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

:

- 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)

Astra Linux

- , 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	/boot LVM 512, 1GB	ext2, ext3, ext4	`ro` (`rw`)
/home		ext4	`noexec, nodev, nosuid`
/tmp	/tmp 250	ext4	`noexec, nodev, nosuid`
/var	. `noexec, nodev, nosuid,` : ○ `noexec` . . ○ `noexec` (, dpkg).	ext4	`defaults` `noexec, nodev, nosuid`
/var/tmp	. /var /var/tmp `noexec,nodev,nosuid`	ext4	`noexec, nodev, nosuid`
swap	. . (swap): . —	swap	

- « » :
  - ufw.
  - hardened. hardened lkrg generic (. astra-safepolicy).

- ( ) « » :
  1. — GRUB 2. , .
  2. **ptrace** — .
  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 — . .

( )

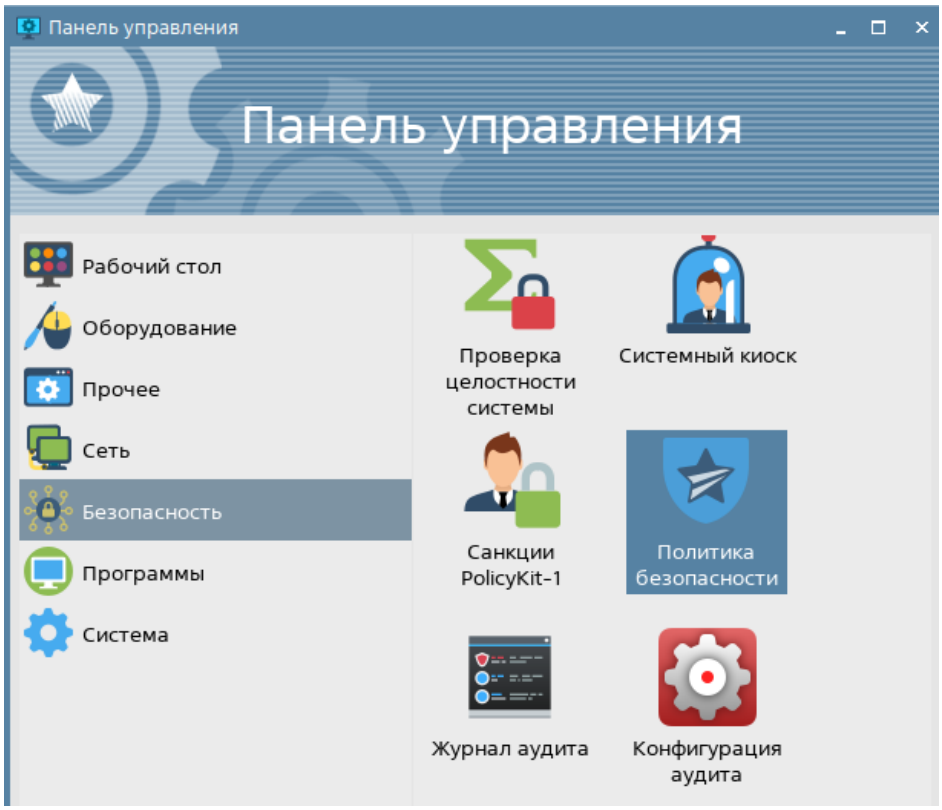
:

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

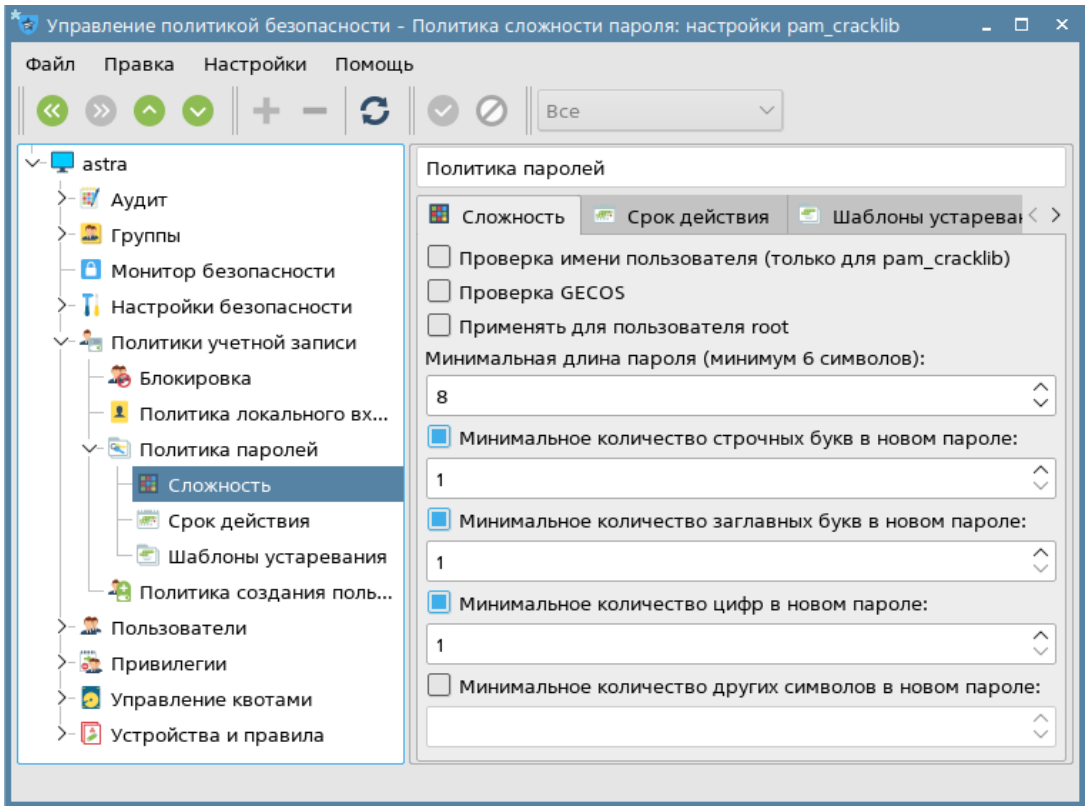
« »

