

Отчет по лабораторной работе №2

Простейший вариант

Шишук Владислав Олегович, НПМбд-03-21

Содержание

Цель работы	5
Задание	6
Выполнение лабораторной работы	7
Выводы	13

Список иллюстраций

0.1	Создание учетной записи	7
0.2	настройка	8
0.3	Создание ключа ssh	8
0.4	Создание ключа pgr	9
0.5	вывод ключей	10
0.6	pgr ключ	11
0.7	ввод ключа	12
0.8	рисунок 8	12

Список таблиц

Цель работы

Изучить идеологию и применение средств контроля версий, освоить умения по работе с git.

Задание

- Создать базовую конфигурацию для работы с git.
- Создать ключ SSH.
- Создать ключ PGP.
- Настроить подписи git.
- Зарегистрироваться на Github.
- Создать локальный каталог для выполнения заданий по предмету.

Выполнение лабораторной работы

1). Создаем учетную запись на <https://github.com> . (рисунок 1)

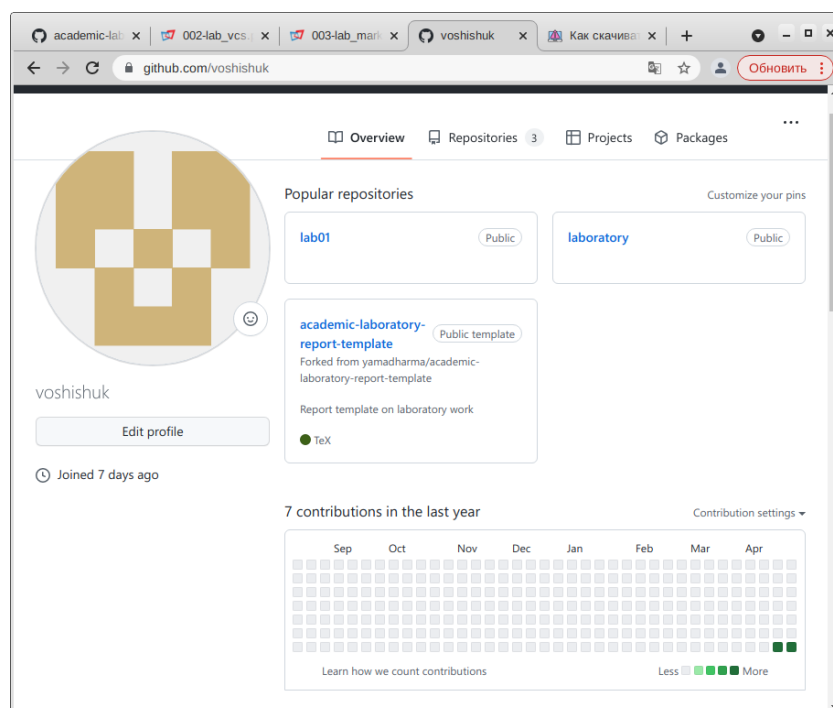


Рис. 0.1: Создание учетной записи

2). Задаем имя и email владельца репозитория. Также настраиваем верификацию и подписание коммитов git. (рисунок 2)

```
/: bash — Konsole
Файл Правка Вид Закладки Настройка Справка
voshishuk@dk8n78 /tmp $ cd ..
voshishuk@dk8n78 / $ git config --global user.name "voshishuk"
voshishuk@dk8n78 / $ git config --global user.email "chennodanbit@mail.ru"
voshishuk@dk8n78 / $ git config --global core.quotepath
voshishuk@dk8n78 / $ git config --global init.defaultBranch master
voshishuk@dk8n78 / $ git config --global core.autocrlf input
voshishuk@dk8n78 / $ git config --global core.safecrlf warn
voshishuk@dk8n78 / $
```

