Национальный Исследовательский Университет
«Московский Энергетический Институт»
Кафедра прикладной математики и искусственного интеллекта

Тема: Статистический анализ качества кода.

Студент: Ростовых Александра

Москва 2021

Использование cppcheck

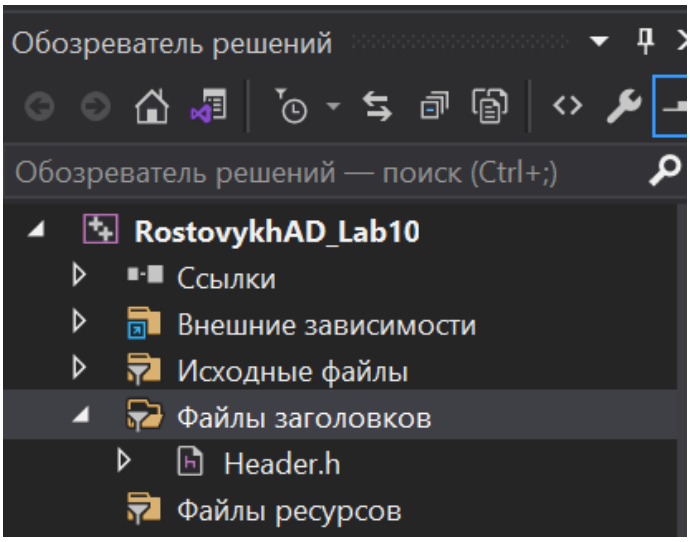
Cppcheck - это инструмент статического анализа кода C / C ++. Он обеспечивает уникальный анализ кода для обнаружения ошибок и фокусируется на обнаружении неопределенного поведения и опасных конструкций кода. Цель состоит в том, чтобы уменьшить количество ложных срабатываний. Cppcheck разработан, чтобы иметь возможность анализировать ваш код C / C ++, даже если он имеет нестандартный синтаксис (распространенный во встроенных проектах).

Цель работы

Научиться проверять качество кода C++ с помощью статического анализатора cppcheck.

1. Создать тестовый проект на C++

Создаем проект на C++. Добавим в проект заголовочный файл Header.h (чтобы понимать, что cppcheck будет просматривать полностью весь проект).



Добавим тестовые функции и тестируемый код в проект:

Файл Header.h:

```
#pragma once
int t() {
	char a[10];
	a[11] = 0;
	return 0;
}
void f() {
	int ct;
	while (ct < 100)
	{
		std::cout << ct;
	}
}
void g() {
	for (int i; i < 1; i++) {
		i++;
```

```
	}
}
double Division(int n, int k) {

	double res = 0;
	return n/k;
}
```

Файл RostovykhAD_Lab10.cpp:

```
#include <iostream>
#include "Header.h"
#include <math.h>
void f(int* ptr) {
	*ptr = 0;
}

void func(int* Arr) {
	Arr = new int[10];
	for (int i = 0; i < 10; i++) Arr[i] = i;
}
bool isNegative(int x)
{
	if (x < 0)
		return true;

}
int main()
{
	struct type1 { int t1; };
	int* a = new int;	// переменная
	int* b = new int[2];  // массив
	delete b;
	delete [] a;
	double d = Division(5, 3);
	double dd = Division(5, 0);
	f();
	g();
	double d1 = 1.5;
	int n = d1;
	int* Ptr = 0;
	func(Ptr);
	for (int i = 0; i < 10; i++) std::cout << Ptr[i] << "  ";
	type1 t;
	std::cout << t.t1;
	bool neg = isNegative(1);
	std::cout << neg;
	int* Ptr1 = 0;
	f(Ptr1);
	double k = sqrt(-3);
	return 0;
}
```

