

МИНИСТЕРСТВО ОБРАЗОВАНИЯ РЕСПУБЛИКИ БЕЛАРУСЬ
БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
МЕХАНИКО-МАТЕМАТИЧЕСКИЙ ФАКУЛЬТЕТ
Кафедра веб-технологий и компьютерного моделирования

ВЛАДЫКОВСКИЙ
Дмитрий Анатольевич

Аннотация к дипломной работе:

**АППАРАТНО-ПРОГРАММНОЕ СРЕДСТВО ДЛЯ
БЛОЧНОГО ШИФРОВАНИЯ ИНФОРМАЦИИ**

Научный руководитель:
старший преподаватель
Вельченко С.А.

Минск, 2023

РЕФЕРАТ

Дипломная работа содержит 64 страницы, 24 рисунка, 3 таблицы, 1 приложение.

Ключевые слова: ШИФРОВАНИЕ, БЛОЧНОЕ ШИФРОВАНИЕ, ПОТОКОВОЕ ШИФРОВАНИЕ, ГОСТ 28147-89.

Цель работы: разработка аппаратно-программного средства для блочного шифрования информации по открытым каналам связи.

Результатом работы является реализация аппаратно-программного средства для защиты информации путем блочного шифрования. В качестве алгоритма шифрования использовался ГОСТ 28147-89. С помощью данного решения можно зашифровать или расшифровать необходимую текстовую информацию для дальнейшего хранения или передачи посредством открытых каналов связи. Предусмотрена возможность шифрования русского и английского языков, загрузку исходников и сохранение результата.

Данная работа принята к публикации на 80-ой научной конференции студентов и аспирантов Белорусского государственного университета, Минск, 10–21 мая 2023 г.

ABSTRACT

The thesis consists of 64 pages, 24 figures, 3 tables, 1 appendix.

Keywords: ENCRYPTION, BLOCK ENCRYPTION, STREAM ENCRYPTION, GOST 28147-89.

Purpose of the work: development of hardware and software tools for block encryption of information over open communication channels.

The result of the work is the implementation of a hardware and software tool for protecting information by block encryption. GOST 28147-89 was used as the encryption algorithm. With this solution, it is possible to encrypt or decrypt the necessary textual information for further storage or transmission through open communication channels. It is possible to encrypt the Russian and English languages, download the source code and save the result.

This work was accepted for publication at the 80th Scientific Conference of students and postgraduates of the Belarusian State University, Minsk, May 10-21, 2023.