

Инструкция по настройке рабочего места Linux RedOS

(применимы для моноблоков iCL Si101.Mi и Ред ОС 7.3 тип лицензии - пользовательская)

СОДЕРЖАНИЕ

ОСНОВНЫЕ ОБОЗНАЧЕНИЯ	5
I. УСТАНОВКА И НАСТРОЙКА ОС.....	5
1. Установка ОС.....	5
2. Проверяем права на директорию и обновляем систему.	6
3. Монтируем второй диск	6
4. Задаём права доступа для групп wheel	8
5. Вводим компьютер в домен	8
6. Наделяем группу <i>Администраторы домена</i> полномочиями sudo	9
7. Подключение по протоколу VNC	9
8. Добавляем сетевые папки пользователя домена	11
9. Подключение по протоколу SSH	11
II. УСТАНОВКА И НАСТРОЙКА ПРОГРАММ	12
10. Установка программ, не входящих в официальный репозиторий Ред ОС	12
11. Установка чата Spark	12
12. <i>Установка и настройка VipNet Client</i>	13
13. Установка Kaspersky Endpoint Security и Агент администрирования	14
16. Установка Консультант Плюс	16
17. Установка Yandex Browser	18
18. Установка браузера Opera	18
19. Установка браузера Google Chrome	19
20. Обновление браузера Chromium	19

21.	Установка 1С клиента .	19
22.	Установка Lotus Notes .	20
23.	Установка и настройка КриптоПро CSP .	21
24.	Установка расширений плагинов и расширений для браузеров.	21
25.	Установка DWGViewer .	22
26.	Установка программы для распознавания текста.	22
27.	Установка Календаря	23
28.	Запись ISO-образов	23
29.	Установка программ для диагностики компьютера и системы	23
III.	ПРОЧИЕ НАСТРОЙКИ	23
30.	Закрываем возможность создавать и записывать файлы на рабочий стол (необязательная настройка).	23
31.	Включаем Line-Out выход для наушников	24
32.	Установка принтера\МФУ.	25
33.	Установка сканера.	26
34.	Установка панели программ в стиле MacOS (необязательная настройка)	26
35.	Производим резервное копирование системы на диск Disk2	27
36.	Удаляем группу Пользователи домена из файла /etc/sudoers	27
IV.	ДОПОЛНИТЕЛЬНЫЕ ИНСТРУКЦИИ	28
37.	Проверка состояния жёсткого диска	28
38.	Использование памяти диска	28
39.	Мониторинг температуры процессора.	28
40.	Информация о процессоре.	28
41.	Информация об оперативной памяти.	29
42.	Информация о системе.	29

43.	Мониторинг работы системы	29
44.	Журналирование.....	30
V.	РЕШЕНИЕ ПРОБЛЕМ	31
45.	Если затрясло экран	31
46.	Если отвалилась панель инструментов	31
47.	Если не выполняются команды dnf update и dnf upgrade	31
48.	Убрать иконку пользователя при запуске системы	31
49.	Установка wine из исходников	32

ОСНОВНЫЕ ОБОЗНАЧЕНИЯ

текст в терминале

#комментарии или действия, выполняемые в граф. интерфейсе. Жирным выделена **важная информация**

текст в файле

дополнительная информация

I. УСТАНОВКА И НАСТРОЙКА ОС

1. Установка ОС

1.1 Записываем ISO-образ на флешку

#если где-то уже установлен Linux, советую воспользоваться **п.38**, если нет, пишем в Windows.

#Заходим в Soft/UltraISO и устанавливаем себе на компьютер.

#вставляем флешку, запускаем программу: *Самозагрузка -> Записать образ жесткого диска -> указываем флешку -> указываем ISO-образ -> Форматировать -> Записать*

#если возникли проблемы, воспользуйтесь [п.28](#).

1.2 Загружаемся со съёмного носителя.

#Выбираем **Установить RED OS**.

1.3 Дата/время

#Екатеринбург, 24-часа

1.4 Клавиатура

#Ставим приоритет английскому языку

1.5 Место установки

#выбираем SSD-диск, он должен идти **первым** по списку. Если это не так, снимаем крышку моноблока и перетыкаем SATA-кабель, давая приоритет **SSD**.
#Создать разделы автоматически.

1.6 Выбор программ

#Рабочая станция с граф окружением **MATE**. Дополнительное ПО: выбираем всё.

1.7 Сеть и имя узла

#Настроить-IPv4 -> Вручную-задаём статический IP. Не забываем указать DNS через запятую без пробелов. Требуется адресация IPv4 для этого соединения. Сохранить

1.8 Пароль ROOT

«суперсложный_пароль».

1.9 Создание пользователя

#Полное имя: **Администратор**. Имя пользователя: **LocalAdmin**. Сделать этого пользователя администратором. Требуется пароль. «среднесложный_пароль»

#Начать установку

#Перезапуск системы

1.10 Лицензия

согласен, готово, завершить

2. Проверяем права на директорию и обновляем систему.

#логинимся в систему

#открываем терминал (Ctrl+Alt+T) и вводим команду:

cd /home/LocalAdmin/.config/dconf/

ls -la

#должно быть примерно так:

drwx-----. 2 LocalAdmin LocalAdmin 4096 фев 19 09:06 .

drwx-----. 10 LocalAdmin LocalAdmin 4096 фев 19 08:51 ..

-rw-r--r--. 1 LocalAdmin LocalAdmin 16966 фев 19 09:06 user

#если нет, вводим:

sudo chown LocalAdmin user

#скачиваем с сервера более свежие версии пакетов

sudo dnf -y update && sudo dnf -y upgrade

3. Монтируем второй диск

#у моноблоков это *HDD* с именем **sdb** в папку **/mnt**.

#для начала посмотрите на разделы дисков, это можно сделать несколькими способами.

#эти команды покажут разделы дисков с указанием таблицы разделов и файловой системы

sudo fdisk -l

sudo parted -l sudo lsblk

#эта команда покажет разделы дисков в блочном формате с указанием фирмы производителя

#устанавливаем и запускаем

sudo dnf -y install lsscsi

sudo lsscsi

#должно быть что-то подобное:

[0:0:0:0] disk ATA KINGSTON SKC6002 0102 /dev/sda

[1:0:0:0] disk ATA ST1000LM048-2E71 0001 /dev/sdb

#если не так, значит вы установили систему на HDD. Возвращаемся к п.5.