fly-admin-smc. :

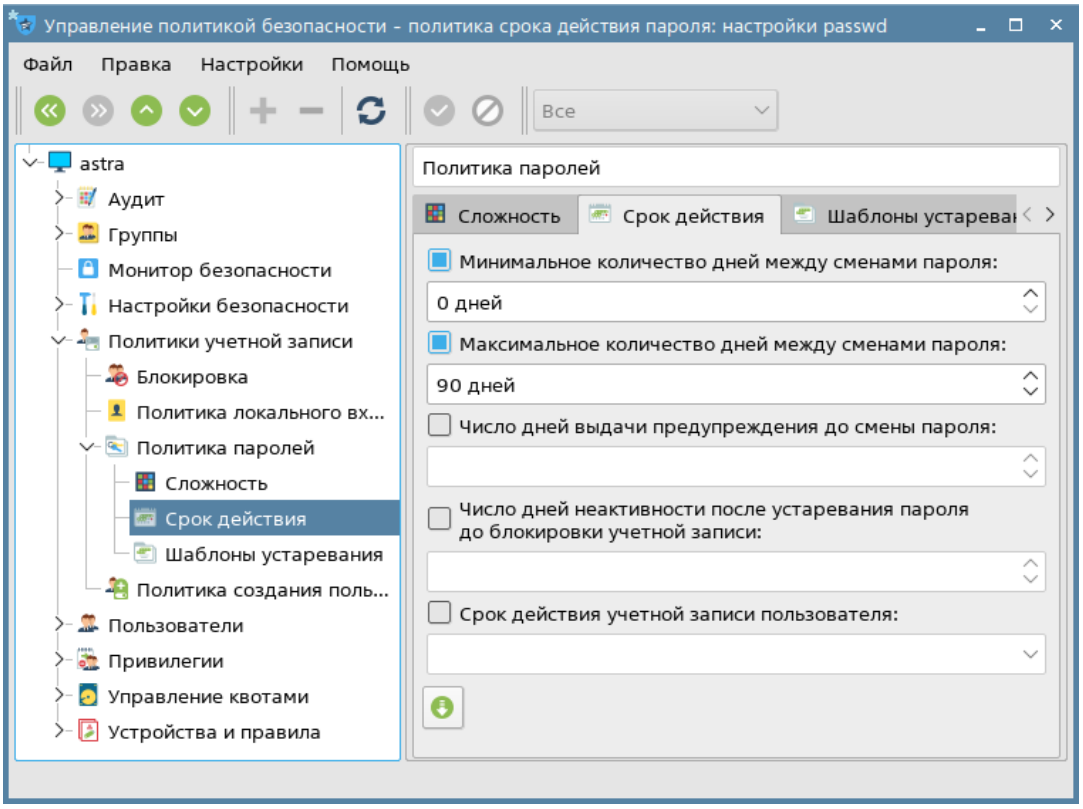
- ( ): — — — (. .);


Панель управления
Панель управления
Рабочий стол
Оборудование
Прочее
Сеть
Безопасность
Программы
Система
Проверка целостности системы
Системный киоск
Санкции PolicyKit-1
Политика безопасности
Журнал аудита
Конфигурация аудита