Рис. 0.2: настройка

3). Создаем ключи ssh по алгоритмам rsa и ed25519 (рисунок 3)

```
/: bash — Konsole
Файл Правка Вид Закладки Настройка Справка
ssh-keygen -L [-f input_keyfile]
ssh-keygen -A [-a rounds] [-f prefix_path]
ssh-keygen -k -f krl_file [-u] [-s ca_public] [-z version_number]
file ...
ssh-keygen -Q [-l] -f krl_file [file ...]
ssh-keygen -Y find-principals -s signature_file -f allowed_signers_file
ssh-keygen -Y check-novalidate -n namespace -s signature_file
ssh-keygen -Y sign -f key_file -n namespace file ...
ssh-keygen -Y verify -f allowed_signers_file -I signer_identity
-n namespace -s signature_file [-r revocation_file]
voshishuk@dk8n78 / $ ssh-keygen -t rsa -b 4096
Generating public/private rsa key pair.
Enter file in which to save the key (/afs/.dk.sci.pfu.edu.ru/home/v/o/voshishuk/.ssh/id_rsa):
/afs/.dk.sci.pfu.edu.ru/home/v/o/voshishuk/.ssh/id_rsa already exists.
Overwrite (y/n)? y
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /afs/.dk.sci.pfu.edu.ru/home/v/o/voshishuk/.ssh/id_rsa
Your public key has been saved in /afs/.dk.sci.pfu.edu.ru/home/v/o/voshishuk/.ssh/id_rsa.pub
The key fingerprint is:
SHA256:1dZr/0t5YJwty82s7frfGF+9k3FhZqs6BD+kbhtybx voshishuk@dk8n78
The key's randomart image is:
+---[RSA 4096]---+
|      . o      |
|      + .      |
|    o . o B    |
|   S = . X +   |
|    . o X +    |
|   ..o.Eo =o@  |
|   oooo.o.o=   |
|    ..o+ =B%   |
+---[SHA256]-----+
voshishuk@dk8n78 / $ ssh-keygen -t ed25519
Generating public/private ed25519 key pair.
Enter file in which to save the key (/afs/.dk.sci.pfu.edu.ru/home/v/o/voshishuk/.ssh/id_ed25519):
/afs/.dk.sci.pfu.edu.ru/home/v/o/voshishuk/.ssh/id_ed25519 already exists.
Overwrite (y/n)? y
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /afs/.dk.sci.pfu.edu.ru/home/v/o/voshishuk/.ssh/id_ed25519
Your public key has been saved in /afs/.dk.sci.pfu.edu.ru/home/v/o/voshishuk/.ssh/id_ed25519.pub
The key fingerprint is:
SHA256:AC6d7ID3KhDYehsuiFphh8nbNKnCv9U38CGM5quM1HU voshishuk@dk8n78
The key's randomart image is:
+---[ED25519 256]---+
|o.o.o.o.o      |
|l=B+++o        |
|@.=.=.+        |
|l+*o=.o=.      |
|o...=E. S .    |
|l.oo.o.+.      |
|l.o.o.+.      |
|..o.          |
|l.o.          |
|l.o.          |
+---[SHA256]-----+
voshishuk@dk8n78 / $
```

Рис. 0.3: Создание ключа ssh

4). Генерируем ключ pgr.(рисунок 4)


```
gpg -- Konsole
Файл  Правка  Вид  Закладки  Настройка  Справка
voshishuk@dk8n78 / $ ssh-keygen -t ed25519
Generating public/private ed25519 key pair.
Enter file in which to save the key (/afs/.dk.sci.pfu.edu.ru/home/v/o/voshishuk/.ssh/id_ed25519):
/afs/.dk.sci.pfu.edu.ru/home/v/o/voshishuk/.ssh/id_ed25519 already exists.
Overwrite (y/n)? y
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /afs/.dk.sci.pfu.edu.ru/home/v/o/voshishuk/.ssh/id_ed25519
Your public key has been saved in /afs/.dk.sci.pfu.edu.ru/home/v/o/voshishuk/.ssh/id_ed25519.pub
The key fingerprint is:
SHA256:AC6d7ID3KhDYehsuiFphh8nbNKnCv9U38CGM5quM1HU voshishuk@dk8n78
The key's randomart image is:
+--[ED25519 256]--+
|o.ooo. |
|=B+++o |
|@.+=.+ |
|++o=.o=. |
|o...=E. S |
|.oo.o..+ |
|.o.o... |
|..o. |
|.o. |
+-----[SHA256]-----+
voshishuk@dk8n78 / $ gpg --full-generate-key
gpg (GnuPG) 2.2.27; Copyright (C) 2021 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) Имеющийся на карте ключ
Ваш выбор? 1
длина ключей RSA может быть от 1024 до 4096.
Какой размер ключа Вам необходим? (3072) 4096
Запрошенный размер ключа - 4096 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: voshishuk
Адрес электронной почты: chennodanbit@mail.ru
Примечание: 1
Вы выбрали следующий идентификатор пользователя:
"voshishuk (1) <chennodanbit@mail.ru>"

Сменить (N)Имя, (C)Примечание, (E)Адрес; (O)Принять/(Q)Выход? 
```

