

Поточный шифр на основе шифра Шеннона

РАКИТСКИЙ АНТОН АНДРЕЕВИЧ

Siberian State University of Telecommunication and Information Sciences (Новосибирск), Россия

e-mail: rakitsky.anton@gmail.com

ЧУСОВИТИН АНТОН РОМАНОВИЧ

Siberian State University of Telecommunication and Information Sciences (Новосибирск), Россия

e-mail: antonion2011@yandex.ru

В 2016 году Рябко Б.Я. была доказана теоретическая надёжность двух шифров Шеннона, и на их основе можно построить эффективные и надёжные методы шифрования данных. В данной работе представлен метод поточного шифрования данных, передаваемых по сети, на базе одного из шифров Шеннона. Подробно описаны особенности его реализации, и представлены результаты экспериментального исследования надёжности такого шифрования.