ЗАСЕКРЕЧИВАНИЕ РЕЧИ НА КАНАЛАХ СВЯЗИ СТАНДАРТА GSM

***Горшков Юрий Георгиевич**, кандидат технических наук, доцент*

Глобальная Система Мобильной связи (GSM) является одной из наиболее распространенных в мире. Стандарт GSM защищен криптографическим алгоритмом A5. В то же время, используемые в сотовых сетях второго поколения 2G алгоритмы A5/1 и A5/2 не обеспечивают достаточный уровень безопасности, что приводит к необходимости применения дополнительных средств шифрования.

В работе рассмотрен алгоритм шифрования A5/1 стандарта GSM, представлена классификация аппаратуры засекречивания речевой информации, приводятся основные характеристики устройств криптографической защиты телефонных переговоров на каналах сотовой связи, предложено решение, позволяющее объективно оценивать качество вокодеров, применяемых в телефонных шифраторах.

***Ключевые слова**: засекречивание речи, GSM, вокодер.*

SPEECH SCRAMBLING IN GSM COMMUNICATION CHANNELS

***Yuri Gorshkov**, Ph.D., Associate Professor*

The paper reviews A5/1 cryptographic algorithm of the GSM standard, presents the classification of voice data scrambling equipment, lists the basic features of devices for cryptographic protection of telephone conversations in cellular network channels, and proposes the solution which enables to objectively estimate the quality of vocoders used in telephone scramblers.

***Keywords:** voice scrambling, GSM, vocoder.*

GSM (Global System for Mobile Communications) стандарт цифровой мобильной сотовой связи с разделением каналов по времени (TDMA) и частоте (FDMA). Разработан под эгидой Европейского института стандартизации электросвязи (ETSI) в конце 80-х годов. Безопасность стандарта обеспечивают алгоритмы: A3 – аутентификации; A8 – генерации криптоключа и A5 – шифрования оцифрованной речи для обеспечения конфиденциальности переговоров между абонентом и базовой станцией [1]. Мобильные станции (телефоны) снабжены смарт-картой с реализацией алгоритмов A3 и A8, а в самом телефоне имеется ASIC-чип с алгоритмом A5. В состав базовых станций входят центры аутентификации, также использующие алгоритмы A3, A8 и A5.

В сетях связи стандарта GSM второго поколения 2G используются две основные разновидности A5: A5/1 – используется странами Северной Америки и Европы; A5/2 – экспортный вариант для остальных стран.

Безопасность передаваемой информации в сотовых сетях третьего поколения 3G обеспечивает алгоритм A5/3. В основе A5/3 – алгоритм Касуми (KASUMI) [2]. Разработан группой SAGE (Security Algorithms Group of Experts), которая является частью Европейского Института по Стандартизации в области Телекоммуникаций (ETSI).

Первая открытая работа по криптоанализу A5/2 отмечена в 1999 году [3].

Публикации по оценке стойкости A5/1 появляются в печати с 1994 года [4];

к наиболее известным работам в этой области следует отнести публикации [5 – 7].

A5/1 – поточный алгоритм шифрования. В нем псевдослучайная последовательность реализуется на основе трех регистров сдвига с линейной обратной связью [6, 7]. Длина регистров 19, 22 и 23 бита соответственно. Сдвигами управляет функция большинства (также известная как majority: $m(a1, a2, a3) = a1a2 \vee a2a3 \vee a1a3)$, в каждом регистре есть контрольный бит: восьмой в первом регистре (обозначим $a1$), десятый во втором

(обозначим $a2$) и в третьем (обозначим $a3$). Биты нумеруются справа налево. При очередном такте сдвигаются состояния только тех регистров, у которых значения контрольных бит совпадают

со значением функции m. Функция управления сдвигом и $m(a1, a2, a3)$ связаны соотношением:

$$c(x) = (a1 \equiv m, a2 \equiv m, a3 \equiv m).$$

Последние биты регистров суммируются по модулю два. Результат сложения становится новым битом гаммы. Гамма накладывается на открытый текст, вследствие чего получается шифртекст. На одном ключе генерируется 114 бит гаммы.

