|  |
| --- |
| Описание: Описание: для прик эмбл |
| МИНОБРНАУКИ РОССИИ |
| Федеральное государственное бюджетное образовательное учреждениевысшего профессионального образования"Российский технологический университет"МИРЭА |
| Институт «Комплексной безопасности и специального приборостроения» |
| Кафедра «Управление и моделирование систем» (КБ-3) |
|  |

|  |  |
| --- | --- |
| **Практика №5 по дисциплине** | |
|  | |
| **« Основы информационной безопасности »**  **«Обеспечение криптографической защиты информации**  **в современных операционных системах. Linux.»** | |
|  | |
| Выполнил студент группы БИСО-03-19 | **Коннов Я.В.** |

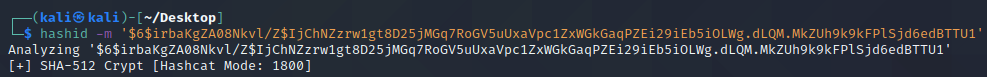
Москва 2020

**Hash и новый пользователь**

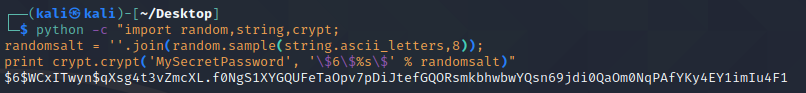
Посмотрим hash пользователя в файле /etc/shadow



Cкопируем его и определим тип с помощью утилилиты hashid



Сгенерируем новый hash SHA-512 для пароля ‘MySecretPassword’



Cгенерированный hash:

$6$WCxITwyn$qXsg4t3vZmcXL.f0NgS1XYGQUFeTaOpv7pDiJtefGQORsmkbhwbwYQsn69jdi0QaOm0NqPAfYKy4EY1imIu4F1

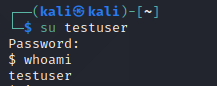
Создадим нового пользователя – testuser



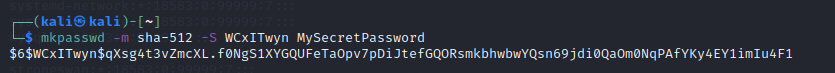
Установим сгенерированный нами hash данному пользователю



Зайдём под новым пользователем, используя новый пароль



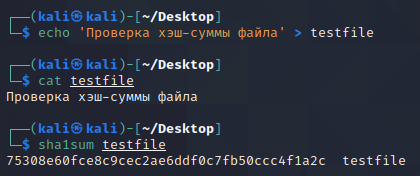
C помощью mkpasswd, зная соль, расчитаем hash нашего пароля



Сгенерированный ранее и данный hash полностью идентичные.

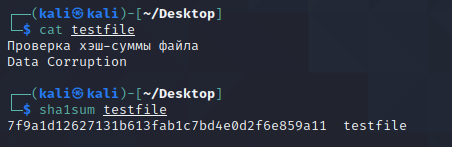
**Контрольная сумма**

Создадим файл с текстом 'Проверка хэш-суммы файла' в нём и найдём его хэш-сумму.



Хэш-сумма файла: 75308e60fce8c9cec2ae6ddf0c7fb50ccc4f1a2c

Теперь внесём свои изменения в данный файл и вновь найдём его хэш-сумму

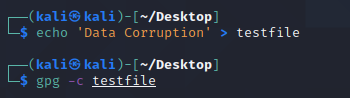


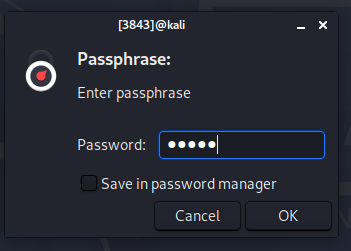
Хэш-сумма файла: f9a1d12627131b613fab1c7bd4e0d2f6e859a11

Мы можем видеть, что хэш-сумма изменилась. Следовательно, файл также был изменён.

