На правах рукописи

САВЕЛЬЕВ Максим Феликсович

МЕТОД ЗАЩИЩЕННОЙ ПЕРЕДАЧИ ИНФОРМАЦИИ НА ОСНОВЕ КОДОВОГО ЗАШУМЛЕНИЯ

Специальность: 05.13.19 - «Методы и системы защиты информации, информационная безопасность»

Автореферат диссертации на соискание ученой степени кандидата технических наук

Санкт-Петербург - 2003 г.

Работа выполнена на кафедре «Информационная безопасность компьютерных систем» Санкт-Петербургского государственного политехнического университета.

Научный руководитель: Доктор технических наук, профессор, Зегжда Петр Дмитриевич

Официальные оппоненты: Доктор технических наук, профессор Мирончиков Евгений Тимофеевич

Кандидат технических наук, с.н.с. Егоров Владимир Викторович

Ведущая организация: Санкт-Петербургский государственный университет телекоммуникаций (СПбГУТ).

Защита состоится «___» июня 2003 г. в _____ часов на заседании диссертационного совета Д212.229.27 в Санкт-Петербургском государственном политехническом университете по адресу: 195251, Политехническая ул., д.29, Главное здание, ауд. 118.

С диссертационной работой можно ознакомиться в Фундаментальной библиотеке Санкт-Петербургского государственного политехнического университета.

Автореферат разослан «___» мая 2003 г.

Ученый секретарь
диссертационного совета Платонов В. В.

Общая характеристика работы

Актуальность. В настоящее время вычислительные и телекоммуникационные системы, в том числе и сети радиосвязи, используются практически во всех сферах народного хозяйства, существенно повышая производительность труда работников. Однако известно, что более 80% компаний и агентств несут убытки из-за различных нарушений конфиденциальности и целостности данных, используемых в этих системах. Поэтому проблема защиты информации практически во всех вычислительных и телекоммуникационных системах становится все более актуальной. Само понятие защиты информации является весьма многогранным и включает различные аспекты, но в диссертационной работе рассматриваются только вопросы защиты информации, передаваемой по каналам связи, от перехвата технически оснащенным противником.

Для обеспечения конфиденциальности передаваемой информации в основном используются методы криптографии, но существуют случаи, когда достичь этого можно без применения криптографических методов. Такие альтернативные методы были предложены многими исследователями: А. Вайнером, В.А.Яковлевым, В.И. Коржиком, Е.Т. Мирончиковым и др. Например, метод А.Вайнера основан на достижениях теории информации и кодирования и позволяет при определенных условиях обеспечить надежную передачу конфиденциальных сообщений по открытым каналам связи. Необходимый уровень защиты конфиденциальных сообщений в этом случае обеспечивается не за счет воздействия на параметры каналов утечки информации, а за счет вероятностного кодирования при передаче и необходимого декодирования при приеме сообщений. В основе метода Вайнера лежит предположение, что канал утечки имеет более низкое качество, чем канал легитимных пользователей. При выполнении этого предположения вероятностное кодирование и декодирование в каналах связи обеспечивает на приемнике перехватчика увеличение количества ошибок, создающее эффект зашумления передаваемых сообщений.

Диссертационная работа базируется на трудах Яковлева В.А., Мирончикова Е.Т., Коржика В.И. и других и посвящена задаче разработки метода передачи конфиденциальной информации по открытым каналам на основе кодового зашумления. Принципиальным преимуществом метода кодового зашумления является совершенная секретность в теоретико-информационном смысле, что позволяет использовать данный метод при любых предположениях о вычислительных возможностях перехватчика.

Цель работы состоит в разработке метода вероятностного кодирования и декодирования информации в вычислительных и телекоммуникационных системах и сетях связи для обеспечения повышенной степени защиты конфиденциальных сообщений при передаче по открытым каналам.

Для достижения поставленной цели в работе решались следующие задачи:

1. Построение и исследование математической модели системы передачи конфиденциальных сообщений по незащищенным каналам связи с перехватом.
2. Разработка метода кодового зашумления и системы передачи конфиденциальных сообщений на основе кодов Рида-Соломона.
3. Разработка алгоритмов вероятностного кодирования и декодирования, включая быстрые алгоритмы восстановления сообщений из принятых синдромов-сообщений.
4. Оценка вероятностей успешного перехвата конфиденциальных сообщений при использовании разработанного метода передачи на основе кодового зашумления.
5. Разработка рекомендаций по применению предложенного метода кодового зашумления.