Линейные функции обратной связи удобно представлять с помощью полиномов, сопоставляя каждому биту регистра соответствующую степень переменной x. В шифре A5/1 функции обратной связи задаются следующими полиномами:

$x^{19} + x^{18} + x^{17} + x^{14} + 1$ для R1,
$x^{22} + x^{21} + 1$ для R2,
$x^{23} + x^{22} + x^{21} + x^{8} + 1$ для R3.

Например, в первом регистре суммируются биты с номерами 18, 17, 16 и 13. Результат становится новым значением крайнего правого бита (рис. 1).

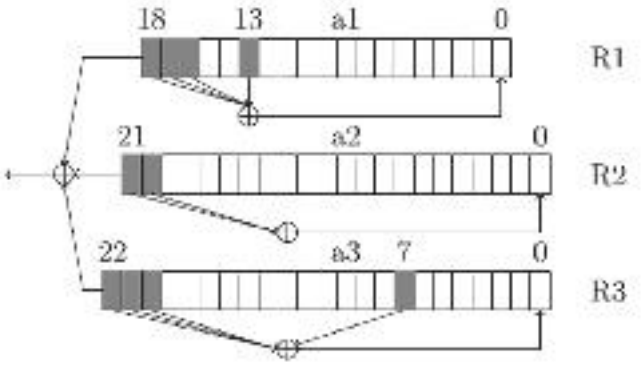

Рис. 1. *Структура регистров сдвига A5/1*

На рис. 1 символами *a1, a2, a3* отмечены контрольные биты, а темным цветом выделены биты, от которых существенно зависят функции обратной связи.

Классификация аппаратуры засекречивания телефонных переговоров.

При ведении телефонных переговоров по каналам сети общего пользования (ТфОП) защиту всего трафика (прохождения сигнала от абонента до абонента) обеспечивают специальные устройства засекречивания речевой информации аналогового типа (иногда именуемые маскираторами или «скремблерами») и дискретного типа (вокодеры с шифраторами). Классификация аппаратуры засекречивания представлена на рис. 2 [8, 9].

Известны два основных метода засекречивания речевого сигнала (Р.С.). Они разделяются по способу передачи по каналу связи: аналоговое засекречивание и дискретизация или выделение параметров Р.С., представленных в цифровом виде, с последующим шифрованием. (В первом случае в канале связи – сигнал с фрагментами Р.С., во втором – сигнал с выхода модема, использующего один из стандартных видов модуляции; скорости передачи 2400, 4800, 7200 или 9600 бит/сек).

Аппаратура засекречивания аналогового типа относится к средствам криптографической защиты. Под криптографической защитой или засекречиванием понимается изменение характеристик речевого сигнала (Р.С.),таким образом, чтобы сигнал, переданный в канал связи, обладал свойствами неразборчивости и занимал такую же полосу частот спектра, что и исходный открытый сигнал.

Аппаратура засекречивания дискретного типа включает вокодер, шифратор и модем.

Средства криптографической защиты телефонных переговоров на каналах сотовой связи.

В зарубежных телефонных шифраторах стандарта GSM применяются алгоритмы шифрования AES, RSA, Twofish, Triple DES.

AES (Advanced Encryption Standard) - симметричный алгоритм блочного шифрования (размер блока 128 бит, ключ 128/192/256 бит), принят в качестве стандарта шифрования правительством США.

RSA (Rivest, Shamir, Adleman) - криптографический алгоритм с открытым ключом.

Twofish - симметричный алгоритм блочного шифрования с размером блока 128 бит и длиной ключа до 256 бит.

Triple DES (3DES) - симметричный блочный шифр.

В отечественной аппаратуре засекречивания телефонии применяется алгоритм

ГОСТ 28147-89 – стандарт симметричного шифрования.

