

Запуск insmod з параметром amount=5 (var_1 == NULL при i = 2)

```
Please press Enter to activate this console.
/ # insmod hello.ko amount=5
[ 54.047475] hello: loading out-of-tree module taints kernel.
[ 54.065150] Entered parameter is between 5 and 10
[ 54.065260] Hello World!
[ 54.065795] Hello World!
[ 54.066169] Unhandled fault: page domain fault (0x81b) at 0x00000008
[ 54.067259] pgd = (ptrval)
[ 54.067595] [00000008] *pgd=48b99835, *pte=00000000, *ppte=00000000
[ 54.069373] Internal error: : 81b [#1] SMP ARM
[ 54.070215] Modules linked in: hello(0+)
[ 54.071272] CPU: 0 PID: 62 Comm: insmod Tainted: G          0      4.19.219 #1
[ 54.071935] Hardware name: Generic DT based system
[ 54.073519] PC is at helloinit+0xc8/0x1000 [hello]
[ 54.074062] LR is at 0xcea33a2f
[ 54.074406] pc : [<bf0050c8>]   lr : [<cea33a2f>]   psr: 800f0013
[ 54.074990] sp : c8be3e90 ip : 40000000 fp : 000f411e
[ 54.075452] r10: 006000c0 r9 : bf0010b8 r8 : c135434c
[ 54.075988] r7 : 00000000 r6 : 00000000 r5 : bf002000 r4 : 00000003
[ 54.076633] r3 : 00000017 r2 : 08000000 r1 : 0000000c r0 : 945600f0
[ 54.077327] Flags: Ncv IRQs on FIQs on Mode SVC_32 ISA ARM Segment none
[ 54.078037] Control: 10c5387d Table: 48bac06a DAC: 00000051
[ 54.078622] Process insmod (pid: 62, stack limit = 0x(ptrval))
[ 54.079248] Stack: (0xc8be3e90 to 0xc8be4000)
[ 54.079950] 3e80:                                c1788300 bf005000 fffff000 00000000
[ 54.081152] 3ea0: c8be2000 0011b1f8 00000051 c0302dd8 c8ba3200 0000065f 00000000 00000000
[ 54.082389] 3ec0: 00000000 00000000 00000000 00000000 6e72656b 00006c65 00000000 00000000
[ 54.083463] 3ee0: 00000000 00000000 00000000 00000000 00000000 00000000 bf002040 6dc644a9
[ 54.084493] 3f00: 00000000 bf002040 0012c5b4 c8bf5400 e0c92364 c03d5d78 0012c5b4 00000000
[ 54.085397] 3f20: e0c92364 00001364 0012c5b4 00000000 e0c92364 c03d88f4 e0c8129e e0c81380
[ 54.086419] 3f40: e0c81000 00011364 e0c91a44 e0c91a44 e0c8e238 00003000 00003040 00000000
[ 54.087399] 3f60: 00000000 00000000 0000170c 0000002c 0000002d 00000017 00000000 00000010
[ 54.088361] 3f80: 00000000 6dc644a9 0011b1f8 b6ff5950 00011364 00000000 c0301204 c8be2000
[ 54.089276] 3fa0: 00000000 c0301000 0011b1f8 b6ff5950 0011b250 00011364 0011b1f8 00000000
[ 54.090229] 3fc0: 0011b1f8 b6ff5950 00011364 00000000 00000001 be81aea0 001086c4 000f411e
[ 54.091155] 3fe0: be81ab58 be81ab48 0003b270 b6eaf1b0 600f0010 0011b250 00000000 00000000
[ 54.093642] [<bf0050c8>] (helloinit [hello]) from [<c0302dd8>] (do_one_initcall+0x54/0x214)
[ 54.095002] [<c0302dd8>] (do_one_initcall) from [<c03d5d78>] (do_init_module+0x64/0x2a4)