Методы исследования: для решения поставленных задач использовались методы теории информации, теории кодирования, методы линейной алгебры для расширенных полей характеристики два, методы комбинаторики и теории вероятности.

Научная новизна диссертационной работы состоит в следующем:

1. Предложен метод кодового зашумления для кодов с большим основанием, позволяющий передачу секретных сообщений без применения криптографии.
2. Предложен алгоритм быстрого восстановления переданной информации из принятой последовательности с кодовым зашумлением.
3. Разработана система передачи конфиденциальных сообщений по открытому каналу с шумом при наличии перехватчика.
4. Вычислены оценки вероятности успешного перехвата правильного сообщения противником и оценки достоверности доведения информации по основному каналу до законного пользователя.

Практическая ценность работы подтверждается возможностью использования полученных результатов для систем передачи конфиденциальных сообщений и актами о внедрении полученных результатов в части передачи конфиденциальных сообщений по открытым каналам с кодовым зашумлением от ЦНИИ РТК и Московского Федерального

государственного предприятия Аттестационный центр "Желдоринформзащита МПС РФ", в учебном процессе СПбГУТ. На основе результатов диссертационной работы были разработаны учебно-методические материалы, используемые для подготовки специалистов на кафедре «Информационная безопасность компьютерных систем» СПбГПУ.

Основные положения, выносимые на защиту:

1. Метод кодового зашумления на основе использования кодов Рида-Соломона для вычислительных и телекоммуникационных систем и сетей связи, в которых все используемые каналы, включая каналы перехватчика, являются каналами с шумом.
2. Алгоритм быстрой обработки принятой из канала последовательности-синдрома после коррекции ошибок и снятия кодового зашумления с целью восстановления переданной информации.
3. Система передачи конфиденциальных сообщений с вероятностным кодированием по открытому каналу с перехватом, характеристики которой оцениваются по критерию вероятности успешного перехвата.
4. Методика расчета оценки вероятности успешного перехвата правильного сообщения противником и оценки достоверности доведения сообщения получателю по основному каналу..

Публикации. По теме диссертации опубликовано 9 научных статей и докладов.

Объем и структура работы. Диссертационная работа состоит из введения, четырех глав, заключения и списка использованной литературы из 65 наименований.

Содержание работы

В первой главе рассматриваются проблемы передачи конфиденциальных сообщений по незащищенным каналам связи при наличии перехватчика и проводится анализ систем передачи. На основании проведенного анализа разработана математическая модель системы передачи по незащищенным каналам с перехватом, получены и проанализированы математические соотношения, связывающие параметры системы передачи с ее характеристиками. Модель канала с перехватом приведена на рис.1.

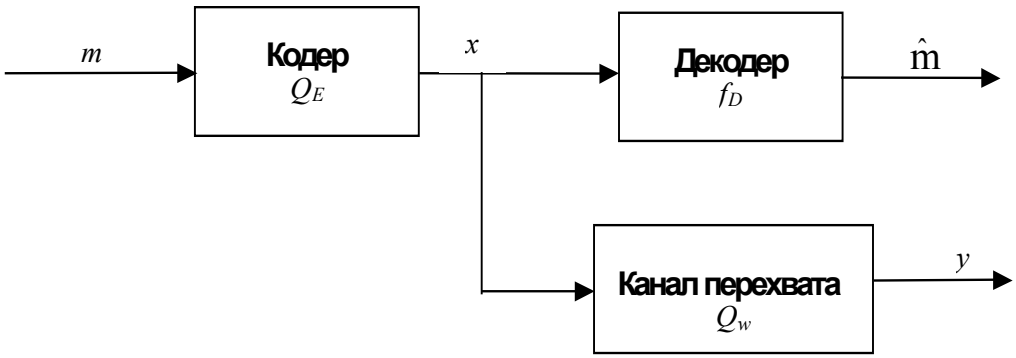

Рис. 1. Модель канала с перехватом.

