Отчет по лабораторной работе №14

Тема:

Программирование в командном процессоре ОС UNIX. Расширенное программирование.

Российский Университет Дружбы Народов

Факультет Физико-Математических и Естественных Наук

Дисциплина: Операционные системы

Студент:Ясмин Бен бадр

Группа: НКНбд-01-20

Москва, 2021г.

Введеник GDB

начинающих реверсеров, знающих особенности обратного проектирования, и желающих изучить такой отладчик как GDB

как подсказка тем кто постоянно работает с IDA, Ghidra или любым другим мощным и надежным инструментом, но в силу тех или иных обстоятельств решить задачу проще и быстрее с помощью GDB, и не очень хочется залезать в официальную документацию и снова все вспоминать

Введеник Gcc

GCC - это свободно доступный оптимизирующий компилятор для языков C, C++.

Программа gcc, запускаемая из командной строки, представляет собой надстройку над группой компиляторов. В зависимости от расширений имен файлов, передаваемых в качестве параметров, и дополнительных опций, gcc запускает необходимые препроцессоры, компиляторы, линкеры.

Файлы с расширением .cc или .C рассматриваются, как файлы на языке C++, файлы с расширением .c как программы на языке C, а файлы с расширением .o считаются объектными.

Введеник Splint

splint ("безопасный программный линт") представляет собой реализацию lint, то есть инструмент для статической проверки программ на C для уязвимостей безопасности и ошибок кодирования. С минимальными усилиями Splint можно использовать в качестве лучшего ворса.

Цель работы

Приобрести простейшие навыки разработки, анализа, тестирования и отладки приложений в ОС типа UNIX/Linux на примере создания на языке программирования C калькулятора с простейшими функциями.

Ход работы:

1. 1. В домашнем каталоге создайла подкаталог ~/work/os/lab_prog.

```
[benbaderyasmine@localhost ~]$ mkdir work
mkdir: cannot create directory ‘work’: File exists
[benbaderyasmine@localhost ~]$ cd work
[benbaderyasmine@localhost work]$ cd os
[benbaderyasmine@localhost os]$ mkdir lab_prog
[benbaderyasmine@localhost os]$ cd lab_prog
```

2. Создайте в нём файлы: calculate.h, calculate.c, main.c. Это будет примитивнейший калькулятор, способный складывать, вычитать, умножать и делить, возводить число в степень, брать квадратный корень, вычислять sin, cos, tan. При запуске он будет запрашивать первое число, операцию, второе число. После этого программа выведет результат и остановится.

```
[benbaderyasmine@localhost lab_prog]$ touch calculate.h
[benbaderyasmine@localhost lab_prog]$ touch calculate.c
[benbaderyasmine@localhost lab_prog]$ touch main c
```