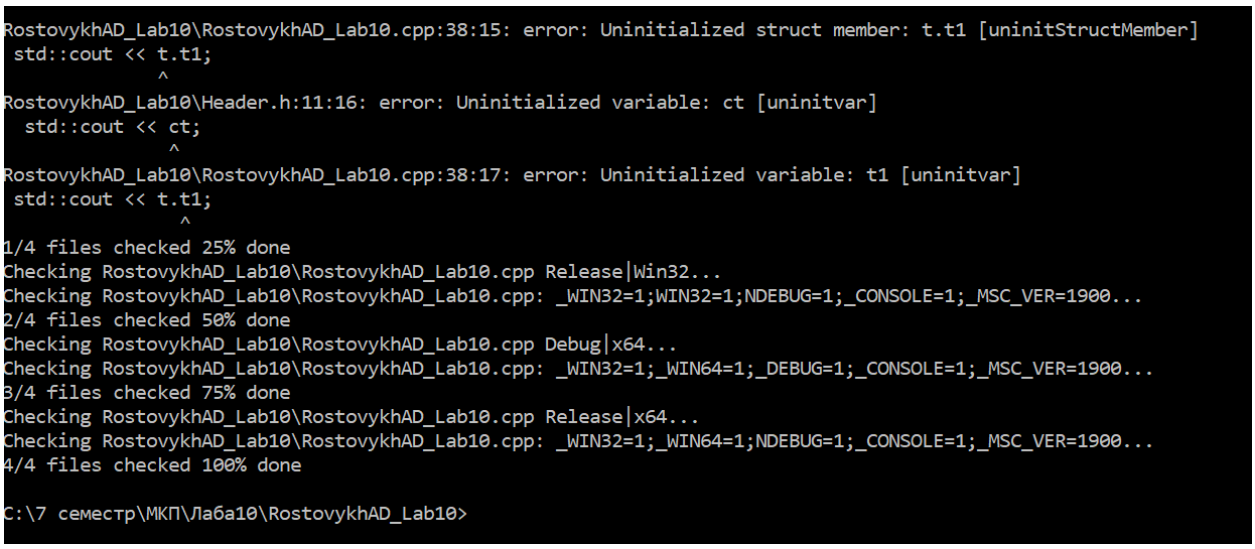
Из приведенного выше кода видно, что он имеет ошибки, такие как, например, выход за границы массива, взятие корня из отрицательного числа, разыменование пустого указателя и так далее.

2. Настроить проверку качества кода с помощью cppcheck после компиляции (через интерфейс командной строки)

Наберем в командной строке следующую команду (предварительно добавив cppcheck после установки в переменную PATH):
C:\7 семестр\МКП\Лаба10\RostovykhAD_Lab10>cppcheck --project=RostovykhAD_Lab10.sln