Источник информации генерирует последовательность символов из двоичного алфавита D = \{0,1\}. Сообщениями являются блоки двоичных символов $M = (m_1, m_2, ..., m_k) \in D^k = \mathcal{M}$. Эти сообщения являются случайными величинами с равномерным распределением вероятностей

$$P_{\mathcal{M}}(M) = 2^{-k},\ M \in Dk.$$

Оба канала (основной и перехватчика) имеют двоичные входные алфавиты и двоичные выходные алфавиты, причем входные алфавиты обоих каналов совпадают и обозначаются буквой $\Omega = \{0, 1\}$, а выходной алфавит перехватчика буквой $\mathcal{Y} = \{0, 1\}$. Кодирующее устройство отображает каждое сообщение $m = = (m_1, m_2, ..., m_k)$ в некоторое кодовое слово $x = (x_1, x_2, ..., x_n)$, принадлежащее множеству Ω^n, где $k < n$.

Декодер основного канала (легальный приемник) осуществляет отображение f_D: $\Omega^n \to D^k$, вычисляя оценку $\hat{m} = f_D(x)$ соответствующего блока источника.

Математическая модель разрабатывалась и исследовалась с целью поиска путей обобщения метода передачи с кодовым зашумлением на случай основного канала с шумом. В данной модели канала с перехватом рассматривается единственный отправитель сообщений и несколько получателей (такая модель рассматривается как модель широковещательного канала). При исследовании модели широковещательного канала главная проблема заключалась в организации передачи информации от передатчика ко всем приемникам с максимально возможными скоростями передачи. В канале с перехватом модель системы передачи аналогична, но главным отличием является то, что необходимо достичь возможно большей скорости передачи от отправителя к законному получателю при условии, что другие приемники могут получать информацию с незначительной скоростью.

Анализ работы системы передачи информации по каналам с перехватом в терминах теории информации показывает, что методы передачи сообщений с кодовым зашумлением относятся к классу совершенно секретных криптографических систем по К. Шеннону, так как средняя взаимная информации между переданными сообщениями и принятыми перехватчиком сигналами равна нулю.

В математической модели передаваемые сообщения являются синдромами, которые определяются используемым линейным кодом. При использовании линейных кодов для вероятностного кодирования все пространство последовательностей разбивается на смежные классы по некоторому линейному коду.

$$P\left(C_s,\varepsilon\right)=\sum_{e\in C_s}\varepsilon^{w(e)}\left(1-\varepsilon\right)^{n-w(e)},$$

где $w(e)$ — вес Хемминга вектора e, ε – вероятность ошибки в основном канале, C – код, s – синдром, n- длина кода.

Смежные классы характеризуются своими спектрами (количеством последовательностей с заданным весом Хемминга). Каждому смежному классу сопоставляется единственное сообщение и для его передачи используется любая последовательность из этого класса. Если перехватчик получает эту последовательность из канала без единой ошибки, то он прочитает сообщение, так как сможет определить номер смежного класса. Вероятность таких событий называется вероятностью успешного перехвата. В работе найдено соотношение, связывающее вероятность успешного перехвата со спектральными свойствами используемых кодов. Разработана методика выбора параметров используемого кода таким образом, чтобы вероятность успешного перехвата была сделана сколь угодно малой.

В работе рассмотрены методы вычисления вероятностей смежных классов для используемого вероятностного кодирования в канале с перехватом и некоторые схемы оптимального декодирования сообщений перехватчиком. Показано, что вероятность успешного перехвата совпадает с вероятностью самого линейного кода. Эту вероятность обозначим через $P(C,\varepsilon)$, где C - множество кодовых слов, а ε - вероятность ошибки в канале. Показано, что вероятность успешного перехвата складывается из вероятности безошибочной передачи по каналу перехвата и суммы вероятностей того, что набор ошибок в этом канале совпадет с некоторым кодовым словом из кода C. Другими словами, вероятность успешного перехвата определяется выражением

$$P(C,\varepsilon)=(1-\varepsilon)^n+P\left(e\in C\setminus 0\right),$$

где n – длина слов используемого кода.

Благодаря тому, что для величины $P_{ud}(C,\varepsilon) = P(e \in C \setminus 0)$ определено множество границ, в работе выведены формулы для оценки вероятности успешного перехвата.

