} \\ \text{на 11 разрядов} \end{array} \qquad \begin{array}{c} \text{дополнитель-} \\ \text{ная матрица} \end{array} \\ \left| \begin{array}{cccccccccccc|cccc} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ a_{15} & a_{14} & a_{13} & a_{12} & a_{11} & a_{10} & a_9 & a_7 & a_6 & a_5 & a_3 & & a_8 & a_4 & a_2 & a_1 \end{array} \right| \end{array}$$



$$\begin{aligned}
a_1 &= a_3 \oplus a_5 \oplus a_7 \oplus a_9 \oplus a_{11} \oplus a_{13} \oplus a_{15} \\
a_2 &= a_3 \oplus a_6 \oplus a_7 \oplus a_{10} \oplus a_{11} \oplus a_{14} \oplus a_{15} \\
a_4 &= a_5 \oplus a_6 \oplus a_7 \oplus a_{12} \oplus a_{13} \oplus a_{14} \oplus a_{15} \\
a_8 &= a_9 \oplus a_{10} \oplus a_{11} \oplus a_{12} \oplus a_{13} \oplus a_{14} \oplus a_{15}
\end{aligned}$$

Полное множество разрешенных комбинаций можно получить, суммируя по модулю 2 строки соответствующей матрицы во всех возможных сочетаниях.

Пример. С помощью матрицы  $M_{(15,11)}$  закодировать следующую комбинацию с 11 информационными разрядами: 11111000000

Для этого складываем последние пять строк дополнительной матрицы по модулю 2.

$$\begin{array}{r}
1011 \\
1100 \\
1101 \\
1110 \\
\hline
1111 \\
1011
\end{array}$$

Следовательно, контрольные разряды данной кодовой комбинации  $a_1=1, a_2=1, a_4=0, a_8=1$ .

Располагаем контрольные разряды на соответствующих позициях и получаем окончательную запись кода Хэмминга:

$$\begin{array}{cccccccccccccccc}
a_{15} & a_{14} & a_{13} & a_{12} & a_{11} & a_{10} & a_9 & a_8 & a_7 & a_6 & a_5 & a_4 & a_3 & a_2 & a_1 \\
1 & 1 & 1 & 1 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 1
\end{array}$$

### Кодер и декодер кода Хэмминга

Кодер. Схема кодирующего устройства на четыре информационных разряда представлена на рис. 16

