# VOICE CODER MOBILE — НОВОЕ РЕШЕНИЕ ПО ЗАЩИТЕ ПЕРЕГОВОРОВ В СЕТЯХ СОТОВОЙ СВЯЗИ


В.Смирнов
signal@gin.ru

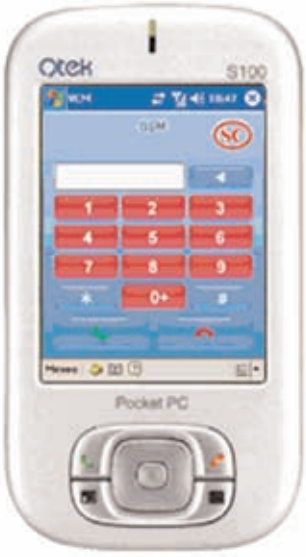
**Тема прослушивания телефонных переговоров давно не нова. Достаточно вспомнить термин "нетелефонный разговор", прочно вошедший в лексику граждан еще в советские времена. Однако в последнее время, с совершенствованием технологий передачи и обработки информации, эта тема получила новое развитие. Контролировать несанкционированный доступ к линии – дело дорогое, неблагодарное и практически нереализуемое, поэтому обеспечить полную безопасность переговоров без применения специальных устройств защиты невозможно. В компании "Сигнал-КОМ" разработан ряд программных и программно-аппаратных комплексов, предназначенных для защиты информации при ее хранении и передаче по каналам связи. Об одном из них и пойдет речь.**

В прессе пишут о скандалах в высших эшелонах власти ряда стран, связанных с прослушиванием переговоров высокопоставленных чиновников. Это заставляет серьезно задуматься о проблеме защиты от прослушивания. Сейчас этим вопросом озабочены не только службы безопасности, но и представители органов власти, политики, бизнесмены и простые граждане. Слишком велика бывает цена от потери самой незначительной информации, даже не являющейся какой-либо тайной. Особое беспокойство вызывает безопасность переговоров в сетях сотовой связи, несанкционированный доступ к которым можно получить не только через оборудование провайдеров, но и путем эфирного перехвата информации.

В соответствии с Уголовным кодексом Российской Федерации деятельность по несанкционированному прослушиванию телефонных переговоров преследуется по закону. Однако без принятия соответствующих защитных мер нельзя быть уверенным в полной безопасности – тем более, что к прослушиванию часто привлекаются бывшие сотрудники спецслужб, вооруженные многолетним опытом и соответствующей техникой.

Сейчас для защиты переговоров используется либо скремблерное, либо вокодерное оборудование. При этом только вокодерное оборудование, обеспечивающее передачу речи в цифровом виде с использованием шифрования, обладает гарантированной стойкостью засекречивающих преобразований и позволяет полностью защитить абонентов от прослушивания.

Программно-аппаратные комплексы для защиты сотовой телефонии, реализующие вокодерные преобразования,




**Программный комплекс Voice Coder Mobile**

**Технические характеристики комплекса Voice Coder Mobile**

| | | |
|---|---|---|
| Схема защиты речевого сигнала | Вокодер – шифратор – модем | |
| Режим связи (защищенный) | Полный дуплекс | |
| Стандарт сети | Сети сотовой связи | GSM-900/1800 |
| | Требования к оператору | Наличие услуги передачи данных – CSD |
| | Скорость/режим передачи данных | 9600 бит/с / асинхронный (прозрачный и непрозрачный) |
| Защита информации | Алгоритм шифрования | ГОСТ 28147-89 |
| | Ключевая система | Сеансовые ключи на основе протокола Диффи-Хэллмана на эллиптических кривых – ECDH (Elliptic Curve Diffie-Hellman) |
| | Метод распределения ключей | Инфраструктура Открытых Ключей на базе Удостоверяющего Центра e-Notary, генерация ключей – на стороне абонента. Опционально поддерживается режим работы без сертификатов |
| | Длина ключа | 256 бит |
| | Ключевая мощность | 10e+77 |
| Речевые преобразования | Программная реализация | Процессоры семейства ARM с частотой не ниже 400 МГц |
| | Алгоритм сжатия речи | TETRA (4800 бит/с) |
| | Слоговая разборчивость речи | 97% |
| | Эхокомпенсатор | Уровень подавления эха 20–25 дБ |
| Особенности реализации | Пользовательский интерфейс | В виде графического номеронабирателя с возможностью вызова абонентов из справочника "Контакты" |
| | Контроль безопасности | В режиме без сертификатов контроль атаки типа "man-in the middle" |
| | Требования к операционной системе | Windows Mobile 2003 / Windows Mobile 5.0 |

представляют собой высокотехнологичное оборудование. Стоимость его на российском рынке в зависимости от фирмы-производителя колеблется от 2000 до 4000 долл., что ограничивает число его потребителей.

С появлением нового класса интеллектуальных мобильных устройств (коммуникаторов и смартфонов) специалистам компании "Сигнал-КОМ" удалось создать относительно недорогое программное решение для защиты переговоров.

Voice Coder Mobile (VCM) – это программный комплекс, предназначенный для широкого класса мобильных устройств. VCM включает в себя высококачественный модуль параметрического сжатия речевого сигнала (вокодер) на скорости 4800 бит/с, модули синхронизации, криптографии, эхокомпенсации и другие устройства, работающие по сложнейшим алгоритмам в режиме реального времени.

В качестве системы управления ключевой информацией используется Инфраструктура Открытых Ключей (Public Key Infrastructure – PKI) на базе Удостоверяющего Центра (УЦ) e-Notary компании "Сигнал-КОМ". PKI позволяет создавать корпоративные и публичные защищенные виртуальные сети сотовой связи, которые предусматривают строгую аутентификацию абонентов, адресное шифрование информации и ведение сетевых телефонных справочников ограниченного доступа на сайте УЦ (www.e-notary.ru). Каждый абонент имеет возможность самостоятельно изготовить секретный и открытый ключи, сформировать запрос и получить сертификат, соединившись с УЦ e-Notary через Интернет. Тот факт, что генерация ключей производится самим абонентом, гарантирует, что никто не сможет расшифровать передаваемую информацию и прослушать разговор.

Опционально комплекс VCM поддерживает и режим работы без сертификатов. В этом случае все его защитные свойства сохраняются, но не обеспечивается строгая криптографическая аутентификация абонентов и не поддерживаются функции телефонных справочников.

Основные технические характеристики комплекса Voice Coder Mobile приведены в таблице.

В настоящее время программный комплекс действует на базе мобильных устройств, оснащенных процессором семейства ARM с тактовой частотой не ниже 400 мГц под управлением ОС Windows Mobile 2003/Windows Mobile 5.0. Однако в ближайшем будущем компания планирует создать версию, управляемую ОС Symbian 9.0. Это существенно расширит перечень используемых мобильных устройств.