Рассмотрены оценки меры неопределенности (нормированной условной энтропии), которую имеет перехватчик при использовании в основном канале вероятностного кодирования. Показано, что вычисление условной энтропии сообщений сводится к вычислению энтропии на множестве синдромов. Но так как распределение весов Хемминга в используемом коде, как правило, неизвестно, то приходится для этой энтропии использовать различные оценки сверху и снизу.

$$H(S) \geq -\log P(C, \varepsilon)$$

На основе анализа математической модели сформулирована решаемая в диссертации научная задача, которая формализуется следующим образом: разработать метод передачи конфиденциальной информации по незащищенным каналам связи с шумом при достаточно низкой сложности реализации, гарантирующий сколь угодно малую вероятность успешного перехвата и сколь угодно малую вероятность ошибки в канале легитимных пользователей.

Во второй главе проведен анализ выбора кодов для реализации общего метода передачи информации на основе кодового зашумления. В результате исследования функциональных зависимостей основных параметров показано, что для конструктивного метода кодового зашумления необходимо использовать достаточно “технологичные” коды, то есть такие коды, которые могут быть построены для любых значений параметров (длины кода, скорости передачи и минимального кодового расстояния Хемминга) и для которых существуют простые способы вычисления спектров. Этим условиям удовлетворяют коды Рида-Соломона, задаваемые над достаточно большими конечными полями. Поэтому для разработки метода кодового зашумления в работе использованы коды Рида-Соломона.

В работе предложено использовать код Рида–Соломона над полем $GF(2^m)$ длины n, $0 < n <= 2^m - 1$, с k информационными символами и минимальным кодовым расстоянием $d = n - k + 1$. Данные коды имеют эффективные алгоритмы исправления ошибок. Построим для используемого кода порождающую и проверочную матрицы, которые обозначим через G и H, соответственно. Порождающая матрица имеет размер k x n, а проверочная матрица имеет размер $(n - k)$ x n.

Для построения системы передачи проведем предварительные преобразования, позволяющие представить порождающую матрицу в следующем виде:

$$G(p(x)) = \begin{bmatrix} 1 & \dots & p(x) \\ \dots & 1 & \dots \\ \dots & \dots & 1 \end{bmatrix}$$

где все элементы на главной диагонали равны единице, а в правом верхнем углу расположен полином, который имеет минимальную степень среди всех полиномов, которые могут быть получены элементарными преобразованиями матрицы. Результат таких преобразований позволяет разбить матрицу G на две части, которые будем называть ступенями кода. Тогда определим порождающую и поверочную матрицу для каждой из полученных ступеней. Для кода первой ступени порождающую матрицу обозначим через G_1 (она имеет размер kXn, где $k_1 < k$). Для этой порождающей матрицы находим проверочную матрицу, обозначаемую H_1. Порождающую матрицу кода второй ступени обозначим через G_2. Для этой порождающей матрицы проверочной будет проверочная матрица исходного кода. Причем проверочная матрица для порождающей матрицы G_2 может быть получена из матрицы H вычеркиванием первых k_1 столбцов. Тогда каждое сообщение от отправителя А к получателю В является линейной комбинацией строк матрицы G_2, а коэффициенты этой линейной комбинации представляют собой передаваемые информационные символы.

Кодовые слова, порожденные матрицей G_1, предназначены для кодового зашумления передаваемых сообщений по основному каналу связи от отправителя А к получателю В. Таким образом, к передаваемому сообщению необходимо добавлять кодовое слово кода первой ступени, выбранное в соответствии с равномерным распределением на множестве всех кодовых слов кода первой ступени. Генераторный полином кода первой ступени имеет степень $(n - k_1)$. Корни генераторного полинома имеют вид α^h, α^{h+1}, ..., α^{h+n-k_1-1}, где α— примитивный элемент поля $GF(2^m)$. Этот код имеет минимальное кодовое расстояние $d = n - k_1 + 1$. Таким образом, преобразования исходной матрицы заключаются в том, чтобы выбрать порождающую подматрицу G_1, генерирующую кодовые слова с минимальным расстоянием Хемминга $d = n - k_1 + 1$ и выше.

Если в основном канале в процессе передачи ошибок не произошло, то для того, чтобы снять кодовое зашумление, достаточно умножить принятую последовательность на проверочную матрицу H_1 кода первой ступени. Тогда сообщениями, передаваемыми по основному каналу, являются кодовые слова, принадлежащие коду второй ступени. Число возможных различных сообщений равно $2^{m(k-k_1)}$. Все возможные сообщения, а также кодовые слова, используемые для кодового зашумления, являются кодовыми словами исходного кода с порождающей матрицей G.

