Установка ключей Astra Digsig

```
sudo apt install astra-digsig-oldkeys -y
sudo mkdir -p /etc/digsig/keys/legacy/kaspersky
sudo cp -v kaspersky_astra_pub_key.gpg /etc/digsig/keys/legacy/kaspersky
sudo update-initramfs -u -k all
sudo reboot
```

Установка и настройка PostgreSQL

```
sudo apt install postgresql-14 -y
sudo sed -i 's/^.*shared_buffers =.*/shared_buffers = 1024MB/g'
/etc/postgresql/14/main/postgresql.conf
sudo sed -i 's/^.*max_stack_depth =.*/max_stack_depth = 7MB/g'
/etc/postgresql/14/main/postgresql.conf
sudo sed -i 's/^.*work_mem =.*/work_mem = 16MB/g'
/etc/postgresql/14/main/postgresql.conf
sudo sed -i 's/^.*max_connections =.*/max_connections = 151/g'
/etc/postgresql/14/main/postgresql.conf
sudo sed -i 's/^.*max_parallel_workers_per_gather
=.*/max_parallel_workers_per_gather = 0/g'
/etc/postgresql/14/main/postgresql.conf
sudo sed -i 's/^.*maintenance_work_mem =.*/maintenance_work_mem = 128MB/g'
/etc/postgresql/14/main/postgresql.conf
sudo systemctl restart postgresql
sudo usermod -a -G shadow postgres
sudo setfacl -d -m u:postgres:r /etc/parsec/macdb
sudo setfacl -R -m u:postgres:r /etc/parsec/macdb
sudo setfacl -m u:postgres:rx /etc/parsec/macdb
sudo setfacl -d -m u:postgres:r /etc/parsec/capdb
sudo setfacl -R -m u:postgres:r /etc/parsec/capdb
sudo setfacl -m u:postgres:rx /etc/parsec/capdb
```

Создание системного пользователя и группы

```
sudo adduser --system --shell /sbin/nologin --disabled-password --disabled-
login --no-create-home ksc
sudo groupadd kladmins
sudo gpasswd -a ksc kladmins
sudo usermod -g kladmins ksc
```

Настройка базы данных для ksc

```
sudo pdpl-user -l 0:0 ksc
sudo -u postgres psql -c "CREATE USER \"ksc\" WITH PASSWORD 'strongpass'
CREATEDB;"
```

```
sudo -u postgres psql -c "CREATE DATABASE \"kav\" ENCODING 'UTF8' OWNER
\"ksc\";"
sudo -u postgres psql -c "GRANT ALL PRIVILEGES ON DATABASE \"kav\" TO
\"ksc\";"
sudo -u postgres psql -c "GRANT ALL PRIVILEGES ON ALL TABLES IN SCHEMA
\"public\" TO \"ksc\";"
sudo -u postgres psql -c "GRANT ALL PRIVILEGES ON ALL SEQUENCES IN SCHEMA
\"public\" TO \"ksc\";"
```

Настройка сервисов Kaspersky (if ALSE 1.8+ installed)

```
sudo mkdir -pv /etc/systemd/system/kladminserver_srv.service.d
sudo tee /etc/systemd/system/kladminserver_srv.service.d/override.conf <<
EOF
[Service]
User=
User=ksc
CapabilitiesParsec=PARSEC_CAP_PRIV_SOCK
ExecStart=
ExecStart=/opt/kaspersky/ksc64/sbin/klserver -d from_wd
Create a directory /etc/systemd/system/klwebsrv_srv.service.d and create a
file named override.conf with the following content:
EOF

sudo mkdir -pv /etc/systemd/system/klwebsrv_srv.service.d
sudo tee /etc/systemd/system/klwebsrv_srv.service.d/override.conf << EOF
[Service]
User=
User=ksc
CapabilitiesParsec=PARSEC_CAP_PRIV_SOCK
ExecStart=
ExecStart=/opt/kaspersky/ksc64/sbin/klcsweb -d from_wd
EOF
```

Подготовка ответов для установки KSC

```
tee /tmp/ksc_install/answers.txt << EOF
EULA_ACCEPTED=1
PP_ACCEPTED=1
KLSRV_UNATT_SERVERADDRESS=adm-infra.digrub.local
KLSRV_UNATT_DBMS_INSTANCE=localhost
KLSRV_UNATT_DBMS_PORT=5432
KLSRV_UNATT_DB_NAME=kav
KLSRV_UNATT_DBMS_LOGIN=ksc
KLSRV_UNATT_DBMS_PASSWORD=strongpass
KLSRV_UNATT_KLADMINSGROUP=kladmins
KLSRV_UNATT_KLSRVUSER=ksc
KLSRV_UNATT_KLSVCUSER=ksc
```

```
EOF
export KLAUTOANSWERS=/tmp/ksc_install/answers.txt
sudo -E apt install ./ksc64_15.0.0-12912_amd64.deb -y
```