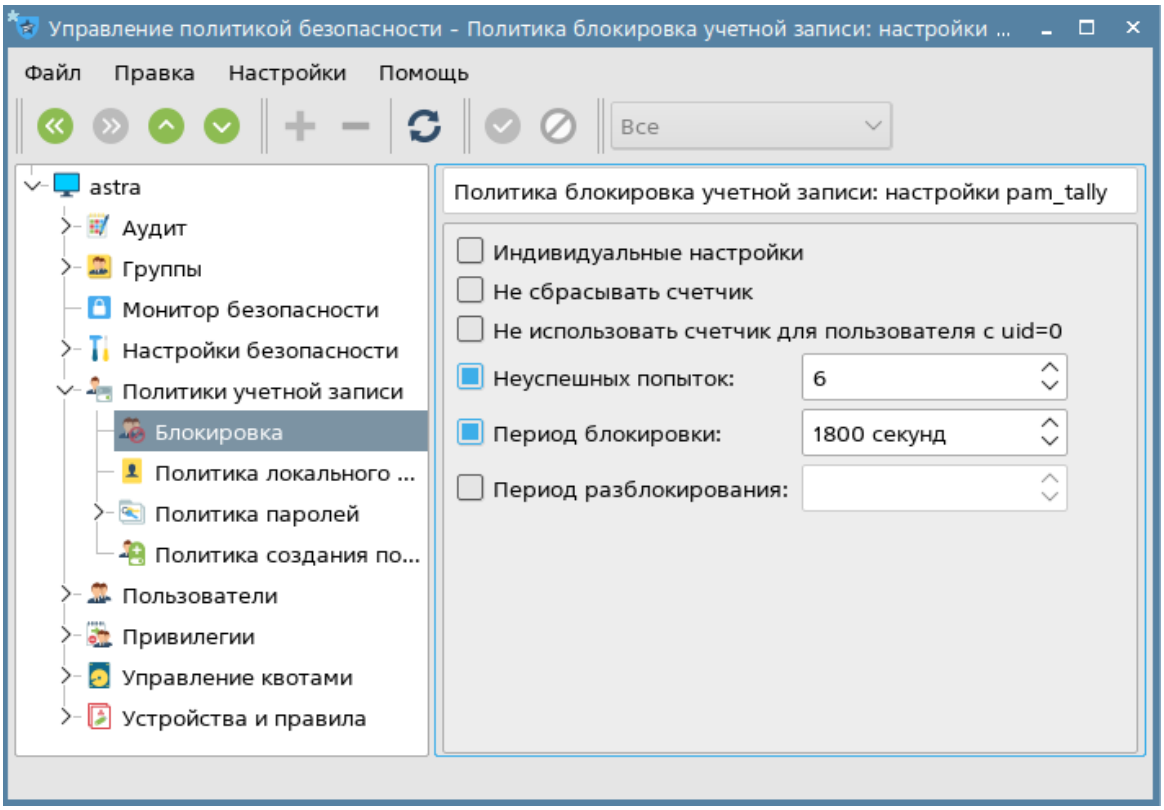
- — — (. .):
  - — 8;
  - ;
  - ;
  - ;


Управление политикой безопасности - Политика сложности пароля: настройки pam_cracklib
Файл
Правка
Настройки
Помощь
Все
astra
Аудит
Группы
Монитор безопасности
Настройки безопасности
Политики учетной записи
Блокировка
Политика локального вх...
Политика паролей
Сложность
Срок действия
Шаблоны устарева
Политика создания поль...
Пользователи
Привилегии
Управление квотами
Устройства и правила
Политика паролей
Сложность
Срок действия
Шаблоны устарева
Проверка имени пользователя (только для pam_cracklib)
Проверка GECOS
Применять для пользователя root
Минимальная длина пароля (минимум 6 символов):
8
Минимальное количество строчных букв в новом пароле:
1
Минимальное количество заглавных букв в новом пароле:
1
Минимальное количество цифр в новом пароле:
1
Минимальное количество других символов в новом пароле:

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



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



- — **<Ctrl+S>**.

:

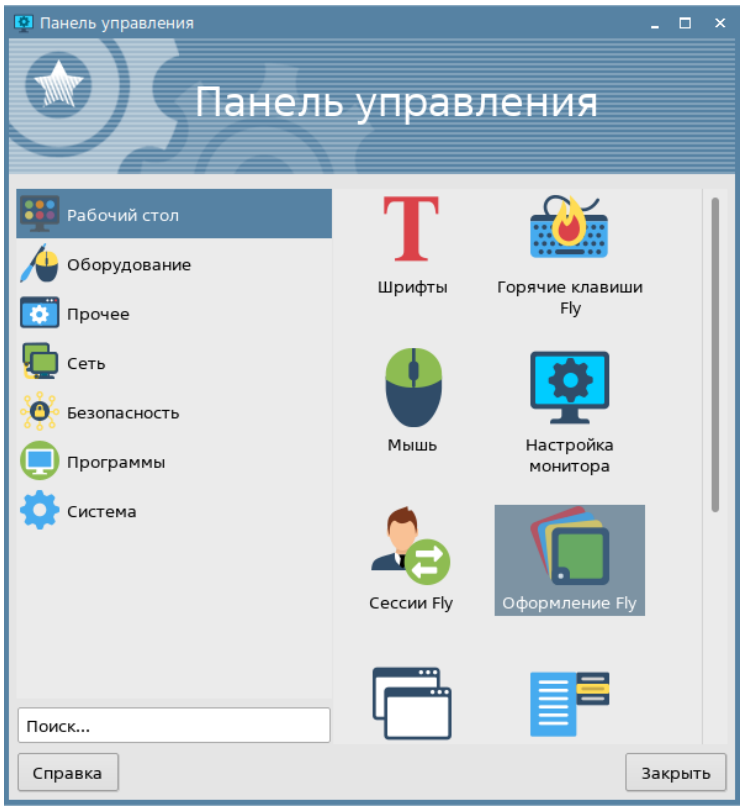
- `/etc/pam.d/common-password password requisite pam cracklib.so minlen=8 dcredit=-1, ucredit=-1 lcredit=-1;`
- `/etc/login.defs PASS_MAX_DAYS 90, LOGIN_RETRIES 6 LOGIN_TIMEOUT 1800.`

