



МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное образовательное учреждение высшего
образования

РТУ МИРЭА

«МИРЭА – Российский технологический университет»

Институт кибербезопасности и цифровых технологий

Кафедра КБ-2 «Информационно-аналитические системы кибербезопасности»

Практическая работа № 4

«Методы компрометации операционных систем Linux и Windows при наличии
физического доступа. Способы защиты от них»

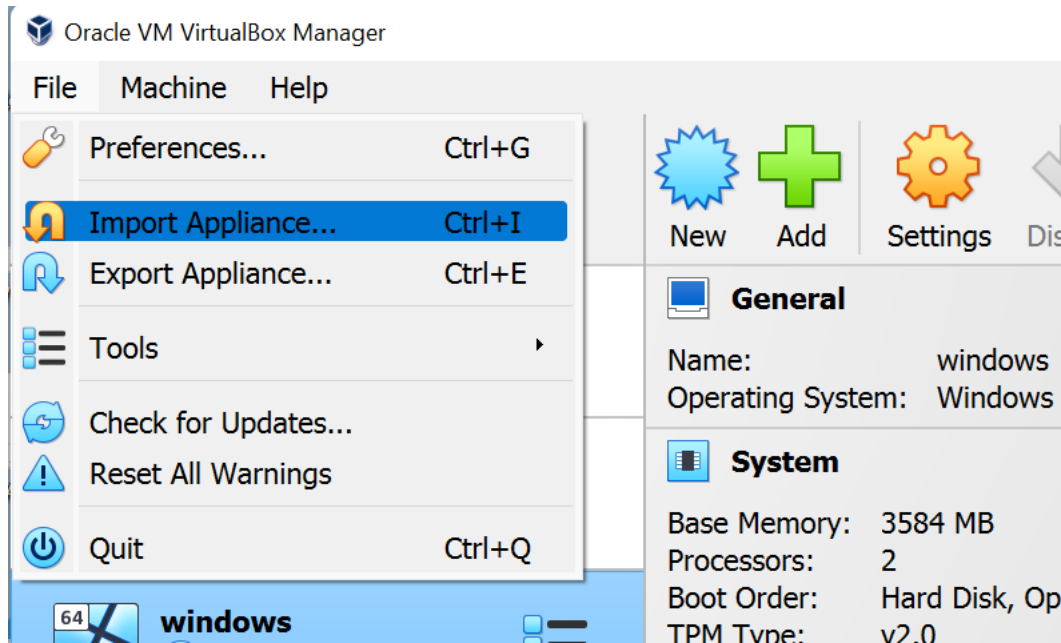
по дисциплине «Безопасность операционных систем»

Москва

2023

1. Подготовка рабочего окружения

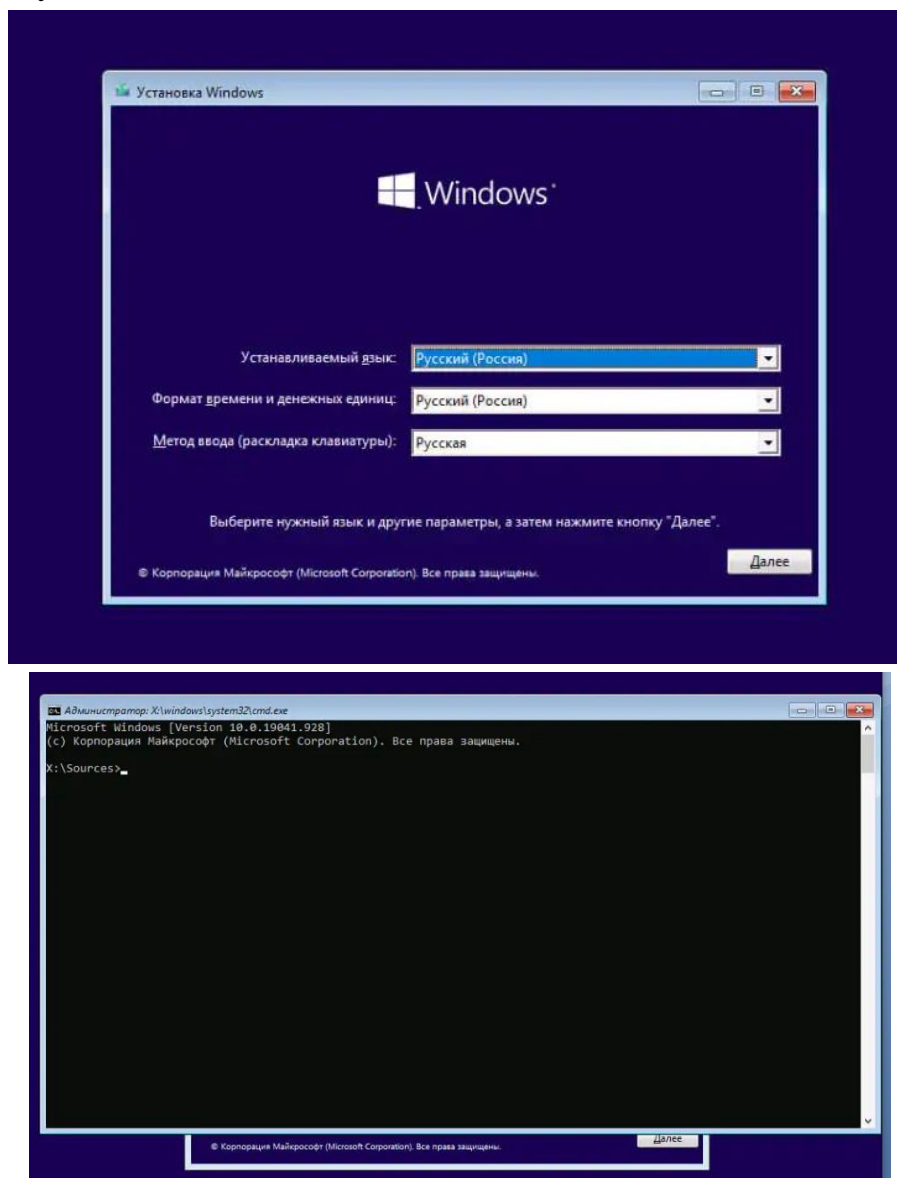
Из сетевой папки скачайте файлы виртуальных машин, необходимых для выполнения практического занятия Windows_pro.ova и Ubuntu.ova (сначала windows!!!). В VirtualBox выберите меню как показано на рисунке



Импортируйте сначала Windows_pro.ova, затем Ubuntu.ova. Таким образом Вы развернули 2 виртуальные машины и мы готовы приступить к практическому занятию №4.