#открываем терминал и вводим поочерёдно команды:

#создаём таблицу разделов в формате **gpt**

sudo parted /dev/sdb mktable gpt

#создаём раздел диска **sdb**, который будет называться **sdb1** с файловой системой **ext4** и отводим ему 100% места на диске

sudo parted /dev/sdb mkpart primary ext4 0% 100%

#форматируем созданный раздел

sudo mkfs.ext4 /dev/sdb1

#заходим в корневой каталог директории монтирования

cd /mnt/

#создаём в нём директорию **Disk2**, в которую смонтируем наш HDD

sudo mkdir Disk2

#выходим из корневого каталога пользователей

cd

#открываем текстовым редактором **Vim**, файл с настройками автомонтирования. **i** – редактировать, **Esc** – закончить редактировать, **:wq!** или **ZZ** – сохранить и выйти

sudo vim /etc/fstab

#прописываем в самом конце файла, следующий текст, соблюдая табуляцию столбцов:

/dev/sdb1	/mnt/Disk2	ext4	defaults	1 2
------------------	-------------------	-------------	-----------------	------------

#что монтируем	#куда монтируем	#формат файловой системы	#Опции	#очередь
----------------	-----------------	--------------------------------	--------	----------

#перезагружаемся

reboot

4. Задаём права доступа для групп **wheel**.

#эта группа уже создана по умолчанию в RedOS. Но желательно в этом убедиться.

#открываем терминал и вводим поочерёдно команды:

#смотрим какие группы есть в системе.

cat /etc/group

#посмотреть в каких группах состоит админ

groups LocalAdmin

#локальный админ **LocalAdmin** должен состоять в группах: **LocalAdmin** и **wheel**.

#если нет, выполняем:

su -

usermod -aG wheel LocalAdmin

exit

#удалить пользователя из группы можно так:

su -

gpasswd -d пользователь группа

exit

#задаём директории Disk2 в которую примонтирован **HDD** доступ на чтение/запись/выполнение для всех:

sudo chmod 777 /mnt/Disk2/

#можно зайти в директорию **Disk2**, создать там файл и убедиться, что всё работает.

#создаём символическую ссылку диска на рабочем столе пользователя:

sudo ln -s /mnt/Disk2 ~/Рабочий\ стол/

#это аналог ярлыка в Windows

5. Вводим компьютер в домен

#открываем терминал и вводим команду:

#установка из репозитория программы

sudo dnf -y install join-to-domain

#ввод компьютера в домен

#Заходим: *Системные -> Ввод ПК в домен*

#Заполняем строки: **Имя домена**, **Имя компьютера**, **Имя администратора** домена и **Пароль** администратора домена. Жмём Да.

#Вылезет окошко «Компьютер успешно введен в домен»

#проверяем доступность домена

realm list

#проверяем новое имя компьютера

hostname

#Если имя осталось прежним, меняем имя компьютера принудительно:

sudo hostnamectl set-hostname ИМЯ_КОМПЬЮТЕРА

6. Наделяем группу *Администраторы домена* полномочиями **sudo**.

#логинимся под root

su -

#заходим в редактор настроек root. Сам файл находится тут: /etc/sudoers i – редактировать, Esc – закончить редактировать, :wq! – сохранить и выйти

visudo

#ищем строчку:

Allows people in group wheel to run all commands

%wheel ALL=(ALL) ALL

#и прописываем под ней дополнительную строку:

%Администраторы\ домена ALL=(ALL) ALL

#теперь все члены группы Администраторы домена могут выполнять команды от привилегии sudo.

#если производите настройку пользователю домена, то под строкой %Администраторы\ домена укажите следующее:

%Пользователи\ домена ALL=(ALL) ALL

#переводим раскладку на английский, если ещё не перевели. Esc – закончить редактировать.

:wq!

#выход из root

exit

#Чтобы вводить в терминале команды от локального администратора, находясь под обычным пользователем, нужно набрать:

su LocalAdmin

#или ваша учётка, если вы администратор домена

#Перезагружается

reboot

#Заходим -> выбираем «Нет в списке?» и вводим поочерёдно Имя пользователя домена и Пароль учётной записи, под которой вы собираетесь залогиниться.

smetaninpv

#например, у вас своё имя

#так же можно добавить ярлык Disk2 на рабочий стол

sudo ln -s /mnt/Disk2 /home/пользователь@компьютер/Рабочий\ стол/

7. Подключение по протоколу **VNC**.

#все манипуляции проделываем от root

su -
#устанавливаем пакет программы удалённого доступа x11vnc
dnf -y install x11vnc
#Задаём пароль
x11vnc -storepasswd "пароль" /etc/vncpasswd
#закрываем права на редактирование файла с паролем
chmod 544 /etc/vncpasswd
#заходим в сервисную директорию и редактируем файл для автозапуска сервиса x11vnc.service
vim /lib/systemd/system/x11vnc.service
#Заполняем файл следующим содержимым:
#Через запятую, без пробелов введите **ip-адреса**, которые будут подключаться к настраиваемой машине по протоколу VNC (пример: **192.168.1.15,192.168.1.26**)
[Unit]
Description=x11vnc server for GDM
After=display-manager.service
[Service]
ExecStart=/usr/bin/x11vnc -allow **ip_адреса** -many -shared -forever -nomodtweak -capslock -display :0 -auth guess -noxdamage -rfbauth /etc/vncpasswd
Restart=on-failure
RestartSec=3
[Install]
WantedBy=graphical.target
#даём файлу **x11vnc.service** права на выполнение
chmod ugo+x /lib/systemd/system/x11vnc.service
#Перезагружаем демона
systemctl daemon-reload
#Добавляем службу в автозагрузку и запускаем её
systemctl enable x11vnc.service
systemctl start x11vnc.service
#Запускаем службу и проверяем статус, должен быть «active (running)»
systemctl status x11vnc.service
#выходим из-под root
exit
#Далее устанавливаем на вашей Windows-машине клиент VNC (примеры клиентов:) и прописываем в строке поиска **ip-адрес:5900**.
#Вводим **пароль**, ставим галочку сохранить и проверяем подключение.
#Удалённый доступ будет работать только после авторизации пользователя

8. Добавляем сетевые папки пользователя домена

#Домашняя папка -> Файл -> Соединиться с сервером -> заполняем следующие строки: тип **Ресурс Windows**, сервер **ip-адрес сервера**, папка (например, /**Obmen**), **Имя домена**, **Имя пользователя** которому подключаете диск, его **Пароль** -> ставим галочки: запомнить этот пароль, добавить закладку. **Имя закладки** называем интуитивно понятно: **Обмен**.

#создаём ярлыки на рабочем столе для более удобного входа

#правой кнопкой на рабочий стол -> Создать кнопку запуска -> указываем Тип: **Местоположение**, Имя: **Обмен**, расположение указываем с именем домена и пользователя, для быстрой аутентификации.

#Ниже приведены примеры:

smb://Обмен; имя_пользователя@ip-адрес_сервера_обмена

#логотип для сетевого диска выбираем: **mate-disk-usage-analyzer.png** -> Ок.

