ФЕДЕРАЛЬНОЕ АГЕНТСТВО СВЯЗИ
Северо-Кавказский филиал
ордена Трудового Красного Знамени федерального государственного
бюджетного образовательного учреждения высшего образования
«Московский технический университет связи и информатики»

МЕТОДИЧЕСКИЕ УКАЗАНИЯ
по выполнению практических занятий

по дисциплине

Многоканальные цифровые системы передачи и средства их защиты

для студентов очной и заочной форм обучения
Направление подготовки 11.03.02
Инфокоммуникационные технологии и системы связи
профиль Защищенные системы и сети связи

Ростов-на-Дону

2019

МЕТОДИЧЕСКИЕ УКАЗАНИЯ

по выполнению практических занятий по дисциплине

Многоканальные цифровые системы передачи и средства их защиты

Составитель: П.С.Шевчук, проф. кафедры ИТСС

Рассмотрено и одобрено
на заседании кафедры ИТСС
Протокол от «26» августа 2019 г. № 1

ПРАКТИЧЕСКОЕ ЗАНЯТИЕ №2

Синтез и расчет структур линейных кодов

Линейные блочные коды

Линейные блочные коды — это класс кодов с контролем четности, которые можно описать парой чисел *(n, k)*. В процессе кодирования блок из *k* символов сообщения (вектор сообщения) преобразуется в больший блок из *n* символов кодового слова (кодовый вектор), образованного с использованием элементов данного алфавита. Если алфавит состоит только из двух элементов (0 и 1), код является двоичным и включает двоичные разряды (биты). Последующее обсуждение линейных блочных кодов будет подразумевать именно двоичные коды.

k-битовые сообщения формируют набор из 2^k последовательностей сообщения, называемых *k-кортежами* (k-tuple) (последовательностями *k* цифр), k-битовые блоки могут формировать 2^n последовательности, также именуемые k-*кортежами.* Процедура кодирования сопоставляет с каждым из 2^k Л-кортежей сообщения *один* из 2^k л-кортежей. Блочные коды представляют взаимно однозначное соответствие, в силу чего 2^k k-кортежей сообщения *однозначно* отображаются в множество из 2^k л-кортежей кодовых слов; отображение производится согласно таблице соответствия. Для *линейных кодов* преобразование отображения является, конечно же, *линейным.*

Векторные пространства

Множество всех двоичных n-кортежей, Vn, называется *векторным пространством* над двоичным полем двух элементов (0 и 1). В двоичном поле определены две операции, сложение и умножение, причем результат этих операций принадлежит этому же множеству двух элементов. Арифметические операции сложения и умножения определяются согласно обычным правилам для алгебраического поля [4]. Например, в двоичном поле правила сложения и умножения будут следующими.

Сложение Умножение

$$0 \oplus 0 = 0 \quad 0 \cdot 0 = 0$$
$$0 \oplus 1 = 1 \quad 0 \cdot 1 = 0$$
$$1 \oplus 0 = 1 \quad 1 \cdot 0 = 0$$
$$1 \oplus 1 = 0 \quad 1 \cdot 1 = 1$$

Операция сложения, обозначаемая символом "$\oplus$", — это та же операция сложения по модулю 2, которая описывалась в разделе 2.9.3. Суммирование двоичных n-кортежей всегда производится путем сложения по модулю 2. Хотя для простоты мы чаще будем использовать для этой операции обычный знак +.

Векторные подпространства

Подмножество S векторного пространства *Vn* называется *подпространством,* если для него выполняются следующие условия.

1. Множеству S принадлежит нулевой вектор.
2. Сумма любых двух векторов в S также принадлежит *S (свойство замкнутости).*

При алгебраическом описании *линейных блочных кодов* данные свойства являются фундаментальными. Допустим, Vi и Vj — два кодовых слова (или кодовых вектора) в двоичном блочном коде (n, k*).* Код называется *линейным* тогда и только тогда, когда (Vi $\oplus$ Vj) также является кодовым вектором. Линейный блочный код — это такой код, в

котором вектор, не принадлежащий подпространству, нельзя получить путем сложения любых кодовых слов, принадлежащих этому подпространству.
Например, векторное пространство V4 состоит из следующих шестнадцати 4-кортежей.

0000 0001 0010 0011 0100 0101 0110 0111

1000 1001 1010 1011 1100 1101 1110 1111

Примером подмножества V4, являющегося подпространством, будет следующее.

0000 0101 1010 1111

Легко проверить, что сложение любых двух векторов подпространства может дать в итоге лишь один из векторов подпространства. Множество из 2^k n-кортежей называется *линейным блочным кодом* тогда и только тогда, когда оно является подпространством векторного пространству Vn всех n-коргежей. На рис. 6.10 показана простая геометрическая аналогия, представляющая структуру линейного блочного кода. Векторное пространство Vn можно представить как составленное из 2^n n-кортежей. Внутри этого векторного пространства существует подмножество из 2^k л-кортежей, образующих подпространство. Эти 2^k вектора или точки показаны разбросанными среди более многочисленных 2^n точек, представляющих допустимые или возможные кодовые слова. Сообщение кодируется одним из 2^k возможных векторов кода, после чего передается. Вследствие наличия в канале шума приниматься может измененное кодовое слово (один из 2^n векторов пространства n-кортежей). Если измененный вектор не слишком отличается (лежит на небольшом расстоянии) от действительного кодового слова, декодер может обнаружить сообщение правильно. Основная задача выбора конкретной части кода подобна цели выбора семейства модулирующих сигналов, и в контексте рис. 2.1ее можно определить следующим образом.

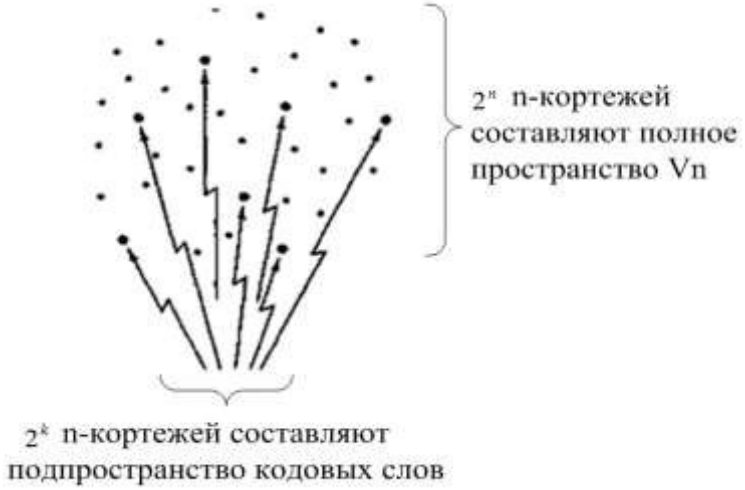


Рисунок 2.1 – Структура линейного блочного кода

1. Наполняя пространство Vn максимальным количеством кодовых слов, мы боремся за эффективность кодирования. Это равносильно утверждению, что мы хотим ввести лишь *небольшую избыточность* (избыток полосы).

2. Мы хотим, чтобы кодовые слова были *максимально удалены друг от друга,* так что даже если векторы будут искажены в ходе передачи, их все еще можно будет с высокой вероятностью правильно декодировать.

Пример линейного блочного кода (6,3)

Приведем необходимые предварительные замечания относительно кода (6,3). Он состоит из $2^k = 2^3 = 8$ векторов сообщений и, следовательно, восьми кодовых слов. В векторном пространстве V6 имеется 2^n (2^6 = шестьдесят четыре) 6-кортежей.
Нетрудно убедиться, что восемь кодовых слов, показанных в табл. 2.1, образуют в V6 подпространство (есть нулевой вектор, сумма любых двух кодовых слов дает кодовое слово этого же подпространства). Таким образом, эти кодовые слова представляют *линейный блочный код,* определенный в разделе 6.4.2. Может возникнуть естественный вопрос о соответствии кодовых слов и сообщений для этого кода (6, 3). Однозначного соответствия для отдельных кодов (n, *k)* не существует; хотя, впрочем, здесь нет полной свободы выбора. Подробнее о требованиях и ограничениях, сопровождающих разработку кода, будет рассказано в разделе 6.6.3.

Таблица 2.1. Соответствие кодовых слов и сообщений

Вектор сообщения	Кодовое слово
000	000000
100	110100
010	011010
110	101110
001	101001
101	011101
011	110011
111	000111

Матрица генератора

При больших *k* реализация *таблицы соответствия* кодера становится слишком громоздкой. Для кода (127,92) существует 2^{92} или приблизительно 5×10^{27} кодовых векторов. Если кодирование выполняется с помощью простой таблицы соответствия, то представьте, какое количество памяти нужно для такого огромного числа кодовых слов! К счастью, задачу можно значительно упростить, по мере необходимости генерируя необходимые кодовые слова, вместо того чтобы хранить их в памяти постоянно. Поскольку множество кодовых слов, составляющих линейный блочный код, является k-мерным подпространством n-мерного двоичного векторного пространства ($k < n$), всегда можно найти такое множество n-кортежей (с числом элементов, меньшим 2^k), которое может генерировать все 2^k кодовых слова подпространства. О генерирующем множестве векторов говорят, что оно *охватывает* подпространство. Наименьшее *линейно независимое* множество, охватывающее подпространство, называется *базисом* подпространства, а число векторов в этом базисном множестве является размерностью подпространства. Любое базисное множество *k* линейно независимых n-кортежей V1, V2,..., Vk можно использовать для генерации нужных векторов линейного блочного кода, поскольку каждый вектор кода является линейной комбинацией V1, V2,..., Vk. Иными словами, каждое из множества 2^k кодовых слов {U} можно представить следующим образом.

$$U = m_1V_1 + m_2V_2 + \ldots + m_kV_k$$

Здесь mi = (0 или 1) — цифры сообщения, а $i = 1,\ldots, k$.

Вообще, *матрицу генератора* можно определить как массив размером k x n.

$$G = \begin{bmatrix} V_1 \\ V_2 \\ \vdots \\ V_{k1} \end{bmatrix} = \begin{bmatrix} v_{11} & v_{12} & \cdots & v_{1m} \\ v_{21} & v_{22} & \cdots & v_{2m} \\ \vdots & & & \\ v_{k1} & v_{k2} & \cdots & v_{km} \end{bmatrix} \tag{2.1}$$

Кодовые векторы принято представлять векторами-строками. Таким образом, сообщение m (последовательность *k* бит сообщения) представляется как вектор-строка (матрица 1 x *k,* в которой 1 строка и *k* столбцов).

$$m = m_1, m_2, \ldots, m_k$$

В матричной записи генерация кодового слова U будет выглядеть как произведение m и G

$$U = mG, \tag{2.2}$$

где умножение матриц C = AB выполняется по следующему правилу.

$$c_{ij} = \sum_{k=1}^{n} a_{ik} b_{kj} \quad i = 1, \ldots, l \quad j = 1, \ldots, m$$

Здесь A — матрица размером l x *n,* B — матрица размером n x *m,* а результирующая матрица C имеет размер l x *m.* Для примера, рассмотренного в предыдущем разделе, матрица генератора имеет следующий вид.

$$G = \begin{bmatrix} V_1 \\ V_2 \\ V_3 \end{bmatrix} = \begin{bmatrix} 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 & 0 & 1 \end{bmatrix} \tag{2.3}$$

Здесь V1, V2 и V3 — три *линейно независимых вектора* (подмножество восьми кодовых векторов), которые могут сгенерировать все кодовые векторы. Отметим, что сумма любых двух генерирующих векторов в результате не дает ни одного генерирующего вектора (противоположность свойству замкнутости). Покажем, как с использованием матрицы генератора, приведенной в выражении (2.3), генерируется кодовое слово U4 для четвертого вектора сообщения 110 в табл. 2.1.

$$U_4 = \begin{bmatrix} 1 & 1 & 0 \end{bmatrix} \begin{bmatrix} V_1 \\ V_2 \\ V_3 \end{bmatrix} = 1 \cdot V_1 + 1 \cdot V_2 + 0 \cdot V_3 =$$
$$= 110100 + 011010 + 000000 =$$
$$= 101110 \ (\textit{кодовое слово для вектора сообщения } 110)$$

Таким образом, кодовый вектор, соответствующий вектору сообщения, является линейной комбинацией строк матрицы G. Поскольку код полностью определяется матрицей G, кодеру нужно помнить лишь *k* строк матрицы G, а не все 2^k кодовых вектора. Из приведенного примера можно видеть, что матрица генератора размерностью 3 x 6,

приведенная в уравнении (2.3), полностью заменяет исходный массив кодовых слов размерностью 8 x 6, приведенный в табл. 2.1, что значительно упрощает систему.

Систематические линейные блочные коды

Систематический линейный блочный код (systematic linear block code) *(n, k)* — это такое отображение n-мерного вектора сообщения в n-мерное кодовое слово, что часть генерируемой последовательности совмещается с *k* символами сообщения. Остальные (n - *k)* бит — это биты четности. Матрица генератора систематического линейного блочного кода имеет следующий вид.

$$G = \begin{bmatrix} & \vdots & \\ P & \vdots & I_k \\ & \vdots & \end{bmatrix} = \begin{bmatrix} p_{11} & p_{12} & \cdots & p_{1(n-k)} & 1 & 0 & \cdots & 0 \\ p_{21} & p_{22} & \cdots & p_{2(n-k)} & 0 & 1 & \cdots & 0 \\ \vdots & & & & & & \vdots & \\ p_{k1} & p_{k2} & \cdots & p_{k(n-k)} & 0 & 0 & \cdots & 1 \end{bmatrix} \quad (2.4)$$

Здесь P — массив четности, входящий в матрицу генератора, pij = (0 или 1), а Ik — единичная матрица размерностью k x k (у которой диагональные элементы равны 1, а все остальные — 0). Заметим, что при использовании этого систематического генератора процесс кодирования еще больше упрощается, поскольку нет необходимости хранить ту часть массива, где находится единичная матрица. Объединяя выражения (2.3) и (2.4), можно представить каждое кодовое слово в следующем виде.

$$u_1, u_2, \ldots, u_n = [m_1, m_2, \ldots m_k] \times \begin{bmatrix} p_{11} & p_{12} & \cdots & p_{1(n-k)} & 1 & 0 & \cdots & 0 \\ p_{21} & p_{22} & \cdots & p_{2(n-k)} & 0 & 1 & \cdots & 0 \\ p_{k1} & p_{k2} & \cdots & p_{k(n-k)} & 0 & 0 & \cdots & 1 \end{bmatrix},$$

где

$$\begin{aligned} u_i &= m_1 p_{1i} + m_2 p_{2i} + \ldots + m_k p_{ki} && для\ \ i = 1, \ldots, (n-k) \\ &= m_{i-n+k} && для\ \ i = (n-k+1), \ldots, n \end{aligned}$$

Для данного k-кортежа сообщения

$$m = m_1, m_2, \ldots, m_k$$

и k-кортежа кодовых векторов

$$U = u_1, u_2, \ldots, u_k$$

систематический кодовый вектор можно записать в следующем виде.

$$U = \underbrace{p_1, p_2, \ldots, p_{n-k}}_{биты\ четности}, \underbrace{m_1, m_2, \ldots, m_k}_{биты\ сообщения}, \quad (2.5)$$

где

$$p_1 = m_1 p_{11} + m_2 p_{12} + \ldots + m_k p_{k1}$$
$$p_2 = m_1 p_{12} + m_2 p_{22} + \ldots + m_k p_{k2}$$
$$p_{(n-k)} = m_1 p_{1(n-k)} + m_2 p_{2(n-k)} + \ldots + m_k p_{k(n-k)} \qquad (2.6)$$

Систематические кодовые слова иногда записываются так, чтобы биты сообщения занимали левую часть кодового слова, а биты четности — правую. Такая перестановка не влияет на свойства кода, связанные с процедурами обнаружения и исправления ошибок, поэтому далее рассматриваться не будет.

Для кода (6,3), кодовое слово выглядит следующим образом.

$$U = [m_1, m_2, m_3] \underbrace{\left[\begin{array}{ccc:ccc} 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 & 0 & 1 \end{array}\right]}_{P \qquad I_3} = \qquad (2.7)$$

$$= \underbrace{m_1 + m_3}_{u_1}, \underbrace{m_1 + m_2}_{u_2}, \underbrace{m_2 + m_3}_{u_3}, \underbrace{m_1}_{u_4}, \underbrace{m_2}_{u_5}, \underbrace{m_3}_{u_6} \qquad (2.8)$$

Выражение (2.8) позволяет получить некоторое представление о структуре линейных блочных кодов. Видно, что избыточные биты имеют разное происхождение. Первый бит четности является суммой первого и третьего битов сообщения; второй бит четности — это сумма первого и второго битов сообщения; а третий бит четности — сумма второго и третьего битов сообщения. Интуитивно понятно, что, по сравнению с контролем четности методом дублирования разряда или с помощью одного бита четности, описанная структура может предоставлять более широкие возможности обнаружения и исправления ошибок.

Проверочная матрица

Определим матрицу H, именуемую *проверочной,* которая позволит нам декодировать полученные вектора. Для каждой матрицы *(k* x n) генератора G существует матрица H размером (n - *k)* x n, такая, что строки матрицы G ортогональны к строкам матрицы H. Иными словами, $GH^T=0$, где H^T — *транспонированная* матрица H, а 0 — нулевая матрица размерностью k x (n-k). H^T— это матрица размером n x (n-k), строки которой являются столбцами матрицы H, а столбцы — строками матрицы H. Чтобы матрица H удовлетворяла требованиям ортогональности систематического кода, ее компоненты записываются в следующем виде.

$$H = \left[I_{n-k} \quad \vdots \quad P^T \right] \qquad (2.9)$$

Следовательно, матрица H^T имеет следующий вид.

$$H^T = \begin{bmatrix} I_{n-k} \\ \cdots\cdots \\ P \end{bmatrix} = \qquad (2.10,a)$$

$$= \begin{bmatrix} 1 & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 \\ \vdots & & & \\ 0 & 0 & \cdots & 1 \\ p_{11} & p_{12} & \cdots & p_{1,(n-k)} \\ p_{21} & p_{22} & \cdots & p_{2,(n-k)} \\ \vdots & & & \\ p_{k1} & p_{12} & \cdots & p_{k,(n-k)} \end{bmatrix} \qquad (2.10,6)$$

Нетрудно убедиться, что произведение UH^T любого кодового слова U, генерируемого G, и матрицы H^T дает следующее.

$$UH^T = p_1 + p_1, p_2 + p_2, \ldots, p_{n-k} + p_{n-k} = 0,$$

где биты четности $p_1, p_2, \ldots, p_{n-k}$ определены в уравнении (2.6). Таким образом, поскольку *проверочная матрица* H создана так, чтобы удовлетворять условиям ортогональности, она позволяет проверять принятые векторы на предмет их принадлежности заданному набору кодовых слов. U будет кодовым словом, генерируемым матрицей G, тогда и только тогда, когда $UH^T=0$.