**программ в файле calcule.c

emacs@localhost.localdomain

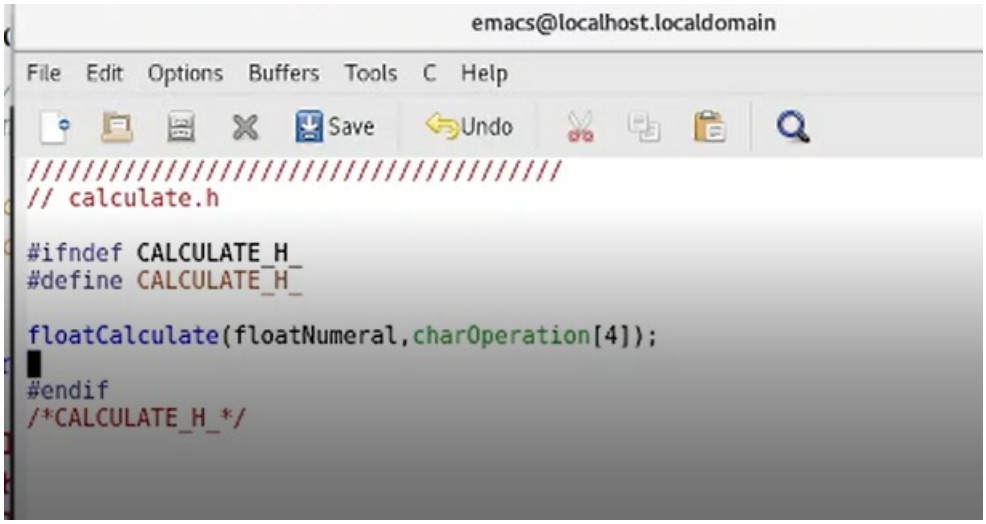
File Edit Options Buffers Tools C Help

Save Undo

```
#include<stdio.h>
#include<math.h>
#include<string.h>
#include"calculate.h"

float
Calculate(floatNumeral,charOperation[4])
{
  float SecondNumeral;
  if(strncmp(Operation,"+",1) == 0)
    {
      printf("Второе слагаемое: ");
      scanf("%f",&SecondNumeral);
      return(Numeral + SecondNumeral);
    }
  else if(strncmp(Operation,"-",1) == 0)
    {
     printf("Вычитаемое: ");
     scanf("%f",&SecondNumeral);
     return(Numeral - secondNumeral);
    }
  else if(strncmp(Operation,"*",1) == 0)
    {
      printf("Множитель: ");
```

**программ в файле calcule.h



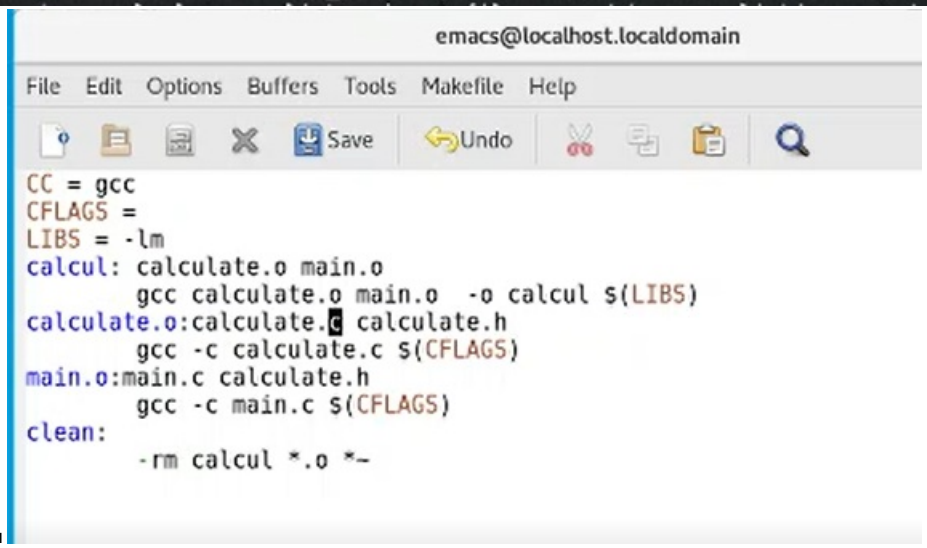
**программ в


```
#include <stdio.h>
#include "calculate.h"
int
main (void)
{
  float Numeral;
  char Operation[4];
  float Result;
  printf("Число: ");
  scanf("%f",&Numeral);
  printf("Операция (+,-,*,/,pow,sqrt,sin,cos,tan): ");
  scanf("%s",&Operation);
  Result = Calculate(Numeral, Operation);
  printf("%6.2f\n",Result);
  return 0;
}
```