#скрываем ярлыки примонтированных дисков с рабочего стола

#устанавливаем программу редактирования рабочего стола

sudo dnf -y install dconf-editor dconf-devel

#Системные -> Редактор dconf -> далее org -> mate -> caja -> desktop -> заходим в **volumes-visible** и снимаем галочку **Use default value**. **Custom value** выставяем значение **False** -> справа сверху жмём на часы -> Apply

9. Подключение по протоколу SSH.

#открываем терминал и вводим:

#разрешить подключаться следующим ip-адресам

sudo vim /etc/hosts.allow

#в конце файла записываем следующие

#прописываем ip с пробелами через запятую (пример):

sshd: 192.168.1.124, 192.168.1.10, 192.168.1.200

:wq!

#запретить подключаться всем, кроме ip-адресов из списка **hosts.allow**

sudo vim /etc/hosts.deny

#в конце файла записываем следующие:

sshd: ALL

:wq!

#редактируем файл настроек, меняем стандартный порт с 22 на **2002**, меняем интернет протокол на **IPv4**, отключаем аутентификацию под **root** (вход должен производиться от имени пользователя, в дальнейшем можно перелогиниться под **root**. Это нужно для ведения журнала: кто и когда заходил.)

#открываем терминал и вводим:

sudo vim /etc/ssh/sshd_config

#ищем строки:

#Port 22

```
#AddressFamily any
```

```
...
```

```
#PermitRootLogin prohibit-password
```

```
#редактируем их следующим образом, не забываем убрать решётки (раскомментировать):
```

```
Port 2002
```

```
AddressFamily inet
```

```
...
```

```
PermitRootLogin no
```

```
#сохраняемся, оповещаем SELinux об изменении порта и перезапускаем службу
```

```
:wq!
```

```
sudo semanage port -a -t ssh_port_t -p tcp 2002
```

```
sudo systemctl restart sshd
```

```
#На Windows-машине скачиваем и запускаем клиента Putty.
```

```
#В поле Host Name (or IP address) вводим ip-адрес машины к которой подключаемся. В поле port вводим 2002. Больше ничего не меняем -> Open.
```

```
#Вводим логин вашей учётной записи или локального администратора (не забываем, что под root система не впустит), вводим пароль.
```

```
#Чтобы подключиться из Linux-машины, откройте терминал и введите:
```

```
ssh имя_пользователя@ip-адрес
```

II. УСТАНОВКА И НАСТРОЙКА ПРОГРАММ

10. Установка программ, не входящих в официальный репозиторий Ред ОС

```
#заходим на HDD
```

```
cd /mnt/Disk2
```

```
#скачиваем архив с программами (если что, копия архива находится здесь \\0.12.55.98\Обмен\Сметанин П.В\linux)
```

```
wget --load-cookies /tmp/cookies.txt "https://drive.google.com/uc?export=download&confirm=$(wget --quiet --save-cookies /tmp/cookies.txt --keep-session-cookies --no-check-certificate 'https://drive.google.com/uc?export=download&id=1xcjb5j0CntQOzgnH1BELvhKB1vGRcemC' -O- | sed -rn 's/. *confirm=([0-9A-Za-z_]+). */\1\n/p')&id=1xcjb5j0CntQOzgnH1BELvhKB1vGRcemC" -O- | sed -rn 's/. *confirm=([0-9A-Za-z_]+). */\1\n/p')&id=1xcjb5j0CntQOzgnH1BELvhKB1vGRcemC" -O repo.tar && rm -rf /tmp/cookies.txt
```

```
#распаковываем архив и заходим в директорию с установочными файлами
```

```
tar -xvf repo.tar
```

```
cd /mnt/Disk2/repo/
```

11. Установка чата **Spark**

#Будучи в директории **/mnt/Disk2/repo/** устанавливаем программу
sudo dnf -y install ./spark-*.rpm
#Далее открываем: *Прочее* -> *Spark*
#Вводим данные: логин, пароль, ip-адрес сервера. Ставим галочки: *Сохранить пароль*, *Автоматический вход*.
#Дополнительно -> *Security* -> *Disabled* -> *Ок* -> *Войти*.
#Добавляем в автозагрузку: *Центр управления* -> *Запуск приложений* -> *Добавить*. В графе Имя пишем: **Spark**.
#В графе Команда пишем команду:
/bin/sh "/opt/Spark/Spark" %U
#Добавить -> *Заккрыть*

12. Установка и настройка **VipNet Client**.

#устанавливаем программу
sudo dnf -y install vipnetclient-gui_gost_ru_*.rpm
sudo dnf -y install libxcb-devel-1.14-2.el7.i686 libxcb-doc-1.14-2.el7.noarch
#файлы **.dst** и **пароль**, сохраняем для удобства в корне **Disk2**.
#открываем терминал и вводим:
#указываем полный путь к **.dst** файлу и прописываем свой пароль
sudo vipnetclient installkeys /mnt/Disk2/LARM-Sal-PTOUD-СметанинПВ/abc_0001.dst --psw пароль_vipnet_пользователя
#включаем журналирование критичных ошибок
sudo vipnetclient debug --loglevel 0
#включаем проверку обновлений справочников и ключей на транспортном сервере
sudo vipnetclient debug --mftp-reconnect
#настраиваем передачу данных по протоколу TCP. Включаем автоматический режим.
sudo vipnetclient debug --tcp-tunnel-mode auto
#включаем автозапуск ViPNet Client
sudo vipnetclient debug --autostart
#останавливаем службу ViPNet Client
sudo systemctl stop vipnetclient
#включаем видимость туннелируемых узлов по реальным адресам
sudo vipnetclient debug --tunnel-visibility 0
#выполняем настройки маршрутизации клиента
#редактируем файл **/etc/vipnet.conf**
sudo vim /etc/vipnet.conf
#ищем строки:
; trusted=

```

...
; iptables=off
#редактируем их следующим образом, не забываем убрать точки с запятой (раскомментировать):
trusted=ip_адреса_dns_серверов_вашей_организации_через_запятую_без_пробелов
...
iptables=off
#сохраняемся, оповещаем SELinux об изменении порта и перезапускаем службу
:wq!
#редактируем настройки маршрутизации системы, даём приоритет dns-именам
sudo vim /etc/authselect/nsswitch.conf
#ищем строки:
hosts:    files resolve [!UNAVAIL=return] myhostname mdns4_minimal [NOTFOUND=return] dns
#редактируем их следующим образом:
hosts:    files resolve [!UNAVAIL=return] myhostname dns mdns4_minimal
#стартуем и на всякий случай перезапускаем клиента
sudo systemctl start vipnetclient
sudo systemctl restart vipnetclient
#ознакомиться с основными параметрами
sudo vipnetclient info
#просмотр журнала IP-пакетов
sudo vipnetclient dbviewer
#проверка нарушения целостности, где пароль – это пароль администратора сетевого узла VipNet организации
sudo vipnetclient info --regulations --psw пароль_vipnet_нашей_организации
#создаём директорию для хранения критически важных событий
sudo mkdir /var/log/vipnetlog
#производим запись критически важных событий в лог, где пароль – это пароль администратора сетевого узла VipNet организации
sudo vipnetclient eventlog --psw пароль_vipnet_нашей_организации --output /var/log/vipnetlog/
#Запустить графический интерфейс программы: Системные -> ViPNet Client for Linux -> правой кнопкой Поместить на рабочий стол -> Открыть от Администратора
#Для обновления версии VipNet без удаления:
sudo rpm -U
vipnetclient-gui-4.6.0-2691.x86_64.rpm

```

13. Установка Kaspersky Endpoint Security и Агент администрирования.