- , `/etc/pam.d/common-password.` `«...pam_unix.so» remember=4.`
- `sudo ,` . :
  - `sudo visudo;`
  - `/etc/sudoers «Defaults timestamp_timeout=0».`

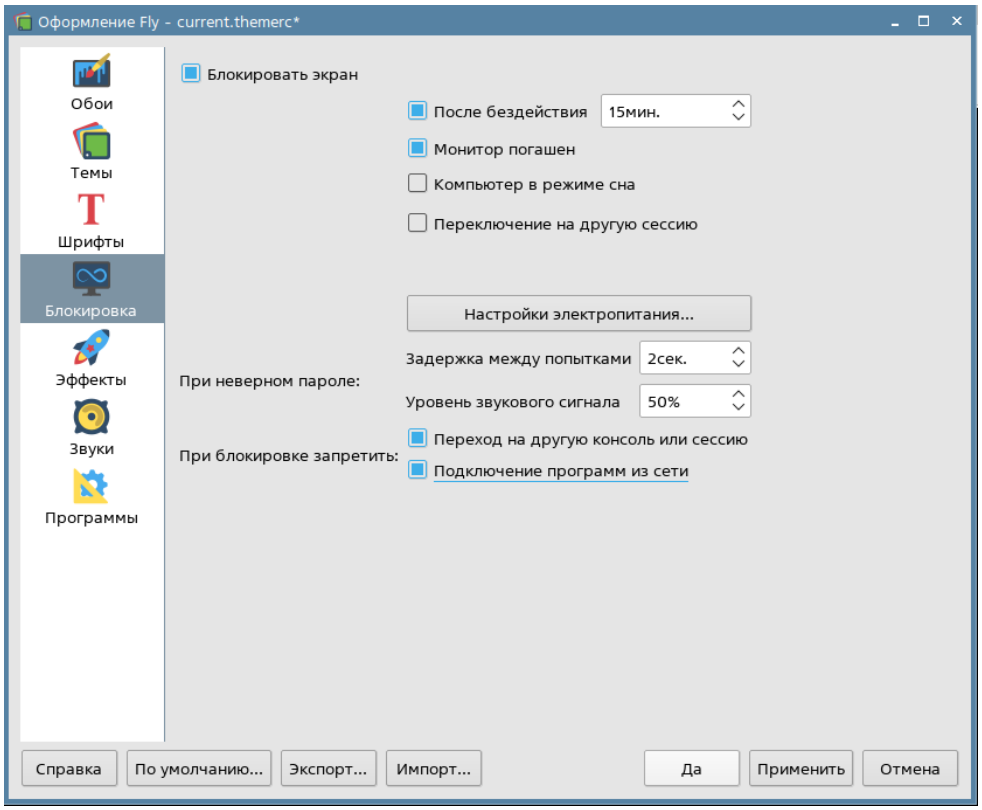
.

:

- fly-admin-theme: — — — **Fly** (. .);


Панель управления
Панель управления
Рабочий стол
Оборудование
Прочее
Сеть
Безопасность
Программы
Система
Шрифты
Горячие клавиши Fly
Мышь
Настройка монитора
Сессии Fly
Оформление Fly
Поиск...
Справка
Закрыть

- (. .):
  - :
    - 15 .;
    - ;
    - ;
  - :
    - ;
    - ;


Оформление Fly - current.themerc*
Обои
Темы
Шрифты
Блокировка
Эффекты
Звуки
Программы
Блокировать экран
После бездействия
15мин.
Монитор погашен
Компьютер в режиме сна
Переключение на другую сессию
Настройки электропитания...
Задержка между попытками
2сек.
При неверном пароле:
Уровень звукового сигнала
50%
При блокировке запретить:
Переход на другую консоль или сессию
Подключение программ из сети
Справка
По умолчанию...
Экспорт...
Импорт...
Да
Применить
Отмена

