

УДК 621.391

В.И. Грабчак

Военный институт РВ и А Сумского государственного университета

ИССЛЕДОВАНИЕ ДОСТОВЕРНОСТИ ПЕРЕДАЧИ ДАННЫХ В АСУВ С ИСПОЛЬЗОВАНИЕМ КАСКАДНЫХ ТЕОРЕТИКО-КОДОВЫХ СХЕМ

Исследуется достоверность передаваемых данных в АСУВ с использованием каскадных теоретико-кодовых схем в каналах с независимыми и группирующимися ошибками в различных режимах функционирования

каскадные теоретико-кодовые схемы, достоверность передачи данных, модели каналов с независимыми и группирующимися ошибками

Введение

Постановка проблемы в общем виде и анализ литературы. Одним из эффективных способов защиты данных от ошибок, которые возникают при передаче по каналам связи, является помехоустойчивое кодирование [1, 2]. Мощным средством обеспечения информационной скрытности, является шифрование [3, 4]. Перспективным направлением в развитии комплексных механизмов обеспечения информационной скрытности и достоверности передачи данных в АСУВ, являются каскадные теоретико-кодовые схемы, которые позволяют за счет совмещения помехоустойчивого кодирования и шифрования информации интегрировано обеспечить защиту передаваемых данных от случайного воздействия ошибок и несанкционированного просмотра противником [5, 6]. Их практическое использование позволяет реализовать в одном устройстве методы канального кодирования и специального преобразования данных.

Целью статьи является исследование достоверности передачи данных с использованием каскадных теоретико-кодовых схем в дискретных каналах с независимыми и группирующимися ошибками в различных режимах функционирования.

Результаты исследований

Исследование достоверности передачи данных в каналах с независимыми ошибками. Предположим, что при передаче кодового слова ошибки возникают независимо с вероятностью P_o . Тогда вероятность ошибки кратности I на длине блока n

$$P(i, n) = C_n^i P_o^i (1 - P_o)^{n-i}. \quad (1)$$

Вероятность искажения кодовой комбинации не менее, чем m ошибками запишется в виде

$$P(\geq m, n) = \sum_{i=m}^n P(i, n).$$

После подстановки в (1) получим, что для модели с независимыми ошибками значение $P(\geq m, n)$ определяется как

$$P(\geq m, n) = \sum_{i=m}^n C_n^i P_o^i (1 - P_o)^{n-i}. \quad (2)$$

Если код исправляет все ошибки (t – число исправляемых ошибок (n, k, d) блоковым кодом) в пределах радиуса упаковки кода и не исправляет другие ошибки то

$$P_{од}(n) = P(> t, n) = \sum_{i=t+1}^n C_n^i P_o^i (1 - P_o)^{n-i}. \quad (3)$$

Для пересчета вероятности ошибки декодирования на один символ $P_{ош}$ воспользуемся выражением [2]

$$P_{ош} = \frac{d}{n} P_{од}(n).$$

После подстановки в (3) получим

$$P_{ош} = \frac{d}{n} \sum_{i=t+1}^n C_n^i P_o^i (1 - P_o)^{n-i} = \frac{d}{n} \left(1 - \sum_{i=0}^t C_n^i P_o^i (1 - P_o)^{n-i} \right). \quad (4)$$

Для расчета энергетического выигрыша от кодирования (ЭВК) рассмотрим зависимость вероятности P_o от соотношения энергия сигнала к спектральной плотности мощности шума. Условная вероятность ошибочного приема полностью известных равновероятных сигналов при условии оптимального приема определяется выражением [7]

$$P_o = \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{-\sqrt{E(1-b_s)/N_o}} \exp\left(-\frac{y^2}{2}\right) dy = V\left(\sqrt{\frac{E(1-b_s)}{N_o}}\right), \quad (5)$$

