ЗАЩИТА ГОЛОСОВОЙ ИНФОРМАЦИИ В СЕТЯХ ПОДВИЖНОЙ РАДИОСВЯЗИ

Дударенков А.О., Зельманский О.Б.

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Зельманский О.Б. – к.т.н.,доцент

Для защиты речевой информации в сетях подвижной радиосвязи предлагается программно-аппаратный модуль, обеспечивающий предварительное шифрование речевой информации до ее передачи на мобильное устройство и соответствующее дешифрование на выходе принимающего мобильного устройства.

В настоящее время тема обеспечения конфиденциальности речевой информации при использовании сетей подвижной радиосвязи остается одним из проблемных пунктов в организации информационной безопасности. В связи с чем, защита речевой информации в сетях подвижной радиосвязи является повседневной задачей. В большинстве случаев данная задача решается путем шифрования речевой информации на основе программных средств, что не позволяет подтвердить отсутствие незадекларированных возможностей и оценить их эффективность. Таким образом, задача защиты речевой информации, передаваемой по сетям радиосвязи, является весьма актуальной.

Исследование стандартов мобильной связи GSM, UTMS, LTE, целью которого был анализ инструментов обеспечения безопасности переговоров, показало большое количество существующих уязвимостей в алгоритмах шифрования, ставящих под угрозу вопрос конфиденциальности информации во время разговора. Использование базисных компонентов кодирования речи, таких как скремблеры или вокодерные системы, возможно в совокупности с криптографическими алгоритмами с целью имитации шума для дополнительного снижения разборчивости речи.

Соответственно для защиты речевой информации предлагается программно-аппаратный модуль, который подключается к мобильному устройству связи и осуществляет шифрование речевого сигнала до его непосредственной подачи в мобильное устройство.

При разработке программно-аппаратного модуля были изучены уже имеющиеся мировые аналоги, опыт и методы обеспечения безопасности переговоров популярными производителями смартфонов [1-7]. Исследование операционной систем Android показало, что в ней практически не имплементированы какие-либо инструменты защиты информации и имеется много уязвимостей, связанных с получением прав полного доступа к ядру. В свою очередь операционная система iOS позволяет осуществлять процессинг программ на виртуальной машине [8].

Первым этапом разработки стало создание программного модуля, обеспечивающего шифрование и дешифрование речевого сигнала. Для этого была применена библиотека классов NAudio на базе языка программирования C#. Тестирование программного модуля выглядит следующим образом. Исходный аудиофайл, содержащий речь, загружается в программное средство Wave Viewer и воспроизводится акустической системой. Данные, загруженные и отображаемые в средстве Wave Viewer, шифруются, а результаты сохраняются в аудиофайле. После этого данный аудиофайл, содержащий зашифрованный сигнал, также загружается в программное средство Wave Viewer, воспроизводится и записывается с помощью микрофона уже другого персонального компьютера или телефона. Затем записанный зашифрованный аудио сигнал расшифровывается, загружается в программное средство Wave Viewer и воспроизводится акустической системой.

Вторым этапом является разработка аппаратной составляющей с целью установки на нее разработанного программного модуля, что позволит получить независимый программно-аппаратный модуль совместимый с большинством мобильных устройств.

Список использованных источников:

17. Архитектура BlackBerry [Электронный ресурс]. – Режим доступа : https://us.blackberry.com/enterprise/blackberry-connect/.

18. Техника для спецслужб. Крипто смарт телефон «Cancort» [Электронный ресурс]. – Режим доступа : www.sis-tss.ru/2010-06-26-06-44-58/7817-kripto-smart-telefon-cancort.html.

19. Технология криптофон [Электронный ресурс]. – Режим доступа : www.cryptophone.de/en/background/cryptophone-technology/encryption-engine/

20. Скремблер «Guard Bluetooth» компании «Логос» [Электронный ресурс]. – Режим доступа : http://www.shpionam.net/skrembler-guard-bluetooth.html.

21. Техника для спецслужб. Устройство для защиты разговоров по смартфону «Референт PDA» [Электронный ресурс]. – Режим доступа : http://www.bnti.ru/des.asp?itm=3630&tbl=04.03.05.02.

22. Техника для спецслужб. Криптотелефон «StealthPhone» [Электронный ресурс]. – Режим доступа : www.bnti.ru/des.asp?itm=6220&tbl=04.03.07.02.

23. Aparna R. A Review on Cryptographic Algorithms for Speech Signal Security / Chitra D. P. // ITETICS – 2016 – №5.

24. Стандрат iOS11 2018 [Электронный ресурс] : Datasheet / Apple. – Режим доступа : https://apple.com/business/docs/iOS_Security_Guide.pdf.