

## Red Book: Astra Linux Special Edition ( x.7)

- 
- ```

● Astra Linux
○
○
●
○
○ ( )
■
■
■
■
■ bash
○ ( <<> <<>)
■
■
■
○
■
■
● <<> <<>

```

# Astra Linux



- Astra Linux Special Edition .10015-01 ( 1.7)
- Astra Linux Special Edition .10015-10 ( , "" ""
- Astra Linux Special Edition .10015-17
- Astra Linux Special Edition .10015-37 ( 7.7)
- Astra Linux Special Edition .10152-02 ( 4.7)

- , SSD.
- , .

- — - ().

- «» BIOS .



«» :

- 8;
- ( );
- , .

- BIOS- Intel SGX ( ).

- «» «» . , , , «» - .

- (, , ).
- (WiFi, Bluetooth).
- WiFi — VPN.

- Intel Execute Disable Bit (XD-Bit) AMD No Execute Bit (NX-Bit) .

- « » ILO, RSA, iDRAC, ThinkServer EasyManage, AMT, iMana — , , , IP KVM.

- Intel Intel-SA-00086 Intel Management Engine ( ) Intel Management Engine ( — BIOS, ).  
Intel-SA-00086 Detection Tool. : <https://www.intel.ru/content/www/ru/ru/support/articles/000025619/software.html>.

- , , .
- , Intel, .
- secureboot (usb-flash astra-secureboot, , , BIOS) [Astra Linux SecureBoot](#) .

- « » «> » .

Astra Linux Special Edition x.7 .

- « » , :  
/ — ;  
/boot — ;  
/home — ;  
/tmp — , ;  
/var/tmp — . .

 , , .

:

|          | /                                                                                                                  |                  |                                   |
|----------|--------------------------------------------------------------------------------------------------------------------|------------------|-----------------------------------|
| /        | ( , /boot )                                                                                                        | ext4             | defaults                          |
| /boot    | <div> /boot LVM</div><br>512, 1GB | ext2, ext3, ext4 | ro<br><br>( rw)                   |
| /home    |                                                                                                                    | ext4             | noexec, nodev, nosuid             |
| /tmp     | /tmp 250                                                                                                           | ext4             | noexec, nodev, nosuid             |
| /var     | .<br>noexec, nodev, nosuid, :<br>◦ noexec . .<br>◦ noexec ( , dpkg).                                               | ext4             | defaults<br>noexec, nodev, nosuid |
| /var/tmp | .<br>/var /var/tmp noexec,nodev,nosuid                                                                             | ext4             | noexec, nodev, nosuid             |
| swap     | <div> .. (swap): .<br/>—</div>  | swap             |                                   |

- « » :
  - ufw.
  - hardened. hardened lkrng generic (. [astra-safepolicy](#)).

- ( ) « » :
  1. — GRUB 2. , .
  2. **pttrace** — .
  3. **sudo** — sudo.
  4. — , ., () , . root.
  5. — (pipe). , , ( ). astra-admin.
  6. — ;
  7. — astra-admin.
  8. **ulimits** — , /etc/security/limits.conf.
- «» « » .
  1. — .
  2. — , ELF.
  3. — , .
- «» « » :
  1. — .



. .10015-01 97 01-1 « «Astra Linux Special Edition». . 1».

- « GRUB » «» Grub. Grub — . .

( )

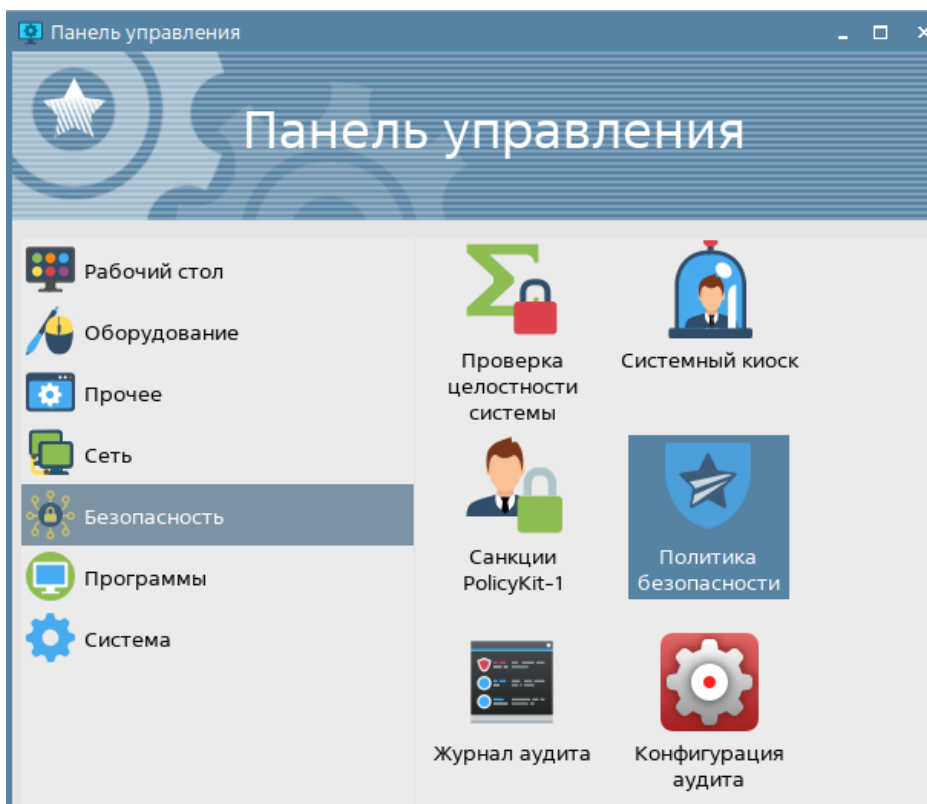
:

- — 8;
- , ;
- — 90;
- — 6;
- , — 1800 .