где E – энергия сигнала; N_o – спектральная плотность мощности белого шума; b_s – коэффициент взаимной корреляции между сигналами; $V(x)$ – интеграл ошибок. Так, для случая использования двоичного фазоманипулированного (ФМ) сигнала с манипуляцией фазы на 180° коэффициент взаимной корреляции $b_s = -1$. Вероятность P_o для таких сигналов определяется выражением

$$P_o = 0,5 \left(1 - \Phi\left(\sqrt{\frac{2E}{N_o}}\right) \right) = 1 - \Phi\left(\sqrt{\frac{2E}{N_o}}\right),$$

где $\Phi(x)$ и $\Phi'(x)$ – табулированные функции, представляющие собой интегралы вероятностей:

$$\Phi(x) = \frac{2}{\sqrt{2\pi}} \int_0^x \exp\left(-\frac{y^2}{2}\right) dy = 1 - \frac{2}{\sqrt{2\pi}} \int_{-x}^{-\infty} \exp\left(-\frac{y^2}{2}\right) dy;$$

$$\Phi'(x) = \frac{1}{\sqrt{2\pi}} \int_{-\infty}^x \exp\left(-\frac{y^2}{2}\right) dy = 1 - \frac{1}{\sqrt{2\pi}} \int_x^{\infty} \exp\left(-\frac{y^2}{2}\right) dy.$$

Применение (n, k, d) блочных кодов, обнаруживающих и исправляющих ошибки, приводит к увеличению избыточности передаваемых данных. Если зафиксировать энергию сообщения, передаваемого в канал, то энергия, приходящаяся на один символ, уменьшится пропорционально внесенной избыточности.

Для расчета вероятности ошибки на символ на выходе декодера по выражению (4) с учетом внесенной избыточности отношение энергии сигнала к спектральной плотности мощности шума в выражении (5) уменьшим в $R = k/n$ раз. Окончательное соотношение для вероятности ошибки символа использованием помехоустойчивого (n, k, d) блочного кода запишется в виде:

$$P_{\text{ош}} = \frac{d}{n} \sum_{i=t+1}^n C_n^i \left(V \left(\sqrt{\frac{kE(1-b_s)}{nN_0}} \right) \right)^i \left(1 - V \left(\sqrt{\frac{kE(1-b_s)}{nN_0}} \right) \right)^{n-i} = \frac{d}{n} \left(1 - \sum_{i=0}^t C_n^i \left(V \left(\sqrt{\frac{kE(1-b_s)}{nN_0}} \right) \right)^i \left(1 - V \left(\sqrt{\frac{kE(1-b_s)}{nN_0}} \right) \right)^{n-i} \right).$$

Для двоичных ФМ сигналов последнее выражение переписывается в виде:

$$P_{\text{ош}} = \frac{d}{n} \sum_{i=t+1}^n C_n^i \left(1 - \Phi' \left(\sqrt{\frac{2kE}{nN_0}} \right) \right)^i \left(\Phi' \left(\sqrt{\frac{2kE}{nN_0}} \right) \right)^{n-i} = \frac{d}{n} \left(1 - \sum_{i=0}^t C_n^i \left(1 - \Phi' \left(\sqrt{\frac{2kE}{nN_0}} \right) \right)^i \left(\Phi' \left(\sqrt{\frac{2kE}{nN_0}} \right) \right)^{n-i} \right).$$

Достоверность передаваемых кодограмм при использовании теоретико-кодовых схем определяется, прежде всего, долей веса вектора ошибок вектора e , приходящегося на искусственное внесение теоретико-кодовой схемой, т.е. величиной $\rho = w(e) / t$. Следовательно, выражение по оценке вероятности ошибки символа с использованием теоретико-кодовой схемы, построенной по помехоустойчивому (n, k, d) блочному коду запишется в виде:

$$P_{\text{ош}} = \frac{d}{n} \sum_{i=(1-\rho)t+1}^n C_n^i \left(V \left(\sqrt{\frac{kE(1-b_s)}{nN_0}} \right) \right)^i \left(1 - V \left(\sqrt{\frac{kE(1-b_s)}{nN_0}} \right) \right)^{n-i} = \frac{d}{n} \left(1 - \sum_{i=0}^{(1-\rho)t} C_n^i \left(V \left(\sqrt{\frac{kE(1-b_s)}{nN_0}} \right) \right)^i \left(1 - V \left(\sqrt{\frac{kE(1-b_s)}{nN_0}} \right) \right)^{n-i} \right) \quad (8)$$

