УДК 621.396.931

Паук С.М., Потапов В.Г., Тараненко А.Г., Ткалич О.П.

БЕЗОПАСНОСТЬ И ЗАЩИТА ИНФОРМАЦИИ В ЦИФРОВЫХ СИСТЕМАХ СОТОВОЙ СВЯЗИ

Системы сотовой связи (ССС) являются одним из видов современных цифровых телекоммуникационных систем. В таких системах необходимо исключить несанкционированный доступ к системе, обеспечить конфиденциальность абонентской информации и защитить информацию от ошибок, вызванных не идеальностью канала связи.

Выделяются два основных направления защиты информации в системах общего доступа: обеспечение безопасности информации и защита от ошибок, вызванных помехами в канале связи. Анализ этих мероприятий позволяет определить порядок эксплуатации системы, максимально удовлетворяющий потребности абонента.

В аналоговых сотовых системах применялись мероприятия по защите информации в виде различных методов помехоустойчивого кодирования, однако вопросом исправления ошибок уделялось недостаточное внимание. Обеспечение безопасности информации также было недостаточным для надежного исключения несанкционированного доступа к системе.

Целью статьи является анализ методов обеспечения безопасности и защиты информации в цифровой ССС типа GSM.

Методы обеспечения безопасности и защиты информации в системе GSM

В цифровых ССС безопасность информации понимается как исключение несанкционированного использования системы и обеспечении конфиденциальности переговоров мобильных абонентов [1]. Рассмотрим мето obile Subscriber Identity), код доступа PIN (Personal Identification Number), код разблокировки PUK (Personal Unblocking Key), индивидуальный ключ аутентификации K_i, алгоритм аутентификации А3, алгоритм вычисления ключа шифрования А8. Принцип аутентификации показан на рис.1. Из центра аутентификации через центр коммутации на МС передается случайное число р. Модуль SIM обрабатывает числа р и K_i по алгоритму А3 и формирует число x_1, которое передается центру коммутации.

Аналогично формируется число x_2 в центре аутентификации.

Центр коммутации сравнивает числа x_1 и x_2. При их равенстве право на доступ к системе подтверждается. Числа р и K_i также используются для вычисления ключей шифрования K_c по алгоритму А8.

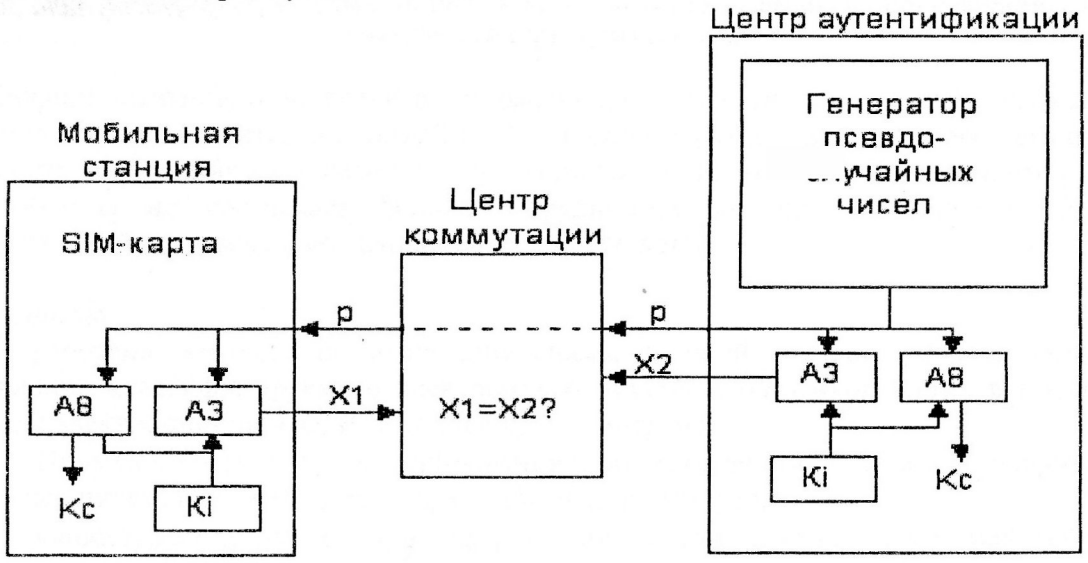


Рис. 1. Аутентификация мобильной станции

Шифрование сообщений выполняется по команде CMC (Ciphering Mode Command), передаваемой из центра коммутации на МС. Принцип шифрования показан на рис. 2.

