УТВЕРЖДАЮ

Главный инженер Нижегородского ИВЦ

«\_\_\_»\_\_\_\_\_\_\_\_\_\_Ю.В.Яковуник

**ИНСТРУКЦИЯ   
по установке операционной системы CentOS 7   
из типового образа ГВЦ в режиме «kickstart»**

Оглавление

[1. Общие положения 3](#_Toc103587253)

[2. Этапы развёртывания сервера с использованием ISO-образа 3](#_Toc103587254)

[3. Установка ОС 4](#_Toc103587255)

[4. Настройка времени 8](#_Toc103587256)

[5. Работа с файрволами 8](#_Toc103587257)

[6. Привязка к серверу управления контентом (репозиторию) 9](#_Toc103587258)

[7. Настройка сервиса записи логов Journald. 10](#_Toc103587259)

[8. Установка пакетов для анализа производительности сервера. 10](#_Toc103587260)

[9. Блокировка стандартных пользователей. 10](#_Toc103587261)

[10. Отключение ssh для пользователя root. 11](#_Toc103587262)

# Общие положения

1. В целях унификации сопровождения ИС/АСУ на полигонах ГВЦ с физическим и виртуальным размещением серверов принят к использованию типовой образ ОС Linux (CentOS 7), в формате iso с использованием метода быстрой установки операционных систем (kickstart) на базе RedHat/CentOS..
2. Настоящий документ является инструкцией, описывающей автоматизированное развертывание ОС Centos 7 на серверах всех ЦОД, ИВЦ в рамках Единого ЦОД Главного вычислительного центра – филиала ОАО «РЖД». Инструкция составлена в соответствии с Типовыми требованиями к настройкам серверных операционных систем семейства Linux на базе RHEL/CentOS (далее – Типовые требования).
3. В настройках параметров TCP/IP сетевого интерфейса серверов должно быть перечислено несколько IP-адресов серверов DNS/WINS в соответствии с распоряжением №ГВЦ-266/р от 05.07.2017г.
4. Именование серверов выполняется в строгом соответствии с правилами именования и заполнения обязательных атрибутов объектов службы глобального каталога ОАО «РЖД».

# Этапы развёртывания сервера с использованием ISO-образа

Согласно Типовым требованиям, для настройки серверной ОС Linux на базе CentOS или RHEL рекомендуется выполнить установку ОС с использованием эталонного образа, а так же обязательно выполнить следующие настройки:

настройка сетевых интерфейсов;

настройка подключения к серверу управления контентом (репозиториям);

установка и настройка агента мониторинга ОС;

установка и настройка агента СРК.

Помимо этого, для серверов дорожного уровня необходимо произвести настройку подключения к региональным серверам NTP.

Остальные настройки, указанные в типовых требованиях (локальное резервное копирование конфигурации, разбивка дискового пространства, ролевая модель и т.д.), производятся автоматически при kickstart-инсталляции системы из типового образа. В случае ручной инсталляции операционной системы требуется обязательное применение настроек, описанных в Типовых требованиях.

Ниже описаны этапы автоматизированной установки ОС.

# Установка ОС

1. Запустить сервер (виртуальную машину), смонтировать эталонный образ, отправить Ctrl-Alt-Del для перезагрузки. Последовательность действий показана на рисунках 1и 2.

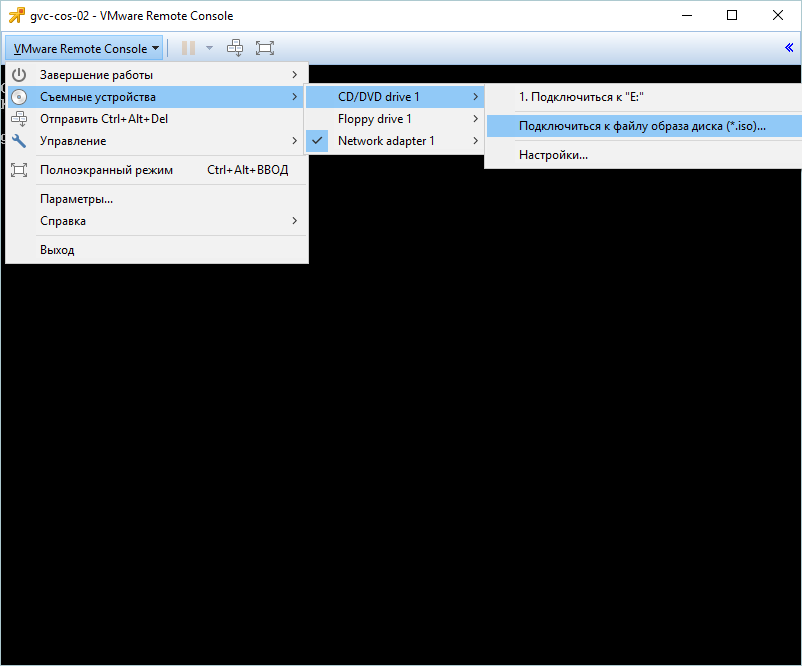


Рис.1 Монтирование образа в VMware Remote Console.