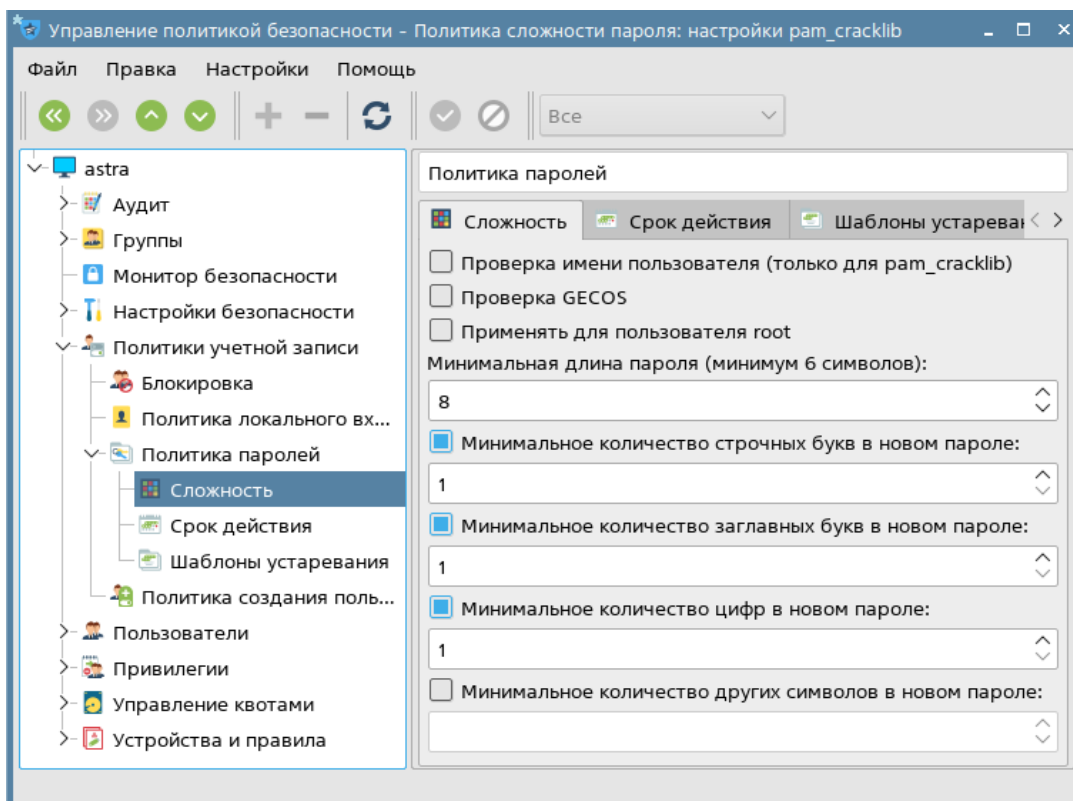
« »

fly-admin-smc. :

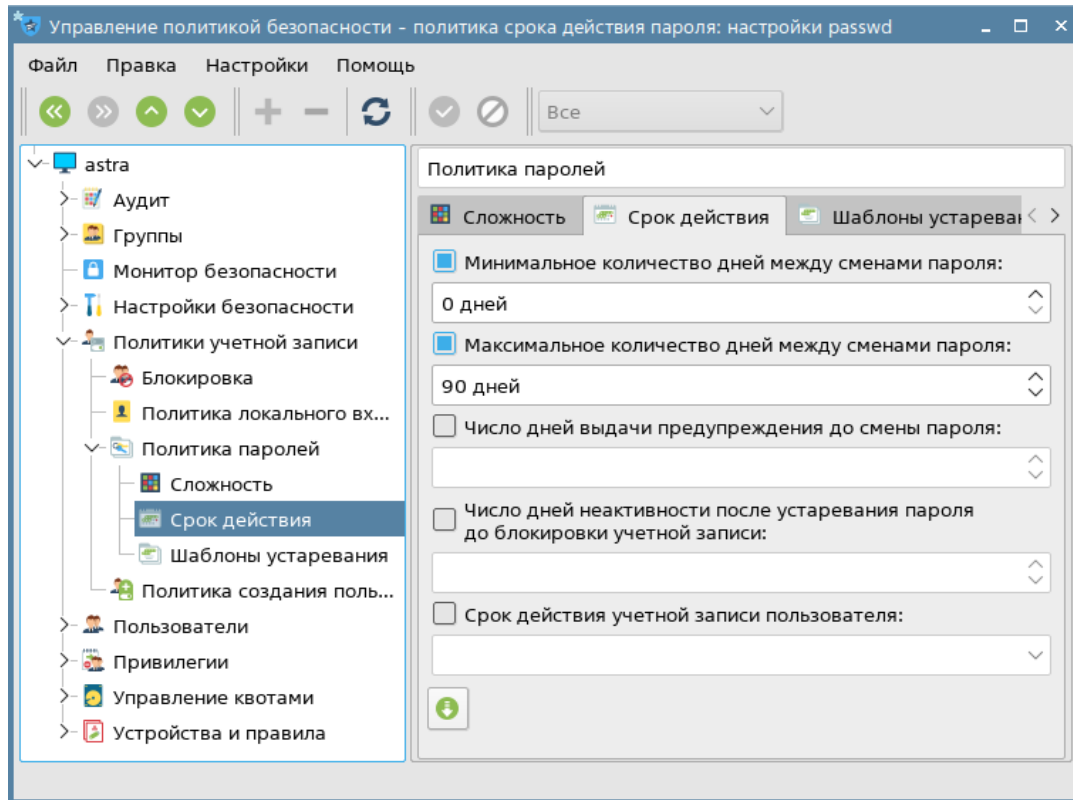
- ( ): — — — (..);