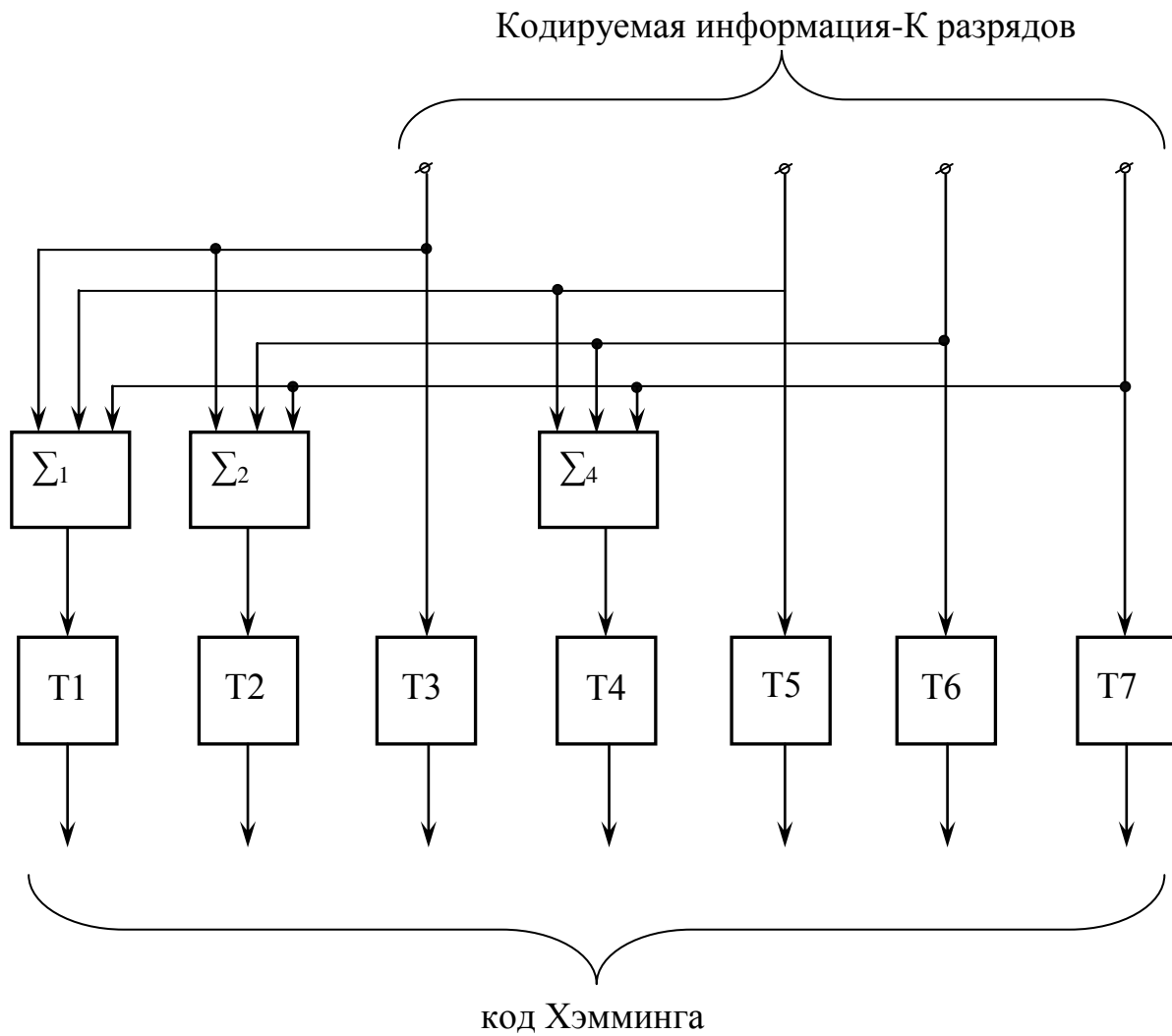


Рис.16

Со схемы управления поступает сигнал на кодирование  $k$  разрядной информации. Эта комбинация избыточного кода переписывается в информационные разряды  $n$ -разрядного регистра (триггеры Т3, Т5, Т6 и Т7).

Выходные импульсы сумматоров 1, 2, 4 устанавливают триггеры проверочных разрядов в положение 0 или 1 в соответствии с вышеприведенными равенствами.

Сформированная таким образом в регистре Т1-Т7 комбинация кода Хэмминга импульсом, поступающим с блока управления, считывается в линию связи.

Декодер.