[ 54.095873] [<c03d5d78>] (do_init_module) from [<c03d88f4>] (sys_init_module+0x154/0x194)
[ 54.096667] [<c03d88f4>] (sys_init_module) from [<c0301000>] (ret_fast_syscall+0x0/0x54)
[ 54.097445] Exception stack(0xc8be3fa8 to 0xc8be3ff0)
[ 54.098075] 3fa0:                                0011b1f8 b6ff5950 0011b250 00011364 0011b1f8 00000000
[ 54.099014] 3fc0: 0011b1f8 b6ff5950 00011364 00000000 00000001 be81aea0 001086c4 000f411e
[ 54.099864] 3fe0: be81ab58 be81ab48 0003b270 b6eaf1b0
[ 54.100885] Code: e5860000 03a06000 eb4edc68 e1a07006 (e1c600f8)
[ 54.102105] ---[ end trace 85a3df76c29b6f3e ]---
Segmentation fault
/ #
```

```
lelly@lelly-super-pc: ~/Lab5
Файл Правка Вид Поиск Терминал Вкладки Справка

[ 6.416744] input: gpio-keys as /devices/platform/gpio-keys/input/input0
[ 6.423292] rtc-pl031 9010000.pl031: setting system clock to 2021-12-22 19:31:43 UTC (1640201503)
[ 6.431898] uart-pl011 9000000.pl011: no DMA platform data
[ 6.540220] Freeing unused kernel memory: 2048K
[ 6.558821] Run /init as init process

Please press Enter to activate this console.
/ # insmod hello.ko amount=5
[ 54.047475] hello: loading out-of-tree module taints kernel.
[ 54.065150] Entered parameter is between 5 and 10
[ 54.065260] Hello World!
[ 54.065795] Hello World!
[ 54.066169] Unhandled Fault: page domain fault (0x81b) at 0x00000000
[ 54.067259] pgd = (ptrval)
[ 54.067595] [00000000] *pgd=48b99835, *pte=00000000, *ppte=00000000
[ 54.069373] Internal error: : 81b [#1] SMP ARM
[ 54.070215] Modules linked in: hello(0+)
[ 54.071272] CPU: 0 PID: 62 Comm: insmod Tainted: G          0      4.19.219 #1
[ 54.071935] Hardware name: Generic DT based system
[ 54.073519] PC is at helloinit+0xc8/0x1000 [hello]
[ 54.074062] LR is at 0xcea33a2f
[ 54.074406] pc : [<bf0050c8>]   lr : [<cea33a2f>]   psr: 800f0013
[ 54.074990] sp : c8be3e90   lp : 40000000   fp : 000f411e
[ 54.075452] r10: 006000c0   r9 : bf0010b8   r8 : c135434c
[ 54.075988] r7 : 00000000   r6 : 00000000   r5 : bf002000   r4 : 00000003
[ 54.076633] r3 : 00000017   r2 : 00000000   r1 : 0000000c   r0 : 945600f0
[ 54.077327] Flags: Nzcv IRQs on FIQs on Mode SVC_32 ISA ARM Segment none
[ 54.078037] Control: 10c5387d Table: 48bac06a DAC: 00000051
[ 54.078622] Process insmod (pid: 62, stack limit = 0x(ptrval))
[ 54.079248] Stack: (0xc8be3e90 to 0xc8be4000)
[ 54.079950] 3e80:                                c1788300 bf005000 fffff000 00000000
[ 54.081152] 3ea0: c8be2000 0011b1f8 00000051 c0302dd8 c8ba3200 0000065f 00000000 00000000
[ 54.082389] 3ec0: 00000000 00000000 00000000 00000000 6e72656b 00006c65 00000000 00000000
