ТЕСТИРОВАНИЕ СРЕДСТВ ЗАСЕКРЕЧИВАНИЯ РЕЧИ

***Горшков Юрий Георгиевич**, кандидат технических наук, доцент, г. Москва*

Рассмотрены вопросы защиты речевой информации на каналах связи телефонной сети общего пользования (ТфОП). Предложена методика тестирования аппаратно-программных средств засекречивания речи. Приведены данные тестирования телефонных шифраторов и программы засекречивания речевых сигналов.

***Ключевые слова**: защита речевой информации, телефонный шифратор, программа засекречивания, тестирование.*

TESTING OF MEANS OF THE SPEECH ENCRYPTION

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

Questions of protection of the voice information in public switched telephone network (PSTN) channels are considered. The testing methodology of hardware and software of speech encryption is offered. Test data of telephone scramblers and software of voice signals encryption are submitted.

***Keywords**: protection of the voice information, telephone scramblers, software of encryption, testing.*

Введение

Телефонные шифраторы находят все более широкое применение для решения задач безопасности ведения переговоров на каналах связи сети общего пользования. На этапе выбора телефонной аппаратуры засекречивания потребитель, как правило, располагает ограниченной информацией, относящейся к реализованным криптографическим алгоритмам и числу ключевых установок. Такие важные для пользователя характеристики, как время вхождения шифраторов в синхронизацию, параметры речепреобразующих устройств или вокодеров не всегда соответствуют заявленным данным или отсутствуют.

В статье рассмотрены вопросы тестирования средств засекречивания с целью получения реальных характеристик защищенной речевой связи.

Характеристики телефонных шифраторов

Зарубежными и российскими компаниями-разработчиками в последние годы представлено для коммерческого применения значительное количество образцов телефонных шифраторов. Основная цель средств засекречивания речевой информации – преобразование исходного речевого сигнала по заданному закону для достижения минимальной остаточной разборчивости, а также обеспечение значительного пространства ключей и высокой стойкости засекреченного сигнала к криптоанализу [1-9].

Российскими специалистами телефонные шифраторы коммерческого применения по способу защиты речевого сигнала (Р.С.) принято делить на два класса: аналогового типа (с использованием речепреобразующего устройства и шифратора) и дискретного типа - выделение параметров Р.С., представленных в цифровом виде на основе вокодеров, с последующим шифрованием [1, 3].

Зарубежные криптографы аппаратуру засекречивания также разделяют на *Аналоговую* (Scramblers) и *Цифровую* - Digital Voice Protection (DVP) [6].

Аналоговая аппаратура (Scramblers) включает 4 вида засекречивающих преобразований [7]:

1. Time-Domain Scramblers (TDS) - с преобразованиями во временной области;
2. Frequency-Domain Scramblers (FDS) - частотные преобразования;
3. Time-Frequency Scrambling (TFS) - частотно-временные преобразования;
4. Encryption by using Pseudo-Noise Sequences (ENS) - шифрование с использованием псевдошумовых последовательностей.

Трудности реализации аппаратно-программных средств засекречивания связаны с ограниченной полосой пропускания канала связи, в сочета-

нии с требованиями по обеспечению устойчивой работы на каналах среднего и низкого качества, сохранению высокого качества восстановленной на приемной стороне речи, ограничениями на вносимую временную задержку, вычислительную сложность используемых алгоритмов.

Возможность отдельных телефонных шифраторов помимо засекречивания переговоров обеспечивать криптографическую защиту факсимильной информации выводят их в разряд эффективных универсальных средств защиты нетекстовой информации корпоративных систем связи.

На рис. 1 представлен внешний вид телефонного шифратора Snapfone (Израиль, Snapshield, Ltd).

Рис. 1**. Внешний вид шифратора **Snapfone

Данные компании-разработчика по шифратору ***Snapfone***: высокий уровень безопасности FIPS 140-2 (уровень 2); минимальное время задержки речи; шифрование: 3DES, ключ 192 бит; алгоритм генерации ключей: Diffie-Hellman, ключ 1024 бит.