Система распределения ключей в сетях засекреченной телефонной связи реализуется с использованием протокола **Диффи-Хеллмана** (Diffie-Hellman, DH) - криптографический протокол, позволяющий двум и более абонентам получить общий секретный ключ, используя неза-

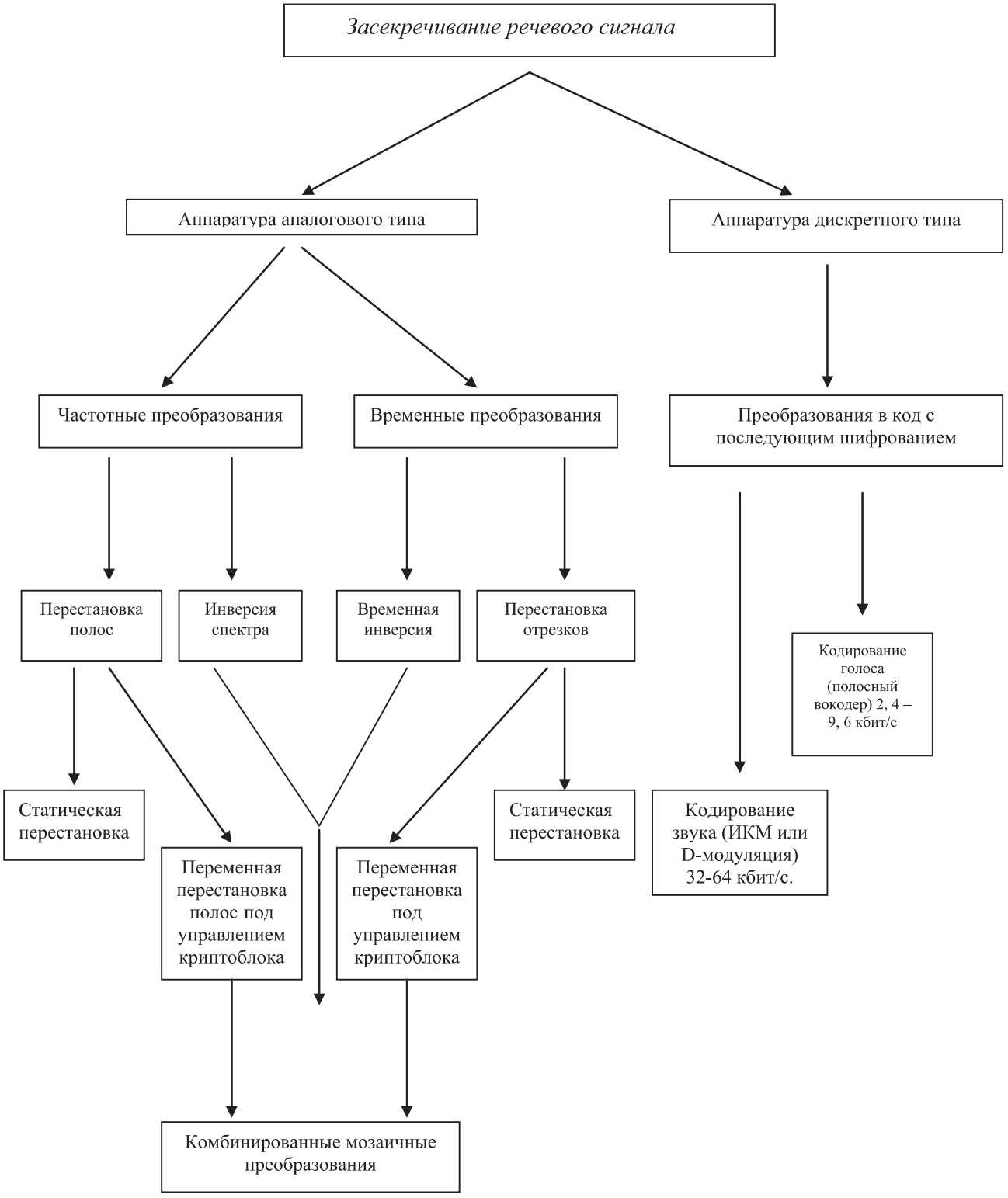

Рис. 2. *Классификация аппаратуры засекречивания телефонных переговоров*

щищенный от перехвата канал связи. Полученный ключ используется для засекречивания переговоров с помощью алгоритмов симметричного шифрования.