Данной командой мы проведем анализ всех файлов проекта и увидим следующий результат:

```
C:\7 семестр\МКП\Лаба10\RostovykhAD_Lab10>cppcheck --project=RostovykhAD_Lab10.sln
Checking RostovykhAD_Lab10\RostovykhAD_Lab10.cpp Debug|Win32...
Checking RostovykhAD_Lab10\RostovykhAD_Lab10.cpp: _WIN32=1;WIN32=1;_DEBUG=1;_CONSOLE=1;_MSC_VER=1900...
RostovykhAD_Lab10\Header.h:4:3: error: Array 'a[10]' accessed at index 11, which is out of bounds. [arrayIndexOutOfBounds]
 a[11] = 0;
  ^
RostovykhAD_Lab10\RostovykhAD_Lab10.cpp:18:0: error: Found a exit path from function with non-void return type that has missing
 return statement [missingReturn]
  return true;
^
RostovykhAD_Lab10\RostovykhAD_Lab10.cpp:43:19: error: Invalid sqrt() argument nr 1. The value is -3 but the valid values are '0
.0:'. [invalidFunctionArg]
 double k = sqrt(-3);
                  ^
RostovykhAD_Lab10\RostovykhAD_Lab10.cpp:26:9: error: Mismatching allocation and deallocation: b [mismatchAllocDealloc]
 delete b;
        ^
RostovykhAD_Lab10\RostovykhAD_Lab10.cpp:25:11: note: Mismatching allocation and deallocation: b
 int* b = new int[2];  // P?P°C?C?PёP?
          ^
RostovykhAD_Lab10\RostovykhAD_Lab10.cpp:26:9: note: Mismatching allocation and deallocation: b
 delete b;
        ^
RostovykhAD_Lab10\RostovykhAD_Lab10.cpp:27:12: error: Mismatching allocation and deallocation: a [mismatchAllocDealloc]
 delete [] a;
           ^
RostovykhAD_Lab10\RostovykhAD_Lab10.cpp:24:11: note: Mismatching allocation and deallocation: a
 int* a = new int;      // PїPчC?PчP?P?PчP?P?P°C?
          ^
RostovykhAD_Lab10\RostovykhAD_Lab10.cpp:27:12: note: Mismatching allocation and deallocation: a
 delete [] a;
           ^
RostovykhAD_Lab10\RostovykhAD_Lab10.cpp:8:3: warning: Possible null pointer dereference: ptr [nullPointer]
 *ptr = 0;
  ^
RostovykhAD_Lab10\RostovykhAD_Lab10.cpp:41:14: note: Assignment 'Ptr1=0', assigned value is 0
 int* Ptr1 = 0;
            ^
 int* Ptr1 = 0;
            ^
RostovykhAD_Lab10\RostovykhAD_Lab10.cpp:42:4: note: Calling function 'f', 1st argument 'Ptr1' value is 0
 f(Ptr1);
   ^
RostovykhAD_Lab10\RostovykhAD_Lab10.cpp:8:3: note: Null pointer dereference
 *ptr = 0;
  ^
RostovykhAD_Lab10\RostovykhAD_Lab10.cpp:36:44: error: Null pointer dereference: Ptr [nullPointer]
 for (int i = 0; i < 10; i++) std::cout << Ptr[i] << "  ";
                                           ^
RostovykhAD_Lab10\RostovykhAD_Lab10.cpp:34:13: note: Assignment 'Ptr=0', assigned value is 0
 int* Ptr = 0;
           ^
RostovykhAD_Lab10\RostovykhAD_Lab10.cpp:36:44: note: Null pointer dereference
 for (int i = 0; i < 10; i++) std::cout << Ptr[i] << "  ";
                                           ^
RostovykhAD_Lab10\Header.h:22:10: error: Division by zero. [zerodiv]
 return n/k;
        ^
RostovykhAD_Lab10\RostovykhAD_Lab10.cpp:29:26: note: Calling function 'Division', 2nd argument '0' value is 0
 double dd = Division(5, 0);
                      ^
RostovykhAD_Lab10\Header.h:22:10: note: Division by zero
 return n/k;
        ^
RostovykhAD_Lab10\Header.h:9:9: error: Uninitialized variable: ct [uninitvar]
 while (ct < 100)
        ^
RostovykhAD_Lab10\Header.h:15:14: error: Uninitialized variable: i [uninitvar]
 for (int i; i < 1; i++) {
             ^
RostovykhAD_Lab10\RostovykhAD_Lab10.cpp:27:12: error: Memory is allocated but not initialized: a [uninitdata]
 delete [] a;
           ^
RostovykhAD_Lab10\RostovykhAD_Lab10.cpp:26:9: error: Memory is allocated but not initialized: b [uninitdata]
 delete b;
        ^
```



Ошибка: Выход за границы массива:

RostovykhAD_Lab10\Header.h:4:3: error: Array 'a[10]' accessed at index 11, which is out of bounds. [arrayIndexOutOfBounds]

```
 a[11] = 0;
  ^
```

Ошибка: Функция, определенная как void возвращает значение:

RostovykhAD_Lab10\RostovykhAD_Lab10.cpp:18:0: error: Found a exit path from function with non-void return type that has missing return statement [missingReturn]

```
  return true;
^
```

Ошибка: Взятие корня из отрицательного числа:

RostovykhAD_Lab10\RostovykhAD_Lab10.cpp:43:19: error: Invalid sqrt() argument nr 1. The value is -3 but the valid values are '0.0:'. [invalidFunctionArg]

```
 double k = sqrt(-3);
            ^
```

Ошибка: Несоответствие выделения и удаления памяти:

RostovykhAD_Lab10\RostovykhAD_Lab10.cpp:26:9: error: Mismatching allocation and deallocation: b [mismatchAllocDealloc]

```
 delete b;
       ^
```

Предупреждение: Возможное разыменование пустого указателя:

RostovykhAD_Lab10\RostovykhAD_Lab10.cpp:8:3: warning: Possible null pointer dereference: ptr [nullPointer]

```
 *ptr = 0;
  ^
```

Ошибка: Разыменование пустого указателя:

RostovykhAD_Lab10\RostovykhAD_Lab10.cpp:36:44: error: Null pointer dereference: Ptr [nullPointer]

```
 for (int i = 0; i < 10; i++) std::cout << Ptr[i] << "  ";
                                           ^
```

Ошибка: Деление на ноль:

RostovykhAD_Lab10\Header.h:22:10: error: Division by zero. [zerodiv]
return n/k;
^
RostovykhAD_Lab10\RostovykhAD_Lab10.cpp:29:26: note: Calling function 'Division', 2nd argument '0' value is 0
double dd = Division(5, 0);
^

Ошибка: Неинициализированная переменная:

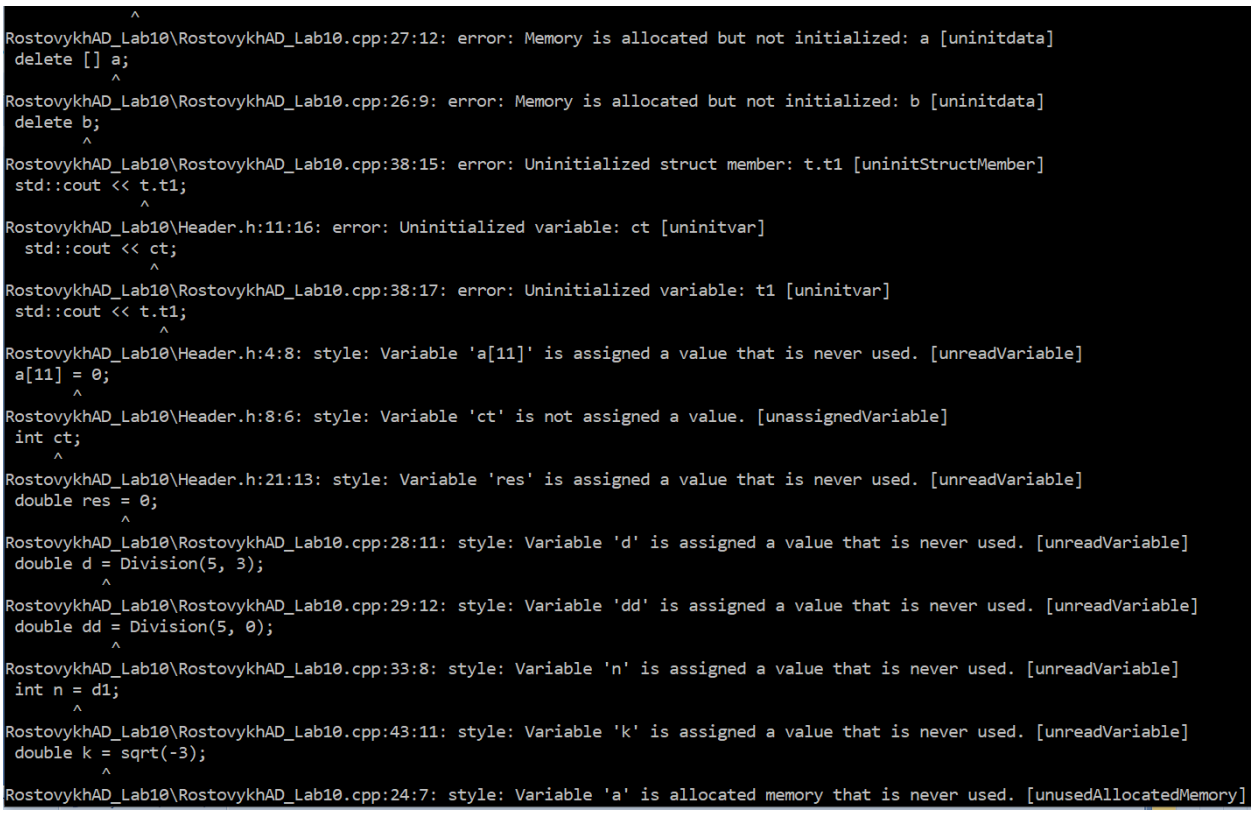
RostovykhAD_Lab10\Header.h:9:9: error: Uninitialized variable: ct [uninitvar]
while (ct < 100)
^