Рис. 0.4: Создание ключа gpg

5). Выводим список ключей. (рисунок 5)

```
/: bash — Konsole
Файл  Правка  Вид  Закладки  Настройка  Справка

длина ключей RSA может быть от 1024 до 4096.
Какой размер ключа Вам необходим? (3072) 4096
Запрошенный размер ключа - 4096 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: voshishuk
Адрес электронной почты: chennodanbit@mail.ru
Примечание: 1
Вы выбрали следующий идентификатор пользователя:
  "voshishuk (1) <chennodanbit@mail.ru>"

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 энтропии.
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 энтропии.
gpg: ключ CB368712A367C7D0 помечен как абсолютно доверенный
gpg: сертификат отзыва записан в '/afs/.dk.sci.pfu.edu.ru/home/v/o/voshishuk/.gnupg/openpgp-revocs
.d/96F9548E7931FDC4EA9AA836CB368712A367C7D0.rev'.
открытый и секретный ключи созданы и подписаны.

pub   rsa4096 2022-04-30 [SC]
      96F9548E7931FDC4EA9AA836CB368712A367C7D0
uid    voshishuk (1) <chennodanbit@mail.ru>
sub    rsa4096 2022-04-30 [E]

voshishuk@dk8n78 / $ gpg --list-secret-keys --keyid-format LONG
gpg: проверка таблицы доверия
gpg: marginals needed: 3 completes needed: 1 trust model: pgp
gpg: глубина: 0 достоверных: 1 подписанных: 0 доверие: 0-, 0q, 0n, 0m, 0f, 1u
/afs/.dk.sci.pfu.edu.ru/home/v/o/voshishuk/.gnupg/pubring.kbx
-----
sec   rsa4096/300EDF05D0F210B6 2022-04-23 [SC]
      1EC13593F0CF464898811E4C300EDF05D0F210B6
uid    [ неизвестно ] voshishuk <chennodanbit@mail.ru>
ssb    rsa4096/23F8CE130BE2B65E 2022-04-23 [E]

sec   rsa4096/CB368712A367C7D0 2022-04-30 [SC]
      96F9548E7931FDC4EA9AA836CB368712A367C7D0
uid    [ абсолютно ] voshishuk (1) <chennodanbit@mail.ru>
ssb    rsa4096/5F35287DED2C02DD 2022-04-30 [E]

voshishuk@dk8n78 / $
```