1. Использование установочного диска (образа) для компрометации ОС Windows

Смонтируйте установочный образ ОС Windows в CD-привод виртуальной машины Windows_pro и загрузитесь с него. Когда вы увидите начальный экран установки Windows, нажмите сочетание клавиш *shift+F10*, чтобы открыть командную строку.



В Windows есть функция, которая называется «залипание клавиш», которую можно открыть, нажав 5 раз клавишу *Shift* на экране входа Windows 10. Заменяя исполняемый файл функции «залипание клавиш» (*sethc.exe*), ссылкой на исполняемый файл командной строки (*cmd.exe*), вы можете запустить командную строку прямо с экрана входа в систему.

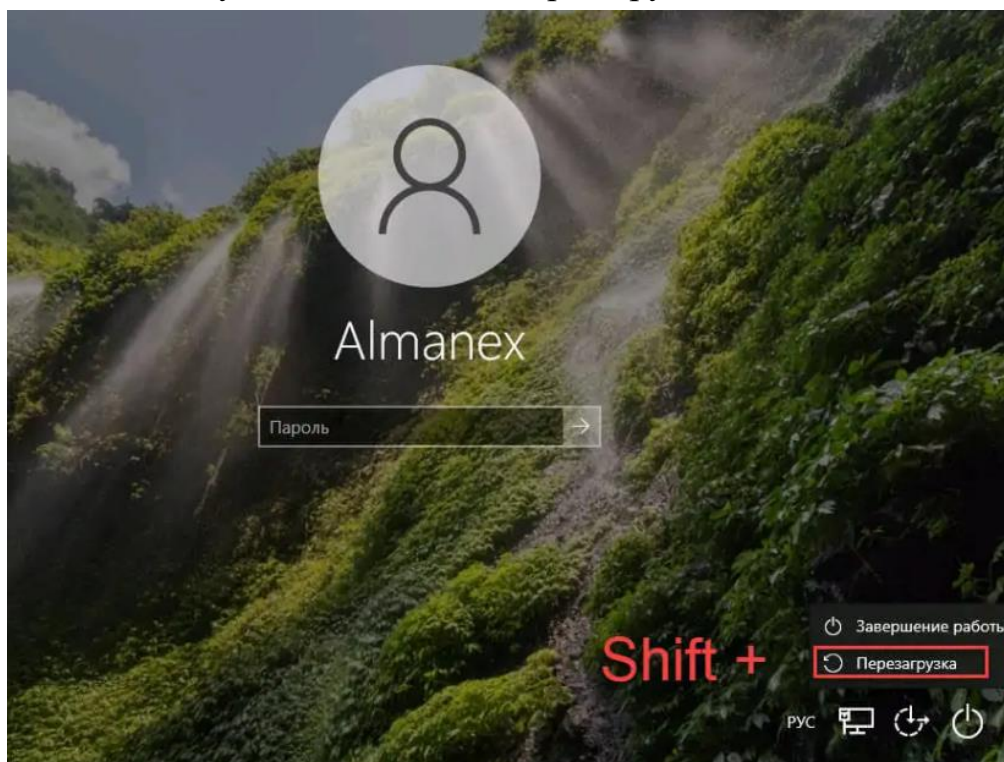
Для этого выполните следующие команды:

```
move c:\windows\system32\sethc.exe c:\windows\system32\sethc_orig.exe
```

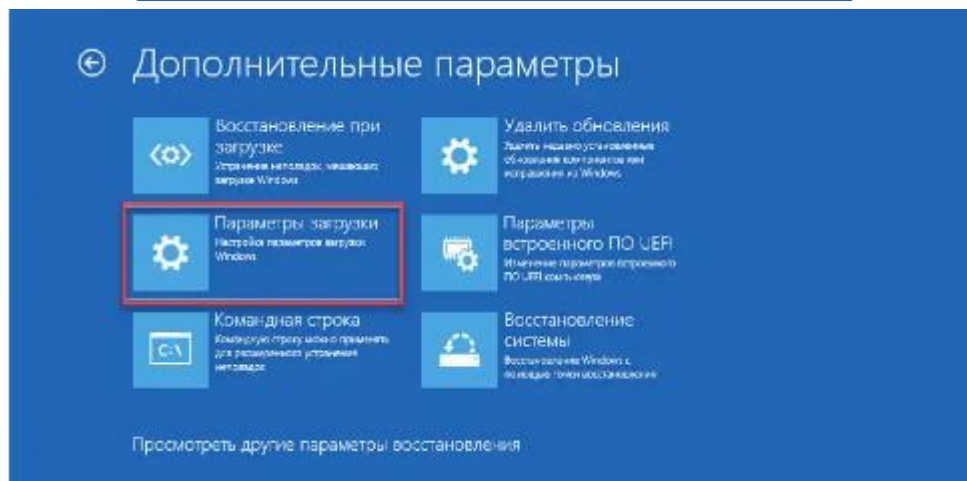
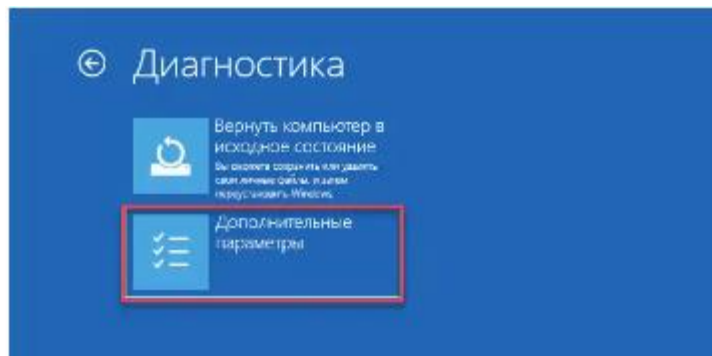
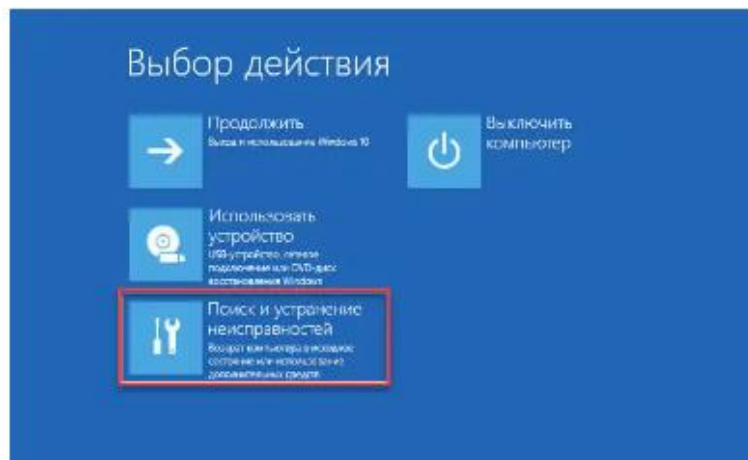
```
copy c:\windows\system32\cmd.exe c:\windows\system32\sethc.exe
```

Далее перезагрузитесь.