13.1.Ставим Агент администрирования.

cd /mnt/Disk2/repo

#устанавливаем программу

sudo dnf -y install klnagent64-*.x86_64.rpm

#запускаем скрипт

sudo /opt/kaspersky/klnagent64/lib/bin/setup/postinstall.pl

#при запросах вводим следующие параметры

Please enter Administration Server DNS-name or static IP-address

IP_адрес_вашего_сервера_администрирования_касперского

Please enter Administration Server port number [14000]:

Enter

Please enter Administration Server ssl port number [13000]:

Enter

Please enter 'Y' to confirm that you want to use SSL encryption

or enter 'N' to use non-encrypted communication [Y]:

y

The Network Agent being installed can be used as connection gateway. It will allow you to connect to Administration Server using the specified connection gateway.

1 Do not configure connection gateway

2 Do not use connection gateway

3 Connect to server using connection gateway

4 Use as connection gateway

Please choose connection gateway mode: [1]:

1

13.2. Ставим Kaspersky Endpoint Security.

14. ***cd /mnt/Disk2/repo***

#устанавливаем программу

sudo dnf -y install kesi-*.x86_64.rpm

#установка языка программирования Perl, если он не установлен

sudo dnf install -y perl-Getopt-Long

#запуск скрипта установки

sudo /opt/kaspersky/kesi/bin/kesi-setup.pl

#при запросах вводим следующие параметры

#Жмём **Enter** и пролистываем лицензионное соглашение до конца.

I confirm that I have fully read, understand, and accept the terms and

conditions of this End User License Agreement [y/n]:

y

Please answer either 'y' or 'n'.

I confirm that I have fully read, understand, and accept the terms and conditions of this End User License Agreement [y/n]:

y

I am aware and agree that my data will be handled and transmitted #including to third countries as described in the Privacy Policy. I confirm that I have fully read and understand the Privacy Policy [y/n]:

y

I confirm that I have fully read, understand, and accept the terms and conditions of the Kaspersky Security Network Statement #KSN Statement is available here: '/opt/kaspersky/kesl/doc/ksn_license.ru' [y/n]:

y

Do you want to use the GUI? [y/n]:

y

Specify user to grant the 'admin' role to (leave empty to skip):

Enter

#Далее обновляемся и заходим на сервер Касперского и из группы нераспределённых добавляем в группу **Пользователи**.

15. Установка офисного пакета **P7 офис**.

cd /mnt/Disk2/repo

#устанавливаем программу

sudo dnf -y install r7-office.rpm

#Далее заходим: *Офис -> P7-Офис. Профессиональный (десктопная версия) - О программе -> Загрузить файл лицензии -> выбираем место куда скопировали лицензию -> Добавить.*

#После чего удалить файл лицензии со своего компьютера.

#Добавляем по умолчанию: *Параметры -> Предпочтительные приложения -> Офис -> Просмотрщик документов: **LibreOffice Draw**; Текстовый процессор: **P7-Офис**; Редактор электронных таблиц: **P7-Офис**.*

#Выполняем кастомные настройки. Запускаем Документ -> Файл -> Дополнительные параметры -> снимаем галочку Включить отображение комментариев в тексте -> ставим галочку Сделать файлы совместимыми с более старыми версиями MS Word -> Настройка макросов: Отключить все -> Применить

16. Установка **Консультант Плюс**.

#открываем терминал и вводим:

#устанавливаем **Wine**

sudo dnf -y install wine winetricks

#настраиваем **winetricks** от имени пользователя

winetricks riched30 winhttp

#обновляем до последней версии wine

sudo winetricks --self-update

#смотрим версию, должна быть **wine-6.0 (Staging)**

wine --version

#запускаем конфигуратор Wine

winecfg

#На вкладке **Графика** убираем галочку в пункте "Разрешить менеджеру окон декорировать окна".

#На вкладке **Приложения** выставаем версию Windows: *Windows 10*.

#устанавливаем программы для автоматического монтирования сетевой папки

#открываем файл и вписываем под строкой **+auto.master** следующее содержимое:

sudo vim /etc/auto.master

/mnt/samba /etc/auto.samba --ghost

:wq!

#создаём файл для автоматического монтирования и вписываем в него следующее содержимое:

sudo vim /etc/auto.samba

share -fstype=cifs,rw,noperm,username=guest,password= ://10.12.24.4/Consultant

share1 -fstype=cifs,rw,noperm,username=guest,password= ://10.12.24.4/region

:wq!

#запускаем службу autofs и добавляем её в автозагрузку

sudo systemctl start autofs.service

sudo systemctl enable autofs.service

#настраиваем Wine

winecfg

#На вкладке **Диски** добавляем диск **F** и указываем путь **/mnt/samba/share**

#На вкладке **Диски** добавляем диск **G** и указываем путь **/mnt/samba/share1**

Дополнительно -> тип Сетевой диск -> Применить -> ОК.

#поочерёдно запускаем обе версии консультанта и проверяем. Первый запуск может быть долгим

wine F:\cons.exe /linux /yes

wine G:\cons.exe /linux /yes

#копируем иконку

sudo cp -r /mnt/Disk2/repo/cons.ico /usr/share/icons/

#создадим ярлык на рабочем столе пользователя

#Все действия с файлом проводим от имени пользователя

cd ~/Рабочий\стол/

vim ConsultantPlus.desktop

#вписываем следующее содержимое:

```
[Desktop Entry]
Name=ConsultantPlus
Exec=wine F:\cons.exe /linux /yes
Type=Application
StartupNotify=true
Comment=ConsultantPlus
Icon=/usr/share/icons/cons.ico
StartupWMClass=cons.exe
```

vim ConsultantPlusRegion.desktop

#вписываем следующее содержимое:

```
[Desktop Entry]
Name=ConsultantPlusRegion
Exec=wine G:\cons.exe /linux /yes
Type=Application
StartupNotify=true
Comment=ConsultantPlusRegion
Icon=/usr/share/icons/cons.ico
StartupWMClass=cons.exe
```

#даём права на выполнение

chmod ugo+x Cons.desktop

chmod ugo+x Region.desktop

#Запускаем с рабочего стола и проверяем.