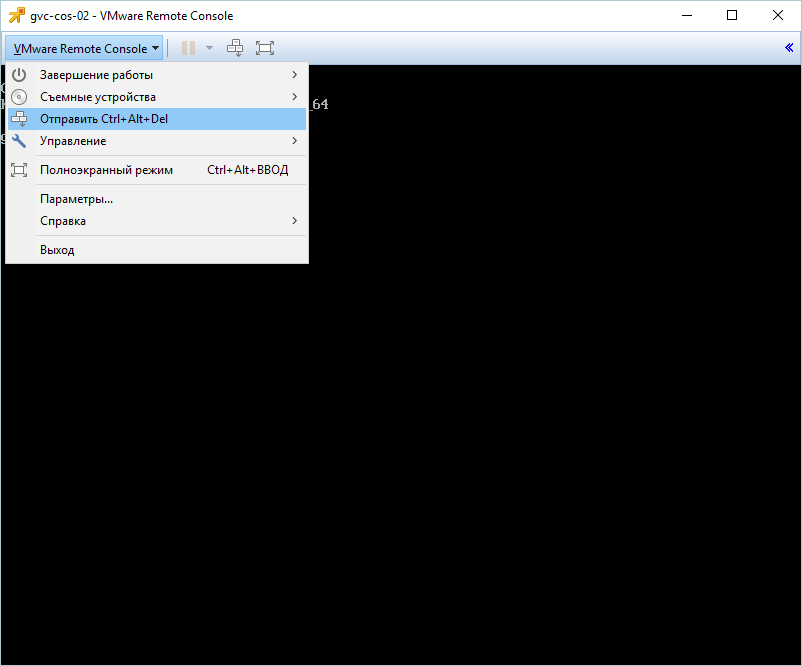


Рис.2 Монтирование образа в VMware Remote Console.

1. В окне загрузчика, представленном на рисунке 3, выбрать пункт Kickstart.

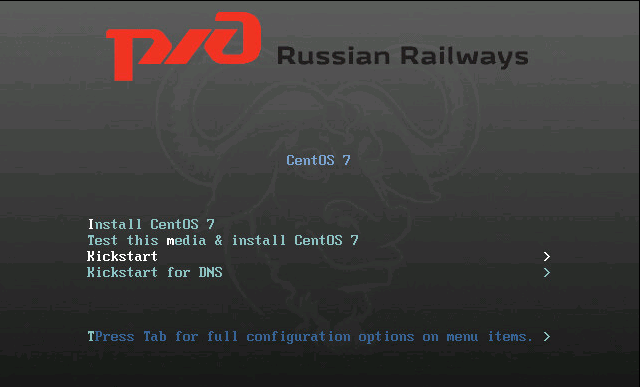


Рис.3 Окно выбора вариантов загрузки.

1. В открывшемся дополнительном меню, представленном на рисунке 4, выбрать:

Install from cdrom kickstart MBR BOOT to VMware – для виртуальных серверов

Install from cdrom kickstart MBR BOOT to Hardware – для аппаратных серверов

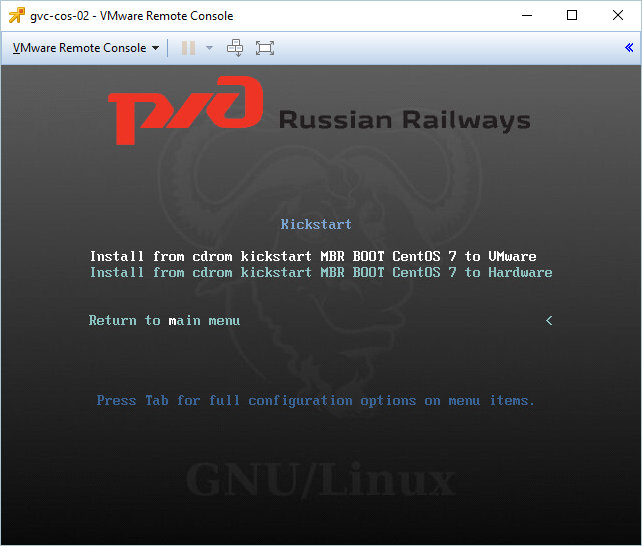


Рис.4 Меню выбора варианта установки ОС

1. Ожидать окончание процесса установки. На рисунке 5 приведён скриншот промежуточного этапа процесса инсталляции ОС.

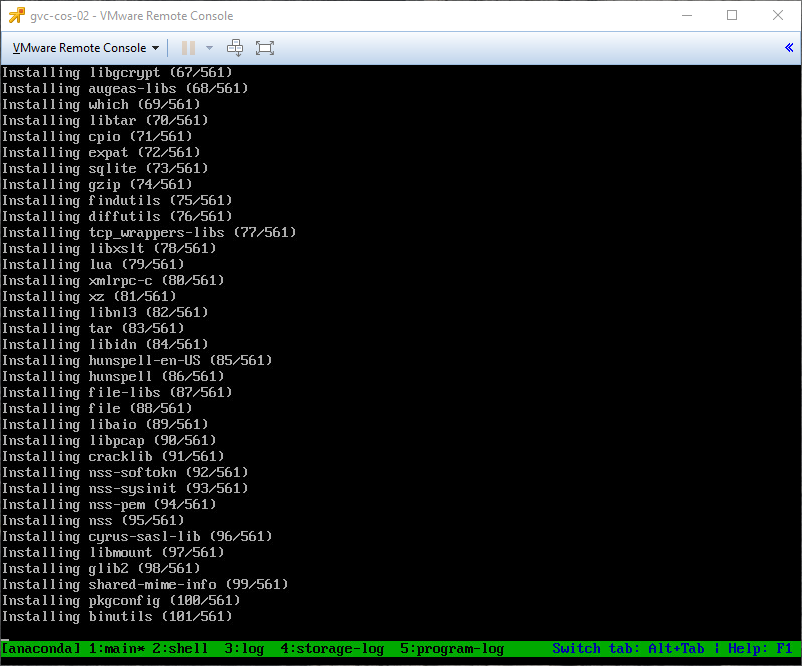


Рисунок 5.Промежуточные результаты установки ОС.

