МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное образовательное учреждение
высшего образования
«МИРЭА – Российский технологический университет»
РТУ МИРЭА

Практическое занятие № 5
«Обеспечение криптографической защиты информации
в современных операционных системах. Linux.»

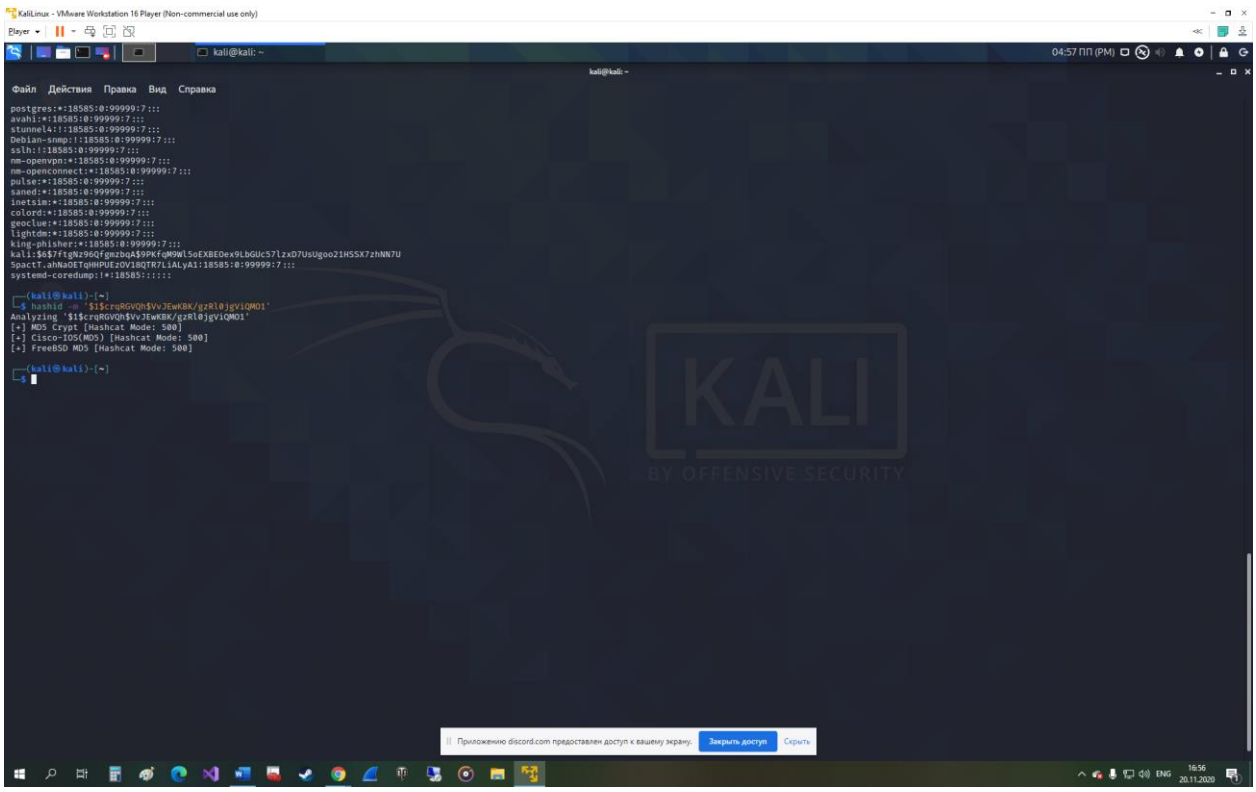
	Основы информационной безопасности
	(наименование дисциплины (модуля) в соответствии с учебным планом)
Уровень	бакалавриат
	(бакалавриат, магистратура, специалитет)
Форма обучения	очная
	(очная, очно-заочная, заочная)
Направление(-я) подготовки	10.05.05 Безопасность информационных технологий в правоохранительной сфере
	(код(-ы) и наименование(-я))
Институт	комплексной безопасности и специального приборостроения ИКБСП
	(полное и краткое наименование)
Кафедра	КБ-2 «Прикладные информационные технологии»
	(полное и краткое наименование кафедры, реализующей дисциплину (модуль))

Используются в данной редакции с учебного года 2020/21
(учебный год цифрами)

