



**ПРОГРАММНЫЙ КОМПЛЕКС  
«СИСТЕМА КОНТРОЛЯ ДЕЙСТВИЙ ПОСТАВЩИКОВ ИТ-УСЛУГ»**

**РУКОВОДСТВО АДМИНИСТРАТОРА.  
КОМАНДЫ КОНСОЛИ АДМИНИСТРИРОВАНИЯ**

**RU.33654484.0004-02 91 05**

**Листов 12**

## СОДЕРЖАНИЕ

1 Введение.....	3
1.1 Область применения.....	3
1.2 Краткое описание возможностей.....	3
1.3 Уровень подготовки администратора.....	4
2 Общие сведения.....	5
2.1 Перечень утилит консоли администрирования СКДПУ.....	5
Перечень сокращений.....	9
Перечень таблиц.....	11
Лист регистрации изменений.....	12

## 1 ВВЕДЕНИЕ

### 1.1 Область применения

Настоящий документ предназначен для администраторов СКДПУ и содержит перечень и описание команд консоли администрирования для доступа к администрируемым устройствам (серверам, сетевым устройствам, оборудованию для обеспечения безопасности и веб-интерфейсам администрирования).

### 1.2 Краткое описание возможностей

Основные возможности СКДПУ приведены в [таблица 1](#).

**Таблица 1 – Основные возможности СКДПУ**

Основные возможности	Описание
Контроль доступа	СКДПУ позволяет создать политику управления доступом на основе прав пользователей: целевые учетные записи, протоколы, интервалы времени и типы сеансов.
Единая точка входа в систему (SSO)	Для доступа к учетным записям достаточно предоставить имя пользователя и пароль в СКДПУ.
Поддержка нескольких протоколов администрирования	СКДПУ поддерживает следующие протоколы администрирования устройств и серверов: RDP/TSE, SSH, TELNET, VNC, SFTP/SCP и т.д.
Отслеживание активности и запись сеансов	Регистрация и возможность записи всех действий, выполненных на управляемых устройствах в течение графического сеанса (RDP/TSE или VNC) или сеанса командной строки (SSH, TELNET).
Управление паролями	СКДПУ позволяет изменять пароли на управляемых устройствах по запросу или через заданные интервалы времени.
Работа без использования агентов	СКДПУ работает без использования специальных агентов на администрируемых устройствах или на рабочих станциях администраторов.

Основные возможности	Описание
Статистика и отчеты о действиях	Возможность формировать рабочую статистику/отчеты и экспортировать эти данные в формате CSV через интерфейс администратора.
Делегирование функций администрирования СКДПУ	Средства управления профилями позволяют определить, какие действия будут доступны каждому пользователю СКДПУ (например, создание пользователей, управление правами и т.д.)
Анализ потока и распознавание текста	СКДПУ позволяет в реальном времени обнаруживать определенные строки символов в сессиях SSH и анализировать содержимое сеансов подключения к удаленному рабочему столу ( RDP/TSE).
Контроль в реальном времени	Администраторы СКДПУ могут просматривать активные сеансы подключения к удаленному рабочему столу и SSH в СКДПУ в реальном времени.
Поддержка Web Service	Вся информация о пользователях, учетных записях, устройствах, правах доступа в СКДПУ может вводиться или быть доступна с помощью Web Service API.

### 1.3 Уровень подготовки администратора

Администратор должен обладать следующими знаниями:

- Системное администрирование ОС Windows/Linux и активного сетевого оборудования;
- Базовые знания сетевых протоколов;
- Администрирование СКДПУ и умение с его помощью реализовывать корпоративную политику безопасности, в части относящейся к информационному обмену;
- Знание и соблюдение требований конфиденциальности (секретности) при проведении работ.

## 2 ОБЩИЕ СВЕДЕНИЯ

СКДПУ предоставляет консоль администратора с «командной строкой» для управления доступом к системе через REST интерфейс, а также для смены паролей доступа.

Для того чтобы войти в консоль, необходимо подключиться к СКДПУ, используя SSH-клиент:

```
$ ssh wabadmin@<ip> -p 2242
# super
Ввести пароль wabsuper
# sudo -s
```

Группа команд, доступных пользователю, зависит от учетной записи пользователя. Пользователи, чьи учетные записи включают в себя консоль администратора, получают право использовать все команды, перечисленные в настоящем документе. Для того чтобы получить список команд, необходимо ввести запрос `help` в консоли.

Справку для каждой команды можно получить, введя запрос `help commande` или `commande -h`.

Также может быть использовано автозаполнение (клавиша `tab`), чтобы вводить команды.