17. Установка **Yandex Browser**.

cd /mnt/Disk2/repo

#устанавливаем программу

sudo dnf -y install Yandex.rpm

#Далее заходим: *Интернет* -> правой кнопкой мыши *Yandex Browser (beta)* -> *Поместить на Рабочий стол*.

#Далее производим все кастомные настройки браузера.

18. Установка браузера **Opera**.

cd /mnt/Disk2/repo

sudo dnf -y install opera-stable_74.0.3911.75_amd64.rpm

#Далее заходим: Интернет -> правой кнопкой мыши Opera -> Поместить на Рабочий стол.

#Далее производим все кастомные настройки браузера.

19. Установка браузера **Google Chrome**.

#открываем терминал и вводим:

#скачиваем последнюю стабильную версию из репозитория Google.

wget https://dl.google.com/linux/direct/google-chrome-stable_current_x86_64.rpm

#устанавливаем браузер

sudo dnf -y localinstall google-chrome-stable_current_x86_64.rpm

#Далее заходим: Интернет -> правой кнопкой мыши Google Chrome -> Поместить на Рабочий стол.

#Далее производим все кастомные настройки браузера.

20. Обновление браузера **Chromium**.

#открываем терминал и вводим:

#он уже установлен, поэтому выполняем обновление из репозитория Ред ОС

sudo dnf -y install chromium

#Далее заходим: Интернет -> правой кнопкой мыши Веб-браузер Chromium -> Поместить на Рабочий стол.

#Далее производим все кастомные настройки браузера.

21. Установка **1С клиента**.

21.1. Терминальная версия.

#Интернет -> Remmina -> Поместить на Рабочий стол.

#Правой кнопкой по ярлыку на рабочем столе -> Переименовать -> пишем 1С

#Запускаем -> жмём значок «+» -> название: 1С -> протокол: RDP -> заполняем данные: Сервер, Имя пользователя, Пароль и Домен. Разрешение: Использовать клиентское разрешение

#Жмём Сохранить «по умолчанию» и Сохранить и подключить.

#Принимаем сертификат -> переключаем в полноэкранный режим (в последующем эта настройка сохранится по умолчанию).

#Завершать через Пуск – Завершение сеанса

21.2. Консольная версия

#открываем терминал и вводим:

cd /mnt/Disk2/repo/1C

#устанавливаем вспомогательные пакеты

sudo dnf -y install webkitgtk3-* .rpm webkitgtk3-devel-* .rpm

#устанавливаем пакеты программы 1С. Пакеты прописываем через пробел

```
sudo dnf -y install 1c-enterprise-*-client-*.rpm 1c-enterprise-*-common-*.rpm 1c-enterprise-*-server-*.rpm 1c-enterprise-*-client-nls-*.rpm 1c-enterprise-*-ws-*.rpm 1c-enterprise-*-ws-nls-*.rpm 1c-enterprise-*-crs-*.rpm
```

#копируем иконку

```
sudo cp -r /mnt/Disk2/repo/1C/1c.ico /usr/share/icons/
```

#Заходим: Офис -> правой кнопкой мыши 1С:Предприятие x86_64 -> Добавить эту кнопку запуска на рабочий стол.

#Запускаем приложение -> Добавление информационной базы -> Добавление в список существующей -> Наименование: **Имя вашей базы** -> выбираем **На сервере**

1С:Предприятия -> Кластер серверов: **Имя вашего сервера 1С** -> Имя информационной базы: **Имя вашей информационной базы** -> Далее -> Вариант

аутентификации: **Запрашивать имя и пароль** -> всё остальное по умолчанию -> Готово.

#Далее выделяем базу нажимаем Настройка -> Адреса Интернет-сервисов -> Список общих баз и вводим:

```
ip_адрес_сервера_1С/Диск:/1С_Bases_v8i/ИмяБазы.v8i -> Ок.
```

#Пробуем зайти, проверяем.

22. Установка Lotus Notes.

#спускаемся в директорию и запускаем .exe файл при помощи эмулятора wine

```
cd /mnt/Disk2/repo/Lotus/LNB9/
```

```
wine setup.exe
```

#поднимаемся на директорию выше и запускаем .exe файлы при помощи эмулятора wine

```
cd ..
```

```
wine 901FP5SHF237_W32_basic.exe
```

```
wine eztwain_setup.exe
```

#После установки Lotus Notes выполняем подмену папок.

#Wine -> Wine File -> заходим в директорию **C:\Lotus** и удаляем всю папку Notes.

#Wine -> Wine File -> заходим в директорию **Z:\mnt\Disk2\repo\Lotus** -> выделяем папку **Notes** -> Файл -> Копировать -> указываем путь **C:\Lotus**

#Тем самым мы подменили установленную папку Notes на нашу. При установке Lotus из-под Wine, часть файлов теряется, поэтому этот костыль, пока единственный способ подружить RedOS 7.3 с Lotus Notes.

#удаляем лишние ссылки с рабочего стола **IBM Notes (Basic).lnk, EZTwain Pro User Guide.lnk, EZTwain Pro User Guide.desktop**

#правой кнопкой на ярлык с иконкой логотипа **IBM Notes (Basic)** на рабочем столе -> в графе Команда меняем путь на: **wine C:\Lotus\Notes\notes.exe -sa** -> Закрыть -> запускаем программу

#в Имя пользователя выбираем Другой и указываем путь к вашему **id-файлу**. Войти.

#Рабочая область -> Контакты - Дополнительно -> Подключения -> Заходим в подключение -> CMEDIA/GOVERNMENT -> Изменение подключения -> Дополнительно

#проверяем, чтобы Адрес конечного сервера выглядели следующим образом (в примере представлены **виртуальные ip-адреса** Аппарата губернатора ЯНАО)

```
# CMEDIA/GOVERNMENT 11.0.0.3
```

```
# CMEDIA2/GOVERNMENT 11.0.0.4
```

```
# MAIL/GOVERNMENT 11.0.0.5
```

#Узнать виртуальный адрес можно так: **VipNet Client for Linux** -> Сетевые узлы -> **SERV-AG-S1** -> Адрес узла.

23. Установка и настройка КристоПро CSP.

```
#спускаемся в директорию
cd /mnt/Disk2/repo/CryptoPRO/
#даём скрипту права на выполнение
sudo chmod ugo+x install_gui.sh
#запускаем скрипт
sudo ./install_gui.sh
#В открывшемся окне: Next -> выбираем всё -> Next -> Install -> Ok -> Enter the license now
#вводим номер лицензии -> Enter -> Ok -> Exit -> Yes
#просмотр лицензии
/opt/cproscsp/sbin/amd64/cpconfig -license -view
#если лицензия не подошла, её можно повторно ввести через терминал
/opt/cproscsp/sbin/amd64/cpconfig -license -set номер лицензии
#установка драйвера Рутокен
sudo dnf -y install ifd-rutokens
#установка драйвера Jakarta
sudo dnf -y localinstall /mnt/Disk2/repo/CryptoPRO/cproscsp-rdr-jakarta-*.rpm
#установка средства управления сертификатами
sudo dnf -y install token-manager
#установка ПО для подписи файлов gostcrypto
sudo dnf -y install gostcryptogui caja-gostcryptogui
#Запустить CryptoPRO можно так: Администрирование -> Ключевые носители и сертификаты
#Администрирование -> Подпись и шифрование файлов
```

24. Установка расширений плагинов и расширений для браузеров.