Для реализации метода разработаны алгоритмы обнаружения и исправления ошибок, основанные на использовании синдромов и представляющие практический интерес для построения любой конкретной системы с вероятностным кодированием.

С целью сравнения сложности реализации алгоритмов исправления ошибок в качестве примеров приведены некоторые распространенные методы исправления ошибок. Представленные результаты описывают кодовые конструкции и алгоритмы декодирования, необходимые для реализации предлагаемого метода кодового зашумления.

В третьей главе предлагается общий метод организации кодового зашумления и реализации вероятностного кодирования, включая алгоритмы обработки принятых сигналов на приемной стороне и методы быстрого восстановления переданных сообщений.

Для решения задачи выделения информационных символов вычисляется аналог псевдообратной матрицы для матрицы B, составленной из базисных векторов слова-синдрома. Чтобы преодолеть трудности вычислений псевдообратных матриц в конечных полях большой размерности, в матрице B базисных векторов размера $(b \times c)$ все элементы представляются как полиномы от переменной x с коэффициентами из поля $GF(2)$.

$$L_k(x) = \begin{bmatrix} L_{1,1}(x) & L_{1,2}(x) & \ldots & L_{1,c}(x) \\ L_{2,1}(x) & L_{2,2}(x) & \ldots & L_{2,c}(x) \\ .. & .. & \ldots & .. \\ L_{b,1}(x) & L_{b,2}(x) & \ldots & L_{b,c}(x) \end{bmatrix}.$$

Полученную матрицу обозначим $L_k(x)$. Матрицу $L_k(x)$ можно представить в следующей форме

$$L_k(x) = A(x)F(x)B(x),$$

где $A(x)$ и $B(x)$ матрицы размеров $(b \times b)$ и $(c \times c)$ соответственно с единичными детерминантами, а матрица $F(x)$ - диагональная матрица размера $(b \times c)$. Элементами диагональной матрицы $F(x)$ являются полиномы. Используя это разложение, можно найти псевдообратную матрицу $L_k^{-1} = B^{-1}(x)F^{-1}(x)A^{-1}(x)$. Переходя к элементам используемого конечного поля, из матрицы $L_k^{-1}(x)$ получаем псевдообратную матрицу B^{-1}. Таким образом, операция восстановления информационных символов из принятого слова-синдрома сводится к умножению сообщения- синдрома на псевдообратную матрицу B^{-1}.

В работе показано, что при реализации описанного метода передачи на основе кодового зашумления у противника появляется возможность проведения атаки, направленной на снятие кодового зашумления без вычисления синдрома. Действительно, может оказаться, что матрица, составленная из строк порождающей матрицы кода второй ступени, содержит нулевую подматрицу размера ((k-r) x r) или меньше. Если порождающая матрица кода второй ступени содержит указанную нулевую подматрицу, то противник попытается исследовать соответствующие символы кодового слова, содержащие только символы кодового зашумления. Если окажется, что в процессе передачи по каналу эти символы были безошибочны, то противник может снять кодовое зашумление и получит доступ к самому сообщению, а не синдрому этого сообщения. Это может скомпрометировать конфиденциальность переданного сообщения. Чтобы избежать возможной атаки такого рода при вероятностном кодировании, полученном с помощью двухступенчатой порождающей матрицы, следует отдельно проверить указанное свойство порождающей подматрицы кода второй ступени.

Предложенный метод передачи информации на основе кодового зашумления достаточно прост для реализации даже при достаточно длинных кодах Рида-Соломона и практически исключает возможность перехвата.