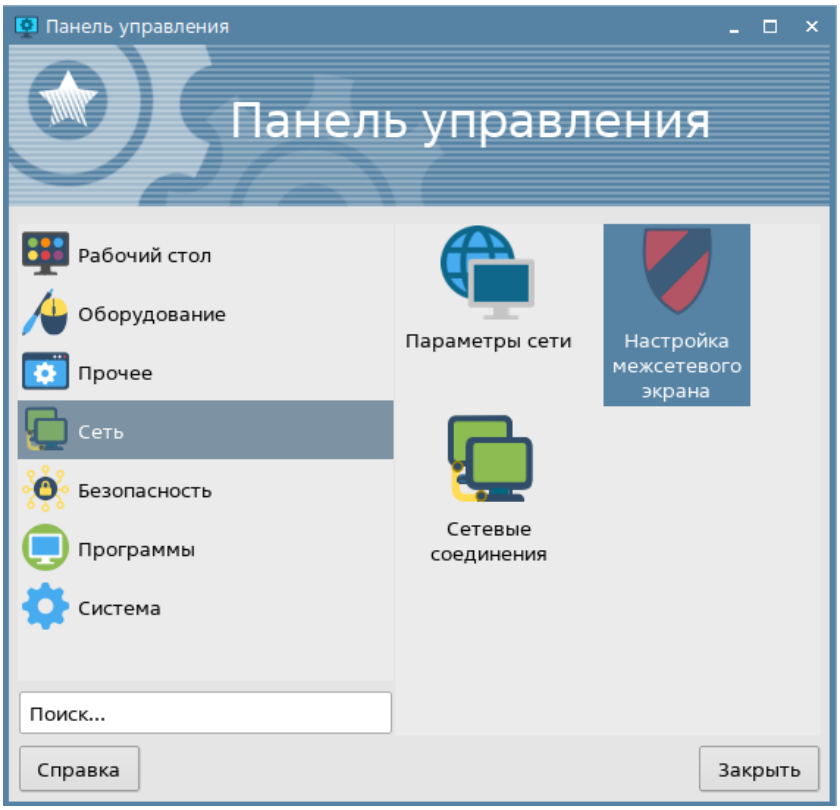
- .

ufw : , .

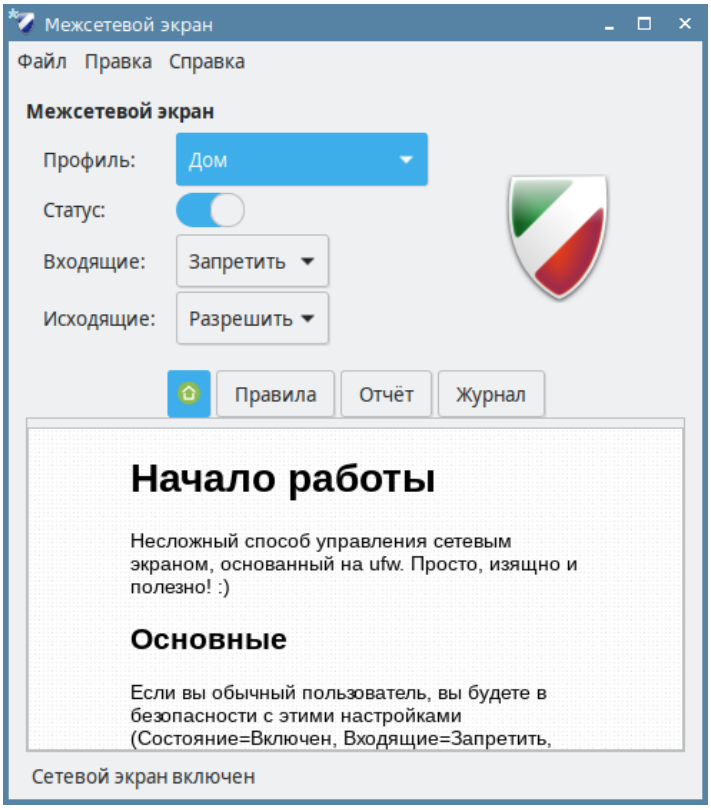
« »

ufw gufw. :

