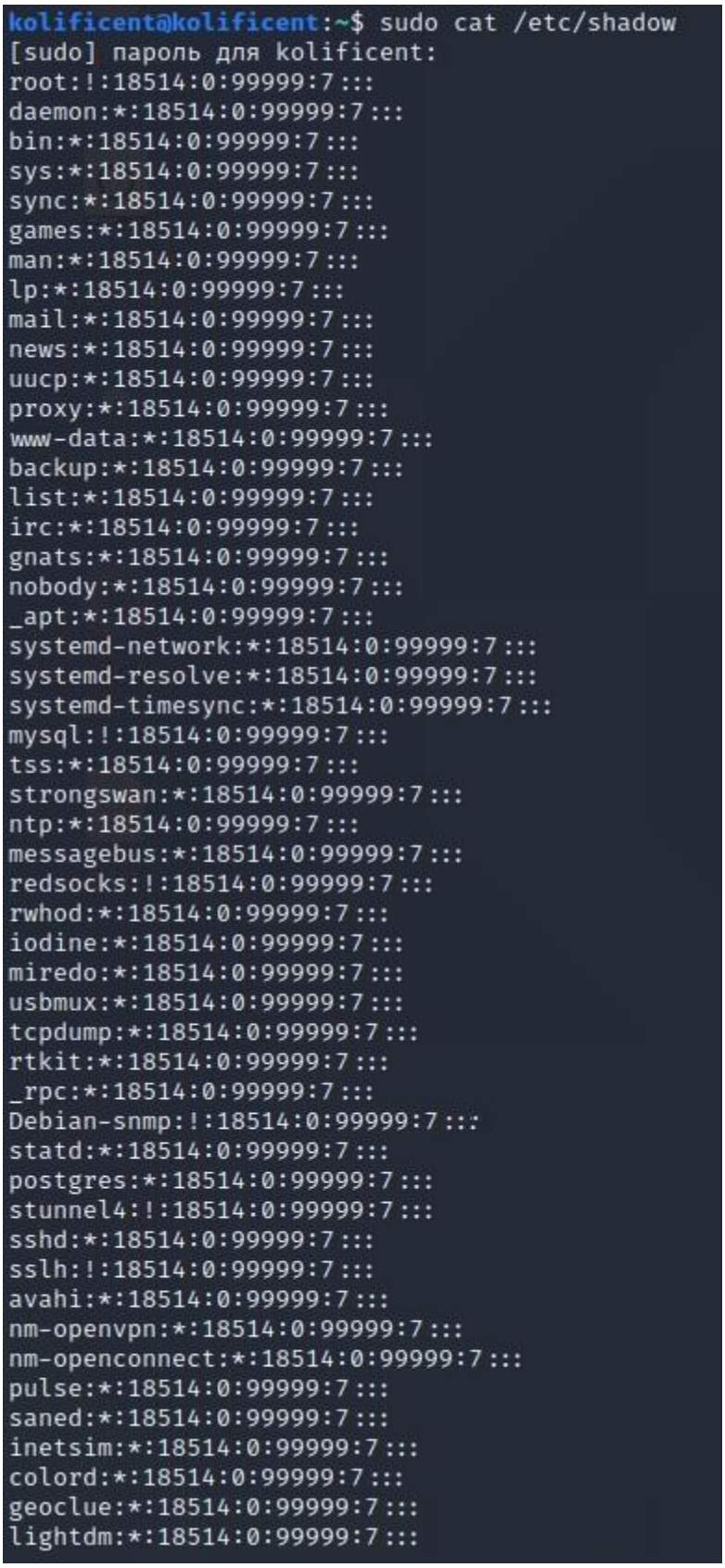
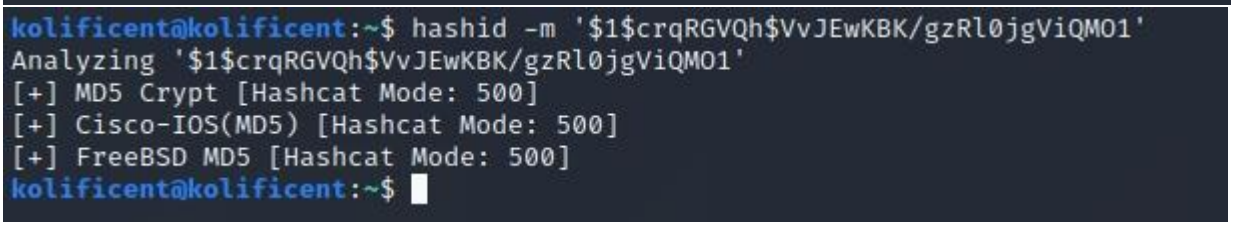
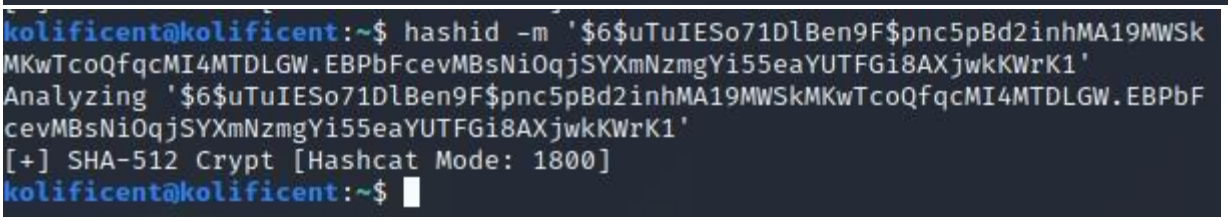
Булгаков Алексей БАСО-02-20