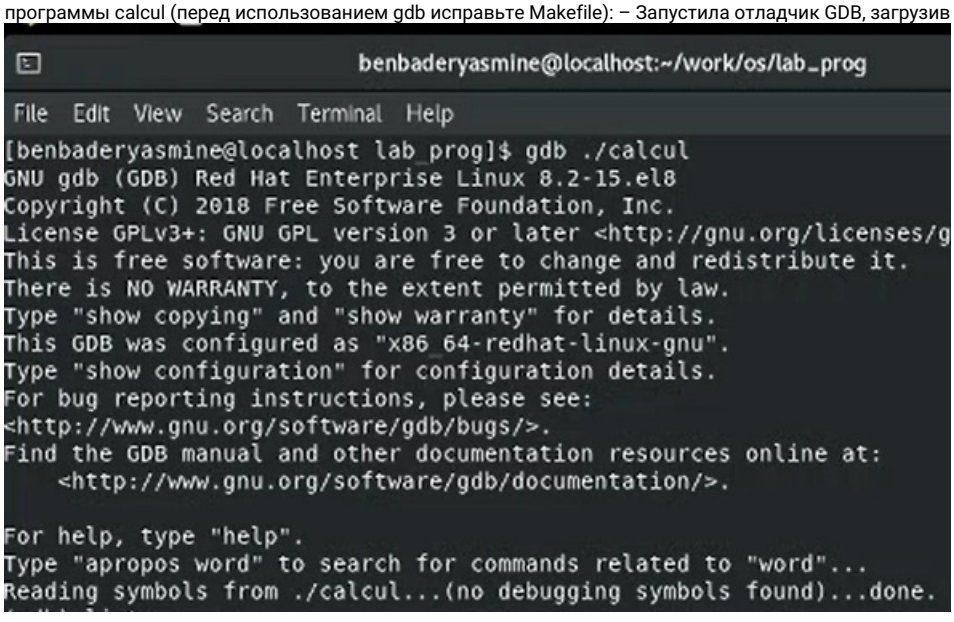
файле main.c 3. Выполните компиляцию программы посредством gcc:

```
[benbaderyasmine@localhost lab_prog]$ gcc -c calculate.c
[benbaderyasmine@localhost lab_prog]$ gcc -c main.c
[benbaderyasmine@localhost lab_prog]$ gcc -c calculate.o main.o -o calcul -lm
```

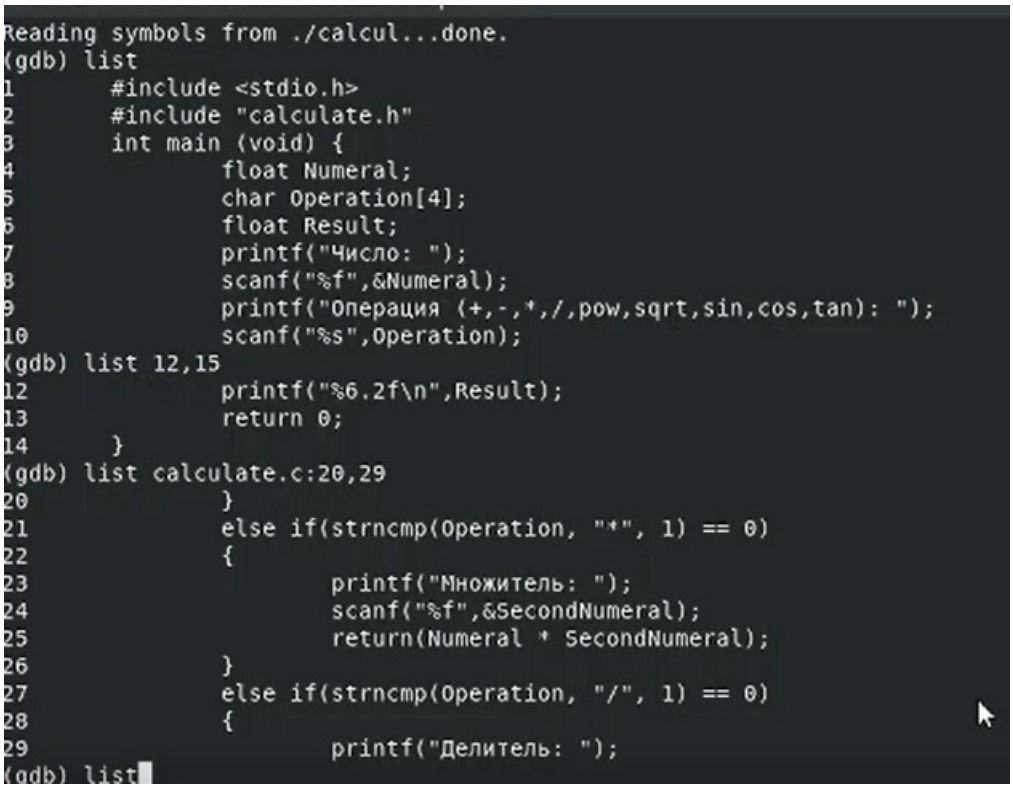
4. Создайте Makefile со содержанием



5. С помощью gdb выполнила отладку программы calcul (перед использованием gdb исправьте Makefile): – Запустила отладчик GDB, загрузив в него программу для отладки: gdb ./calcul



