УТВЕРЖДЕНО
BY.PTHK.47001-01 34 02-ЛУ

Комплекс программно-аппаратный «Шлюз BelVPN 4.7»

РУКОВОДСТВО АДМИНИСТРАТОРА СКЗИ

BY.PTHK.47001-01 34 02

Листов 15

2025

Руководство Администратора СКЗИ

1. Назначение

Данный документ описывает функциональные возможности для существующей роли «Администратора СКЗИ» в продукте «Комплекс программно-аппаратный Шлюз BelVPN 4.7». Помимо этого, ниже описаны рекомендации по эксплуатации и важные замечания с точки зрения безопасности, касающиеся соответствия продукта стандартам и нормативно-правовым актам Республики Беларусь.

2. Описание

Роль Администратора СКЗИ необходима для выполнения общих сервисов СКЗИ, в том числе криптографических: генерация ключей, установление защищённого соединения.

В СКЗИ также выделена роль Оператора CLI. Эта роль необходима для выполнения общих сервисов, указанных для предыдущей роли, но посредством интерпретатора команд в консоли (далее – cisco-like console), расширяет предыдущую роль по доступному функционалу.

Роли Администратора и Оператора CLI предлагается возложить на одно физическое лицо (на одного юридического представителя).

Уровень доступа роли Администратор СКЗИ можно описать уровнем доступа связанной с ролью учётной записи «user» в операционной системе S-Terra OS (далее – ОС) ПАК.

Администратор СКЗИ имеет ограниченные права и не имеет возможности их расширить. Администратор СКЗИ имеет возможность копировать файл запроса сертификата в директорию монтирования USB, изменять только разрешённые конфигурационные файлы сервисов. Администратор СКЗИ не имеет возможности устанавливать ПО.

Администратор СКЗИ имеет право:

1. выполнять встроенные (builtin) команды bash;
2. выполнять ограниченный набор команд от своего имени, приведённые в Приложении А;
3. выполнять ограниченный набор команд от привилегированного пользователя (sudo), приведённый в файле /etc/sudoers.d/user-sudoers на ПАК и в Приложении Б.

3. Аутентификация

Администратор СКЗИ может авторизоваться только локально, через отвечающий за это сервис (systemd-logind), со следующими реквизитами «по умолчанию»:

```
Логин: user
Пароль: Cisc_01234
```

После чего система затребует новый пароль:

– минимальная длина составляет 10 символов;

– использовать минимум 1 цифру, 1 строчную букву, 1 прописную букву, 1 спецсимвол.

4. Функции

Функции доступные Администратору, а также общий порядок работы с СКЗИ, изложено ниже:

1. Выполнить вход в систему и выполнить смену пароля в соответствии с политикой.

Примечание: для дальнейшей смены пароля или при желании сгенерировать высокоэнтропийный (стойкий) пароль. Администратор может воспользоваться встроенной в СКЗИ утилитой strong_pass с соответствующими ключами (см. ключ --help).

Генерация psk минимальной длинны:

```
strong_pass -psk
```

Пример вывода:

```
sg7JRAIZqg9CYSnAUTUkjA==
```

Генерация psk заданной длинны:

```
strong_pass --n_psk 20
```

Пример вывода:

```
py2Z4Rym+W1ULsnCfSZs9WKLPlY=
```

2. Произвести инициализацию продукта;

Инициализация продукта происходит путем выполнения соответствующего скрипта после запуска (подсказка по вводу размещены в верхней части экрана, пока продукт не инициализован). В момент инициализации необходимо ввести данные лицензии. Инициализация продукта:

```
/opt/VPNagent/bin/init.sh
```

3. В целях повышения безопасности информации Администратора, в продукте применён метод разделения секрета на части. Основной сервис может корректно и безопасно функционировать только при наличии двух частей, при этом части не должны располагаться на одном физическом носителе информации. В связи с этим, в самом начале, перед выполнением настройки защищённого соединения:

ОБЯЗАТЕЛЬНО: выполнить перенос одной части разделённого секрета на другой носитель информации, например USB flash устройство. Части располагаются по пути `/opt/VPNAgent/bin/.sterra.ps1` *и* `/opt/VPNAgent/bin/.sterra.ps2` . При необходимости произвести работы(обслуживание) КПА, администратор передаёт устройство, изъяв частичные секреты. Подробнее о способе переноса в Приложении В.