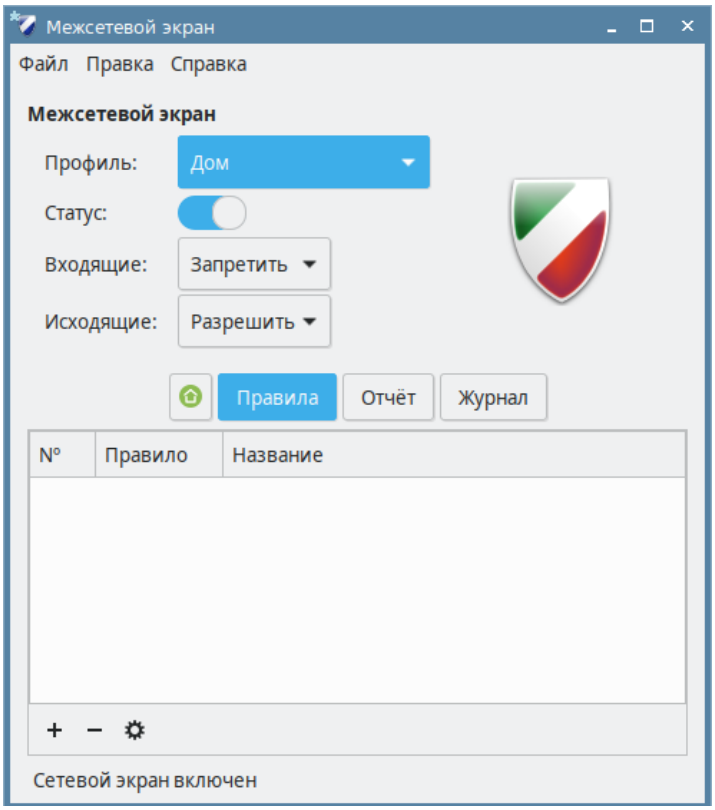
- ( ): — — — (. .);


Панель управления
Панель управления
Рабочий стол
Оборудование
Прочее
Сеть
Безопасность
Программы
Система
Параметры сети
Настройка межсетевого экрана
Сетевые соединения
Поиск...
Справка
Закрыть

- (. .):


Межсетевой экран
Файл Правка Справка
Межсетевой экран
Профиль:
Дом
Статус:
Входящие:
Запретить
Исходящие:
Разрешить
Правила
Отчёт
Журнал
Начало работы
Несложный способ управления сетевым экраном, основанный на ufw. Просто, изящно и полезно! :)
Основные
Если вы обычный пользователь, вы будете в безопасности с этими настройками (Состояние=Включен, Входящие=Запретить,
Сетевой экран включен

- (. .):



ufw , :

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

ufw, :

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

, :

```

```

, , :

```
sudo ufw show builtins
```

bash

:

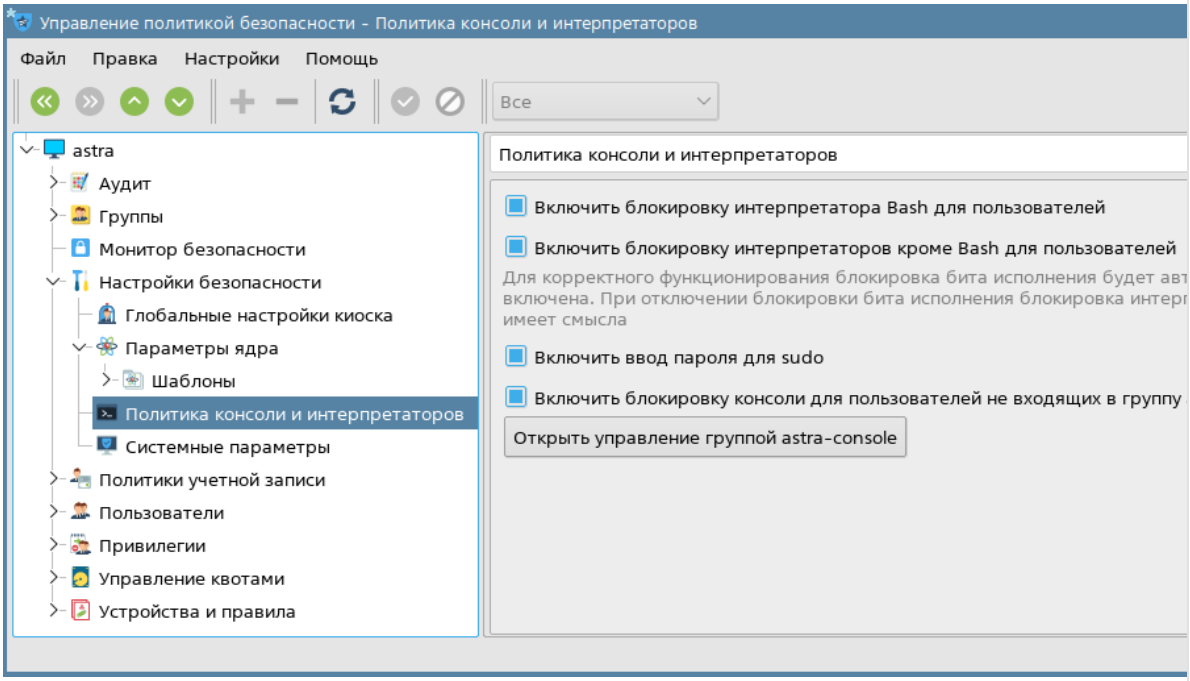
- ;
- bash ( ).