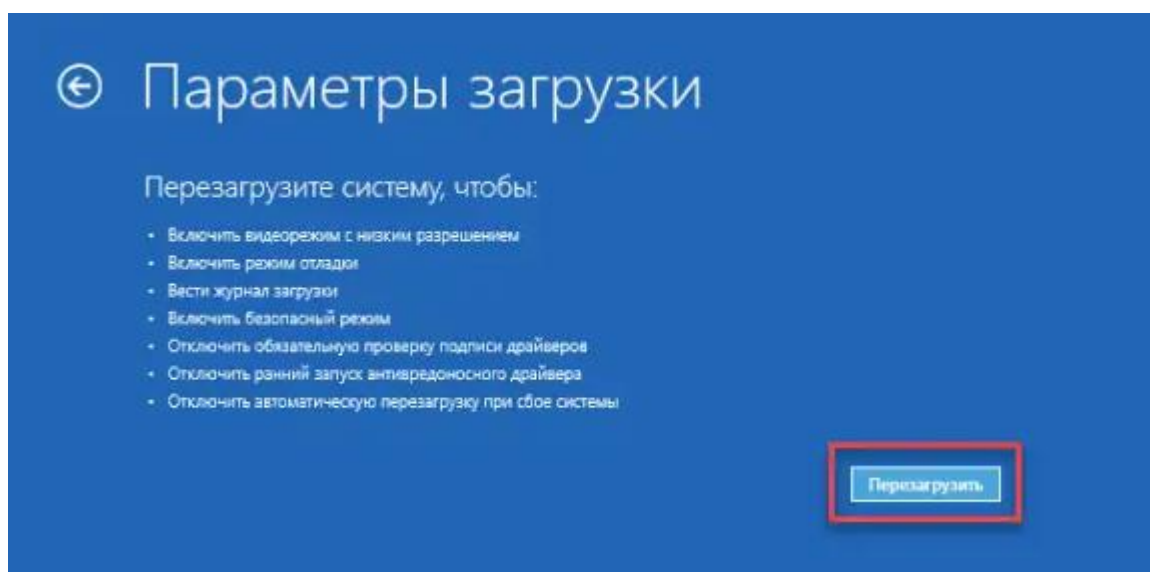
В предыдущей версии Windows вы могли просто запустить переименованный ярлык для доступа к командной строке прямо с экрана входа в систему. Однако «Microsoft Defender» теперь блокирует эти попытки, поэтому требуются дополнительные действия. Нам придется загрузиться в безопасный режим. Для этого кликните меню «Питание» в правом нижнем углу экрана входа в систему. Затем, удерживая клавишу Shift, нажмите «Перезагрузить».



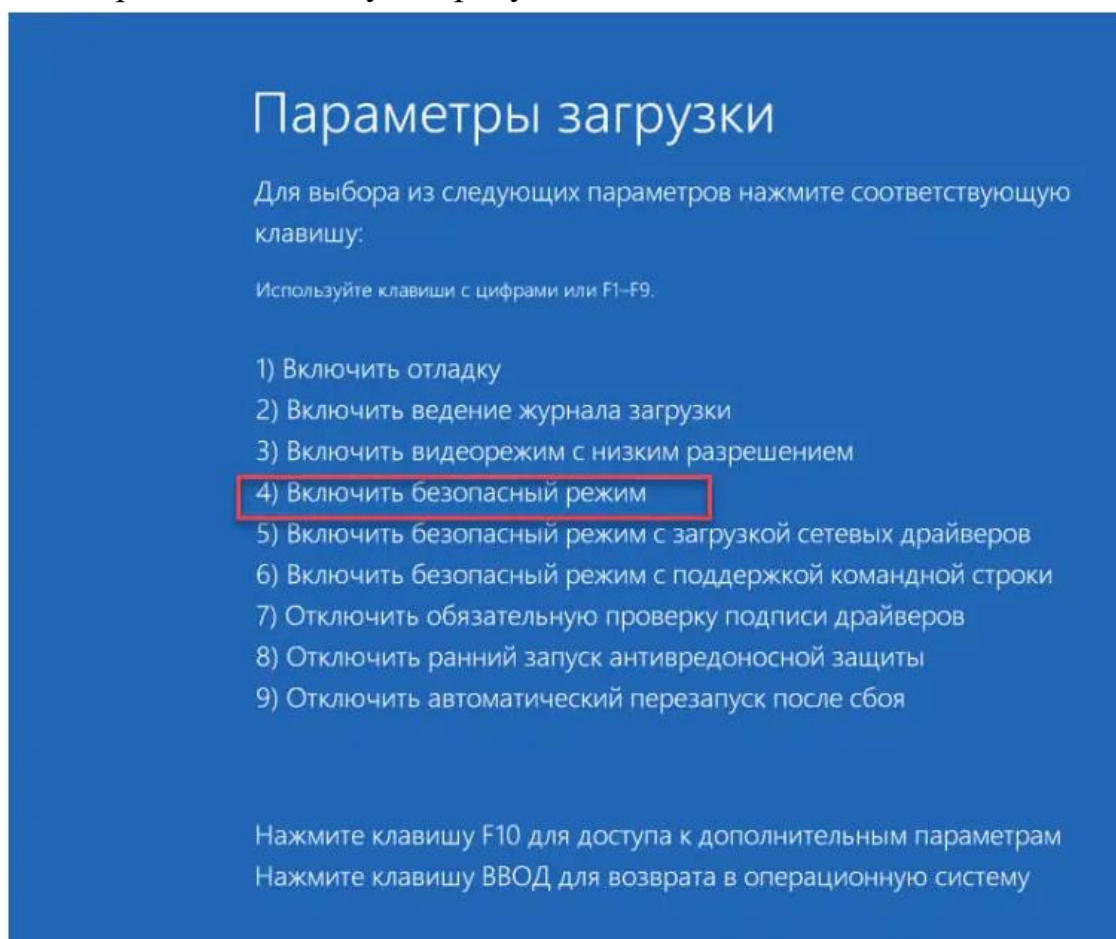
Затем вы увидите меню дополнительных настроек. Кликните «Поиск и устранение неисправностей» → «Дополнительные параметры» → «Параметры загрузки».