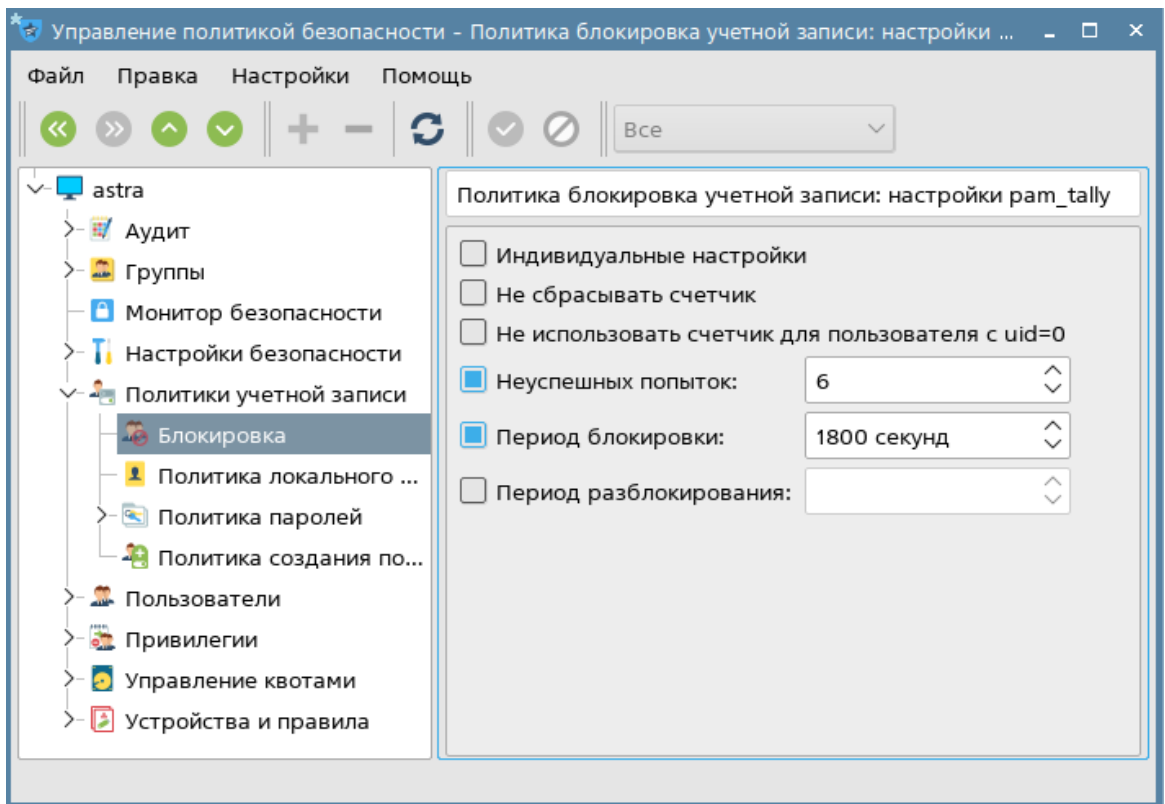
- — — (..):
  - — 8;
  - ;
  - ;



- — <Ctrl+S>;
- — (..):
  - «0 »;
  - «90 »;



- — <Ctrl+S>;
- — (..):
  - 6;
  - «1800 »;



- — <Ctrl+S>.

:

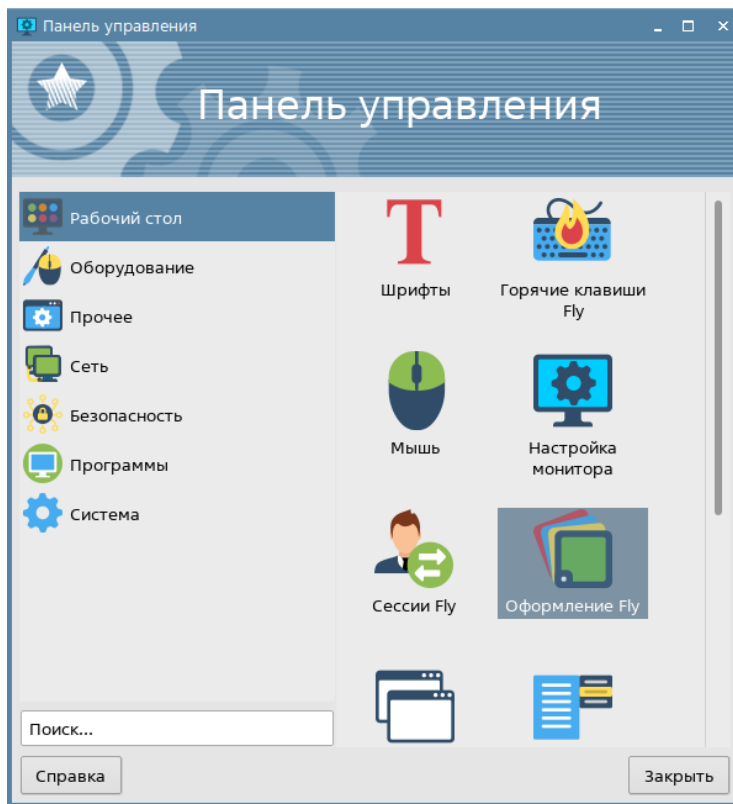
- /etc/pam.d/common-password password requisite pam cracklib.so minlen=8 dcredit=-1, ucredit=-1 1 credit=-1;
- /etc/login.defs PASS\_MAX\_DAYS 90, LOGIN\_RETRIES 6 LOGIN\_TIMEOUT 1800.

