ВШПИ МФТИ, 2 курс, осень 2025
Низкоуровневое программирование, вопросы к экзамену
Препод: Мещерин И.С. aka @mesyarik

Все вопросы вида “как сделать X” подразумевают, что вы должны уметь продемонстрировать на своем ноутбуке эти действия.
Все вопросы вида “что такое X” подразумевают, что вы должны уметь показать на своем ноутбуке пример данного объекта или явления.

При подготовке и при ответах на вопросы можно пользоваться справкой Linux (командой man). Также можно (и даже рекомендуется) пользоваться заранее заготовленными сниппетами кода для демонстрации примеров, но оставлять для себя комментарии в коде запрещено.

Во время экзамена пользоваться конспектами (кроме заготовленного кода), учебниками, а также любыми онлайн-средствами (Google и AI-помощники) запрещено. Однако принимающий может вам разрешить воспользоваться Google или AI во время ответа на какой-либо вопрос по своему усмотрению.

Раздел 1. Линковка и библиотеки. Понятие сисколлов

1. Стадии сборки. Как увидеть, из каких этапов состоит сборка программы через g++? Что получается в результате каждого из этапов? Как выполнить каждый из этапов по отдельности? Чем объектный файл отличается от исполняемого? Как дизассемблировать исполняемый файл?
2. Что такое линковка? Что такое библиотеки (либы)? Покажите на примере простейшей программы, как вручную с помощью ld слинковать объектный файл со стандартной либой C++. Как добиться, чтобы полученный исполняемый файл удалось запустить?
3. Что такое статическая и динамическая линковка, статические и динамические либы? Как принудительно сделать статическую линковку вместо динамической и зачем это бывает нужно? Что делает команда ldd и как она работает? Как собрать программу с либой C++, расположенной по нестандартному адресу? Как создать свою динамическую либу и собрать программу с ее использованием? Для чего нужны переменные LD_PRELOAD, LD_LIBRARY_PATH? Что такое rpath и как его использовать? Как посмотреть, какие вызовы библиотечных функций делает данная программа в ходе выполнения?
4. Формат ELF. Какие типы ELF-файлов существуют? Покажите по одному примеру каждого типа. Из каких основных секций состоят ELF-файлы? Что хранится в секциях strtab, shstrtab, interp, dynamic? Какие есть утилиты для чтения содержимого ELF-файлов? Для чего нужна утилита objcopy? Приведите пример использования.
5. Что такое символы в терминах линковщика? Что такое манглирование и как (в общих чертах) оно работает? Как по манглированному имени восстановить исходное? Как посмотреть список символов в данном ELF-файле? Что делает команда strip? Какое бывает связывание у символов (global, local и weak)? Какая бывает видимость у символов (default, hidden, protected)?
6. Запуск программы. Что происходит при запуске бинаря до начала функции main, а также после ее окончания (вопрос с открытым ответом, чем подробнее, тем лучше)? Кто и когда вызывает конструкторы и деструкторы глобальных объектов? Как попросить g++ поставить точку старта программы на конкретную функцию? Почему происходит segfault, если точка старта программы выбрана неудачно? Как сделать, чтобы segfault в таком случае не было?
7. Дебаг. Что такое сборка в дебаг-режиме и в чем ее отличие от обычной? Как с помощью gdb отлаживать программу: поставить breakpoint на строчку кода или на функцию, делать шаги по строчкам (с заходом в функции и без него), выводить текущие значения переменных? Как посмотреть backtrace от текущего места исполнения? Что означает фраза “core dumped” и как с помощью gdb посмотреть содержимое coredump-файла после того, как программа упала?

8. Что такое системный вызов (сисколл)? Как посмотреть в режиме реального времени, какие сисколлы происходят во время работы какой-нибудь программы? Как посмотреть мануал для данного сисколла? Покажите использование сисколлов на примере read и write. Как использовать возвращаемые значения этих сисколлов? Как проверить, успешно ли был выполнен сисколл, а в случае неудачи узнать, какая ошибка произошла?