6. – Для запуска программы внутри отладчика введила команду run: run – Для постраничного (по 9 строк) просмотра исходного код используйте



команду list: list

7. – Для просмотра строк с 12 по 15 основного файла используйте list с параметрами: list 12,15

– Для просмотра определённых строк не основного файла используйте list с параметрами: list calculate.c:20,29

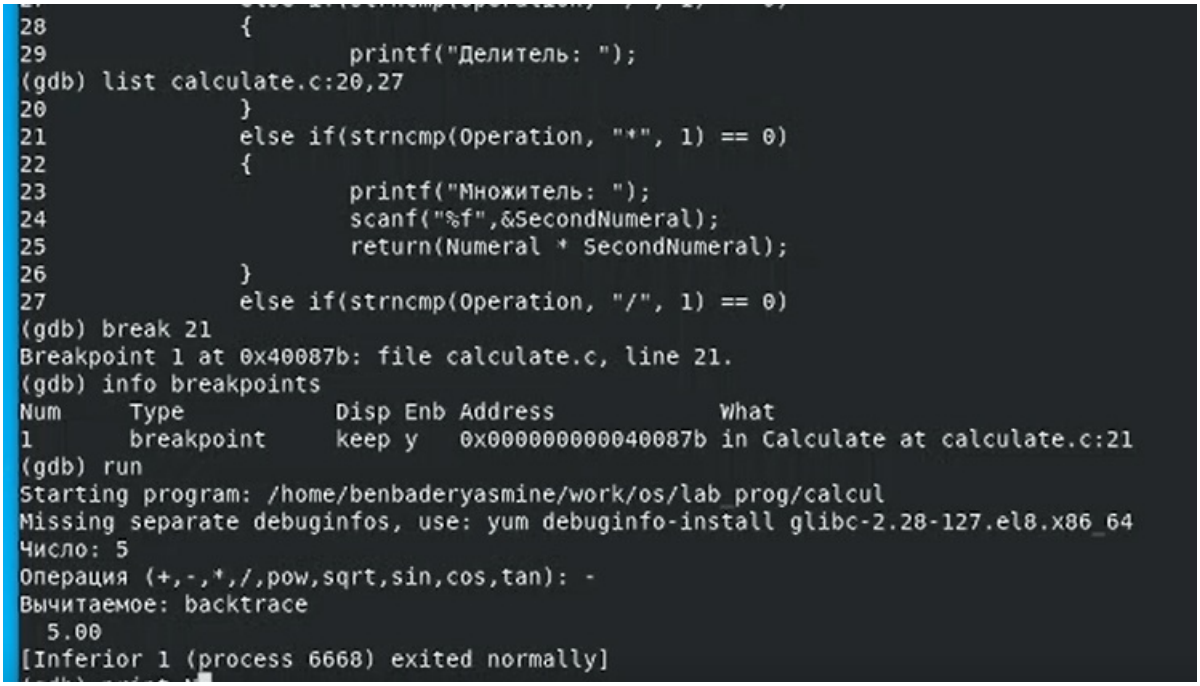
– Установите точку останова в файле calculate.c на строке номер 21: list calculate.c:20,27 break 21

– Выведите информацию об имеющихся в проекте точка останова: info breakpoints

– Запустила программу внутри отладчика и убедитесь, что программа остановится в момент прохождения точки останова: run

5

backtrace



а команда backtrace покажет весь стек вызываемых функций от начала программы до текущего места.