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

« »

, , , fly-admin-smc. :

- ( ): — — — ;
- — .

, , (.).

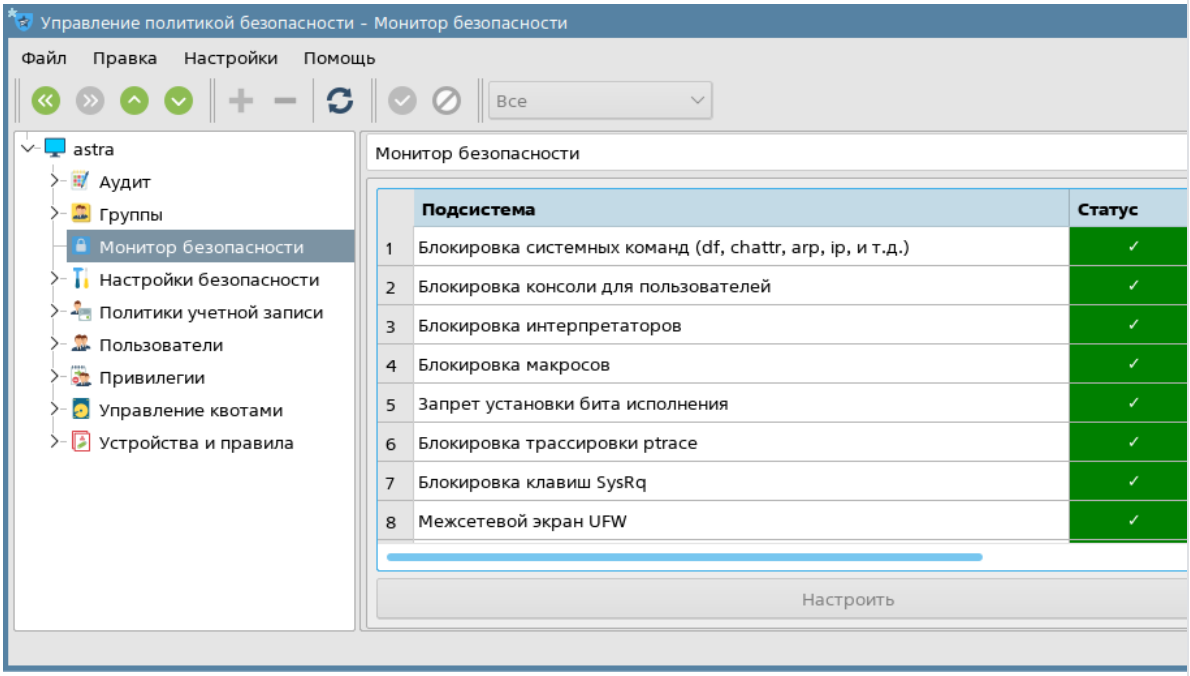
« »	sudo astra-overlay enable
	sudo astra-mount-lock enable
	sudo astra-shutdown-lock enable

.

« »

, fly-admin-smc. :

- ( ): — — — ;
- . , , (.).



, , :

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

:

- — . , ;
- — ;
- — , ;
- — , .

(«» «»)

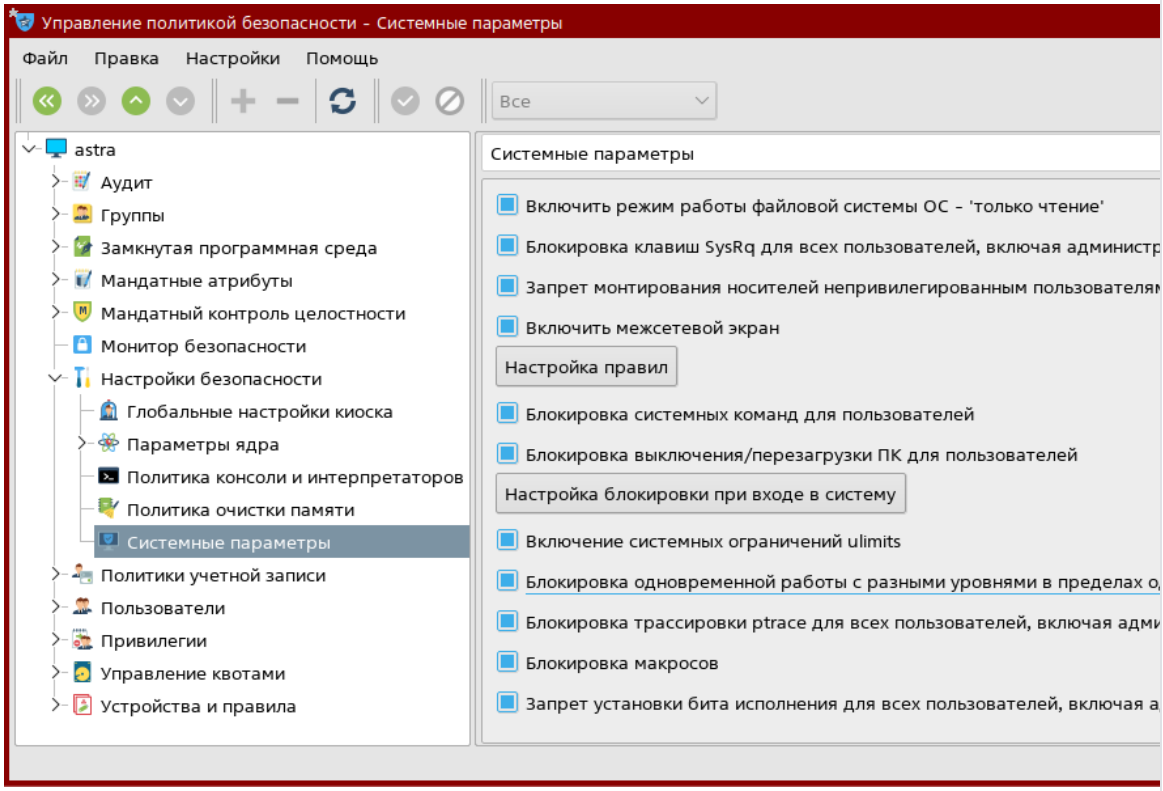
, , PARSEC_CAP_SUMAC, sumac. 000 sumac libsumacrunner.so.