Нажмите кнопку «Перезагрузить» Ваш компьютер перезагрузится, затем спросит, какой вариант запуска вы хотите использовать.

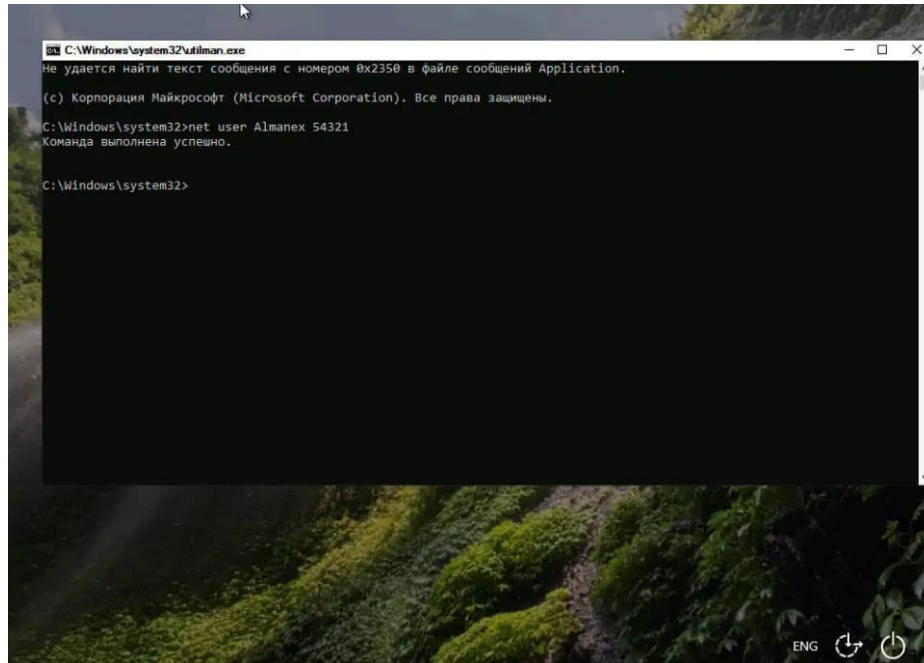


Нажмите клавишу 4, чтобы выбрать Безопасный режим. Это загрузит Windows с минимальным набором драйверов и служб, не позволяя Защитнику Microsoft блокировать командную строку.



После перезагрузки на экране входа в Windows в безопасный режим, нажмите 5 раз клавишу «Shift». Это должно вызвать командную строку с правами

администратора.



Теперь вы можете сбросить пароль своей учетной записи или создать новую учетную запись.

Отчёт:

- Прodelайте процедуру компрометации ОС тем же методом, но без использования функции «залипание клавиш», создайте пользователя baso-0*-1-фамилия. (screenshot)

2. Методы компрометации ОС Linux при наличии физического доступа

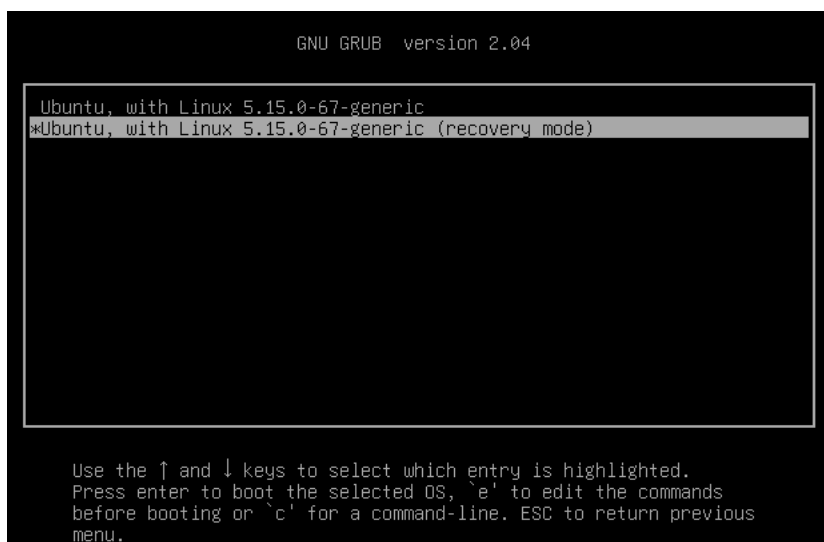
2.1 Есть доступ к меню выбора операционных систем GRUB

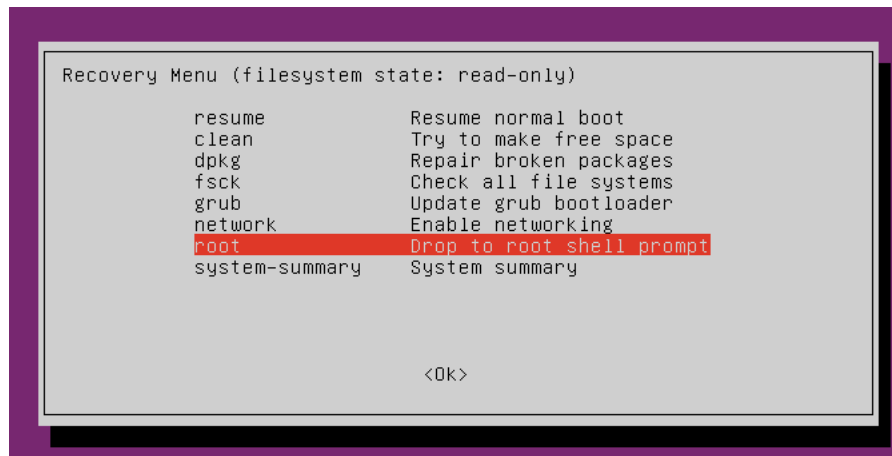
GRUB (*GRand Unified Bootloader*) программа-загрузчик операционных систем. **GRUB** позволяет пользователю при загрузке задавать произвольные параметры и передавать их в ядро Multiboot-совместимой ОС для дальнейшей обработки.