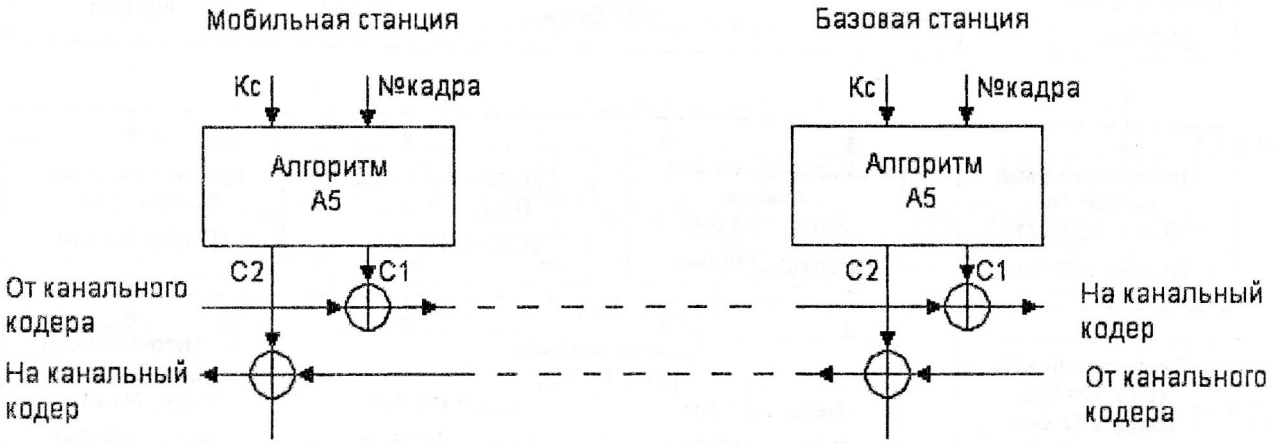


Рис. 2. Шифрование и дешифрование сообщений

В МС и в базовой станции (БС) по алгоритму А5 формируются псевдослучайные последовательности C_1 и C_2. Входными данными для этого алгоритма служат ключ шифрования и номер временного кадра [2].

При шифровании последовательности C_1 и C_2 суммируются по модулю 2 с выходными битами канальных кодеров МС и БС. При дешифровании такие же последовательности суммируются по модулю 2 с принятыми битами, в результате исходное сообщение восстанавливается. Для несанкционированной расшифровки сообщения необходимо определить текущий номер кадра и текущий ключ шифрования, после чего требуется сформировать две синхронные псевдослучайные цифровые последовательности. Ключ шифрования изменяется при каждом новом установлении связи, а период повторения номера кадра равен $T \approx 3{,}5$ часа. Это значительно затрудняет несанкционированную расшифровку.

Защита информации от ошибок выполняется канальными кодеками, которые входят в состав МС и БС.