Раздел 2. Файлы и файловые системы

9. Что такое файловый дескриптор? Расскажите про сисколлы open, close и lseek для работы с файлами. Реализуйте программу cp с помощью данных сисколлов, а также read и write. Что произойдет, если сделать lseek на позицию больше чем размер файла и записать туда что-либо?
10. Перенаправление ввода-вывода. Как в терминале направить вывод команды в файл с перезаписью файла? А без перезаписи, в режиме добавления в файл? Как перенаправить вывод одного из потоков (cout или cerr) в файл или в другой поток? Как подавить вывод какого-то из потоков? Что делает команда tee? Что делают сисколлы dup и dup2? Реализуйте программу tee.
11. Файловые системы. Что такое файловая система? Какие виды файлов существуют в Linux (обычные файлы, директории, …)? Покажите примеры каждого вида файлов. Что из себя представляют директории с точки зрения файловой системы? Что такое inode и как узнать inode для файлов в данной директории? Что такое виртуальная файловая система? Покажите примеры файлов, которым не соответствует никакое дисковое пространство. Что такое swapfile?
12. Как пользоваться функциями opendir, readdir? Как пользоваться сисколлами stat, fstat, lstat, fstatat? Как на Си реализовать программу ls с помощью всего этого?
13. Как работает и какие сисколлы использует программа mv? Как работает и какие сисколлы использует программа rm? Напишите упрощенную реализацию и того, и другого.
14. Жесткие и символические ссылки. В чем разница? Как создать жесткую ссылку, символическую ссылку, что они представляют из себя с точки зрения файловой системы? Как работает и какие сисколлы использует программа ln в случае создания жестких ссылок и символических ссылок? Напишите упрощенную реализацию.
15. Права доступа к файлам. Как посмотреть, как изменить права доступа? Почему r и x - это разные права? Как понимать эти права доступа для директорий? Как поменять владельца файла, как поменять группу владельца? Какие сисколлы используются для всего вышеперечисленного? Что такое sticky bit? Что такое suid-бит, что означают права доступа s и S у файла? Покажите примеры файлов, которые ими обладают. Что такое атрибуты файлов, какие они бывают, как посмотреть и как поменять атрибуты файлов?
16. Как из терминала посмотреть, какие файловые дескрипторы сейчас открыты у данного процесса и какие файлы им соответствуют? Как из терминала посмотреть, какие процессы сейчас держат открытым данный файл? Какие команды есть в терминале для этого и как эти команды реализовать на языке Си?
17. Блочные и символьные устройства. В чем разница? Приведите примеры того и другого. Как прочитать данные с какого-нибудь символьного устройства, а также отправить данные на устройство? Что такое виртуальные устройства, что такое /dev/null, /dev/random, /dev/zero? Как сделать, чтобы приложение направило свой stdout / stderr на определенный терминал? Где в файловой системе хранится информация о CPU, об оперативной памяти, о жестких дисках / SSD?

Раздел 3. Память

18. Виртуальная память. Что это такое и зачем нужно? Что такое страничная организация памяти, таблицы страниц, как они устроены и где хранятся? Что такое page fault, в чем отличие minor от major page fault? Что такое TLB cache? Как происходит обращение процессора по адресу к памяти с учетом всего вышеназванного (вопрос с открытым ответом)? В какой ситуации возникает ошибка Segmentation fault и что в этой ситуации происходит на уровне ОС и процессора?
19. На какие секции делится адресное пространство процесса? В чем разница между секциями .data, .rodata и .bss? Зачем нужны сисколлы brk и sbrk? Покажите использование сисколлов mmap и

munmap базовом сценарии. Как посмотреть, как выглядит в данный момент адресное пространство процесса?

20. Можно ли запросить конкретный виртуальный адрес для выделения памяти? Почему при обращении за границу массива segfault происходит не всегда? Покажите пример использования mremap. Как с помощью mmap загрузить файл в оперативную память? Можно ли таким образом поменять файл? В чем разница между MAP_SHARED и MAP_PRIVATE? Зачем нужен сисколл msync?
21. Какие бывают права доступа к памяти? Зачем нужен сисколл mprotect и как им пользоваться? Покажите, как с помощью mmap и mprotect загрузить код из библиотеки в память на выполнение. Что означает ошибка Illegal intstruction? Покажите пример программы на Си, которая приводит к этой ошибке (естественным путем, т.е. не генерируя эту ошибку из кода напрямую).
22. Как реализованы функции malloc и free в стандартной библиотеке Си? Расскажите про механизм бакетов, малые и большие бакеты. Как malloc выбирает, какой бакет использовать? Как происходит освобождение бакетов и слияние соседних свободных бакетов? Что такое fastbins? Какие сисколлы использует malloc для работы с памятью?