FIPS (Federal Information Processing Standards) 140-2 (уровень 2): государственный стандарт США, описывающий требования к шифрованию и связанных с ним мерам безопасности в ИТ - продуктах, которые используются для обработки конфиденциальной информации не имеющей гриф «секретно».

На рис. 2 представлена структура защищенной корпоративной системы связи с использованием шифраторов семейства Snap.

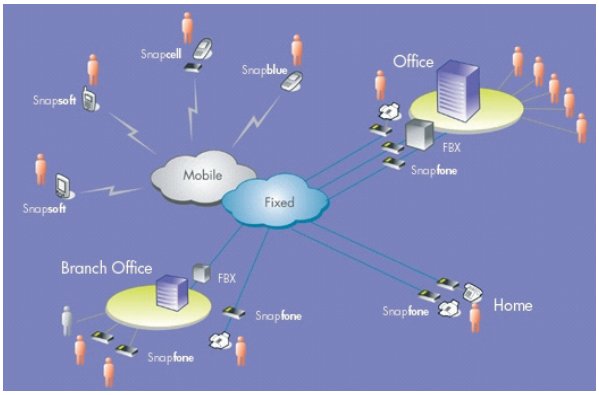

***Рис. 2.** Структура защищенной корпоративной системы связи с использованием шифраторов семейства Snap*

Данные компании-разработчика по телефонному шифратору «**Орех-2**» (Украина): относится к аппаратуре засекречивания аналогового типа; вид преобразований - частотно-временные перестановки; словесная разборчивость не менее 85%; задержка речевого сигнала 0.32 сек; время синхронизации не более 10 сек; разрядность ключа 128 бит; сеансовый ключ формируется автоматически для каждого сеанса связи и составляет 10 в 36-й степени возможных комбинаций.

Тестирование телефонных шифраторов

На кафедре «Информационная безопасность» МГТУ им. Н.Э. Баумана выполнены поисковые исследования, в ходе которых разработана методика тестирования телефонных шифраторов с использованием стенда аппаратно-программных средств. Методика включает в себя многоканальную регистрацию открытых речевых сигналов, засекреченных линейных передач и восстановленной речи с их последующим многоуровневым вейвлет-анализом. Аппаратные средства стенда: телефонный аппарат Panasonic KX-TS2363RUW – 2 шт.; автоматическая телефонная станция (АТС) Panasonic KX-T61610B; автономный 4-х канальный комплекс регистрации телефонных переговоров «ОСА А4Р»; телефонный шифратор – 2 шт. (рис. 3).

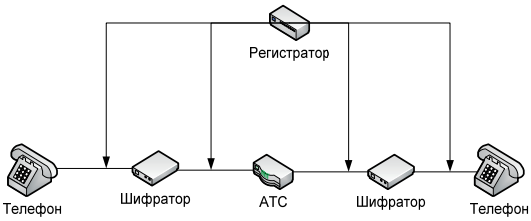

***Рис. 3**. Структура стенда тестирования*

Программные средства: RightMark Audio Analyzer 6.2.1 (RMAA) – программа для тестирования аналоговых и цифровых реализаций звуковых устройств; WaveView-MWA – программа многоуровневого вейвлет-анализа с возможностью построения сонограмм (изображений «видимый звук») повышенного частотно-временного разрешения нестационарных сигналов [10, 11].

Результаты тестирования шифратора Snapfone

1. Телефонный шифратор относится к аппаратуре дискретного типа Digital Voice Protection (DVP).

2. Вокодер телефонного шифратора обеспечивает высокое качество синтезированного речевого сигнала.

3. Время вхождения в синхронизацию не превышает 100 мсек, что соответствует заявленным данным.

На рис. 4 представлен сигнал линейной передачи шифратора Snapfone.