Большинство проверок cppcheck по умолчанию не включает. Среди них следующие категории проверок, каждая из которых может включаться/выключаться независимо:

error — явные ошибки, которые анализатор считает критическими и обычно они приводят к багам (включено по умолчанию);
warning — предупреждения, здесь даются сообщения о небезопасном коде;
style — стилистические ошибки, сообщения появляются в случае неаккуратного кодирования (больше похоже на рекомендации);
performance — проблемы производительности, здесь cppcheck предлагает варианты, как сделать код быстрее (но это не всегда даёт прирост производительности);
portability — ошибки совместимости, обычно связано с различным поведением компиляторов или систем разной разрядности;
information — информационные сообщения, возникающие в ходе проверки (не связаны с ошибками в коде);
unusedFunction — попытка вычислить неиспользуемые функции (мёртвый код), не умеет работать в многопоточном режиме;
missingInclude — проверка на недостающий #include (например, используем random, а подключить stdlib.h забыли).

Включаются проверки параметром --enable, список категорий проверок перечисляется через запятую.
Добавим проверки:

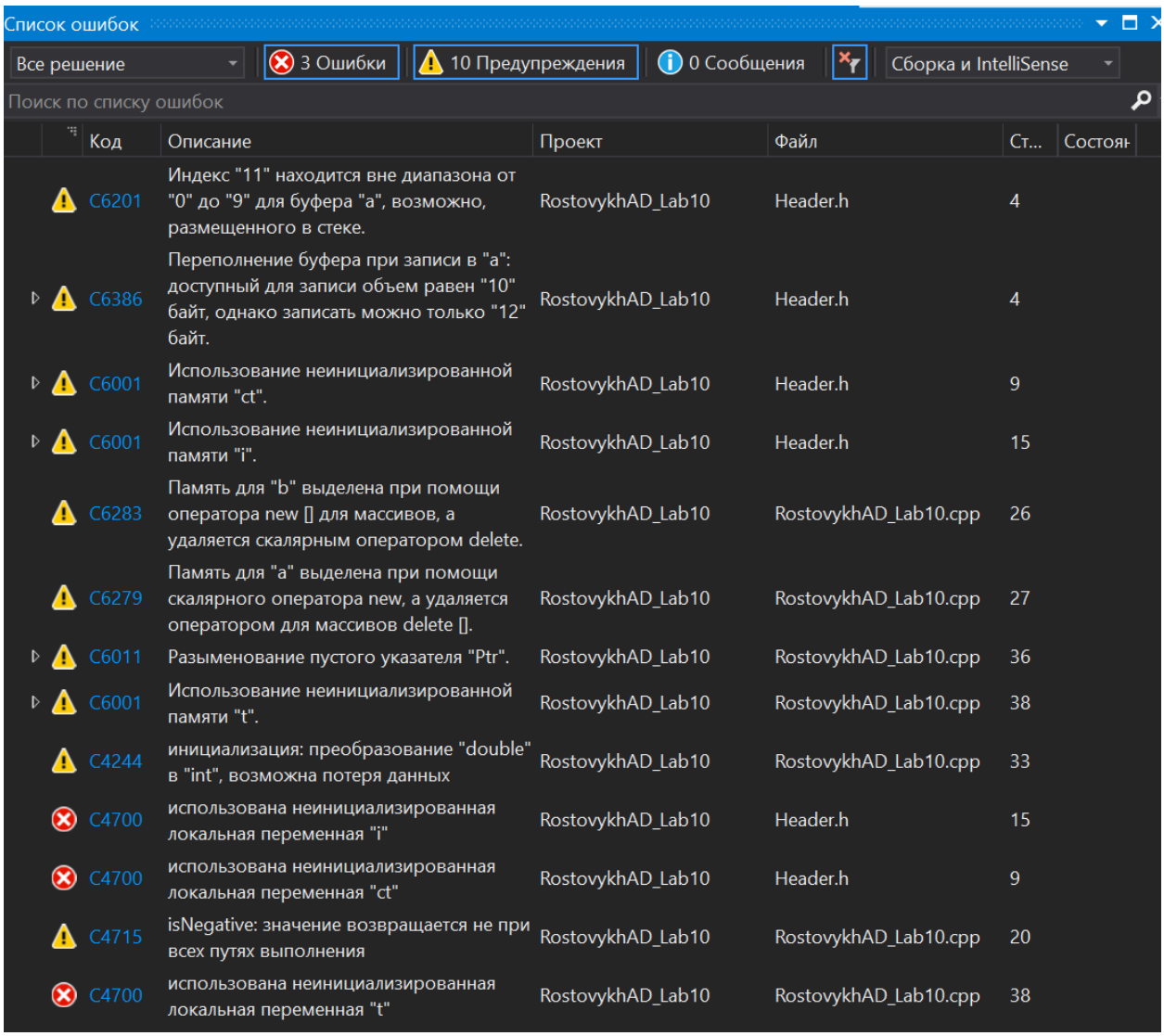
```
C:\7 семестр\МКП\Лаба10\RostovykhAD_Lab10>cppcheck -q --enable=all --project=RostovykhAD_Lab10.sln
RostovykhAD_Lab10\Header.h:4:3: error: Array 'a[10]' accessed at index 11, which is out of bounds. [arrayIndexOutOfBounds]
 a[11] = 0;
  ^
RostovykhAD_Lab10\RostovykhAD_Lab10.cpp:18:0: error: Found a exit path from function with non-void return type that has missing ret
urn statement [missingReturn]
  return true;
^
RostovykhAD_Lab10\RostovykhAD_Lab10.cpp:43:19: error: Invalid sqrt() argument nr 1. The value is -3 but the valid values are '0.0:'
. [invalidFunctionArg]
 double k = sqrt(-3);
                 ^
RostovykhAD_Lab10\RostovykhAD_Lab10.cpp:26:9: error: Mismatching allocation and deallocation: b [mismatchAllocDealloc]
 delete b;
        ^
RostovykhAD_Lab10\RostovykhAD_Lab10.cpp:25:11: note: Mismatching allocation and deallocation: b
 int* b = new int[2];  // P?P°C?C?PёP?
          ^
RostovykhAD_Lab10\RostovykhAD_Lab10.cpp:26:9: note: Mismatching allocation and deallocation: b
 delete b;
        ^
RostovykhAD_Lab10\RostovykhAD_Lab10.cpp:27:12: error: Mismatching allocation and deallocation: a [mismatchAllocDealloc]