Контроль с помощью синдромов

Пусть $r = r_1, r_2, \ldots, r_n$ — принятый вектор (один из 2^n n-кортежей), полученный после передачи $U = u_1, u_2, \ldots, u_n$ (один из 2n n-кортежей). Тогда r можно представить в следующем виде.

$$r = U + e \qquad (2.11)$$

Здесь $e = e_1, e_2, \ldots, e_n$ — вектор ошибки или ошибочная комбинация, внесенная каналом. Всего в пространстве из 2n n-кортежей существует 2n -1 возможных ненулевых ошибочных комбинаций. Синдром сигнала r определяется следующим образом.

$$S = rH^T \qquad (2.12)$$

Синдром — это результат проверки четности, выполняемой над сигналом r для определения его принадлежности заданному набору кодовых слов. При положительном результате проверки синдром S равен 0. Если r содержит ошибки, которые можно исправить, то синдром (как и симптом болезни) имеет определенное ненулевое значение, что позволяет отметить конкретную ошибочную комбинацию. Декодер, в зависимости от того, производит ли он прямое исправление ошибок или использует запрос ARQ, участвует в локализации и исправлении ошибки (прямое исправление ошибок) или посылает запрос на повторную передачу (ARQ). Используя уравнения (2.11) и (2.12), мы можем представить синдром r в следующем виде.

$$\begin{aligned} S &= (U + e)H^T = \\ &= UH^T + eH^T \end{aligned} \qquad (2.13)$$

Но для всех элементов набора кодовых слов $UH^T = 0$. Поэтому

$$S = eH^T \tag{2.14}$$

Из сказанного выше очевидно, что контроль с помощью синдромов, проведенный над искаженным вектором кода или над ошибочной комбинацией, вызвавшей его появление, даст один и тот же синдром. Важной особенностью линейных блочных кодов (весьма важной в процессе декодирования) является взаимно однозначное соответствие между синдромом и исправимой ошибочной комбинацией.

Интересно также отметить два необходимых свойства проверочной матрицы.

1. В матрице H не может быть столбца, состоящего из одних нулей, иначе ошибка в соответствующей позиции кодового слова не отразится в синдроме и не будет обнаружена.

2. Все столбцы матрицы H должны быть различными. Если в матрице H найдется два одинаковых столбца, ошибки в соответствующих позициях кодового слова будут неразличимы.

Пример 2.1. Контроль с помощью синдромов

Пусть передано кодовое слово U=101110 из примера линейного блочного кода (6,3) и принят вектор r=001110, т.е. крайний левый бит принят с ошибкой. Нужно найти вектор синдрома $S = rH^T$ и показать, что он равен eH^T.

Решение

$$S = rH^T =$$

$$= \begin{bmatrix} 0 & 0 & 1 & 1 & 1 & 0 \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 0 & 1 \end{bmatrix} =$$

= [l, 1 + 1, l + l] = [l 0 l] (синдром искаженного вектора кода)

Далее проверим, что синдром искаженного вектора кода равен синдрому ошибочной комбинации, которая вызвала эту ошибку.

$S = eH^T = \begin{bmatrix} 100000 \end{bmatrix} H^T = \begin{bmatrix} 100 \end{bmatrix}$ (синдром ошибочной комбинации)

Исправление ошибок

Итак, мы обнаружили отдельную ошибку и показали, что контроль с помощью синдромов, выполняемый как на искаженном кодовом слове, так и на соответствующей ошибочной комбинации, дает один и тот же синдром. Этот момент является ключевым, поскольку мы имеем возможность не только определить ошибку, но и (поскольку существует взаимно однозначное соответствие между исправимой ошибочной комбинацией и синдромом) исправить подобные ошибочные комбинации. Давайте так расположим 2" л-кортежей, которые представляют собой возможные принимаемые векторы, в так называемой *нормальной* матрице, чтобы первый ряд содержал все кодовые слова, начиная с кодового слова с одними нулями, а первый столбец — все исправимые

ошибочные комбинации. Напомним, что в число основных свойств линейного кода входит то, что набор кодовых слов должен содержать член в виде вектора, состоящего из одних нулей. Каждая строка сформированной матрицы, именуемая *классом смежности,* состоит из ошибочной комбинации в первом столбце, называемой *образующим элементом класса смежности,* за которой следуют кодовые слова, подвергающиеся воздействию этой ошибочной комбинации. Нормальная матрица для кода (и, *k)* имеет следующий вид.

$$\begin{array}{ccccccc} U_1 & U_2 & \cdots & U_i & \cdots & U_{2^k} \\ e_2 & U_2+e_2 & \cdots & U_i+e_2 & \cdots & U_{2^k}+e_2 \\ e_3 & U_2+e_3 & \cdots & U_i+e_3 & \cdots & U_{2^k}+e_3 \\ \vdots & \vdots & & & & \\ e_j & U_2+e_j & \cdots & U_i+e_j & \cdots & U_{2^k}+e_j \\ e_{2^{n-k}} & U_2+e_{2^{n-k}} & \cdots & U_i+e_{2^{n-k}} & \cdots & U_{2^k}+e_{2^{n-k}} \end{array} \qquad (2.15)$$

Отметим, что кодовое слово U1 (кодовое слово со всеми нулями) имеет два значения. Оно является кодовым словом, а также может рассматриваться как ошибочная комбинация e, — комбинация, означающая отсутствие ошибки, так что r = U. Матрица содержит все 2^n n-кортежей, имеющихся в пространстве *Vn.* Каждый n-кортеж упомянут *только один раз,* причем ни один не пропущен и не продублирован. Каждый класс смежности содержит 2^k n-кортежей. Следовательно, всего классов смежности будет $(2^n/2^k) = 2^{n-k}$.

Алгоритм декодирования предусматривает замену искаженного вектора (любого *n*-кортежа, за исключением указанного в первой строке) правильным кодовым словом, указанным вверху столбца, содержащего искаженный вектор. Предположим, что кодовое слово Ui (i = 1,..., 2^k) передано по каналу с помехами, в результате чего принят (искаженный) вектор Ui + ej. Если созданная каналом ошибочная комбинация ej является образующим элементом класса смежности с индексом *j* = 1,...,2^{n-k}, принятый вектор будет правильно декодирован в переданное кодовое слово Ui. Если ошибочная комбинация не является образующим элементом класса, то декодирование даст ошибочный результат.

Синдром класса смежности

Если ej является образующим элементом класса смежности или ошибочной комбинацией *j-го* класса смежности, то вектор Ui + ej является n-кортежем в этом классе смежности. Синдром этого n-кортежа можно записать в следующем виде.

$$S = (U_i + e_j)H^T = U_i H^T + e_j H^T$$

Поскольку Ui — это вектор кода и $UiH^T = 0$, то, как и в уравнении (2.14), мы можем записать следующее.

$$S = (U_i + e_j)H^T = e_j H^T \qquad (2.16)$$

Вообще, название *класс смежности* (или *сомножество)* — это сокращение от *"множество* чисел, имеющих совместные свойства". Что же все-таки общего между членами каждой данной строки (класса смежности)? Из уравнения (2.16) видно, что каждый член класса смежности имеет *один и тот же синдром.* Синдром каждого класса смежности отличается от синдромов других классов смежности; именно этот синдром используется для определения ошибочных комбинаций.

Декодирование с исправлением ошибок

Процедура декодирования с исправлением ошибок состоит из следующих этапов.

1. С помощью уравнения $S = rH^T$ вычисляется синдром r.

2. Определяются образующие элементы класса смежности (ошибочные комбинации) e, синдром которых равен rH^T**.**

3. Полагается, что эти ошибочные комбинации вызываются искажениями в канале.

4. Полученный исправленный вектор, или кодовое слово, определяется как U = r + ej. Можно сказать, что в результате вычитания определенных ошибок мы восстановили верное кодовое слово. *(Замечание:* в арифметических операциях по модулю 2 операция вычитания равносильна операции сложения.)

Локализация ошибочной комбинации

Возвращаясь к примеру3, мы составляем матрицу из 2^6 = шестидесяти четырех 6-кортежей, как это показано на рис. 2.2. Правильные кодовые слова — это восемь векторов в первой строке, а *исправимые ошибочные комбинации* — это семь ненулевых *образующих элементов классов смежности* в первом столбце. Заметим, что все однобитовые ошибочные комбинации являются исправимыми. Отметим также, что после того, как исчерпываются все однобитовые ошибочные комбинации, еще остаются некоторые возможности для исправления ошибок, поскольку учтены еще не все шестьдесят четыре 6-кортежа. Имеется один образующий элемент класса смежности, с которым ничего не сопоставлено; а значит, остается возможность исправления еще одной ошибочной комбинации. Эту ошибочную комбинацию (один из n-кортежей в оставшемся образующем элементе класса смежности) можно выбрать произвольным образом. На рис. 2.2 эта последняя исправимая ошибочная комбинация выбрана равной комбинации с двумя ошибочными битами 010001. Декодирование будет правильным тогда и только тогда, когда ошибочная комбинация, введенная каналом, будет одним из образующих элементов классов смежности.

000000 110100 011010 101110 101001 011101 110011 000111

000001 110101 011011 101111 101000 011100 110010 000110

000010 110110 011000 101100 101011 011111 110001 000101

000100 110000 011110 101010 101101 011001 110111 000011

001000 111100 010010 100110 100001 010101 111011 001111

010000 100100 001010 111110 111001 001101 100011 010111

100000 010100 111010 001110 001001 111101 010011 100111

010001 100101 001011 111111 111000 001100 100010 010110

Рисунок 2.2 – Пример нормальной матрицы для кода (6, 3)

Определим синдром, соответствующий каждой последовательности исправимых ошибок, вычислив ejH^T для каждого образующего элемента.

$$S = e_j \begin{bmatrix} 100 \\ 010 \\ 001 \\ 110 \\ 011 \\ 101 \end{bmatrix}$$

Результаты приводятся в табл. 2.2. Поскольку все синдромы в таблице различны, декодер может определить ошибочную комбинацию e, которой соответствует каждый синдром.

Таблица 2.2. Таблица соответствия синдромов

Ошибочная комбинация	Синдром
000000	000
000001	101
000010	011
000100	110
001000	001
010000	010
100000	100
010001	111

Пример исправления ошибки

Мы принимаем вектор r и рассчитываем его синдром с помощью выражения S = rH^T. Затем, используя таблицу соответствия синдромов (табл. 2.2), составленную в предыдущем разделе, находим соответствующую ошибочную комбинацию, которая является оценкой ошибки (далее будем обозначать ее через $\hat{e}$). Затем декодер прибавляет $\hat{e}$ к r и оценивает переданное кодовое слово U.

$$\hat{U} = r + \hat{e} = (U + e) + \hat{e} = U + (e + \hat{e}) \tag{2.17}$$

Если правильно вычислили ошибку: $\hat{e}$ = e, тогда оценка $\hat{U}$ совпадает с переданным кодовым словом U. С другой стороны, если оценка ошибки неверна, декодер неверно

определит переданное кодовое слово и мы получим *необнаружимую ошибку декодирования.*

Пример 2.2. Исправление ошибок

Пусть передано кодовое слово U=101110 из примера и принят вектор r = 001 ПО. Нужно показать, как декодер, используя таблицу соответствия синдромов (табл. 2.2), может исправить ошибку.

Решение

Рассчитывается синдром r.

$$S = [001\ 1\ 10]H^T=[100]$$

С помощью табл. 2,2 оценивается ошибочная комбинация, соответствующая приведенному выше синдрому.

$$\hat{e} = 1\ 0\ 0\ 0\ 0\ 0$$

Исправленный вектор равен следующему.

$$\begin{aligned}\hat{U} &= r + \hat{e} = \\ &= 0\ 0\ 1\ 1\ 1\ 0 + 1\ 0\ 0\ 0\ 0\ 0 = \\ &= 1\ 0\ 1\ 1\ 1\ 0\end{aligned}$$

Поскольку оцененная ошибочная комбинация в этом примере совпадает с действительной ошибочной комбинацией, процедура исправления ошибки дает $\hat{U}$ = U. Можно видеть, что процесс декодирования искаженного кодового слова путем предварительного обнаружения и последующего исправления ошибки можно сравнить с аналогичной медицинской процедурой. Пациент (потенциально искаженный вектор) приходит в медицинское учреждение (декодер). Врач проводит серию тестов (умножение на H^T), чтобы определить симптомы болезни (синдром). Допустим, врач нашел характерные пятна на рентгенограмме пациента. Опытный врач может непосредственно установить связь между симптомом и болезнью (ошибочной комбинацией). Начинающий врач может обратиться к медицинскому справочнику (табл. 2.2) для определения соответствия между симптомом (синдромом) и болезнью (ошибочной комбинацией). Последний шаг заключается в назначении соответствующего лечения, которое устранит болезнь (уравнение (2.17)). Продолжая аналогию двоичных кодов и медицины, можно сказать, что уравнение (2.17) — это несколько необычный способ лечения. Пациент излечивается в результате повторного заболевания той же болезнью.

Реализация декодера

Если код небольшой, например рассмотренный ранее код (6, 3), декодер может быть реализован в виде довольно простой схемы. Рассмотрим шаги, которые должны быть предприняты декодером: (1) вычислить синдром, (2) локализовать ошибочную комбинацию и (3) осуществить сложение по модулю 2 ошибочной комбинации и принятого вектора (что приводит к устранению ошибки). В примере 2.2, имея искаженный вектор, мы покажем, как с помощью последовательности этих шагов можно получить исправленное кодовое слово. Сейчас мы рассмотрим схему, показанную на рис. 2.3, где реализованы логические элементы исключающего ИЛИ и И, которые позволяют получить тот же результат для любой *комбинации с одним ошибочным битом* в коде (6, 3). Из табл. 2.2 и уравнения (2.16 можно записать все разряды синдрома через разряды принятых кодовых слов.

$$S = rH^T$$

$$S = [r_1 \;\; r_2 \;\; r_3 \;\; r_4 \;\; r_5 \;\; r_6] \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 0 & 1 \end{bmatrix}$$

и

$$s_1 = r_1 + r_4 + r_6$$
$$s_2 = r_2 + r_4 + r_5$$
$$s_3 = r_3 + r_5 + r_6$$

Мы используем эти выражения для синдромов при связывании схемы на рис. 2.3. Логический элемент "исключающее ИЛИ" — это и есть реализация той самой операции сложения (или вычитания) по модулю 2, поэтому он обозначен тем же символом "+". Маленький кружок в конце каждой линии, входящей в элемент И, означает операцию логического дополнения сигнала.

Искаженный сигнал подается на декодер одновременно в верхней части схемы, где происходит вычисление синдрома, и в нижней, где синдром преобразуется в соответствующую ошибочную комбинацию. Ошибка устраняется путем повторного добавления ее к принятому вектору, что дает в итоге исправленное кодовое слово.

Заметим, что с методической точки зрения рис. 2.3 составлен так, чтобы выделить алгебраические этапы декодирования — вычисление синдрома и ошибочной комбинации, а также выдачу исправленных выходных данных. В реальной ситуации код (n, *k)* обычно конфигурируется в систематическом виде.

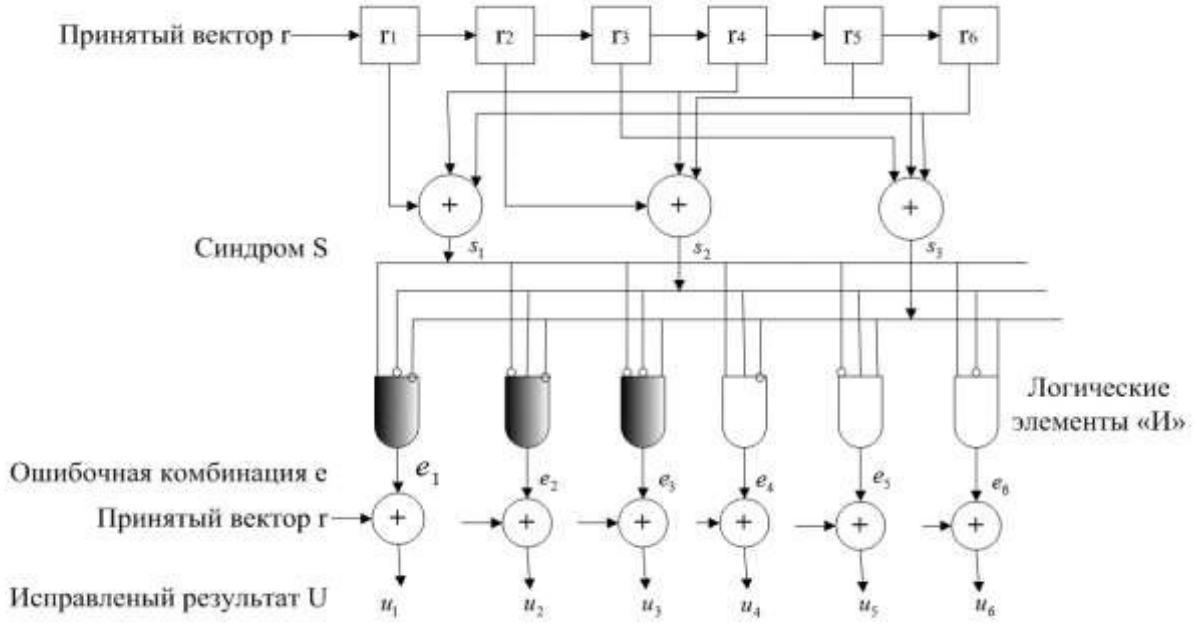


Рисунок 2.3 – Схема реализации декодера для кода (6, 3)

Декодеру не нужно выдавать полное кодовое слово; на выходе у него должны быть только биты данных. Поэтому схема на рис. 2.3 упрощается за счет удаления заштрихованных элементов. Для более длинных кодов такая реализация намного сложнее; в данной ситуации более предпочтительной методикой декодирования является последовательная схема, а не рассмотренный здесь параллельный метод [4]. Важно также подчеркнуть, что схема на рис. 2.3 позволяет определять и исправлять только комбинации кода (6, 3) с одним ошибочным битом. Исправление комбинаций с двумя ошибочными битами потребует дополнительной схемы.

Векторные обозначения

Выше кодовые слова, ошибочные комбинации, принятые векторы и синдромы обозначались как векторы U, e, r и S. Для упрощения записи индексы, сопутствующие конкретному вектору, в основном, опускались. Хотя, если быть точным, каждый из векторов U, e, r и S должен записываться в следующем виде.

$$x_j = \{x_1, x_2, \ldots, x_i, \ldots\}$$

Рассмотрим диапазон индексов *j* и i в контексте кода (6, 3), приведенного в табл. 2.1. Для кодового слова Uj индекс $j = 1,\ldots 2^k$ показывает, что имеется $2^3 = 8$ отдельных кодовых слов, а индекс j= 1,...,n демонстрирует, что каждое кодовое слово составлено из $n = 6$ бит. Для исправимой ошибочной комбинации ej индекс $j = 1,\ldots,2^{n-k}$ означает, что имеется $2^3 = 8$ образующих элементов классов смежности (7 ненулевых исправимых ошибочных комбинаций), а индекс i= 1,...,n указывает, что каждая ошибочная комбинация составлена из $n = 6$ бит. Для принятого вектора r, индекс $j = 1,\ldots,2^n$ показывает, что имеется $2^6 = 64$ n-кортежей, прием которых возможен, а индекс i=1,...,n указывает, что каждый принятый n-кортеж состоит из $n = 6$ бит. И наконец, для синдрома Sj индекс j = 1,...,n - k означает, что каждый синдром состоит из n - $k = 3$ бит. В этой главе индексы часто опускаются, и векторы Uj, ej, rj и Sj зачастую обозначаются как U, e, r, и S. Читателю следует помнить, что для этих векторов индексы всегда подразумеваются, даже в тех случаях, когда они опущены для простоты записи.

ПРАКТИЧЕСКОЕ ЗАНЯТИЕ 3.

ОБРАЗУЮЩИЕ ПОЛИНОМЫ И ФОРМИРОВАНИЕ ПСЕВДОСЛУЧАЙНЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ

МЕТОДЫ ГЕНЕРАЦИИ СЛУЧАЙНЫХ ЧИСЕЛ

Использование случайных чисел. Ряд алгоритмов защиты сети, основанных на средствах криптографии, предполагает использование случайных чисел. К таким алгоритмам относятся:

1. Схемы взаимной идентификации. Сценарии распределения ключей (рис. 6.4, 6.5) в процессе установления соединения используют оказии, чтобы исключить возможность атаки на основе воспроизведения сообщений. Использование случайных чисел для оказий не дает шанса оппоненту определить или угадать значение оказии.
2. Генерирование сеансовых ключей, выполняемое либо центром распределения ключей, либо одним из участников соединения.
3. Генерирование ключей для алгоритма RSA-шифрования с открытым ключом.