.

« »

, fly-admin-smc. :

- ( ): — — — ;
- — (. .);



- — **<Ctrl+S>**.

, , :

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

, :

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

, :

() ELF, (), .

ELF digsig_verif, Linux :

- (), ( );
- , , ( );
- ( ).

digsig_verif :

- , , ;
- , , , ( );
- .

. : .

, . .

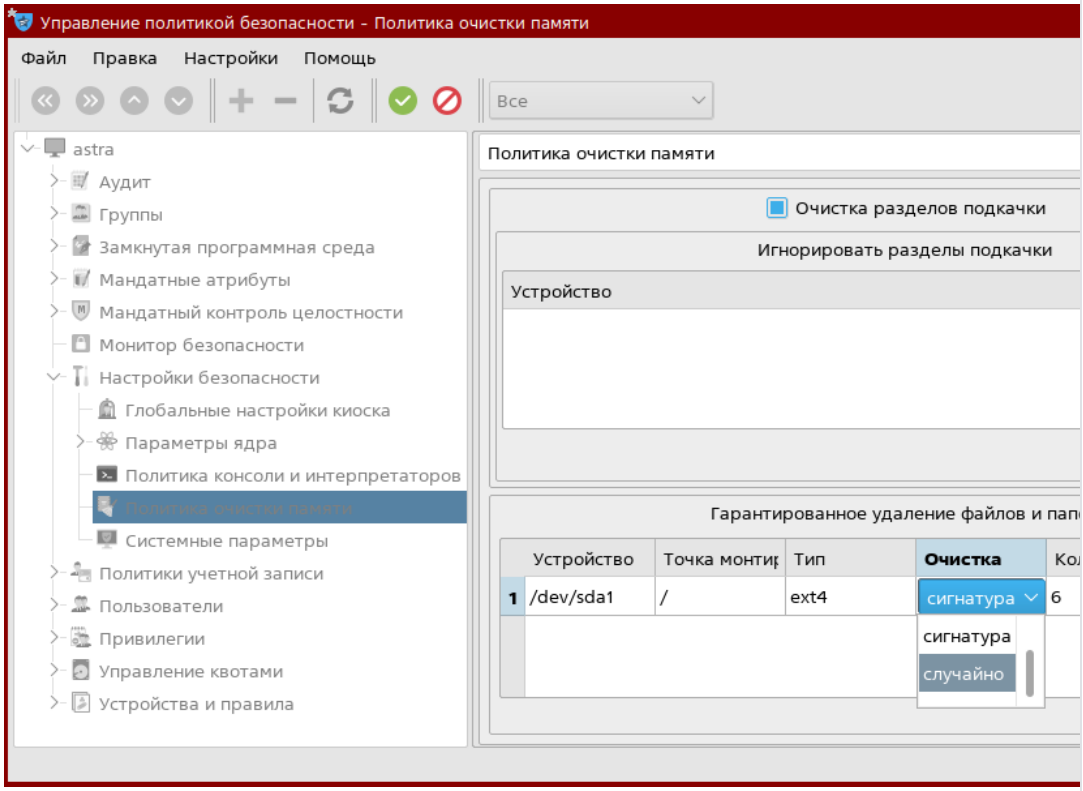
, , . : 11111111, 01010101, 10101010, 00000000. . , , 6, , , : 11111111, 01010101, 10101010, 00000000, 11111111, 01010101.

, .

« »

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, , (.. ,).

«» «»

(), , :

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**.

, , () , :

- 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.