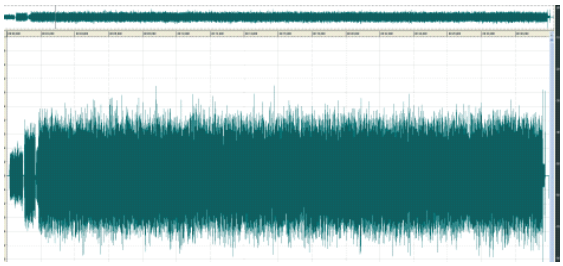

***Рис. 4**. Сигнал линейной передачи шифратора Snapfone*

Результаты тестирования шифратора «Орех-2»

На рис. 5 представлен «стартовый» сигнал синхронизации шифратора «Орех-2» (части «а», «б»).

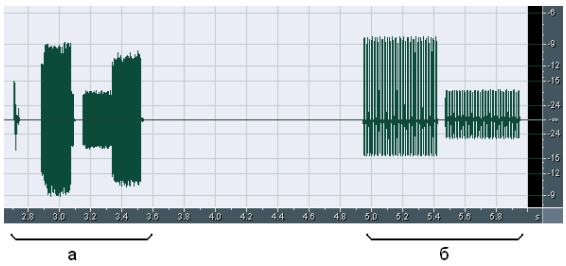

***Рис. 5**. «Стартовый» сигнал синхронизации шифратора «Орех-2» (части «а», «б»)*

На рис. 6 представлена структура линейной передачи шифратора «Орех-2». В начале и конце кадра видны сигналы «подсинхронизации» с частотой 2100 Гц. Наблюдаются временные перестановки кадровой структуры и инверсия речевого сигнала.

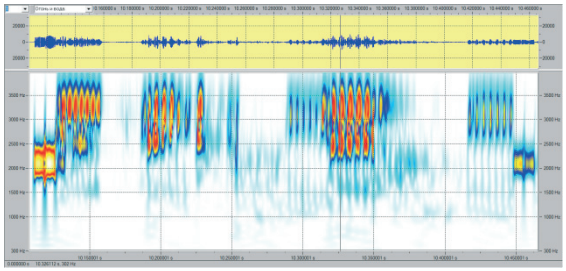

***Рис. 6**. Вейвлет-сонограмма линейной передачи шифратора «Орех-2»*

По результатам тестирования шифратора «Орех-2» можно сделать следующие выводы.

1. Телефонный шифратор относится к аппаратуре аналогового типа (Scramblers). Вид преобразований - временные перестановки (TDS) с общей инверсией сигнала, в отличие от данных разработчика: частотно-временные перестановки (TFS).

2. Речепреобразующее устройство обеспечивает достаточно высокое качество восстановленного сигнала.

3. Время вхождения в синхронизацию не превышает 10 сек.; задержка речевого сигнала в режиме засекречивания составляет 0.64 сек., что в два раза превышает данные разработчика. (Известно, что «комфортные» условия переговоров абонентов обеспечиваются в том случае, если задержка речи не превышает 0.3 сек. [1]).

Программа засекречивания речевых сигналов WAVELET-FONE

Разработка кафедры «Информационная безопасность» МГТУ им. Н.Э. Баумана предназначена для обеспечения безопасности речевой связи на коммутируемых телефонных каналах сети общего пользования [4]. Засекречивание передаваемой информации осуществляется многоуровневым вейвлет-преобразованием речевого сигнала по заданному ключу с последующим его восстановлением на приемном конце. Основные характеристики: общее количество ключей: 1,3×1015; диапазон рабочих частот 300 – 3400 Гц; частота дискретизации 8000 Гц, разрядность 16 бит.

Отличительные особенности: возможность построения многоуровневой защиты речевой информации с адаптацией под канал связи; повышенное качество восстановленного речевого сигнала по сравнению с аппаратурой засекречивания, использующей алгоритмы быстрого преобразования Фурье [12]; асинхронный режим работы.