Рис. 0.5: вывод ключей

6). Далее выводим ргр ключ с помощью команды `gpg --armor --export` “отпечаток улюча” (рисунок 6)

```
/ : bash — Konsole
Файл Правка Вид Закладки Настройка Справка
voshishuk@dk8n78 / $ gpg --armor --export 300EDF05D0F210B6
-----BEGIN PGP PUBLIC KEY BLOCK-----

mQINBGJj0bwBEADXRoc+6TRvTD/hT9rtuYmiqKF7Ry2wH1pbu37YGV1Np6gkGEH
BfoQa8P+X+so/5DEEIS1gVj1NgrTpSw9YBZJ+3jp4mo+/f31SChR3u+nBX1xFpMI
eqtkQsk1RMVGE6Dur00Ama8uQz3iW2bWs7tVQubxNrf+IWh10D116+2zGNJcTxJc
BBK252MianUd9eKAcZU9prdnAizcgmg9SKLPP794Lp9S0949cX1PwtvayrhRT5FM
1EkXmWsyKXAY+TJbC3A7Vkk9popI2N9mf6T8cFkUFgFk317YQDzruuH96jVOKM8R
nT2ZzWK6U/b4J0tjJ4YA+WtFAIaozSmgbs43jKk10YArpVRwd4bYa+VHowkPLtZs
vb1DZMV+kQ3bdjI3HCSKWUEqYewxyZADbwSmvNDsAWOQ9hsJLkSUDbwJNFHXRHGz
Agdf2uY6dthIqhKfJIKeVWwIFPCHx+Y95xYKsSHKsY1iq5xWtZVynUg8ZAQoRgz
XVR3U+O/F61lgBwgyTLKjT29PtI02H730nGLYwWw+DGfOZzzX27ENORxySJJaZnd
/yrZVpc61VK/XwdJgmAEv63LHBBKSb7StzUDVAewkUDn3nJR1+saN/ly1Wg3L1wQ
u0+huC4rrEHHS3Frag0V12rYrAYxFPASyFR2ImZQAazqUx8vURs9I0p6FWaRAQAB
tCB2b3NoaXnodWsePGNoZW5ub2RhbmJpdEBtYW1sLnJ1PokCTgQTAQ0BYhBB7B
NZPwz0ZImIEeTDA03wXQ8hC2BQJiY9g8AhsDBQsJCACCBHUKCQGLAgQWAgMBAh4B
AheAAaoJEDA03wXQ8hC2w8QAMf8nubw9RsJ8h2D3qcyIhYCYomPU0A0iRfdyPdo
OahNFQKLrdh14POKofaCZL8qVe+8uLM2Jt6c68tvuH7ooCHvyW02yqcUHRQm1v8
Qc4DPTLAKxIzPHu5D08F/p0LGLK8DmLKH4+GzRRs0aKJ11Gnwptz5RqALPzP8gN
fWPvTTzNnCCkXU023jU7PeU4ozZqJB36TTFudL/J4Hgb11qy81wFXKzYmZdAH
s1PZRsTVZM4INyWRnM9oIzG+KopM5YNW0rkGfD0N6ERNd+VUq58w/th3rJsenSY
b991FrUdiL3+MHVPuGsT9z/G18TnPuJY9PNJ04jPnx7Rxqy8cIjL7gOSTp8dra
S9ZLBFL1dgW7yw56140cwS3rjeP0LcWkYSIJvhtqhsrVp1W+2a6K22aU1vSn7az
jPoFIfm1QR6vGLKAAT0/z6SaItYGo+S9YmPQ/vjoQEUVVRfQdE/Ma84yucwo3Ss
29LZUB0IrAiQUoawckF/6GB7TC4w3L7vNgQZsUA/V48pfsApSB25TFkHCrSgeEv
GdkPVeEuAmmvGLMKPIgdzMN32bM1LCH7xE4YdGgOK0Upg2TuYDz+hsRo0ruyFPdv
omBhEnHCuPiY4iAHTnJXqmPMLzRJ45GsI/yq2mayAafSsBRVERQ0VL350gsz2Pc
Hjt+uQINBGJj0bwBEACzzceK4F4/IW501xfao7m7HGKQHEX1U7LGiJfHAAq7C7c
qeW7T/6ewpeXJTtZ4QbxF9/hvtj0xkh1zI0bsvMKSa9BkMvhVaZaPozUekD2JZ5
ete+K1yPERTutZDPSCH2sK4UbeRwWg02qrjZ1j03iMj3P9tb0ZrxcqL VyekmKHQ
ARnNZxi4yqgKE0+p+xxQh2WRHmYPTfaIfJABDq91mQdTMQfvetBvd4FqHkth7KrH
9RPkJGSUpPCMF+8qSMZ+0j/yB/ZKu+Bp8e00AEEKtK06IP4dg5sgNN1Y+5LT4SI
XIDYIukF9vBfA2++JyT+ZPRK6ca28P/YfUpHRZCYtAipmC010XnIa4Bhk61TH0cy
4Nklwy1tkphB1i6DiVjeGfcsGrSa9nMqWfTbxQw4rYeqM8scw/jMEU5JPjxn1BI
4EshjA1DaFtzHy1w0LUQIfkMZH0YKddH2a8g1lWZ1310M8+SJIrf/NZk8JKFZmI
HR1sVQW9KkxMwp3Wm7dzA035xSyIfeJ5Wk4VbT0QAYNYq/OsFx40cvxNy8795rY+
vNMg/thSDM+6e07qhsKNKh1MrZBJ12uo5HVoFnyMLVy6IMSvfu81E0366jd04Mz
h6k9F2WNCHM/fDXuj1C5SYAoHmhts/Io6Qui1Na8WnOaY2ZL8g1K5MT2YIJ6QAR
AQABiQ12BBGBCAAgFiEEHs1k/DPRKiYgR5MMA7fBdDyELyFAmJj0bwCGwwACgkQ
MA7fBdDyELyJRAApXdvYYjVcB01sv+ooISF/1UVhBwEgrs3qR1SfrgELFM6wdzI
LQh17WmqE4qi17m9KUD3e8cghoTeS8TWGxZKWNFFg66oBz5QCBSjJxrb+KxyHRS1
Hnkeq34zejAh5Kn2kMjzAx2zw4KaJtKsRdQMDK77N3l7+1bZ7fzsJqpHdi3/aoQ9
b38LQnFTI0nQnFhwymGiMx8VLW8u1FXjtw/I+kfcsShfJ4uPnMQUTnQZ2sBvYVXS
B4m8SJLCxa506EKm2FKa/4mq0A9Rab92/GjwAd1suPs0fncB+WliV40qhKHEnMYy
GkVwF4imMR3tv1th6EyJcexVQIE+UBmWNPi6yz7gMvn/V6Adi+jID2pg32GaCnw
fYyY4YmivWptK/za7XF0LcoNBzoRwHYqJjNck0oiRBD0s+S857RAPPF5+S0Q0w
9qdoSVz9nUpOPYGB/Cgz0nrW4PxyMf0CE1RMW7Q52QQVUo+e1LVWHLT5TERfRNs
6dHJq8SE3s1XwQJTa100U7A71W8aoBg7j8CGug9H5YyhfvdnJOPc99PzhUn9DFw
mOYhWAAANV0up4RVIU9ChA37qn7jooyPCtMIdUMF5B6J0Q5bcHre+oNvKqxIGU51w
Kr4uS+mNV+6oVhybyraf2/37MI53zdsZIZf22HSW2YqJnR0e1IviqVduCtU=
=mxbs
-----END PGP PUBLIC KEY BLOCK-----

voshishuk@dk8n78 / $ git config --global user.signingkey <PGP fingerprint>
bash: синтаксическая ошибка рядом с неожиданным маркером «newline»
voshishuk@dk8n78 / $ git config --global commit.gpgsign
voshishuk@dk8n78 / $ git config --global gpg.program
voshishuk@dk8n78 / $
```