4. В зависимости от выбранного типа аутентификации: сгенерировать запроса на получение сертификата открытого ключа (СОК), например системы ГосСУОК. Подробнее изложено в Приложении Г;

5. В зависимости от выбранного типа аутентификации импортировать полученные сертификата открытого ключа (СОК) и список отозванных сертификатов (СОС), например системы ГосСУОК. Подробнее изложено в Приложении Г;

6. В зависимости от выбранного типа аутентификации сгенерировать высокоэнтропийный (стойкий) предварительно распределённый ключ (PSK), запомнить его, внести в конфигурацию всех задействованных СКЗИ;

Примечание: надёжный PSK гарантирует высокую трудность для злоумышленника и может при должном подходе обезопасить данные Администратора. Поэтому для работы СКЗИ по PSK необходимо сгенерировать высокоэнтропийный (стойкий) ключ. Администратор может воспользоваться встроенной в СКЗИ утилитой strong_pass с соответствующими ключами (см. ключ --help).

7. Выполнить настройка сетевых сервисов через утилиты, конфигурационные файлы, сетевые утилиты способом, приведенным в Приложении Д;

8. Сервис логов включен по умолчанию, перезагрузить его можно с помощью команды:

```
sudo vpn_service retart
```

9. Также в СКЗИ доступен просмотр и фильтрация логов;

Пример потокового вывода событий на экран:

```
tail –f /var/log/belvpngate.log
```

Пример ввода фильтра:

```
cat /var/log/belvpngate.log | grep
```

10. Предусмотрена возможность отключения/запуска/автозагрузки сервисов, в том числе и критических. Подробнее в Приложении Е;

11. Работа с утилитами СКЗИ в том числе и инициализация СКЗИ отражена в Приложении Ж;

12. Работа с утилитами мониторинга OS, ядра и аппаратной части (например: lshw, atop, dmesg) приведена в Приложении З.

Приложение А

Утилиты доступные учётной записи «user»

grep – утилита для поиска по строкам, исходя из шаблона;

kill – утилита для отсылки сигналов процессам. Ограничена по политике доступа для учётной записи «user»;

nslookup – утилита для формирования dns-запроса;

passwd – утилита для смена пароля;

ping – утилита для ICMP-запросов;

sudo – утилита для выполнение команд с правами другого пользователя;

traceroute – утилита для трассировки в сети в рамках ICMP/TCP/UDP;

time – утилита для проверки времени выполнения программ или команд;

sort – утилита для сортировки файлов;

less – утилита для постраничного вывода информации;

pgrep – утилита для поиска процессов по имени;

uptime – утилита для вывода информации о работоспособности системы;

sed – утилита для фильтрации файлов.

Приложение Б

Ограничения политики доступа для учётных записей
(содержимое user-sudoers)