а для двоичных ФМ сигналов в виде:

$$P_{\text{ош}} = \frac{d}{n} \sum_{i=(1-\rho)t+1}^n C_n^i \left(1 - \Phi' \left(\sqrt{\frac{2kE}{nN_0}} \right) \right)^i \left(\Phi' \left(\sqrt{\frac{2kE}{nN_0}} \right) \right)^{n-i} = \frac{d}{n} \left(1 - \sum_{i=0}^{(1-\rho)t} C_n^i \left(1 - \Phi' \left(\sqrt{\frac{2kE}{nN_0}} \right) \right)^i \left(\Phi' \left(\sqrt{\frac{2kE}{nN_0}} \right) \right)^{n-i} \right) \quad (9)$$

С использованием полученных выражений (8), (9) проведем исследования достоверности передачи данных в каналах с независимыми ошибками при использовании каскадных теоретико-кодовых схем.

На рис. 1 приведены зависимости вероятности декодирования кодограмм в каскадных теоретико-кодовых схемах в каналах с независимым распределением ошибок от соотношения энергии ФМ сигнала к спектральной плотности помех при условии оптимального приема полностью известных равновероятных сигналов.

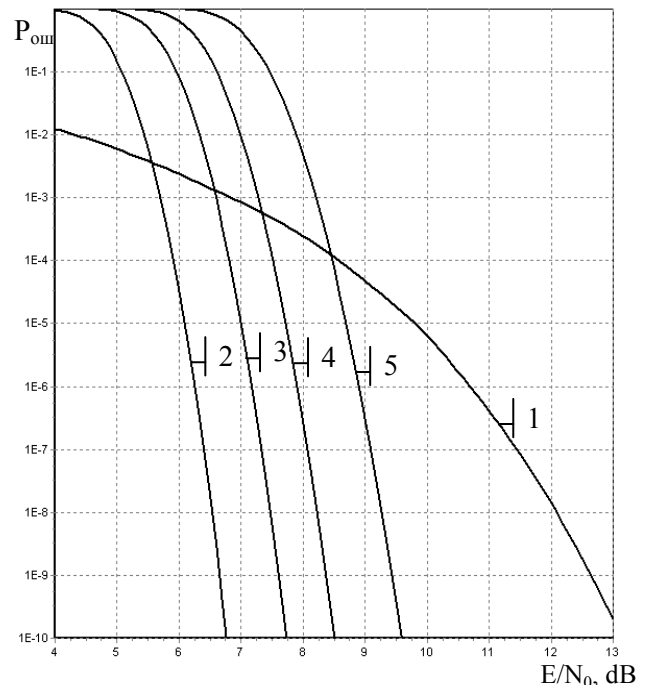


Рис. 1. Зависимости вероятности декодирования кодограмм в каскадных теоретико-кодовых схемах в каналах с независимым распределением ошибок

Зависимости, приведенные на рис. 1, соответствуют параметрам каскадной теоретико-кодовой схемы на эллиптических кодах и случаям:

- 1) без кодирования;
- 2) с применением каскадной теоретико-кодовой схемы и $\rho = 0$ (без внесения ошибок – режим помехоустойчивого кодирования);
- 3) с применением каскадной теоретико-кодовой схемы и $\rho = 0,3$ (режим слабого внесения ошибок для интегрированного обеспечения информационной скрытности и достоверности);
- 4) с применением каскадной теоретико-кодовой схемы и $\rho = 0,5$ (режим среднего внесения

ошибок для интегрированного обеспечения информационной скрытности и достоверности);

5) с применением каскадной теоретико-кодовой схемы и $\rho = 0,7$ (режим сильного внесения ошибок для интегрированного обеспечения информационной скрытности и достоверности).

