



```

/
/boot
/home
/tmp
/var/tmp

```

:

		/		
1	/	(, /boot).	ext4	defaults
2	/boot	. <div>LVM!!!</div> <div>/boot (- LVM) 512.</div>	ext2, ext3, ext4	defaults
3	/home	.	ext4	noexec,nodev,nosuid
4	/tmp	. <div>/tmp 250</div>	ext4	noexec,nodev,nosuid
5	/var	. <div>noexec,nodev,nosuid, :</div> <div> <div>o noexec , ;</div> <div>o noexec (, dpkg);</div> </div>	ext4	defaults noexec,nodev,nosuid
6	/var/tmp	. <div>/var /var/tmp noexec,nodev,nosuid.</div>	ext4	noexec,nodev,nosuid
7	swap	<div>  <div>.. (swap):</div> </div>	swap	



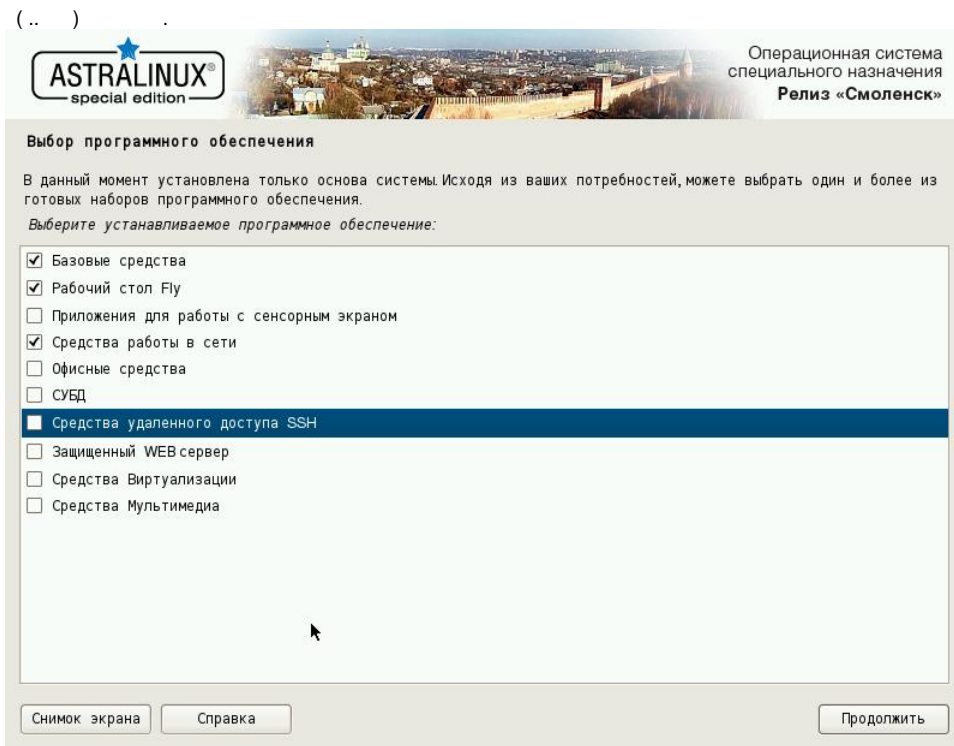
```

( /boot) ext4.
, /tmp 250

```

« () Ext2/Ext3/Ext4, (..) () »
 « , 1 » .10015-01 97 01-1, 2020., . 17.3.1 « »

- /home /tmp /var/tmp noexec,nodev,nosuid
- Astra Linux Special Edition .10015-01 (1.6) .
 - apache2.service
 - bind9.service
 - exim4 dovecot.service
 - ejabberd.service
 - nfs-client.target
 - ntp
 - nfs-server.service
 - nmbd.service
 - smbd.service
 - snmpd.service
 - pppd-dns.service
 - ssh.service
 - vsftpd.service
 - winbind.service
 - bluetooth.service
 - openvpn.service
 - sssd.service
 - firewalld.service



o

SSH: SSH, , . , .

