

УНИФИЦИРОВАННЫЕ СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ В КОМПЬЮТЕРИЗИРОВАННЫХ СИСТЕМАХ

Крылова В.А., Мирошник А.Н.

Национальный технический университет

«Харьковский политехнический институт», г. Харьков

В настоящее время стремительный рост информационных технологий, а также распространение компьютеризированных систем и сетей обусловило необходимость создания высокоэффективных аппаратно-программных средств, обеспечивающих достоверную и быструю доставку информации. Известно, что параметры кодера выбирают исходя из некоторого «среднего» состояния канала связи, что приводит либо к уменьшению скорости передачи информации, из-за большей избыточности кода либо к потере связи при ухудшении качества канала. Одним из путей решения данной проблемы является переход к унифицированным средствам защиты информации, в которых коды способны изменять свои параметры на стадии эксплуатации системы связи, обеспечив при этом высокую достоверность за счет перераспределения избыточности кода.

Для построения адаптивных систем кодирования в работе были исследованы двоичные свёрточные коды со скоростью $1/n$. Множество свёрточных кодов, синтезированных из базового со скоростью $R=1/n$ с помощью изменения длины кодового ограничения и порождающих полиномов, получило название гнездовые свёрточные коды. Множество гнездовых свёрточных кодов с длиной кодового ограничения $m-l$ синтезируются путем изменения порождающих полиномов базового кода. При этом было доказано, что если состояния базового и гнездового свёрточных кодов совпадают, то кодовые последовательности тоже равны. Для построения адаптивной системы защиты информации необходимо учитывать, что параметры декодера должны меняться в соответствии с параметрами кодера. Поэтому для декодирования адаптивных свёрточных кодов скорости $R=1/n$ может быть использован алгоритм Витерби. Известно, что базовым элементом решетчатой диаграммы алгоритма Витерби является бабочка, которая реализует главную операцию сложить-сравнить-выбрать (ССВ). Было установлено, что состояния 0, 4, 2 и 6 для кодера с $m=3$ повторяют значения ребер состояний 0, 2, 1 и 3 для кодера с $m=2$. Поэтому доказано, что программируемый процессор Витерби, рассчитанный для декодирования свёрточного кода с длиной кодового ограничения $m=3$, с помощью двух блоков Сложить-Сравнить-Выбрать, может также декодировать и код с длиной кодового ограничения $m+l$ т.д. Для того чтобы адаптации осуществлялась по двум критериям: ЭВК и скорость передачи были исследованы перфорированные свёрточные коды, которые строятся из низкоскоростных кодов с помощью периодической перфорации кодовых символов. Получены оптимальные перфорированные коды, построенные из гнездовых свёрточных кодов со скоростью $1/2$ и длиной кодового ограничения m , которые по своим вероятностным характеристикам превосходят известные оптимальные коды.