ID – 6

SALT – uTuIESo71DlBen9F

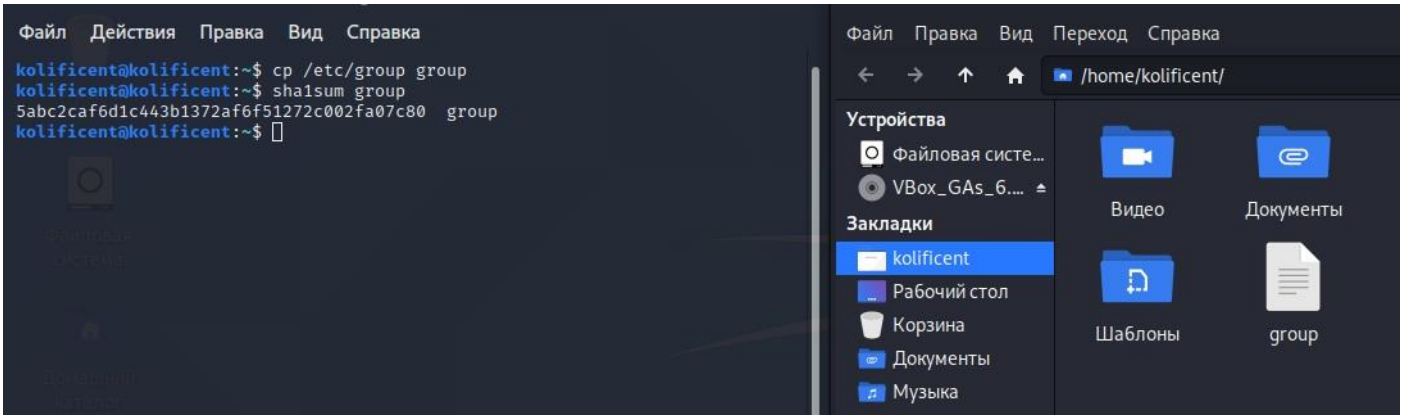
ENCRYPTED - pnc5pBd2inhMA19MWSkMKwTcoQfqcMI4MTDLGW.EBPbFcevMBsNiOqjSYXmNzmgYi55eaYUTFGi8AXjwkKWrK1

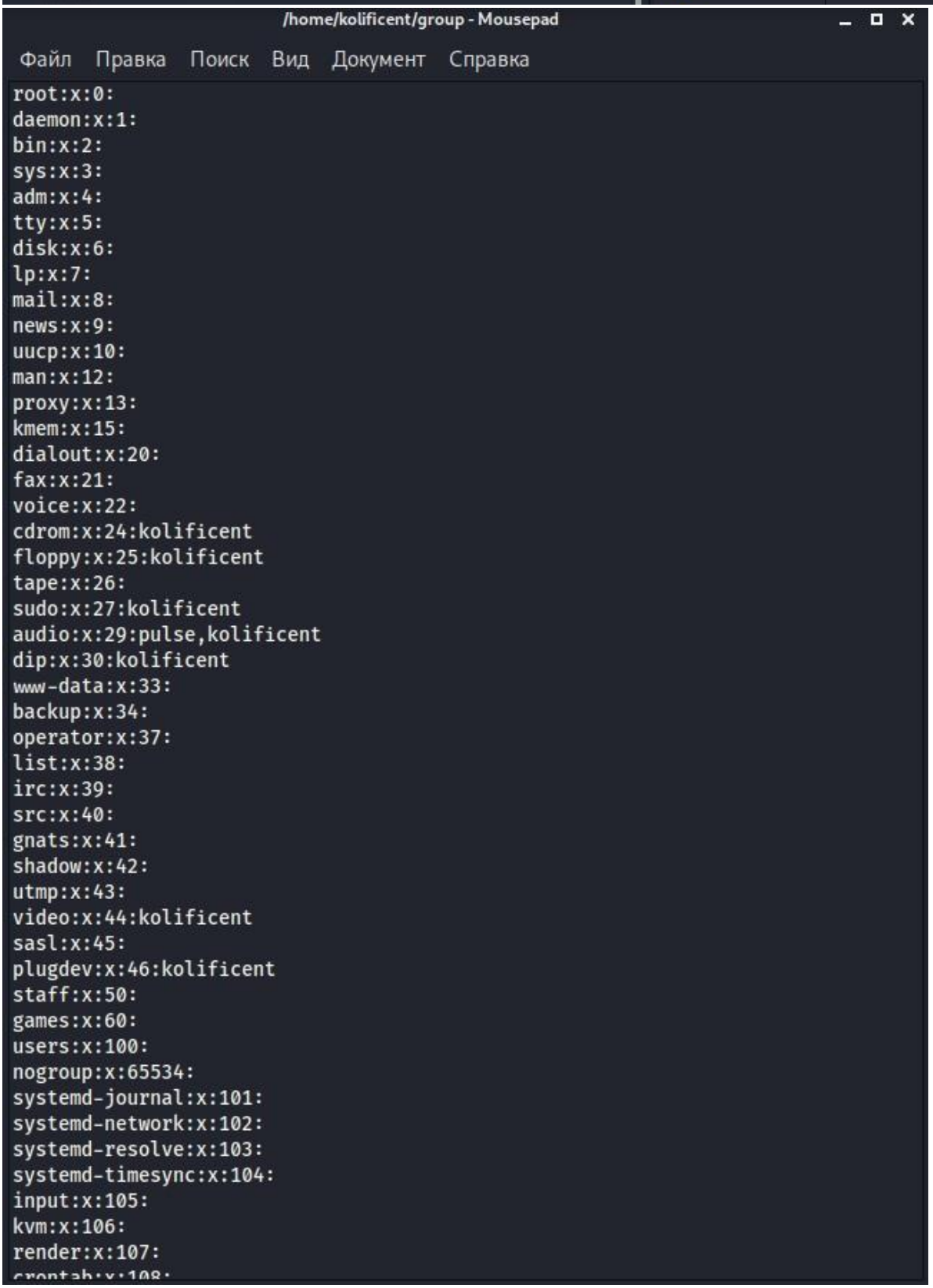
```
kolificent@kolificent:~$ sudo useradd superuser
[sudo] пароль для kolificent:
Попробуйте ещё раз.
[sudo] пароль для kolificent:
Попробуйте ещё раз.
[sudo] пароль для kolificent:
sudo: 3 incorrect password attempts
kolificent@kolificent:~$ :/
bash: :/: Нет такого файла или каталога
kolificent@kolificent:~$ sudo useradd superuser
[sudo] пароль для kolificent:
kolificent@kolificent:~$ user passwd usersuper
bash: user: команда не найдена
kolificent@kolificent:~$ sudo passwd superuser
Новый пароль :
Повторите ввод нового пароля :
passwd: пароль успешно обновлён
kolificent@kolificent:~$
```