В четвертой главе рассмотрены методы расчета вероятностных характеристик системы передачи конфиденциальных сообщений по открытым каналам. Для оценки характеристик системы передачи конфиденциальных сообщений по открытому каналу с перехватом разработана методика расчета оценок вероятности успешного перехвата и достоверности полученной информации

Поскольку система базируется на кодах Рида–Соломона, то символы, которыми оперируют все участники рассматриваемой модели, являются элементами конечного поля $GF(2^r)$. Поэтому для оценки вероятности успешного перехвата наибольший интерес представляет вопрос о безошибочности символов. Сама величина ошибки интереса не представляет, так как любое значение неисправленной ошибки приводит к безуспешному перехвату. Поэтому в работе рассматривается случай, когда сигнал передается без ошибок и передача происходит в основном канале с вероятностью $(1-\varepsilon)^r$, а в канале перехвата с вероятностью $(1-\beta)^r$, где ε и β соответственно вероятности ошибки на двоичный символ в основном канале и канале перехвата. Тогда вероятности того, что символы кода Рида–Соломона будут искажены, равны $1-(1-\varepsilon)^r$ и $1-(1-\beta)^r$ для каждого из рассматриваемых каналов соответственно. Таким образом, несмотря на то, что значения символов кода Рида–Соломона берутся из поля $GF(2^r)$, качество передачи основного канала и возможности перехватчика определяются только двумя величинами —

вероятностью правильного приема и вероятностью неправильного приема, которые в сумме дают единицу. Для оценки вероятности успешного перехвата в рассматриваемой модели канала нужно определить необходимое число исправляемых ошибок в используемом коде основного канала. Для достаточно больших n число исправляемых ошибок может быть представлено гауссовским распределением.

Для увеличения различия между вероятностями ошибки на символ в основном канале и канале перехватчика законные пользователи перед посылкой сообщения должны провести дополнительные операции. В соответствии с этими операциями отправитель получает от получателя случайную последовательность по основному каналу, а затем отправляет получателю поразрядную сумму передаваемого сообщения и принятой случайной последовательности по безошибочному каналу. В качестве безошибочного канала можно использовать тот же основной канал в сочетании с некоторым избыточным кодированием, которое, конечно, считается известным перехватчику. Пересылки всех сигналов контролируются перехватчиком, но в результате даже при оптимальной обработке сигналов перехватчик получит сообщение с набором возможных ошибок, вероятности появления которых соответствуют каскадному соединению основного канала и канала перехватчика. Таким образом, канал перехватчика всегда будет иметь вероятность ошибки $\beta = \varepsilon(1-\delta) + \delta(1-\varepsilon)$, где ε и δ переходные вероятности ошибки в основном канале и канале перехватчика. В этом случае состояние перехватчика отличается тем, что он получает свое сообщение по каналу, в котором вероятность ошибки на символ больше, чем вероятность ошибки на символ в канале законного пользователя. Это различие в дальнейшем усиливается за счет кодового зашумления с увеличением общей длины кодового слова используемого кода и ограничением числа исправляемых ошибок.

В рассматриваемом случае легитимные пользователи обменялись некоторой открытой информацией (случайной последовательностью) по незащищенному каналу. Процедура передачи конфиденциальной информации по открытому каналу с предварительным обменом открытыми сообщениями по незащищенному каналу называется процедурой согласования секретного ключа путем открытого обсуждения общей информации. При открытом обсуждении общей информации по открытому каналу секретная пропускная способность $C(\varepsilon,\delta)$ всегда положительна и равна

$$C(\varepsilon,\delta) = h(\varepsilon+\delta-2\cdot\varepsilon\cdot\delta) - h(\varepsilon),$$

где ε и δ вероятности ошибки в основном канале и канале перехвата, а *h(.)* – функция двоичной энтропии.

В работе рассмотрены зависимости между параметрами каналов, секретной пропускной способностью и параметрами кодов Рида-Соломона. Результаты расчетов представлены в табл.1, где ε - вероятность ошибки на символ в основном канале, δ - вероятность ошибки на символ в канале перехватчика, $C(\varepsilon,\delta)$-секретная пропускная способность канала с открытым обсуждением общей информации, 2^r –мощность конечного поля, n- длина кода Рида –Соломона и R- скорость используемого кода.

Таблица 1.