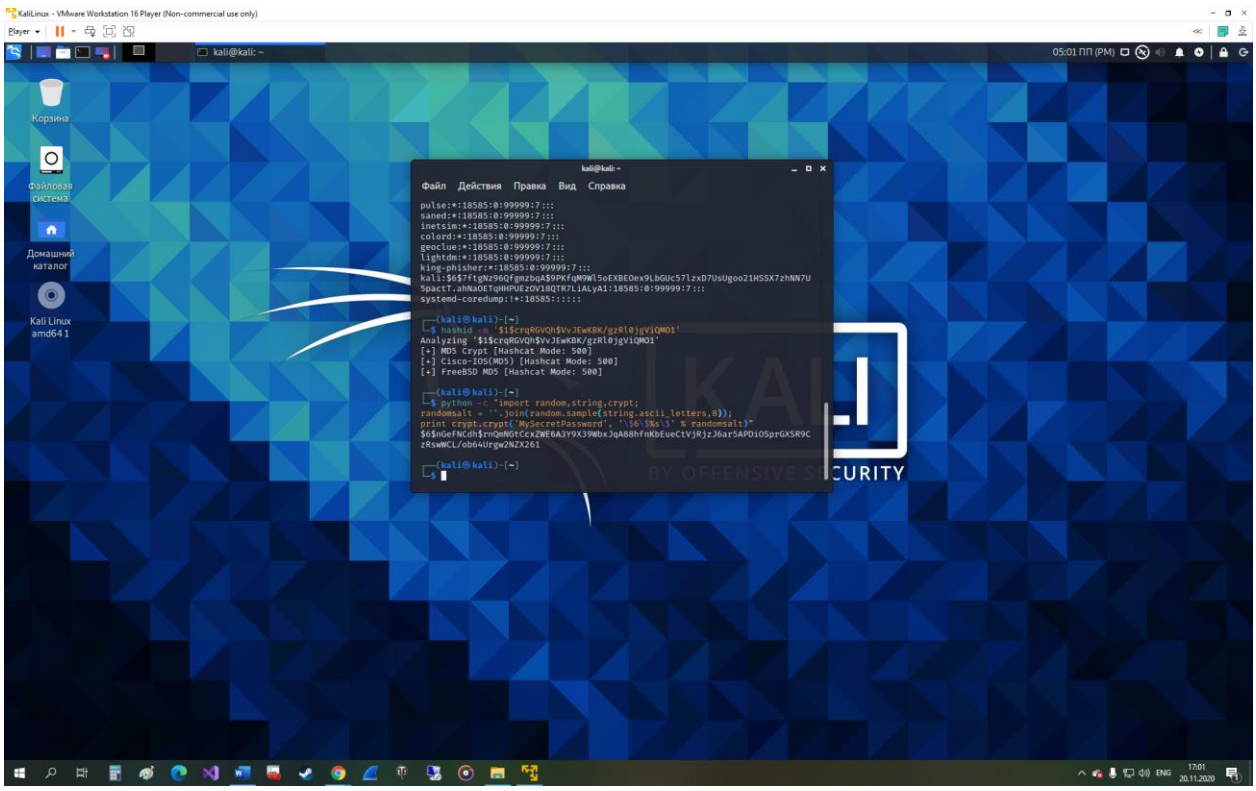
Проверено и согласовано «____» _____20___г. _____ _____
(подпись директора Института/Филиала с расшифровкой)

Москва 2020 г.