- , /etc/pam.d/common-password. «...pam\_unix.so» remember=4.
- sudo , . :
  - sudo visudo;
  - /etc/sudoers «Defaults timestamp\_timeout=0».

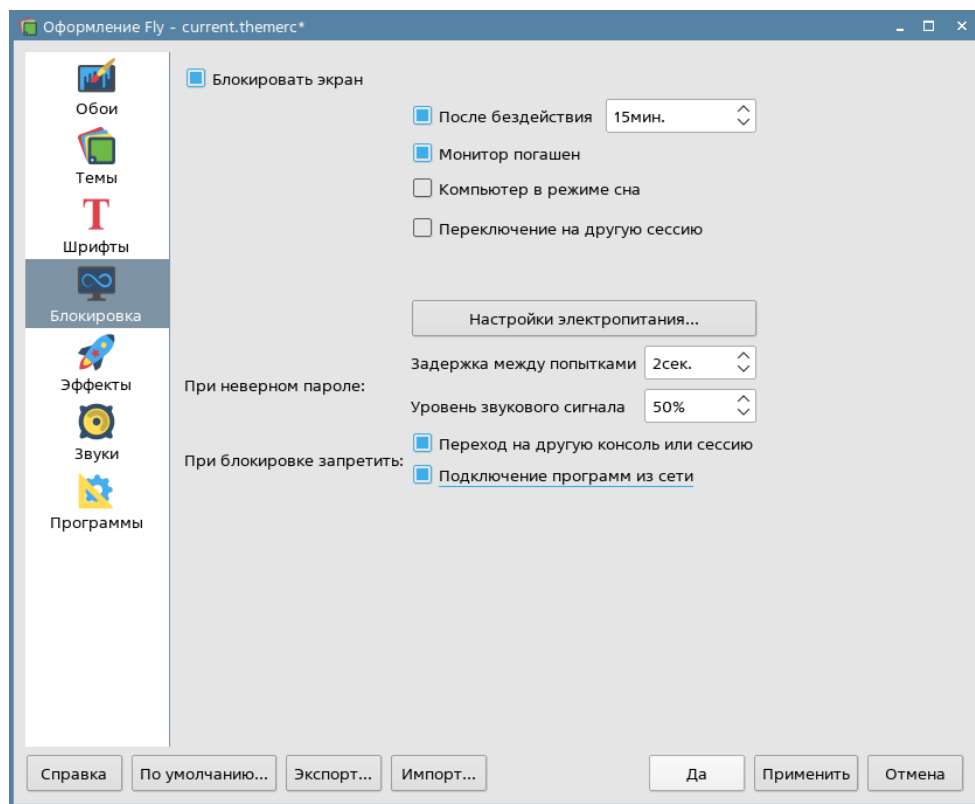


:

- fly-admin-theme: — — — Fly (. .);



- ( . . ) :  
○ :  
■ : 15 . ;  
○ :  
■ :  
■ :



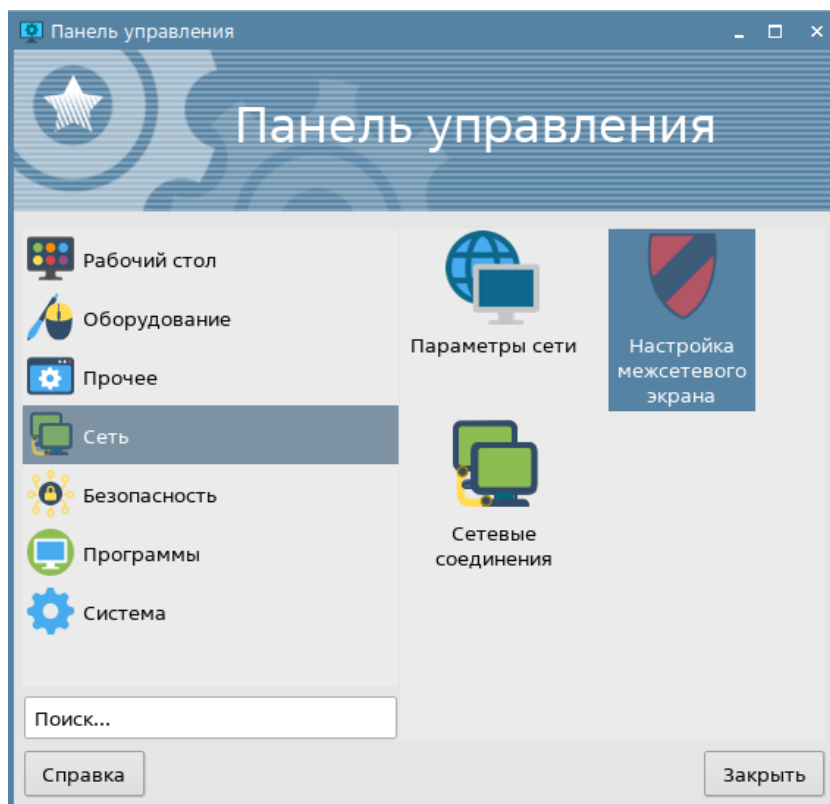
- 0.

ufw : , .