Результаты тестирования программы WAVELET-FONE

На рис. 7 представлена блок-схема алгоритма засекречивания речи. Развернутое описание многоуровневого вейвлет-преобразования программы WAVELET-FONE при шифровании речевого сигнала приведено в [13].

На рис. 8 представлена сонограмма тестовой записи речевого сигнала в 2-х канальном частотном режиме засекречивания.

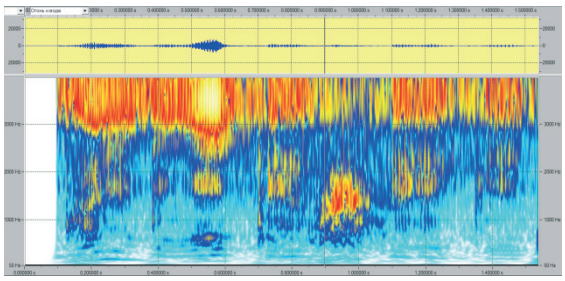

***Рис. 8**. Вейвлет-сонограмма тестовой записи речевого сигнала в 2-х канальном частотном режиме засекречивания*

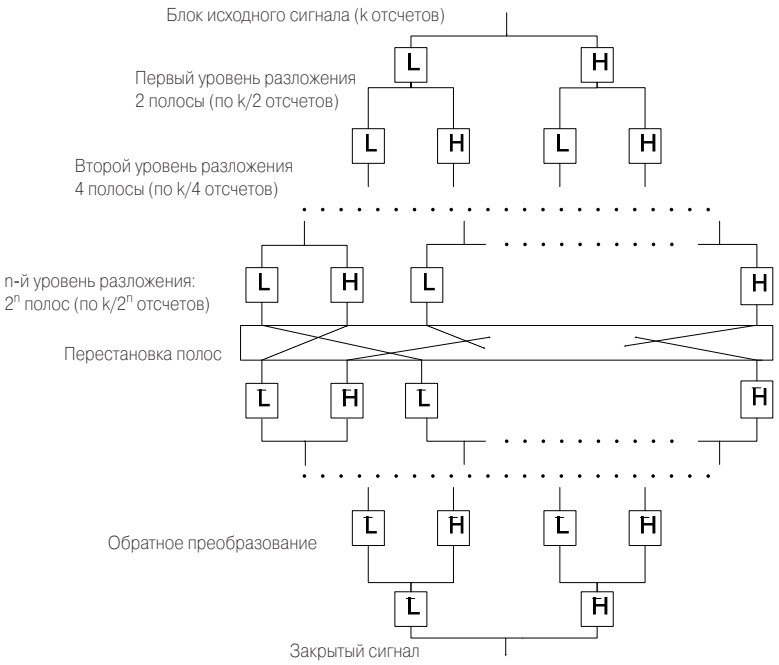

Рис. 7. *Блок-схема алгоритма засекречивания речи программы WAVELET-FONE*

На рис. 9 - сонограмма восстановленного речевого сигнала.

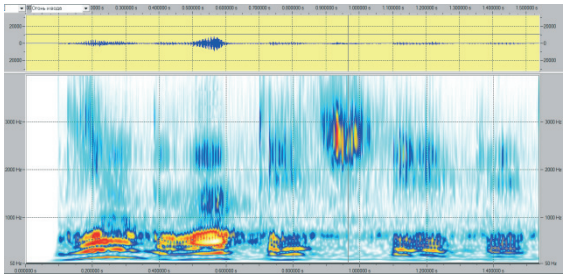

Рис. 9. *Вейвлет-сонограмма восстановленного речевого сигнала*

В программе WAVELET-FONE задан набор вейвлетов: Coiflet, Daubechies, Shannon. Преобразования речевых сигналов (рис. 8, 9) получены с использованием вейвлета Shannon (рис. 10):

$$\psi(x,z) = sc\left(\frac{-2\pi^2 x}{z^2}\right)e^{2i\pi x}, \qquad sc(a) = \frac{\sin(\pi a)}{\pi a}$$