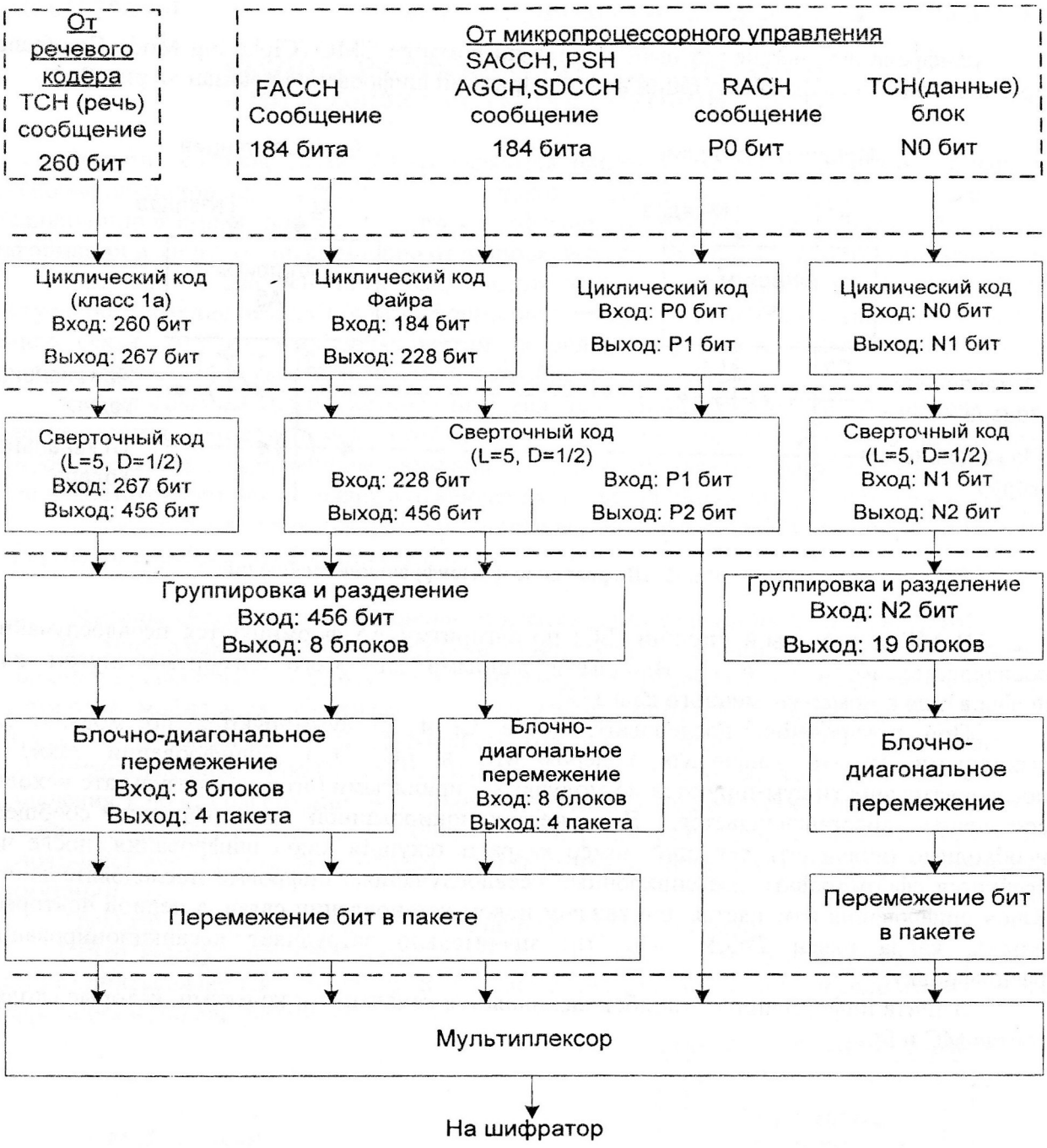
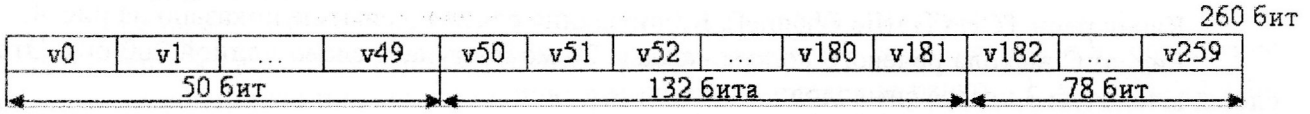
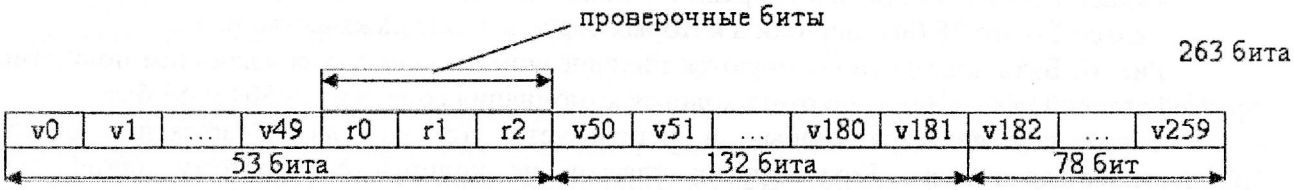


Рис. 3. Помехоустойчивое кодирование сигналов трафика и управления.

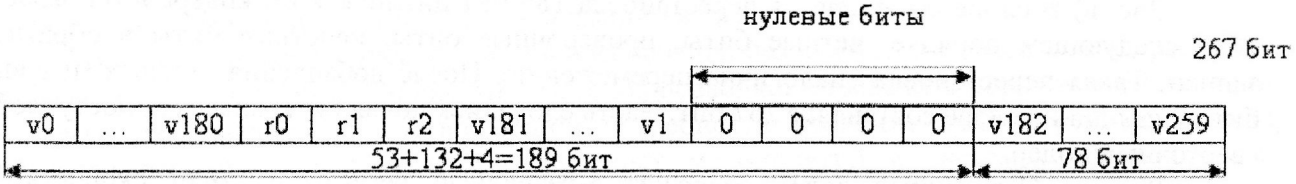
Канальный кодек обеспечивает повышение помехоустойчивости передачи цифровых сигналов за счет циклического и сверточного кодирования, а также перемежения. На рис. 3 показано, что выполнение этих преобразований зависит от вида логического канала.