Рис. 0.6: pgp ключ

7). Вводим ключ на GitHub.(рисунок 7)

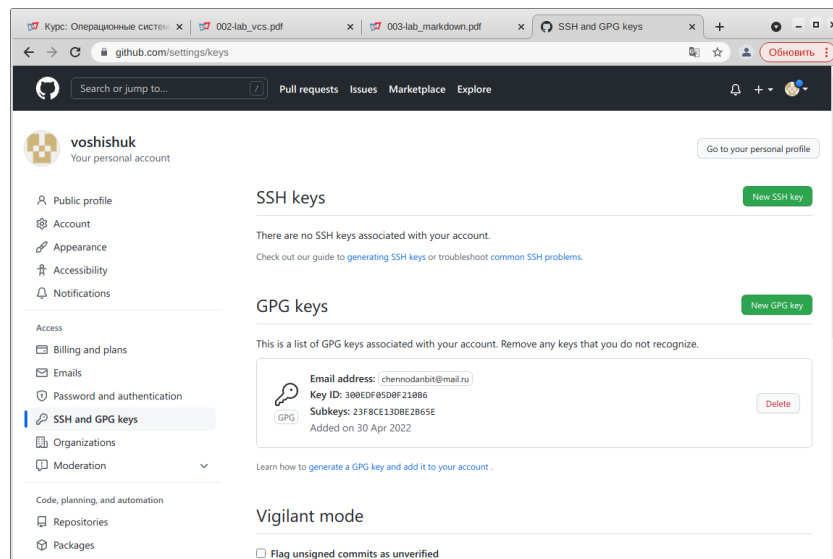


Рис. 0.7: ввод ключа

8). К сожалению, при настройке gh терминал писал что, команды gh не найдены. (рисунок 8)

```
voshishuk@dk8n78 / $ git config --global gpg.program
voshishuk@dk8n78 / $ gh auth login
bash: gh: команда не найдена
voshishuk@dk8n78 / $ mkdir -p ~/work/study/2021-2022/OS
voshishuk@dk8n78 / $ cd ~/work/study/2021-2022/OS
voshishuk@dk8n78 ~/work/study/2021-2022/OS $ gh repo create study_2021-2022_os-intro
bash: gh: команда не найдена
```

Рис. 0.8: рисунок 8

Выводы

Освоил некоторые навыки по работе с Git, применил средства контроля версий за время выполнения данной лабораторной работы.