При формировании ограничений доступа применена модель белого списка: пользователь не может напрямую запускать произвольные команды от root — только те, что перечислены. Также предоставлены базовые операции администрирования сети и сервисов, просмотр логов без запроса на пароль суперпользователя.

```
Cmnd_Alias BIN_COMMANDS = \
/usr/bin/vtysh, /usr/bin/tcpdump, /usr/bin/iperf, /usr/bin/iperf3, \
/usr/bin/atop, /usr/bin/htop, /usr/bin/netstat, /usr/bin/ss, /usr/bin/sensors, \
/usr/bin/journalctl, /usr/bin/lshw, /usr/bin/lscpu, /usr/bin/lsusb, \
/usr/bin/dmesg, /usr/bin/du, /usr/bin/df, /usr/bin/date, /usr/bin/ipt-save, \
/usr/bin/sync, /usr/bin/about, \
/usr/bin/cleanup, /usr/bin/vpn_service

Cmnd_Alias SBIN_COMMANDS = \
/usr/sbin/hwinfo, /usr/sbin/iptraf, /usr/sbin/iptraf-ng, /usr/sbin/ip, \
/usr/sbin/iptunnel, /usr/sbin/iftop, /usr/sbin/brctl, /usr/sbin/hping3, \
/usr/sbin/ethtool, /usr/sbin/ifconfig, /usr/sbin/iptables, /usr/sbin/ip6tables,
\
/usr/sbin/arping, /usr/sbin/reboot, /usr/sbin/poweroff, /usr/sbin/dhclient, \
/usr/sbin/ifup, /usr/sbin/ifdown, /usr/sbin/route, /usr/sbin/sysctl, \
/usr/sbin/dpkg-reconfigure, /usr/sbin/netsniff-ng, /usr/sbin/flowtop, \
/usr/sbin/ifpps, /usr/sbin/ipvsadm, /usr/sbin/opennhrpctl

user    ALL=(root) NOPASSWD: /usr/bin/systemctl is-enabled *
user    ALL=(root) NOPASSWD: /usr/bin/systemctl status *

user    ALL=(root) NOPASSWD: /usr/bin/systemctl start *, \
! /usr/bin/systemctl start vpngate, ! /usr/bin/systemctl start vpnlog, \
! /usr/bin/systemctl start vpnsvcwd, ! /usr/bin/systemctl start vpndrv
user    ALL=(root) NOPASSWD: /usr/bin/systemctl stop *, \
! /usr/bin/systemctl stop vpngate, ! /usr/bin/systemctl stop vpnlog, \
! /usr/bin/systemctl stop vpnsvcwd, ! /usr/bin/systemctl stop vpndrv, !
/usr/bin/systemctl stop syslog-ng
user    ALL=(root) NOPASSWD: /usr/bin/systemctl restart *, \
! /usr/bin/systemctl restart vpngate, ! /usr/bin/systemctl restart vpnlog, \
! /usr/bin/systemctl restart vpnsvcwd, ! /usr/bin/systemctl restart vpndrv
user    ALL=(root) NOPASSWD: /usr/bin/systemctl disable *, \
! /usr/bin/systemctl disable vpngate, ! /usr/bin/systemctl disable vpnlog, \
! /usr/bin/systemctl disable vpnsvcwd, ! /usr/bin/systemctl disable vpndrv, !
/usr/bin/systemctl stop syslog-ng
user    ALL=(root) NOPASSWD: /usr/bin/systemctl enable *, \
! /usr/bin/systemctl enable vpngate, ! /usr/bin/systemctl enable vpnlog, \
! /usr/bin/systemctl enable vpnsvcwd, ! /usr/bin/systemctl enable vpndrv

user    ALL=(root) NOPASSWD: BIN_COMMANDS
user    ALL=(root) NOPASSWD: SBIN_COMMANDS
user    ALL=(root) NOPASSWD: /opt/VPNagent/bin/*