Как следует из приведенных на рис. 1 зависимостей, применение каскадных теоретико-кодовых схем с рекомендуемыми параметрами позволяет обеспечить требуемые показатели достоверности передачи данных в АСУВ в каналах с независимым распределением ошибок. Действительно, предлагаемые конструкции позволяют обеспечить передачу кодограмм с показателем потери достоверности $P_{\text{ош}} < 10^{-9}$ и получить энергетический выигрыш от кодирования 2,5 – 5, 0 дБ в зависимости от режима использования теоретико-кодовых схем для интегрированного обеспечения информационной скрытности и достоверности.

Исследование достоверности передачи данных в каналах с группирующимися ошибками. Воспользуемся описанием модели канала и методикой расчета вероятности ошибки декодирования детально рассмотренных в работах [8, 9, 10, 11].

В качестве модели дискретного симметричного канала с группирующимися ошибками рассмотрим упрощенную модель Беннета-Фройлиха [11], которая характеризуется следующими допущениями:

- ошибки могут возникать только в пределах пакета ошибок с постоянной вероятностью $P_{\varepsilon} = 1$ (сплошные пакеты);

- примыкание и взаимное перекрытие сплошных пакетов отсутствуют;

- постоянная вероятность P_{Π} – вероятность того, что с данной позиции начнется сплошной пакет ошибок любой длины;

- $P(l)$ – вероятность возникновения сплошного пакета длины l ;

- $P_{\Pi}(l)$ – вероятность того, что с данной позиции начнется сплошной пакет ошибок длины l , $P_{\Pi}(l) = P_{\Pi} \cdot P(l)$.

Для задания упрощенной модели Беннета-Фройлиха достаточно задать вероятность P_{Π} и распределение $P(l)$. Значение вероятности P_{Π} и распределение $P(l)$ можно получить экспериментально на достаточно большом объеме выборки [11]. Воспользуемся методикой оценки эффективности помехоустойчивого кодирования в каналах с группирующимися ошибками, впервые предложенной в [8, 9]. Рассмотрим упрощенную модель Беннета-Фройлиха с непересекающимися пакетами ошибок и возможным их примыканием друг к другу [9]. В этом случае на длине блока из n символов может произойти не более

$$\lambda' = \lfloor n/l \rfloor$$

блоков ошибок длины l .

Число сочетаний ξ пакетов на длине из n символов определяется значением биномиального коэффициента

$$C_{\lambda'+n-\xi}^{\xi} = C_{n-\xi}^{\xi}.$$

Тогда выражение для вероятности возникновения ξ пакетов длины l ошибок на блоке из n символов запишется в виде:

$$P_{\xi}(l, n) = C_{n-\xi}^{\xi} \cdot P_{\Pi}(l)^{\xi} \cdot (1 - P_{\Pi})^{n-\xi l},$$

а вероятность ошибки декодирования определяется как

$$P_{\text{од}} = 1 - (1 - P_{\Pi})^n - \sum_{l=1}^n \sum_{\substack{\xi=1 \\ l < \xi l \leq n}}^{\lambda'} C_{n-\xi}^{\xi} \cdot P_{\Pi}(l)^{\xi} \cdot (1 - P_{\Pi})^{n-\xi l}. \quad (10)$$

С учетом доли веса вектора ошибок приходящегося на искусственное внесение теоретико-кодовой схемой выражение по оценке вероятности ошибки символа для рассмотренной модели канала запишется в виде:

$$P_{\text{од}} = \frac{d}{n} \left[1 - \left(1 - V \left(\sqrt{\frac{kE(1-b_s)}{nN_0}} \right) \right)^n - \sum_{\xi=1}^{(1-\rho)t} C_n^{\xi} \cdot \left(V \left(\sqrt{\frac{kE(1-b_s)}{nN_0}} \right) \right)^{\xi} \cdot \left(1 - V \left(\sqrt{\frac{kE(1-b_s)}{nN_0}} \right) \right)^{n-\xi} \right] = \frac{d}{n} \left[1 - \sum_{\xi=0}^{(1-\rho)} C_n^{\xi} \cdot \left(V \left(\sqrt{\frac{kE(1-b_s)}{nN_0}} \right) \right)^{\xi} \cdot \left(1 - V \left(\sqrt{\frac{kE(1-b_s)}{nN_0}} \right) \right)^{n-\xi} \right], \quad (11)$$