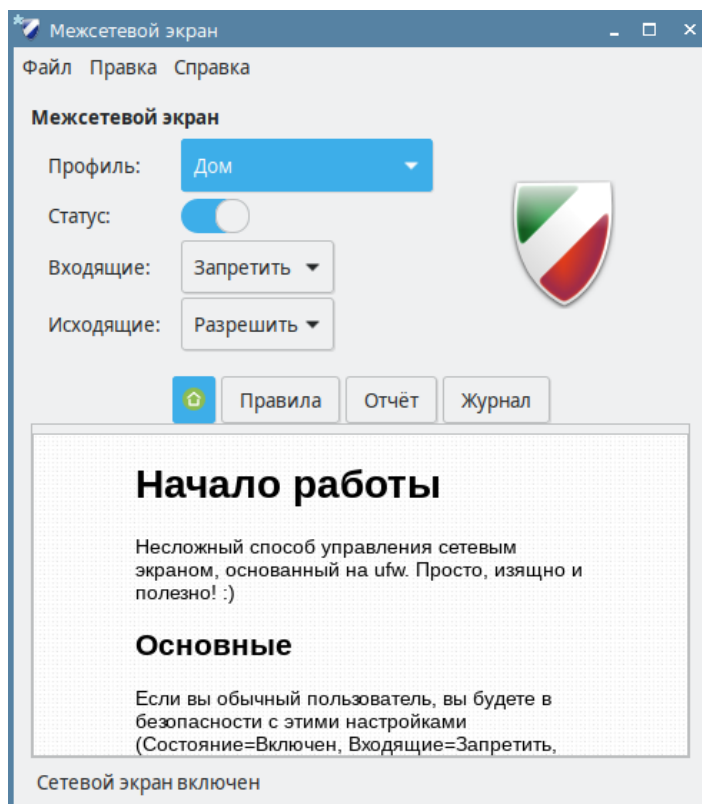
« »

ufw gufw. :

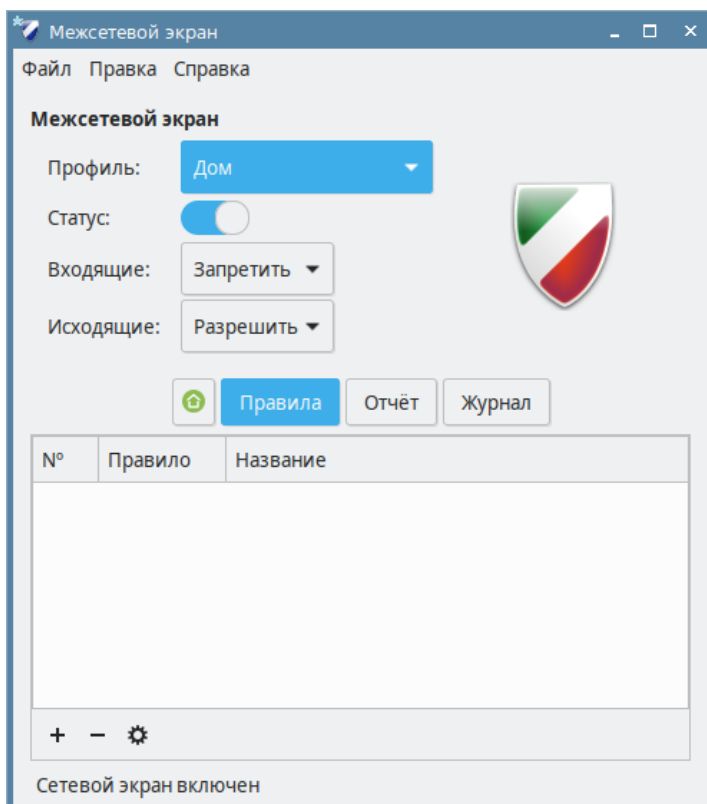
- ( ) : — — — ( . );



- (. .):



- □ (. .):



ufw, :

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

ufw, :

```
sudo astra-ufw-control status
```

, :

, , :

```
sudo ufw show builtins
```

**bash**

:

- ;
- bash().