user    ALL=(root) NOPASSWD: /usr/local/bin/klish
```

```
user    ALL=(root) NOPASSWD: /usr/local/bin/umount-usb

user    ALL=(root) NOPASSWD: /usr/bin/sudoedit /etc/ifaliases.cf
user    ALL=(root) NOPASSWD: /usr/bin/sudoedit /opt/VPNagent/bin/ps_folders.txt
user    ALL=(root) NOPASSWD: /usr/bin/sudoedit /etc/network/interfaces
user    ALL=(root) NOPASSWD: /usr/bin/sudoedit /etc/network/if-.d/
user    ALL=(root) NOPASSWD: /usr/bin/sudoedit /etc/hosts
user    ALL=(root) NOPASSWD: /usr/bin/sudoedit /etc/sysctl.conf
user    ALL=(root) NOPASSWD: /usr/bin/sudoedit /etc/hostname
user    ALL=(root) NOPASSWD: /usr/bin/sudoedit /etc/keepalived/*
user    ALL=(root) NOPASSWD: /usr/bin/sudoedit /etc/syslog-ng/*
user    ALL=(root) NOPASSWD: /usr/bin/sudoedit /etc/frr/*
user    ALL=(root) NOPASSWD: /usr/bin/sudoedit /etc/chrony/*
user    ALL=(root) NOPASSWD: /usr/bin/sudoedit /etc/snmp/*
user    ALL=(root) NOPASSWD: /usr/bin/sudoedit /etc/dhcp/*

user    ALL=(root) NOPASSWD: /usr/bin/sudoedit /etc/default/isc-dhcp-server
user    ALL=(root) NOPASSWD: /usr/bin/sudoedit /etc/modules
user    ALL=(root) NOPASSWD: /usr/bin/sudoedit /etc/resolv.conf
user    ALL=(root) NOPASSWD: /usr/bin/sudoedit /etc/modprobe.d/blacklist.conf

user    ALL=(root) NOPASSWD: /usr/bin/grep * /var/log/*
user    ALL=(root) NOPASSWD: /usr/bin/cat  * /var/log/*
user    ALL=(root) NOPASSWD: /usr/bin/tail * /var/log/*

user    ALL=(root) NOPASSWD: /usr/bin/cp * usbdev/*
user    ALL=(root) NOPASSWD: /usr/bin/cp * /home/user/usbdev/*
user    ALL=(root) NOPASSWD: /usr/bin/cp /opt/VPNagent/bin/.sterra.ps* usbdev/*
user    ALL=(root) NOPASSWD: /usr/bin/cp /opt/VPNagent/bin/.sterra.ps*
/home/user/usbdev/*
user    ALL=(root) NOPASSWD: /usr/bin/mv ^/opt/VPNagent/bin/.sterra.ps1
usbdev/([^.]|.[^.])+$
user    ALL=(root) NOPASSWD: /usr/bin/mv ^/opt/VPNagent/bin/.sterra.ps1
/home/user/usbdev/([^.]|.[^.])+$
user    ALL=(root) NOPASSWD: /usr/bin/mv ^/opt/VPNagent/bin/.sterra.ps2
usbdev/([^.]|.[^.])+$
user    ALL=(root) NOPASSWD: /usr/bin/mv ^/opt/VPNagent/bin/.sterra.ps2
/home/user/usbdev/([^.]|.[^.])+$

user    ALL=(root) NOPASSWD: /usr/bin/ln -s /home/user/usbdev/*
/opt/VPNagent/bin/.sterra.ps*

user    ALL=(root) NOPASSWD: /usr/bin/mkdir usbdev/*
user    ALL=(root) NOPASSWD: /usr/bin/mkdir /home/user/usbdev/*

user     ALL=(root) NOPASSWD: /usr/bin/rm ^/var/belvpn/containers/([^.]|.[^.])+$
user    ALL=(root) NOPASSWD: /usr/bin/rm /opt/VPNagent/bin/.sterra.ps1
user    ALL=(root) NOPASSWD: /usr/bin/rm /opt/VPNagent/bin/.sterra.ps2
user    ALL=(root) NOPASSWD: /usr/bin/rm
^/opt/VPNagent/bin/db/crls/([^.]|.[^.])+$
```