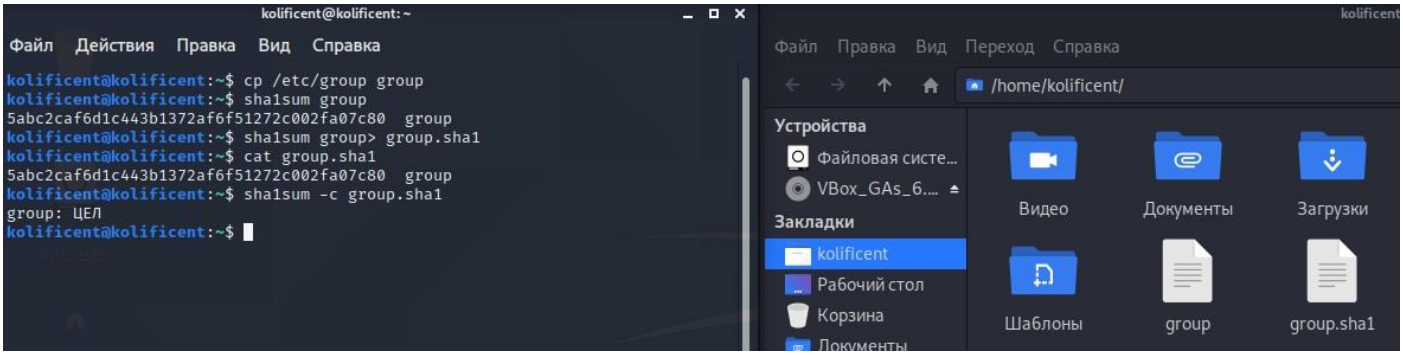
```
systemd-coredump:!*:18514::::::
vboxadd:!:18514::::::
superuser:$6$jKnJgT2E9Eha7cL.$xcP19oaq1He1a5CFjYI5A8iqHXqk9qeqbS0hch5V2pLOq
/aMi7A9HivSlBwdWL/xlrchE6nfOSDxHJOL1MZxa/:18563:0:99999:7:::
kolificent@kolificent:~$
```

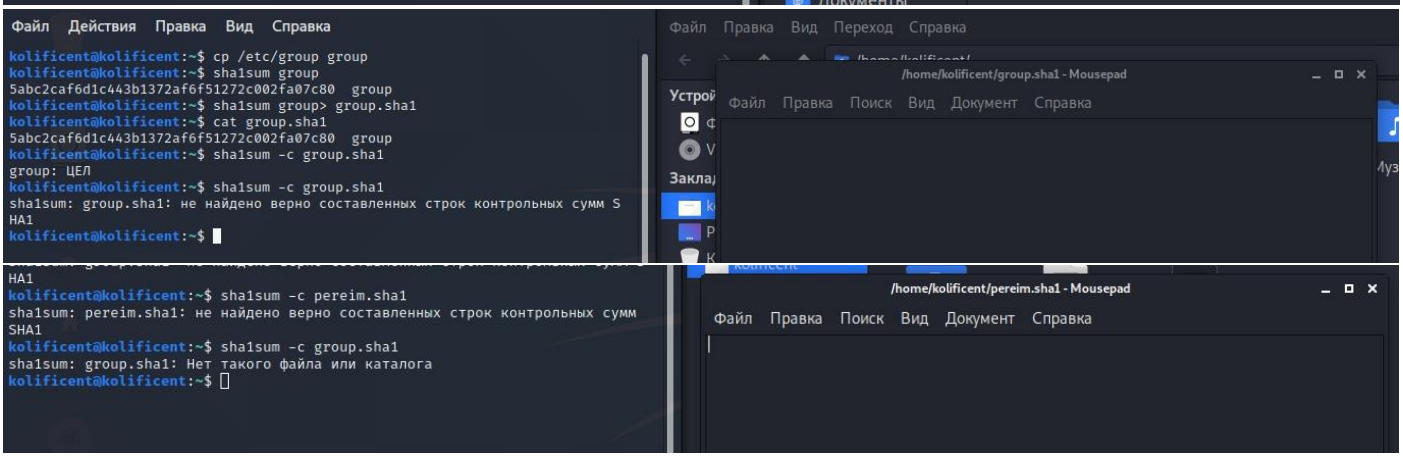
```
kolificent@kolificent:~$ su superuser
Пароль:
$ whoami
superuser
```

```
kolificent@kolificent:~$ su superuser
Пароль:
$ whoami
superuser
$ mkpasswd -m sha-512 -S jKnJgT2E9Eha7cL. -R 5000 kolificent
$6$rounds=5000$jKnJgT2E9Eha7cL.$mHJnBq.BTSuSvzC0KdeL9nUZVSFUAywsgoKVNookRa.
UJg73PeH66CcD0ASQeN1NsSHIuYFB5kl8grOdayRXD/
```