2.1.1 Recovery mode

Recovery mode встроенный режим восстановления ОС. В этом режиме операционная система загружает только базовые службы, переходит в режим командной строки и выполняет вход под пользователем *root*.

Если у вас одна операционная система (как у нас), то для отображения меню GRUB при загрузке необходимо удерживать кнопку *Shift*. В меню GRUB выбираем *advanced options*, далее выбираем строчку с надписью *recovery mode*, далее в *recovery menu* выбираем пункт *root*. У вас запустится консоль с правами *root*.





Теперь мы можем выполнять команды, но для того чтобы результаты сохранялись необходимо перевести корневую файловую систему в режим записи командой

```
mount -o remount,rw /
```

Теперь для установки нового пароля или создания нового пользователя достаточно набрать команду

```
passwd имя_пользователя или useradd имя_пользователя
```

Для завершения работы перезагрузитесь командой *reboot*.

2.1.1 Изменение параметров загрузки

В загрузчике Grub вы можете менять параметры, передаваемые ядру. Например, вы можете передать параметр *init*, который попросит ядро выполнить вместо системы инициализации вашу команду.

Войдите в меню GRUB. Выберите строчку с вашей системой, нажмите *e*. Откроется редактор конфигурации выбранной секции. Здесь необходимо найти строку, начинающуюся со слова *linux*. В конце неё есть два параметра: *quiet splash* (на рисунке подчёркнуты красным).

```
GNU GRUB version 2.04

insmod ext2
set root='hd0,msdos5'
if [ x$feature_platform_search_hint = xy ]; then
  search --no-floppy --fs-uuid --set=root --hint-bios=hd\
0,msdos5 --hint-efi=hd0,msdos5 --hint-baremetal=ahci0,msdos5 f6af04e9-8\
b7a-454f-a05f-46a6249c363a
else
  search --no-floppy --fs-uuid --set=root f6af04e9-8b7a-\
454f-a05f-46a6249c363a
fi
echo      'Loading Linux 5.15.0-67-generic ...'
linux     /boot/vmlinuz-5.15.0-67-generic root=UUID=f\
6af04e9-8b7a-454f-a05f-46a6249c363a ro quiet splash $vt_handoff_
echo      'Loading initial ramdisk ...'
initrd    /boot/initrd.img-5.15.0-67-generic

Minimum Emacs-like screen editing is supported. TAB lists
completions. Press Ctrl-x or F10 to boot, Ctrl-c or F2 for a
command-line or ESC to discard edits and return to the GRUB
menu.
```

Первый параметр указывает на минимальный вывод информации во время загрузки, второй параметр указывает на отображение заставки. Заставку необходимо отключить, иначе можем не увидеть консоль. Вместо этих параметров напишем *verbose init=/bin/bash*, далее нажимаем *ctrl+x* для загрузки с текущей конфигурацией.

```
Ubuntu [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help

[ 1.605445] usbcore: registered new interface driver usbhid
[ 1.605943] usbhid: USB HID core driver
[ 1.614179] e1000 0000:00:03:0 eth0: (PCI:33MHz:32-bit) 08:00:27:ce:ce:9d
[ 1.614540] e1000 0000:00:03:0 eth0: Intel(R) PRO/1000 Network Connection
[ 1.617315] e1000 0000:00:03:0 enp0s3: renamed from eth0
[ 1.617675] input: VirtualBox USB Tablet as /devices/pci0000:00/0000:00:06.0/
usb2/2-1/2-1:1.0/0003:80EE:0021.0001/input/input6
[ 1.618997] hid-generic 0003:80EE:0021.0001: input,hidraw0: USB HID v1.10 Mou
se [VirtualBox USB Tablet] on usb-0000:00:06.0-1/input0
Begin: Loading essential drivers ... done.
Begin: Running /scripts/init-premount ... done.
Begin: Mounting root file system ... Begin: Running /scripts/local-top ... done.
Begin: Running /scripts/local-premount ... done.
Begin: Will now check root file system ... fsck from util-linux 2.34
[/usr/sbin/fsck.ext4 (1) -- /dev/sda5] fsck.ext4 -a -C0 /dev/sda5
/dev/sda5: clean, 161291/1605632 files, 2109307/6421760 blocks
done.
[ 1.703566] EXT4-fs (sda5): mounted filesystem with ordered data mode. Opts:
(null). Quota mode: none.
done.
Begin: Running /scripts/local-bottom ... done.
Begin: Running /scripts/init-bottom ... done.
bash: cannot set terminal process group (-1): Inappropriate ioctl for device
bash: no job control in this shell
root@(none):/#
```

Теперь можно установить новый пароль пользователя или добавить нового пользователя.

Если возникла ошибка, то скорее всего она связана с тем, что раздел в котором мы хотим сделать изменения примонтирован в режиме «только для

чтения». Перемонтируйте его в режиме «чтение-запись».