1. В процессе установки ОС из образа, предлагается ввести сетевые настройки.

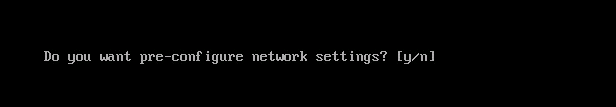


Рисунок 6. Приглашение для ввода сетевых настроек.

Данные для ввода (для каждого сервера данные могут отличаться от приведенных ниже):

домен: grw.oao.rzd

ip-адрес: 10.24.209.35

префикс: 20

шлюз: 10.24.222.200

Маска: 255.255.240.0

база для поиска: grw.oao.rzd

dns-серверы: 10.24.222.0, 10.24.222.1

По окончанию ввода настроек, предлагается проверить корректность введенных данных, пример на рисунке 7. *Внимание! IP-адресс и имя необходимо изменить!*.

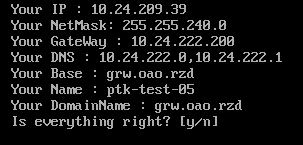


Рисунок 7.Проверка правильности сетевых настроек.

1. Для настройки ОС вход осуществлять под учётной записью *adminptk* или *adminos*. Первоначально настроенные пароли показаны в таблице 1.

|  |  |
| --- | --- |
| Учётная запись | Пароль |
| *adminos* | P@ssw0rd |
| *adminptk* | J41BLrHp |

Таблица 1. Учётные данные для настройки ОС.

1. В процессе входа происходит автоматический запрос на смену пароля. Необходимо ввести сначала старый пароль, а затем ввести новый пароль, удовлетворяющий минимальным требованиям, согласно Типовым требованиям. Процесс смены пароля показан на рисунке 8. Смену пароля необходимо выполнить для всех встроенных УЗ

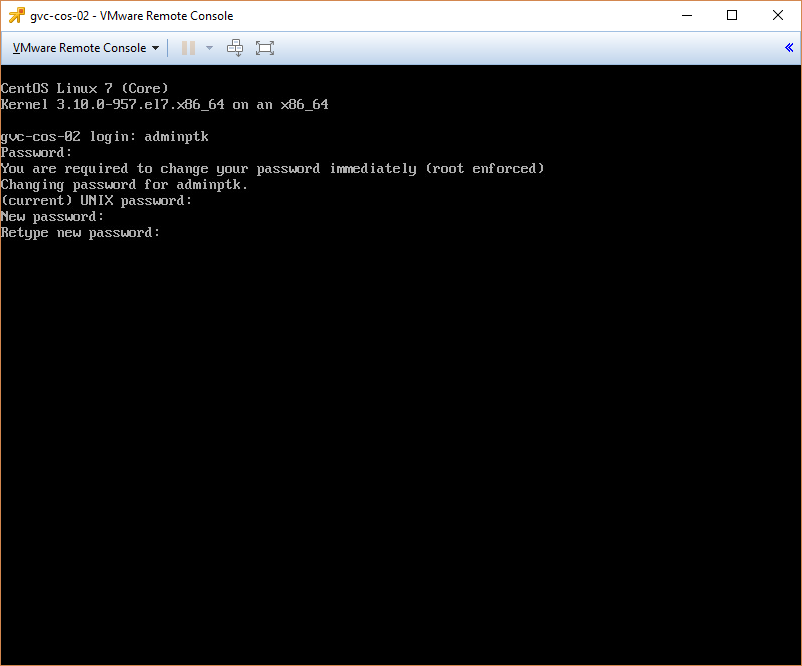


Рисунок 8. Смена пароля.