Раздел 4. Процессы и треды

23. Что такое процесс? Как посмотреть все процессы в системе? Что такое pid, ppid? Как посмотреть дерево процессов? Как посмотреть потребление памяти, потребление CPU каждым из процессов? Что такое uid, euid и cwd данного процесса, как их узнать и как поменять?
24. Что такое приоритет процесса, какой он бывает, как его узнать и как поменять? Что такое CPU affinity данного процесса, как его узнать и как поменять? Что такое process capabilities в Linux, какие они бывают? Как выдать процессу определенные capabilities, как посмотреть имеющиеся?
25. Расскажите про сисколлы fork и exec. Какие версии сисколла exec существуют и в чем разница между ними? В чем необычность функций fork и exec, что происходит при их вызове? Покажите пример вызова из программы другой программы, используя fork+exec. Что такое fork-бомба?
26. Какие бывают состояния у процессов? Как в терминале приостановить процесс, как возобновить приостановленный процесс? Как пользоваться командами fg и bg? Что такое процессы-зомби, как они возникают? Как посмотреть, в каком состоянии находится сейчас какой-либо процесс? Что делает сисколл wait, как им пользоваться? Что делает функция sleep в Си?
27. Что такое rlimit для процесса? Как пользоваться функциями getrlimit и setrlimit? Покажите, как из кода программы запросить себе больший размер стека, чем дан изначально. Как установить процессу ограничение на использование памяти и/или процессорного времени? Что произойдет, если эти ограничения будут превышены?
28. Расскажите про библиотеку seccomp. Покажите на примере, как запретить программе вызывать определенные сисколлы. Как получить ошибку Bad system call (core dumped)?
29. Что такое сигналы? Как послать сигнал процессу из терминала, а также из кода программы? Перечислите известные вам стандартные сигналы с объяснением, для чего они применяются. Какова стандартная реакция процессов на каждый из сигналов? Как вручную из терминала вызвать у стороннего процесса segfault? Как из кода послать сигнал самому себе? Как в коде программы заснуть до прихода сигнала?
30. Как сделать кастомный обработчик сигналов? Покажите на примере, как из кода программы перехватывать segfault и делать что-то нестандартное при его наступлении. Что, если во время обработки сигнала приходит другой сигнал? Как можно заблокировать получение других сигналов во время обработки сигнала? Что, если сигнал приходит во время выполнения сисколла? Что такое signal-safety и что такое реентрабельная функция?
31. Что такое pipes? Покажите в коде пример создания pipe и общения между двумя процессами с помощью pipe. В какой ситуации возникает ошибка Broken pipe? Как реализовать аналог оператора | в bash на Си?
32. Что такое fifo-файлы? Как создать такой файл из терминала, а также программно? Покажите пример общения между двумя процессами с помощью fifo-файла. Что, если несколько процессов пишут в один и тот же fifo? Что, если несколько процессов читают один и тот же fifo?

33. Что такое разделяемая память? Какие сисколлы существуют для создания и управления разделяемой памятью? Покажите на примере, как устроить общение через разделяемую память между двумя процессами. Как посмотреть, какие участки разделяемой памяти существуют в ОС и кто их создал? Как посмотреть, какие страницы разделяемой памяти сейчас использует данный процесс?
34. Что такое потоки выполнения (треды, threads, нити)? Покажите пример создания и использования thread на C++. Покажите пример параллельной обработки из двух тредов каких-либо данных. Что делают методы join и detach? Что происходит, если main завершается, но при этом еще не все треды завершили свою работу?
35. Что такое race condition? Приведите пример, когда возникает UB из-за одновременного изменения одних и тех же данных из разных тредов. Что такое мьютекс? Приведите пример решения проблемы race condition с помощью мьютекса. Что такое deadlock и как он может возникнуть?
36. Как реализовать std::thread, используя сисколлы? Как пользоваться сисколлом clone и какие у него есть параметры? Покажите, как надо вызывать сисколл clone, чтобы создать полноценный std::thread. Что из себя представляют треды с точки зрения ОС? Что такое тред-группа? Что такое tid, tgid, как их узнать, в чем разница с pid? Как послать сигнал отдельному треду?
37. Что такое семафоры в Linux, для чего они нужны? Что позволяет делать сисколл futex? Покажите набросок реализации std::mutex с использованием сисколла futex. (Можно использовать std::atomic без объяснения.)