2.1.3 Однопользовательский режим

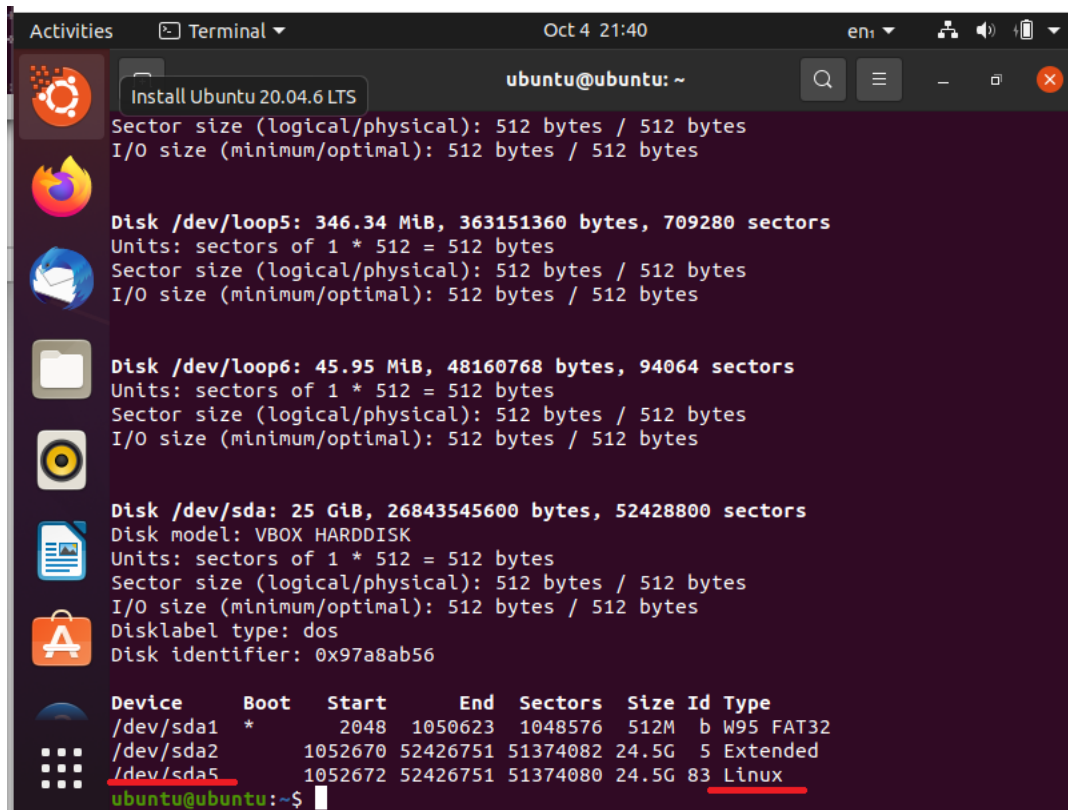
Однопользовательский режим, также известный как режим обслуживания, представляет собой режим, в котором ОС многопользовательского компьютера загружается в одного суперпользователя.

Войдите в меню GRUB. Выберите строчку с вашей системой, нажмите *e*. Откроется редактор конфигурации выбранной секции. Здесь необходимо найти строку, начинающуюся со слова *linux*. В конце строки добавьте *single*, далее нажмите *ctrl+x* для загрузки в однопользовательском режиме.

Теперь можно установить новый пароль пользователя или добавить нового пользователя.

2.2 Нет доступа к меню выбора операционных систем GRUB

Если у вас по тем или иным причинам отключён загрузчик операционных систем GRUB, то пароль можно сбросить с помощью любого LiveCD с Linux. Для этого необходимо загрузиться с LiveCD, в терминале командой *fdisk -l* узнать раздел с нашей ОС



```
ubuntu@ubuntu: ~  
Sector size (logical/physical): 512 bytes / 512 bytes  
I/O size (minimum/optimal): 512 bytes / 512 bytes  
  
Disk /dev/loop5: 346.34 MiB, 363151360 bytes, 709280 sectors  
Units: sectors of 1 * 512 = 512 bytes  
Sector size (logical/physical): 512 bytes / 512 bytes  
I/O size (minimum/optimal): 512 bytes / 512 bytes  
  
Disk /dev/loop6: 45.95 MiB, 48160768 bytes, 94064 sectors  
Units: sectors of 1 * 512 = 512 bytes  
Sector size (logical/physical): 512 bytes / 512 bytes  
I/O size (minimum/optimal): 512 bytes / 512 bytes  
  
Disk /dev/sda: 25 GiB, 26843545600 bytes, 52428800 sectors  
Disk model: VBOX HARDDISK  
Units: sectors of 1 * 512 = 512 bytes  
Sector size (logical/physical): 512 bytes / 512 bytes  
I/O size (minimum/optimal): 512 bytes / 512 bytes  
Disklabel type: dos  
Disk identifier: 0x97a8ab56  
  
Device      Boot      Start          End      Sectors  Size Id Type  
/dev/sda1   *            2048       1050623     1048576   512M  b W95 FAT32  
/dev/sda2                1052670     52426751    51374082   24.5G  5 Extended  
/dev/sda5                1052672     52426751    51374080   24.5G  83 Linux  
ubuntu@ubuntu:~$
```

Наша ОС находится в разделе */dev/sda5*, с типом раздела Linux.

Примонтируем наш корневой раздел командой

```
mount /dev/sda5 /media/sda5
```

Далее с помощью команды `chroot`, которая используется для открытия оболочки с корневым каталогом, отличным от используемого в текущей оболочке, и мы передадим папку, в которую смонтировали жесткий диск

```
chroot /media/sda5
```

chroot операция изменения корневого каталога в Unix-подобных операционных системах. Программа, запущенная с изменённым корневым каталогом, будет иметь доступ только к файлам, содержащимся в данном каталоге. Поэтому, если нужно обеспечить программе доступ к другим каталогам или файловым системам (например, `/proc`), нужно заранее примонтировать в целевом каталоге необходимые каталоги или устройства.

Теперь можно установить новый пароль пользователя или добавить нового пользователя.

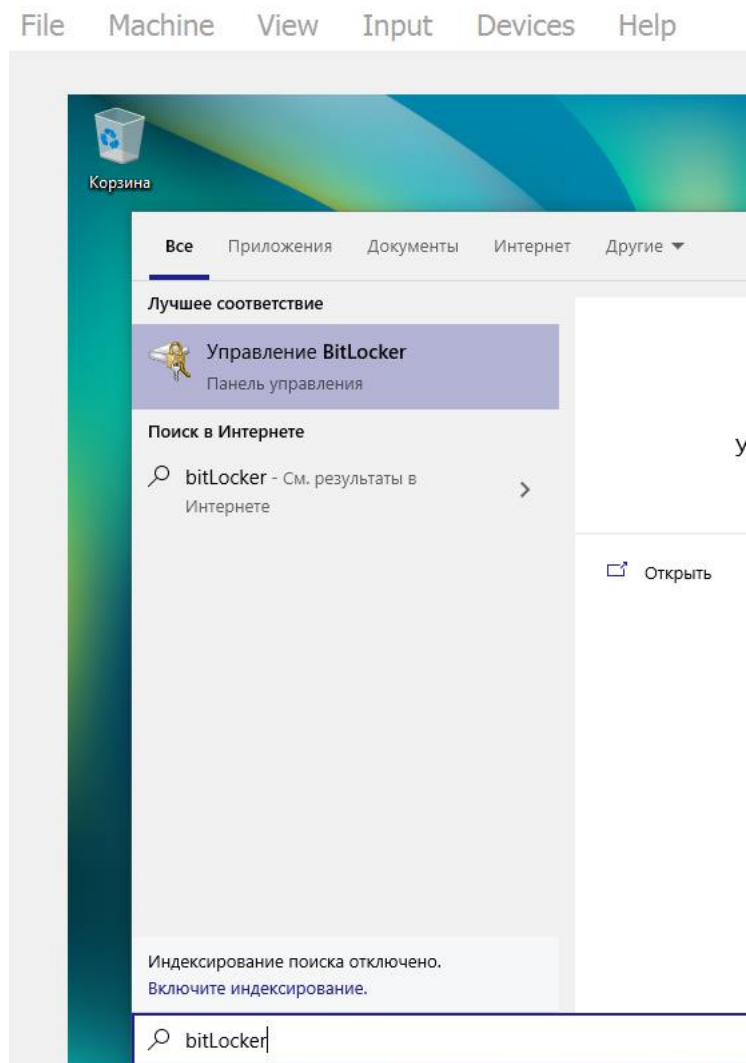
Отчёт:

- Выполните все упражнения, создавая в каждом нового пользователя baso-0*-21-фамилия-№ упражнения (screenshot).

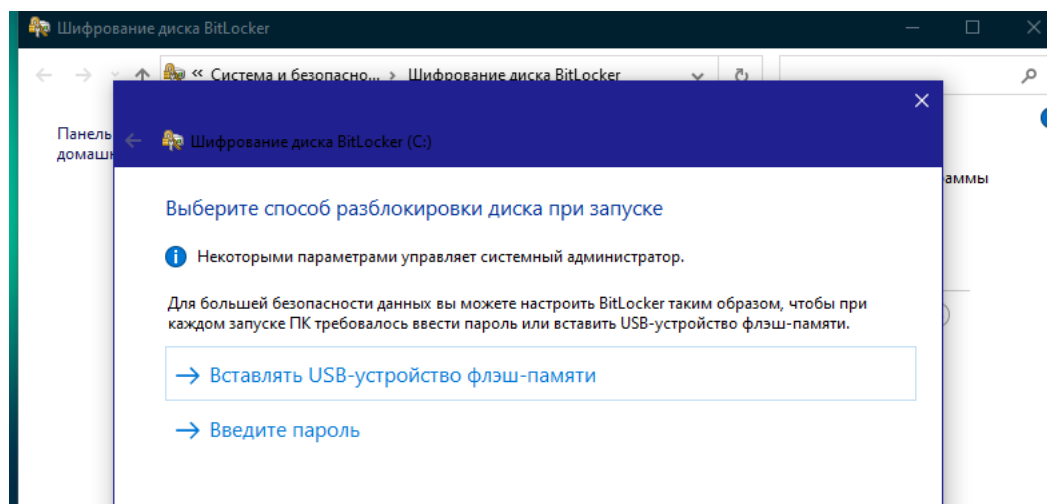
3. Методы защиты ОС от атак с наличием физического доступа к устройству

3.1 Шифрование разделов ОС Windows встроенным средством BitLocker

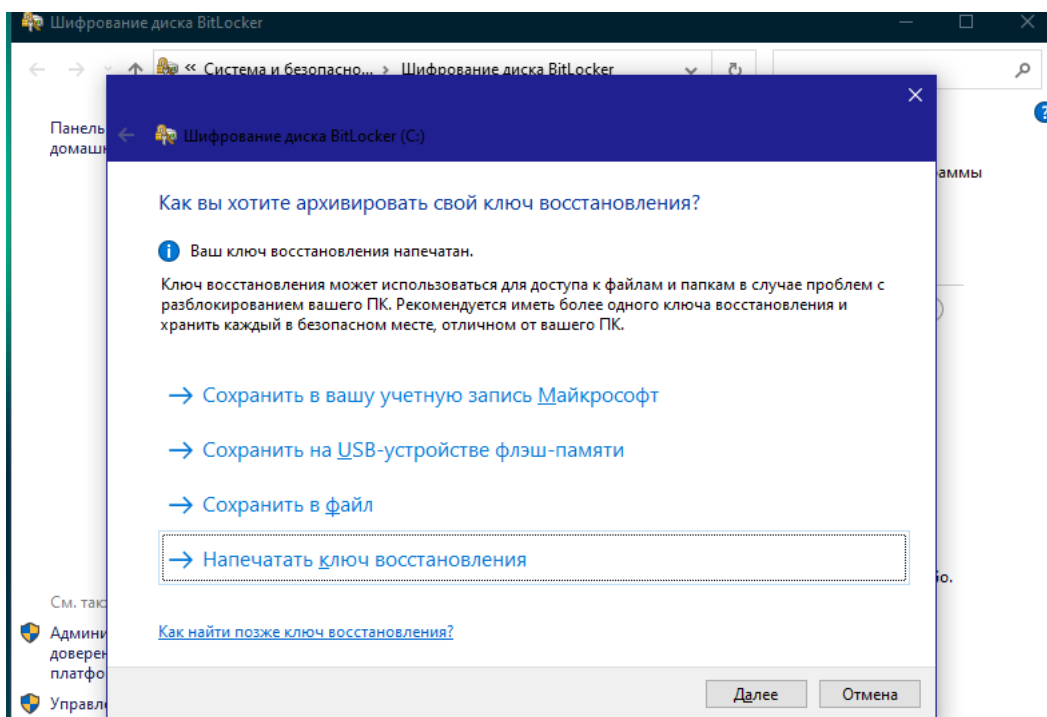
В поиске наберите BitLocker и перейдите в оснастку управления настройками BitLocker