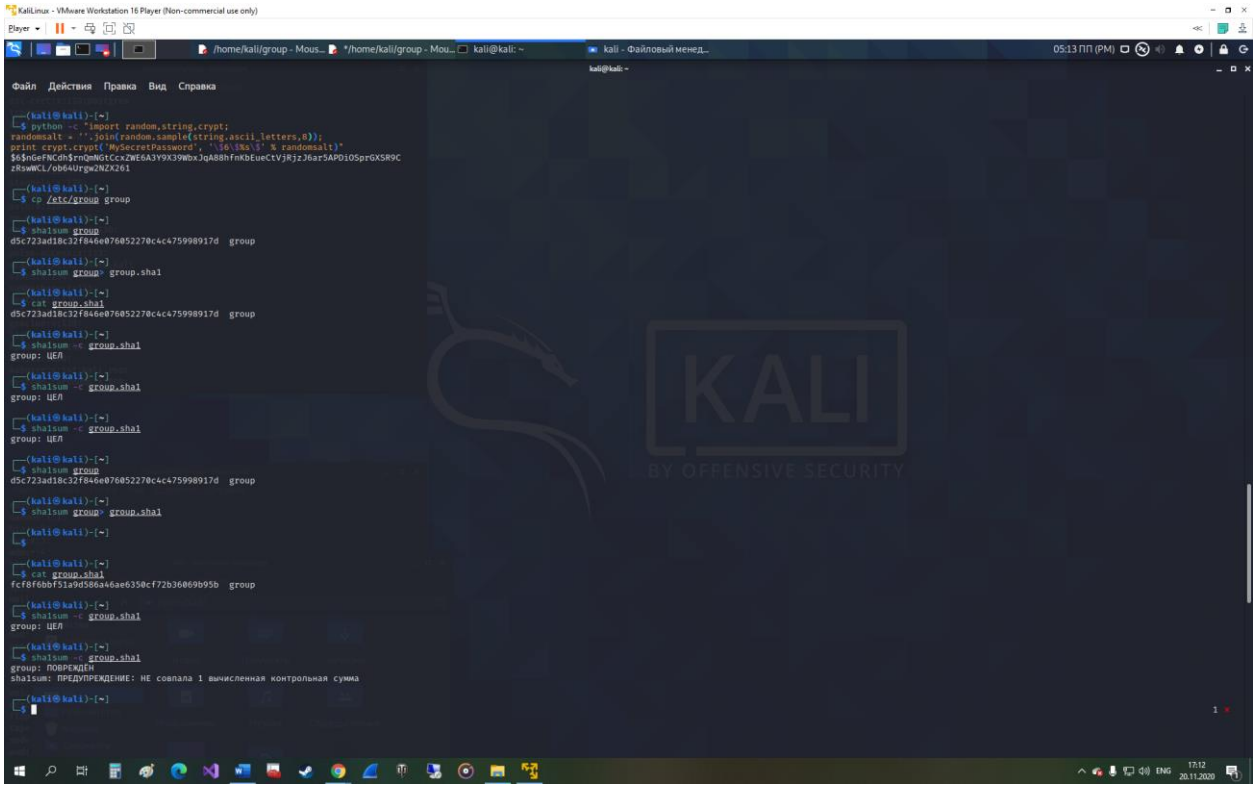
1.7 Задание. Определение типа hash

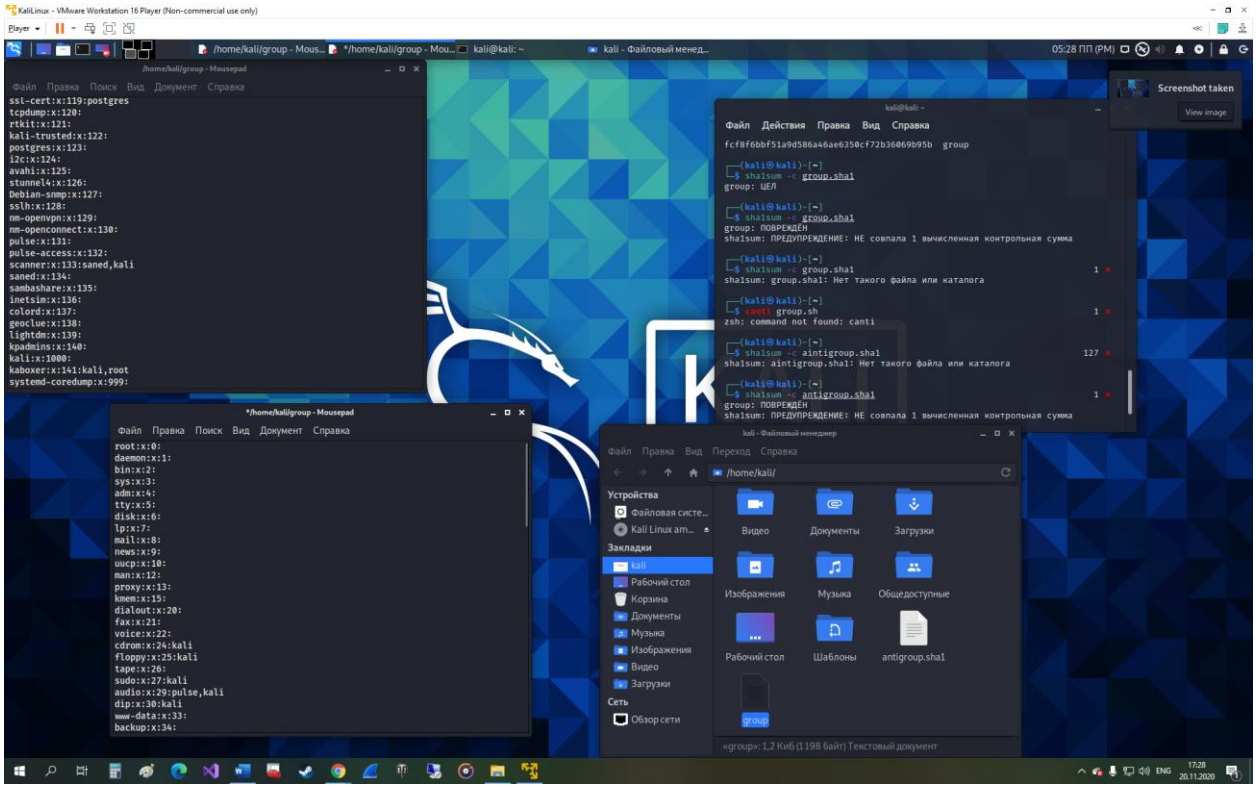


1.8 Задание. Создание hash в Linux

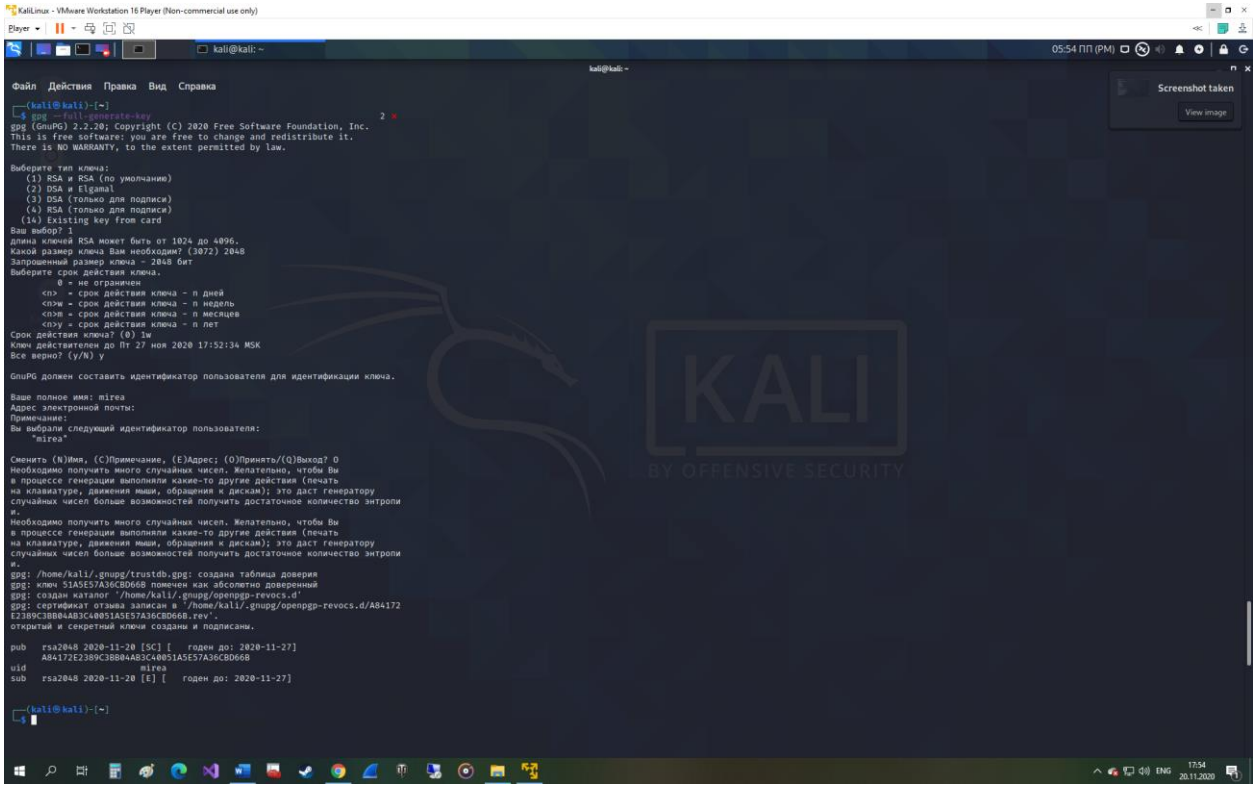


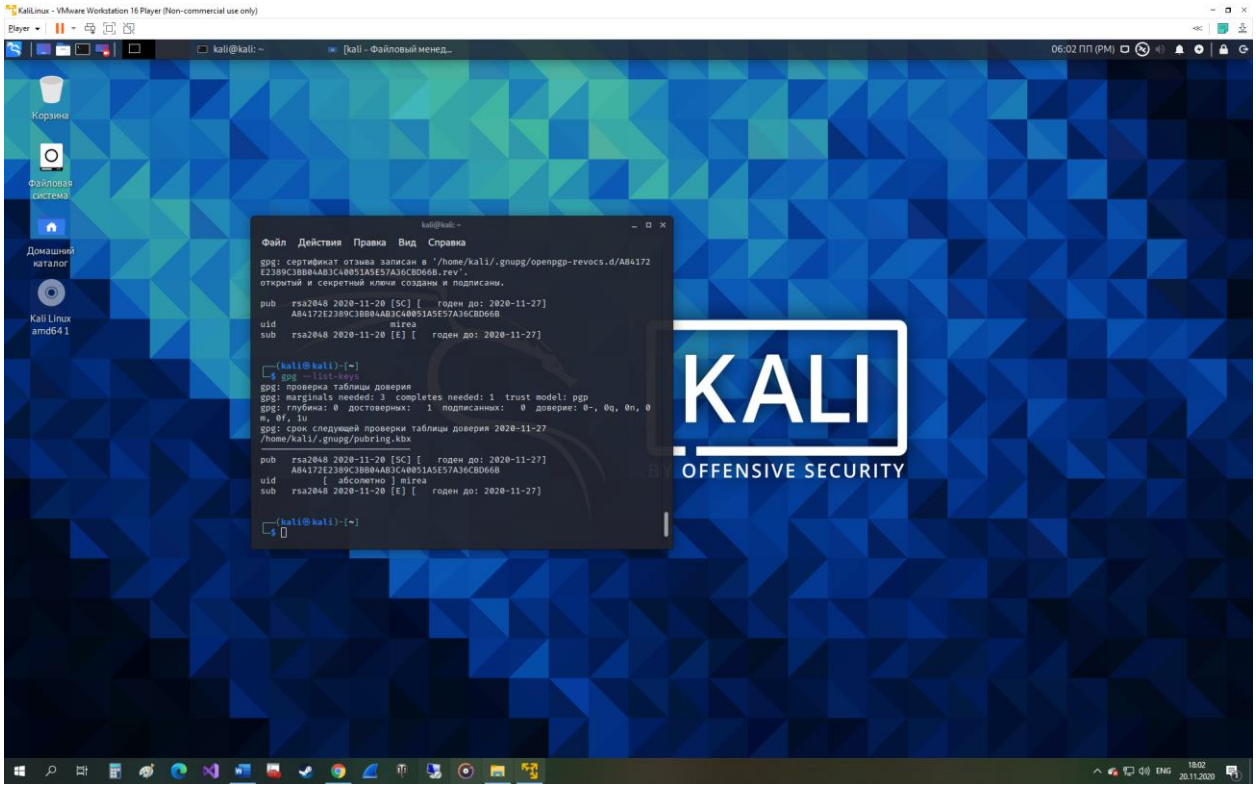
1.9 Задание. Проверка контрольных сумм

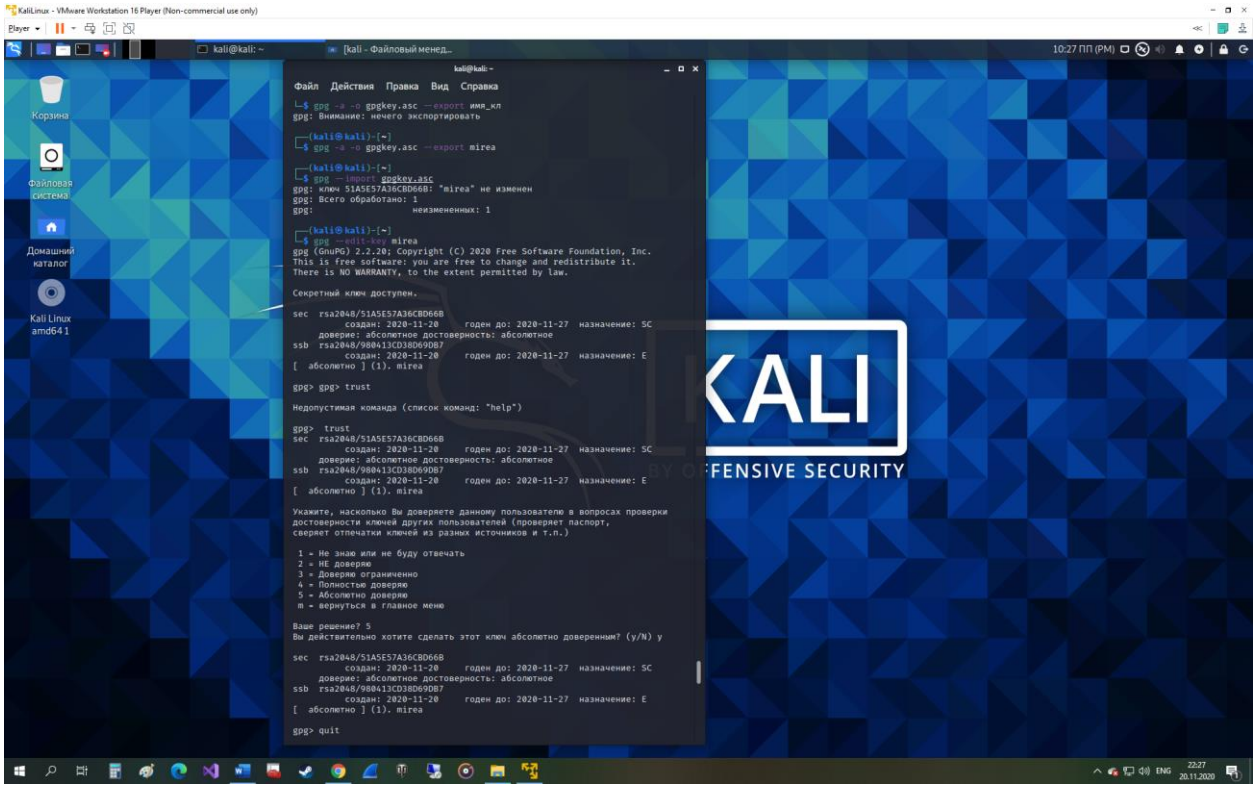


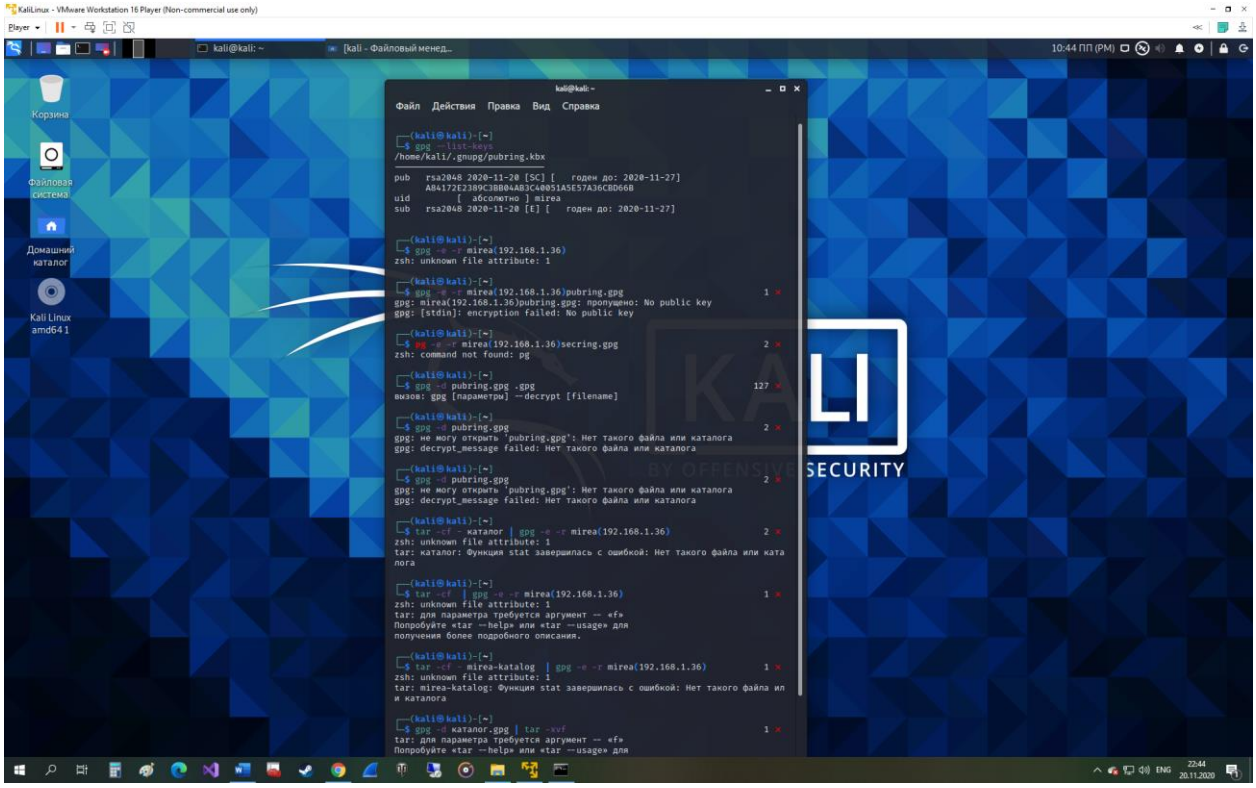


2.1.2 Задание. Шифрование с использованием ключей

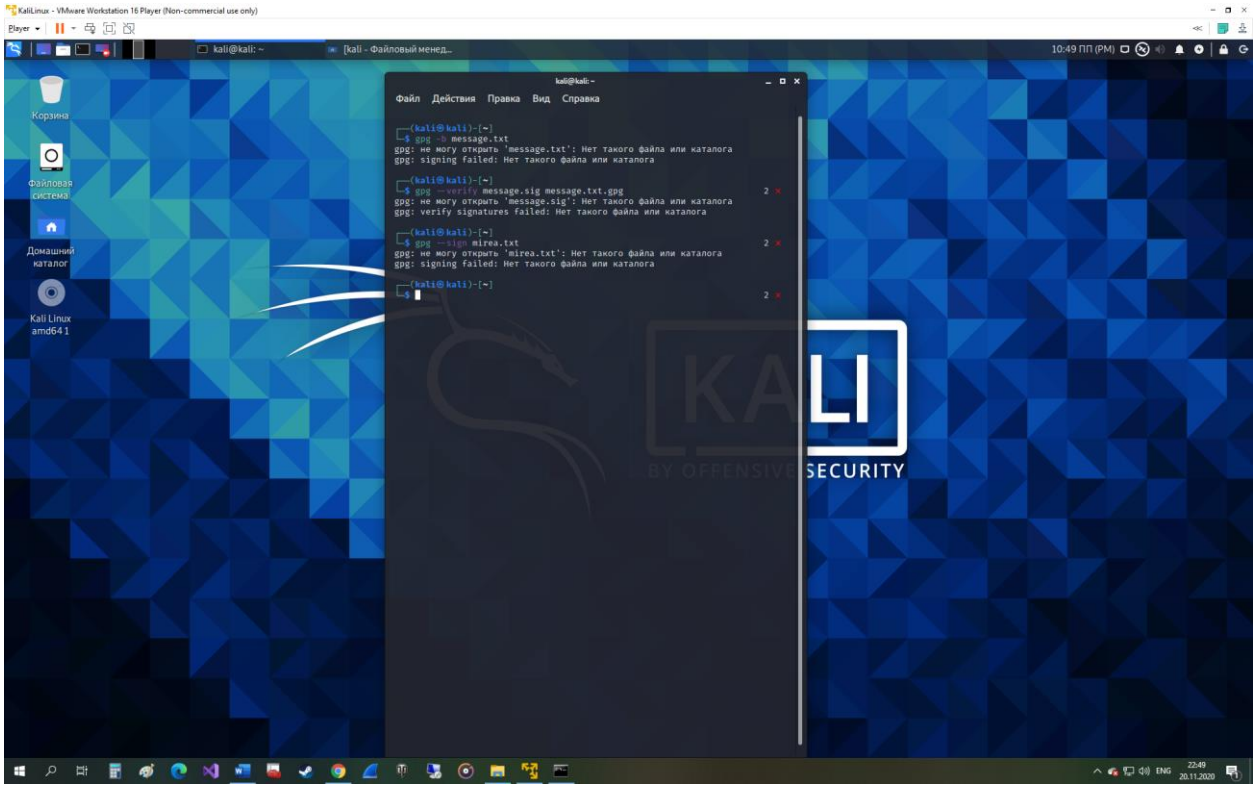

KaliLinux - VMware Workstation 16 Player (Non-commercial use only)
Player
kali@kali: ~
05:54 ПП (PM)
kali@kali: ~