Приложение В

Описание способа переноса частей разделённого секрета

Инструкция по осуществлению переноса одной из частей секрета sterra.ps на внешний к СКЗИ USB-носитель:

1. Вставить USB-носитель в устройство;
2. Убедиться в автоматическом создании в СКЗИ отдельной директории в /home/user/usbdev/;
3. Перенести один из частей секрета в эту директорию командой:

sudo mv /opt/VPNagent/bin/.sterra.ps1 usbdev/<дир. для USB>/

4. Создать символическую ссылку на этот путь командой:

sudo ln -s /home/user/usbdev/<дир. для USB>/.sterra.ps1 /opt/VPNagent/bin/.sterra.ps1

5. Проверить работоспособность сервисов после перезагрузки:

sudo vpn_service restart

Описание способа переноса частей разделённого секрета для передачи ПАК производителю

Инструкция по осуществлению переноса частей секрета sterra.ps на внешний к СКЗИ USB-носитель:

1. Вставить USB-носитель в устройство;
2. Убедиться в автоматическом создании в СКЗИ отдельной директории в /home/user/usbdev/;
3. Перенести части секрета в эту директорию командой:

sudo mv /opt/VPNagent/bin/.sterra.ps2 usbdev/<дир. для USB>/

4. Проверить неработоспособность сервисов после перезагрузки:

sudo vpn_service restart

5. Передать устройство;
6. Получить устройство;
7. Вставить USB-носитель в устройство;
8. Убедиться в автоматическом создании в СКЗИ отдельной директории в /home/user/usbdev/;
9. Перенести части секрета из этой директории командой:

sudo mv usbdev/<дир. для USB>/ /opt/VPNagent/bin/.sterra.ps2

10. Проверить неработоспособность сервисов после перезагрузки:

sudo vpn_service restart

Приложение Г

Работа с инфраструктурой открытых ключей (PKI)

Важные задачи с PKI:

1. Генерация запроса на СОК:

sudo cert_mgr create -subj "CN=gate21,SN=andr,NQ=YU,GN=YU,S=12,C=BY,L=Minsk,ST=Minsk,O=Sterra,OU=TEST,T=title, OID=1" -kc gate21 -f /opt/certs/dntest.req

2. Импорт личного СОК в базу СКЗИ:

В случае расширения .cer:

sudo cert_mgr import -f <путь к файлу сертификата> -kc <имя контейнера> -kcp <пароль контейнера>

В случае расширения .p7b:

sudo cert_mgr import -f <путь к файлу сертификата> -i < id личного сертификата> -kc <имя контейнера> -kcp <пароль контейнера>

2.1 Импорт доверенного СОК в базу СКЗИ:

Для корректной работы необходимо выполнить импорт всей цепочки доверенных УЦ (Корневого (КУЦ) и Республиканского (РУЦ), при их наличии).

При импорте сертификата РУЦ в случае расширения .cer:

sudo cert_mgr import -f <путь к файлу сертификата>

При импорте сертификата РУЦ в случае расширения .p7b:

sudo cert_mgr import -f <путь к файлу сертификата> -i <id сертификата УЦ>

При импорте сертификата КУЦ в случае расширения .cer:

sudo cert_mgr import -f <путь к файлу сертификата> -t

При импорте сертификата КУЦ в случае расширения .p7b:

sudo cert_mgr import -f <путь к файлу сертификата> -i <id сертификата УЦ> -t

3. Импорт СОС в базу СКЗИ:

sudo cert_mgr import -f (путь к файлу .p7b) -i <id списка отозванных сертификатов в архиве>

Примечание: списки отозванных сертификатов действительны примерно 30 дней. Необходимо следить за их актуальностью и вовремя обновлять.

Опционально:

4. Показать базу сертификатов СКЗИ:

Полностью:

sudo cert_mgr show

Конкретный объект:

sudo cert_mgr show -i < id объекта в базе>

5. Удалить СОК из базы СКЗИ:

sudo cert_mgr remove -i < id объекта в базе>

6. Удалить СОС из базы СКЗИ

*sudo rm /opt/VPNagent/bin/db/crls/**

7. Проверить состояние СОК в базе СКЗИ:
Полностью:

sudo cert_mgr check

Конкретный объект:

sudo cert_mgr check -i < id СОК>

Приложение Д

Работа с сетевыми сервисами

vtysh – утилита для конфигурации frr;

tcpdump / netsniff-ng – сниффер;

iperf[3] / iptraf-ng / hping3 – утилита для генерации трафика / отладки различных протоколов;

ip – утилита для настройки сетевых интерфейсов / маршрутов / мостов;

iptunnel – утилита для настройки ip-туннелей;

brctl – утилита для настройки сетевых мостов;

ethtool / *ifconfig* – утилита для настройки параметров сетевых интерфейсов;

ip[6]tables – утилита для работы с netfilter;

arping – утилита для работы с ARP;

dhclient – утилита для отправки DHCP запрос;

ifup – включить интерфейс;

ifdown – выключить интерфейс;

route – утилита для работы со статической маршрутизацией;

ifpps – утилита для сбора сетевой статистики;

ipvsadm – утилита для настройки Virtual Server;

opennhrpctl – утилита для настройки NHRP.