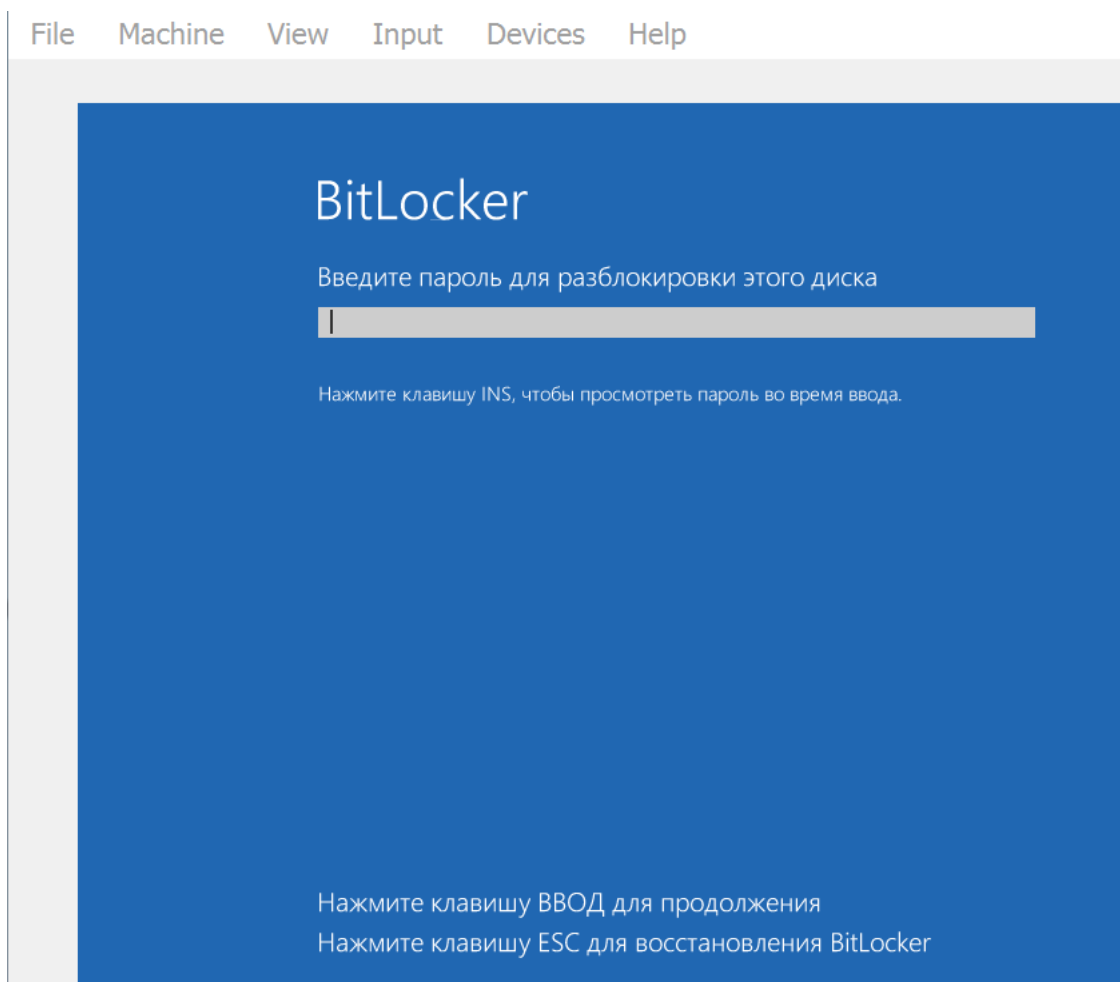
Далее нажимаем «включить BitLocker», далее выбираем режим разблокировки «Введите пароль», как показано на рисунке



Устанавливаем пароль, выбираем вариант восстановления ключа «Напечатать ключ восстановления»



Сохраняем его на диск в формате pdf, далее выбираем «только занятое пространство», выбираем «совместимый метод шифрования» и перезагружаем ОС. При старте ОС увидим запрос на ввод пароля для расшифровки разделов жесткого диска



3.2 Защита загрузчика GRUB

Для защиты загрузчика необходимо добавить в конфигурационный файл загрузчика `/etc/grub.d/00_header` строки следующие после `##Passw`

```
GNU nano 4.8 /etc/grub.d/00_header Modified
if [ "x${GRUB_BUTTON_CMOS_ADDRESS}" != "x" ] && [ "x${GRUB_BUTTON_CMOS_CLEAN}" = "x" ] ; then
    cat <<EOF
cmosclean ${GRUB_BUTTON_CMOS_ADDRESS}
EOF
fi

# Play an initial tune
if [ "x${GRUB_INIT_TUNE}" != "x" ] ; then
    echo "play ${GRUB_INIT_TUNE}"
fi

if [ "x${GRUB_BADRAM}" != "x" ] ; then
    echo "badram ${GRUB_BADRAM}"
fi

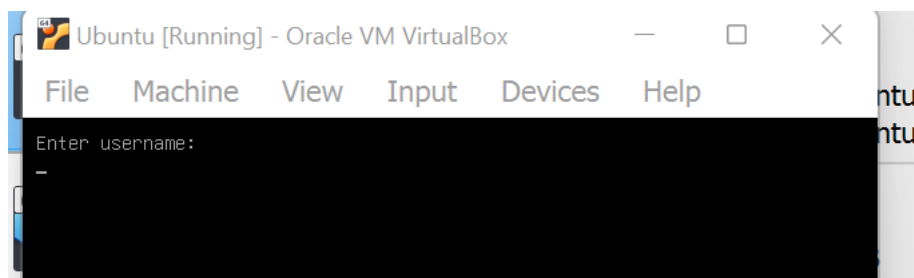
## Passw
cat << EOF
set superusers="root"
password_pbkdf2 root grub.pbkdf2.sha512.10000.D12DDF19881F32C9E4684EA128D422E8>
EOF
```

где значение `password_pbkdf2` (пароль на загрузчик) генерируется командой `password_pbkdf2`

```
Activities Terminal Oct 5 06:29
user@user-PC: ~
user@user-PC: ~
user@user-PC:~$ grub-mkpasswd-pbkdf2
Enter password: 
```

```
Activities Terminal Oct 5 06:29
user@user-PC: ~
user@user-PC: ~ root@user-PC: /home/user
user@user-PC:~$ grub-mkpasswd-pbkdf2
Enter password:
Reenter password:
PBKDF2 hash of your password is grub.pbkdf2.sha512.10000.D9DAFFB3379A8D60ACACD1
A Files 876AA5EC6F7E4B64FDB626B7A3C93BF35ADD095A52E61CD19D80150B04973A3E0541988E1
A3C8E3C4758645D3C184CEAB17.FCFC2A6D28DA4E598912428038244B1CAF002AD8162802B92E7
9E239B04683DB770A2296FCF8CC2A73B1D8AADC5C35DAF31CB33EB34F0F8D8F5C6894EF307829
user@user-PC:~$
```

Полученное значение необходимо вставить в конфигурационный файл. Далее обновляем конфигурацию загрузчика командой `update-grub` и перезагружаемся.



Теперь загрузчик защищен.

Отчёт:

- Ознакомьтесь с материалом и распишите возможности BitLocker.
- Напишите методы шифрования разделов в ОС Linux (какие программы).