Раздел 5. Ассемблер и устройство процессора

38. Что такое ассемблер? Какие есть разновидности ассемблера? Что такое регистры? Перечислите основные регистры в архитектуре x86 и их предназначение. Расскажите про основные ассемблерные инструкции и их синтаксис: mov, арифметические инструкции, логические инструкции.
39. Инструкции безусловного и условного перехода в ассемблере. Регистр флагов. Какие есть условные переходы и как (идейно) они работают? Как написать аналоги if, while и for на ассемблере?
40. Как использовать в программе на Си ассемблерную функцию из другого файла? Покажите на примере функции проверки числа на простоту. Как с помощью gdb делать отладку ассемблерного кода? Как просматривать текущие значения регистров, как делать пошаговое исполнение ассемблерных инструкций?
41. Инструкции call и ret. Что такое стековый фрейм? Что такое stack pointer и base pointer, регистры rbp и rsp? Что происходит на уровне ассемблера при вызове функций и при возврате из них? Где хранятся аргументы функций при вызове? Где хранится результат функции сразу после вызова? Что делает флаг компиляции -fno-omit-frame-pointer, зачем он нужен?
42. Что такое атака переполнения буфера и какие средства защиты от нее существуют? Что такое stack protector, для чего он используется, что делает флаг компиляции -fno-stack-protector? Как получить ошибку “Stack smashing detected”? Что такое ASLR и как его отключить?
43. Кэши процессора. Сколько уровней кэша есть в процессоре, зачем они нужны? Как узнать размеры кэшей своего процессора? Что такое кэш-линия? Почему делать обход матрицы по строкам эффективнее, чем по столбцам? Покажите эксперимент, доказывающий, что кэш-линии существуют. Покажите эксперимент, доказывающий, что существуют кэши разных уровней.
44. Что такое branch prediction, в чем его идея? Покажите эксперимент, доказывающий существование данного явления. Как подсказать компилятору (средствами C++20, а также без него), какая из веток if более вероятна? Как это отразится на ассемблерном коде?
45. Что такое istruction-level parallelism в процессоре? Покажите эксперимент, доказывающий существование этого явления. Что такое out-of-order execution в процессоре, к каким неожиданным эффектам это может приводить? Что такое спекулятивное исполнение кода в процессоре? Расскажите в общих чертах, к каким уязвимостям оно может приводить.
46. Что такое векторные инструкции? Что такое Intel intrinsics, какие они бывают? Что такое SIMD, AVX? Какие специальные регистры процессора используются для векторных инструкций? Покажите на примерах, как применить векторизацию для ускорения какого-либо кода.

47. Как делать ассемблерные вставки в коде на Си? Расскажите о синтаксисе в общих чертах. Зачем нужно слово volatile? Приведите простейший пример, сделайте обмен значений двух переменных через ассемблерную вставку. Как с помощью ассемблерной вставки узнать количество тактов процессора, прошедшее между двумя данными строчками кода? Как применяются ассемблерные вставки в криптографии для защиты от timing attacks?
48. Какие есть режимы работы у процессора и чем они отличаются? Чем принципиально отличается вызов сисколла от вызова обычной функции? Что делает ассемблерная инструкция syscall? Покажите пример кода, где она встречается. Покажите, как сделать сисколл execve напрямую через ассемблерную вставку. Что такое привилегированные инструкции процессора и что к ним относится?
49. Что такое прерывание, какие они бывают? Что такое interrupt descriptor table? Чем похожи и чем отличаются прерывание и вызов сисколла? Как сгенерировать прерывание с помощью ассемблерной вставки напрямую? Как ОС с помощью механизма прерываний держит под контролем все процессы?

Доп вопросы по выбору

Это не вошло в лекции, и поэтому этих вопросов не будет в билетах, они также не будут задаваться по инициативе принимающего. Однако вы можете по собственной инициативе выучить какой-то из этих вопросов и рассказать принимающему в конце экзамена (как вопрос по выбору). За это вы можете получить до +1 балла к оценке на экзамен. Однако необходимо соблюдение двух условий:

1) Один вопрос может быть выбран не более чем двумя студентами;
2) Вопрос по выбору можно рассказывать, только если ваша оценка за экзамен уже хотя бы хор(5).

За неудачно рассказанный вопрос по выбору оценка за экзамен не может быть снижена.

1. Сисколл ptrace и как им пользоваться. Как реализовать простейший дебаггер с возможностью ставить breakpoint на начало функции и с возможностью выводить backtrace?
2. Что такое отладочные регистры процессора (DR0-DR7), для чего они нужны, как ими пользоваться? Как реализовать watchpoints в дебаггере?
3. Что такое PLT (procedure linkage table) и GOT (global offset table) в ELF-файлах? Зачем нужны, какие проблемы решают? Объясните на примерах.
4. Позиционно независимый код. Параметры компиляции -fpie и -fno-pie. Зачем нужен, какие проблемы решает? Как это выглядит в ассемблере и в объектном файле?
5. Что такое vDSO? Как это помогает оптимизировать работу некоторых сисколлов (каких, например)? Покажите на конкретных примерах, как с помощью этого механизма удается избежать прямого вызова сисколлов.
6. Что такое уязвимость Meltdown https://en.wikipedia.org/wiki/Meltdown_(security_vulnerability)? Покажите на конкретном примере (с кодом), подробно объясните суть этой уязвимости.
7. Что такое уязвимость Spectre https://en.wikipedia.org/wiki/Spectre_(security_vulnerability)? Покажите на конкретном примере (с кодом), подробно объясните суть этой уязвимости.

   …

Если этот список вопросов недостаточен, по вашему запросу с согласования лектора @mesyarik можно добавить сюда и другие вопросы (но не любые, а только относящиеся к курсу).