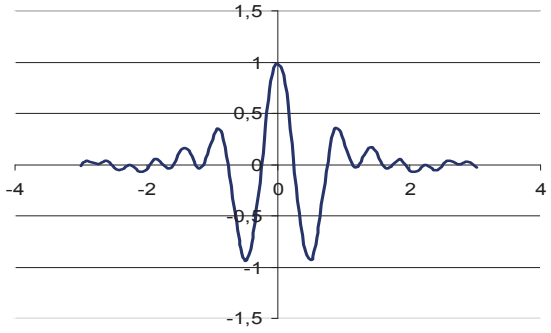

Рис. 10. *Вид вейвлета Shannon*

Тестирование засекречивающих преобразований программы WAVELET-FONE выполнялось средствами анализа RightMark Audio Analyzer 6.2.1. и WaveView-MWA.

Параметры речепреобразующего тракта программы засекречивания: неравномерность АЧХ (в полосе от 40 Гц до 15 кГц) +0.02, -0.01 дБ; нелинейные искажения 0.011%; уровень шума -91,7 дБ; интермодуляционные искажения 0.018 %.

По результатам тестирования следует, что засекречивающие преобразования программы WAVELET-FONE относятся к аналоговым (Scramblers). Вид преобразований - частотные перестановки (FDS). За счет незначительных суммарных искажений речепреобразующего тракта обеспечивается высокое качество восстановленного речевого сигнала.

Заключение

Проведенные исследования подтвердили целесообразность тестирования аппаратно-программных средств засекречивания речевой информации коммерческого применения.

С использованием разработанной методики получены объективные первичные характеристики шифратора дискретного типа «Snapfone» и аналогового - «Орех-2». Тестирование программы засекречивания речи WAVELET-FONE показало, что она может найти применение для защиты биомедицинских акустических сигналов - звуков

сердца и легких в соответствии с требованиями стандарта ISO/IEC 24745:2011 «Информационные технологии: - методы обеспечения безопасности; - защита биометрической информации». Необходимый уровень криптографической защиты, при передаче биометрической информации по каналам связи, может быть обеспечен введением предварительного шифрования биомедицинских сигналов.

Литература

1. Кравченко В.Б. Защита речевой информации в каналах связи // Специальная техника. 1999. № 4. С. 2-9; № 5. С. 2-11.
2. Горшков Ю.Г. Засекречивание речи на каналах связи стандарта GSM // Вопросы кибербезопасности. 2013. № 1(1). С. 55-60.
3. Горшков Ю.Г. Анализ и засекречивание речевого сигнала: Учебное пособие. М.: Издательство МГТУ им. Н.Э. Баумана. 2007. 36 с.
4. Горшков Ю.Г. Новые решения речевых технологий безопасности // Специальная техника. 2006. № 4. С. 41-47.
5. G. Dhanya, J. Jayakumari. A Review of Analog Speech Scrambling for Secure Communication. Progress In Science and Engineering Research Journal ISSN 2347-6680 (E), Vol 02, Issue: 04/06, July-August 2014, pp.194-198.
6. H. Beker, F. Piper. Secure Speech Communications. New York, NY: Academic Press. 1985. 267 p.
7. H.H. Kohad, V.R. Ingle, M.A. Gaikwad. An Overview of Speech Encryption Techniques. International Journal of Engineering Research and Development. e-ISSN: 2278-067X, p- ISSN: 2278-800X, Vol 3, Issue 4, August 2012, pp. 29-32.
8. B. Goldburg, E. Dawson, S. Sridharan. The automated cryptanalysis of analog speech scramblers. Advances in Cryprology: Proceedings of EUROCRYPT91. New York Springer- Verlag, 1991, pp. 422-430.
9. B. Goldburg, S. Sridharan, E.Dawson. Design and Cryptanalysis of Transform-Based Analog Speech Scramblers. IEEE Journal on Selected Areas in Communications, Vol 11, No 5, June 1993, pp. 735-744.
10. 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. 2011. № 4. С. 78-87.
11. Горшков Ю.Г. Многоуровневый вейвлет-анализ акустических сигналов при решении задач фоноскопической экспертизы // Материалы XX Международной научной конференции «Информатизация и информационная безопасность правоохранительных органов». 24-25 мая 2011. Москва. С. 379-387.
12. Djamel Kehil, Youcef Ferdi, Sahim Kissar. Speech Encryption Using FFT Transform with Enhanced Security. International Review on Computers and Software, Vol 4, No 4, July 2009, pp. 447-451.
13. Горшков Ю.Г., Кузин А.Ю., Цирлов В.Л. Засекречивание речевой информации на основе вейвлетов // Вестник МГТУ им. Н.Э. Баумана. Серия: Приборостроение. 2011. № SPEC. С. 138-145.

