УДК 004.056

# АЛГОРИТМ ФОРМИРОВАНИЯ КЛЮЧА ШИФРОВАНИЯ В SIM-КАРТЕ

Магистрант Волчанин С.В.
Канд. техн. наук, доцент Лихачевский Д.В.
Белорусский государственный университет информатики и радиоэлектроники

Аутентификация (авторизация идентификатора абонента) позволяет избежать клонирования мобильного телефона абонента – абоненту назначается временный идентификационный номер пользователя IMSI, а так же индивидуальный 128-битный ключ авторизации Ki. Ключ Ki известен двум сторонам. В аутентификации используется SIM-карта и Центр Авторизации (Authentication Center AuC). Auc генерирует 128 битовое значение RAND и посылает мобильной станции (MC), в ответ получает 32-битное значение SRES=A3(RAND, Ki), которое сравнивает с вычисленным самостоятельно тем же алгоритмом A3.

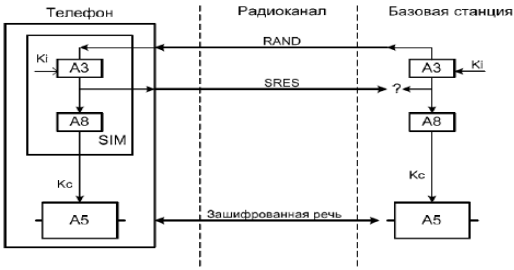


Рисунок 1 – Идентификация в стандарте GSM

Алгоритмом A8 на MC используя полученный RAND и имеющийся Ki, вычисляется сеансовый ключ Kc. Так же, он вычисляется и Центром Авторизации. После чего радиоканал считает шифрованным. Ключ Kc имеет длину 64 бит, образуется добавлением к 54 битам, полученным данным алгоритмом, десяти нулевых битов – это значение и является входом для алгоритма шифрования A5 разговора.

**Литература**

1. Информационная безопасность и защита информации: справочник. В 3 т. / под ред. В.П. Мельников, С.А. Клейменов, А.М. Петраков. – М. : Академия, 2008. – Т. 3. – 336 с.