МИНИСТЕРСТВО ОБРАЗОВАНИЯ РЕСПУБЛИКИ БЕЛАРУСЬ

УЧРЕЖДЕНИЕ ОБРАЗОВАНИЯ

“БРЕСТСКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ”

**ИНТЕЛЕКТУАЛЬНЫЕ ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ**

ОТЧЁТ

По лабораторной работе № \_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Выполнил:

Студент группы ИИ-22

Копанчук Евгений Романович

Проверил\_\_:

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Брест – 2023

**Ход работы**

**TEST MILLER RABIN**

|  |
| --- |
| #include <iostream>  #include <iomanip>  #include <string>  #include <cmath>  #include <vector>  #include <ctime>  using namespace std;  long long mulmod(long long a, long long b, long long m) {  long long res = 0;  a %= m;  while (b > 0) {  if (b % 2 == 1) {  res = (res + a) % m;  }  a = (a \* 2) % m;  b /= 2;  }  return res;  }  long long powmod(long long a, long long b, long long m) {  long long res = 1;  while (b > 0) {  if (b % 2 == 1) {  res = mulmod(res, a, m);  }  a = mulmod(a, a, m);  b /= 2;  }  return res;  }  bool testMillerRabin(long long n, int k) {  if (n <= 1 || (n > 2 && n % 2 == 0)) {  return false;  }  long long d = n - 1;  int s = 0;  while (d % 2 == 0) {  d /= 2;  s++;  }  for (int i = 0; i < k; i++) {  long long a = rand() % (n - 1) + 1;  long long x = powmod(a, d, n);  if (x == 1 || x == n - 1) {  continue;  }  bool found = false;  for (int r = 1; r < s; r++) {  x = mulmod(x, x, n);  if (x == n - 1) {  found = true;  break;  }  }  if (!found) {  return false;  }  }  return true;  }  int main() {  setlocale(LC\_ALL, "ru");  cout << "Введите число для проверки на простоту: ";  long long n;  cin >> n;  if (testMillerRabin(n, 100))  cout << "Число " << n << " является простым.\n";  else  cout << "Число " << n << " не является простым.\n";  return 0;  } |

**OUTPUT**

|  |
| --- |
|  |