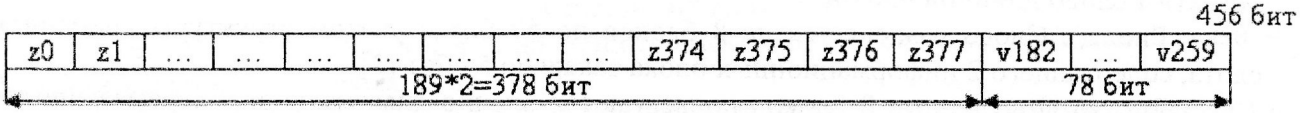
а) выход с речевого кодера



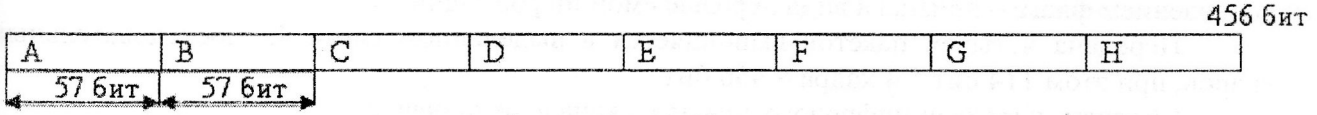
б) циклический код (класс 1а)



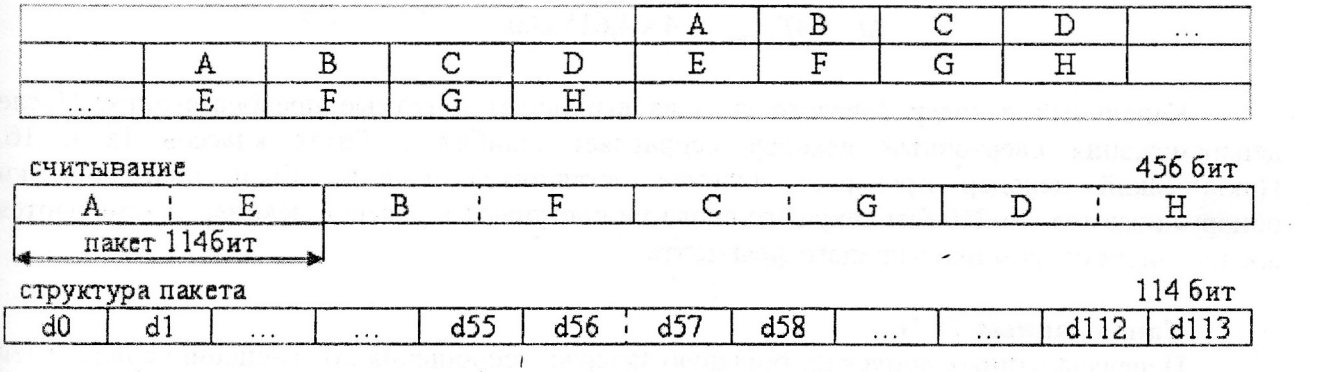
в) битовая перестановка



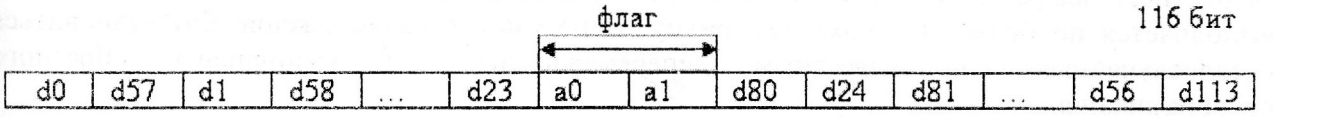
г) сверточный код (класс 1)



д) разделение на блоки



е) блочно-диагональное перемежение



ж) перемежение в пакете

Рис. 4. Помехоустойчивое кодирование в речевом канале TCH

Канал речи TCH (Traffic Channel). Кодирование речевого сигнала показано на рис. 4.

Рис. а) С выхода речевого кодера каждые 20 мс поступает слово длиной 260 бит. Это слово делится на 3 класса символов:

- класс 1а – это 50 бит, ошибки в которых сильно влияют на качество синтезированной речи;
- класс 1б – это 132 бита с умеренным влиянием ошибок на качество речи;
- класс 2 – это 78 бит, ошибки в которых слабо влияют на качество речи.