[ 54.083463] 3ee0: 00000000 00000000 00000000 00000000 00000000 00000000 bf002040 6dc644a9
[ 54.084493] 3f00: 00000000 bf002040 0012c5b4 c8bf5400 e0c92364 c03d5d78 0012c5b4 00000000
[ 54.085397] 3f20: e0c92364 00001364 0012c5b4 00000000 e0c92364 c03d88f4 e0c8129e e0c81380
[ 54.086419] 3f40: e0c81000 00001364 e0c91c0c e0c91a44 e0c8e238 00003000 00003040 00000000
[ 54.087399] 3f60: 00000000 00000000 0000170c 0000002c 0000002d 00000017 00000000 00000010
[ 54.088361] 3f80: 00000000 6dc644a9 0011b1f8 b6ff5950 00011364 00000000 c0301204 c8be2000
[ 54.089276] 3fa0: 00000000 c0301000 0011b1f8 b6ff5950 0011b250 00011364 0011b1f8 00000000
[ 54.090229] 3fc0: 0011b1f8 b6ff5950 00011364 00000000 00000001 be81aea0 001086c4 000f411e
[ 54.091155] 3fe0: be81ab58 be81ab48 0003b270 b6eaf1b0 600f0010 0011b250 00000000 00000000
[ 54.093642] [<bf0050c8>] (helloinit [hello]) from [<c0302dd8>] (do_one_initcall+0x54/0x214)
[ 54.095002] [<c0302dd8>] (do_one_initcall) from [<c03d5d78>] (do_init_module+0x64/0x2a4)
[ 54.095873] [<c03d5d78>] (do_init_module) from [<c03d88f4>] (sys_init_module+0x154/0x194)
[ 54.096667] [<c03d88f4>] (sys_init_module) from [<c0301000>] (ret_fast_syscall+0x0/0x54)
[ 54.097445] Exception stack(0xc8be3fa8 to 0xc8be3ff0)
[ 54.098075] 3fa0:                                0011b1f8 b6ff5950 0011b250 00011364 0011b1f8 00000000
[ 54.099014] 3fc0: 0011b1f8 b6ff5950 00011364 00000000 00000001 be81aea0 001086c4 000f411e
[ 54.099864] 3fe0: be81ab58 be81ab48 0003b270 b6eaf1b0
[ 54.100885] Code: e5860000 03a06000 eb4edc68 e1a07006 (e1c600f8)
[ 54.102105] ---[ end trace 85a3df76c29b6f3e ]---
```

Запуск objdump:

```
lelly@lelly-super-pc: ~/Lab5
pr_info("Hello World!");
84: e3009000 movw r9, #0
88: e340a060 movt sl, #96 ; 0x60
8c: e3409000 movt r9, #0
for (i = 0; i < amount; i++) {
90: e3a04000 mov r4, #0
94: e5953000 ldr r3, [r5]
98: e1530004 cmp r3, r4
9c: 9a00000e bls dc <init_module+0xdc>
a0: e3a02010 mov r2, #16
a4: e1a0100a mov r1, sl
a8: e5980018 ldr r0, [r8, #24]
ac: ebfffffe bl 0 <kmem_cache_alloc_trace>
    if (i == 2) var_1 = NULL;
b0: e3540002 cmp r4, #2
for (i = 0; i < amount; i++) {
b4: e2844001 add r4, r4, #1
    var_1->next = kmalloc(sizeof(struct head_list), GFP_KERNEL);
b8: e5860000 str r0, [r6]
    if (i == 2) var_1 = NULL;
bc: 03a06000 moveq r6, #0
    var_1->time = ktime_get();
c0: ebfffffe bl 0 <ktime_get>
    var_2 = var_1;
c4: e1a07006 mov r7, r6
    var_1->time = ktime_get();
c8: e1c600f8 strd r0, [r6, #8]
    pr_info("Hello World!");
cc: e1a00009 mov r0, r9
d0: ebfffffe bl 0 <prinfo>
    var_1 = var_1->next;
d4: e5966000 ldr r6, [r6]
d8: eaffffed b 94 <init_module+0x94>
}
```