а для двоичных ФМ сигналов в виде:

$$P_{\text{од}} = \frac{d}{n} \left[1 - \left(\Phi' \left(\sqrt{\frac{2kE}{nN_0}} \right) \right)^n - \sum_{\xi=1}^{(1-\rho)t} C_n^{\xi} \cdot \left(1 - \Phi' \left(\sqrt{\frac{2kE}{nN_0}} \right) \right)^{\xi} \cdot \left(\Phi' \left(\sqrt{\frac{2kE}{nN_0}} \right) \right)^{n-\xi} \right] = \frac{d}{n} \left[1 - \sum_{\xi=0}^{(1-\rho)} C_n^{\xi} \cdot \left(1 - \Phi' \left(\sqrt{\frac{2kE}{nN_0}} \right) \right)^{\xi} \cdot \left(\Phi' \left(\sqrt{\frac{2kE}{nN_0}} \right) \right)^{n-\xi} \right]. \quad (12)$$

На рис. 2 приведены зависимости вероятности декодирования кодограмм в каскадных теоретико-кодовых схемах в каналах с группирующимися ошибками от соотношения энергии ФМ сигнала к спектральной плотности помех при условии оптимального приема полностью известных равновероятных сигналов.

Зависимости на рис. 2 соответствуют случаям:

- 1) без кодирования;
- 2) с применением каскадной теоретико-кодовой схемы и $\rho = 0$ (без внесения ошибок – режим помехоустойчивого кодирования);

3) с применением каскадной теоретико-кодовой схемы и $\rho = 0,3$ (режим слабого внесения ошибок для интегрированного обеспечения информационной скрытности и достоверности);

4) с применением каскадной теоретико-кодовой схемы и $\rho = 0,5$ (режим среднего внесения ошибок для интегрированного обеспечения информационной скрытности и достоверности);

5) с применением каскадной теоретико-кодовой схемы и $\rho = 0,7$ (режим сильного внесения ошибок для интегрированного обеспечения информационной скрытности и достоверности).

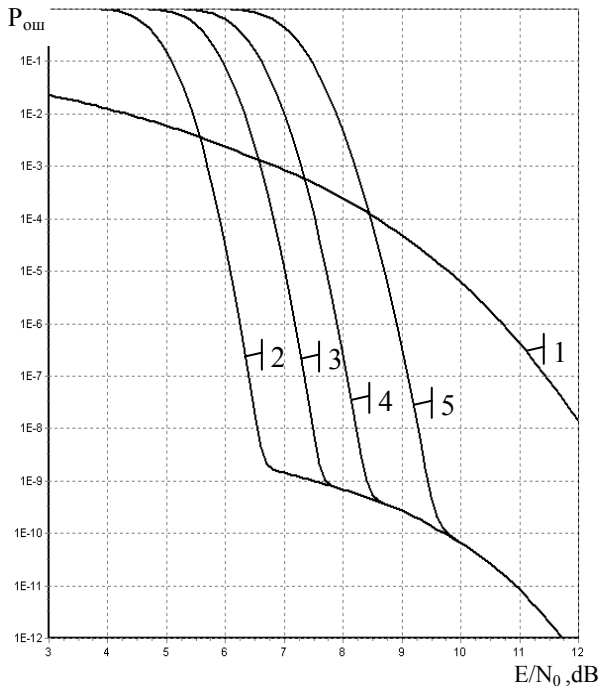


Рис. 2. Зависимости вероятности декодирования кодограмм в каскадных теоретико-кодовых схемах в каналах с группируемыми ошибками