Из этих приложений вытекает два четких и необязательно сочетаемых требования к используемой последовательности случайных чисел: случайность и непредсказуемость.

Случайность. Традиционно при генерировании последовательности якобы случайных чисел требуется, чтобы последовательность получаемых чисел была случайной в некотором вполне определенном статистическом смысле. Для проверки любой последовательности на случайность обычно служат два критерия:

– однородность распределения: распределение чисел в последовательности должно быть однородным, т.е. частота появления в последовательности конкретного значения должна быть примерно одинаковой для всех значений;

– независимость: ни одно из значений последовательности не должно логически выводиться из других значений.

Существуют вполне четкие алгоритмы для проверки того, что некоторая последовательность чисел соответствует заданному распределению, но вот алгоритма, позволяющего «доказать» независимость, нет. Здесь применяется ряд тестов, позволяющих лишь продемонстрировать, что последовательность не является независимой. Общая стратегия состоит в применении таких тестов до тех пор, пока убеждение в независимости последовательности не станет достаточно правдоподобным.

Использование последовательности чисел, кажущихся статистически случайными, часто вытекает из криптографической структуры самого алгоритма шифрования.

Например, одним из главных требований схемы RSA-шифрования с открытым ключом является возможность генерирования простых чисел. При этом совсем не просто определить, является ли данное достаточно большое число N простым. Непосредственная проверка предполагает деление числа N на каждое целое число, меньшее $\sqrt{N}$. Если N оказывается порядка, скажем, 10150, что не является нереальным для современных методов криптографии с открытым ключом, то такая проверка оказывается сегодня далеко за рамками аналитических знаний человека и вычислительных возможностей компьютера. Однако существует ряд эффективных алгоритмов проверки простоты числа с помощью использования последовательности случайно выбранных целых чисел в относительно простых вычислениях. Если такая последовательность достаточно длинная (но существенно меньше, чем $\sqrt{10150}$), простота тестируемого числа может быть определена почти наверняка.

Такой подход, известный как рандомизация, служит для создания многих алгоритмов. По существу, если проблема чрезмерно сложна или требует очень много времени для точного решения, то для нахождения решения с любой требуемой долей уверенности применяется более простой и более быстрый способ, основанный на рандомизации.

Непредсказуемость. В приложениях типа взаимной идентификации или генерирования сеансовых ключей требование статистической случайности последовательности чисел оказывается не настолько важным, насколько требование непредсказуемости элементов последовательности. В «истинно» случайной последовательности каждое число статистически независимо от других чисел последовательности и, таким образом, непредсказуемо. Однако истинно случайные числа используются очень редко, чаще применяются последовательности чисел, которые выглядят случайными, но на самом деле генерируются с помощью некоторого алгоритма. В этом случае приходится заботиться о том, чтобы противник не имел возможности предсказать последующие элементы последовательности на основе предыдущих.

Физические источники случайных чисел. Нельзя сказать, что источники истинно случайных чисел являются очень распространенными устройствами. Потенциально такими источниками могут быть физические генераторы шумов, такие как импульсные детекторы ионизирующего излучения, газоразрядные лампы и конденсаторы с утечкой тока. Однако такие устройства могут найти весьма ограниченное применение в приложениях защиты сети. Здесь имеются проблемы как со случайностью, так и с точностью получаемых при этом чисел, не говоря уже о проблемах подключения такого рода устройств к каждой системе в сети. (Хотя известны случаи удачных применений их в генерации ключей, например, в российском криптографическом устройстве «Криптон»). Альтернативой может быть использование какого-нибудь из проверенных и опубликованных наборов случайных чисел. Однако такие наборы предлагают весьма ограниченный источник чисел по сравнению с потенциальными требованиями приложений защиты большой сети. К тому же хотя числа из подобных наборов действительно демонстрируют статистическую случайность, они вполне предсказуемы, так как оппонент, который знает, какой набор принят за основу, просто может взять его копию.

Поэтому криптографические приложения обычно используют алгоритмические методы генерирования случайных чисел. Соответствующие алгоритмы являются детерминированными и поэтому порождают последовательности чисел, которые статистически не случайны. Однако если алгоритм достаточно хорош, порождаемые им последовательности чисел выдерживают многие разумные тесты на случайность. Такие числа часто называют псевдослучайными.

Генераторы псевдослучайных последовательностей

Основная проблема классической криптографии долгое время заключалась в трудности генерирования непредсказуемых двоичных последовательностей большой длины с применением короткого случайного ключа. Существенный прогресс в разработке и анализе этих генераторов был достигнут лишь к началу шестидесятых годов.

Получаемые программно из ключа случайные или псевдослучайные ряды чисел называются на жаргоне отечественных криптографов гаммой, по названию — буквы γ греческого алфавита, которой в математических записях обозначаются случайные величины.

Интересно отметить, что в книге «Незнакомцы на мосту», написанной адвокатом разведчика Абеля, приводится термин «гамма», который специалисты ЦРУ пометили комментарием «музыкальное упражнение?», т.е. в пятидесятые годы они не знали его смысла.

Следует при этом подчеркнуть, что заслуга конструирования длинных псевдослучайных рядов с «хорошими» статистическими свойствами полностью принадлежит криптографии. Не следует думать, что они нужны лишь криптографам — картографирование Венеры стало возможным, когда длина периода случайного ряда импульсов превысила 1040. Фотографирование этой планеты нельзя было сделать потому, что она всегда закрыта

плотным слоем облаков. Локация же ее с Земли затруднена обилием помех и высокими требованиями к разрешению. Поэтому зондирование выполнялось случайной последовательностью импульсов указанного периода. После 300 зондирований, на что ушло более полугода, была получена карта, где различимы объекты размером около километра, а по высоте разрешение получено такое, какое достигнуто не везде на Земле. Генераторы псевдослучайных чисел используются очень широко в сотнях программных приложений — от конструирования ядерных реакторов и радиолокационных систем раннего обнаружения до поисков нефти и до многоканальной связи.

Можно сформировать три основных общих требования, которым должны удовлетворять криптографически стойкие генераторы псевдослучайных последовательностей и получаемые с их помощью гаммы:

1. Период гаммы должен быть достаточно большим для шифрования сообщений различной длины.
2. Гамма должна быть трудно предсказуемой. Это значит, что если известны тип генератора и кусок гаммы, то невозможно предсказать следующий за этим куском бит гаммы или предшествующий этому куску бит гаммы.
3. Генерирование гаммы не должно быть связано с большими техническими и организационными трудностями.

Самая важная характеристика генератора псевдослучайных чисел — это информационная длина его периода, после которого числа будут либо просто повторяться, либо их можно будет предсказать.

Эта длина практически определяет возможное число ключей криптосистемы. Чем эта длина больше, тем сложнее подобрать ключ.

Второе из указанных выше требований связано со следующей проблемой: на основании чего можно сделать заключение, что гамма конкретного генератора действительно является непредсказуемой?

Пока в мире нет универсальных и практически достоверных критериев для проверки этого свойства (см. обсуждение этого вопроса выше).

Чтобы гамма считалась случайной и непредсказуемой, как минимум, необходимо, чтобы ее период был очень большим, а различные комбинации бит определенной длины равномерно распределялись по всей ее длине. Это требование статистически можно толковать и как сложность закона генерации псевдослучайной последовательности чисел.

Если по достаточно длинному отрезку этой последовательности нельзя ни статистически, ни аналитически определить этот закон генерации, то в принципе этим можно удовлетвориться.

И, наконец, третье требование должно гарантировать возможность практической реализации генераторов псевдослучайных последовательностей с учетом требуемого быстродействия и удобства практичного использования.

Проблема генерации псевдослучайных последовательностей существует уже третье столетие. Одним из первых было предложение получать их как значения дробной части многочлена первой степени:

$$Y(n) = Ent\ (a \times n + b),\ a, b = const.$$

Если n пробегает значения натурального ряда чисел, то поведение Y(n) выглядит весьма хаотичным. Еще Карл Якоби доказал, что при рациональном коэффициенте a множество {Y(n)} конечно, а при иррациональном — бесконечно и всюду плотно в интервале от 0 до 1. Для многочленов больших степеней такая задача была решена лишь в 1916 г. выдающимся математиком прошедшего века Германом Вейлем. Кроме того, он установил критерий равномерности распределения любой функции от натурального ряда чисел. Небезынтересно привести его в краткой формулировке.

КРИТЕРИЙ ВЕЙЛЯ. Чтобы ряд X1, X2, X3, … был распределен равномерно в интервале от 0 до 1, необходимо и достаточно, чтобы для любой интегрируемой по Риману функции f(x) было справедливо соотношение $P\{f(M(x)) = Mf(x)\} = 1$.

Это соотношение выражает свойство, называемое эргодичностью и заключающееся в том, что среднее по реализациям псевдослучайных чисел равно среднему по всему их множеству с вероятностью 1.

Таким образом, Вейль доказал, что эргодичность гарантирует отсутствие экзотичности в поведении последовательности Xn.

Однако эти результаты далеки от практики получения псевдослучайных рядов чисел. Дело в том, что теорема Якоби относится к действительным числам x, которые не могут быть использованы при вычис-лениях, потому что иррациональные действительные числа требуют для своей записи бесконечное число знаков. Попытки замены настоящего иррационального числа его приближением на ЭВМ для генерации псевдослучайной последовательности опасны, так как получаемые последовательности оканчиваются циклами с коротким периодом.

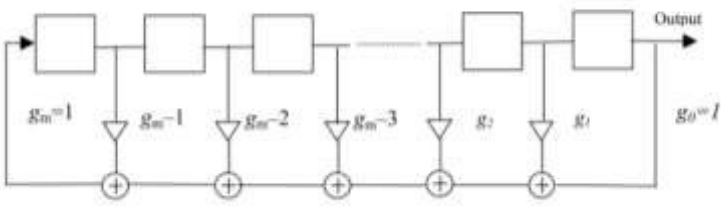
Наиболее давний вычислительный способ генерации псевдослучайных чисел на ЭВМ принадлежит Джону фон Нейману и относится к 1946 г. Этот способ базируется на том, что каждое последующее случайное число образуется возведением предыдущего в квадрат с последующим отбрасыванием цифр с обоих концов. Способ Неймана оказался ненадежным и очень быстро от него отказались.

Завершают доказательство непригодности полиномиальных и других функциональных преобразований натурального ряда чисел для получения псевдослучайных последовательностей результаты Пуанкаре. В частности, он установил, что непрерывное отображение T области U(x) числового пространства в себя обязательно приводит к короткой цикличности траекторий T(x) для всюду плотного в U множества точек. Ряды чисел, созданные такими методами, отягощены периодичностями.

Генератор последовательности Фибоначчи. Интересные классы генераторов случайных чисел неоднократно предлагались многими специалистами по целочисленной арифметике. В частности, Джордж Марсалиа и Ариф Зейман предложили класс генераторов псевдослучайных последовательностей, основанный на использовании последовательностей Фибоначчи, — в этой последовательности каждый последующий член, за исключением первых двух ее членов, равен сумме двух предыдущих:

{0, 1, 1, 2, 3, 5, 8, 13, 21, 34 …}.

Если эта последовательность применяется для начального заполнения массива большой длины, то, используя этот массив, можно создать генератор случайных чисел Фибоначчи с запаздыванием, где складываются не соседние, а удаленные числа. Марсалиа и Зейман предложили ввести в схему Фибоначчи «бит переноса», который может иметь начальное значение 0 или 1. Построенный на этой основе генератор «сложения с переносом» приобретает интересные свойства, на их основе можно создавать последовательности, период которых значительно больше, чем у применяемых в настоящее время конгруэнтных генераторов. По образному выражению Марсалиа, генераторы этого класса можно рассматривать как усилители случайности: «Вы берете случайное заполнение длиной в несколько тысяч бит и генерируете длинные последовательности случайных чисел». Один из вариантов генератора последовательности Фибоначчи
показан на рис.



Здесь квадратами обозначены разряды генератора, треугольниками — умножение на коэффициенты (на практике в зависимости от коэффициента там либо есть соединение с последующей логикой, либо его нет). Плюсы в кружках — это операция XOR: 0 + 0 = 0, 0 + 1 = 1, 1 + 1 = 0.

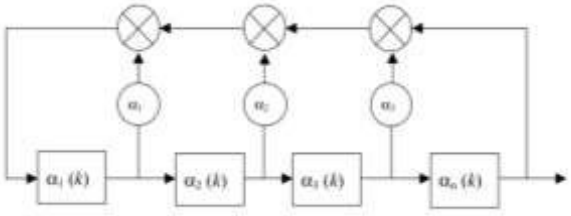
Рекуррентные двоичные последовательности. Линейные последовательности максимальной длины в основном получают с помощью генераторов, использующих в качестве основных элементов N-каскадные регистры сдвига и сумматоры по модулю 2 (фильтр Хаффмана). Генератор состоит из хорошо отработанных стандартных импульсных элементов и при минимальном их числе обеспечивает получение последовательности с максимальным периодом (М-последовательность). Достоинствами такого типа генератора являются фиксированная амплитуда, легко и в весьма широком диапазоне регулируемая ширина спектра сигнала, а также возможность путем небольших усложнений получать сдвинутые по шкале времени сигналы.

На рис. представлена схема N-разрядного регистра сдвига, выходные сигналы которого после обработки при помощи специальной цифровой логической схемы снова вводятся в регистр, замыкая тем самым цепь рециркуляции. Этот регистр является базой для построения генератора псевдослучайных последовательностей. При этом необходимо выполнение следующих условий:

– должно быть задано правило подключения сумматоров (α0, α2, …, αN);

– α0 и αN всегда равны 1 (поэтому на схеме их можно не указывать);

– из всех αi, i∈ {1, 2, …, N – 1}, хотя бы одно должно иметь значение ‘1’.



Фильтр Хаффмана

Циклические свойства генератора последовательности определяются так называемым характеристическим полиномом

$$\phi(x) = \sum_{k=0}^{N} \alpha_k x,k$$

где α0 = αN = 1, αj∈ {0,1}, j = 1,2, …, N – 1.

Период последовательности будет максимальным в том случае, когда многочлен ϕ(x) удовлетворяет условиям примитивности и неприводимости. В нахождении такого многочлена заключается основная задача синтеза генератора псевдослучайных последовательностей максимальной длины (ГППМД).

ГППМД составляют основу так называемых генераторов псевдослучайных чисел. Для этого к регистру сдвига добавляются сумматоры по модулю 2. При работе регистра сдвига на выходе этих элементах образуются М-последовательности {ak+s}, задержанные относительно исходной последовательности {ak}, полученной на выходе цепи обратной связи, на определенное число тактов. Величину задержки можно регулировать в пределах от N + 1 до T = 2N – 1. При этом на выходе данного генератора получаются равномерно распределенные псевдослучайные числа.

Благодаря своему свойству цикличности, М-последовательности получили большое распространение в задачах помехоустойчивого кодирования, что дало возможность использования фильтров Хаффмана в качестве простых кодирующих и декодирующих устройств.

Метод линейного сравнения (конгруэнтные генераторы).Безусловно, самым популярным алгоритмом для генерирования псевдослучайных чисел является алгоритм, предложенный
Д.Х. Лемером (Lehmer) и называемый методом линейного сравнения (конгруэнтным способом).

Этот алгоритм имеет четыре следующих параметра:

т модуль сравнения $m > 0$,

a множитель $0 \le a < m$,

c приращение $0 \le c < m$,

X0 начальное или порождающее число $0 \le X0 < m$.

Последовательность случайных чисел {X} получается с помощью итераций соотношения

$$Xn+1= (aXn + c) \bmod m.$$

При этом если т, a, c и X0 являются целыми, то будет получена последовательность целых чисел из диапазона $0 \le Xn < m$.

Выбор значений a, c и m оказывается очень важным в отношении разработки хорошего генератора случайных чисел.

Цель работы:

1. Закрепить теоретические знания по генераторам М-последовательностей;
2. Изучить методику и получить практические навыки по исследованию основных свойств М-последовательностей;
3. Научиться формировать структурные схемы генераторов М-последовательностей, построенных на основе регистров сдвига.
4. Изучить принципы построения радиоприемных устройств для приема ШПС.

Основные положения по технике безопасности

В приборах и устройствах, используемых в лабораторной установке, имеются высокие напряжения, опасные для жизни. Поэтому в процессе выполнения работы студенты должны соблюдать высокую дисциплину на занятии, точно, четко и своевременно выполнять все требования преподавателя и работников лаборатории.

Во избежание поражения электрическим током при выполнении лабораторной работы **запрещается:**

- самостоятельно включать аппаратуру;
- извлекать и вскрывать блоки лабораторных установок и измерительных приборов;
- заменять предохранители в блоках и измерительных приборах при включенной аппаратуре;
- прикасаться руками или какими-либо предметами (отвертками, оголенными концами проводов и т.п.) к зажимам и гнездам лабораторной установки и измерительных приборов.

В случае поражения электрическим током **немедленно:**

- выключить напряжение сети, освободить пострадавшего от токонесущих цепей, обеспечив собственную безопасность;
- доложить руководителю занятий о случившемся;
- оказать пострадавшему медицинскую помощь.

Эксплуатационные вопросы

1. Перед включением приборов необходимо провести их внешний осмотр и подготовку к работе, обратив внимание на наличие их заземления.
2. При проведении исследований необходимо соблюдать последовательность выполнения операций, указанных в настоящем руководстве.

Выбор сигнала в помехозащищенных радиоканалах

Постоянный большой интерес к широкополосным методам и системам передачи информации объясняется в основном их высокой помехоустойчивостью и скрытностью (помехозащищенностью). Реализация широкополосных методов и систем предполагает применение широкополосных сигналов, полоса частот которых существенно превышает полосу частот передаваемого сообщения. База широкополосных сигналов B_c удовлетворяет следующему условию

$$B_c = F_c * T_c >> 1 \qquad (1)$$

где F_c - полоса частот сигнала;

T_c - длительность сигнала.

Величина B_c характеризует количество информации, которое может нести сигнал.

В технической литературе часто используется понятие широкополосный метод или широкополосный канал. Широкополосным будем называть такой метод передачи сообщений, при котором используется широкополосный сигнал. По методу расширения спектра различают сигналы с расширением полосы частот и с расширением полосы частот несущей сигнала (сложные сигналы).

Сигнал с расширением полосы образуется путем угловой модуляции с большим индексом синусоидальной несущей. Такие сигналы имеют базу, удовлетворяющую условию (1). Сигналы с расширением спектра несущей могут быть образованы либо путем дополнительной модуляции несущей детерминированной функцией, либо путем использования широкополосной несущей. При расширении спектра синусоидальной несущей можно модулировать расширяющей функцией ее амплитуду, фазу или частоту. Тогда аналитическая запись несущей с расширенным спектром будет иметь вид (рассмотрим только модуляцию фазы)

$$U_{фм}(t) = A_c \cos[\omega_0 t + M_\varphi g(t) + \varphi] \qquad (2)$$

где A_c - амплитуда несущей сигнала;

ω_0 - частота несущей;

φ_0 - начальная фаза;

M_φ - индекс фазовой модуляции;

$g(t)$ - расширяющая функция.

Как правило, расширяющая функция является цифровой детерминированной периодической функцией. Это объясняется тем, что именно такие функции наиболее технологичны при их формировании и обработке. Можно по аналогии с формулой (1) ввести понятие базы расширяющей функции

$$B_g = F_g * T_g >> 1 \qquad (3)$$

где F_g – полоса частот функции $g(t)$,

T_g - период функции $g(t)$.