Файл Действия Правка Вид Справка
kolificent@kolificent:~$ cp /etc/group group
kolificent@kolificent:~$ sha1sum group
5abc2caf6d1c443b1372af6f51272c002fa07c80 group
kolificent@kolificent:~$
Файл Правка Вид Переход Справка
/home/kolificent/
Устройства
Файловая систе...
VBox_GAs_6....
Закладки
kolificent
Рабочий стол
Корзина
Документы
Музыка
Видео
Документы
Шаблоны
group

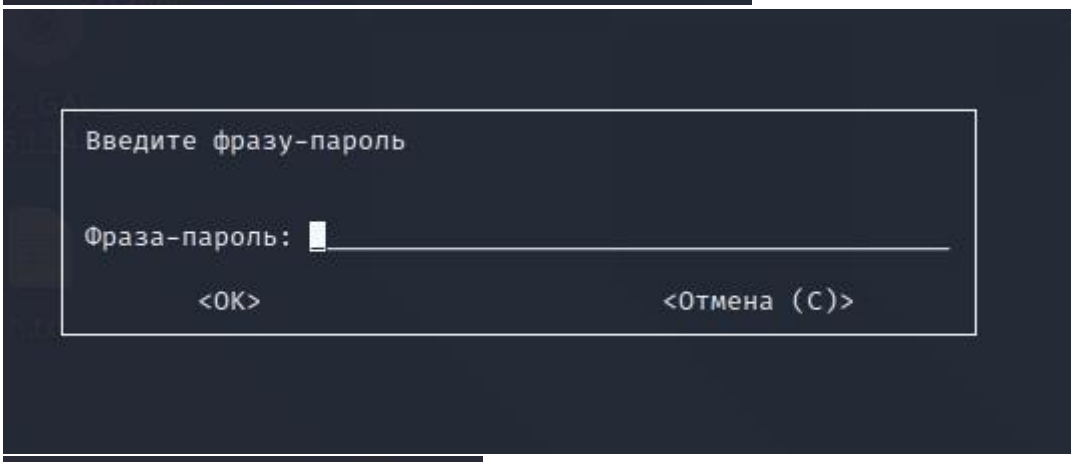

/home/kolificent/group - Mousepad
Файл Правка Поиск Вид Документ Справка
root:x:0:
daemon:x:1:
bin:x:2:
sys:x:3:
adm:x:4:
tty:x:5:
disk:x:6:
lp:x:7:
mail:x:8:
news:x:9:
uucp:x:10:
man:x:12:
proxy:x:13:
kmem:x:15:
dialout:x:20:
fax:x:21:
voice:x:22:
cdrom:x:24:kolificent
floppy:x:25:kolificent
tape:x:26:
sudo:x:27:kolificent
audio:x:29:pulse,kolificent
dip:x:30:kolificent
www-data:x:33:
backup:x:34:
operator:x:37:
list:x:38:
irc:x:39:
src:x:40:
gnats:x:41:
shadow:x:42:
utmp:x:43:
video:x:44:kolificent
sasl:x:45:
plugdev:x:46:kolificent
staff:x:50:
games:x:60:
users:x:100:
nogroup:x:65534:
systemd-journal:x:101:
systemd-network:x:102:
systemd-resolve:x:103:
systemd-timesync:x:104:
input:x:105:
kvm:x:106:
render:x:107:
crontab:x:108:

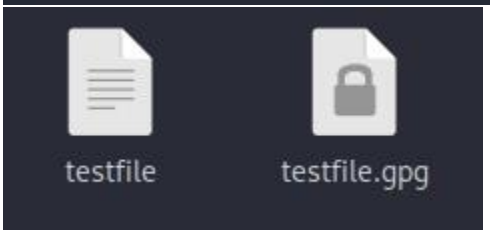

kolificent@kolificent: ~
Файл Действия Правка Вид Справка
kolificent@kolificent:~$ cp /etc/group group
kolificent@kolificent:~$ sha1sum group
5abc2caf6d1c443b1372af6f51272c002fa07c80 group
kolificent@kolificent:~$ sha1sum group> group.sha1
kolificent@kolificent:~$ cat group.sha1
5abc2caf6d1c443b1372af6f51272c002fa07c80 group
kolificent@kolificent:~$ sha1sum -c group.sha1
group: ЦЕЛ
kolificent@kolificent:~$
Файл Правка Вид Переход Справка
/home/kolificent/
Устройства
Файловая систе...
VBox_GAs_6....
Закладки
kolificent
Рабочий стол
Корзина
Документы
Видео
Документы
Загрузки
Шаблоны
group
group.sha1