1. Для удобства пользования консолью отключить Tmux

sudo yum remove tmux

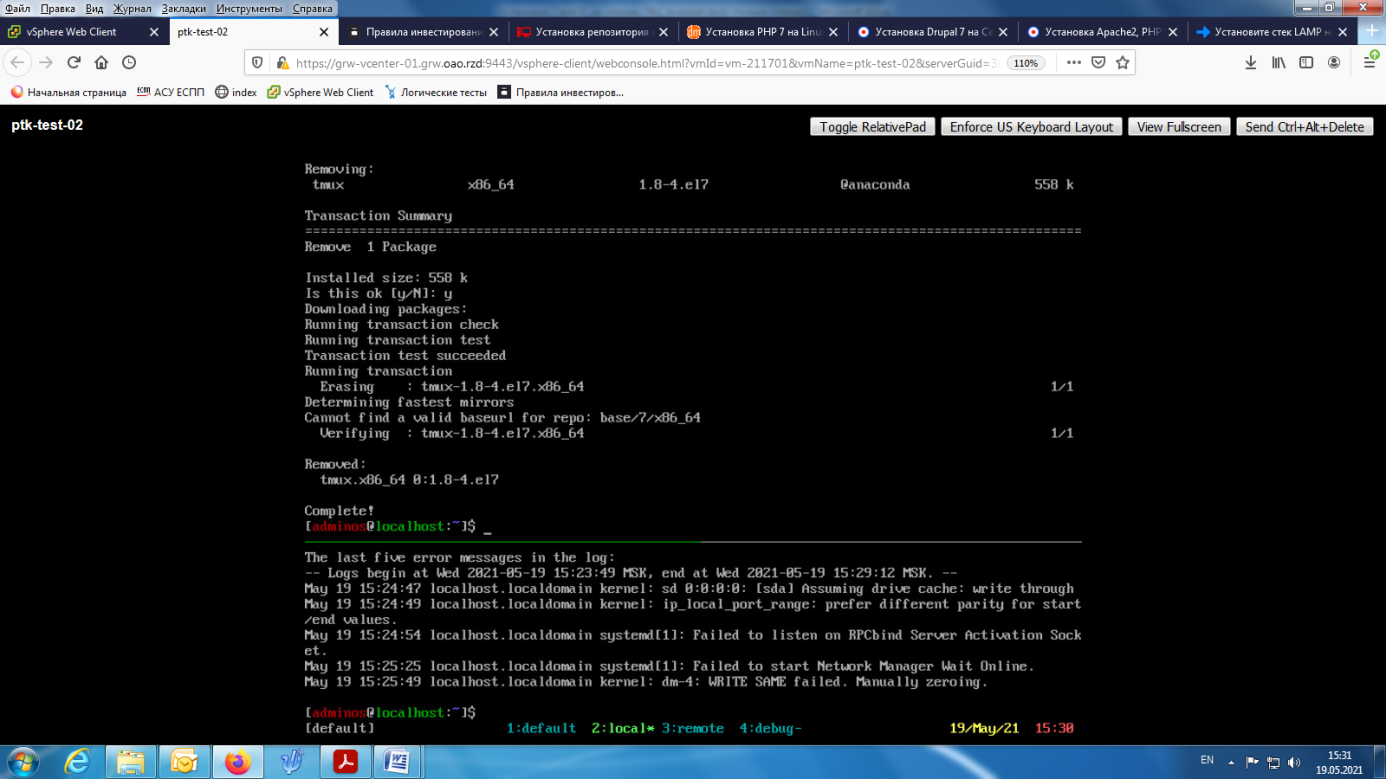


Рисунок 9. Удаление Tmux.

1. Так же для удобства использования консоли переключиться на вторую консоль

Alt + F2

и выполнить вход под учетной записью *adminptk* или *adminos.*

1. Установить пароль для пользователя root (длина пароля не менее 12 символов):