На сайте «Бюро Научно-Технической Информации «Техника для спецслужб» представлены данные отечественных телефонных шифраторов стандарта GSM (http://www.bnti.ru/index.asp?tbl=03.07.01). К одной из последних разработок относится «Устройство криптографической защиты переговоров в сетях сотовой связи «Аппаратура 605» (рис. 3).

Рис. 3. *Внешний вид устройства криптографической защиты «Аппаратура 605»*

В последние годы в нашей стране для защиты информации, содержащую коммерческую тайну потребителям предлагаются телефонные шифраторы с использованием криптографического алгоритма ГОСТ 28147-89: «SMP-Атлас», «Талисман-GSM», «ФРАКТАЛ GSM», «Специализированный телефонный аппарат «GSM». Гарантированный уровень безопасности переговоров сотовой связи обеспечивается, также, отечественными разработками: «Криптотелефон «STEALTHPHONE», «Двухпроцессорный крипто смарт телефон», «Крипто смарт телефон «Cancort», «Криптотелефон GSM «М-539».

Зарубежными компаниями криптографические средства защиты телефонных переговоров абонентам сотовой связи поставляются с 2000 года. Одна из первых разработок – «Siemens TopSec GSM», Rohde&SchwarzSIT GmbH. С уровнем создания современных зарубежных систем засекреченной телефонии стандарта GSM можно ознакомиться на сайте http://www.securevoice-gsm.com. На рис. 4 представлен внешний вид шифратора «Sectera Wireless GSM Phone», General Dynamics (http://www.gdc4s.com).

Рис. 4. *Внешний вид шифратора «Sectera Wireless GSM Phone»*

Маскираторы телефонных переговоров. К маскираторам телефонии стандарта GSM (аппаратура аналогового типа) следует отнести:

1. Устройство «ALT-COTA» («Орешек-GSM»). Внешний вид устройства представлен на рис. 5.

Рис. 5.

2. Устройство маскирования телефонных сообщений (УМТС) в каналах GSM связи «Резеда» (рис. 6).

Рис. 6.

На сайте http://www.skrembler.ru представлены характеристики одной из последних разработок «Скремблер «GUARD Bluetooth».

Оценка качества вокодеров, используемых в телефонных шифраторах.

Современные зарубежные телефонные шифраторы сотовой связи коммерческого применения включают, как правило, вокодеры с использованием алгоритма RPE-LTP[10, 11]. В некоторых отечественных разработках информация о применяемых вокодерах отсутствует, либо заменяется рекламной, например: «уникальный голосовой кодек с линейным предсказанием». В то же время от качества вокодеров зависят такие важные характеристики как разборчивость речи и узнаваемость диктора.

Специалистами кафедры «Информационная безопасность» МГТУ им. Н.Э. Баумана и ЗАО «НПО «Эшелон» создан исследовательский комплекс высокоточного частотно-временного анализа речевого сигнала [12]. Программные средства комплекса за счет применения технологии многоуровневого вейвлет-анализа позволяют

