**Безопасность GSM сетей: шифрование данных**

**Карпов Денис, ИКТпр-51**

**Поволжский Государственный Университет Телекоммуникаций и Информатики**

Доступность сотовой связи уже давно никого не удивляет. Однако, кажущаяся простота этого явления современности на самом деле содержит в себе немало интересного. Все данные в сети GSM шифруются при помощи новейших алгоритмов защиты сигнала.

Для передачи данных сотовый телефон использует радиоканал, который может быть доступен любому – защитить сигнал можно только при помощи серьезных алгоритмов криптографии. В настоящее время для защиты мобильного сигнала используется алгоритм А5, а с недавнего времени – новая версия А5/3. Подобная система шифрования довольно надежна, но если в руки злоумышленника попадет хотя бы один ключ, то современные компьютеры взломают шифр за считанные секунды.

А5 — это поточный алгоритм шифрования, используемый для обеспечения конфиденциальности передаваемых данных между телефоном и базовой станцией в европейской системе мобильной цифровой связи GSM (Groupe Spécial Mobile).

Шифр основан на побитовом сложении по модулю два (булева операция "исключающее или") генерируемой псевдослучайной последовательности и шифруемой информации. В A5 псевдослучайная последовательность реализуется на основе трёх линейных регистров сдвига с обратной связью. Регистры имеют длины 19, 22 и 23 бита соответственно. Сдвигами управляет специальная схема, организующая на каждом шаге смещение как минимум двух регистров, что приводит к их неравномерному движению. Последовательность формируется путём операции "исключающее или" над выходными битами регистров.

Алгоритм A5 в настоящее время — это целое семейство шифров. Для описания возьмем А5/1, как родоначальника этого семейства. Изменения в производных алгоритмах опишем отдельно.

В этом алгоритме каждому символу открытого текста соответствует символ шифротекста. Текст не делится на блоки (как в блочном шифровании) и не изменяется в размере. Для упрощения аппаратной реализации и, следовательно, увеличения быстродействия используются только простейшие операции: сложение по модулю 2 (XOR) и сдвиг регистра.

Формирование выходной последовательности происходит путём сложения потока исходного текста с генерируемой последовательностью (гаммой). Особенность операции XOR заключается в том, что применённая чётное число раз, она приводит к начальному значению. Отсюда, декодирование сообщения происходит путём сложения шифротекста с известной последовательностью.

В качестве вывода можно сказать, что применяемый уже сейчас алгоритм шифрования A5/3 был взломан группой хакеров, что показывает, что несмотря на всю надёжность и кажущуюся сложность алгоритмов шифрования данных мобильных сетей, необходимо разрабатывать всё новые стандарты, способные сохранить конфиденциальность информации. Это является одной из задач специальности обучения автора.

**Список литературы:**

1. КриптоАРМ [Электронный ресурс]: интернет-портал о шифрах – режим доступа к порталу: <https://cryptoarm.ru/shifrovanie-gsm-svyazi>
2. Википедия [Электронный ресурс]: текстовые электронные данные – режим доступа к порталу: <https://ru.wikipedia.org/wiki/A5_(%D0%B0%D0%BB%D0%B3%D0%BE%D1%80%D0%B8%D1%82%D0%BC_%D1%88%D0%B8%D1%84%D1%80%D0%BE%D0%B2%D0%B0%D0%BD%D0%B8%D1%8F)>