ε	δ	$C(\varepsilon,\delta)$	2^r	n	R
0.000001	0.000001	0.0000194	2^{16}	65533	0.0000153
0.00001	0.00001	0.000161	2^{13}	8191	0.000122
0.0001	0.0001	0.001273	2^{13}	8191	0.00122
0.0001	0.0002	0.00247	2^{13}	8191	0.00244
0.0001	0.0003	0.003618	2^{10}	1023	0.00293
0.001	0.0001	0.000987	2^{10}	1023	0.000978
0.001	0.0002	0.001962	2^{9}	511	0.001957
0.001	0.0003	0.002934	2^{10}	1023	0.00293
0.01	0.0001	0.000649	2^{11}	2047	0.000489
0.01	0.0002	0.001297	2^{12}	4095	0.00122

Для создания системы передачи с параметрами, указанными в табл.1, достаточно выбрать неприводимый полином над полем GF(2) подходящей степени, а все остальное - конструкция вероятностного кодирования, алгоритмы исправления ошибок и восстановления информационных символов могут быть выполнены программными средствами в соответствии с разработанными рекомендациями. Реальными затратами в процессе эксплуатации являются только затраты времени на передачу информации в обоих направлениях по основному каналу. Эти затраты времени зависят от объемов передаваемой открытой и конфиденциальной информации и могут составлять от долей секунд до нескольких минут.

Методика расчета вероятности успешного перехвата и достоверности доведения сообщения по основному каналу в системе передачи на основе предложенного метода сводится к задаче оценки “хвостов” биномиальных распределений, основанной на экспоненциальной границе Чернова. Параметры этих биномиальных распределений зависят от свойств каналов связи и параметров используемых кодов Рида-Соломона. Обычно применить границу Чернова для оценки требуемых вероятностей довольно

трудно, но в данной задаче возможность использования границы Чернова является следствием особенностей алгебраической структуры кодов Рида-Соломона, которая позволяет легко вычислить спектры используемого кода.

Для оценки вероятности успешного перехвата (и вероятности ошибки в основном канале) в работе использовалась граница Чернова, применение которой позволяет оценить вероятность успешного перехвата сообщения противником и вероятности правильного приема в основном канале

$$\left[\left(\frac{p}{d}\right)^{d}\left(\frac{1-p}{1-d}\right)^{1-d}\right]^{n} = e^{-Xn} \geq \begin{cases} P\left[\frac{1}{n}\sum_{i=0}^{n} x_i \geq d\right], & 1 \geq d > p, \\ P\left[\frac{1}{n}\sum_{i=0}^{n} x_i \leq d\right], & 0 \leq d < p. \end{cases}$$

Расчетные значения параметров биномиальных распределений представлены в табл.2, где β - вероятность ошибки на символ каскадного соединения двух каналов, а P_0 и P - вероятности ошибки для символов кода Рида-Соломона в основном канале и канале перехвата соответственно.

Таблица 2.

ε	δ	$\beta = \varepsilon + \delta - 2\cdot\varepsilon\cdot\delta$	2^r	$P_0=1-(1-\varepsilon)^r$	$P=1-(1-\beta)^r$
0.00001	0.00001	$1.99998\ 10^{-5}$	2^{20}	0.0002	0.0004
0.00001	0.00002	$2.99996\ 10^{-5}$	2^{20}	0.0002	0.0006
0.00001	0.00003	$3.99994\ 10^{-5}$	2^{20}	0.0002	0.0008
0.0001	0.0001	0.00019998	2^{20}	0.001998	0.003992
0.0001	0.0001	0.00019998	2^{17}	0.001699	0.003394
0.0001	0.0002	0.00029996	2^{17}	0.001699	0.005087
0.0001	0.0003	0.00039994	2^{17}	0.001699	0.006777
0.001	0.001	0.001998	2^{15}	0.014895	0.029554
0.001	0.002	0.002996	2^{15}	0.014895	0.04401
0.001	0.003	0.003994	2^{15}	0.014895	0.057826

Используемая граница Чернова для оценки “хвостов” биномиальных распределений дает обычно гораздо более точный результат, чем другие формы закона больших чисел.

Итоговые результаты представлены в табл.3.

Таблица 3.

P	P_0	d	X	n	nX	t
0.0004	0.0002	0.0003	$5.9475\ 10^{-6}$	10485575	6.2	314
0.0006	0.0002	0.0004	$1.6423\ 10^{-5}$	10485575	17.2	419
0.0008	0.0002	0.0005	$2.8231\ 10^{-5}$	10485575	29.6	524
0.003992	0.001998	0.002995	$5.9445\ 10^{-5}$	10485575	62.3	3140
0.003394	0.001699	0.002546	$5.0532\ 10^{-5}$	131071	6.6	333
0.005087	0.001699	0.003393	0.0001396	131071	18.2	444
0.006777	0.001699	0.004238	0.00024011	131071	31.4	555
0.029554	0.014895	0.022225	0.0004441	32767	14.5	728
0.057826	0.014895	0.03658	0.0021299	32767	69.7	143

В этой таблице символ d обозначает долю исправляемых ошибок от длины кодового слова кода Рида-Соломона, X-значение показателя границы Чернова, показатель экспоненты в границе Чернова равен произведению nX (оценка вероятности успешного перехвата имеет вид 10-Xn), а t- число исправляемых ошибок.

