С. А. Осмоловский (Москва, ООО «Стокос»). **Принципы восстановления целостности информации кодовыми методами.**

Проблема обеспечения целостности информации в информационно-телекоммуникационных системах (ИТКС) является одной из важнейших, так как потребитель, получивший сообщение, должен быть уверен, что это сообщение идентично по содержанию отправленному и отправлено тем абонентом, который указан в реквизитах сообщения. В противном случае обесценивается смысл применения этой ИТКС.

Поэтому в современных ИТКС применяются средства обеспечения (контроля) целостности в виде электронной цифровой подписи или имтовставки, которые могут только выявить факт «недоверия» к сообщению или части его, требующим повторной передачи «забракованного» массива. Методы контроля целостности строятся на формировании избыточной комбинации без преобразования информационной части контролируемого сообщения. Длина ключа для известных методов контроля целостности значительно короче длины проверяемого сообщения. Вероятность ошибки при проверке целостности зависит от числа ключей и не может иметь строгой оценки.

Известны стохастические (n, k)-коды с обнаружением ошибки [1], использующие стохастическое преобразование кодовых блоков на длине n, и обладающие следующими основными свойствами:

— после кодирования со стохастическим преобразованием всего кодового блока поступающая в канал информация имеет квазислучайный характер;

— после любого искажения в канале и выполнения обратного стохастического преобразования имеет с равной вероятностью любое из $2^n - 1$ возможных (кроме передаваемого) исходных значений по правилам q-ичного симметричного канала ($q = 2^n$);

— вероятность необнаруженной ошибки зависит только от числа избыточных символов $r = n - k$ и числа искаженных кодовых блоков и независимо от порядка введения избыточности (вида кода) равна: $P_{\text{ош}} = P_{\text{иск}}(2^k - 1)/(2^n - 1) < 2^{-(n-k)}$, где $P_{\text{иск}}$ — вероятность искажения блока в канале.

Сформулируем понятие восстановления целостности информации без повторной передачи и оценим возможность решения такой задачи.

Под кодовым восстановлением целостности информации будем понимать обработку информации после ее искажения в произвольном канале при обеспечении требуемой достоверности восстановления, устанавливаемой выбором параметров кодовой конструкции, без повторной передачи информации.

Сформулируем задачу для кодового восстановления целостности информации.

Как любое восстановление целостности кодовое восстановление должно обладать двумя важнейшими свойствами.

1. Использование в каналах с произвольным законом распределения ошибок.

2. Должна быть контролируемая и задаваемая при проектировании (нормируемая) степень надежности и достоверности восстановления целостности, оцениваемые вероятностями успешного (полного) восстановления и наличия ошибки в восстановленном сообщении.

При рассмотрении методов кодового восстановления целостности информации будем исходить из сложившейся традиции рассматривать восстановление целостности как двухэтапного процесса, на первом из которых осуществляется контроль целостности в виде выделения правильно принятых элементов (символов) кода.

Естественным вариантом кодового восстановления целостности информации является применение каскадного кода, имеющего на первой ступени код с обнаружением ошибок и код Рида–Соломона на второй ступени, обеспечивающий исправление стертых на первой ступени кодовых блоков с обнаруженными ошибками. Однако такой каскадный код имеет очевидный недостаток в виде большой кодовой избыточности.

Можно использовать идею неполного декодирования, когда исправление ошибок выполняется только при кратности ошибки t, а при кратности ошибки $t+1$ и выше выполняется обнаружение ошибок [2].

Вопрос состоит в том, чтобы при декодировании очередного блока выбрать надежный критерий использования режима либо исправления, либо обнаружения ошибок.

Кодовое восстановление целостности информации строится на следующих принципах.

1. Сохранить использования принципа обнаружения ошибок, который может иметь гарантированную в произвольном канале верхнюю границу для вероятности ошибки декодирования в q-ичном симметричном канале.

2. Использовать в качестве основы для режима обнаружения ошибки проверочной матрицу двоичного (n,k)-кода с кодовым расстоянием d, обычно применяемого для исправления ошибок по критерию максимума правдоподобия.

3. Построить процесс исправления ошибок как двухэтапный с выделением (локализацией) правильно принятых символов с помощью многократного обнаружения ошибки по отдельным подмножествам символов кода и последующим исправлением в качестве стираний остальных символов, воспринимаемых как искаженные символы, так как они не объявлены неискаженным, или отказом от декодирования при кратности ошибки, превышающей исправляющую способность кода (обнаружение неисправимых ошибок).

4. Использовать при выделении неискаженных символов только выполнившихся проверочных соотношений (построение алгоритма декодирования как алгоритма правильных проверок, т. е. принцип обнаружения ошибок).

5. Использовать все возможные ненулевые $2^{n-k}-1$ проверочные соотношения исходного двоичного (n,k)-кода для единообразного выделения менее чем $d-1$ неискаженных символов, проверки условия исправления или обнаружения неисправляемых ошибок и возможности обнаружения ошибочной локализации.

6. Для обеспечения требуемой вероятности ошибки декодирования в произвольном канале использовать следующие приемы:

— код с обнаружением ошибок строить как ансамбль кодов, сменяемых, как при использовании имитовставки, за счет начальных установок (ключа);

— применить свойства q-ичного симметричного канала (преобразования q-ичных символов)

— применять за счет l-перемежения двоичного кода такой размер q-ичного символа ($q=2^l$), чтобы соблюдалось условие для верхней границы вероятности ошибки: $P_{\text{ош}} \leqslant q^{-1}$.

Предлагаемую сигнальную конструкцию можно одновременно рассматривать как помехоустойчивый код с исправлением ошибок, для которого можно провести сопоставление с другими кодами, аналогичными по применению (коды Хэмминга, Боуза–Чоудхури–Хоквингема, Рида–Соломона и пр.) по параметрам кодов [3]:

— число исправляемых ошибок; стохастический код исправляет $t=d^{-2}$ искаженных q-ичных символов, где d — кодовое расстояние исходного двоичного кода;

— вероятность ошибки после декодирования в конкретном канале связи; код при исправлении $t \leqslant d-2$ искаженных символов, вероятность ошибки декодирования после выполнения операций проверки правильности локализации имеет верхнюю границу $P_{\text{ош}} \leqslant q^{-(d-t-1)}$;

— код для восстановления целостности имеет низкую сложность реализации из-за двоичных операций декодирования, число которых с ростом q не растет, а уменьшается.

Для использования средств восстановления целостности информации в протоколе канального уровня, вписывающегося в стек протоколов ИТКС, создано программное

обеспечение драйвера под операционной системой Linux, решающее одновременно ряд задач защиты информации [4].

Работа выполнена при поддержке РФФИ проект № 06-07-89170.

СПИСОК ЛИТЕРАТУРЫ

1. *Коржик В. И.*, *Осмоловский С. А.*, *Финк Л. М.* Универсальное стохастическое кодирование в системах с решающей обратной связью. — Проблемы передачи информации, 1974, т. X, в. 4, с. 25–29.
2. *Мак-Вильямс Ф.*, *Дж. Слоэн Н. Дж.* Теория кодов, исправляющих ошибки. М.: Связь, 1979, 744 с.
3. *Осмоловский С. А.* Стохастические методы защиты информации. М.: Радио и связь, 2003, 320 с.
4. Патент России 2292122 на «Способ комплексной защиты информации». Автор Осмоловский С. А., приоритет 11.05.2005.