#Будем делать на примере браузера **Chromium**.

24.1. Установка расширения Госуслуги.

#открываем терминал и вводим:

```
cd /mnt/Disk2/repo/
sudo dnf -y install ifcplugin-chromium
```

#Запускаем **Chromium** и переходим по ссылке: <https://chrome.google.com/webstore/detail/расширение-для-плагина-ro/pbefkdcndngodfeigfdgiogdnmbgcfha?hl=ru&authuser=1>

#Установить -> Установить расширение

24.2. Установка расширения CryptoPro Browser Plug-in.

```
cd /mnt/Disk2/repo/cades_linux_amd64
```

#устанавливаем нужные пакеты

sudo dnf -y install ./cprosp-pki*rpm

#Запускаем **Chromium** и переходим по ссылке: <https://chrome.google.com/webstore/detail/cryptopro-extension-for-c/iifchhfnnmpdbibifmljnfjhpififfog?hl=ru>

#Установить -> Установить расширение

#Заходим на страницу и проверяем подпись: https://www.cryptopro.ru/sites/default/files/products/cades/demopage/cades_bes_sample.html

24.3. Установка расширения **Контур.Плагин**.

cd /mnt/Disk2/repo/

sudo dnf -y install kontur.plugin_amd64.rpm

#Далее переходим по ссылке: https://install.kontur.ru/kekep?_ga=2.232358492.2121287449.1613045347-237475827.1613045347

#Скачать расширение -> Установить -> Установить расширение (Диагност)

#Выбираем «Что ещё можно сделать?» -> в раскрывающемся списке выбираем Скачать RPM-пакет Диаг.Плагин -> Сохранить

cd /mnt/Disk2/repo/

sudo dnf -y install diag.plugin-3.1.0.210-1.x86_64.000865.rpm

#Переходим по ссылке: https://install.kontur.ru/kekep?_ga=2.232358492.2121287449.1613045347-237475827.1613045347

#Жмём Далее -> произойдёт проверка -> Установить -> скопировать ссылку и перезагрузить браузер **Chromium**, после чего вставить скопированную ссылку в адресную строку.

25. Установка **DWGViewer**.

#открываем терминал и вводим:

#устанавливаем пакет OpenGL

sudo dnf -y install freeglut-devel

cd /mnt/Disk2/repo/

sudo dnf install VariCAD_View_*.rpm

#Далее заходим: Графика -> VariCAD Viewer.

#Открывать файлы через: File -> Open.

26. Установка программы для распознавания текста.

#открываем терминал и вводим:

#устанавливаем программу распознавания текста и два словаря рус и англ

sudo dnf -y install yagf aspell-ru aspell-en

sudo dnf -y install yagf-0.9.5-5.el7.i686

#чтобы получать изображение со сканера установим дополнительные программы

sudo dnf -y install xsane libksane libksane-devel pantum-drivers-sane

sudo dnf -y install perl-Image-Sane sane-backends-daemon sane-backends-devel sane-frontends xsane-gimp

#Далее заходим: *Офис* -> *YAGF* -> *Правка* -> *Настройки* -> выбираем язык распознаваемого текста *Русский-английский* -> кнопка *Языки* -> ставим галочки *Английский*, *Русский*, *Русский-Английский* -> *Ок* -> *Обработка изображений* -> снимите галочку *Обрезать изображение при загрузке* -> *Ок*.
#Попробуйте что-нибудь отсканировать и распознать.

27. Установка Календаря

```
cd /mnt/Disk2/repo/
```

#распаковываем архив

```
tar jxvf Rainlendar_*.tar.bz2
```

```
sudo cp -r rainlendar2 /usr/share/
```

#заходим: *Параметры* -> *Запуск приложений* -> *Добавить* -> в *Имя* вписываем *Railendar* -> в *Команда* вписываем путь [/usr/share/rainlendar2/rainlendar2](#) -> *Сохранить* -> *Закреть*

#скрипт будет запущен сразу после перезагрузки

28. Запись ISO-образов

#вставляем флешку

#открываем терминал и вводим:

```
sudo dnf -y install gnome-multi-writer
```

#заходим: *Системные* -> *MultiWriter* -> значок папки -> выбираем *ISO-образ* -> *Начать запись* -> соглашаемся и вводим пароль

29. Установка программ для диагностики компьютера и системы

#тут большой список инструментов, которые могут пригодиться системному администратору

```
sudo dnf -y install gnome-disk-utility gparted lm_sensors hwloc lshw inxi htop lsscsi
```

```
sudo dnf -y install libX11-devel freetype-devel zlib-devel libxcb-devel libxslt-devel libgcrypt-devel libxml2-devel gnutls-devel
```

```
sudo dnf -y install libpng-devel libjpeg-turbo-devel libtiff-devel gstreamer-devel dbus-devel fontconfig-devel stress-ng
```

```
sudo dnf -y install git gettext-devel openssl-devel perl-CPAN perl-devel zlib-devel
```

```
sudo dnf groupinstall "Development Tools"
```

III. ПРОЧИЕ НАСТРОЙКИ

30. Закрываем возможность создавать и записывать файлы на рабочий стол (необязательная настройка).

#открываем терминал и вводим:

```
sudo chattr +i ~/Рабочий\ стол
```

#Это делается для сохранения места на SSD, все файлы пользователя должны храниться либо на сетевом диске, либо в директории **Disk2**.

#Проверяем, пробуем что-нибудь создать или перекинуть на рабочий стол.

#для отключения блокировки вводим

sudo chatter -i ~/Рабочий\стол

31. Включаем Line-Out выход для наушников

#открываем терминал и вводим:

sudo vim /etc/modprobe.d/alsa-base.conf

#в открывшемся окне находим строки:

options bt87x index=-2

options cx88_alsa index=-2

options saa7134-alsa index=-2

options snd-atiixp-modem index=-2

options snd-intel8x0m index=-2

options snd-via82xx-modem index=-2

options snd-usb-audio index=-2

options snd-usb-caiaq index=-2

options snd-usb-ua101 index=-2

options snd-usb-us122l index=-2

options snd-usb-usx2y index=-2

...

options snd-pcsp index=-2

...

options snd-usb-audio index=-2

#меняем значение -2 на **10**. Закрываем, сохраняем.

wq!

