УДК 621.39

Студ. В.И. Яцкевич, М.С. Клочко
Науч. рук. доц. Н.Н. Буснюк
(Кафедра информационных систем и технологий, БГТУ)

УСТРОЙСТВА И МЕТОДЫ ШИФРОВАНИЯ В СИСТЕМАХ МОБИЛЬНОЙ СВЯЗИ

Устройства шифрования. В мобильной связи устройства шифрования часто используются для защиты конфиденциальных данных, таких как текстовые сообщения, фотографии и банковские данные, которые передаются между мобильными устройствами и сотовыми станциями.

Некоторые мобильные приёмопередатчики имеют встроенные устройства шифрования, которые позволяют защитить хранящуюся на них информацию от несанкционированного доступа. Например, iPhone использует аппаратное шифрование, чтобы защитить данные пользователя, хранящиеся на устройстве.

Также существуют специализированные устройства шифрования для мобильной связи, такие как SIM-карты с защитой данных и USB-ключи для шифрования данных на ПК и мобильных устройствах.

Алгоритмы шифрования. В качестве алгоритма шифрования в GSM используются алгоритмы из семейства A5:

A5/1 – поточный шифр, наиболее распространенный на сегодня.

A5/2-вариант предыдущего алгоритма, но изначально задумывался, как сильно ослабленная версия A5/1. В настоящее время не используется.

A5/3-блочный шифр. Разработан в 2002 году с целью заменить устаревший A5/1. Однако у алгоритма найден ряд уязвимостей и в настоящее время он используется только в 3GPP сетях.

В системах мобильной связи, применяющих для доступа абонентов к каналам связи технологию CDMA, используется блочное шифрование с применением кодов Уолша и Голда, а также псевдослучайных битовых последовательностей.

ЛИТЕРАТУРА

1. Буснюк, Н.Н., Мельянец Г.И. Системы мобильной связи. Учебно-методическое пособие. – Минск : БГТУ, 2018. – 153 с.

2. Голиков А. М. Кодирование и шифрование информации в системах связи. Часть 2. Шифрование. – Изд-во Томского государственного ун-та систем управления и радиоэлектроники, 2016. – 490 с.