**GPG**

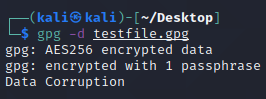
Создадим файл и зашифруем его с помощью gpg используя пароль:12345



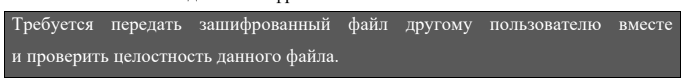


Был создан файл testfile.gpg

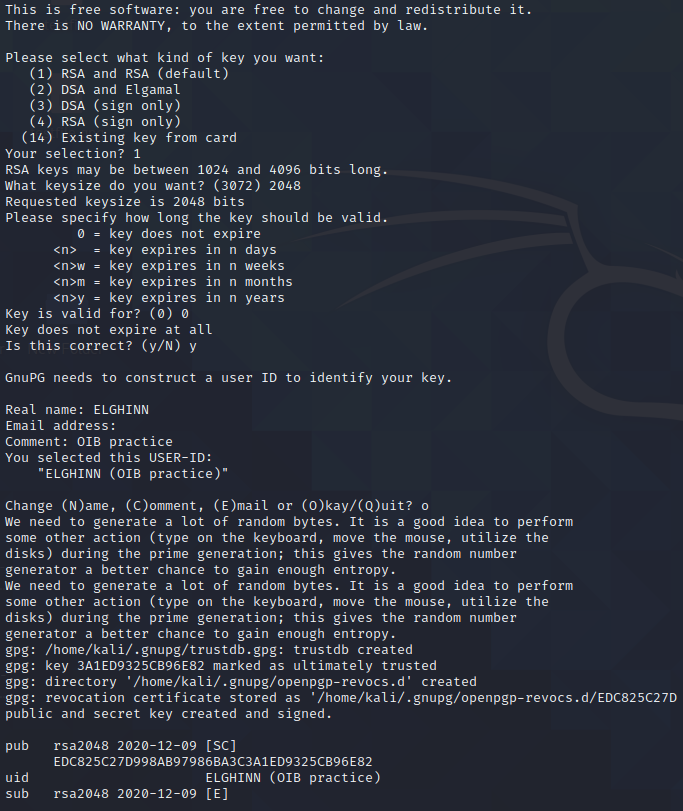
Попытаемся расшифровать его



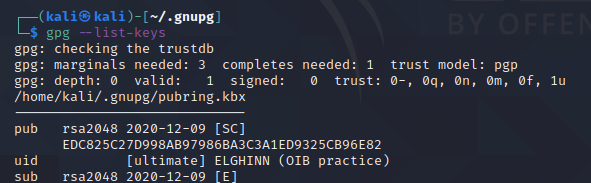
В итоге получим содержимое нашего файла



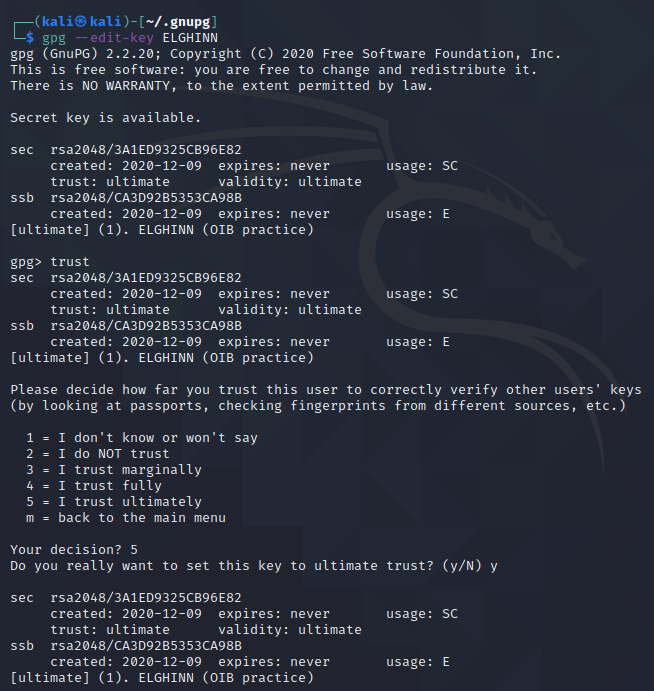
Создадим пару ключей



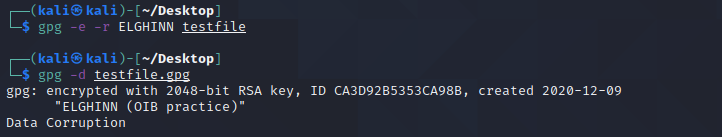
Посмотрим список доступных ключей



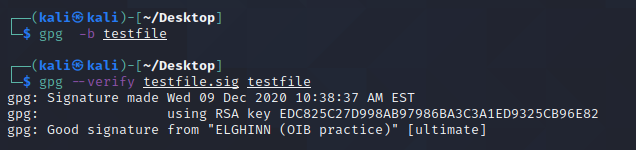
Установим уровень доверия для данного ключа