sudo passwd root

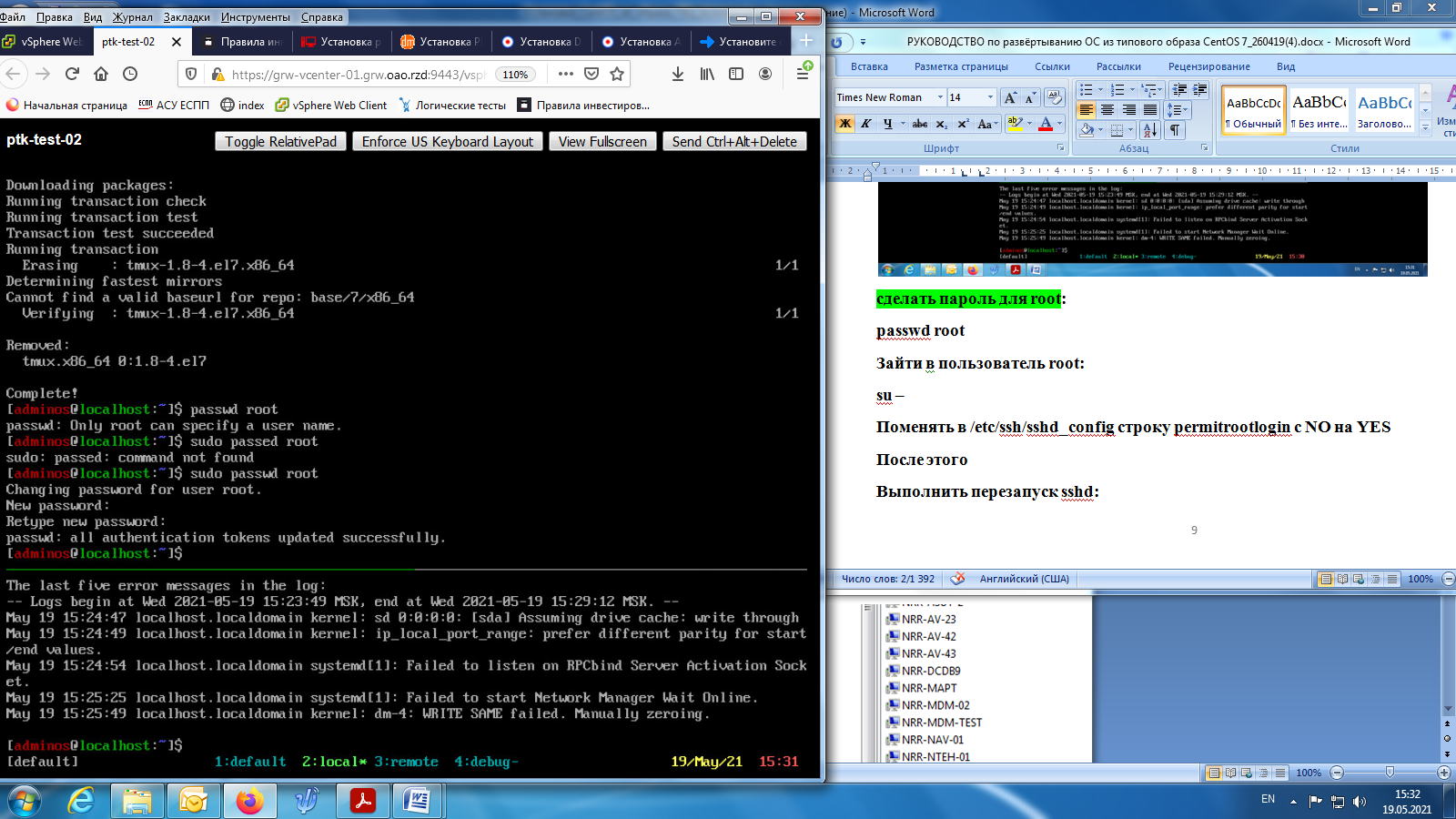


Рисунок 10. Установка пароля.

1. Выполнить вход в систему пользователем root:

su –

# Настройка времени

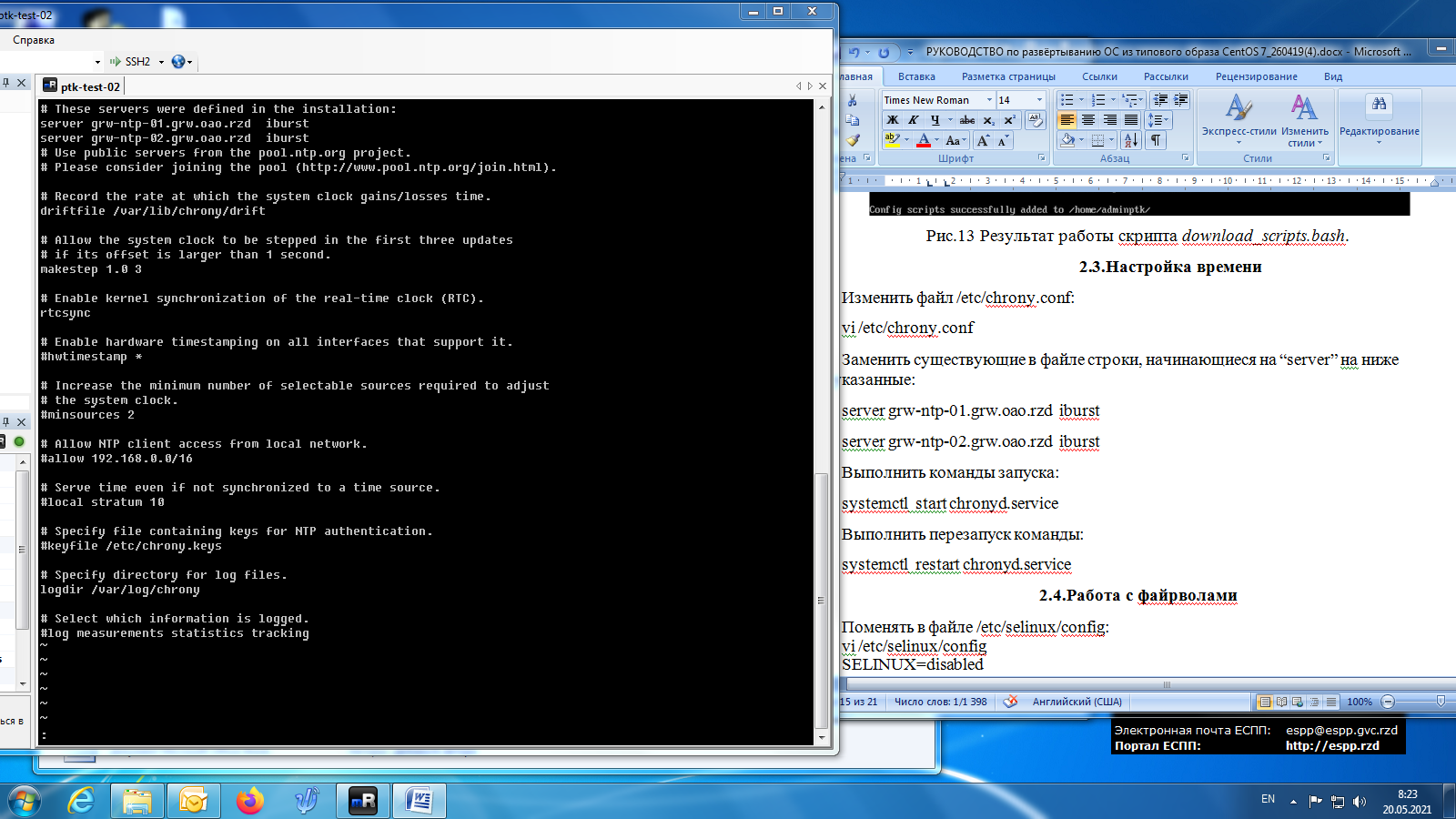
Изменить файл /etc/chrony.conf:

vi /etc/chrony.conf

Заменить существующие в файле строки, начинающиеся на “server” на ниже указанные:

server grw-ntp-01.grw.oao.rzd  iburst

server grw-ntp-02.grw.oao.rzd  iburst

  
Рисунок 12. Отрывок файла chrony.conf

Выполнить команду запуска:

systemctl start chronyd.service

Выполнить перезапуск сервиса:

systemctl restart chronyd.service

# Работа с файрволами

Выполнить редактирование файла /etc/selinux/config:

vi /etc/selinux/config

SELINUX=disabled

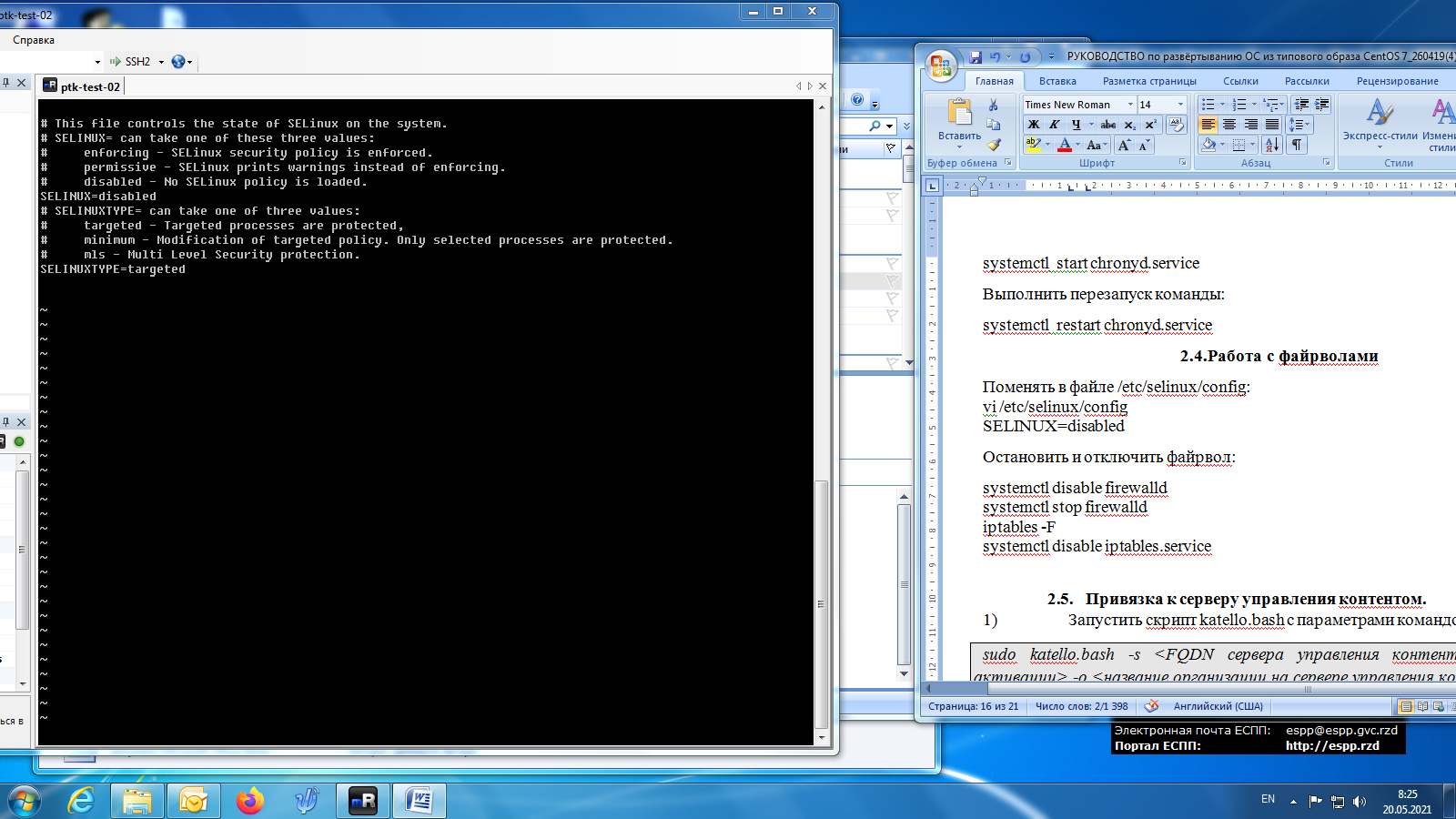


Рисунок 13. Отрывок файла

Остановить и отключить файрвол, поочередно выполнив команды:

systemctl stop firewalld

systemctl disable firewalld

iptables -F

systemctl disable iptables.service

# Привязка к серверу управления контентом (репозиторию)

1. Для того, чтобы подключиться к интернет-репозиторию, нужно настроить прокси для wget и yum. Подключение к интернет-репозиторию нежелательно!