Файл Действия Правка Вид Справка
kolificent@kolificent:~$ cp /etc/group group
kolificent@kolificent:~$ sha1sum group
5abc2caf6d1c443b1372af6f51272c002fa07c80 group
kolificent@kolificent:~$ sha1sum group> group.sha1
kolificent@kolificent:~$ cat group.sha1
5abc2caf6d1c443b1372af6f51272c002fa07c80 group
kolificent@kolificent:~$ sha1sum -c group.sha1
group: ЦЕЛ
kolificent@kolificent:~$ sha1sum -c group.sha1
sha1sum: group.sha1: не найдено верно составленных строк контрольных сумм SHA1
kolificent@kolificent:~$
Файл Правка Вид Переход Справка
/home/kolificent/group.sha1 - Mousepad
Файл Правка Поиск Вид Документ Справка

SHA1
kolificent@kolificent:~$ sha1sum -c pereim.sha1
sha1sum: pereim.sha1: не найдено верно составленных строк контрольных сумм SHA1
kolificent@kolificent:~$ sha1sum -c group.sha1
sha1sum: group.sha1: Нет такого файла или каталога
kolificent@kolificent:~$
/home/kolificent/pereim.sha1 - Mousepad
Файл Правка Поиск Вид Документ Справка

```
kolificent@kolificent:~$ touch testfile
kolificent@kolificent:~$ sudo gpg -c testfile
[sudo] пароль для kolificent:
kolificent@kolificent:~$ gpg -d testfile.gpg
gpg: данные зашифрованы алгоритмом AES256
gpg: прервано пользователем
gpg: зашифровано одной фразой-паролем
gpg: сбой расшифровки: No secret key
kolificent@kolificent:~$ gpg -d testfile.gpg
gpg: данные зашифрованы алгоритмом AES256
gpg: зашифровано одной фразой-паролем
gpg: сбой расшифровки: Bad session key
kolificent@kolificent:~$ gpg -d testfile.gpg
gpg: данные зашифрованы алгоритмом AES256
gpg: зашифровано одной фразой-паролем
kolificent@kolificent:~$
```





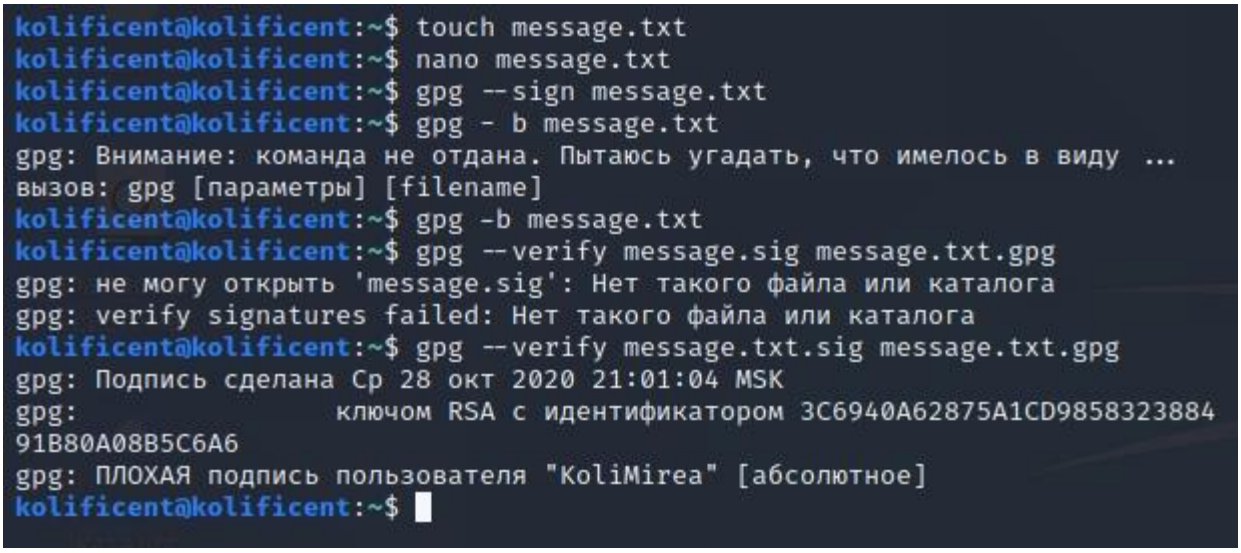
```
kolificent@kolificent:~$ gpg --full-generate-key
gpg (GnuPG) 2.2.20; Copyright (C) 2020 Free Software Foundation, Inc.
This is free software: you are free to change and redistribute it.
There is NO WARRANTY, to the extent permitted by law.

Выберите тип ключа:
   (1) RSA и RSA (по умолчанию)
   (2) DSA и Elgamal
   (3) DSA (только для подписи)
   (4) RSA (только для подписи)
  (14) Existing key from card
Ваш выбор? 1
длина ключей RSA может быть от 1024 до 4096.
Какой размер ключа Вам необходим? (3072) 2048
Запрошенный размер ключа - 2048 бит
Выберите срок действия ключа.
         0 = не ограничен
      <n>  = срок действия ключа - n дней
      <n>w = срок действия ключа - n недель
      <n>m = срок действия ключа - n месяцев
      <n>y = срок действия ключа - n лет
Срок действия ключа? (0) 0
Срок действия ключа не ограничен
Все верно? (y/N) y

GnuPG должен составить идентификатор пользователя для идентификации ключа.

Ваше полное имя: KoliMirea
Адрес электронной почты:
Примечание:
Вы выбрали следующий идентификатор пользователя:
    "KoliMirea"

Сменить (N)Имя, (C)Примечание, (E)Адрес; (O)Принять/(Q)Выход? o
Необходимо получить много случайных чисел. Желательно, чтобы Вы
в процессе генерации выполняли какие-то другие действия (печать
на клавиатуре, движения мыши, обращения к дискам); это даст генератору
случайных чисел больше возможностей получить достаточное количество энтропи
и.
Необходимо получить много случайных чисел. Желательно, чтобы Вы
в процессе генерации выполняли какие-то другие действия (печать
на клавиатуре, движения мыши, обращения к дискам); это даст генератору
случайных чисел больше возможностей получить достаточное количество энтропи
и.
gpg: ключ 8491B80A08B5C6A6 помечен как абсолютно доверенный
gpg: сертификат отзыва записан в '/home/kolificent/.gnupg/openpgp-revocs.d/
3C6940A62875A1CD985832388491B80A08B5C6A6.rev'.
открытый и секретный ключи созданы и подписаны.

pub   rsa2048 2020-10-28 [SC]
      3C6940A62875A1CD985832388491B80A08B5C6A6
uid                      KoliMirea
sub   rsa2048 2020-10-28 [E]
```

```
kolificent@kolificent:~$ gpg --list-keys
gpg: проверка таблицы доверия
gpg: marginals needed: 3  completes needed: 1  trust model: pgp
gpg: глубина: 0  достоверных:   2  подписанных:   0  доверие: 0-, 0q, 0n, 0
m, 0f, 2u
/home/kolificent/.gnupg/pubring.kbx
------------------------------------
pub   rsa2048 2020-10-28 [SC]
      C1A55D25F8C4870EEBF9C7311FA0E39BDCA8060E
uid         [  абсолютно ] Alexey
sub   rsa2048 2020-10-28 [E]

pub   rsa2048 2020-10-28 [SC]
      3C6940A62875A1CD985832388491B80A08B5C6A6
uid         [  абсолютно ] KoliMirea
sub   rsa2048 2020-10-28 [E]
```