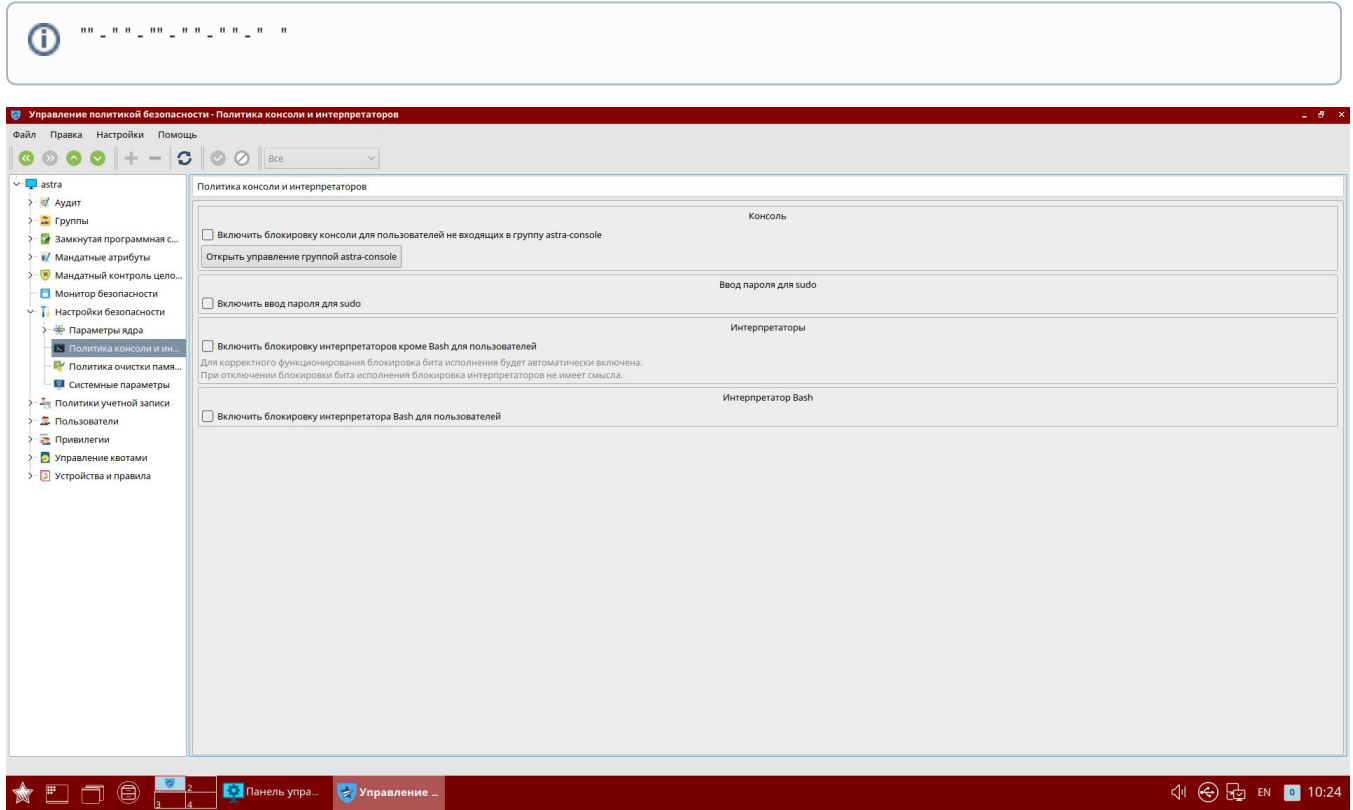
- " " :
 1. ;
 2. ;
 3. hardened. hardened lkrg generic (. [astra-safepolicy](#))
 4. ;
 5. (, SSD-);
 6. EXT- (, SSD-);
 7. ;
 8. ;
 9. ufw;
 10. ulimits;
 11. ptrace;

- "" Grub (). [Grub2](#)

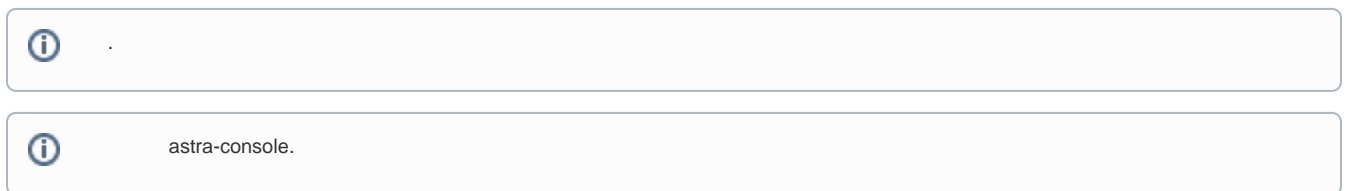
- , .
- HARDENED, , [Grub2](#)
- , Intel Management Engine (MEI). , [Intel Management Engine \(Intel ME\)](#).
- . - .
- , Intel, .
- /boot ro (rw).
- secureboot (usb-flash astra-secureboot, , BIOS) [Astra Linux SecureBoot](#)
- - / .
- (.. , sleep, suspend-to-disk, hibernation, ..).
- .

