Министерство образования Республики Беларусь

Учреждение образования

БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ИНФОРМАТИКИ И РАДИОЭЛЕКТРОНИКИ

Факультет непрерывного и дистанционного обучения

Кафедра информатики

**Индивидуальная практическая работа №1**

по дисциплине

" Методы защиты информации. Часть 2"

Выполнил студент гр. 493551 Авхимович Алексей Валерьевич

E-mail: [droon2112@gmail.com](mailto:droon2112@gmail.com)

Минск 2018

**Часть 2.1. 2. Блочные шифры. AES.**

**Изучите теоретические сведения, содержащие требования к реализации блочных шифров.**

**Цель:** реализовать на языке программирования C++ алгоритм блочного шифрования AES.

**Результат:** Программа шифрования, осуществляющая криптографическое преобразование введенного текста с помощью алгоритма блочного шифрования AES.

**Общая постановка задачи:**  Создать программу, читающую данные из файла, шифрующие и дешифрующие их с помощью алгоритма блочного шифрования AES.

**ЛИТЕРАТУРА**

1. Концепция государственной политики в области информатизации. В ред. указа Президента Республики Беларусь от 07.08.2002 N 433
2. Концепция развития банковской системы Республики Беларусь на 2001 – 2010 годы. Зарегистрировано в Национальном реестре правовых актов Республики Беларусь 29 мая 2002 г. № 1/3717.
3. Концепция развития национальной платежной системы Республики Беларусь до 2010 года с учетом мировых тенденций. Утверждена Постановлением Правления Национального банка Республики Беларусь от 26.05.2004 № 84.
4. Инструкция по организации функционирования автоматизированной системы межбанковских расчетов Республики Беларусь. Зарегистрирована в Национальном реестре правовых актов Республики Беларусь 5 января 2001 г. N 8/4715
5. Гайкович В., Першин А. Безопасность электронных банковских систем. М.: Единая Европа, 1994.