Рис. б) Биты класса 1а кодируются циклическими кодом с порождающим полиномом третьей степени $p(x)=x^3+x+1$, поэтому кодовая комбинация содержит $n=50+3=53$ бита.

Такой код является слабым и используется только для обнаружения ошибок циклическим декодером. Биты других классов не кодируются, поэтому длина слова составляет 263 бита.

а) слово речевого кодера

Рис. в) В слове выполняется перестановка 185 бит циклического кодера и бит класса 1б в следующем порядке: четные биты, проверочные биты, нечетные биты в обратной записи. Такая перестановка аналогична перемежению. После добавления четырех нулевых бит общая длина слова составляет 267 бит. Часть слова, исключая биты класса 2, поступает в сверточный кодер.

Рис. г) Сверточный кодер содержит 5-разрядный регистр и имеет скорость ½. Входные 189 бит преобразуются в выходные 189*2=378 бит. Эти биты и биты класса 2 образуют слово длинной 456 бит.

Рис. д). Слово разделяется на 8 блоков по 57 бит с учетом структуры временного слота, содержащего 2 информационных блока также по 57 бит [2].

Рис. е) Полученные 8 блоков подвергаются блочно-диагональному перемежению. С выхода перемежителя считываются 4 вида двойных блоков или пакетов длиной по 114 бит.

Рис. ж) Завершающей операцией кодера является перемежение бит в каждом пакета с добавлением флага – признака вида передаваемой информации.

Передача четырех пакетов выполняется в выделенном слоте 4х последовательных кадров, при этом 114 бит * 4 кадра = 456 бит.

Скорость передачи цифрового сигнала в канале речи равна:

$$\frac{n}{\Delta t}=\frac{456бит}{4T_{кадра}}=\frac{456бит}{4\times 4{,}61538мс}=24{,}7\ Кбит/с$$

Канальный декодер речевого сигнала выполняет обратные преобразования. После деперемежения сверточный декодер исправляет ошибки в битах классов 1а и 1б. Циклический декодер проверяет наличие оставшихся ошибок. Если такие ошибки обнаруживаются, то 260 бит текущего слова не поступают в речевой декодер, а заменяются аналогичным словом предыдущего фрагмента.

Канал данных TCH

Передача данных допускает большую задержку сообщения по сравнению с передачей речи. Поэтому перемежение на рис.3. выполняется после разделения выходных бит сверточного кадра не на 8, а на 19 блоков. Завершающее битовое перемежение также выполняется по более сложному алгоритму. В результате расположение бит становиться псевдослучайным, но известным деперемежителю для выполнения обратного преобразования.

Каналы управления.

Сообщение канала случайного доступа RACH согласно рис.3 кодируется слабым циклическим кодом и сверточным кодом. Перемежение не применяется, т.к. сообщение содержит однотипную информацию, повторяющуюся достаточно редко – 1 раз в 235мс. При такой частоте повторения влиянием пакетов ошибок можно пренебречь. Сообщения других каналов длиной 184 бит кодируются по общей схеме.

Высокая помехоустойчивость передачи этих сообщений обеспечивается циклическим кодом с порождающим полиномом четвертой степени

$$p(x) = (x^{23} + 1)(x^{17} + x^3 + 1) = x^{40} + ... + 1$$

Выходная комбинация циклического кодера содержит n=184+40=224 бита. После добавления четырех нулевых бит получают слово длиной 228 бит, поступающее в сверточный кодер. Выходное слово сверточного кодера длиной 456 бит разделяется на 8 блоков с последующим блочным и внутрипакетным перемежением.

Рассмотренные преобразования цифровых сигналов обеспечивают заданные требования к безопасности и защите информации в системе GSM.

В статье проведен анализ методов обеспечения безопасности и защиты информации в цифровой ССС типа GSM. Знание этих методов позволяет определить порядок эксплуатации системы, максимально удовлетворяющий потребности абонента. Рассмотренные методы являются основой для изучения аналогичных мероприятий в системах сотовой связи следующих поколений.

Список литературы

1. *Чекалин А.А., Заряев А.В.* и др. Защита информации в системах мобильной связи. – М.: Горячая линия – Телеком, 2005. – 171с.

2. *Потапов В.Г., Тараненко А.Г.* и др. Распределение частотно-временного ресурса в цифровых системах связи: Материалы VI МНТК АВІА – 2004. – К.: НАУ, 2004. – 4 с.

Поступила 01.09.2006