- `vim /etc/passwd` `login_local no`

fly-admin-smc:



- , astra-console;
- sudo;
- bash ;
- bash ;





:

```
astra-console-lock enable
```

sudo:

```
astra-sudo-control enable
```



, , , /etc/sudoers



Defaults timestamp_timeout=0



/etc/sudoers :

```
sudo visudo
```

bash:

```
astra-interpreters-lock enable
```

bash:

```
astra-bash-lock enable
```



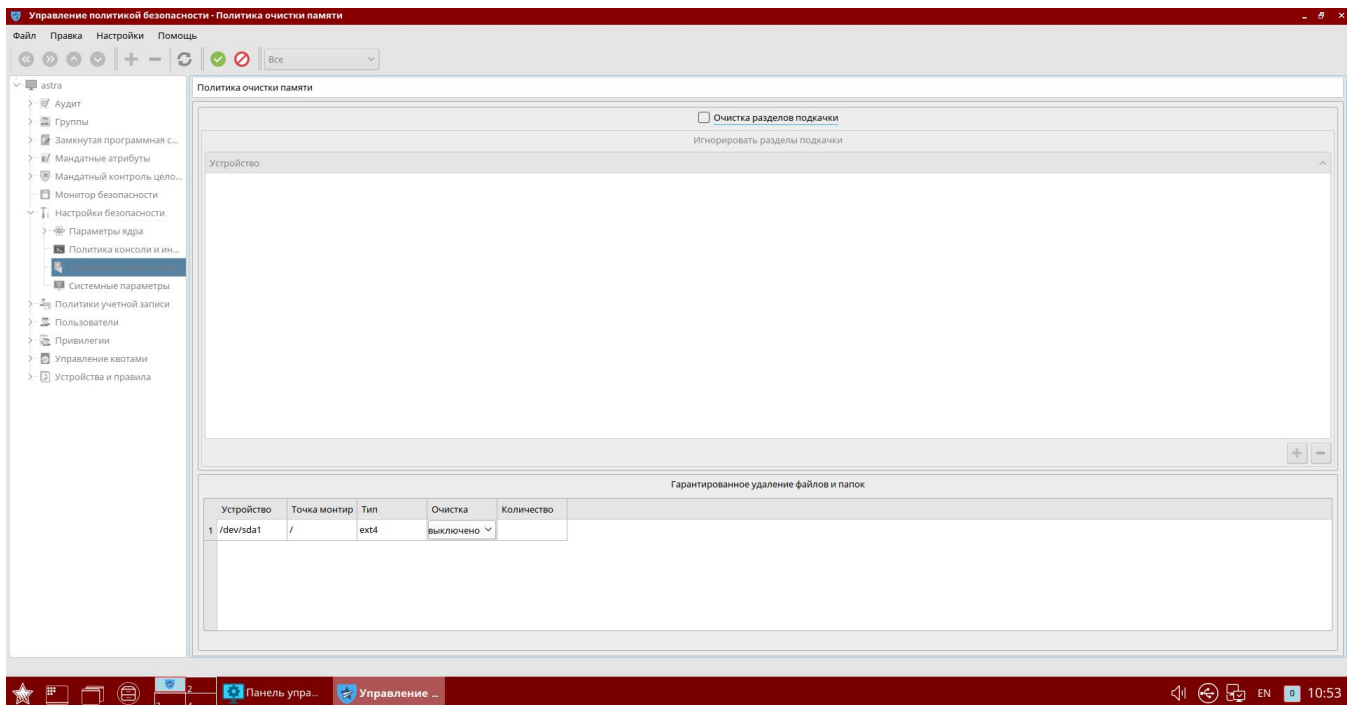
Astra Linux SE . , () , (, , .) . , , .