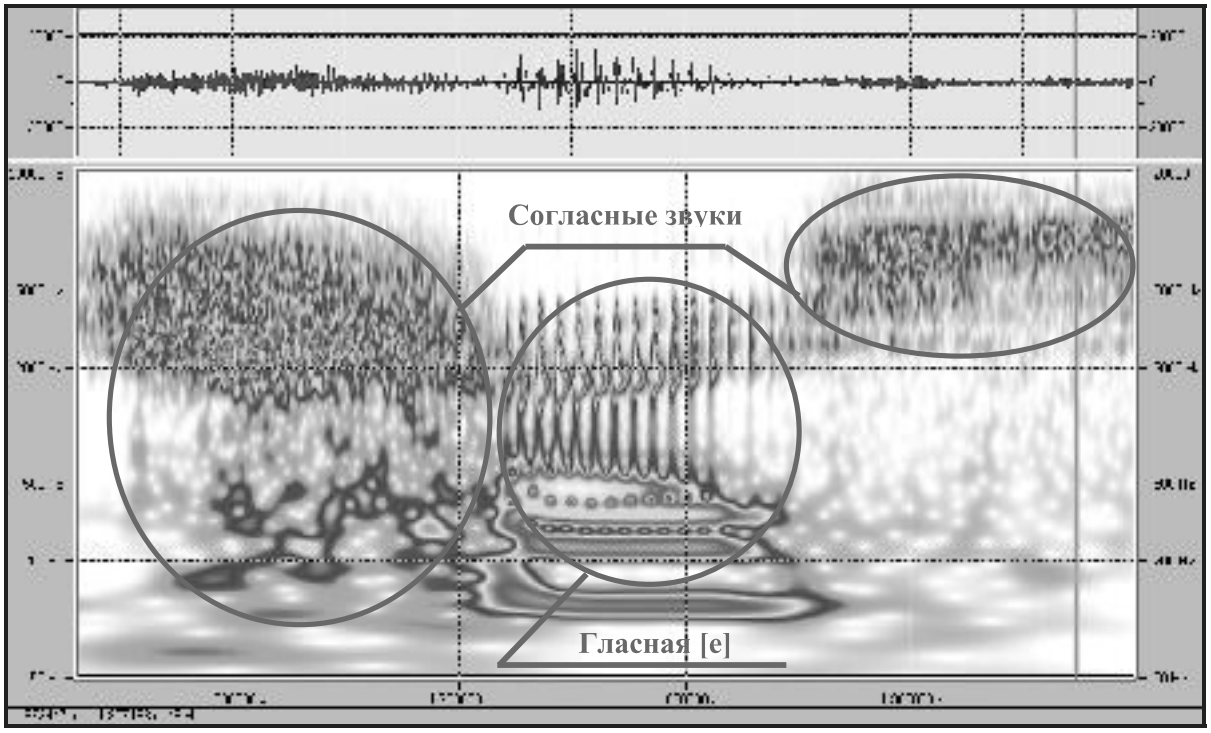

Рис. 7. *Вейвлет-сонограмма слова [шесть]*

получать параметры не только гласных, но и согласных звуков. Основой предлагаемой методики определения качества вокодеров является сравнительный анализ вейвлет-сонограмм (частотно-временного представления «видимый звук») исходного и синтезированного сигналов. Методика является объективной, ее применение позволит повысить эффективность работы слушателей-экспертов. На рис. 7 представлена вейвлет-сонограмма слова [шесть].

Заключение.

На каналах стандарта GSM второго поколения 2G криптографические алгоритмы A5/1 и A5/2 не обеспечивают достаточный уровень защиты речевой информации.

Применение дополнительных средств шифрования с реализацией алгоритма ГОСТ 28147-89 обеспечивает гарантированный уровень защиты всего телефонного трафика связи (от абонента до абонента). Объективная оценка качества вокодеров, применяемых в телефонных шифраторах может быть осуществлена при их тестировании с использованием технологии многоуровневого вейвлет-анализа.

Литература

1. Ross Anderson, Mike Roe «A5 – The GSM Encryption Algorithm», 1994.
2. Universal Mobile Telecommunications System (UMTS); Specification of the 3GPP confidentiality and integrity algorithms; Document 2: Kasumi specification. ETSI (2007).
3. Wagner D. et al. The real-time cryptanalysis of A5/2 // Crypto'99 (Santa Barbara, August 15-19, 1999): Proc. Berlin: Springer-erl., 1999. P. 12-21.
4. AndersonR. Subject: A5 // posting to Newsgroups: sci.crypt, alt.security, uk.telecom; 17 June 1994.
5. Golic J. Cryptanalysis of alleged A5 stream cipher // Adv. Cryptology. Workshop on the theory and application of cryptographic techniques EUROCRYP T'97 (Konstanz, May 11-15, 1997): Proc. Berlin: Springer- Verl., 1997. P. 239-255. (Lect. Notes Comput. Sci.; Vol. 1233).
6. BiryukovA., ShamirA., Wagner D. Real time cryptanalysis of A5/1 on a PC // Fast Software Encryption Workshop FSE'2000. (New York, April 10-12, 2000): Proc. Berlin: Springer-Verl., 2001. P. 1-18. (Lect. Notes Comput. Sci.; Vol. 1978).