Завершающие шаги установки

```
/opt/kaspersky/ksc64/sbin/kladduser -n ksc -p P@ssw0rd
sudo /opt/kaspersky/ksc64/lib/bin/setup/postinstall.pl
```

После выполнения скрипта установки вам будет предложено настроить Administration Server. Пример интерактивного ввода:

```
Choose the Administration Server installation mode:
1) Standard
Enter Administration Server DNS-name or static IP-address:
ipa.virt.int
Enter Administration Server SSL port number [13000]:
Define the approximate number of devices that you intend to manage:
1) 1 to 100 networked devices
Enter the security group name for services:
kladmins
Enter the account name to start the Administration Server service. The
account must be a member of the entered security group:
kscadmin
Enter the account name to start other services. The account must be a member
of the entered security group:
kscadmin
Choose the database type to connect to:
1) MySQL
2) Postgres
Enter the range number (1 or 2):
2
Enter the database address:
localhost
Enter the database port:
5432
Enter the database name:
kav
```

Настройка Web-консоли

```
sudo tee /etc/ksc-web-console-setup.json << EOF
{
 "address": "127.0.0.1",
 "port": 1443,
 "trusted":
"127.0.0.1|13299|/var/opt/kaspersky/klnagent_srv/1093/cert/klserver.cer|KSC
Server",
```

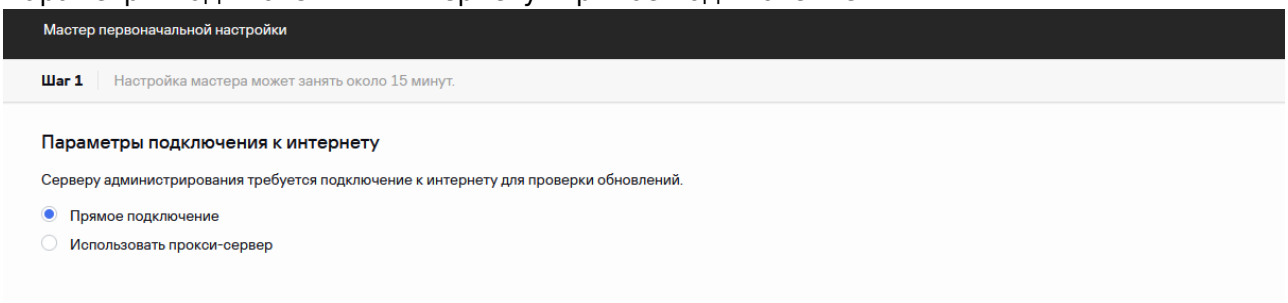
```
 "acceptEula": true
}
EOF

sudo apt install
/media/cdrom/KSC15\(15.0.0.12912+14.2.0.26967\)_643.46856491.00069-10/15.0.0
.12912\ \(Linux\)/Web\ console/ksc-web-console-15.0.136.x86_64.deb
```

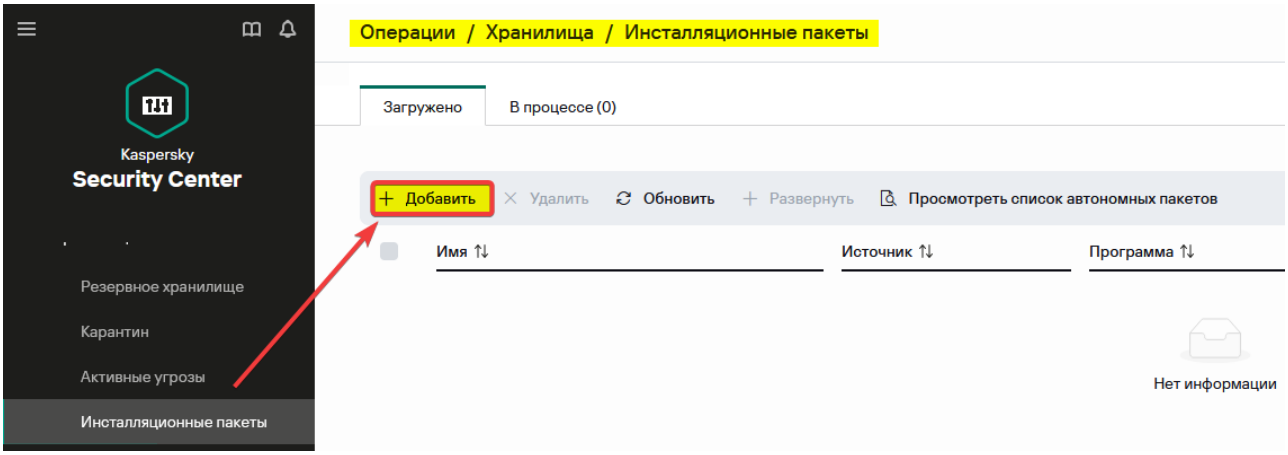
Следуя данной инструкции, вы выполните установку и настройку всех необходимых компонентов для работы Kaspersky Security Center в вашей системе.