Таким образом, промодулированная синусоидальная несущая будет сама сложным сигналом, база которого определяется выражением (3).

В цифровых системах связи длительность ШПС и скорость передачи информации R связаны соотношением $T=1/R$. Поэтому база ШПС

$$B = F/R$$

характеризует расширение спектра ШПС относительно спектра сообщения

В качестве расширяющих функций, можно использовать различные кодовые (числовые) последовательности, в соответствии с которыми проводится манипуляция параметров несущей. Если используется двоичная последовательность, то сформированный на ее основе сигнал носит название бинарного. В настоящее время широкое применение в помехозащищенных радиоканалах находят линейные и нелинейные кодовые последовательности. Среди линейных последовательностей наиболее часто используются коды Баркера, Голда, последовательности Лежандра, М – последовательности и другие, относящиеся к линейным рекуррентным последовательностям. Основные требования к выбору последовательностей g(t) заключается в анализе их корреляционных свойств и размера ансамбля.

Свойства М – последовательности

Максимальность периода М – последовательности следует из того, что в процессе ее формирования генератор принимает все возможные состояния за исключением одного, когда во всех разрядах генератора записаны нули, ибо сумма по модулю два любого количества нулей равна нулю и генератор из этого состояния выйти не может. Поэтому период М – последовательности равен $L = 2^k - 1$.

Для дальнейшего рассмотрения материала следует сделать небольшое отступление и обсудить вопросы, связанные с корреляционными свойствами ПСП. Для их характеристики используются главным образом периодические и апериодические АКФ. По определению эргодических процессов, к которым по умолчанию относят детерминированные ПСП, корреляционная функция определяется как

$$k(\tau) = \frac{1}{T_s}\int_0^{T_s} S_{ПСП}(t) * S_{ПСП}(t-\tau)dt. \qquad (4)$$

Поскольку ПСП изменяют свое значение лишь в дискретные моменты времени, имеется возможность рассчитывать значение корреляционной функции лишь тогда, когда задержка τ кратна длительности элемента ПСП $\tau_э$. В промежутках между ними значение корреляционной функции изменяется линейно. Для расчета ПСП должны быть представлены в алгебраической форме в соответствии с уже известными правилами перехода.

Известно, что значение корреляционной функции рассчитываются по следующему правилу: для каждого дискретного временного сдвига между опорной ПСП и сдвинутой копией (другой ПСП в случае ВКФ) подсчитывается алгебраическая сумма попарных произведений элементов опорной ПСП и сдвинутой копии. Легко заметить, что она равна разности между количеством совпадений и несовпадений знака в опорной ПСП и копии. Отсюда следует вывод о том что периодические корреляционные функции имеют период, равный периоду ПСП, а апериодические действительно апериодичны.

М – последовательности обладают рядом полезных свойств, определивших их широкое применение для целей расширения спектра сигналов. К ним относятся следующие:

1. Цикличность. Это свойство заключается в том, что в М-последовательности периода N любые N элементов, взятые подряд, образуют период.

2. Уравновешенность. Это свойство заключается в том, что число единиц за период М-последовательности отличается от числа нулей не более, чем на единицу.

3. Свойство серий. Число серий за период М-последовательности, состоящих из одного символа, двух, трех, и т.д., образуют геометрическую прогрессию с множителем 0.5. Серией называется группа одноименных следующих друг за другом символов.

4. Статистическая независимость. Различные циклические перестановки М-последовательности статистически не зависят друг от друга, что выражается функцией их взаимной корреляции. Эта функция при любом циклическом сдвиге равна — *1/N,* при отсутствии сдвига 1.

5. При суммировании по модулю 2 М-последовательности с ее циклическим сдвигом образуется М-последовательность той же структуры с периодом, равным периоду исходной последовательности, но отличающаяся от нее циклическим сдвигом.

6. В результате суммирования по модулю 2 двух М-последовательностей различных периодов образуется М-последовательность с периодом, равным наименьшему периоду суммируемых последовательностей.

7. В М-последовательности содержатся все n-значные комбинации символов, кроме одной - запрещенной, каждая из которых встречается только один раз за период.

- объем ансамбля М – последовательностей (количество М – последовательностей разной структуры и одинакового периода) определяется формулой

$$N_м = \varphi(2^k - 1)/k, \qquad (5)$$

где $\varphi(2^k - 1)$ - функция Эйлера, численно равная количеству целых чисел, взаимно простых (т.е. не имеющих общих делителей) с аргументом этой функции.

Объем ансамбля М – последовательностей наиболее употребимых периодов представлен в таблице 1.

Таблица 1.

k	5	6	7	8	9	10	11	12	13	14	15	16
$N_м$	6	8	18	16	48	60	176	144	630	576	1800	2048

Для целого ряда применений объем ансамбля М – последовательностей недостаточен и остро встает задача создания ПСП, корреляционные свойства которых были бы не намного хуже корреляционных свойств М – последовательностей, а объем ансамбля был бы значительно больше.

Одним из наиболее распространенных способов получения больших ансамблей ПСП является применение последовательностей Голда (ПГ). ПГ образуются в результате сложения по модулю два двух М – последовательностей одинакового периода. Корреляционные свойства ПСП при этом ухудшаются незначительно, а переход к ПГ дает увеличение ансамбля более чем в 6000 раз. Примерно вдвое увеличиваются выбросы АКФ и ВКФ и незначительно ухудшаются периодические корреляционные функции.

Синтез генераторов М-последовательностей

Благодаря вышеперечисленным свойствам М-последовательности широко применяют в радиотехнических системах. Для пояснения этих свойств рассмотрим пример.

Допустим, что сдвигающий регистр (рис. 1) состоит из трех триггерных ячеек *Т1*, *Т2, Т3,* которые выполняют роль дискретных элементов задержек, и сумматора по модулю 2. На триггеры поступают сдвигающие импульсы, которые на рис. 1 не доказаны. Они следуют с тактовой частотой $1/\tau_0$. Каждый тактовый импульс вызывает изменение состояния (напряжения на выходе) всех триггеров. При этом напряжение на выходе каждого триггера (символ) становится равным напряжению (символу) на его входе для

предыдущего такта. Символы могут принимать два значения, которые условно обозначим 0 и 1. При суммировании любых комбинаций входных символов на выходе сумматора получаются только символы 0 и 1. Правило суммирования символов в двоичной системе счисления (с двумя возможными значениями символов) по модулю 2 (mod2) определяется табл. 2.

Таблица 2.

Суммирование по mod 2

Сумма	**0**	**1**
0	**0**	**1**
1	**1**	**0**

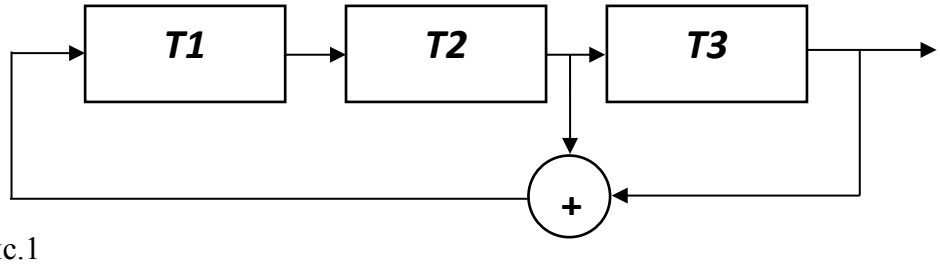


Рис.1

Выясним, в каких состояниях может находиться схема, представленная на рис. 1. Предположим, что в исходном состоянии символ на одном из выходов триггеров отличается от нуля, например символ на выходе триггера *T1* имеет значение 1, а на выходе *T2* и *T3* — значение 0. Тогда исходное состояние сдвигающего регистра характеризуется комбинацией выходных символов 100. На входе *T1* символ равен 0, так как согласно с табл. 2 символ на выходе сумматора равен 0+0=0. С поступлением на вход схемы очередного Сдвигающего импульса символы со входов триггеров «переходят» на их выходы. Новое установившееся состояние регистра описывается комбинацией выходных символов 010. На входе *T1* появляется 1, так как в соответствии с табл. 2 выходной символ сумматора равен 1+0=1. Аналогично определяются все состояния регистра, приведенные в табл. 3.

Таблица 3

Номер такта	**Вход T1**	**Выходы**			**Номер такта**	**Вход T1**	**Выходы**		
		T1	**T2**	**T3**			**T1**	**T2**	**T3**
.	.	.	.	.	6	0	0	1	1
.	.		.	.	7	1	0	0	1
.	.	.	.	.	8	0	1	0	0
1	0	1	0	0	9	1	0	1	0
2	1	0	1	0	.	.	.	.	.
3	1	1	0	1	.	.	.	.	.
4	1	1	1	0	.	.	.	.	.
5	0	1	1	1	.	.	.	.	.

Из рассмотрения табл. 3 видно, что состояния регистра (символы на выходе *T1, T2, T3)* различны для тактов 1—7, а для последующих тактов они повторяются. Так как число разрядов регистра k=3, а основание системы счисления (число используемых символов) p=2, то число возможных различных состояний регистра $p^k = 2^3=8$.

В табл. 3 отсутствует нулевая комбинация 000, так как её наличие согласно табл. 2 приводит к обращению в нуль всех символов во всех остальных комбинациях. Поэтому

в табл. 3 приведены только возможные для нормальной работы схемы (рис. 1) состояния регистра, число которых 2^3—1=7. После семи тактов состояния регистра повторяются.

Символы можно считывать с выхода любого триггера. В этом случае получаются последовательности, сдвинутые во времени (табл. 3).

Необходимо отметить, что при заданных *k* и *p* период последовательностей определяется схемой включения отводов сдвигающего регистра (выходов триггеров) в цепь обратной связи. Он может быть получен и меньше максимально возможного. Выбор соединений отводов сдвигающего регистра в цепи обратной связи для получения максимального периода последовательности при заданном числе разрядов регистра и основания системы счисления к настоящему моменту полностью определен и решается с помощью таблиц неприводимых многочленов.

При рассмотрении работы схемы рис. 1 было сделано допущение, что исходное состояние регистра характеризуется комбинацией 100. Из табл. 3 видно, что в качестве исходного можно взять любое состояние регистра. Это вызовет лишь сдвиг последовательности во времени.

Число единиц и нулей в периоде последовательности соответственно 4 и 3, причем сумма их равна N.

Сумма двух М-последовательностей, сдвинутых друг относительно друга, является М-последовательностью. В этом можно убедиться, суммируя согласно правилам табл. 2 любые последовательности из табл.3.

Это является следствием того, что сдвинутые М-последовательности можно получить с помощью одной и той же схемы.

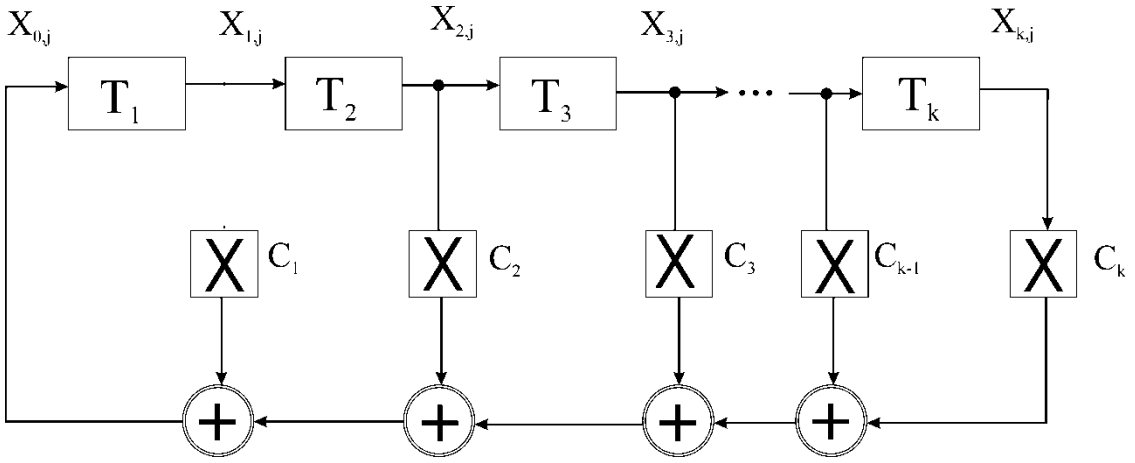


Рис.2

Цифровой автомат формирования М-последовательностей. Общая схема цифрового автомата, формирующего М-последовательность, приведена на рис. 2. Его основу составляет сдвигающий регистр с триггерами *T1*, *T2, ...*, T_k, которые осуществляют задержку входного символа на один такт длительностью τ_0. Допустим, что используются *p* различных символов: 0, 1, 2, ..., *p*—1, которые образуют конечное множество символов S=S(0, 1, ..., *p—1).* Символы на выходах триггеров при j-м такте обозначены через $x_{1,j}, x_{2,j}, \ldots, x_{k,j}$, причем $x_{i,j} \in S$. Символ на входе первого триггера обозначен $x_{0,j}$. Символ на выходе *l-го* триггера на (j+1)-м такте $x_{l,j+1} = x_{l-1,j}$, так как с каждым тактом символ со входа «переходит» на выход. Символы с выходов триггеров поступают на ум-

ножители, с выходов которых снимают символы $c_1 x_{1,j}$, $c_2 x_{2,j}$,..., $c_k x_{k,j}$ Множители $C_l \in S$.

Умножение любого числа на нуль означает, что символ на выходе умножителя всегда равен нулю. Это эквивалентно разрыву цепи между выходом триггера и сумматором. Следовательно умножитель может быть опущен. Например при p=2 (символы 0 и 1) множитель c_l может принимать значения 1 или 0, т.е. выходы триггеров или подсоединены к сумматорам, или нет.

Можно записать, что символ на входе *T1* в *j*-том такте равен:

$$x_{0,j} = c_1, x_{1,j} + c_2 x_{2,j} + \ldots + c_l x_{l,j} + \ldots + c_{k-1} x_{k-1,j} + c_k x_{k,j} \qquad (5)$$

Выражение (5) является линейным рекуррентным уравнением. Оно позволяет по известным *k* символам на выходах триггеров найти символ $x_{0,j}$, который в последующем такте перейдет на выход *T1*.

Анализ работы цифрового автомата формирования М-после-довательности на основе рекуррентного уравнения (5) показывает, что работа этого автомата полностью определяется характеристическим многочленом

$$f(x)=a_0 x^k + a_1 x^{k-1} + \ldots + a_{k-1} x + a_k , \qquad (6)$$

коэффициенты которого связаны с множителями c_1, ..., c_k следующим соотношением:

$$c_n = (-1)^{k+1} a_n \qquad (7)$$

Отрицательные значения c_n (7) можно свести с помощью сравнения по mod*p* к положительному числу множества *S*.

Для двоичных М-последовательностей, состоящих из символов 0 и 1 *(p=2),* множители c_n и коэффициенты a_n согласно (7) равны, т. е. $c_n = a_n$, причем $c_n = a_n = 1$.

Таким образом, для определения структуры цифрового автомата (необходимо знать характеристический многочлен степени *k.* Из теории М-последовательноетей известно, что характеристический многочлен *f(x)* степени *k,* во-первых, должен быть неприводимым, т. е. его нельзя представить в виде произведения многочленов меньших степеней, а во-вторых, он должен быть первообразным (примитивным) относительно двучлена x^N—1, т. е. характеристический многочлен *f(x)* (6) должен делить x^N—1 без остатка. Поэтому характеристический многочлен является первообразным корнем уравнения x^N—1. Если характеристический многочлен является первообразным, то он является и неприводимым.

Таким образом, чтобы при заданных *N, k* и *p* определить структуру регистра для формирования М-последовательности с периодом $N=p^k$—1, необходимо в качестве характеристического многочлена взять первообразный многочлен степени *k.*

Поскольку двоичные М-последовательности играли и играют особо важную роль в радиотехнических системах, то их свойства были изучены достаточно глубоко, в том числе и характеристические многочлены. Известны таблицы в которых приведены неприводимые многочлены до степени *k*=34. В Приложении 1 приведены в двоичной форме коэффициенты характеристических многочленов a_n для *k*=3...11, т. е. *N=7*... 2047, совпадающие с множителями c_n в схеме цифрового автомата (рис. 2), т. е. $a_n=c_n$. Характеристическому многочлену *f(x)* (6) в Прил. 1 соответствует последовательность представленных в виде 1 или 0. В каждом столбце указана степень многочлена *k* и его коэффициенты. В Прил. 1 приведены только те характеристические многочлены, которые порождают М-последовательности. Соответственно период М-последовательности

$N=2^h$—1. Знание коэффициентов a_n позволяет однозначно построить цифровой автомат формирования М-последовательностей. Если $a_n=c_n=1$, то выход *n-го* триггера подключен к сумматору по mod 2, если $a_n=c_n=0$, то выход *n-го* триггера к сумматору по mod 2 не подключен.

В Прил. 1 приведены значения $k+1$ коэффициента $a_n, n=\overline{0,k}$. Коэффициент $a_0=1$ всегда по определению. Для определения структуры цифрового автомата, изображенного на рис. 2, необходимо учитывать коэффициенты $a_n, n=\overline{1,k}$.

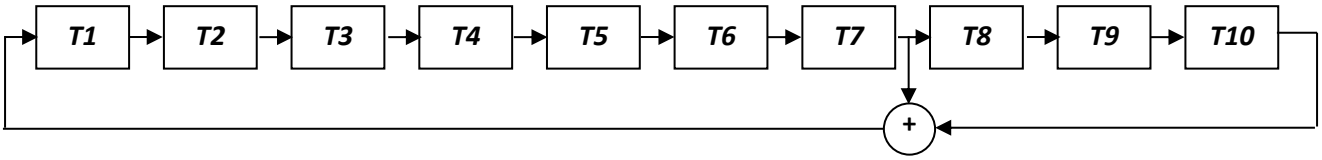


Рис. 3

Для примера на рис. 3 изображена схема цифрового автомата формирования М-последовательности *с* $k=10$ и $N=2^{10}$—1=1023. В качестве характеристического многочлена взят многочлен с коэффициентами 10000001001 (первый в столбце с $k=10$ Прил. 1). В соответствии с коэффициентами многочлена на сумматор по mod 2 поступают символы с выходов 7-го и 10-го триггеров.

Длительность М-последовательности $T=N\tau_0$, где $N=p^k$—1, τ_0 - длительность одиночного импульса (символа). Для двоичных М-последовательностей $N=2^k$—1. Если тактовая частота в сдвигающем регистре $f_T=1/\tau_0$, то $T=\left(2^k-1\right)/f_T$. В табл. 4 приведены длительности периода М-последовательности для $k=7...$ 89 с тактовой частотой f_T=1 МГц.

Таблица 4

Регистр длины *k*	Длина последовательности	Длительность периода последовательности
7	127	$1{,}27*10^{-4}$ с
8	255	$2{,}55*10^{-4}$ с
9	511	$5{,}11*10^{-4}$ с
10	1 023	$1{,}023*10^{-3}$ с
11	2 047	$2{,}047*10^{-}3$ с
12	4 095	$4{,}095*10^{-3}$ с
13	8 191	$8{,}191*10^{-3}$ с
17	131 071	$1{,}31*10^{-1}$ с
19	524 287	$5{,}24*10^{-1}$ с
23	8 388 607	8,388 с
27	134 217 727	13,421 с
31	2 147 483 647	35,8 мин
43	879 609 302 207	101,7 дня
61	2 305 843 009 213 693 951	$7{,}3*10^4$ лет
89	618 970 019 642 690 137 449 562 111	$1{,}95*10^6$ лет

ЗАДАНИЕ НА ВЫПОЛНЕНИЕ ПРАКТИЧЕСКОЙ РАБОТЫ

1. Изучить структурную схему генератора М-последовательности и уяснить принцип ее работы.