7. Киселев С.А., Токарева Н.Н. О сокращении ключевого пространства шифра A5/1 и обратимости функции следующего состояния в поточном генераторе // Дискретный анализ и исследование операций. Март – апрель 2011. Том 18, № 2. С. 51-63.
8. Горшков Ю.Г. Анализ и засекречивание речевого сигнала: Учебное пособие. – М.: Издательство МГТУ им. Н.Э. Баумана, 2006. – 26 с.
9. Кравченко В.Б. Защита речевой информации в каналах связи // Специальная техника, № 4-5, 1999.
10. K.Hellwig, P.Vary, D. Massaloux, ectl. Speech Codec for the European Mobile Radio System. IEEE Global Communications Conference, 1989. P. 1065-1069.
11. ETSI Speech processing functions General Description, GSM06.01-1999, Version 8.0.1. P. 22-53.
12. Горшков Ю.Г. Исследовательский комплекс частотно-временного анализа речевого сигнала с использованием вейвлет-технологии // Вестник Московского государственного технического университета им. Н.Э. Баумана. Серия: Приборостроение № 4, 2011. С. 78-87.

References

1. Ross Anderson, Mike Roe «A5 – The GSM Encryption Algorithm», 1994.
2. Universal Mobile Telecommunications System (UMTS); Specification of the 3GPP confidentiality and integrity algorithms; Document 2: Kasumi specification. ETSI (2007).
3. Wagner D. et al. The real-time cryptanalysis of A5/2 // Crypto'99 (Santa Barbara, August 15-19, 1999): Proc. Berlin: Springer-erl., 1999. P. 12-21.
4. AndersonR. Subject: A5 // posting to Newsgroups: sci.crypt, alt.security, uk.telecom; 17 June 1994.
5. Golic J. Cryptanalysis of alleged A5 stream cipher // Adv. Cryptology. Workshop on the theory and application of cryptographic techniques EUROCRYPT'97 (Konstanz, May 11-15, 1997): Proc. Berlin: Springer- Verl., 1997. P. 239-255. (Lect. Notes Comput. Sci.; Vol. 1233).
6. BiryukovA., ShamirA., Wagner D. Real time cryptanalysis of A5/1 on a PC // Fast Software Encryption Workshop FSE'2000. (New York, April 10-12, 2000): Proc. Berlin: Springer-Verl., 2001. P. 1-18. (Lect. Notes Comput. Sci.; Vol. 1978).
7. Kiselev C.A., Tokareva N.N. O sokrashchenii cliuchevogo prostranstva shifra A5/1 i obratimosti funktcii sleduiushchego sostoianiia v potochnom generatore // Diskretny`i` analiz i issledovanie operatcii`. Mart – aprel` 2011. Tom 18, № 2. C. 51-63.
8. Gorshkov Iu.G. Analiz i zasekrechivanie rechevogo signala: Uchebnoe posobie. – M.: Izdatel`stvo MGTU im. N.E`. Baumana, 2006. – 26 s.
9. Kravchenko V.B. Zashchita rechevoi` informatcii v kanalakh sviazi // Spetcial`naia tekhnika, № 4-5, 1999.
10. K.Hellwig, P.Vary, D. Massaloux, ectl. Speech Codec for the European Mobile Radio System. IEEE Global Communications Conference, 1989. P. 1065-1069.
11. ETSI Speech processing functions General Description, GSM06.01-1999, Version 8.0.1. P. 22-53
12. Gorshkov Iu.G. Issledovatel`skii` kompleks chastotno-vremennogo analiza rechevogo signala s ispol`zovaniem vei`vlet-tekhnologii // Vestneyk Moskovskogo gosudarstvennogo tekhnicheskogo universiteta im. N.E`. Baumana. Seriia: Priborostroenie № 4, 2011. S. 78-87.