 delete [] a;
           ^
RostovykhAD_Lab10\RostovykhAD_Lab10.cpp:24:11: note: Mismatching allocation and deallocation: a
 int* a = new int;      // PїP‹C?P‹P?P‹P?P?P°C?
          ^
RostovykhAD_Lab10\RostovykhAD_Lab10.cpp:27:12: note: Mismatching allocation and deallocation: a
 delete [] a;
           ^
RostovykhAD_Lab10\RostovykhAD_Lab10.cpp:8:3: warning: Possible null pointer dereference: ptr [nullPointer]
 *ptr = 0;
  ^
RostovykhAD_Lab10\RostovykhAD_Lab10.cpp:41:14: note: Assignment 'Ptr1=0', assigned value is 0
 int* Ptr1 = 0;
              ^
RostovykhAD_Lab10\RostovykhAD_Lab10.cpp:42:4: note: Calling function 'f', 1st argument 'Ptr1' value is 0
 f(Ptr1);
   ^
RostovykhAD_Lab10\RostovykhAD_Lab10.cpp:8:3: note: Null pointer dereference
 *ptr = 0;
  ^
RostovykhAD_Lab10\RostovykhAD_Lab10.cpp:36:44: error: Null pointer dereference: Ptr [nullPointer]
 for (int i = 0; i < 10; i++) std::cout << Ptr[i] << "  ";
                                           ^
RostovykhAD_Lab10\RostovykhAD_Lab10.cpp:34:13: note: Assignment 'Ptr=0', assigned value is 0
 int* Ptr = 0;
            ^
RostovykhAD_Lab10\RostovykhAD_Lab10.cpp:36:44: note: Null pointer dereference
 for (int i = 0; i < 10; i++) std::cout << Ptr[i] << "  ";
                                           ^
RostovykhAD_Lab10\Header.h:22:10: error: Division by zero. [zerodiv]
 return n/k;
         ^
RostovykhAD_Lab10\RostovykhAD_Lab10.cpp:29:26: note: Calling function 'Division', 2nd argument '0' value is 0
 double dd = Division(5, 0);
                      ^
RostovykhAD_Lab10\Header.h:22:10: note: Division by zero
 return n/k;
         ^
RostovykhAD_Lab10\RostovykhAD_Lab10.cpp:37:8: style: Local variable 't' shadows outer function [shadowFunction]
 type1 t;
       ^
RostovykhAD_Lab10\Header.h:2:5: note: Shadowed declaration
int t() {
    ^
RostovykhAD_Lab10\RostovykhAD_Lab10.cpp:37:8: note: Shadow variable
 type1 t;
       ^
RostovykhAD_Lab10\Header.h:9:9: error: Uninitialized variable: ct [uninitvar]
 while (ct < 100)
        ^
RostovykhAD_Lab10\Header.h:15:14: error: Uninitialized variable: i [uninitvar]
 for (int i; i < 1; i++) {
              ^
RostovykhAD_Lab10\RostovykhAD_Lab10.cpp:27:12: error: Memory is allocated but not initialized: a [uninitdata]
```