Файл Действия Правка Вид Справка
Screenshot taken
View image
┌──(kali㉿kali)-[~]
└─$ gpg --full-generate-key
gpg (GnuPG) 2.2.20; Copyright (C) 2020 Free Software Foundation, Inc.
This is free 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) 1w
Ключ действителен до Пт 27 ноя 2020 17:52:34 MSK
Все верно? (y/N) y
GnuPG должен составить идентификатор пользователя для идентификации ключа.
Ваше полное имя: mirea
Адрес электронной почты:
Примечание:
Вы выбрали следующий идентификатор пользователя:
"mirea"
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: /home/kali/.gnupg/trustdb.gpg: создана таблица доверия
gpg: ключ 51A5E57A36CBD66B помечен как абсолютно доверенный
gpg: создан каталог '/home/kali/.gnupg/openpgp-revocs.d'
gpg: сертификат отзыва записан в '/home/kali/.gnupg/openpgp-revocs.d/A84172
E2389C3BB04AB3C40051A5E57A36CBD66B.rev'.
открытый и секретный ключи созданы и подписаны.
pub rsa2048 2020-11-20 [SC] [годен до: 2020-11-27]
A84172E2389C3BB04AB3C40051A5E57A36CBD66B
uid mirea
sub rsa2048 2020-11-20 [E] [годен до: 2020-11-27]
┌──(kali㉿kali)-[~]
└─$
ENG
17:54
20.11.2020


KaliLinux - VMware Workstation 16 Player (Non-commercial use only)