SSD . (SSD): ext4

fly-admin-smc



" " " " " " " " " " " "



• ;
• ;



:

```
astra-swapwiper-control enable
```

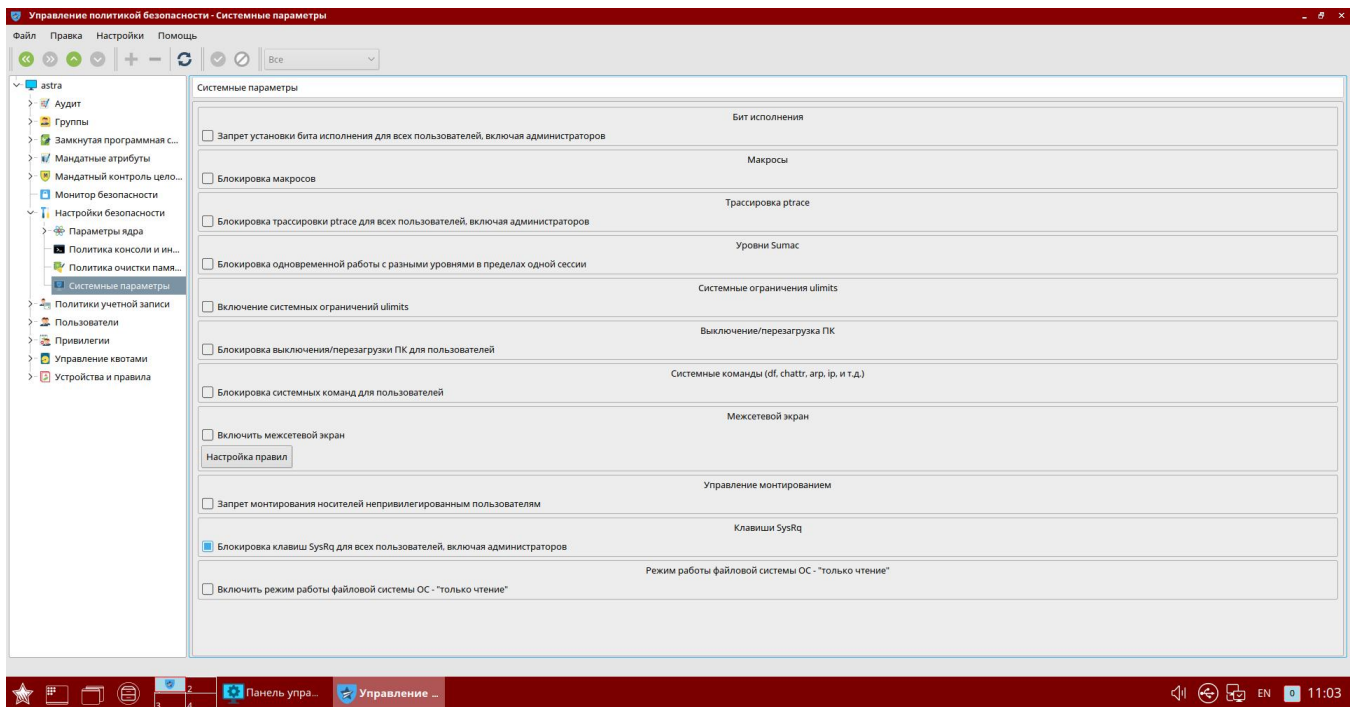
:

```
astra-secdel-control enable
```

fly-admin-smc



```
"" _ "" _ "" _ "" _ ""
```



- ;
- ;
- ptrace;
- ;
- ulimits;
- / ;
- ;
- ;
- ;
- SysRq , ;
- _ " "

! , , . , , (,) .



```
astra-nochmodx-lock enable
```

```
:
```

```
astra-macros-lock enable
```

```
ptrace:
```

```
astra-ptrace-lock enable
```

```
:
```

```
astra-sumac-lock enable
```

```
ulimits:
```

```
astra-ulimits-control enable
```

```
/ :
```

```
astra-shutdown-lock enable
```

```
:
```

```
astra-commands-lock enable
```

```
:
```

```
astra-ufw-control enable
```

```
:
```

```
astra-mount-lock enable
```

```
SysRq , :
```

```
astra-sysrq-lock enable
```