Приложение Е
Работа с сервисами ОС

Команды, которые запускают и останавливают критические сервисы СКЗИ и требуют дополнительного подтверждения прав перед выполнением:

/bin/cleanup – очистка критических объектов в рамках СКЗИ;

/bin/vpn_service – работа с подтверждением с критическими сервисами СКЗИ.

Пример: *sudo vpn_service restart*

Для работы с сервисами используется утилита systemctl, а учётная запись «user» может выполнять её только через sudo.

Доступны следующие команды:

is-enabled – проверка состояния сервиса: будет ли он автоматически запускаться при старте ОС (автозагрузка);

status – проверка текущего состояния сервиса;

start – запуск сервиса;

stop – останова сервиса;

restart – перезапуск сервиса;

enable – добавление сервиса в автозагрузку;

disable – исключения сервиса из автозагрузки.

Администратору СКЗИ **запрещено** использовать команды *stop/restart* в контексте сервисов СКЗИ(таких как vpngate, vpnlog, vpndrv).

Приложение Ж
Утилиты СКЗИ

cert_mgr – утилита для работы с СОК/СОС и создание запросов на СОК;

belvpn_verify – утилита для проверки целостности СКЗИ;

cs_console – утилита для перехода в режим конфигурирования СКЗИ в рамках роли Администратор СКЗИ. После входа необходимо зайти в привилегированный режим и ввести пароль;

dp_mgr – утилита управление политикой работой с трафиком по умолчанию;

drv_mgr – утилита работы с VPN-драйвером;

init.sh – скрипт инициализации СКЗИ;

integr_mgr – утилита для высчитывания / проверки хэша файла;

key_mgr – утилита для работы с pre-shared key;

klogview – сниффер в рамках VPN-драйвера;

lic_mgr – утилита для работы с лицензией СКЗИ;

log_mgr – утилита для настройки логирования СКЗИ;

lsp_mgr – утилита для работы с LSP-конфигурацией СКЗИ. LSP-конфигурация (local security policy) — это конечная конфигурация, которую понимает драйвер и работает с ней.

reset_product_settings.sh – скрипт для обновления настроек СКЗИ в соответствии с лицензией;

sa_mgr – утилита для работы с SA (security association);

stverify – утилита для проверки подписи в рамках СКЗИ (содержит открытый ключ производителя);

ver_show – утилита для вывода версии продукта.

st_digest – утилита вычисляет хэш файлов на основании белорусских алгоритмов(belt).

strong_pass – утилита для генерации пароля с заданной длинной символов.

Приложение 3

Утилиты мониторинга

htop / atop – real-time вывод состояния процессора, оперативной памяти;

netstat / ss – вывод о состоянии сокетов;

sensors – вывод о состоянии датчиков;

journalctl – systemd-утилита для работа с логами и состоянием сервисов ОС;

lshw / hwifno – вывод информации об аппаратной части;

lscpu – вывод информации о процессоре;

lsusb – вывод информации о USB;

dmesg – вывод информации из ядра;

du – вывод информации о директориях;

df – вывод информации о файловых системах;

date – установка и вывод даты и времени;

iftop – real-time вывод о состоянии сетевого трафика и интерфейсов;

Лист регистрации изменений									
	Номера листов (страниц)				Всего листов (страниц) в докум.	№ документа	Входящий № сопроводительного докум. и дата	Подп.	Дата
Изм.	измененных	замененных	новых	аннулированных					