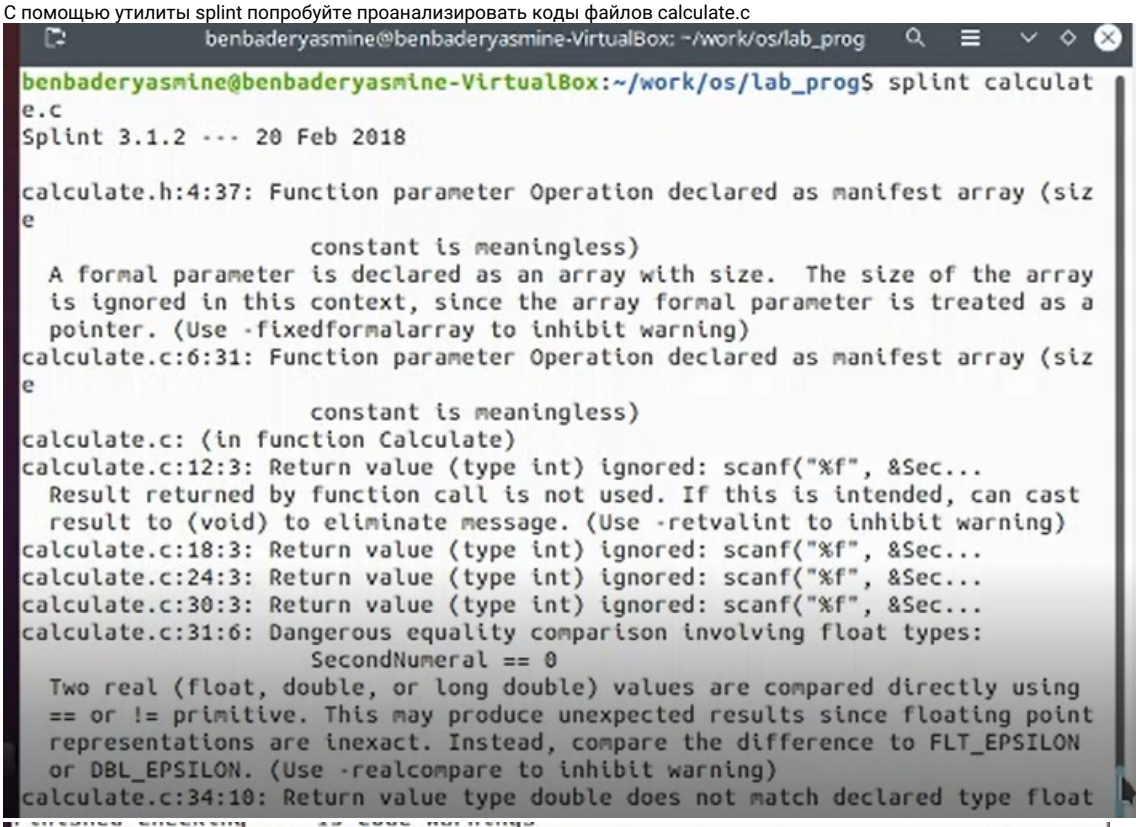
– Посмотрила, чему равно на этом этапе значение переменной Numeral, введя: print Numeral На экран выведено число 5.

– Сравнила с результатом вывода на экран после использования команды: display Numeral

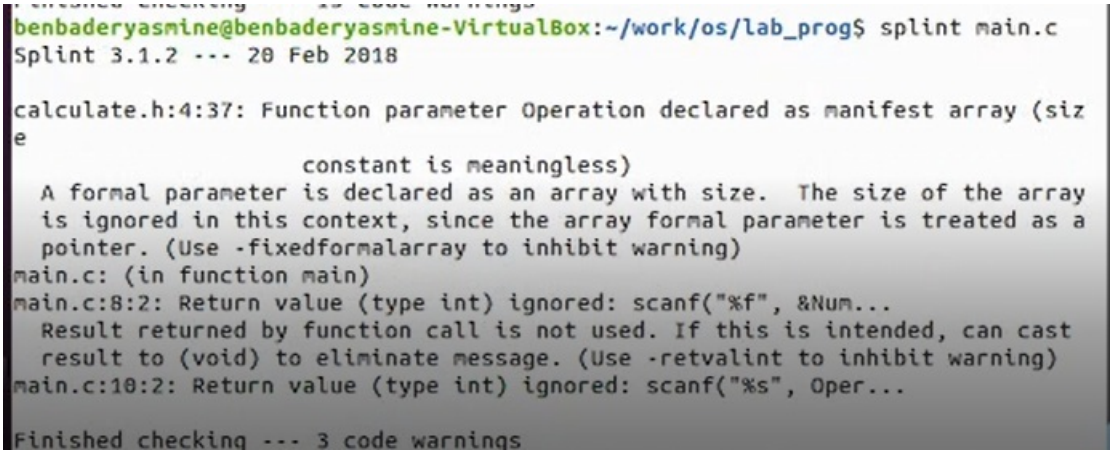
– Уберила точки останова: info breakpoints delete 1

```
(gdb) print Numeral
$1 = 5
(gdb) display Numeral
1: Numeral = 5
(gdb) info breakpoints
Num     Type           Disp Enb Address            What
1       breakpoint     keep y   0x000000000040087b in Calculate at calculate.c:21
        breakpoint already hit 1 time
(gdb) delete 1
```