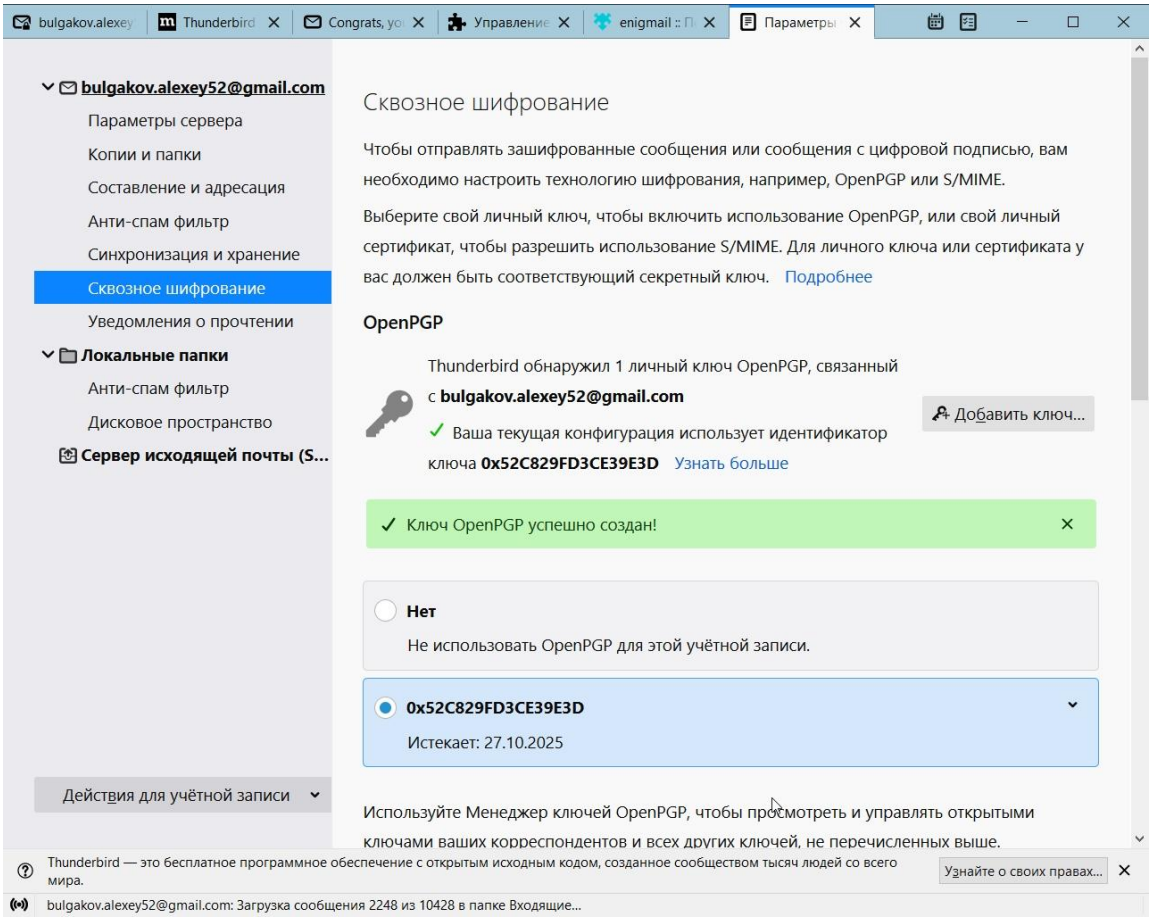
```
kolificent@kolificent:~$ gpg -a -o gpgkey.asc --export KoliMirea
kolificent@kolificent:~$ --import gpgkey.asc
bash: --import: команда не найдена
kolificent@kolificent:~$ gpg --import gpgkey.asc
gpg: ключ 8491B80A08B5C6A6: "KoliMirea" не изменен
gpg: Всего обработано: 1
gpg:                    неизмененных: 1
```

