ФОРМИРОВАТЕЛЬ СЛУЧАЙНОЙ ЧИСЛОВОЙ ПОСЛЕДОВАТЕЛЬНОСТИ С ИСПОЛЬЗОВАНИЕМ МЕТЕОРНОГО РАДИОКАНАЛА

Репка М.В.
Научный руководитель – д.т.н., проф. Антипов И. Е.
Харьковский национальный университет радиоэлектроники
(61166, Харьков, пр. Ленина,14, каф. Радиоэлектронных устройств,
тел. (057) 702-14-44)

This paper presents a device for the formation of random number sequences using the meteor-burst channel. The device can be used to protect information transmitted by any channel. The block diagram and working principles are presented in this paper.

Симметричное шифрование – способ шифрования, в котором для шифрования и расшифровывания применяется один и тот же криптографический ключ.

Устройство, рассмотренное в работе, обеспечивает реализацию способа защиты информации с использованием метеорного радиоканала. Представленный в работе способ обеспечивает защиту ключей симметричного шифрования от перехвата.

В данной работе рассмотрен метод формирования СЧП, основанный на измерении интервалов времени между метеорными радиоотражениями. Способ основан на двух физических факторах. Независимо от места и времени возникновения метеорного следа, одновременно излучённые в двух пунктах сигналы, отражаясь от данного следа, принимаются также одновременно. Передний фронт сигнала, отражённого от метеорного следа настолько крутой, что исключает неоднозначность в определении момента начала существования МРК [1]. Скорость изменения амплитуды сигнала при метеорном распространении составляет 400…500 дБ/с [2]. Это даже позволяет использовать его для синхронизации тактового генератора при обмене информацией. Одним из главных достоинств такого метода является простота технической реализации, которая напрямую связана с требованиями, предъявляемыми к стабильности генератора. К немаловажному достоинству следует также отнести отсутствие неоднозначности в определении начала метеорного радиоотражения. Недостатком такого метода является тот факт, что он не обеспечивает какое либо уменьшение зоны возможного пассивного прослушивания канала, образованного отражением от метеорного следа.

Практически данный способ можно реализовать следующим образом. В двух пунктах, оснащённых системой защиты информации с использованием МРК, в эфир непрерывно излучаются зондирующие сигналы с периодом T_s. Количество излучённых сигналов непрерывно считается счётчи-

ками. В момент приёма зондирующего сигнала от удалённого корреспондента (одновременно в обоих пунктах), происходит считывание состояния счётчиков, затем их обнуление и начало нового счёта. Считанная информация (одинаковая в обоих пунктах) равна времени, прошедшему от начала последнего метеорного следа до начала текущего, выраженному в количестве интервалов T_s. Данная информация будет основой для формирования СЧП, с которой будет впоследствии сформирован ключ для симметричного алгоритма шифрования. Основная задача устройства – это подсчёт интервалов между пачками импульсов входного сигнала. Структурная схема формирователя СЧП приведена ниже.

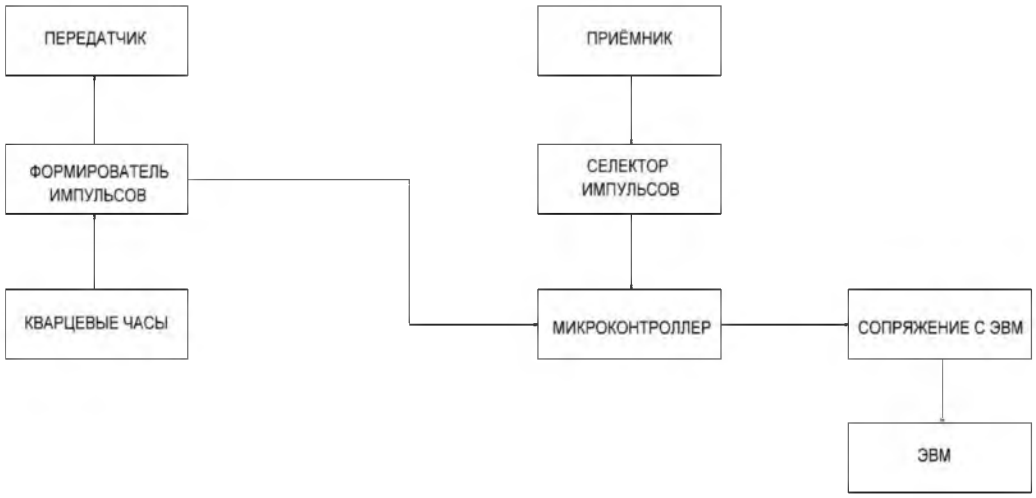

Рисунок 1 – Структурная схема устройства формирователя СЧП

Устройство состоит из микроконтроллера AT90S8515, схемы Max 232 (сопряжение с ЭВМ) и ЭВМ. Для формирования случайной числовой последовательности импульсы входного сигнала подаются на вход МК, который используется для обработки внешних прерываний таймера-счётчика. Когда на вход начинают подаваться импульсы, происходит внешнее прерывание, запускается счётчик таймера, который отсчитывает длительность интервала. После окончания интервала импульсов, значение счётчика передаётся в ЭВМ, регистр обнуляется и МК переходит в режим ожидания следующей пачки импульсов.

Литература:

1. Кащеев Б. Л., Бондарь Б. Г. Метеорная связь. Киев: Учебно-методический кабинет Министерства высшего образования, 1989. –76 с.

2. Антипов И. Е., Бондарь Б. Г., Кащеев Б. Л. О процедуре синхронизации при метеорной связи ; Харьк. ин-т радиоэлектроники. - Харьков, 1993. – 5 с. Деп. в УкрИНТЭИ N 475 – Ук93.