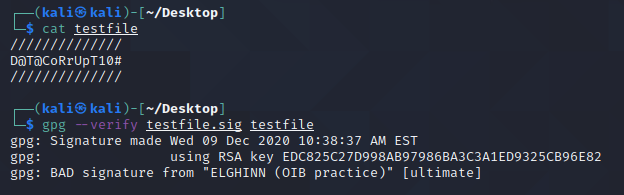
Попробуем зашифровать файл с помощью сгенерированного ключа, а затем прочитать его

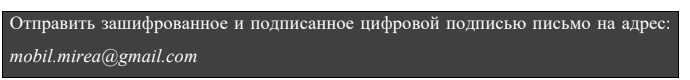


Создадим ключ и проверим наш файл

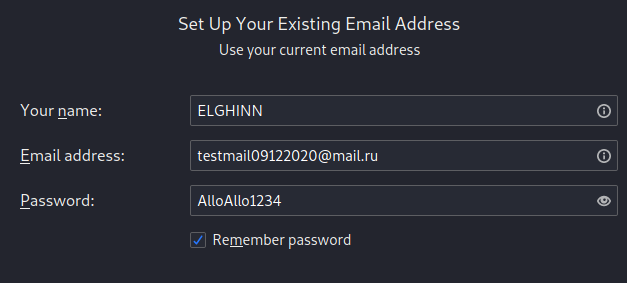


Изменим файл и проверим ещё раз

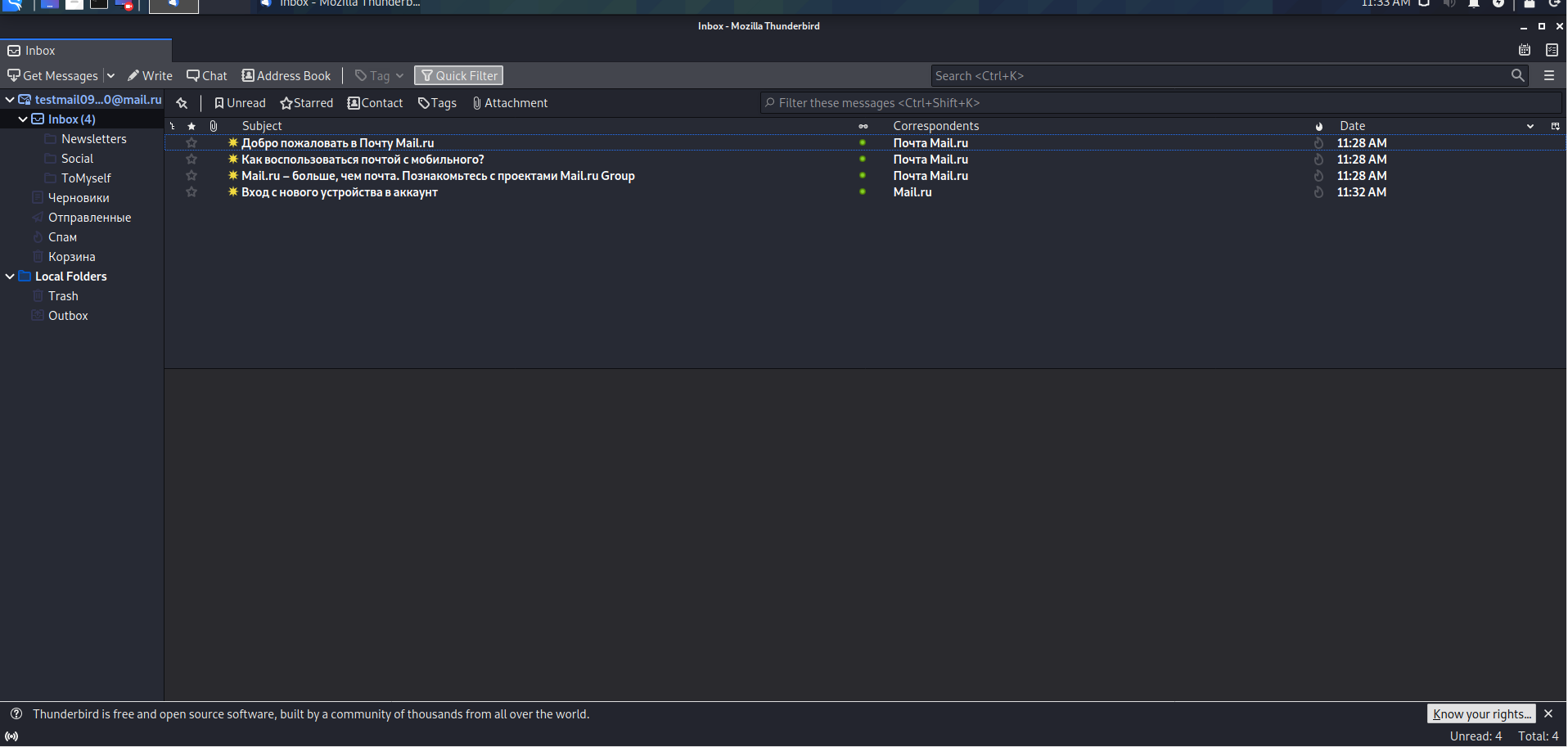




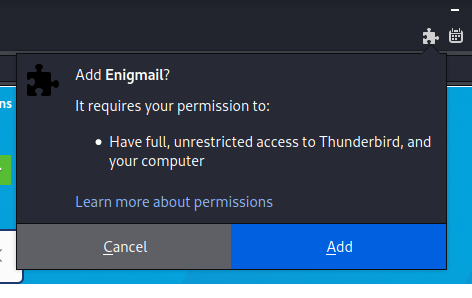
Скачаем Mozilla Thunderbird и настроим почтовый клиент