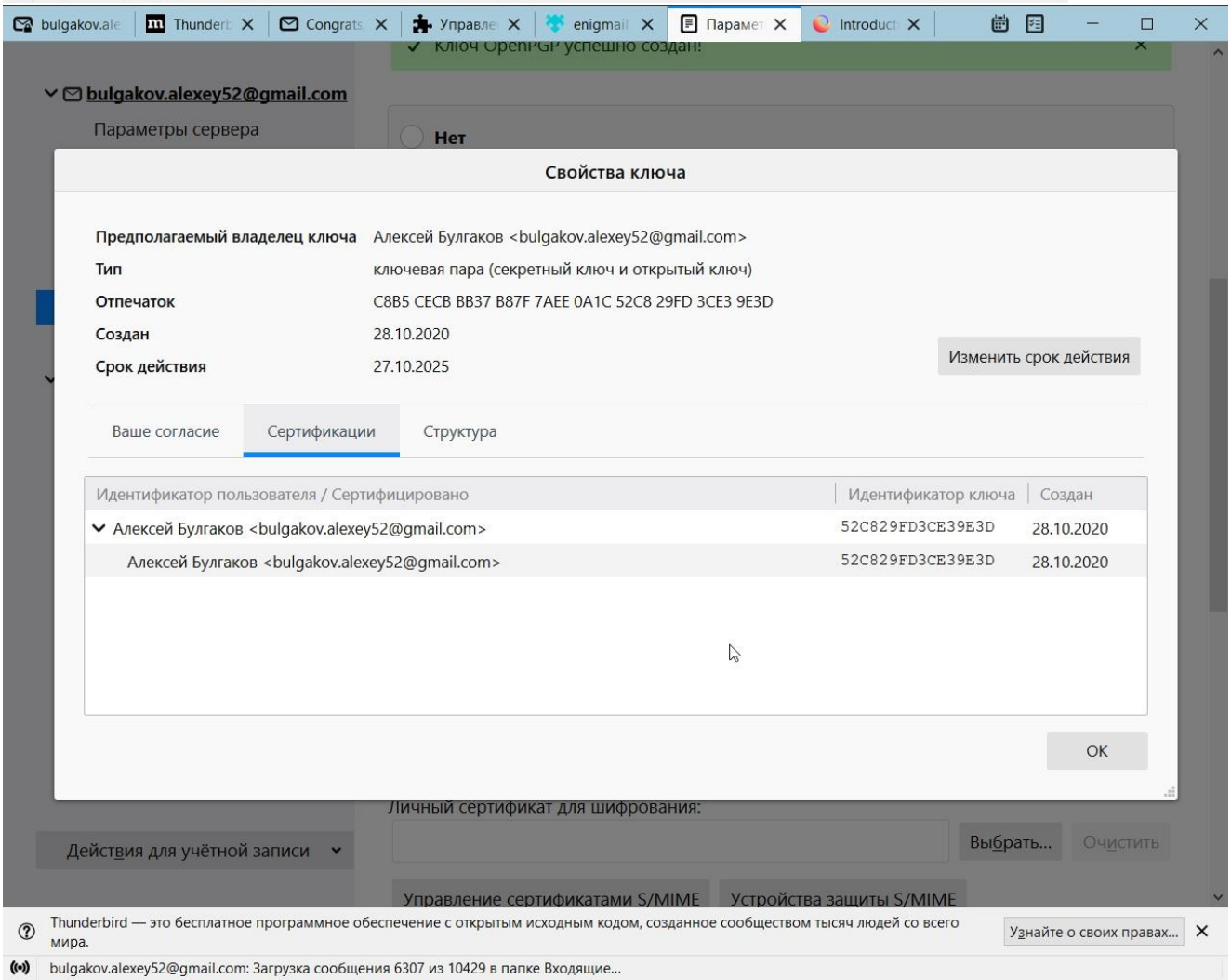
```
kolificent@kolificent:~$ gpg --edit-key KoliMirea
gpg (GnuPG) 2.2.20; Copyright (C) 2020 Free Software Foundation, Inc.
This is free software: you are free to change and redistribute it.
There is NO WARRANTY, to the extent permitted by law.

Секретный ключ доступен.

sec  rsa2048/8491B80A08B5C6A6
         создан: 2020-10-28     годен до: никогда     назначение: SC
     доверие: абсолютное достоверность: абсолютное
ssb  rsa2048/398BEDFC05D90152
         создан: 2020-10-28     годен до: никогда     назначение: E
[  абсолютно ] (1). KoliMirea

gpg> trust
sec  rsa2048/8491B80A08B5C6A6
         создан: 2020-10-28     годен до: никогда     назначение: SC
     доверие: абсолютное достоверность: абсолютное
ssb  rsa2048/398BEDFC05D90152
         создан: 2020-10-28     годен до: никогда     назначение: E
[  абсолютно ] (1). KoliMirea

Укажите, насколько Вы доверяете данному пользователю в вопросах проверки
достоверности ключей других пользователей (проверяет паспорт,
сверяет отпечатки ключей из разных источников и т.п.)

 1 = Не знаю или не буду отвечать
 2 = НЕ доверяю
 3 = Доверяю ограниченно
 4 = Полностью доверяю
 5 = Абсолютно доверяю
 m = вернуться в главное меню

Ваше решение? 5
Вы действительно хотите сделать этот ключ абсолютно доверенным? (y/N) y

sec  rsa2048/8491B80A08B5C6A6
         создан: 2020-10-28     годен до: никогда     назначение: SC
     доверие: абсолютное достоверность: абсолютное
ssb  rsa2048/398BEDFC05D90152
         создан: 2020-10-28     годен до: никогда     назначение: E
[  абсолютно ] (1). KoliMirea
```

```
kolificent@kolificent:~$ touch newkey
kolificent@kolificent:~$ gpg -e -r KoliMirea newkey
kolificent@kolificent:~$ gpg -d newkey.gpg
gpg: зашифровано 2048-битным ключом RSA с идентификатором 398BEDFC05D90152,
 созданным 2020-10-28
      "KoliMirea"
kolificent@kolificent:~$ tar -cf - grija | gpg -e -r KoliMirea
9
 9
E
QX<V(q
C
x'нр
_
xem
x
,
}fJ*
p
ó
E
r
-Ow|b
gF
n
V
M
`d
JKT
W
]
A
R
V
-
!s
X
I
)["
Q
!
Y
I
tar: grija: Функция stat завершилась с ошибкой: Нет такс
ла или каталога
tar: Завершение работы с состоянием неисправности из-за возникших ошибок
e_V
b
9
2
\b
ls
r9
qt
';
Гy
hN
A,
f
```