8. С помощью утилиты splint попробуйте проанализировать коды файлов calculate.c



и main.c.



Вывод

Изучила как Приобрести простейшие навыки разработки, анализа, тестирования и отладки приложений в ОС типа UNIX/Linux на примере создания на языке программирования С калькулятора с простейшими функциями.

Ответы на контрольные вопросы:

1. Дополнительную информацию о этих программах можно получить с помощью функций info и man.
2. Unix поддерживает следующие основные этапы разработки приложений: -создание исходного кода программы;

- представляется в виде файла; -сохранение различных вариантов исходного текста; -анализ исходного текста; Необходимо отслеживать изменения исходного кода, а также при работе более двух программистов над проектом программы нужно, чтобы они не делали изменений кода в одно время. - компиляция исходного текста и построение исполняемого модуля; -тестирование и отладка; -проверка кода на наличие ошибок -сохранение всех изменений, выполняемых при тестировании и отладке. 3. Использование суффикса ".c" для имени файла с программой на языке Си отражает удобное и

полезное соглашение, принятое в ОС UNIX. Для любого имени входного файла суффикс определяет какая компиляция требуется. Суффиксы и префиксы указывают тип объекта. Одно из полезных свойств компилятора Си — его способность по суффиксам определять типы файлов. По суффиксу .c компилятор распознает, что файл abcd.c должен компилироваться, а по суффиксу .o, что файл abcd.o является объектным модулем и для получения исполняемой программы необходимо выполнить редактирование связей. Простейший пример командной строки для компиляции программы abcd.c и построения исполняемого модуля abcd имеет вид: gcc -o abcd abcd.c. Некоторые проекты предпочитают показывать префиксы в начале текста изменений для старых (old) и новых (new) файлов. Опция – prefix может быть использована для установки такого префикса. Плюс к этому команда bzr diff -p1 выводит префиксы в форме которая подходит для команды patch -p1. 4. Основное назначение компилятора с языка Си заключается в компиляции всей программы в целом и получении исполняемого модуля. 5. При разработке большой программы, состоящей из нескольких исходных файлов заголовков, приходится постоянно следить за файлами, которые требуют перекомпиляции после внесения изменений. Программа make освобождает пользователя от такой рутинной работы и служит для документирования взаимосвязей между файлами. Описание взаимосвязей и соответствующих действий хранится в так называемом make-файле, который по умолчанию имеет имя makefile или Makefile. 6. makefile для программы abcd.c мог бы иметь вид: # # Makefile # CC = gcc CFLAGS = LIBS = -lm calcul: calculate.o main.o gcc calculate.o main.o -o calcul $(LIBS) calculate.o: calculate.c calculate.h gcc -c calculate.c $(CFLAGS) main.o: main.c calculate.h gcc -c main.c $(CFLAGS) clean: -rm calcul *.o *~