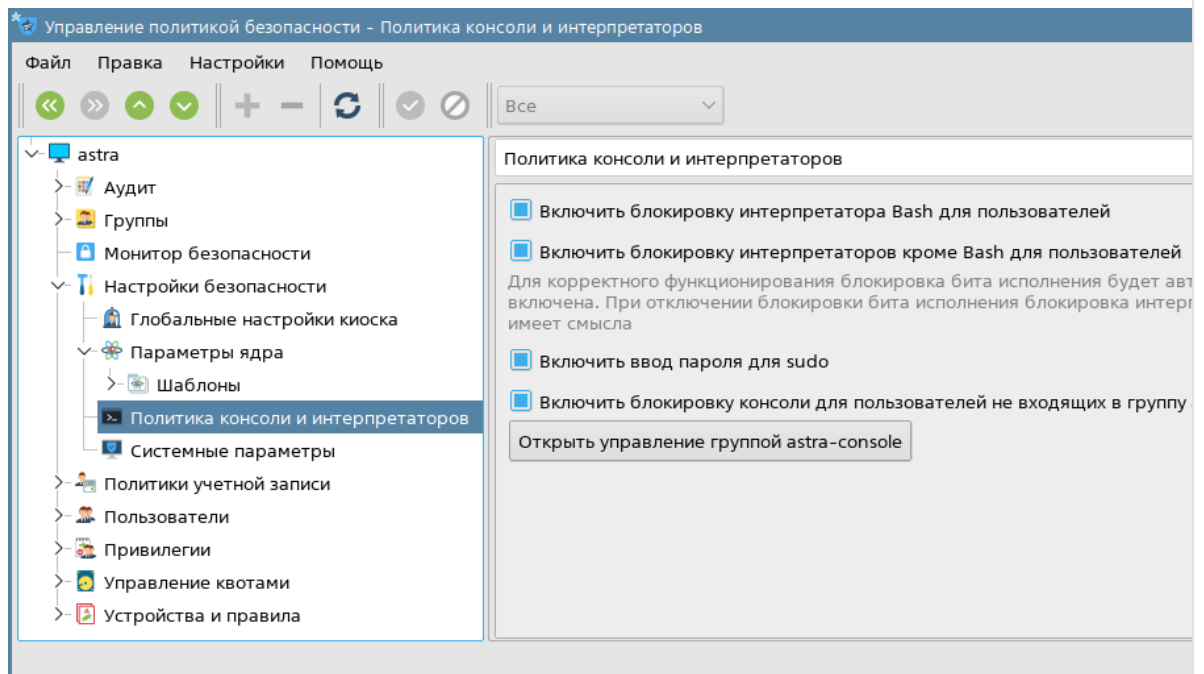


- astra-admin.
- bash , , bash, .
- bash , astra-admin :
  - bash;
  - .

« »

bash ( — ) fly-admin-smc. :

- ( ) : — — — ;
- — :
  - Bash (..);
  - Bash (..);



- — <Ctrl+S>.

:

- :

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

- bash:

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

:

- 1:

```
sudo astra-interpreters-lock status
sudo astra-bash-lock status
```

, :

- 2:

```
sudo astra-interpreters-lock is-enabled
sudo astra-bash-lock is-enabled
```

, :

- 3:  
astra-security-monitor:

```
sudo astra-security-monitor
```

:

```
sudo astra-security-monitor
...
```

```
bash

:12921 :0 :174955

ptrace
sumac
sysrq
UFW
ulimits

ELF
xattr

Overlay
sudo
SSH root
SSH fail2ban

1
Docker 2 docker-isolation
audit
audit-net
```

df, chattr, arp, ip.



, , ... .

750 (rwx r-x ---).

:

sudo astra-commands-lock enable

, :

sudo astra-commands-lock status

, :

:

|     |                                                                                       |
|-----|---------------------------------------------------------------------------------------|
|     |                                                                                       |
| « » | overlay , . , . , .<br>overlay , , ., /home , .<br>.                                  |
|     | , floppy, astra-admin.<br>.                                                           |
|     | /bin/systemctl 750 (rwx --- ---) fly-dmrc.<br>systemctl sudo. <Ctrl+Alt+Delete>.<br>. |

« »

, , , fly-admin-smc. :

- ( ): — — — ;
- — .

, , ( . ).

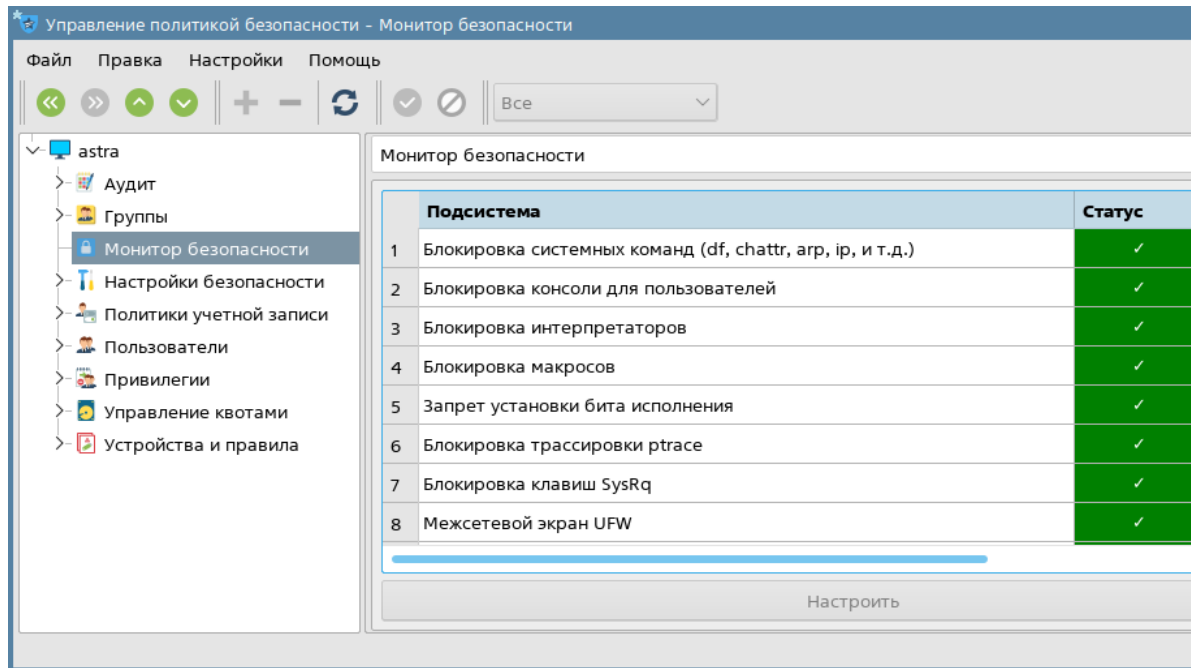
|     |                                 |
|-----|---------------------------------|
|     |                                 |
| « » | sudo astra-overlay enable       |
|     | sudo astra-mount-lock enable    |
|     | sudo astra-shutdown-lock enable |



