Содержание

(Подписчикам доступно 14 статей)

ВВЕДЕНИЕ В ASSEMBLER

Зачем учить ассемблер в 2020 году

Погружение в ассемблер, урок 1

Ты решил освоить ассемблер, но перед этим хочешь понять, что тебе это даст как программисту? Стоит ли входить в мир программирования через ассемблер, или лучше начать с какого-нибудь языка высокого уровня? И вообще, нужно ли знать ассемблер, чтобы стать полноценным программистом? Давай разберемся.

Антон Карев, 20 октября 2020 года

Делаем первые шаги в освоении асма

Погружение в ассемблер, урок 2

Ты решил освоить ассемблер, но не знаешь, с чего начать и какие инструменты для этого нужны? Сейчас расскажу и покажу — на примере программы «Hello, world!». А попутно объясню, что процессор твоего компьютера делает после того, как ты запускаешь программу.

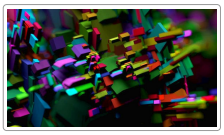
Антон Карев, 16 июня 2020 года

Осваиваем арифметические инструкции

Погружение в ассемблер, урок 3

Прочитав эту статью, ты научишься пользоваться арифметическими и логическими инструкциями, а также инструкциями сдвига. Попутно узнаешь, как создавать подпрограммы. А в конце напишешь простенькую игрушку «Угадай число».

Антон Карев, 8 июля 2020 года



Как работают переменные, режимы адресации, инструкции условного перехода

Погружение в ассемблер, урок 4

На ассемблере ты можешь хранить переменные двумя способами: в регистрах и в памяти. С регистрами все понятно, а вот с памятью могут возникнуть проблемы. Также ты узнаешь два способа размещения переменных, которыми пользоваться нельзя, и три — которыми можно, какие бывают режимы адресации и как это знание поможет тебе кодить на ассемблере более эффективно.

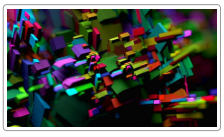
Антон Карев, 11 августа 2020 года

Учимся работать с памятью

Погружение в ассемблер, урок 5

В этой статье я познакомлю тебя с сегментной адресацией и сегментными регистрами, расскажу, как распределяется первый мегабайт оперативной памяти, и покажу получение прямого доступа к видеопамяти в текстовом режиме. Но главное — мы поностальгируем по фильму «Хакер» и напишем психоделическую программу, которой позавидовали бы его герои!

Антон Карев, 14 сентября 2020 года

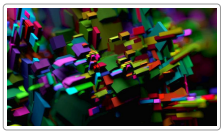


Работаем с большими числами и делаем сложные математические вычисления

Погружение в ассемблер, урок 6

Как ты знаешь, регистры процессора 8088 — 16-битные. Однако при необходимости ты можешь работать через эти регистры не только с 16-битными числами, но и с числами большей разрядности: и с 32-битными, и даже более крупными. В этой статье я сначала расскажу как, а затем мы нарисуем знаменитый фрактал — множество Мандельброта.

Антон Карев, 6 октября 2020 года

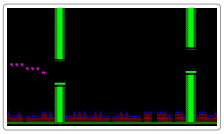


Сокращаем размер программы

Погружение в ассемблер, урок 7

Из этой статьи ты узнаешь несколько трюков, которые помогут тебе сокращать размер ассемблерных программ. Попутно окунешься в настроение «Клуба моделирования железной дороги» Массачусетского технологического института, где такие трюки в свое время ценились особенно высоко.

Антон Карев, 15 октября 2020 года



Floppy Bird

Пишем на ассемблере клон игры Flappy Bird, который уместится в бутсектор

Хочешь попрактиковаться в кодинге на ассемблере? Давай вместе шаг за шагом создадим игру и запустим ее прямо из загрузочного сектора твоего компьютера. Если ты думаешь, что 512 байт маловато для полноценной игры, не спеши с выводами. К концу статьи ты сможешь сделать ее своими руками!

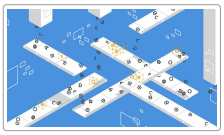
Антон Карев, 23 марта 2020 года

МикроБ

Пишем бейсик на ассемблере и умещаем в 512 байт

Хочешь попрактиковаться в кодинге на ассемблере? Давай создадим интерпретатор бейсика и запустим его прямо из загрузочного сектора твоего компьютера, уместив его в 512 байт. Скорее всего, это будет самая сложная программа в твоей жизни, и когда ты создашь ее своими руками, сможешь без зазрения совести называть себя хакером!

Антон Карев, 13 мая 2020 года

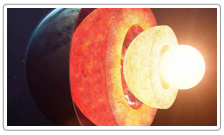


Вирус для Windows

Создаем простейшую вредоносную программу на ассемблере

Конструирование вирусов — отличный стимул изучать ассемблер. И хотя вирус, в принципе, можно написать и на C, это будет как-то не по-хакерски и вообще неправильно. Следующий далее текст — заметка Криса Касперски, которая раньше не публиковалась в «Хакере». Из нее ты узнаешь, как создаются вирусы и как написать простой вирус для Windows при помощи FASM.

Крис Касперски, 25 февраля 2020 года



Давай напишем ядро!

Создаем простейшее рабочее ядро операционной системы

Разработка ядра по праву считается задачей не из легких, но написать простейшее ядро может каждый. Чтобы прикоснуться к магии кернел-хакинга, нужно лишь соблюсти некоторые условности и совладать с ассемблером. В этой статье мы на пальцах разберем, как это сделать.

Арджун Сридхаран, 18 июня 2018 года

64-битный привет

Архитектура x86-64 под скальпелем ассемблерщика

32-битная эпоха уходит в прошлое, сдаваясь под натиском новых идей и платформ. Оба флагмана рынка (Intel и AMD) представили 64-битные архитектуры, открывающие дверь в мир больших скоростей и производительных ЦП. Это настоящий прорыв — новые регистры, новые режимы работы… попробуем с ними разобраться?

Крис Касперски, 1 ноября 2005 года

Ассемблерные извращения

Натягиваем стек по-хакерски

Ассемблер предоставляет практически неограниченную свободу для самовыражения и всевозможных извращений, что выгодно отличает его от языков высокого уровня. Вот мы и воспользуемся этой возможностью, извратившись не по-детски и сотворив со стеком то, о чем приплюснутый Си только мечтает.

Крис Касперски, 1 декабря 2006 года

Самый маленький шелл-код

Создаем 44-байтовый Linux x86 bind shellcode

Ты наверняка знаешь, что практически каждый эксплоит содержит в своем составе так называемый shell-код, выполняющийся при работе эксплоита. Может показаться, что писать shell-код — удел избранных, однако все не так страшно. В этой статье я расскажу, как написать простой bind shellcode, после чего мы его доработаем и сделаем одним из самых компактных в своем классе.

Олег Бойцев, 30 марта 2017 года