References

1. Kravchenko V.B. Zaschita rechevoy informatsii v kanalah svyazi // Spetsialnaya tehnika, 1999, No 4, pp. 2-9; No 5, pp. 2-11.
2. Gorshkov Yu.G. Zasekrechivanie rechi na kanalah svyazi standarta GSM // Voprosyi kiberbezopasnosti, 2013, No 1(1), pp. 55-60.
3. Gorshkov Yu.G. Analiz i zasekrechivanie rechevogo signala: Uchebnoe posobie. M.: Izdatelstvo MGTU im. N.E. Baumana, 2007, 36 p.
4. Gorshkov Yu.G. Novyie resheniya rechevyih tehnologiy bezopasnosti // Spetsialnaya tehnika, 2006, No 4, pp. 41-47.
5. G. Dhanya, J. Jayakumari. A Review of Analog Speech Scrambling for Secure Communication. Progress In Science and Engineering Research Journal ISSN 2347-6680 (E), Vol 02, Issue: 04/06, July-August 2014, pp.194-198.
6. H. Beker, F. Piper. Secure Speech Communications. New York, NY: Academic Press, 1985, 267 p.
7. H.H. Kohad, V.R. Ingle, M.A. Gaikwad. An Overview of Speech Encryption Techniques. International Journal of Engineering Research and Development. e-ISSN: 2278-067X, p- ISSN: 2278-800X, Vol 3, Issue 4, August 2012, pp. 29-32.
8. B. Goldburg, E. Dawson, S. Sridharan. The automated cryptanalysis of analog speech scramblers. Advances in Cryprology: Proceedings of EUROCRYPT91. New York Springer-Verlag, 1991, pp. 422-430.
9. B. Goldburg, S. Sridharan, E.Dawson. Design and Cryptanalysis of Transform-Based Analog Speech Scramblers. IEEE Journal on Selected Areas in Communications, Vol 11, No 5, June 1993, pp. 735-744.
10. Gorshkov Yu.G. Issledovatelskiy kompleks chastotno-vremennogo analiza rechevogo signala s ispolzovaniem veyvlet-tehnologii // Vestnik MGTU im. N.E. Baumana. Seriya: Priborostroenie, 2011, No 4, pp. 78-87.
11. Gorshkov Yu.G. Mnogourovnevyiy veyvlet-analiz akusticheskih signalov pri reshenii zadach fonoskopicheskoy ekspertizyi // Materialyi XX Mezhdunarodnoy nauchnoy konferentsii «Informatizatsiya i informatsionnaya bezopasnost pravoohranitelnyih organov», 24-25 maya 2011, Moskva, pp. 379-387.
12. Djamel Kehil, Youcef Ferdi, Sahim Kissar. Speech Encryption Using FFT Transform with Enhanced Security. International Review on Computers and Software, Vol 4, No 4, July 2009, pp. 447-451.
13. Gorshkov Yu.G., Kuzin A.Yu., Tsirlov V.L. Zasekrechivanie rechevoy informatsii na osnove veyvletov // Vestnik MGTU im. N.E. Baumana. Seriya: Priborostroenie, 2011, No SPEC, pp. 138-145.