Выполнить команду:

vi /etc/wgetrc

В документе добавить строки:

http\_proxy=http://10.24.222.230:8080

https\_proxy=http://10.24.222.230:8080

proxy\_user=nefed

proxy\_passwd=Berkley

 Выполнить команду:

vi /etc/yum.conf

В документе добавить строки:

proxy=http://10.24.222.230:8080

proxy\_username=nefed

proxy\_password=berkley

**Привязка к РЖД-репозиторию**

Запустить скрипт katello.bash с параметрами командой:

sudo katello.bash -s <FQDN сервера управления контентом> -k <ключ активации> -o <название организации на сервере управления контентом>

Скрипт запустит процесс регистрации, а после предложит обновить пакеты до последней версии (включая ядро ОС), а может и не предложить! При запросе на обновление и перезагрузку, необходимо ввести ‘y’. Консольный вывод скрипта показан на рисунке 12.

Скрипт находится на сервере 10.24.223.220:

scp root@10.24.223.220:/install/katello.bash /opt

Скопировать командой, пароль: **N0veLL**

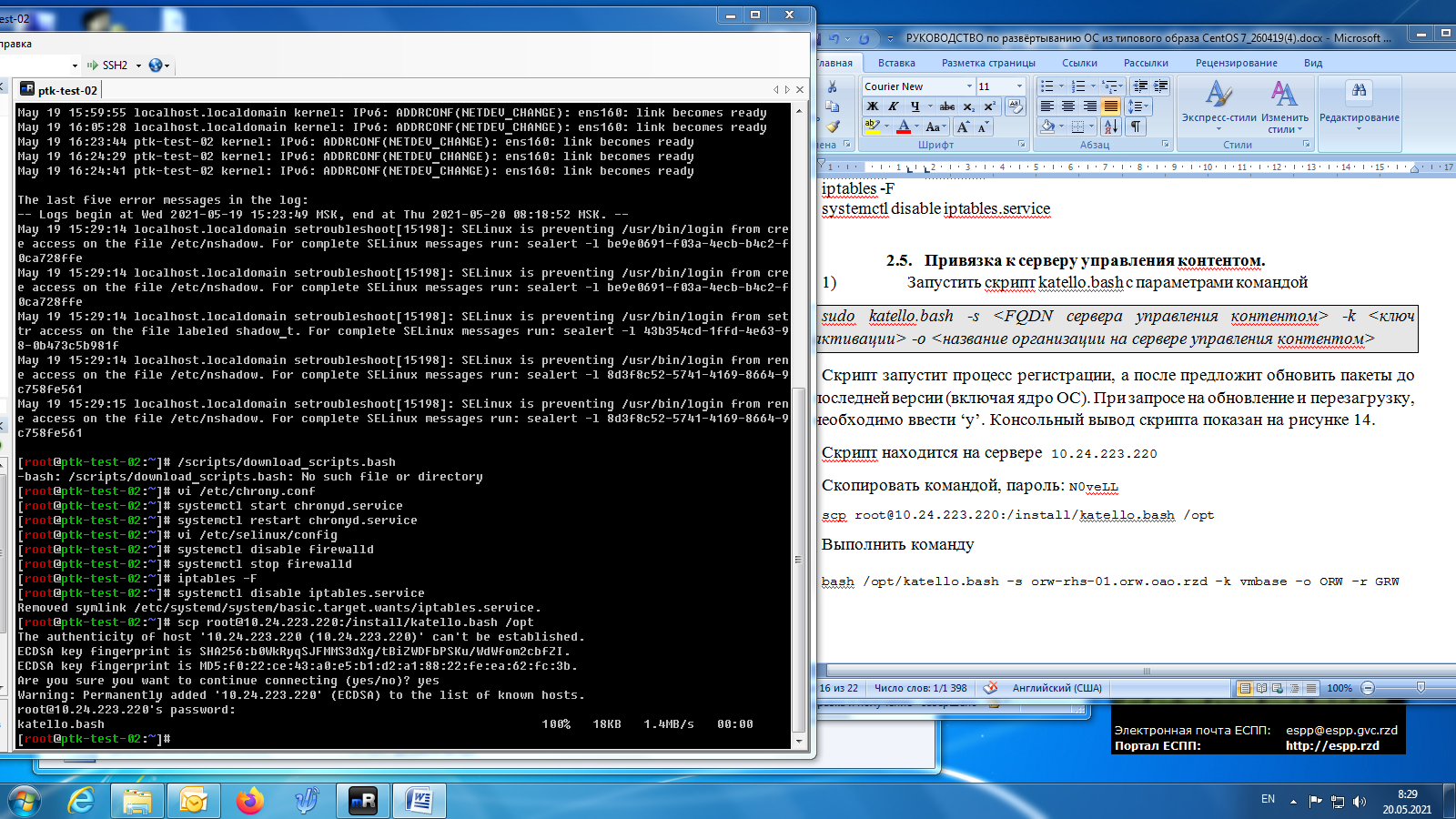


Рисунок 14. промежуточный результат подключения к серверу

Для подключения к репозиторию Нижегородского ИВЦ выполнить команду:

bash /opt/katello.bash -s orw-rhs-01.orw.oao.rzd -k vmbase -o ORW -r GRW

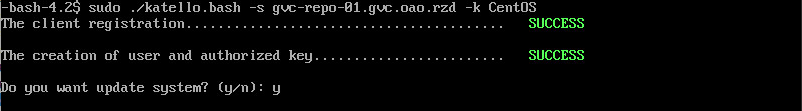


Рисунок 15. Промежуточный вывод скрипта *katello.bash*.