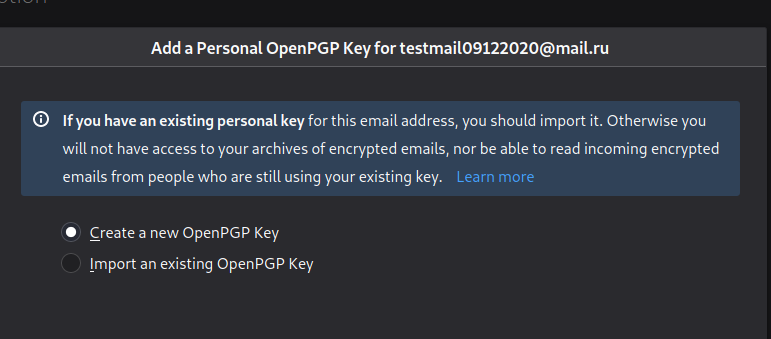
Мы попадем в нашу почту

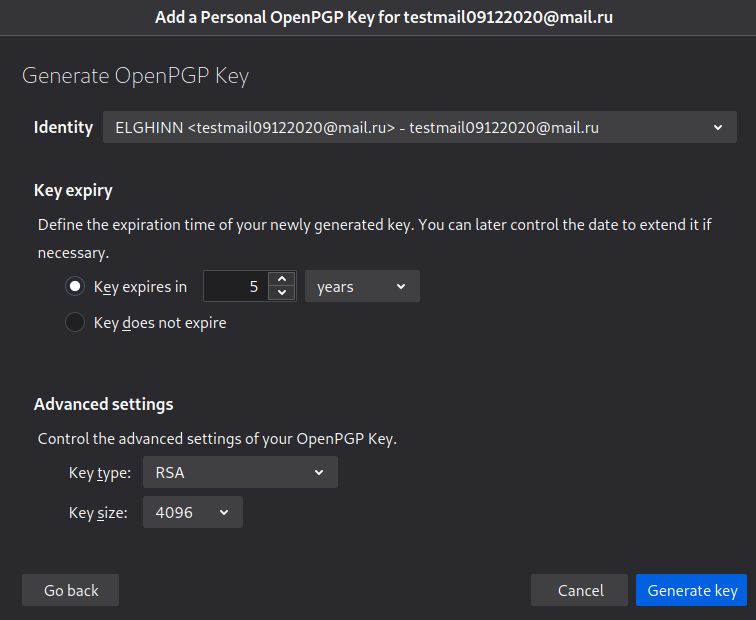


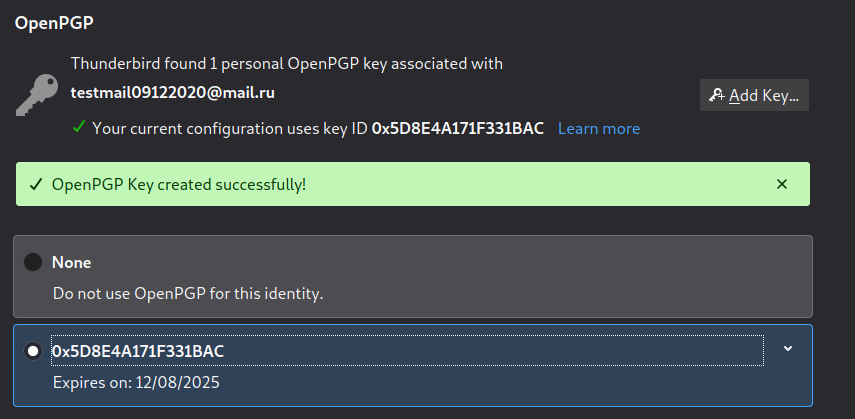
Добавим расширение Enigmail



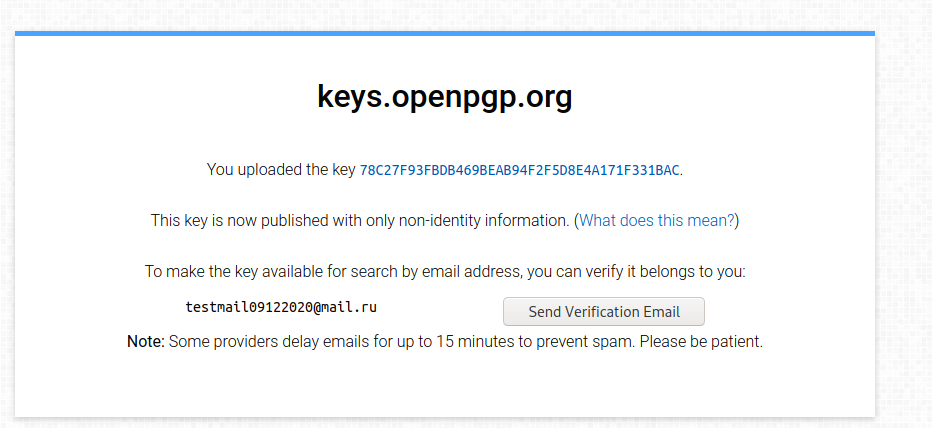
Cоздадим OpenPGP ключ

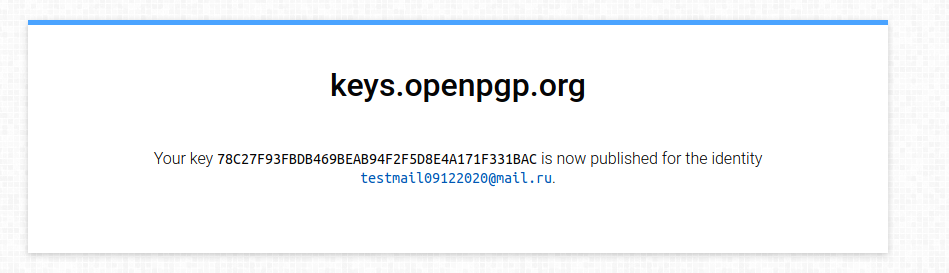


