

РАЗРАБОТКА СИСТЕМЫ КОМПЛЕКСНОЙ ЗАЩИТЫ ИНФОРМАЦИИ СЕТИ СТАНДАРТА GSM

к.т.н., доц. С.Ю. Гавриленко, В.К. Шаповалов, НТУ "ХПИ", г. Харьков

Проанализированы средства и алгоритмы защиты информации в телекоммуникационных сетях стандарта GSM от несанкционированного прослушивания переговоров и клонирования SIM-карты [1 – 5]. Рассмотрен и реализован на языке низкого уровня алгоритм шифрования A5/3, используемый в GSM сетях третьего поколения. Проанализирована криптостойкость алгоритма A5/3, а так же способы улучшения стойкости к атакам и защита от них. Рассмотрены характеристики и особенности реализации единственного сертифицированного в Украине алгоритма шифрования ГОСТ 28147-89. Предложены способы улучшения криптостойкости алгоритма, используемого в сетях мобильной связи, путем внедрения в комплекс алгоритма шифрования ГОСТ 28147-89. Разработана система комплексной защиты информации сети стандарта GSM на основе использования двух алгоритмов A5/3 и ГОСТ28147-89 с последовательной структурой работы шифрования на языке высокого уровня. Проанализированы результаты работы системы, установлены особенности работы и технические характеристики. Проведен сравнительный анализ результатов разработки и установлены следующие достоинства разработанного алгоритма:

- бесперспективность силовой атаки (XSL-атаки в учёт не берутся, так как их эффективность на данный момент полностью не доказана);
- эффективность реализации и соответственно высокое быстродействие на современных мобильных телефонах;
- наличие защиты от навязывания ложных данных (выработка имитовставки) и одинаковый цикл шифрования.

Список литературы: 1. Защита информации в системах мобильной связи: Учебное пособие для вузов. / А.А. Чекалкин, А.В. Заряев, С.В. Скрыль, В.А. Вохминцев и др.; под. общ. ред. А.В. Заряева и С.В. Скрыля. – 2-е изд. испр. и доп. – М.: Горячая линия – Телеком, 2005. – 171 с. 2. Громаков Ю.А. Стандарты и системы подвижной радиосвязи / Ю.А. Громаков. – М.: Эксперт, 1998. – 240 с. 3. Весоловский К. Системы подвижной радиосвязи / К. Весоловский. – М.: Горячая линия – Телеком, 2006. – С. 529. 4. Комашинский В.И. Системы подвижной радиосвязи с пакетной передачей информации. Основы моделирования. / В.И. Комашинский, А.В. Максимов. – М.: Горячая линия – Телеком, 2007. – 173 с. 5. Шнайер Б.И. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке С. / Б.И. Шнайер. – М.: Триумф, 2002. – 816 с.