2. Исследовать процесс формирования М-последовательности регистром сдвига.

3. Составить рекуррентную формулу исследуемой последовательности.

4. Исследовать свойства полученной последовательности.

ПОРЯДОК ВЫПОЛНЕНИЯ ПРАКТИЧЕСКОЙ РАБОТЫ

1. Исследование процесса формирования М-последовательности регистром сдвига.

Для этого:

- получить у преподавателя справочный лист;
- используя теоретический материал методического пособия, построить схему генератора М-последовательности, соответствующую исходным данным, указанным в справочном листе;
- изобразить в отчете полученную М-последовательность. Длительность τ_0 принять равной 1 клетке;
- имитируя подачу на вход схемы тактовых импульсов, изобразить последовательности, снимаемые с выходов всех триггеров генератора.

2. Составить рекуррентную формулу исследуемой последовательности.

3. Исследование свойств полученной последовательности:

- исследовать свойство цикличности;
- исследовать свойство уравновешенности;
- исследовать свойство статистической независимости, для чего:

1. вычислить взаимокорреляционные функции исследуемой последовательности с ее циклическими сдвигами (первый сдвиг равен нулю);

2. построить зависимость функции взаимной корреляции от величины циклического сдвига.

** Расчет производить по формуле* $R(\mu) = \frac{1}{N}\sum_{n=1}^{N} a_n a_{n-\mu}$,

где a_n, $a_{n-\mu}$ *- символы М-последовательностей сдвинутых относительно друг друга. Выражение под знаком суммы будет равно количеству несовпадений символов минус количество совпадений.*

- исследовать свойство 5 М-последовательности.

СОДЕРЖАНИЕ ОТЧЕТА

Отчет должен содержать:

1. Схему генератора исследуемой М-последовательности;
2. Построенные М-последовательности;
3. Рекуррентную формулу М-последовательности;
4. График функции взаимной корреляции М-последовательности с ее циклическим сдвигом от величины сдвига;
5. Рисунок 6 приемного устройства ШПС.
5. Выводы о подтверждении свойств М-последовательности.

КОНТРОЛЬНЫЕ ВОПРОСЫ

1. Что называется базой сигнала? Как связана база сигнала с его информативностью?
2. Преимущества ШПС по отношению к узкополосным сигналам
3. Что называется периодом М-последовательности?
4. Свойства М-последовательностей.
5. Длительность М-последовательности.
6. Что такое рекуррентный неприводимый полином?
7. Принцип формирования генератора М-последовательности.
8. В чем отличие схемы РПрУ для узкополосных сигналов от схемы РПрУ для приема ШПС?
9. От чего зависит количество генерируемых М-последовательностей?
10. Для чего необходимы устройства синхронизации в РПрУ ШПС?

Приложение 1

Характеристические многочлены, порождающие М-последовательности.

$k=3$
1011
1101

$k=4$
10011
11001

$k=5$
100101
101001
101111
110111
111011
111101

$k=6$
1000011
1010111
1011011
1100001
1100111
1101101
1110011

$k=7$
10000011
10001001
10001111
10010001
10011101
10100111
10101011
10111001
10111111
11000001
11001011
11010011
11010101
11100101
11101111
11110001
11110111
11111101

$k=8$
100011101
100101011
100101101
101001101
101011111
101100011
101100101
101101001
101110001
110000111
110001101
110101001
111000011
111001111
111100111
111110101

$k=9$
1000010001
1000011011
1000100001
1000101101
1000110011
1001011001
1001011111
1001101001
1001101111
1001110111
1001111101
1010000111
1010010101
1010100011
1010100101
1010101111
1010110111
1010111101
1011001111
1011010001
1011011011
1011110101
1011111001
1100010011
1100010101
1100011111
1100100011
1100110001
1100111011
1101001111
1101011011
1101100001
1101101011
1101101101
1101110011
1101111111
1110000101
1110001111
1110110101
1110111001
1111000111
1111001011
1111001101
1111010101
1111100011
1111101001
1111111011

$k=10$
10000001001
10000011011
10000100111
10000101101
10001100101
10001101111
10010000001
10010001011
10011000101
10011010111
10011100111
10011110011
10011111111
10100001101
10100011001
10100100011
10100110001
10100111101
10101000011
10101010111
10101101011
10110000101
10110001111
10110010111
10110100001
10111000111
10111100101
10111110111
10111111011
11000010011
11000010101
11000100101
11000110111
11001000011
11001001111
11001011011
11001111001
11001111111
11010001001
11010110101
11011000001
11011010011
11011011111
11011111101
11100010111
11100011101
11100100001
11100111001
11101000111
11101001101
11101010101
11101010110
11101100011
11101111101
11110001101
11110010011
11110110001
11111011011
11111110011
11111111001

$k=11$
100000000101
100000010111
100000101011
100000101101
100001000111
100001100011
100001110001
100001111011
100010001101
100010010101
100010011111
100010101001
100010110001
100011001111
100011010001
100011100001
100011100111
100011101011
100011110101
100100001101
100100010011
100100100101
100100101001
100100111011
100100111101
100101000101
100101010001
100101011011
100101110011
100101110101
100101111111
100110000011
100110001111
100110101011
100110101101
100110111001
100111000111
100111011001
100111100101
100111110111
101000000001
101000000111

$k=11$
101000010011
101000010101
101000101001
101001001001
101001100001
101001101101
101001111001
101001111111
101010000101
101010010001
101010011101
101010100111
101010101011
101010110011
101010110101
101011010101
101011011111
101011101001
101011101111
101011110001
101011111011
101100000011
101100001001
101100010001
101100110011
101100111111
101101000001
101101001011
101101011001
101101011111
101101100101
101101101111

101101111101
101110000111
101110001011
101110010011
101110010101
101110101111
101110110111
101110111101
101111001001
101111011011
101111011101
101111100111
101111101101
110000001011
110000001101
110000011001
110000011111
110001010111
110001100001
110001101011
110001110011
110010000101
110010001001
110010010111
110010011011
110010011101
110010110011
110010111111
110011000111
110011001101
110011010011
110011010101
110011100011
110011101001

110011110111
110100000011
110100001111
110100011101
110100100111
110100101101
110101000001
110101000111
110101010101
110101011001
110101100011
110101101111
110101110001
110110010011
110110011111
110110101001
110110111101
110111001001
110111010111
110111011011
110111100001
110111100111
110111110101
111000000101
111000011101
111000100001
111000100111
111000101011
111000110011
111000111001
111001000111
111001001011
111001010101
111001011111

111001110001
111001111011
111001111101
111010000001
111010010011
111010011111
111010100011
111010111011
111011001111
111011011101
111011110011
111011111001
111100001011
111100011001
111100110001
111100110111
111101011101
111101101011
111101101101
111101110101
111110000011
111110010001
111110010111
111110011011
111110100111
111110101101
111110110101
111111001101
111111010011
111111100101
111111101001

ПРАКТИЧЕСКОЕ ЗАНЯТИЕ 4

СРЕДСТВА ВЫЯВЛЕНИЯ КАНАЛОВ УТЕЧКИ ИНФОРМАЦИИ

• Информационные ресурсы, содержащие сведения, связанные с государственной тайной и конфиденциальной информацией.

• Средства и информационные системы (средства вычислительной техники, сети и системы), программные средства (операционные системы, системы управления базами данных, прикладное программное обеспечение), автоматизированные системы управления, системы связи и передачи данных, технические средства приёма, передачи и обработки информации ограниченного доступа (звукозапись, звукоусиление, звуковоспроизведение, переговорные и телевизионные устройства, средства изготовления, тиражирование документов и другие технические средства обработки графической, смысловой и буквенно-цифровой информации), т.е. системы и средства, непосредственно обрабатывающие конфиденциальную информацию и информацию, относящуюся к категории государственной тайны. Эти средства и системы часто называют техническими средствами приёма, обработки и хранения информации (ТСПИ).

• Технические средства и системы, не входящие в состав ТСПИ, но территориально находящиеся в помещениях обработки секретной и конфиденциальной информации. Такие технические средства и системы называются вспомогательными техническими средствами и системами (ВТСС). К ним относятся: технические средства телефонной, громкоговорящей связи, системы пожарной и охранной сигнализации, радиотрансляции, часофикации, средства и системы передачи данных в системе радиосвязи, контрольно-измерительная аппаратура, электробытовые приборы и т.д., а также сами помещения, предназначенные для обработки информации ограниченного распространения.

• ТСПИ можно рассматривать как систему, включающую стационарное оборудование, периферийные устройства, соединительные линии, распределительные и коммуникационные устройства, системы электропитания, системы заземления.

Технические средства, предназначенные для обработки конфиденциальной информации, включая помещения, в которых они размещаются, представляют *объект ТСПИ.*

1.2. Технические каналы утечки информации. Структура, классификация и основные характеристики

Наибольший интерес с точки зрения образования каналов утечки информации представляют ТСПИ и ВТСС, имеющие выход за пределы *контролируемой зоны* (КЗ), т.е. зоны с пропускной системой. Кроме соединительных линий ТСПИ и ВТСС за пределы контролируемой зоны могут иметь выход проходящие через помещения посторонние проводники, не связанные с ТСПИ и ВТСС (рис. 1.1).

Зона с возможностью перехвата разведывательным оборудованием побочных электромагнитных излучений, содержащих конфиденциальную информацию, называется *опасной зоной*. Пространство вокруг ТСПИ, в котором на случайных антеннах наводится информационный сигнал выше допустимого уровня, называется *опасной зоной* 1.

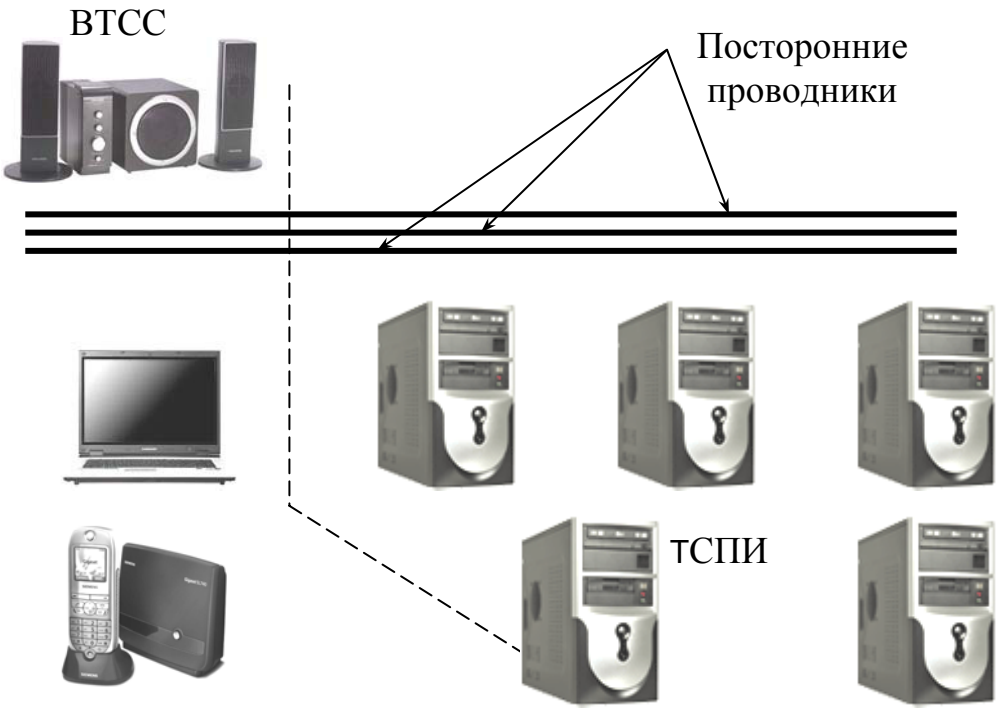


Рис. 1.1. Источники образования возможных каналов утечки информации

Случайными антеннами могут быть цепи ВТСС или посторонние проводники, воспринимающие побочные электромагнитные излучения от средств ТСПИ. Случайные антенны бывают сосредоточенными и распределёнными. Сосредоточенная случайная антенна представляет собой техническое средство с сосредоточенными параметрами (телефонный аппарат, громкоговоритель радиотрансляционной сети и т.д.). Распределённые случайные антенны образуют проводники с распределёнными параметрами: кабели, соединительные провода, металлические трубы.

Информационные сигналы могут быть электрическими, электромагнитными, акустическими и т.д. Они имеют в большинстве случаев колебательный характер, а информационными параметрами являются амплитуда, фаза, частота, длительность.

Под техническим каналом утечки информации (ТКУИ) понимают совокупность объекта разведки, технического средства разведки (ТСР) и физической среды, в которой распространяется информационный сигнал (рис. 1.2). В сущности, под ТКУИ понимают способ получения с помощью ТСР разведывательной информации об объекте [1].

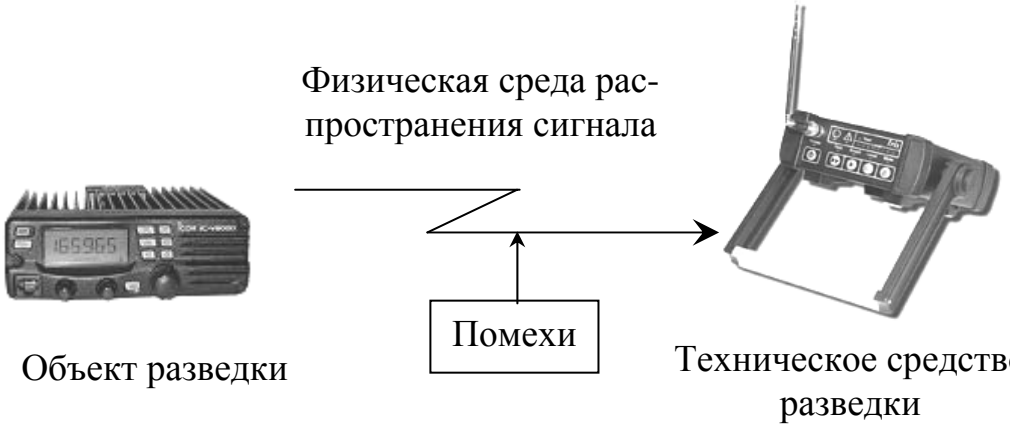


Рис. 1.2. Технический канал утечки информации (ТКУИ)

В зависимости от физической природы сигналы распространяются в определенных физических средах. Средой распространения могут быть газовые (воздушные), жидкостные (водные) и твердые среды. К таким средам относятся воздушное пространство, конструкции зданий, соединительные линии и токопроводящие элементы, грунт и т.п.

Противодействие промышленному и экономическому шпионажу является непрерывным и адекватным новым типам угроз процессом развития методов, средств и способов защиты информации.

Классификация каналов утечки информации представлена на рис. 1.3.

Особенности технических каналов утечки информации определяются физической природой информационных сигналов и характеристиками среды распространения сигналов утекаемой информации. Ниже приведены некоторые особенности технических каналов утечки информации.

Технические каналы утечки информации, обрабатываемой ТСПИ

1. Электромагнитные:

- электромагнитные излучения элементов ТСПИ;
- электромагнитные излучения на частотах работы ВЧ-генераторов ТСПИ;
- излучения на частотах самовозбуждения усилителей низкой частоты.

2. Электрические:

- наводки электромагнитных излучений элементов ТСПИ на посторонние проводники;
- просачивание информационных сигналов в линии электропитания;
- просачивание информационных сигналов в цепи заземления;
- съем информации с использованием закладных устройств.

3. Параметрические:

- перехват информации путем «высокочастотного облучения» ТСПИ.

4. Вибрационные:

- соответствие между распечатываемым символом и его акустическим образом.

Технические каналы утечки информации при передаче ее по каналам связи

1. Электромагнитные каналы:

• электромагнитные излучения передатчиков связи, модулированные информационным сигналом (прослушивание радиотелефонов, сотовых телефонов, радиорелейных линий связи).

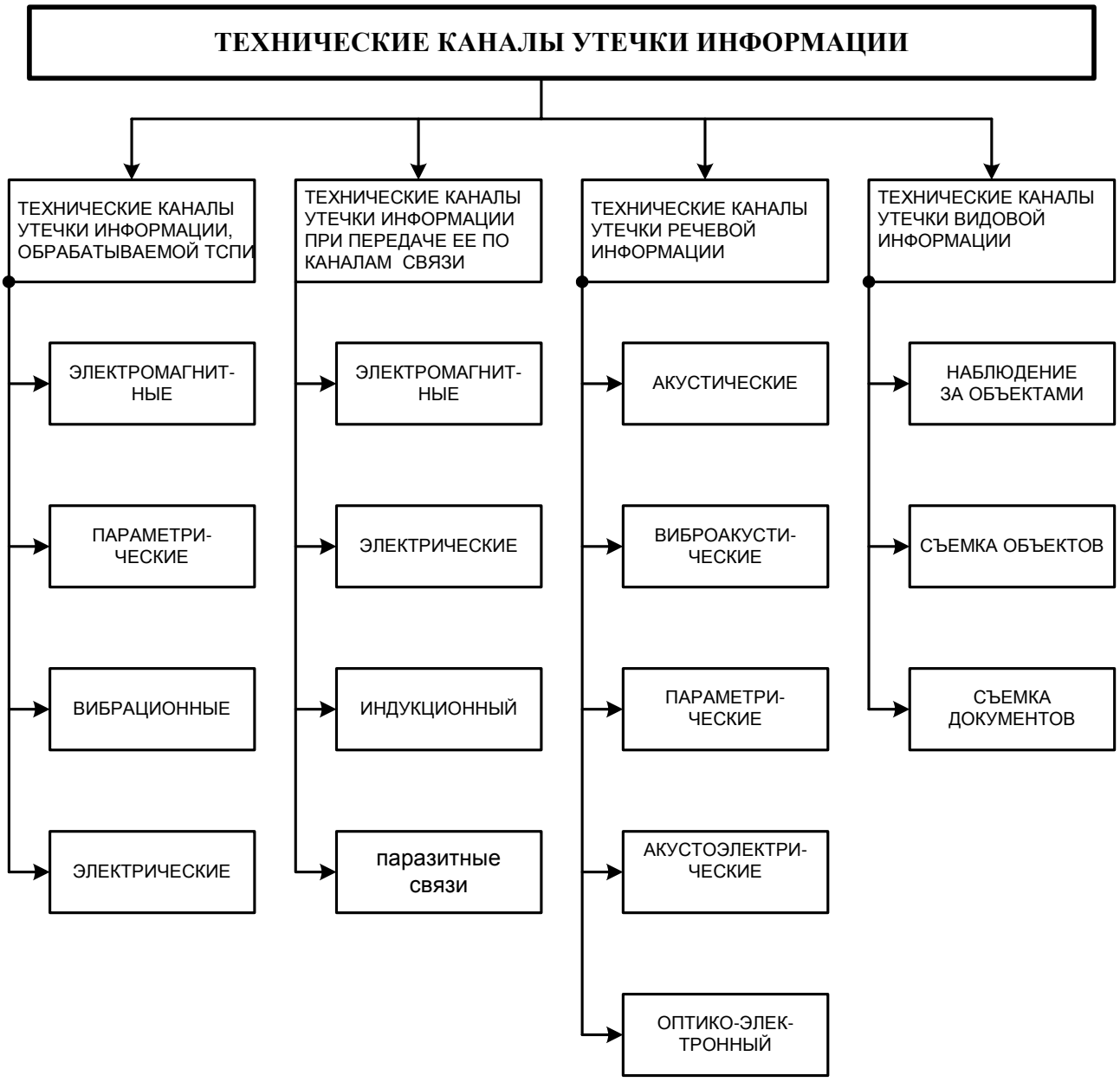


Рис. 1.3. Технические каналы утечки информации

2. Электрические каналы:

• подключение к линиям связи.