« »

, fly-admin-smc. :

- ( ) : — — — ;
- . , , ( . ).



, , :

```
sudo astra-security-monitor
```

:

- — ; , ;
- — ;
- — ;
- — ;

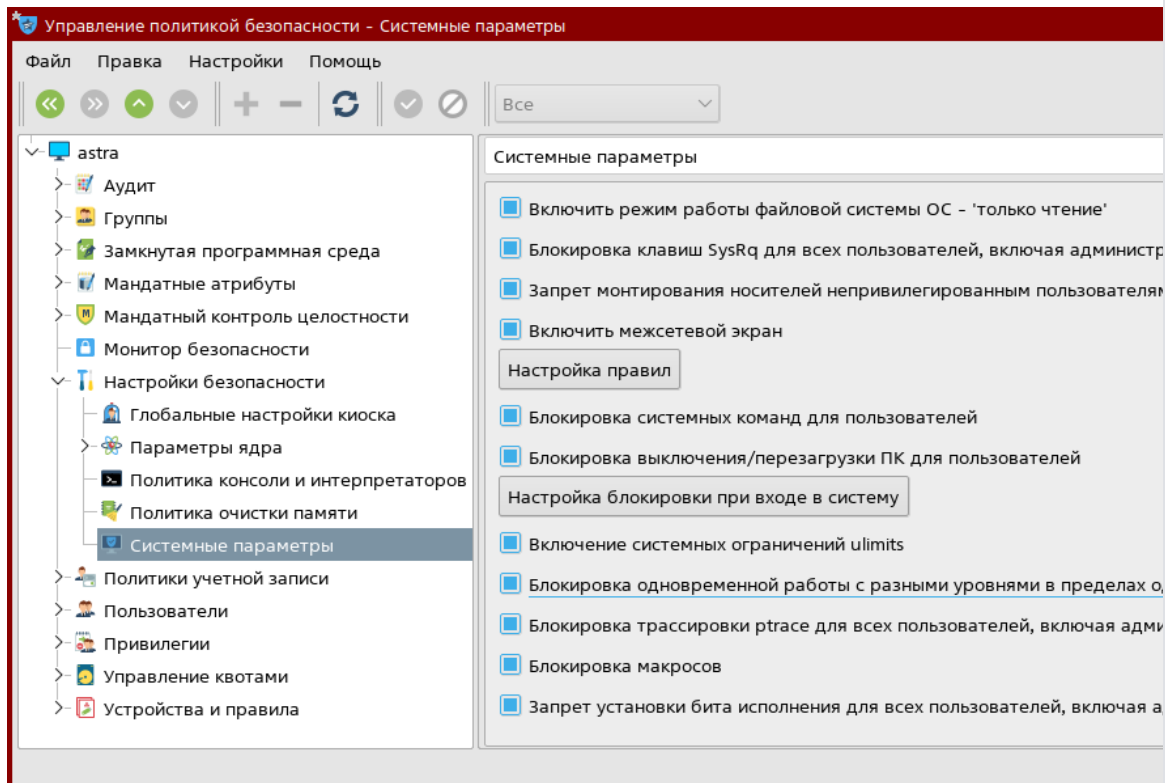
( «» «»)

```
, , PARSEC_CAP_SUMAC, sumac. 000 sumac libsumacrunner.so.
```

« »

, fly-admin-smc. :

- ( ) : — — — ;
- — (..);



- — <Ctrl+S>.

, , :