Зависимости, приведенные на рис. 2, соответствуют параметрам каскадной теоретико-кодовой схемы на эллиптических кодах. При построении зависимостей использована рассмотренная выше упрощенная модель Беннета-Фройлиха с непересекающимися пакетами ошибок и возможным их примыканием друг к другу, заданная следующими параметрами: $P_0 = 10^{-3}$ и $I_{cp} = 1 + 10^{-10}$. Анализ зависимостей, приведенных на рис. 2 показывает, что применение каскадных теоретико-кодовых схем позволяет обеспечить передачу кодограмм с показателем потери достоверности $P_{ош} < 10^{-9}$ и получить энергетический выигрыш от кодирования 2,5 – 5, 0 dB в зависимости от режима использования теоретико-кодовых схем для интегрированного обеспечения информационной скрытности и достоверности. В тоже время, сравнительный анализ зависимостей вероятности ошибок, приведенных на рис. 1 и 2 показывает, что даже незначительное группирование

ошибок приводит к снижению энергетического выигрыша от кодирования и, соответственно, к снижению достоверности передачи данных.

Выводы

Проведенные исследования показали, что применение каскадных теоретико-кодовых схем с алгеброгеометрическими кодами на внешней ступени обобщенного каскадного кода позволяет обеспечить высокие вероятностно-временные показатели – предлагаемые конструкции позволяют обеспечить передачу кодограмм с показателем потери достоверности (вероятностью ошибки) $P_{ош} < 10^{-9}$ и получить энергетический выигрыш от кодирования 2,5 – 5,0 dB в зависимости от режима функционирования. Рост показателя группирования ошибок в канале связи приводит к снижению достоверности передачи данных и повышению вероятности ошибочного приема.

Список литературы

1. Блейхут Р. Теория и практика кодов, контролирующих ошибки: Пер. с англ. – М.: Мир, 1986. – 576 с.
2. Злотник Б. М. Помехоустойчивые коды в системах связи. – М.: Радио и связь, 1989. – 232 с.
3. Молдовян Н.А., Молдовян А.А., Еремеев М.А. Криптография: от примитивов к синтезу алгоритмов. – СПб.: БХВ-Петербург, 2004. – 448 с.
4. Шнайер Б. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си. – М.: Издательство ТРИУМФ, 2003. – 816 с.
5. Кузнецов А.А., Грабчак В.И., Евсеев С.П. Каскадные кодовые схемы защиты информации // Системи обробки інформації. – Х.: ХУПС, 2005 – Вип. 9 (49). – С. 206-211.
6. Стасев Ю.В., Кузнецов А.А., Грабчак В.И., Евсеев С.П. Каскадні схеми захисту інформації на алгеброгеометричних кодах // Системи озброєння і військова техніка. – 2006. – Вип. 1 (5). – С. 82-87.
7. Бондарев В.Н., Трестер Г. Цифровая обработка сигналов. – Х., 2001. – 400 с.
8. Кузнецов А.А. Методика оценки эффективности помехоустойчивого кодирования в каналах с группируемыми ошибками // Электронное моделирование. – 2006. – № 3. – С. 49-60.
9. Кузнецов А.А. Методика оценки энергетической эффективности двоичных блоковых кодов в каналах с группируемыми ошибками. // Моделювання та інформаційні технології. – К.: НАНУ, ІПМЕ, 2005. – № 32. – С. 116-124.
10. Кузнецов А.А. Энергетический выигрыш алгеброгеометрического кодирования // Радиотехника: Всеукр. межвед. науч.-техн. сб. – Х.: ХТУРЭ, 2003. – Вып. 134. – С. 218-222.
11. Коррекция ошибок в оптических накопителях информации / А.П. Титикин, В.В. Петров, А.Г. Бабанин. – К.: Наук думка, 1990. – 172 с.

Поступила в редколлегию 13.09.2006

Рецензент: д-р физ.-мат. наук, проф. С.В. Смеляков, Харьковский университет Воздушных Сил им. И. Кожедуба, Харьков.