End Makefile

В общем случае make-файл содержит последовательность записей (строк), определяющих зависимости между файлами. Первая строка записи представляет собой список целевых (зависимых) файлов, разделенных пробелами, за которыми следует двоеточие и список файлов, от которых зависят целевые. Текст, следующий за точкой с запятой, и все последующие строки, начинающиеся с литеры табуляции, являются командами ОС UNIX, которые необходимо выполнить для обновления целевого файла. Таким образом, спецификация взаимосвязей имеет формат: target1 [target2...]: [:] [dependment1...] [(tab)commands] [#commentary] [(tab)commands] [#commentary], где # — специфицирует начало комментария, так как содержимое строки, начиная с # и до конца строки, не будет обрабатываться командой make; : — последовательность команд ОС UNIX должна содержаться в одной строке make-файла (файла описаний), есть возможность переноса команд (), но она считается как одна строка; :: — последовательность команд ОС UNIX может содержаться в нескольких последовательных строках файла описаний. Приведённый выше make-файл для программы abcd.c включает два способа компиляции и построения исполняемого модуля. Первый способ предусматривает обычную компиляцию с построением исполняемого модуля с именем abcd. Второй способ позволяет включать в исполняемый модуль testabcd возможность выполнить процесс отладки на уровне исходного текста. 7. Пошаговая отладка программ заключается в том, что выполняется один оператор программы и, затем контролируются те переменные, на которые должен был воздействовать данный оператор. Если в программе имеются уже отлаженные подпрограммы, то подпрограмму можно рассматривать, как один оператор программы и воспользоваться вторым способом отладки программ. Если в программе существует достаточно большой участок программы, уже отлаженный ранее, то его можно выполнить, не контролируя переменные, на которые он воздействует. Использование точек останова позволяет пропускать уже отлаженную часть программы. Точка останова устанавливается в местах, где необходимо проверить содержимое переменных или просто проконтролировать, передаётся ли управление данному оператору. Практически во всех отладчиках поддерживается это свойство (а также выполнение программы до курсора и выход из подпрограммы). Затем отладка программы продолжается в пошаговом режиме с контролем локальных и глобальных переменных, а также внутренних регистров микроконтроллера и напряжений на выводах этой микросхемы. 8. – backtrace – выводит весь путь к текущей точке останова, то есть названия всех функций, начиная от main(); иными словами, выводит весь стек функций; – break – устанавливает точку останова; параметром может быть номер строки или название функции; – clear – удаляет все точки останова на текущем уровне стека (то есть в текущей функции); – continue – продолжает выполнение программы от текущей точки до конца; – delete – удаляет точку останова или контрольное выражение; – display – добавляет выражение в список выражений, значения которых отображаются каждый раз при остановке программы; – finish – выполняет программу до выхода из текущей функции; отображает возвращаемое значение,если такое имеется; – info breakpoints – выводит список всех имеющихся точек останова; – info watchpoints – выводит список всех имеющихся контрольных выражений; – splist – выводит исходный код; в качестве параметра передаются название файла исходного кода, затем, через двоеточие, номер начальной и конечной строки; – next – пошаговое выполнение программы, но, в отличие от команды step, не выполняет пошагово вызываемые функции; – print – выводит значение какого-либо выражения (выражение передаётся в качестве параметра); – run – запускает программу на выполнение; – set – устанавливает новое значение переменной – step – пошаговое выполнение программы; – watch – устанавливает контрольное выражение, программа остановится, как только значение контрольного выражения изменится; 9. 1) Выполнили компиляцию программы 2)Увидели ошибки в программе 3) Открыли редактор и исправили программу 4) Загрузили программу в отладчик gdb 5) run — отладчик выполнил программу, мы ввели требуемые значения. 6) программа завершена, gdb не видит ошибок. 10. 1 и 2.) Мы действительно забыли закрыть комментарии; 3.) отладчику не понравился формат %s для &Operation, т.к %s — символьный формат, а значит необходим только Operation. 11. Если вы работаете с исходным кодом, который не вами разрабатывался, то назначение различных конструкций может быть не совсем понятным. Система разработки приложений UNIX предоставляет различные средства, повышающие понимание исходного кода. К ним относятся: – cscope - исследование функций, содержащихся в программе; – splint — критическая проверка программ, написанных на языке Си. 12. 1. Проверка корректности задания аргументов всех использованных в программе функций, а также типов возвращаемых ими значений; 2. Поиск фрагментов исходного текста, корректных с точки зрения синтаксиса языка Си, но малоэффективных с точки зрения их реализации или содержащих в себе семантические ошибки; 3. Общая оценка мобильности пользовательской программы.