

????????? ? ?????????? ????????

syscall

Инструкция процессора, мост между ядром и непривилегированными программами. Для вызова заполняются регистры в соответствии с соглашениями ABI (Application Binary Interface). Есть обновляемая [таблица системных вызовов](#) Номер функции размещается в регистре `rax`, Аргументы функции последовательно в регистрах `rdi`, `rsi`, `rdx`, `r10`, `r8`, `r9`.

`syscall` изменяет регистры `rcx` и `r11`. В регистр `RCX` сохраняется предыдущее значение регистра `RIP` - адрес следующей инструкции, которую будут выполнять приложение после завершения системного вызова, а в `RIP` помещается адрес обработчика системного вызова. Также `syscall` изменяет регистр флагов `RFLAGS` в соответствии с системным вызовом, а старое значение `RFLAGS` сохраняется в регистр `r11`. Поэтому, если программа использует регистры `rcx` и `r11`, то перед выполнением системного вызова эти регистры следует сохранить, например, в стек, чтобы не потерять их содержимое.

Кроме того, системный вызов может возвращать некоторый результат, который помещается в регистр `rax`.

Revision #2

Created 11 November 2025 14:41:29 by Admin

Updated 11 November 2025 14:42:02 by Admin