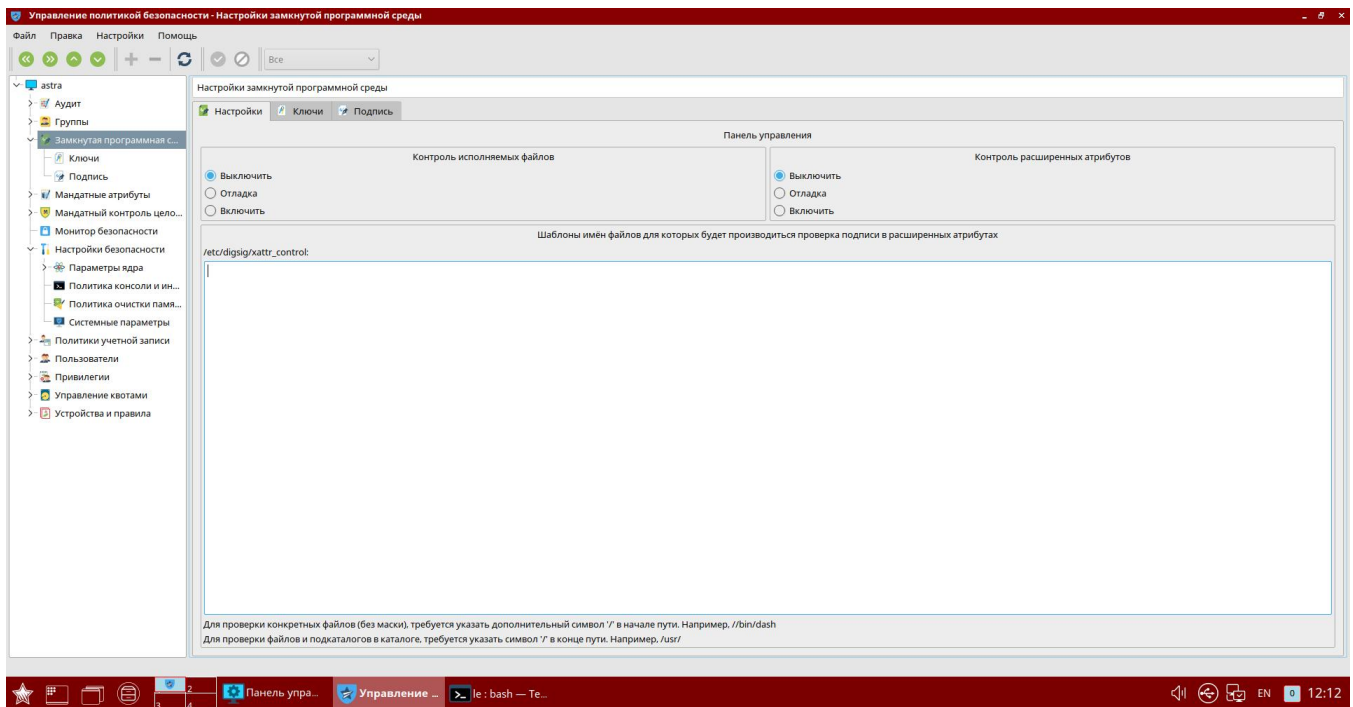
```
_" "
```

```
astra-overlay enable
```

fly-admin-smc:



```
"_ "_ "_ "_ "_ "_ "_ "
```

- (ELF-) xattr () (.16.1).
- :
- ;
- xattr , ;
- , () .
- /opt/.



/etc/digsig/digsig_initramfs.conf (. " "):

Astra Linux Special Edition .10015-01 (1.6) (.16.1):



```
DIGSIG_ELF_MODE=1
DIGSIG_XATTR_MODE=1
```

Astra Linux Special Edition .10015-01 (1.5) (.13.5):



```
DIGSIG_ENFORCE=1
DIGSIG_LOAD_KEYS=1
DIGSIG_USE_XATTR=1
```

:

```
update-initramfs -u -k all
```

i :