Player
kali@kali: ~
[kali - Файловый менед...
06:02 ПП (PM)
Корзина
Файловая система
Домашний каталог
Kali Linux amd64 1
kali@kali: ~
Файл Действия Правка Вид Справка
gpg: сертификат отзыва записан в '/home/kali/.gnupg/openpgp-revocs.d/A84172
E2389C3BB04AB3C40051A5E57A36CBD66B.rev'.
открытый и секретный ключи созданы и подписаны.
pub rsa2048 2020-11-20 [SC] [годен до: 2020-11-27]
A84172E2389C3BB04AB3C40051A5E57A36CBD66B
uid mirea
sub rsa2048 2020-11-20 [E] [годен до: 2020-11-27]
┌──(kali㉿kali)-[~]
└─$ gpg --list-keys
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, 0
m, 0f, 1u
gpg: срок следующей проверки таблицы доверия 2020-11-27
/home/kali/.gnupg/pubring.kbx
pub rsa2048 2020-11-20 [SC] [годен до: 2020-11-27]
A84172E2389C3BB04AB3C40051A5E57A36CBD66B
uid [абсолютно] mirea
sub rsa2048 2020-11-20 [E] [годен до: 2020-11-27]
┌──(kali㉿kali)-[~]
└─$
KALI
OFFENSIVE SECURITY
ENG
18:02
20.11.2020





2.1.3 Задание. Подписи и шифрование


KaliLinux - VMware Workstation 16 Player (Non-commercial use only)
Player
kali@kali: ~
[kali - Файловый менед...
10:49 ПП (РМ)
Корзина
Файловая система
Домашний каталог
Kali Linux amd64 1
kali@kali: ~
Файл Действия Правка Вид Справка
(kali㉿kali)-[~]
$ gpg -b message.txt
gpg: не могу открыть 'message.txt': Нет такого файла или каталога
gpg: signing failed: Нет такого файла или каталога
(kali㉿kali)-[~]
$ gpg --verify message.sig message.txt.gpg
gpg: не могу открыть 'message.sig': Нет такого файла или каталога
gpg: verify signatures failed: Нет такого файла или каталога
(kali㉿kali)-[~]
$ gpg --clear mirea.txt
gpg: не могу открыть 'mirea.txt': Нет такого файла или каталога
gpg: signing failed: Нет такого файла или каталога
(kali㉿kali)-[~]
$
BY OFFENSIVE SECURITY
ENG
22:49
20.11.2020