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

, :

```
sudo astra-sumac-lock status
```

, :

```

0) ELF, 0, .
   ELF    digsig_verif, Linux    :
   •      0,    ();
   •      ,    ,    ( );
   •      ( ).
       digsig_verif    :
   •      , , ;
   •      , , ,    ( );
   •      .
..: .

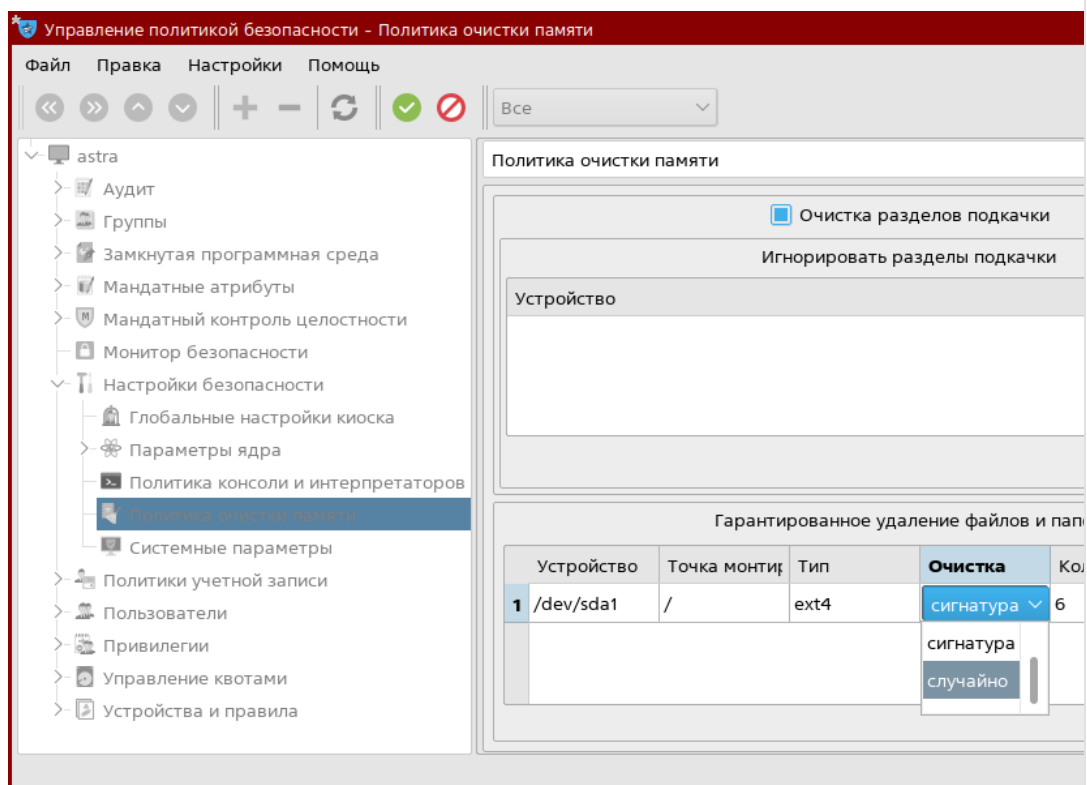
```


, , . :11111111, 01010101, 10101010, 00000000. , , 6, , , :11111111, 01010101, 10101010, 00000000, 11111111, 01010101.


, .

fly-admin-smc. :

- ( ) : — — — ;
- — ;
- , [ + ] , ;
- ( . . ) :
  - :
    - — ;
    - — ;
    - — ;
  - :



- — <Ctrl+S>.

, :

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

, :

```
sudo astra-swapwiper-control status
```

, :

, , /etc/parsec/swap\_wiper.conf IGNORE, .

, :

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

, :

```
sudo astra-secdel-control status
```

, :



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

.

, , /etc/fstab , , :

- secdel — ;
- secdelrnd — ;

., , 6, secdelrnd=6.

```
() parsec.max_ilev 63 — . , init fly-dm, .
```

 Xorg 8.

```
( ext2, ext3, ext4, XFS).
```

```
/etc/parsec/fs-ilev.conf. :<level> <path>,:
```

- <level> — ;
- <path> — / .

```
, <level> , .
```

| <number> | . , ,                        |
|----------|------------------------------|
| high     | max_ilev — , parsec.max_ilev |
| max      | max_ilev — , parsec.max_ilev |
| low      |                              |
| min      |                              |
| exc      | . «*»                        |

```
, . («/») .
```

```
, , /etc, .
```

```
/etc/parsec/fs-ilev.conf, :
```

```
sudo set-fs-ilev enable
```

- (.., sleep, suspend-to-disk, hibernation, ..).

- , , , , /etc/parsec/parsec.conf :
  - : login\_local all #
  - : login\_local no #

- root PAM- pam\_securetty /etc/pam.d/common-auth. «Primary block» :  
 auth required pam\_securetty.so

- , , —. : parsec-kiosk2 ();
- , , ( ) —..

«» «»

- CIFS, (..) ;



NFS :

- :
- NFS 3.

- :
  - ( None DefaultAuthType /etc/cups/cupsd.conf) PARSEC;
  - Exim Dovecot ;

- :
  - postgresql.conf enable\_bitmapscan off ac\_ignore\_socket\_maclabel false;
  - pg\_hba.conf trust();

- XPARSEC -( XPARSEC=Disable -);

- qemu-guest-agent qemu-ga ( ) -m unix-listen -p -t, , (.. , ).

<<>> <<>>

0, , :

1. , PARSEC, ,
2. , , PARSEC\_CAP\_SETMAC PARSEC\_CAP\_CHMAC, .
3. , (, TCP/IP), (PARSEC\_CAP\_SETMAC PARSEC\_CAP\_PRIV\_SOCK) PARSEC, , , .
4. **RabbitMQ** .
5. , wsgi\_mod **Apache**, , wsgi\_mod. wsgi\_mod , .
6. , , **Erlang**.

, , 0 ,:

- vmlinuz-\*, /boot, , /lib/modules, , ;
- security\_operations \*security\*;
- init=<\_\_\_\_>;
- PAM-, /etc/pam.d;
- (PAM-), API libparsec-mac PARSEC, mac\_set\_, parsec\_pdp\_;
- PAM-, PARSEC API libparsec-cap PARSEC, mcap parsec\_;
- , ;
- , , (bash, dash, PHP, Perl, Python, TCL, Ruby);
- CAP\_SYS\_PTRACE ptrace;
- ( );
- ;
- ctl parsecfs ioctl, API- libparsec-.\*.

**Apache2** AstraMode. /etc/apache2/apache2.conf. , AstraMode (), AstraMode on. /etc/apache2/apache2.conf / AstraMode off.



**Apache2** ( www-data), 1.