3. Индукционный канал:

• эффект возникновения вокруг высокочастотного кабеля электромагнитного поля при прохождении информационных сигналов.

4. Паразитные связи:

• паразитные емкостные, индуктивные и резистивные связи и наводки близко расположенных друг от друга линий передачи информации.

Технические каналы утечки речевой информации

1. Акустические каналы:

• среда распространения – воздух.

2. Виброакустические каналы:

• среда распространения – ограждающие строительные конструкции.

3. Параметрические каналы:

• результат воздействия акустического поля на элементы схем, что приводит к модуляции высокочастотного сигнала информационным.

4. Акустоэлектрические каналы:

• преобразование акустических сигналов в электрические.

5. Оптико-электронный (лазерный) канал:

• облучение лазерным лучом вибрирующих поверхностей.

Технические каналы утечки видовой информации

1. Наблюдение за объектами.

Для наблюдения днем применяются оптические приборы и телевизионные камеры. Для наблюдения ночью – приборы ночного видения, тепловизоры, телевизионные камеры.

2. Съемка объектов.

Для съемки объектов используются телевизионные и фотографические средства. Для съемки объектов днем с близкого расстояния применяются портативные камуфлированные фотоаппараты и телекамеры, совмещенные с устройствами видеозаписи.

3. Съемка документов.

Съемка документов осуществляется с использованием портативных фотоаппаратов

1.2.1. Технические каналы утечки информации, обрабатываемой ТСПИ

Электромагнитные каналы утечки информации

Основным каналом утечки информации при ее обработке ТСПИ является электромагнитный канал, обусловленный побочными информативными электромагнитными излучениями основных технических средств обработки информации. К *электромагнитным* относятся каналы утечки информации, возникающие за счет различного вида побочных электромагнитных излучений ТСПИ. Побочные электромагнитные излучения (ПЭМИ) – это паразитные электромагнитные излучения радиодиапазона,

создаваемые в окружающем пространстве устройствами, специальным образом для этого не предназначенными.

Рассмотрим некоторые особенности и свойства электромагнитных каналов.

1.2.1.1. Физическая природа побочных электромагнитных излучений. Основные уравнения электромагнитного поля

Электромагнитное поле представляет собой особый вид материи. Оно, как и вещество, обладает не только энергией, но также массой, количеством движения и моментом количества движения. Поле может превращаться в вещество, как и вещество – в поле. Электромагнитное поле воздействует с определенной силой на заряженные частицы.

Электромагнитное поле определяется во всех точках двумя векторными величинами – электрическим полем и магнитным полем. Электрическое поле характеризуется воздействием на электрически заряженную частицу с силой, пропорциональной заряду частицы и не зависящей от ее скорости. Магнитное поле воздействует на движущуюся частицу с силой, пропорциональной заряду частицы и ее скорости.

Для расчета электромагнитного поля наиболее пригодны уравнения электродинамики в интегральной и дифференциальной формах [35].

Электромагнитное поле характеризуется четырьмя векторными величинами: $\vec{E}$ – напряженность электрического поля (В/м); $\vec{D}$ – электрическая индукция (вектор электрического смещения) ((Кл/м^2); $\vec{H}$ – напряженность магнитного поля (А/м); $\vec{B}$ – магнитная индукция (Тл).

Определение поля в некоторой области пространства требует указания этих векторов в любой ее точке. В общем случае взаимосвязь векторов электромагнитного поля определяется свойствами среды:

$$\vec{D} = \varepsilon \vec{E}; \tag{1.1}$$

$$\vec{B} = \mu \vec{H}, \tag{1.2}$$

где $\varepsilon = \varepsilon_r \varepsilon_0$ – диэлектрическая проницаемость среды; $\varepsilon_0 = 8{,}855 \cdot 10^{-12}$ – диэлектрическая проницаемость вакуума (Ф/м); ε_r – относительная диэлектрическая проницаемость среды, в которой находятся заряды; $\mu = \mu_r \mu_0$ – абсолютная магнитная проницаемость среды; $\mu_0 = 4\pi \cdot 10^{-7}$ – магнитная проницаемость вакуума (Гн/м); μ_r – относительная магнитная проницаемость среды.

Безразмерные величины ε_r и μ_r для воздушной среды близки к единице. Например, для воздушной среды при температуре 0° $\varepsilon_r = 1{,}0006$.

Основными уравнениями электромагнитного поля являются уравнения Максвелла. Первое уравнение Максвелла соответствует вихрям магнитного поля и относится к одному из основных уравнений электродинамики:

$$\mathrm{rot}\,\vec{H} = \vec{\delta} + \frac{\partial \vec{D}}{\partial t}. \qquad (1.3)$$

Физический смысл этого уравнения можно толковать следующим образом: магнитное поле возбуждается совместным действием тока проводимости с плотностью $\vec{\delta}$ и изменением во времени электрического поля (вектора электрического смещения $\vec{D}$). Величина $\frac{\partial \vec{D}}{\partial t}$ называется плотностью тока смещения. Вектор $\vec{\delta}$ указывает направление движения зарядов и по абсолютному значению равен пределу

$$\vec{\delta} = \lim_{\Delta S \to 0} \frac{\Delta I}{\Delta S}, \qquad (1.4)$$

где ΔI – ток через площадку ΔS, перпендикулярную $\vec{\delta}$. Плотность тока проводимости $\vec{\delta} = \gamma \vec{E}$, где γ – удельная проводимость.

Сумму $\vec{\delta} + \frac{\partial \vec{D}}{\partial t}$ называют плотностью полного тока.

Второе уравнение Максвелла выражает скорость изменения магнитной индукции $\vec{B}$ через пространственную производную (rot) напряженности электрического поля $\vec{E}$:

$$\mathrm{rot}\,\vec{E} = -\frac{\partial \vec{B}}{\partial t}. \qquad \textbf{(1.5)}$$

Физический смысл второго уравнения Максвелла состоит в том, что электрическое поле может возбуждаться не только электрическими зарядами, но и изменениями во времени магнитного поля (вектора магнитной индукции $\vec{B}$).

Если изобразить в пространстве произвольную поверхность S с контуром L (рис. 1.4), то можно определить поток вектора $\mathrm{rot}\,\vec{E}$ через эту поверхность.

Согласно (1.5) имеем:

$$\int_S \mathrm{rot}\,\vec{E} d\vec{S} = -\int_S \frac{\partial \vec{B}}{\partial t} d\vec{S}. \qquad \textbf{(1.6)}$$

Векторный символ $d\vec{S}$ обозначает произведение элемента поверхности dS на единичный вектор нормали к ней $\vec{n}_0$.

Применяя теорему Стокса ($\int_S \mathrm{rot}\,\vec{v} dV = \oint_L \vec{v} d\vec{l}$, где $\vec{v}$ – любой вектор) и вынося оператор временной производной за знак интеграла заменим поток вихря $rot\,\vec{E}$ циркуляцией вектора $\vec{E}$ по контуру, охватывающему поток:

$$\oint_L \vec{E} d\vec{l} = -\frac{\partial}{\partial t} \int_S \vec{B} d\vec{S}, \qquad \textbf{(1.7)}$$

где $d\vec{l}$ – произведение элемента линии dl на касательный к ней единичный вектор $\vec{\tau}_0$.

Уравнение (1.7) представляет собой второе уравнение Максвелла в интегральной форме.

Если поверхность S (рис. 1.5) опирается на проводящий контур L (например, проволочный), то выражение (1.7) можно записать как

$$e = -\frac{\partial \Phi}{\partial t}, \qquad (1.8)$$

где циркуляция вектора $\vec{E}$ в этом случае есть не что иное, как ЭДС $e = \oint_L \vec{E} d\vec{l}$, наводимая в контуре изменяющимся потоком вектора магнитной индукции, а $-\frac{\partial}{\partial t} \int_S \vec{B} d\vec{S} = -\frac{d\Phi}{dt}$, где Φ – магнитный поток. В итоге для рассматриваемого случая имеем хорошо известный закон электромагнитной индукции: $e = -\frac{d\Phi}{dt}$.

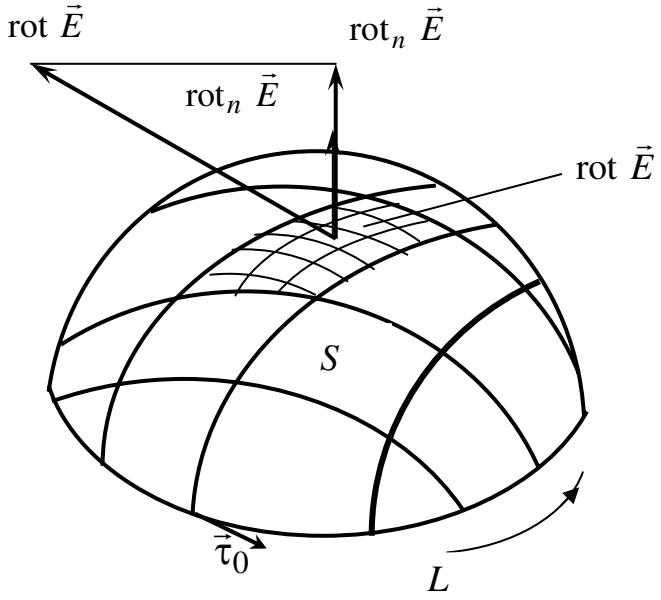


Рис. 1.4

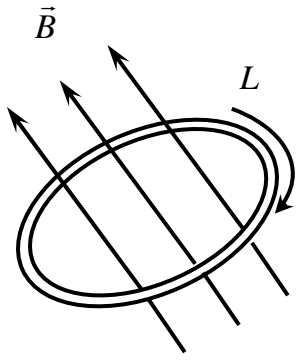


Рис. 1.5

Второе уравнение Максвелла можно рассматривать как обобщенный закон электромагнитной индукции.

Интегральная форма первого уравнения Максвелла может быть получена интегрированием обеих частей уравнения (1.3) по произвольной поверхности S с контуром L и применением теоремы Стокса:

$$\oint_L \vec{H} d\vec{l} = \frac{\partial}{\partial t} \int_S \vec{D} d\vec{S} + \int_S \vec{\delta} d\vec{S}. \qquad (1.9)$$

Интеграл $\int\limits_S \vec{\delta} d\vec{S} = I$ – поток вектора $\vec{\delta}$ через поверхность S – является током проводимости, пересекающим эту поверхность, а составляющая $\frac{\partial}{\partial t}\int\limits_S \vec{D} d\vec{S} = I_{\text{см}}$ – ток смещения. Сумма $I + I_{\text{см}}$ называется полным током.

К основным уравнениям Максвелла относят также следующие два уравнения в дифференциальной форме:

$$\operatorname{div}\vec{D} = \rho; \tag{1.10}$$

$$\operatorname{div}\vec{B} = 0. \tag{1.11}$$

Согласно первому уравнению расходимость электрической индукции равна объемной плотности заряда ρ – величине, определяемой предельным соотношением:

$$\rho = \lim_{\Delta V \to 0} \frac{\Delta q}{\Delta V}, \tag{1.12}$$

где Δq – заряд, содержащийся в элементарном объеме ΔV.

Интегрированием обеих частей уравнения (1.10) по некоторому объему V и применением к левой части формулы Остроградского-Гаусса получим

$$\oint\limits_S \vec{D} d\vec{S} = q. \tag{1.13}$$

Здесь S – поверхность, ограничивающая объем V, а $q = \int\limits_V \rho dV$ – полный заряд в этом объеме.

Равенство (1.13) является интегральной формой уравнения Максвелла (1.10) и является формулировкой теоремы Гаусса: поток электрической индукции через замкнутую поверхность равен заключенному внутри ее заряду.

Интегральную форму уравнения (1.11) получают интегрированием $\operatorname{div}\vec{B}$ по объему V и применением формулы Остроградского-Гаусса:

$$\oint\limits_S \vec{B} d\vec{S} = 0. \tag{1.14}$$

В заключение приведем систему уравнений Максвелла в дифференциальной и интегральной формах.

Интегральная форма:

$$\begin{gathered}
\oint\limits_L \vec{H}\, d\vec{l} = \frac{d}{dt}\int\limits_S \vec{D} d\vec{S} + \int\limits_S \vec{\delta} d\vec{S}, \\
\oint\limits_L \vec{E} d\vec{l} = -\frac{d}{dt}\int\limits_S \vec{B} d\vec{S}, \quad \oint\limits_S \vec{D}\, d\vec{S} = q, \\
\oint\limits_S \vec{B} d\vec{S} = 0.
\end{gathered} \tag{1.15}$$

Дифференциальная форма:

$$\begin{aligned}
&\operatorname{rot}\vec{H}=\frac{\partial\vec{D}}{\partial t}+\vec{\delta},\\
&\operatorname{rot}\vec{E}=-\frac{\partial\vec{B}}{\partial t},\\
&\operatorname{div}\vec{D}=\rho,\\
&\operatorname{div}\vec{B}=0,\\
&\vec{B}=\mu\vec{H},\\
&\vec{D}=\varepsilon\vec{E},\\
&\vec{\delta}=\gamma\vec{E}.
\end{aligned} \qquad (1.16)$$

Преобразованием (исключением $\vec{D}$ и $\vec{B}$) систему уравнений (1.16) можно привести к форме, в которой переменными будут только напряженности электрического и магнитного полей:

$$\operatorname{rot}\vec{H}=\varepsilon_r\varepsilon_0\frac{\partial\vec{E}}{\partial t}+\vec{\delta},\ \operatorname{rot}\vec{E}=-\mu_r\mu_0\frac{\partial\vec{H}}{\partial t},\ \operatorname{div}\vec{E}=\frac{\rho}{\varepsilon_r\varepsilon_0}\ \ (\varepsilon_r=\text{const}),$$
$$\operatorname{div}\vec{H}=0\ \ (\mu_r=\text{const}),\ \vec{\delta}=\gamma\vec{E}\ \ (\text{при}\ \ \vec{E}_{\text{стор}}=0). \qquad (1.17)$$

Системы уравнений (1.15)…(1.17) являются исходными при изучении электромагнитного поля.

Для радиотехники переменное электромагнитное поле представляет основной интерес. Для изучения установившихся электромагнитных процессов, которые характеризуются гармоническими во времени колебаниями, всякую характеризующую поле скалярную величину можно представить как $\psi=\psi_m\cos(\omega t+\varphi_\psi)$. Тогда всякий вектор поля $\vec{V}$ разлагается на компоненты, изменяющиеся по аналогичному закону:

$$\vec{V}=\vec{a}_1V_{1m}\cos(\omega t+\varphi_1)+\vec{a}_2V_{2m}\cos(\omega t+\varphi_2)+\vec{a}_3V_{3m}\cos(\omega t+\varphi_3), \qquad (1.18)$$

где $\vec{a}_1, \vec{a}_2, \vec{a}_3$ – орты некоторой системы координат q_1, q_2, q_3.

Величина $\omega=2\pi f$ называется круговой частотой гармонических колебаний; ψ_m и V_{im} – амплитуды, φ_ψ и φ_i – начальные фазы.

Анализ гармонических процессов значительно упрощается применением метода комплексных амплитуд, когда изображающий вектор рассматривается на комплексной плоскости. По формуле Эйлера

$$e^{j(\omega t+\varphi)}=\cos(\omega t+\varphi)+j\sin(\omega t+\varphi)$$

видно, что скаляр ψ (см. выше) и вектор $\vec{V}$ можно выразить как вещественные части величин

$$\dot{\psi} = \psi_m e^{j(\omega t+\varphi_\psi)};$$
$$\dot{\vec{V}} = \vec{a}_1 V_{1m} e^{j(\omega t+\varphi_1)} + \vec{a}_2 V_{2m} e^{j(\omega t+\varphi_2)} + \vec{a}_3 V_{3m} e^{j(\omega t+\varphi_3)}, \quad (1.19)$$

которые называются их комплексами. В (1.19) $\vec{a}_1, \vec{a}_2, \vec{a}_3$ – орты некоторой системы координат. Таким образом $\vec{\psi} = \mathrm{Re}\,\dot{\psi}$, $\vec{V} = \mathrm{Re}\,\dot{V}$.

Выделим в комплексе $\dot{\vec{V}}$ множитель

$$\dot{\vec{V}} = \vec{a}_1 V_{1m} e^{j\varphi_1} + \vec{a}_2 V_{2m} e^{j\varphi_2} + \vec{a}_3 V_{3m} e^{j\varphi_3}, \quad (1.20)$$

который называют комплексной амплитудой. Через комплексную амплитуду можно выразить комплекс $\dot{\vec{V}}$ как $\dot{\vec{V}} = \dot{\vec{V}}_m e^{j\omega t}$. Дифференцирование комплекса по времени соответствует его умножение на $j\omega$.

Если комплекс $\dot{\vec{V}}$ удовлетворяет некоторому линейному дифференциальному уравнению, то данному уравнению удовлетворяют его вещественная и мнимая части.

С учетом приведенных выше соотношений уравнения Максвелла (1.17) в комплексных значениях принимают форму:

$$\begin{aligned}
&\mathrm{rot}\,\dot{\vec{H}}_m = \dot{\vec{\delta}}_m + j\omega\varepsilon_r\varepsilon_0\dot{\vec{E}}_m;\\
&\mathrm{rot}\,\dot{\vec{E}}_m = -j\omega\mu_r\mu_0\dot{\vec{H}}_m;\\
&\mathrm{div}\,\dot{\vec{H}}_m = 0;\\
&\mathrm{div}\,\dot{\vec{E}}_m = \frac{\dot{\rho}_m}{\varepsilon_r\varepsilon_0};\\
&\dot{\vec{\delta}}_m = \gamma\dot{\vec{E}}_m.
\end{aligned} \quad (1.21)$$

Уравнения (1.21) могут быть упрощены, если учесть, что

$$\varepsilon_r = 1{,}0006.$$

Рассмотрим некоторую область V (рис. 1.6), в которой распределен заряд ($\rho \neq 0$) и присутствует ток ($\vec{\delta} \neq 0$). В некоторой точке M существует электрическое поле, потенциал которого φ есть решение уравнения Пуассона

$$\frac{\partial^2\varphi}{\partial x^2} + \frac{\partial^2\varphi}{\partial y^2} + \frac{\partial^2\varphi}{\partial z^2} = -\frac{\rho}{\varepsilon} \quad (1.22)$$

и выражается формулой

$$\varphi = \frac{1}{4\pi\varepsilon}\int_V \frac{1}{r}\rho\,dV, \quad (1.23)$$

а также магнитное поле, характеризуемое векторным потенциалом $\vec{A}$, определяемым из решения уравнения $\nabla^2\vec{A} = -\mu\vec{\delta}$ как

$$\vec{A} = \frac{\mu}{4\pi}\int_V \frac{1}{r}\vec{\delta}\,dV,$$

где $\nabla = \vec{x}_0\frac{\partial}{\partial x} + \vec{y}_0\frac{\partial}{\partial y} + \vec{z}_0\frac{\partial}{\partial z}$ – оператор Гамильтона.