### 2.1 Перечень утилит консоли администрирования СКДПУ

Описание встроенных утилит СКДПУ и их параметров

#### **WABSetLicence**

Управление лицензией СКДПУ

```
WABSetLicence [-h] [-c | -d | -u] [-f FILE]
```

**-h**

вывод справки

**-c**

генерирование контекстного файла для обновления лицензии, используется совместно с **-f**

**-d**

сброс лицензии

**-u**

обновление лицензии из контекстного файла, используется совместно с **-f**

**-f FILE**

флаг добавления файла *FILE* в архив настроек (можно указать несколько файлов)

#### **WABGetLicence**

Вывод информации о текущей лицензии СКДПУ

```
WABGetLicence
```

#### **WABSessionLogExport**

Контроль объема свободной памяти локального хранилища данных

```
WABSessionLogExport [-h] [-p] [-a] [-P] [--show-orphans]
                    [--sessions SESSION [SESSION ...]] [-s DATE]
```

```

[-e DATE] [--limit-age AGE]
[--critical-end-date DATE]
[--critical-limit-age AGE] [-E] [-F SIZE] [-A AGE]
[--prefer-before DATE]
[--local-storage | --remote-storage]
[--protocol PROTOCOL [PROTOCOL ...]]
[--status STATUS [STATUS ...]]
[--critical | --non-critical]
[--target TARGET [TARGET ...]]
[--target-group TARGET_GROUP [TARGET_GROUP ...]]
[--user USER [USER ...]]
[--user-group USER_GROUP [USER_GROUP ...]]
[-w | --good-only]
[--passphrase-fd FILE_DESCRIPTOR | --passphrase-file
FILE | --passphrase PASSPHRASE]

```

**-h**

вывод справки

**-p**

не удалять сессии

**-a**

не создавать архив

**-P**

удаление "висячих сессий"

**--show-orphans**

отображение списка "висячих сессий"

**--passphrase-fd *FILE\_DESCRIPTOR***загрузка пасс-фразы из файла с дескриптором *FILE\_DESCRIPTOR***--passphrase-file *FILE***загрузка пасс-фразы из файла *FILE***--passphrase *PASSPHRASE***

интерактивный ввод пасс-фразы

**--sessions *SESSION [SESSION ...]***

выборка сессий с указанными идентификаторами

**-s *DATE***учитываются сессии, инициированные после даты *DATE* включительно. Допустимый формат: YYYY-MM-DD\_[HH:MM:SS]**-e *DATE***учитываются сессии, инициированные до даты *DATE* включительно. Допустимый формат: YYYY-MM-DD\_[HH:MM:SS]**--limit-age *AGE***учитываются сессии, чей срок хранения превышает количество указанных дней *AGE*. Допустимые суффиксы: для дней - 'd', для месяцев - 'm'**--critical-end-date *DATE***не учитываются критические сессии, инициированные раньше указанной даты *DATE*. Допустимый формат: YYYY-MM-DD\_[HH:MM:SS]**--critical-limit-age *AGE***не учитываются критические сессии, чей срок хранения превышает количество указанных дней *AGE*. Допустимые суффиксы: для дней - 'd', для месяцев - 'm'

**-E**

при совместном использовании с опциями `-s` и `-e` позволяет учитывать завершившиеся сессии вместо инициированных

**-F *SIZE***

учитываются только самые старые сессии, удаление которых было бы достаточно для достижения минимального свободного размера *SIZE* в байтах (должен использоваться совместно с `--local-storage` или `--remote-storage`)

**-A *AGE***

учитываются сессии, чей срок хранения превышает срок хранения превышает количество дней *AGE*. Допустимые суффиксы: для дней - 'd', для месяцев - 'm'

**--prefer-before *DATE***

учитываются сессии, дата инициирования которых предшествует дате *DATE*. Допустимый формат: `YYYY-MM-DD_[HH:MM:SS]`

**--local-storage**

учитываются только сессии, расположенные в локальном хранилище

**--remote-storage**

учитываются только сессии, расположенные в удаленном хранилище

**--protocol *PROTOCOL* [*PROTOCOL ...*]**

учитываются только сессии, у которых указаны протоколы соединения с целевыми устройствами. Игнорируется, если указан параметр `--sessions`

**--status *STATUS* [*STATUS ...*]**

учитываются только сессии, для которых определен один из статусов:

- success
- killed
- restricted
- interrupted
- crashed
- failed

Игнорируется, если указан параметр `--sessions`

**--critical**

учитываются только критические сессии. Игнорируется, если указан параметр `--sessions`