Схема декодера представлена на рис.17

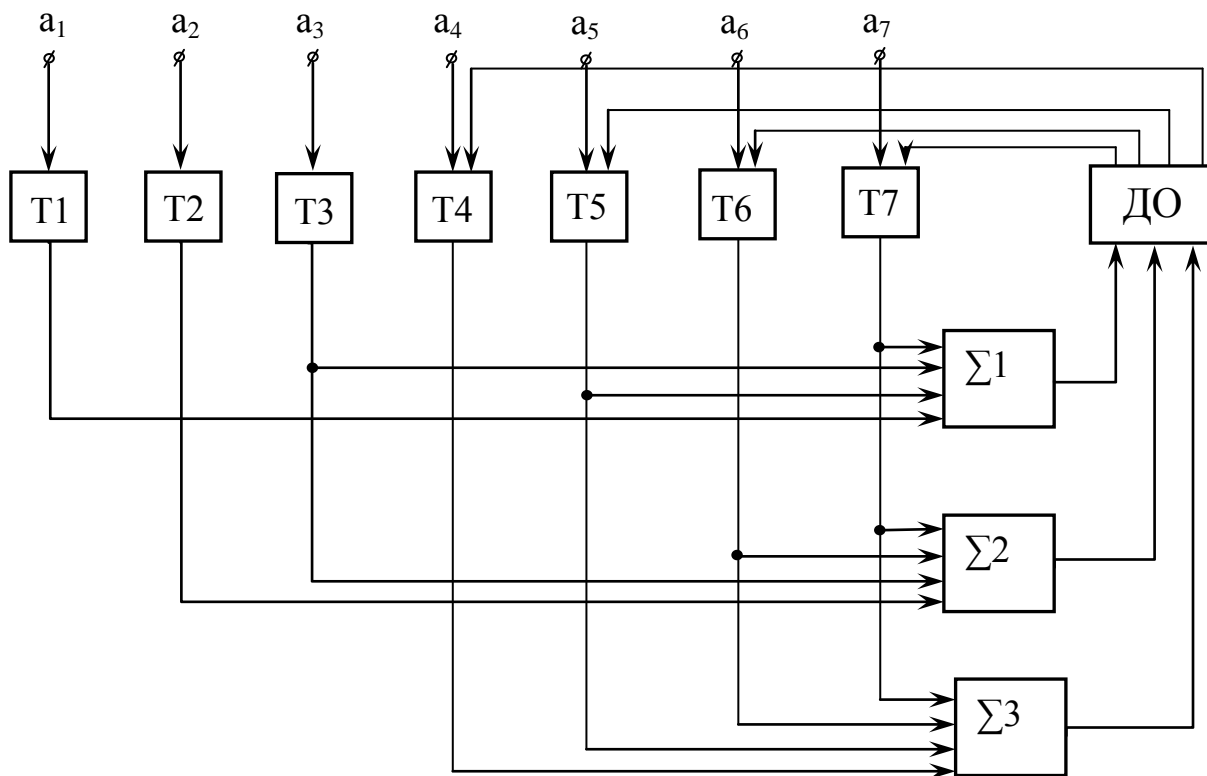


Рис.17

Схема строится на основе совокупности проверочных равенств.

Кодовая комбинация, возможно содержащая ошибку, поступает на n-разрядный приемный регистр (триггеры  $T_1-T_n$ , в нашем случае всего семь разрядов кода Хэмминга). По окончании переходного процесса в триггерах с блока управления на каждый из сумматоров ( $\Sigma_1-\Sigma_3$ ) поступает импульс опроса.

Если проверочные равенства выполняются, на выходах всех сумматоров будет “0”. При наличии ошибки в регистр опознавателей запишется опознаватель этого вектора ошибки. Дешифратор ошибки ДО ставит в соответствие множеству опознавателей множество векторов ошибок. Сигналы с дешифратора поступают только на те разряды, в которых вектор ошибки имеет единицы. Сигналы коррекции воздействуют на счетные входы триггеров. Последние изменяют свое состояние, и таким образом ошибка исправляется. На триггеры проверочных разрядов регистра импульсы коррекции не посылаются, так как после коррекции информация списывается только с информационных разрядов.

### Контрольные вопросы

1. Что такое опознаватели?
2. В чем сущность кода Хэмминга?
3. Как составляются проверочные равенства?
4. Что означает запись кода (7,4)?
5. Где располагаются в коде Хэмминга контрольные разряды?
6. Как по контрольным суммам определяется разряд, в котором произошла ошибка?
7. Из чего состоит матричная запись кода Хэмминга?
8. Как строится дополнительная матрица?
9. Как с помощью матричной записи кода Хэмминга можно получить множество разрешенных комбинаций?
10. Объясните работу кодера и декодера.

## Литература

1. Темников Ф.Е. и др  
Теоретические основы информационной техники, М., “Энергия”, 1971
2. Цымбал В.П.  
Теория информации и кодирование Киев, “Вища школа”, 1977
3. Харкевич А.А.  
Основы радиотехники. М, Связьиздат, 1963
4. Гойхман Э.Ш., Лосев Ю.И.  
Передача информации в АСУ. М., “Связь”, 1976
5. Солодов А.В.  
Теория информации и ее применение к задачам автоматического управления и контроля. М., “Наука”, 1967.
6. Игнатов В.А.  
Теория информации и передачи сигналов. М., “Советское радио”, 1979.

Ю.А.Дадаян

## ПОМЕХОУСТОЙЧИВОЕ КОДИРОВАНИЕ

Учебное пособие для студентов специальности  
“Информационно-измерительная техника и технологии” по курсу  
“Преобразование измерительных сигналов”

Формат 60×90/16. Бумага офсетная. Печать офсетная.  
Усл.и.л.1.0. Тираж 50 экз. Заказ №  
Отдел оперативной полиграфии РГУ нефти и газа им. И. М. Губкина.