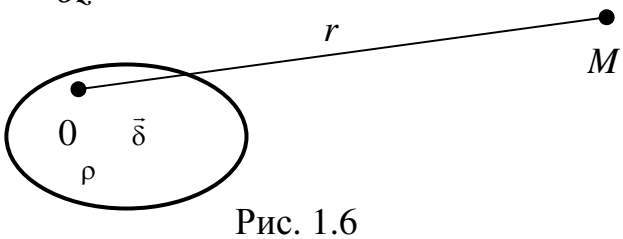


Рис. 1.6

Для решения системы уравнений (1.21) необходимо определить для электромагнитного поля электрический φ и магнитный A запаздывающие потенциалы:

$$\begin{aligned} \varphi(t) &= \frac{1}{4\pi\varepsilon}\int_V \frac{1}{r}\rho(t-\frac{r}{v})dV, \\ \vec{A}(t) &= \frac{\mu}{4\pi}\int_V \frac{1}{r}\vec{\delta}(t-\frac{r}{v})dV, \end{aligned} \tag{1.24}$$

где r – расстояние до точки наблюдения M ; v – фазовая скорость бегущей волны, связанная с постоянной распространения волны в неограниченном пространстве k соотношением $k = \frac{\omega}{v}$. Величины ρ и $\vec{\delta}$ связаны между собой уравнением

$$div\vec{\delta} = -\frac{d\rho}{dt}. \tag{1.25}$$

В комплексной форме выражения запаздывающих потенциалов принимают вид:

$$\begin{aligned} \dot{\varphi}_m &= \frac{1}{4\pi\varepsilon}\int_V \dot{\rho}\frac{e^{-jkr}}{r}dV, \\ \dot{\vec{A}} &= \frac{\mu}{4\pi}\int_V \dot{\vec{\delta}}\frac{e^{-jkr}}{r}dV. \end{aligned} \tag{1.26}$$

Если рассматривать поле, создаваемое одним лишь колеблющимся зарядом $q = \rho_m \Delta V\cos\omega t = q_m\cos\omega t$, расположенным в пространстве ΔV, то согласно (1.26) комплексная амплитуда потенциала этого поля будет

$$\dot{\varphi}_m = \frac{\dot{q}_m}{4\pi\varepsilon}\cdot\frac{e^{-jkr}}{r}, \tag{1.27}$$

а сам потенциал равен:

$$\varphi = \frac{q_m}{4\pi\varepsilon r}\cos(\omega t - kr). \tag{1.28}$$

В этом случае поле имеет форму сферической волны, расходящейся из точки, в которой расположен заряд, со скоростью *v*.

С учетом параметров *A* и φ напряженности магнитного и электрического полей можно выразить как

$$\vec{H} = \frac{1}{\mu\mu_0}\operatorname{rot}\vec{A};$$
$$\vec{E} = -\frac{\partial\vec{A}}{\partial t} - \operatorname{grad}\varphi, \tag{1.29}$$

где

$$\operatorname{grad}\varphi = \begin{cases} \dfrac{d\varphi}{dx} \\ \dfrac{d\varphi}{dy} \\ \dfrac{d\varphi}{dz} \end{cases}$$

1.2.1.2. Элементарный электрический излучатель

Диполь, момент которого изменяется во времени, называют элементарным излучателем. Различают электрический и магнитный излучатели: электрический и магнитный диполи. Диполь, момент которого изменяется по синусоидальному закону, называют гармоническим.

Электрический излучатель соответствует элементу электрического тока. В этом легко убедиться, если рассмотреть производную по времени от момента электрического диполя. Так как электрический момент (векторная величина) $\vec{p} = q\vec{l}$, то $\frac{\partial\vec{p}}{\partial t} = \frac{\partial q}{\partial t}\vec{l} = I\vec{l}$, при этом положительное направление тока *I* совпадает с $\vec{p}$.

По аналогии производная по времени от момента замкнутого витка с током $\vec{m} = -\mu I\vec{S}$ магнитного диполя соответствует элементу магнитного тока $\frac{\partial\vec{m}}{\partial t} = -\mu\vec{S}\frac{\partial I}{\partial t}$.

Рассмотрим элементарный электрический излучатель. Для этого представим отрезок проводника *l*, ориентированный вдоль координатной оси *z* и по которому течет ток $I = I_m\cos\omega t$ (рис. 1.7).

В [35] показано, что при условии постоянства амплитуды тока вдоль всего участка можно условно полагать сосредоточение равных по

абсолютной величине и противоположных по знаку колеблющихся зарядов (рис. 1.8) с комплексными амплитудами

$$\dot{q}_m = \pm \frac{jI_m}{\omega}. \tag{1.30}$$

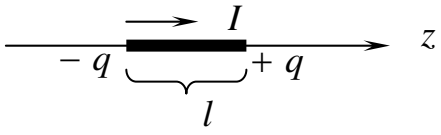


Рис. 1.7

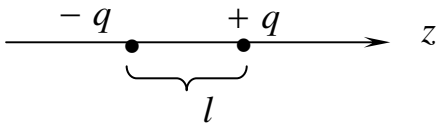


Рис. 1.8

Это значит, что рассматриваемый отрезок с током можно представить как диполь, момент которого $\dot{\vec{p}}_m = \vec{z}_0 lq$ совершает гармонические колебания с частотой ω и имеет комплексную амплитуду

$$\dot{\vec{p}}_m = -j\frac{I_m l}{\omega}\vec{z}_0. \tag{1.31}$$

Изображенный на рис. 1.7 элемент тока (колеблющийся диполь) рассматривается в качестве элементарного излучателя и называется диполем Герца.

Расположив диполь в сферической системе координат (рис. 1.9) получают комплексную амплитуду векторного потенциала элемента тока:

$$\dot{\vec{A}}_m = (\vec{r}_0 \cos\vartheta - \vec{\vartheta}_0 \sin\vartheta)\frac{\mu l I_m}{4\pi r} e^{-jkr}. \tag{1.32}$$

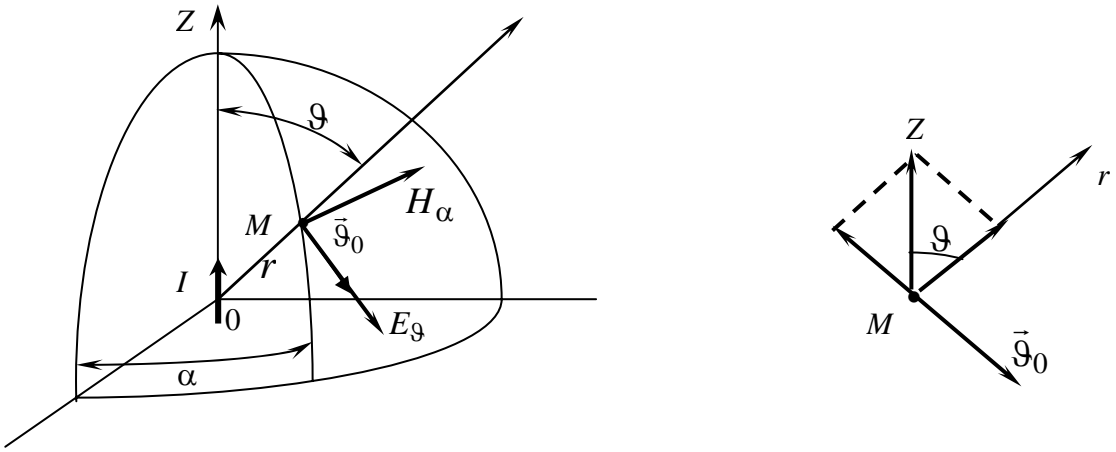


Рис. 1.9

Компоненты поля, создаваемого диполем Герца в произвольной точке пространства $M(r,\vartheta,\alpha)$, определяются по приведенным выше формулам и при переходе от комплексов к векторам поля принимают вид:

$$H_\alpha = \frac{klI_m}{4\pi r}\left[\frac{1}{kr}\cos(\omega t - kr) - \sin(\omega t - kr)\right]\sin\vartheta;$$

$$E_r = \frac{klI_m}{2\pi\omega\varepsilon r^2}\left[\frac{1}{kr}\sin(\omega t - kr) + \cos(\omega t - kr)\right]\cos\vartheta; \qquad (1.33)$$

$$E_\vartheta = \frac{k^2 lI_m}{4\pi\omega\varepsilon r}\left[\left(\frac{1}{k^2 r^2} - 1\right)\sin(\omega t - kr) + \frac{1}{kr}\cos(\omega t - kr)\right]\sin\vartheta;$$

$$H_r = H_\vartheta = E_\alpha = 0.$$

Ближняя зона (зона квазистационарности). Границы этой зоны определяются условиями $r \gg l$ (l – длина элемента тока или плечо вибратора) и $kr \ll 1$, или $r \ll 1/k$. В силу равенства $k = 2\pi/\lambda$ второе условие принимает вид $r \ll \lambda/2\pi$ (условие квазистационарности). Для ближней зоны (на расстояниях от вибратора существенно меньших длины волны) формулы (1.33) можно упростить, отбрасывая малые члены в квадратных скобках и пренебрегая фазовым сдвигом kr:

$$H_\alpha = \frac{lI_m}{4\pi r^2}\sin\vartheta\cos\omega t; \quad E_r = \frac{p_m}{2\pi\varepsilon r^3}\cos\vartheta\sin\omega t;$$

$$E_\vartheta = \frac{p_m}{4\pi\varepsilon r^3}\sin\vartheta\sin\omega t; \quad p_m = \frac{lI_m}{\omega}. \qquad (1.34)$$

Поле согласно (1.34) не имеет волнового характера, так как выражения (1.34) получены в пренебрежении излучением в ближней зоне вследствие его незначительности. Пространственное распределение в этом случае свойственно статическому диполю. Выражения (1.34) содержат одну составляющую вектора напряженности магнитного поля элемента тока и две составляющие вектора напряженности электрического поля вибратора, характеризующиеся в каждый момент времени как «стационарные» величины. Из (1.34) следует, что величины E и H сдвинуты по фазе на угол 90°.

Дальняя зона. Рассмотрим поле на расстояниях, значительно превышающих длину волны, когда $r \gg \lambda$ и $kr \gg 1$. В этом случае можно пренебречь членами порядка $1/k^2 r^2$ и $1/kr$. Тогда уравнения (1.33) принимают вид [35]:

$$H_\alpha = -\frac{klI_m}{4\pi r}\sin\vartheta\sin(\omega t - kr);$$

$$E_r = 0; \qquad (1.35)$$

$$E_\vartheta = -\frac{klW^0 I_m}{4\pi r}\sin\vartheta\sin(\omega t - kr).$$

В (1.35) введено отношение амплитуд E_m и H_m, которое равно $W^0 = \frac{E_m}{H_m} = \sqrt{\frac{\mu}{\varepsilon}}$ и называется волновым сопротивлением неограниченной среды. Для вакуума $W^0 = \sqrt{\frac{\mu_0}{\varepsilon_0}} = 120\pi$ [Ом].

Уравнения (1.35) соответствуют полю излучения. Оно представляет собой сферическую волну. Векторы $\vec{E}$ и $\vec{H}$ расположены перпендикулярно к направлению распространения волны, взаимно перпендикулярны и синфазны. Излучение максимально в экваториальной плоскости ($\vartheta = 90°$) и отсутствует в осевом направлении ($\vartheta = 0$).

Более полное представление об излучении дает диаграмма направленности (рис. 1.10), которую изображают следующим построением. В произвольной меридиональной плоскости откладываются ряд отрезков, пропорциональных амплитуде E_m (или H_m) в данном направлении ϑ для фиксированного расстояния r. Концы этих отрезков будут лежать на двух соприкасающихся окружностях. Полная мощность, излучаемая диполем Герца, определяется выражением

$$\vec{P} = \frac{\pi}{3} I_m^2 W^0 \left(\frac{l}{\lambda}\right)^2. \qquad (1.36)$$

Оно показывает, что излучение резко возрастает при ослаблении условия квазистационарности поля ($l << \lambda$).

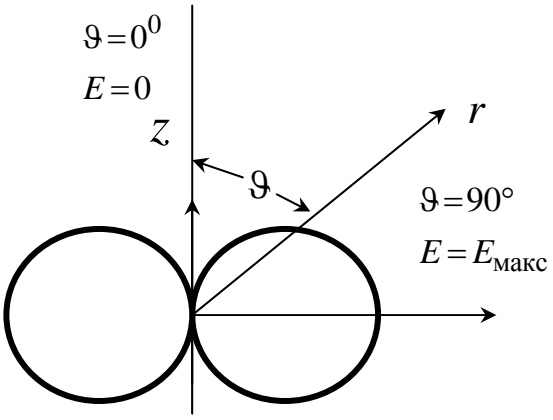


Рис. 1.10. Диаграмма направленности

1.2.1.3. Элементарный магнитный излучатель

В теории электромагнитного поля доказывается [35], что замкнутый виток (рис. 1.11, *а*) с постоянным током на превышающих его размеры расстояниях создает такое же магнитное поле как если бы на его месте находился магнитный диполь (рис. 1.11, *б*) с моментом $\vec{m} = \vec{z}_0 I \mu S$.

При гармоническом токе витка $I = I_m \cos\omega t$ переменный магнитный диполь характеризуется комплексной амплитудой момента $\dot{\vec{m}} = \vec{z}_0 \dot{I}_m \mu S$. Такой виток называют элементарным магнитным излучателем или магнитным диполем Герца.

Решение уравнений Максвелла для магнитного диполя Герца в комплексной форме имеет вид

$$\dot{\vec{E}} = -\vec{\alpha}_0 \frac{j\omega\mu I_m S}{4\pi r}\left(\frac{1}{r} + jk\right)e^{j(\omega t - kr)}\sin\vartheta;$$
$$\dot{\vec{H}} = \frac{I_m S}{4\pi}\left[\vec{r}_0 \frac{2}{r^2}\left(\frac{1}{r} + jk\right)\cos\vartheta + \vec{\vartheta}_0 \frac{1}{r}\left(\frac{1}{r^2} + j\frac{k}{r} - k^2\right)\sin\vartheta\right]e^{j(\omega t - kr)}. \quad (1.37)$$

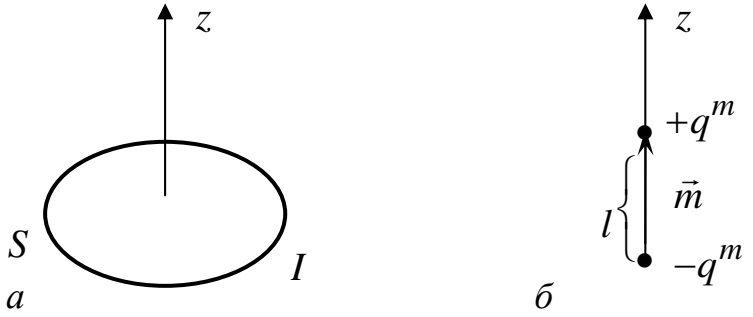


Рис. 1.11

Из (1.37) определяется запись компонент электромагнитного поля:

$$E_\alpha = \frac{I_m k^2 S W^0}{4\pi r}\left[\frac{1}{kr}\sin(\omega t - kr) + \cos(\omega t - kr)\right]\sin\vartheta;$$
$$H_r = \frac{I_m k S}{2\pi r^2}\left[\frac{1}{kr}\cos(\omega t - kr) - \sin(\omega t - kr)\right]\cos\vartheta; \quad (1.38)$$
$$H_\vartheta = \frac{I_m k^2 S}{4\pi r}\left[\left(\frac{1}{k^2 r^2} - 1\right)\cos(\omega t - kr) - \frac{1}{kr}\sin(\omega t - kr)\right]\sin\vartheta;$$
$$E_r = E_\vartheta = H_\alpha = 0.$$

Сравнивая (1.33) и (1.38) отмечаем, что уравнения Максвелла характеризуются перестановочной двойственностью.

Из (1.38) получаем компоненты ближнего поля:

$$E_\alpha = \frac{I_m \mu S \omega}{4\pi r^2}\sin\vartheta\sin\omega t; \quad H_r = \frac{m_m}{2\pi\mu r^3}\cos\vartheta\cos\omega t;$$
$$H_\vartheta = \frac{m_m}{4\pi\mu r^3}\cos\vartheta\cos\omega t; \quad m_m = I_m \mu S \quad (1.39)$$

и поля излучения:

$$E_\alpha = \frac{I_m k^2 S W^0}{4\pi r}\cos(\omega t - kr)\sin\vartheta;\ \ H_r = 0;$$
$$H_\vartheta = -\frac{I_m k^2 S}{4\pi r}\cos(\omega t - kr)\sin\vartheta. \qquad (1.40)$$

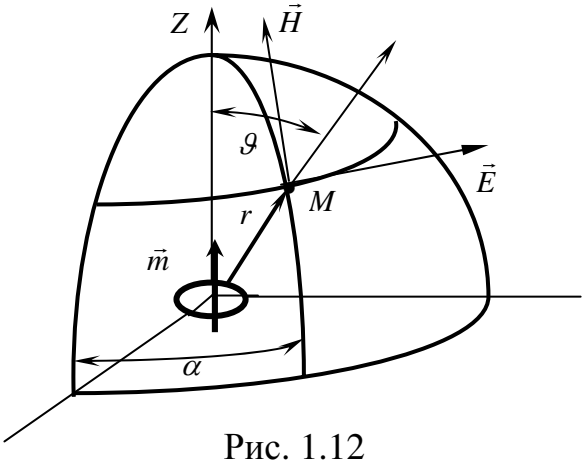


Рис. 1.12

В дальней зоне элементарный магнитный излучатель создает волновое поле, которое отличается от поля элементарного электрического излучателя только ориентацией (рис. 1.12). Диаграмма направленности магнитного излучателя не отличается от диаграммы направленности элементарного электрического излучателя (рис. 1.10).

1.2.1.4. Электромагнитные каналы утечки информации ТСПИ

К побочным электромагнитным излучениям ТСПИ относятся:

- излучения элементов ТСПИ;
- излучения на частотах работы высокочастотных (ВЧ) генераторов ТСПИ;
- излучения на частотах самовозбуждения усилителей низкой частоты (УНЧ) ТСПИ.

Электромагнитные излучения элементов ТСПИ. В ТСПИ, в частности и в линиях связи, входящих в их состав, носителем информации является электрический ток, характеристики которого (сила тока, напряжение, частота и фаза) изменяются по закону информационного сигнала. При прохождении электрического тока по проводникам ТСПИ вокруг них в окружающем пространстве возникает электрическое и магнитное поле. По этой причине элементы ТСПИ можно рассматривать как излучатели электромагнитного поля, составляющие которого модулированы также по закону изменения информационного сигнала.

Высокочастотные электромагнитные излучения передатчиков средств связи, модулированные информационным сигналом, могут перехватывать-

ся портативными средствами радиоразведки и при необходимости передаваться в центр обработки для их раскодирования.

Данный канал перехвата информации наиболее широко используется для прослушивания телефонных разговоров, ведущихся по радиотелефонам, сотовым телефонам или по радиорелейным и спутниковым линиям связи.

Электромагнитные излучения персональных компьютеров. Согласно оценочным данным по каналу ПЭМИН (побочных электромагнитных излучений и наводок) может быть перехвачено не более 1–2 процентов данных, обрабатываемых на персональных компьютерах и других технических средствах передачи информации (ТСПИ) [33]. На первый взгляд может показаться, что этот канал менее опасен по сравнению, например, с акустическим, по которому из помещения может быть перехвачена речевая информации в полном объеме. Но необходимо помнить, что в настоящее время наиболее важная информация, содержащая государственную тайну или технологические секреты, обрабатывается на персональных компьютерах. Специфика канала ПЭМИН такова, что те самые два процента информации, уязвимые для технических средств перехвата – это данные, вводимые с клавиатуры компьютера или отображаемые на мониторе.

Компьютеры порождают электромагнитные излучения, которые не только создают помехи для радиоприема, но также создают технические каналы утечки информации. Соединительные кабели (линии связи), обладающие индуктивностью и емкостью, образуют резонансные контуры, излучающие высокочастотные электромагнитные волны, модулированными сигналами данных.