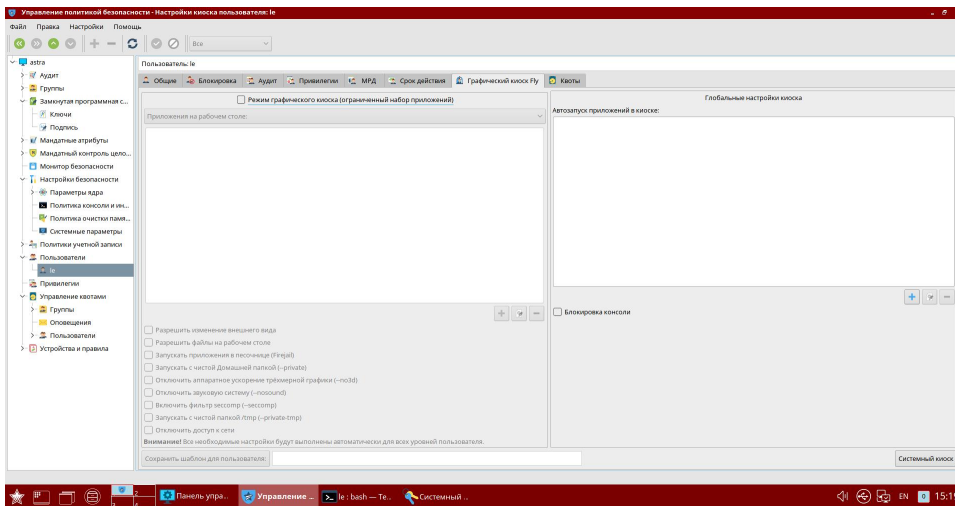
- , , (.16.2.1). fly-admin-kiosk:

i " _ " _ " _ " _ "

. -2: parsec-kiosk2 ().

- , , () . fly-admin-smc (.16.2.2):

i " _ " _ " _ " _ " _ " _ "
" Fly"




- :

```
o / ;  
o ;  
■ , , " (Firejail);  
• , "" :  
o ;  
o ;  
o ;  
o ;  
o seccomp;  
o /tmp;  
o ;
```


- , pam_tally ().
- , /etc/fstab,

sudo edquota

- , (..), :

 Astra Linux Special Edition .10015-01 (1.6) systemdgenie
Astra Linux Special Edition .10015-01 (1.5) chkconfig fly-admin-runlevel

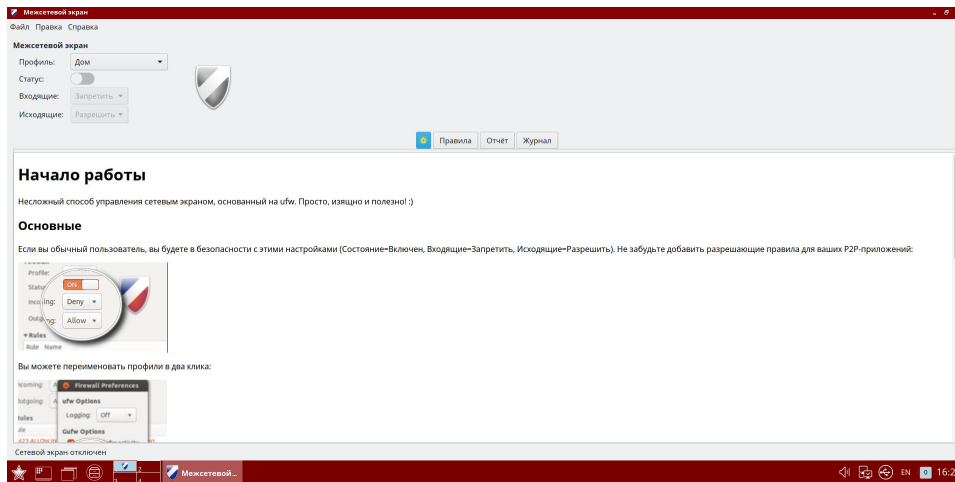
- ufw iptables , : ,

 Astra Linux Special Edition .10015-01 (1.6)


- iptables
- ufw
- gufw

gufw:

 " " " " " " "



- /etc/sysctl.conf (fly-admin-smc /etc/sysctl.conf:

 fs.suid_dumpable=0
kernel.randomize_va_space=2
kernel.sysrq=0
net.ipv4.ip_forward=0
net.ipv4.conf.all.send_redirects=0
net.ipv4.conf.default.send_redirects=0

, ' ' .
:

sudo sysctl -a | more

- ""



00 00

-

00 00

-

00 00

,

A