АУТЕНТИФИКАЦИЯ ПОЛЬЗОВАТЕЛЬСКИХ ДАННЫХ И ИХ ОТПРАВИТЕЛЯ НА ОСНОВЕ АЛГОРИТМА ГОСТ 28147-89

А.М. Тимофеев[1], А.А. Корчинский[2], Д.А. Телипко[2]

[1]*Учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», Минск, Беларусь*

[2]*Учреждение образования «Национальный детский технопарк», Минск, Беларусь*

Одной из основных задач в сфере информационной безопасности является аутентификация пользовательских данных и их отправителя [1]. Для решения этой задачи, в частности, используют криптографические методы и средства, основанные на применении электронных цифровых подписей (ЭЦП) [1, 2]. Однако известные алгоритмы ЭЦП требуют достаточно больших вычислительных ресурсов легитимных пользователей за счет выполнения таких операций, как, например, генерация больших простых чисел, выселение корней квадратных по простому и по составному модулям, возведение в степень больших чисел в большую степень и др. В этой связи целесообразно создавать криптосистемы, которые позволяют решать задачи аутентификации пользовательских данных и их отправителя и, вместе с тем, по сравнению с существующими криптосистемами, более простые в реализации, что являлось целью данной работы. В качестве объекта исследования выбран алгоритм ГОСТ 28147-89. Создана компьютерная программа, которая осуществляет криптографические операции, свойственные для криптосистем симметричного типа. Предложена криптосистема, позволяющая выполнять аутентификацию пользовательских данных, а также проверять подлинность их отправителя на основе симметричного блочного алгоритма ГОСТ 28147-89, которая упрощает известные алгоритмы ЭЦП. Применительно к предложенной криптосистеме выполнены исследования по оценке криптостойкости и среднего времени, необходимого для формирования подписи и ее верификации для легитимных пользователей.

Список литературы

1. Бабенко, Л. К. Криптографическая защита информации: симметричное шифрование / Л. К. Бабенко. – М., Издательство Юрайт, 2020.

2. Милославская, Н. Г. Научные основы построения центров управления сетевой безопасностью в информационно-телекоммуникационных сетях / Н. Г. Милославская. – М., Горячая линия-Телеком, 2021.