Почта: bulgakov.alexey52@gmail.com


bulgakov.alexey52@gmail.com
Параметры сервера
Копии и папки
Составление и адресация
Анти-спам фильтр
Синхронизация и хранение
Сквозное шифрование
Уведомления о прочтении
Локальные папки
Анти-спам фильтр
Дисковое пространство
Сервер исходящей почты (S...
Действия для учётной записи
Сквозное шифрование
Чтобы отправлять зашифрованные сообщения или сообщения с цифровой подписью, вам необходимо настроить технологию шифрования, например, OpenPGP или S/MIME.
Выберите свой личный ключ, чтобы включить использование OpenPGP, или свой личный сертификат, чтобы разрешить использование S/MIME. Для личного ключа или сертификата у вас должен быть соответствующий секретный ключ. Подробнее
OpenPGP
Thunderbird обнаружил 1 личный ключ OpenPGP, связанный с bulgakov.alexey52@gmail.com
Ваша текущая конфигурация использует идентификатор ключа 0x52C829FD3CE39E3D Узнать больше
Добавить ключ...
Ключ OpenPGP успешно создан!
Нет
Не использовать OpenPGP для этой учётной записи.
0x52C829FD3CE39E3D
Истекает: 27.10.2025
Используйте Менеджер ключей OpenPGP, чтобы просмотреть и управлять открытыми ключами ваших корреспондентов и всех других ключей, не перечисленных выше.
Thunderbird — это бесплатное программное обеспечение с открытым исходным кодом, созданное сообществом тысяч людей со всего мира.
Узнайте о своих правах...
bulgakov.alexey52@gmail.com: Загрузка сообщения 2248 из 10428 в папке Входящие...


bulgakov.alexey52@gmail.com
Параметры сервера
Нет
Свойства ключа
Предполагаемый владелец ключа Алексей Булгаков <bulgakov.alexey52@gmail.com>
Тип ключевая пара (секретный ключ и открытый ключ)
Отпечаток C8B5 CECB BB37 B87F 7AEE 0A1C 52C8 29FD 3CE3 9E3D
Создан 28.10.2020
Срок действия 27.10.2025
Изменить срок действия
Ваше согласие
Сертификации
Структура
Идентификатор пользователя / Сертифицировано
Идентификатор ключа
Создан
Алексей Булгаков <bulgakov.alexey52@gmail.com>
52C829FD3CE39E3D
28.10.2020
Алексей Булгаков <bulgakov.alexey52@gmail.com>
52C829FD3CE39E3D
28.10.2020
OK
Личный сертификат для шифрования:
Выбрать...
Очистить
Управление сертификатами S/MIME
Устройства защиты S/MIME
Действия для учётной записи
Thunderbird — это бесплатное программное обеспечение с открытым исходным кодом, созданное сообществом тысяч людей со всего мира.
Узнайте о своих правах...
bulgakov.alexey52@gmail.com: Загрузка сообщения 6307 из 10429 в папке Входящие...

Файл Правка Вид Вставить Формат Настройки Инструменты Справка

Отправить | Орфография | Защита | Сохранить | Вложить

От Алексей Булгаков <bulgakov.alexey52@gmail.com> bulgakov.alexey52@gmail.com | Копия | Скрытая копия

Кому mobil.mirea@gmail.com

Тема Практика №5

Абзац | Пропорциональный

БАСО-02-20; №2; Булгаков Алексей Алексеевич, Проверка связи

OpenPGP

Чтобы отправить сообщение, зашифрованное сквозным методом, вы должны получить и принять открытый ключ для каждого получателя.

Наличие ключей OpenPGP:

Получатель	Статус
mobil.mirea@gmail.com	в порядке

Управление ключами для выбранного получателя...

OK