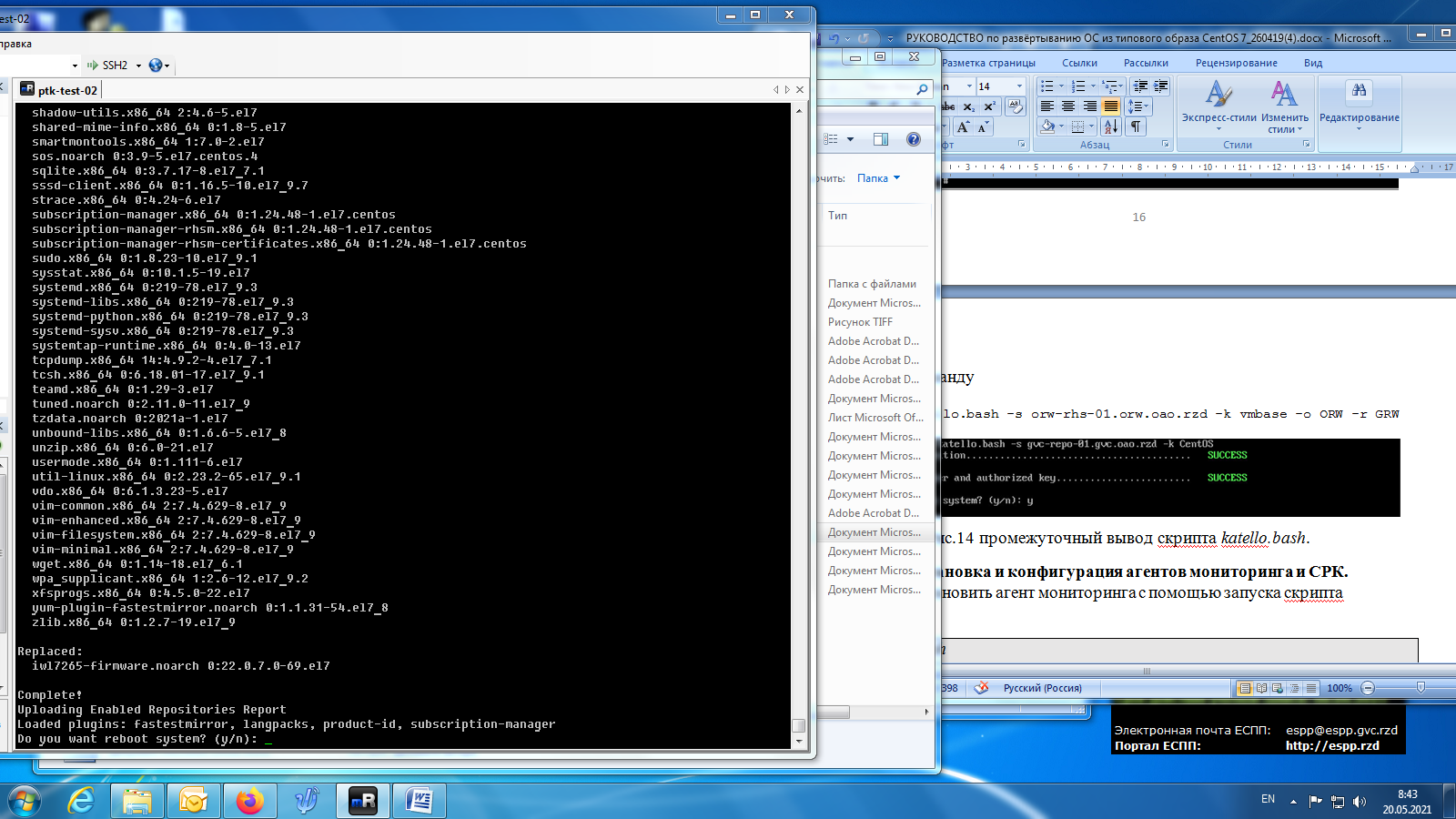


Рисунок 16. Конечный вывод скрипта *katello.bash*.

# Настройка сервиса записи логов Journald.

В файле конфигурации демона /etc/systemd/journald.conf необходимо сделать следующие настройки:

Storage=persistent

Compress=yes

SplitMode=none

SystemMaxUse=600M

systemctl restart systemd-journald

# Установка пакетов для анализа производительности сервера.

Установить пакеты для анализа производительности сервера:

yum install sysstat htop atop apachetop iotop iftop mc ftp telnet bash-completion

# Блокировка стандартных пользователей.

Заблокировать учетные записи *adminptk* и *adminos*, и создать персональные учетные записи для администраторов отдела ПТК

|  |
| --- |
| passwd -l adminptk |
| passwd -l adminos |

# Отключение ssh для пользователя root.

Убедиться, что подключение по протоколу *ssh* для пользователя *root* отключен

vi /etc/ssh/sshd\_config

PermitRootLogin no