#запускаем интерфейс звуковой платы

alsamixer

#далее жмём **F6** -> **0 HAD Intel PCH** -> стрелочкой вверх выставляем максимальные значения следующим выходам: *Master, PCM, Front, Front Mic, Frjnt Mic Boost, Surround, Center, LFE, Line, Line Boost, Rear Mic, Rear Mic Boost*. Меняем значение: *Auto-Mute Mode* на **Disable**. Выходим **Esc**.

#далее заходим: *Параметры* -> *Звук* -> *Оборудование* -> *Встроенное аудио* -> выставляем *Профиль: Аналоговый стерео выход* -> вкладка *Выход* -> выставляем *Канал: Линейный выход*.

#подключаем наушники, проверяем звук.

32. Установка принтера\МФУ.

#устанавливаем драйвера и вспомогательные утилиты

sudo dnf -y install hplip hplip-gui gutenprint manufacturer-PPDs OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript foo2zjs

sudo dnf -y install python3-distro net-snmp python-cups-doc hpijs PyQt4 python-reportlab

#выставляем python3 программой для запуска скриптов .py по умолчанию

sudo ln -fs /usr/bin/python3 /usr/bin/python

#перезапускаем службу печати и добавляем в автозагрузку

sudo systemctl enable cups

sudo systemctl restart cups

32.1. Установка принтеров\МФУ фирмы HP:

#открываем терминал и вводим:

hp-setup

#Setup Device -> Network/Ethernet -> Next -> Выбираем нужный из списка найденных -> Next -> (ничего не трогаем, ждём. Если не найдёт драйвер, указываем нужный PPD file вручную) -> Add Printer -> во всплывающем окне вводим **root** и его **пароль** -> Ok

#Принтер установлен и его можно увидеть в Администрирование -> Управление устройствами HP -> HP Device Manager.

#Отключаем уведомления: Администрирование -> Управление устройствами HP -> Configure -> Preferences -> System Tray Icon -> Always hide -> Ok.

32.2. Установка принтеров\МФУ Kyosera:

#Предварительно зайдите на веб-интерфейс принтера - Настройки безопасности - Защита сети – и убедитесь, что все TLS протоколы включены.

#открываем терминал и вводим:

cd /mnt/Disk2/repo/

#устанавливаем драйвера

sudo dnf -y install kyodialog-0-0.x86_64.rpm

sudo dnf -y install kyocera-sane-2.0-0326.x86_64.rpm

#меняем расположение директорий, для поиска драйвера

sudo rm -rf /usr/share/kyocera

sudo rm -rf /usr/share/kyocera7

sudo chmod 777 /usr/share/ppd/kyocera

sudo ln -s /usr/share/ppd/kyocera/ /usr/share/cups/model/

#перезапускаем службу

sudo systemctl restart cups

#заходим на сервисную страничку службы

sudo system-config-printer

#жмём Добавить и находим нужный вам принтер. Если система попросит установить драйвер, находим подходящий драйвер здесь: ***/usr/share/ppd/kyocera/***

33. Установка сканера.

#Если перед этим вы ещё не устанавливали драйвера устройств, то

#открываем терминал и вводим:

sudo dnf -y install hplip hplip-gui gutenprint manufacturer-PPDs OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript foo2zjs

sudo dnf -y install python3-distro net-snmp python-cups-doc hpijs PyQt4 python-reportlab

#выставляем python3 программой для запуска скриптов .ру по умолчанию

sudo ln -fs /usr/bin/python3 /usr/bin/python

#перезапускаем службу печати и добавляем в автозагрузку

sudo systemctl enable cups

sudo systemctl restart cups

#обнаруживаем устройства в сети

scanimage -L

#Заходим: *Графика -> Утилита сканирования -> выбираем значок трёх параллельных прямых -> Параметры (задаём разрешение, формат и двустороннее сканирование) -> выходим назад, указываем нужный вам сканер -> жмём стрелочку, выбираем автоподатчик\планшет, Изображение (цв. скан)\Текст (чб. скан)-> Сканируем и сохраняем (по умолчанию сохраняет в папке Документы в формате .pdf).*

34. Установка панели программ в стиле MacOS (необязательная настройка)

#это необязательная опция, но придаёт графической оболочке красоту и удобство

#устанавливаем пакеты программ

sudo dnf -y install plank-devel plank-docklets plank-libs

#запускаем панель в фоновом режиме.

plank > /dev/null 2>&1 &

#убираем задний фон панели, делаем его прозрачным

#Системные -> Редактор dconf-> далее org-> mate -> panel -> toplevels -> bottom -> background -> заходим в **color** и в графе **Custom value** указываем **rgba(255,255,255,0)**
-> справа сверху жмём на часы -> Apply

#Системные -> Редактор dconf-> далее org-> mate -> panel -> toplevels -> bottom -> background -> заходим в **type** и в графе **Custom value** указываем **color** -> справа сверху жмём на часы -> Apply

#увеличиваем размер значков

#Системные -> Редактор dconf-> далее org-> mate -> panel -> toplevels -> bottom -> заходим в **size** и в графе **Custom value** указываем **50** -> справа сверху жмём на часы -> Apply

#убираем лишние значки с панели

#Системные -> Редактор dconf-> далее org-> mate -> panel -> general -> заходим в **object-id-list** и в графе **Custom value** указываем **['menu-bar', 'menu-separator', 'window-list', 'notification-area', 'volume-control', 'st-separator', 'clock']** -> справа сверху жмём на часы -> Apply

#меняем фон рабочего стола

*#Системные -> Редактор dconf -> далее org-> mate -> desktop -> background -> заходим в **picture-filename** и в графе **Custom value** указываем **/usr/share/backgrounds/redos/wide/desktop_1.jpg** -> справа сверху жмём на часы -> Apply*
*#Добавляем в автозагрузку: Центр управления -> Запуск приложений -> Добавить. В графе Имя пишем: **Plank**.*
#В графе Команда пишем команду:

plank

#подменяем стандартные значки на наши

sudo chmod 777 ~/.config/plank/dock1/launchers

sudo rm -rf ~/.config/plank/dock1/launchers/*

sudo cp -r /mnt/Disk2/repo/plank_link/* ~/.config/plank/dock1/launchers/

35. Производим резервное копирование системы на диск **Disk2**

*#логинимся под **root***

su -

#заходим на HDD, создаём директорию Backup и даём к ней доступ для всех

cd /mnt/Disk2/

sudo mkdir Backup

sudo chmod 777 Backup

cd Backup/

#создаём переменную с актуальным временем и запускаем побитовое копирование корневой директории в директорию Backup

sudo dd if=/dev/mapper/ro_redos-root conv=sync,noerror bs=64K status=progress | gzip -c > **актуальное_число_и_вермя.gz**

#восстановление:

su -

gunzip -c /mnt/Disk2/Backup/актуальное_число_и_вермя.gz | dd of=/dev/mapper/ro_redos-root status=progress

reboot

36. Удаляем группу Пользователи домена из файла **/etc/sudoers**

*#логинимся под **root***

su -

*#заходим в редактор настроек **root**. Сам файл находится тут: **/etc/sudoers** i – редактировать, Esc – закончить редактировать, :wq! – сохранить и выйти*

visudo

#ищем строчку:

%Пользователи\ домена ALL=(ALL) ALL

#удаляем эту строку. Сохраняем, закрываем.