Приведенные расчетные данные показывает, что разработанные и исследованные метод и система защищенной передачи информации на основе кодового зашумления по открытым каналам связи обеспечивает практически сколь угодно малую вероятность успешного перехвата сообщения противником. Основными инструментами, позволяющим создать рассматриваемый метод, являются конструкции кодов Рида-Соломона. Именно существование таких кодов для любых требуемых значений параметров и простота вычисления спектров этих кодов позволяют решить поставленную задачу.

Однако скорость передачи конфиденциальных сообщений в рассмотренных моделях остается весьма низкой. По-видимому, такая низкая скорость передачи является некоторой “платой” за возможность защищенной передачи. Вопросы повышения скорости передачи в общих каналах связи с перехватом являются задачей дальнейших исследований.

В качестве примера приведено применение метода кодового зашумления в радиорелейных линиях связи.

В работе получены следующие основные результаты:

1. Для систем передачи информации по каналам связи без шума при наличии перехватчика разработана математическая модель, связывающей характеристики системы передачи с параметрами каналов связи и характеристики используемых кодов в схеме кодового зашумления.

2. На основе анализа математических зависимостей сделан вывод о необходимых свойствах кодов, пригодных для получения практичного метода передачи конфиденциальных сообщений на основе кодового зашумления.
3. Разработан метод и система защищенной передачи конфиденциальной информации по открытым каналам на основе кодового зашумления, использующий согласованный выбор параметров кодов Рида-Соломона для обеспечения необходимых вероятностных характеристик безопасности и достоверности.
4. Предложенный метод реализован в виде двухступенчатой схемы вероятностного кодирования и декодирования кодами Рида-Соломона и схемы снятия зашумления, которая включает алгоритм быстрого восстановления информационных символов из принятого синдромного сообщения.
5. Получены оценки вероятности ошибки в основном канале и вероятности успешного перехвата сообщений при предложенном способе вероятностного кодирования, характеризующих степень защиты конфиденциальных сообщений.

Основные результаты диссертации изложены в 9 печатных работах.

1. Курицын К.А., Савельев М.Ф., Открытое обсуждение при согласовании секретного ключа //Сб.тезисов конференции «Методы и технические средства обеспечения безопасности информации», СПбГТУ, 2001 г., С.93-94.

2. Курицын К.А., Савельев М.Ф., Согласование секретного ключа через открытый канал //Проблемы информационной безопасности. Компьютерные системы, № 3, 2001 г., С.39-43.

3. Савельев М.Ф. Линейные коды в каналах с перехватом //Проблемы информационной безопасности. Компьютерные системы, №2, 2002 г., С.47-51.

4. Савельев М.Ф., Дешифрация сообщений по базисным элементам // Сб.тезисов конференции «Методы и технические средства обеспечения безопасности информации», СПбГТУ, 2002 г., С.104-107.

5. Савельев М.Ф. Восстановление сообщений по базисным элементам //Сб.тезисов конференции «Информационная Безопасность Регионов России-2002», СПб, 2002 г., С.39-43.

6. Савельев М.Ф. Анализ сообщений по базисным элементам //Сб.тезисов конференции “Проблемы информационной безопасности в системе Высшей школы”, МИФИ, 2003 г., 105 с.

7. Савельев М.Ф. Защищенная передача сообщений по открытому каналу //Проблемы информационной безопасности. Компьютерные системы, №2, 2003 г., С.92-96.

8. Савельев М.Ф. Оценка вероятности успешного перехвата в каналах с кодовым зашумлением //Проблемы информационной безопасности. Компьютерные системы, №2, 2003 г., С.97-101.

9. Савельев М.Ф. О скорости передачи информации в системе радиорелейной связи с кодовым зашумлением //Проблемы информационной безопасности. Компьютерные системы, №2, 2003 г., С.101-105.