Первоначальная настройка через Web-консоль

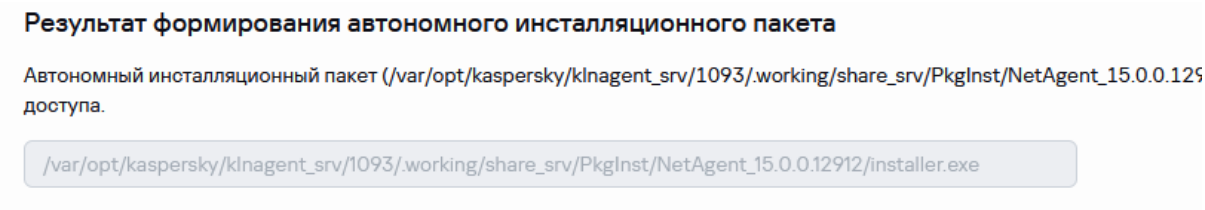
- Выполнить вход в веб-консоль https://adm-infra.digrub.local:1433
- Переключить консоль на русский язык: Settings → Language → Русский → Save
- Запустить мастер первоначальной настройки: KSC Settings → Общие → Запустить мастер первоначальной настройки
- Параметры подключения к интернету: Прямое подключение



- Дождаться загрузки требуемых обновлений (если отсутствует подключение к сети интернет, то будет выведено соответствующее сообщение)
- Защищаемые активы:
  - Защищаемые области:
    - Рабочие станции
  - Операционные системы:
    - Windows
    - Linux
  - Шифрование: Lite encryption (AES56)
  - Пропустить добавление пакетов из интернет репозитория (пакеты будут установлены вручную)
  - Kaspersky Security Network (KSN): Не принимать.
  - Создать задачи администрирования.
  - Если нет данных о почтовом сервере, то в меню «Использовать TLS» выбрать пункт «Не использовать TLS»
- Добавить Инсталляционные пакеты: Операции → Хранилища → Инсталляционные пакеты → Добавить



    - Выбор типа инсталляционного пакета: Создать инсталляционный пакет из файла
        - kesl-12.0.0.6672.zip
        - keswin_12.3.0.493_ru_aes56.zip
        - klnagent-x86_64-15.0.0.12912-deb_ru.tar.gz
        - klnagent-15.0.0.12912-win_ru.zip
    - Подготовить автономные инсталляционные пакеты для Агентов администрирования



        - Операции → Хранилища → Инсталляционные пакеты → Развернуть
        - С использованием автономного инсталляционного пакета
- Иерархия групп → Добавить
    - KO
    - KK
    - ADM
- Добавить плагины управления: Параметры → Веб-плагины → Добавить из файла (zip-архивы предварительно распаковать)
    - kes_linux_12_0_local_12.0.0.754.zip
    - keswin_web_plugin_12.3.0.493.zip
- Добавить задачи для KES (Linux + Windows)
    - Обновление
        - Группа: Управляемые устройства
        - Запуск по расписанию: Ежедневно
    - Проверка целостности системы
        - Запуск по расписанию: Ежедневно (Запускать пропущенные задачи)
    - Поиск вредоносного ПО
        - Запуск по расписанию: Ежедневно (Запускать пропущенные задачи)
- Создать политики KES (Linux + Windows)
    - Для Windows включить проверку съемных дисков при подключении.
        - Запретить остановку задачи проверки.
        - Подробная проверка

From:
https://wiki.virtlab.space/ -

Permanent link:
https://wiki.virtlab.space/russianway:test

Last update: **2025/03/09 22:20**