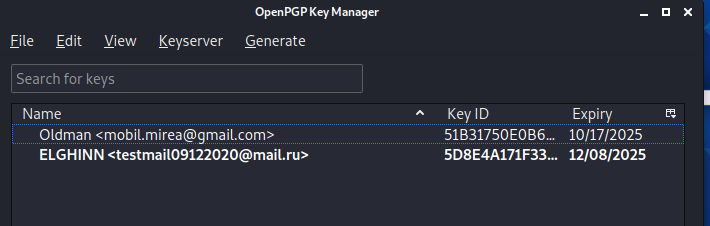


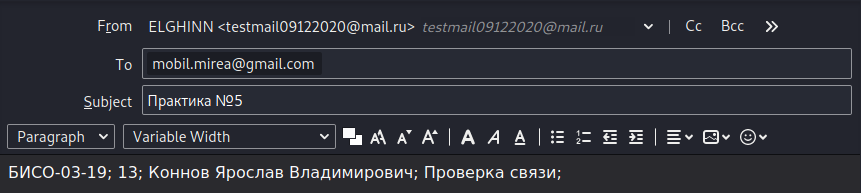


Далее экспортируем ключ в файл и загрузим его на <https://keys.openpgp.org>





Импортируем ключ, привязанный к почте [mobil.mirea@gmail.com](mailto:mobil.mirea@gmail.com#)



Письмо было отправлено