«Инновациялық Еуразия Университетінің Жоғары Екібастұз Колледжі» ЖШС

ТОО «Высший Экибастузский Колледж Инновационного Евразийского

Университета»

Многопрофильное отделение

КУРСОВОЙ ПРОЕКТ

На тему:

«Создание скрипта на Python,для шифрования и дешифрования файлов и архивов»

КП.06120200.1

Руководитель:

\_\_\_\_\_\_\_\_\_С.О. Санатбек

«\_\_\_\_\_»\_\_\_\_\_\_\_\_\_\_\_2024 г.

Выполнил(а) студент:

группы СиБ-322

\_\_\_\_\_\_\_\_\_\_ Басаргин Д.Д

«\_\_\_\_\_»\_\_\_\_\_\_\_\_\_\_\_\_2024 г

Экибастуз 2024

**СОДЕРЖАНИЕ**

|  |  |
| --- | --- |
| Введение | 3 |
| 1.Шифрование AES |  |
| 1.1 Что такое шифрование АES |  |
| 1.2 |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |

1. **Шифрование AES**

**AES** (англ. *Advanced Encryption Standard*;также *Rijndael*, [rɛindaːl] — *рейндал*) — симметричный алгоритм блочного шифрования (размер блока 128 бит, ключ 128/192/256 бит), принятый в качестве стандарта шифрования правительством США по результатам конкурса AES. Этот алгоритм хорошо проанализирован и сейчас широко используется, как это было с его предшественником DES. Национальный институт стандартов и технологий США (англ. *National Institute of Standards and Technology*, NIST) опубликовал спецификацию AES 26 ноября 2001 года после пятилетнего периода, в ходе которого были созданы и оценены 15 кандидатур. 26 мая 2002 года AES был объявлен стандартом шифрования. По состоянию на 2009 год AES является одним из самых распространённых алгоритмов симметричного шифрования. Поддержка ускорения AES была введена фирмой Intel в семейство процессоров x86 начиная с Arrandle в 2010 году, а затем на процессорах Sandy Bridge; фирмой AMD — в Bulldozer с 2011 года.