Появились проверки типа style, которые сообщают нам, например, о введенных, но неиспользованных переменных, а так же о неинициализированных.

3. Собрать проект, проанализировать полученные предупреждения и ошибки

Соберем проект и посмотрим, что нам выдаст окно ошибок и предупреждений:
Видим некоторые ошибки и предупреждения, но их намного меньше, чем выдал нам cppcheck, здесь, например, нет такой ошибки, как деление на ноль, выявленной cppcheck в ходе анализа.


Список ошибок
Все решение
3 Ошибки
10 Предупреждения
0 Сообщения
Сборка и IntelliSense
Поиск по списку ошибок
Код
Описание
Проект
Файл
Ст...
Состоян
C6201
Индекс "11" находится вне диапазона от "0" до "9" для буфера "a", возможно, размещенного в стеке.
RostovykhAD_Lab10
Header.h
4
C6386
Переполнение буфера при записи в "a": доступный для записи объем равен "10" байт, однако записать можно только "12" байт.
RostovykhAD_Lab10
Header.h
4
C6001
Использование неинициализированной памяти "ct".
RostovykhAD_Lab10
Header.h
9
C6001
Использование неинициализированной памяти "i".
RostovykhAD_Lab10
Header.h
15
C6283
Память для "b" выделена при помощи оператора new [] для массивов, а удаляется скалярным оператором delete.
RostovykhAD_Lab10
RostovykhAD_Lab10.cpp
26
C6279
Память для "a" выделена при помощи скалярного оператора new, а удаляется оператором для массивов delete [].
RostovykhAD_Lab10
RostovykhAD_Lab10.cpp
27
C6011
Разыменование пустого указателя "Ptr".
RostovykhAD_Lab10
RostovykhAD_Lab10.cpp
36
C6001
Использование неинициализированной памяти "t".
RostovykhAD_Lab10
RostovykhAD_Lab10.cpp
38
C4244
инициализация: преобразование "double" в "int", возможна потеря данных
RostovykhAD_Lab10
RostovykhAD_Lab10.cpp
33
C4700
использована неинициализированная локальная переменная "i"
RostovykhAD_Lab10
Header.h
15
C4700
использована неинициализированная локальная переменная "ct"
RostovykhAD_Lab10
Header.h
9
C4715
isNegative: значение возвращается не при всех путях выполнения
RostovykhAD_Lab10
RostovykhAD_Lab10.cpp
20
C4700
использована неинициализированная локальная переменная "t"
RostovykhAD_Lab10
RostovykhAD_Lab10.cpp
38