**--non-critical**

учитываются только не критические сессии. Игнорируется, если указан параметр `--sessions`

**--target *TARGET* [*TARGET ...*]**

учитываются только сессии, для которых указаны целевые устройства. Игнорируется, если указан параметр `--sessions`

**--target-group *TARGET\_GROUP* [*TARGET\_GROUP ...*]**

учитываются только сессии, для которых указаны целевые устройства, входящие в указанные группы. Игнорируется, если указан параметр `--sessions`

**--user *USER* [*USER ...*]**

учитываются только сессии, инициированные указанными пользователями. Игнорируется, если указан параметр `--sessions`

**--user-group *USER\_GROUP* [*USER\_GROUP* ...]**

учитываются только сессии, инициированные пользователями, входящими в указанные группы пользователей. Игнорируется, если указан параметр `--sessions`

**-w**

учитываются только сессии, завершившиеся с ошибкой

**--good-only**

учитываются только сессии, завершившиеся без ошибок

**`config-restore.py`**

Восстановление параметров конфигурации из указанной резервной копии

```
config-restore.py [-h] [-S] [-N] [--forcenetwork] -f FILE
```

**-h**

вывод справки

**-f *FILE***

путь к файлу *FILE* резервной копии

**-S**

не происходит восстановление системных настроек

**-N**

не происходит восстановление сетевых настроек и настроек сервера высокой доступности

**--forcenetwork**

использовать `gzip` для сжатия

**`config-backup.py`**

Сохранение резервной копии

```
config-backup.py [-h] [-d DIRECTORY]
```

**-h**

вывод справки

**-d *DIRECTORY***

указание директории *DIRECTORY*, куда будет сохранена резервная копия

## ПЕРЕЧЕНЬ СОКРАЩЕНИЙ

<b>CSV</b>	Comma-Separated Values - текстовый формат, предназначенный для представления табличных данных.
<b>HTTP</b>	HyperText Transfer Protocol (протокол передачи гипертекста)
<b>HTTPS</b>	HyperText Transfer Protocol Secure - расширение протокола HTTP, поддерживающее шифрование.
<b>IP</b>	Internet Protocol (IP, досл. «межсетевой протокол») — маршрутизируемый протокол сетевого уровня стека TCP/IP.
<b>OCR</b>	Optical character recognition - механический или электронный перевод изображений рукописного, машинописного или печатного текста в текстовые данные - последовательность кодов, используемых для представления символов в компьютере (например, в текстовом редакторе).
<b>RDP</b>	Remote Desktop Protocol, протокол удаленного рабочего стола
<b>REST</b>	Representational State Transfer — архитектурный стиль взаимодействия компонентов распределённого приложения в сети. REST представляет собой согласованный набор ограничений, учитываемых при проектировании распределённой гипермедиа-системы.
<b>RFB</b>	Remote FrameBuffer — простой клиент-серверный сетевой протокол прикладного уровня для удалённого доступа к графическому рабочему столу компьютера, используемый в VNC.
<b>RFC</b>	Request for Comments, рабочее предложение – стандарты Интернета в части реализаций.
<b>RLOGIN</b>	Remote LOGIN (удалённый вход в систему)
<b>SCP</b>	Secure Copy Protocol — утилита и протокол копирования файлов между компьютерами, использующий, в отличие от утилиты RCP, в качестве транспорта не RSH, а зашифрованный SSH.
<b>SFTP</b>	SSH File Transfer Protocol — протокол прикладного уровня, предназначенный для копирования и выполнения других операций с файлами поверх надёжного и безопасного соединения.

---

<b>SSH</b>	Secure SHell (безопасная оболочка), протокол защищенной передачи данных
<b>SSO</b>	Single Sign-On — технология, при использовании которой пользователь переходит из одного раздела портала в другой, либо из одной системы в другую, не связанную с первой системой, без повторной аутентификации.
<b>TELNET</b>	TErminaL NETwork - сетевой протокол для реализации текстового интерфейса по сети (при помощи транспорта TCP)
<b>TLS</b>	Transport Layer Security — протокол защиты транспортного уровня
<b>VNC</b>	Virtual Network Computing - система удалённого доступа к рабочему столу компьютера, использующая протокол RFB (англ. Remote FrameBuffer, удалённый кадровый буфер).
<b>APM</b>	Автоматизированное рабочее место
<b>ОС</b>	Операционная система
<b>ПО</b>	Программное обеспечение

---

## **ПЕРЕЧЕНЬ ТАБЛИЦ**

Таблица 1 – Основные возможности СКДПУ.....	3
---	---