#выходим из root

exit

#перезагружаемся

reboot

IV. ДОПОЛНИТЕЛЬНЫЕ ИНСТРУКЦИИ

37. Проверка состояния жёсткого диска

#открываем терминал и вводим:

#устанавливаем программу

sudo dnf -y install gnome-disk-utility

#Далее заходим: Стандартные -> Диски -> Меню (три точки) -> Данные самодиагностики и SMART.

38. Использование памяти диска

#покажет все разделы с указанием свободного места

df -h

#скачиваем программу графической работы с дисками

sudo apt-get install gparted

#Далее: Приложения -> Системные -> GParted

39. Мониторинг температуры процессора.

#устанавливаем программу

sudo dnf -y install lm_sensors

#определяем аппаратную часть системы.

#Везде соглашаемся «y»

sudo sensors-detect

#запускаем программу

sensors

40. Информация о процессоре.

#полная информация о процессоре

lscpu

#скачиваем программу

sudo dnf -y install hwloc

#блочная информация о процессоре

hwloc-ls

41. Информация об оперативной памяти.

#краткая информация об оперативной памяти

free -h

#полная информация об оперативной памяти

cat /proc/meminfo

#ещё один способ узнать информацию об оперативной памяти

vmstat -s

42. Информация о системе.

#скачиваем программу

sudo dnf -y install lshw

#запускаем

sudo lshw -short

#скачиваем программу

sudo dnf -y install inxi

#запускаем

inxi -F

#в графической оболочке это можно сделать через: *Параметры -> Информация о системе*

43. Мониторинг работы системы

#делает снимок всех процессов в системе

ps axu

#чтобы убить процесс

kill PID

#найти определённый процесс

ps axu | grep название приложения

#убить все процессы этого приложения

killall название приложения

#в графической оболочке это можно сделать через: *Системные -> Системный монитор*

44. Журналирование

#содержит глобальные системные логи, в том числе те, которые регистрируются при запуске системы. В этот лог записываются несколько типов сообщений: почта, cron, сервисы, ядро, аутентификация и другие:

/var/log/messages

#содержит информацию, которая регистрируется при загрузке системы.

/var/log/boot.log

#отображает информацию о последней сессии всех пользователей. Это нетекстовый файл, для его просмотра необходимо использовать команду **lastlog**.

/var/log/lastlog

#лог файл Linux содержит информацию о неудачных попытках входа в систему. Для просмотра файла удобно использовать команду **sudo last -f /var/log/btmp**

/var/log/btmp

#регистрирует всю информацию об установке пакетов с помощью **Dnf**.

/var/log/dnf.log

#содержит информацию, относящуюся к аутентификации и авторизации. Например, **SShd** регистрирует здесь все, в том числе неудачные попытки входа в систему.

/var/log/secure

#содержит журнал входов пользователей в систему. С помощью команды **last -f /var/log/wtmp** можно узнать кто и когда вошел в систему.

/var/log/wtmp

#содержит информацию и журналы файлового сервера **Samba**, который используется для подключения к общим папкам **Windows**.

/var/log/samba/

#содержит **.cap** файлы, собранные пакетом **Sysstat**.

/var/log/sa/

#используется системным демоном безопасности, который управляет удаленным доступом к каталогам и механизмами аутентификации.

/var/log/sssd/

Примеры просмотра логов:

#обычный просмотр.

sudo cat /var/log/dnf.log

#просмотр в режиме прокрутки.

sudo less /var/log/dnf.log

#просмотр первых 10 строк.

sudo head /var/log/dnf.log

#просмотр последних 10 строк.

sudo tail /var/log/dnf.log

#просмотр в режиме реального времени.

sudo tail -F /var/log/dnf.log

#просмотр в режиме редактирования.

sudo vim /var/log/dnf.log или ***nano /var/log/dnf.log***

#выводит только строки, содержащие слово **gui**. Вместо **gui** можно подставить любое другое слово.

sudo cat /var/log/dnf.log | grep gui

#в графическом виде все журналы можно просматривать так: *Системные -> Просмотр системных журналов*

V. РЕШЕНИЕ ПРОБЛЕМ

45. Если затрясло экран

#Открываем командную строку:

mc

#F9 -> *Настройки -> Настройки панелей -> Показывать скрытые файлы -> Дальше*

#Заходим в папку */home/пользователь/.config/dconf* и выходим из mc клавишей *F10*

#Набираем в командной строке:

sudo chown имя_пользователя user

cd

46. Если отвалилась панель инструментов

#Открываем командную строку:

mate-panel --reset

47. Если не выполняются команды **dnf update** и **dnf upgrade**

#Открываем командную строку:

#посмотреть список подключенных репозиторий:

dnf repolist

#удалить ненужный

sudo dnf remove epel-release

48. Убрать иконку пользователя при запуске системы

#открываем командную строку и вводим:

#логинимся под root

su -

#заходим в директорию логирования и находим нужного пользователя, редактируем файл

```
cd /var/lib/AccountsService/users/  
ls -la  
vim smetaninpv  
#меняем значение false на true  
SystemAccount=true  
#перелогиниваемся. Лишней иконки быть не должно.  
#Если пользователь, чью иконку отключаем уволился, то его запись можно удалить  
su -  
cd /var/lib/AccountsService/users/  
rm -rf имя_пользователя  
#если не требуется хранить его документы, то удаляем всю домашнюю директорию пользователя  
cd /home/  
rm -Rfv имя_пользователя@имя_домена
```

49. Установка wine из исходников

```
#открываем командную строку и вводим:  
#устанавливаем дополнительные пакеты  
sudo dnf -y install libX11-devel freetype-devel zlib-devel libxcb-devel libxslt-devel libgcrypt-devel libxml2-devel gnutls-devel libpng-devel libjpeg-  
turbo-devel libtiff-devel gstreamer-devel dbus-devel fontconfig-devel  
#скачиваем самую свежую версию  
wget https://dl.winehq.org/wine/source/5.x/wine-5.6.tar.xz  
#распаковываем  
tar -Jxf wine-6.4.tar.xz  
#заходим в распакованную папку  
cd wine-6.4/  
#собираем из исходников (сборка занимает очень много времени)  
./configure --enable-win64  
make  
sudo winemake install  
#смотрим обновлённую версию, должна быть wine-6.4  
wine64 --version
```