Аналогичная ситуация имеет место и при взаимном обмене сигналами между параллельно проложенными кабелями. Исследователями продемонстрировано восстановление сетевых данных через телефонную линию, причем телефонный кабель проходил рядом с кабелем компьютерной сети всего на протяжении двух метров. Еще одна опасность исходит от "активных" атак (высокочастотное навязывание): злоумышленник, знающий резонансную частоту, например, кабеля клавиатуры персонального компьютера, может облучать его на этой частоте, а затем регистрировать коды нажатия клавиш в ретранслируемом резонансном сигнале благодаря вызванным ими изменениям импеданса.

Для ПК высокочастотные излучения находятся в диапазоне до 1 ГГц с максимумом в полосе 50–300 МГц. Широкий спектр обусловлен наличием как основной, так и высших гармоник последовательностей коротких прямоугольных информационных импульсов. К появлению дополнительных составляющих в побочном электромагнитном излучении приводит также применение в вычислительных средствах высокочастотной коммутации.

Говорить о какой-либо диаграмме направленности электромагнитных излучений ПК не имеет смысла, так как расположение его составных частей имеет много комбинаций. ПК имеет линейную поляризацию. Она определяется расположением соединительных кабелей, являющихся основными источниками излучений в ПК с металлическим кожухом на системном блоке.

Уровни побочных электромагнитных излучений ВТ регламентированы по условиям электромагнитной совместимости целым рядом зарубежных и отечественных стандартов. Так, например, согласно публикации «№ 22 CISPR (специальный международный комитет по радиопомехам) для диапазона 230–1000 МГц уровень напряженности электромагнитного поля, излучаемого оборудованием ВТ, на расстоянии 10 м не должен превышать 37 дБ. Однако излучения такого уровня могут быть перехвачены на значительных расстояниях. Следовательно, соответствие электромагнитных излучений средств ВТ нормам на электромагнитную совместимость не обеспечивает сохранение конфиденциальности обрабатываемой в них информации.

Электромагнитные излучения на частотах работы ВЧ генераторов ТСПИ и ВТСС. В состав ТСПИ и ВТСС могут входить различного рода высокочастотные генераторы как-то: задающие генераторы, генераторы тактовой частоты, генераторы стирания и подмагничивания магнитофонов, гетеродины радиоприемных устройств, генераторы измерительных приборов и т.д.

При внешних воздействиях информационного сигнала (например, электромагнитных полей) на элементах ВЧ генераторов индуктируются электрические сигналы. Приемными антеннами для магнитного поля могут служить катушки индуктивности колебательных контуров, сглаживающие дроссели в цепях электропитания и т.д. Приемниками электрического поля являются провода высокочастотных цепей и другие элементы. Индуктированные электрические сигналы могут вызвать модуляцию собственных ВЧ колебаний генераторов и излучение их в окружающее пространство.

Электромагнитные излучения на частотах самовозбуждения УНЧ ТСПИ. Самовозбуждение УНЧ ТСПИ (например, усилителей систем звукоусиления и звукового сопровождения, магнитофонов, систем громкоговорящей связи т.п.) возможно за счет преобразований отрицательных обратных связей (индуктивных или емкостных) в паразитные положительные в результате фазового сдвига сигнала обратной связи на определенных частотах, что приводит к переводу усилителя из режима усиления в режим автогенерации сигналов. Частота самовозбуждения находится в пределах рабочих частот элементов УНЧ (например, полупроводниковых приборов, электровакуумных ламп и т.п.), переходящих в нелинейный режим работы при перегрузке за счет действия положительной обратной связи. Сигнал на

частотах самовозбуждения, как правило, оказывается промодулированным информационным сигналом. Перехват побочных электромагнитных излучений ТСПИ осуществляется средствами радио-, радиотехнической разведки, размещенными за пределами контролируемой зоны.

Зона, в которой возможен перехват побочных электромагнитных излучений с помощью разведывательного приемника с последующей расшифровкой содержащейся в них информации (т.е. зона, в пределах которой отношение «информационный сигнал/помеха» превышает допустимое нормированное значение), называется опасной *зоной 2*.

1.2.2. Электрические каналы утечки информации

Электрические каналы утечки информации образуются за счет:

- наводок электромагнитных излучений ТСПИ на соединительные линии ВТСС и посторонние проводники, выходящие за пределы контролируемой зоны;
- просачивания информационных сигналов в цепи электропитания ТСПИ;
- просачивания информационных сигналов в цепи заземления ТСПИ.

1.2.2.1. Наводки электромагнитных излучений ТСПИ

Наводки возникают при излучении элементами ТСПИ (в том числе и их соединительными линиями) информационных сигналов, а также при наличии гальванической связи соединительных линий ТСПИ и посторонних проводников или линий ВТСС. Уровень наводимых сигналов в значительной степени зависит от мощности излучаемых сигналов, расстояния до проводников, а также длины соединительных линий ТСПИ и посторонних проводников.

Пространство вокруг ТСПИ, в пределах которого на случайных антеннах наводится информационный сигнал выше нормированного уровня, называется (опасной) *зоной 1*.

Случайными антеннами могут быть цепи ВТСС или посторонние проводники, способные принимать побочные электромагнитные излучения.

Случайные антенны могут быть сосредоточенными и распределенными. *Сосредоточенная случайная антенна* представляет собой техническое средство небольшого объема, например телефонный аппарат, громкоговоритель радиотрансляционной сети, реле и т.д. К *распределенным случайным антеннам* относятся случайные антенны с распределенными параметрами (длинные линии): кабели, провода, металлические трубы и другие токопроводящие устройства.

Просачивание информационных сигналов в цепи электропитания. Просачивание возможно при наличии взаимоиндуктивной связи между выходным трансформатором усилителя (например, УНЧ) и трансформатором выпрямительного устройства. Кроме того, токи усиливаемых информационных сигналов замыкаются через источник электропитания, создавая на его внутреннем сопротивлении падение напряжения, которое при недостаточном затухании в фильтре выпрямительного устройства может быть обнаружено в линии электропитания. Информационный сигнал может проникнуть в цепи электропитания также в результате того, что среднее значение потребляемого тока в оконечных каскадах усилителей в большей или меньшей степени зависит от амплитуды информационного сигнала, что создает неравномерную нагрузку на выпрямитель и приводит к изменению потребляемого тока по закону изменения информационного сигнала.

Наводки на вторичные источники питания (ВИП), можно разделить на три вида: наводки в виде переменного напряжения с частотой питающей сети или ее гармоник, высокочастотные наводки, появляющиеся вследствие антенного эффекта проводов питающей сети, наводки, возникающие внутри блока вследствие появления паразитных связей через общие провода питания различных элементов.

Основными причинами появления помехи с частотой питающей сети или ее гармоник являются недостаточное сглаживание пульсаций в ВИП, паразитные связи элементов с первичными цепями ВИП, неэквипотенциальность точек заземления, наличие общих проводов питания, по которым возможна гальваническая связь. Из всех причин только первая не является следствием паразитных процессов. Величина наводки зависит не только от вида паразитной связи, но и от схемы подключения двухфазных ВИП к трехфазной промышленной сети.

В канале связи при емкостной паразитной связи (рис. 1.13) для схемы питания без нулевого провода помеха будет [3]

$$U_{\text{п.п}} = (U_1 C_{\text{п1}} - U_2 C_{\text{п2}}) R_{\text{к}} \omega_{\text{п}} / \sqrt{1 + T_{\text{к}}^2 \omega_{\text{п}}^2}, \qquad (1.41)$$

где $C_{\text{п1}}, C_{\text{п2}}$ – паразитные емкости канала связи с фазными проводами, в общем случае $C_{\text{п1}} \neq C_{\text{п2}}$; $\omega_{\text{п}}$ – частота питающей сети; $R_{\text{к}}, T_{\text{к}}$ – внутреннее сопротивление и постоянная времени канала связи.

Из (1.41) видно, что для снижения наводки необходимо добиваться равенства $C_{\text{п1}} = C_{\text{п2}}$ и $U_1 = U_2$.

Для выполнения равенства $C_{\text{п1}} = C_{\text{п2}}$ необходимо подводку переменных напряжений выполнять симметричной двухпроводной линией с минимально возможным расстоянием между проводами, чаще всего для этого используют витую пару. Выполнение равенства $U_1 = U_2$ не зависит от потребителя и в общем случае не обеспечивается.

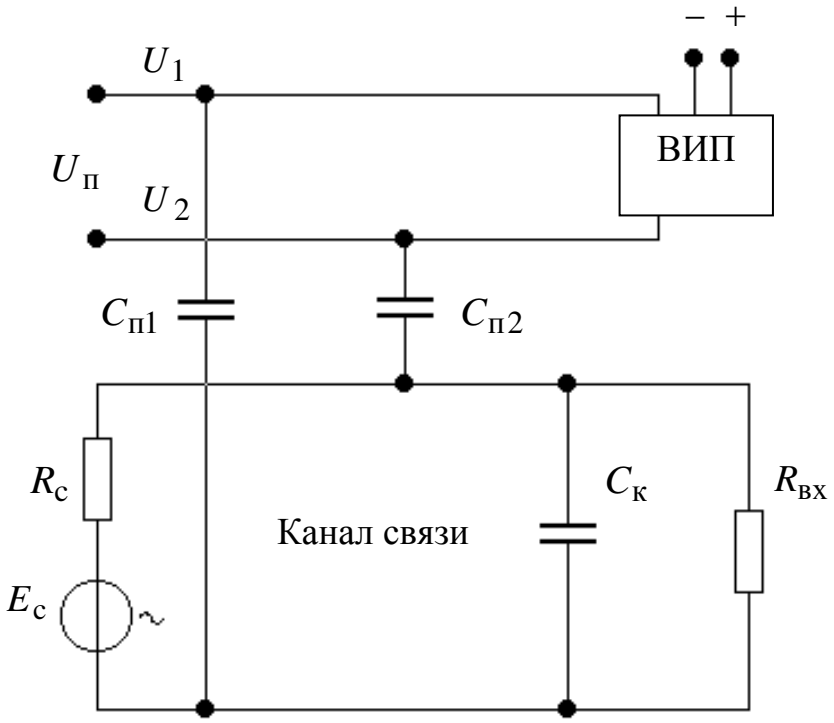


Рис. 1.13. Схема емкостной внешней паразитной связи с первичной цепью ВИП

Помехи в схеме с нулевым проводом можно рассчитать по (1.41), подставив U_0 вместо U_2. В этом случае для снижения наводки имеется только один путь – снижение паразитной емкости $C_{п1}$.

Вторая причина появления наводки с частотой питающей сети заключается в наличии общих проводов.

Просачивание информационных сигналов в цепи заземления. Кроме заземляющих проводников, служащих для непосредственного соединения ТСПИ с контуром заземления, гальваническую связь с землей могут иметь различные проводники, выходящие за пределы контролируемой зоны. К ним относятся нулевой провод сети электропитания, экраны (металлические оболочки) соединительных кабелей, металлические трубы систем отопления и водоснабжения, металлическая арматура железобетонных конструкций и т.д. Все эти проводники совместно с заземляющим устройством образуют разветвленную систему заземления, в которой могут наводиться информационные сигналы. Кроме того, в грунте вокруг заземляющего устройства возникает электромагнитное поле, которое также является источником информации.

Перехват информационных сигналов по электрическим каналам утечки возможен путем непосредственного подключения к соединительным линиям ВТСС и посторонним проводникам специальных устройств съема информации. Для перехвата электромагнитных сигналов используются специальные средства радио- и радиотехнической разведки.

Съем информации по электрическим каналам утечки информации. Для съема информации, обрабатываемой в ТСПИ, применяют главным образом электронные устройства перехвата информации – *закладные устройства.* Электронные устройства перехвата информации, устанавливаемые в ТСПИ, иногда называют *аппаратными закладками.* Они представляют собой мини-передатчики, излучение которых модулируется информационным сигналом. Закладки устанавливаются в ТСПИ как иностранного так отечественного производства.

Перехваченная с помощью закладных устройств информация или непосредственно передается по радиоканалу, или сначала накапливается на специальном запоминающем устройстве, а уже затем по сигналу извне передается на запросивший ее объект.

Электрический канал перехвата информации, передаваемой по кабельным линиям связи, предполагает контактное подключение аппаратуры разведки к кабельным линиям связи.

Самый простой способ – это непосредственное параллельное подключение к линии связи. Но данный факт легко обнаруживается, так как приводит к изменению характеристик линии связи за счет падения напряжения. Поэтому средства разведки к линии связи подключаются или через согласующее устройство, несколько снижающее падение напряжения, или через специальные устройства компенсации падения напряжения. В последнем случае аппаратура разведки и устройство компенсации падения напряжения включаются в линию связи последовательно, что существенно затрудняет обнаружение факта несанкционированного подключения к ней.

Контактный способ используется в основном для снятия информации с коаксиальных и низкочастотных кабелей связи. Для кабелей, внутри которых поддерживается повышенное давление воздуха, применяются устройства, исключающие его снижение, в результате чего предотвращается срабатывание специальной сигнализации.

Электрический канал наиболее часто используется для перехвата телефонных разговоров. При этом перехватываемая информация может непосредственно записываться на диктофон или передаваться по радиоканалу в пункт приема для ее записи и анализа. Устройства, подключаемые к телефонным линиям связи и комплексированные с устройствами передачи информации по радиоканалу, часто называют *телефонными закладками.*

В случае использования сигнальных устройств контроля целостности линии связи, ее активного и реактивного сопротивления факт контактного подключения к ней аппаратуры разведки будет обнаружен. Поэтому спецслужбы наиболее часто используют индуктивный канал перехвата информации, не требующий контактного подключения к каналам связи. В данном канале используется эффект возникновения вокруг кабеля связи электромагнитного поля при прохождении по нему информационных элек-

трических сигналов, которые перехватываются специальными индукционными датчиками. Индукционные датчики используются в основном для съема информации с симметричных высокочастотных кабелей. Сигналы с датчиков усиливаются, осуществляется частотное разделение каналов, и информация, передаваемая по отдельным каналам, записывается на магнитофон или высокочастотный сигнал записывается на специальный магнитофон.

Современные индукционные датчики способны снимать информацию с кабелей, защищенных не только изоляцией, но и двойной броней из стальной ленты и стальной проволоки, плотно обвивающих кабель.

Для бесконтактного съема информации с незащищенных телефонных линий связи могут использоваться специальные низкочастотные усилители, снабженные магнитными антеннами.

Некоторые средства бесконтактного съема информации, передаваемой по каналам связи, могут комплексироваться с радиопередатчиками для ретрансляции в центр ее обработки.

Исходя из выше перечисленных особенностей ТСПИ и ВТСС, а также возможностей современных технических разведок можно заключить, что всегда существует потенциальная опасность возникновения технического канала утечки информации. И эта проблема должна решаться за счет совершенствования применяемого оборудования (ТСПИ и ВТСС), так и применения средств активной защиты.

1.2.3. Параметрический канал утечки информации

Параметрический канал утечки информации используется для перехвата обрабатываемой в технических средствах информации путем их *«высокочастотного облучения»*. При воздействии облучающего электромагнитного поля на элементы ТСПИ происходит переизлучение электромагнитного поля. В ряде случаев возможна модуляция вторичного излучающего поля информационным сигналом. Для исключения взаимного влияния облучающего и переизлученного сигналов может использоваться их временное или частотное разделение. Например, для облучения ТСПИ могут использовать импульсные сигналы, в промежутках между которыми осуществляется прием переизлученных сигналов.

При переизлучении параметры сигналов изменяются. Поэтому данный канал утечки информации часто называют *параметрическим.*

Для перехвата информации по данному каналу применяют специальные высокочастотные генераторы с антеннами, имеющими узкие диаграммы направленности, и специальные радиоприемные устройства.

Информация после обработки в ТСПИ может передаваться по проводным каналам связи, где также возможен ее перехват.

Список литературы

1. Анин Б. Ю. Защита компьютерной информации. СПб.: БХВ Санкт Петербург, 2000. 384 с: ил.
2. Бухвинер В. Е. Телеобслуживание и человекомашинная связь. М.: Радио и связь, 1983
3. Второй московский форум диллеров МЕ // Компьютерра. 1993. № 21. С. 14.
4. Гайкович В. Ю., Першин А. Ю. Безопасность электронных банковских систем. М.: Единая Европа, 1994.
5. Герасименко В. А. Защита информации в автоматизированных системах обработки данных. В 2 х кн. М.: Энергоатомиздат.1994.
6. Герасименко В. А., Малюк А. А. Основы защиты информации. М.: Инкомбук, 1997. 540 с.
7. Грушко А. А., Тимонина Е. Е. Теоретические основы защиты информации. Яхтсмен, 1996.
8. Дружинин Т. В., Сергеева И. В. Качество информации. М.: Радио и связь, 1990. С. 170.
9. Закон РФ об информации, информатизации и защите информации.
10. Касперский Е. Компьютерные вирусы: что это такое и как с ними бороться. М.: СК Пресс, 1998.
11. Корюкова А. А., Дера В. Т. Основы научно технической информации. М.: Высш. шк., 1985.
12. Лопатников Л. И. Популярный экономико математический словарь. М.: Знание, 1990. С. 49.
13. Мафик С. Механизмы защиты в сетях ЭВМ. М.: Мир, 1993.
14. Мельников В. В. Защита информации в компьютерных системах. М.: Финансы и статистика: Электроинформ, 1997.
15. Новик И. Б., Абдуллаев А. Ш. Введение в информационный мир. М.: Наука, 1991. С.7.
16. Программно аппаратные средства обеспечения информационной безопасности. Защита программ и данных: Учеб. пособие для вузов / П. Ю. Белкин, О. О. Михальский, А. С. Першаков и др. М.: Радио и связь, 2000. 168 с.: ил.
17. Программно аппаратные средства обеспечения информационной безопасности. Защита в операционных системах: Учеб. пособие для вузов /Проскурин В.Г., Кругов СВ., Мацкевич И.В. М.: Радио и связь, 2000. 168 с.
18. Расторгуев С. П. Программные методы защиты информации в компьютерах и сетях. М.: Яхтсмен, 1993.
19. Руководящий документ ГТК РФ. Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требований по защите информации. М.: Воениздат, 1992.
20. Руководящий документ ГТК РФ. Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации. М.: Воениздат, 1992.
21. Самосук М. Компьютерное пиратство. // Защита программного обеспечения: Сб./ Под ред. Гроубера. М.: Мир, 1992
22. Семкин С. Н., Семкин А. Н. Основы информационной безопасности объектов обработки информации: Науч. практ. пособие. Орел: 2000. 300 с.
23. Слепов Б. С., Чистяков В. М. Управление процессами использования информационных ресурсов. Новосибирск: Наука, 1984, с. 235.
24. Спесивцев А. П. Защита информации в персональных ЭВМ. М.: Радио и связь, 1992.

25. Теоретические основы компьютерной безопасности: Учебное пособие для вузов / П. Н. Девянин, О. О. Михальский, Д. И. Правиков и др. М.: Радио и связь, 2000. 192 с: ил.
26. Терминологические основы проблематики информационной безопасности // Мат. к заседанию межвед. междисциплинарного сем. по науч. проблемам информ. безопасности 1 марта 2001 г. М.: МГУ, 2001.
27. Хоффман Л. Дж. Современные методы защиты информации: Пер. с англ. М.: Сов. радио, 1980.
28. Цыкин Г. С. Усилители электрических сигналов. М.: Энергия, 1969.
29. Шеннон К. Работы по теории информации и кибернетике. М.: Изд во иностранной литературы, 1963. 489 с.
30. Ярочкин В. И. Безопасность информационных систем. М.: Ось 89, 1996. 320 с. (безопасность предпринимательства).
31. 31. Ярочкин В. И. Система безопасности фирмы. 2 е изд. М.: Ось 89, 1999. 192 с.
32. Ярочкин В. И. Технические каналы утечки информации. М.: ИП КОР, 1994.
33. Шнайдер Б. Прикладная криптография. М.: Мир 1999.