**Липецкий государственный технический университет**

Факультет автоматизации и информатики

Кафедра Автоматизированных систем управления

ЛАБОРАТОРНАЯ РАБОТА №7

по «ОПЕРАЦИОННАЯ СИСТЕМА LINUX»

Работа с SSH

Студент Самойлов В.Д.

Группа АИ-17

Руководитель

Доцент Кургасов В.В.

Липецк 2019г.

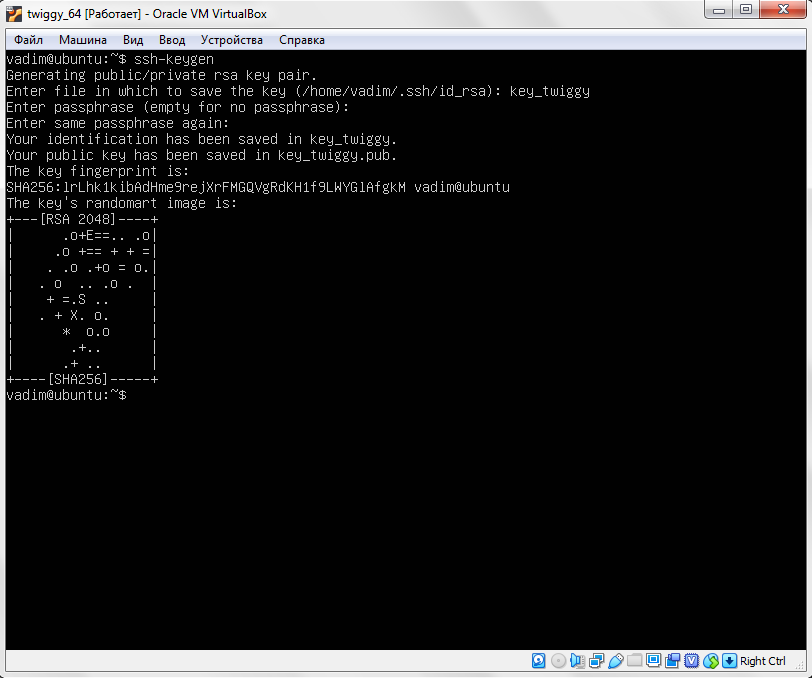
Цель работы

Лабораторная работа предназначена для целей практического ознакомления с программным обеспечением удаленного доступа к распределённым системам обработки данных.

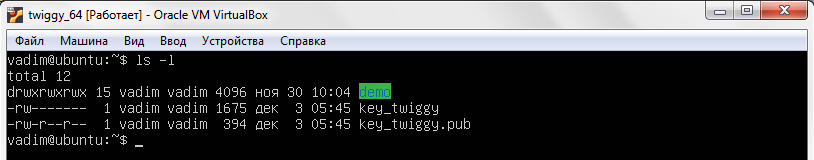
Задание кафедры

1. Создание ключа SSH из Linux.
2. Перемещение ключа на удаленный хост.
3. Создание конфигурационного файла, с помощью которого авторизация не требовала указать ключ идентификации.

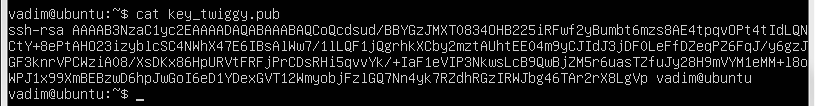
Ход работы

1. С помощью утилиты ssh-keygen создадим пару 2048 битных RSA ключей.
2. Пример создания ключа идентификации

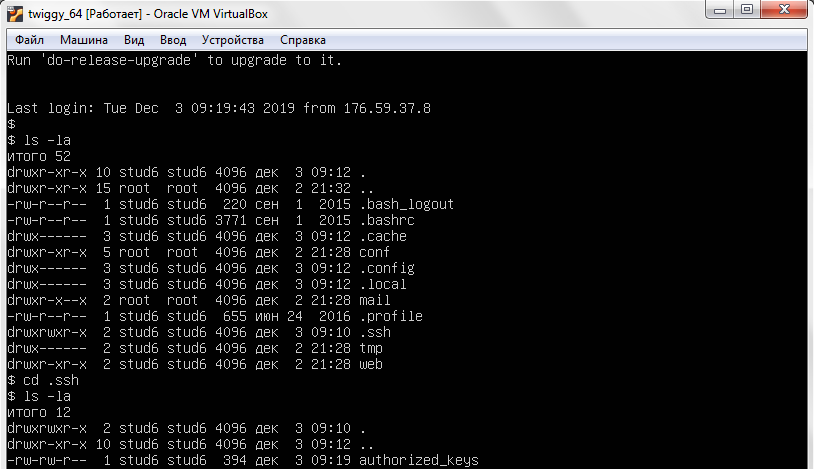
Результатом выполнения команды будет создано 2 файла: секретный ключ key\_twiggy и публичный ключ key\_twiggy.pub



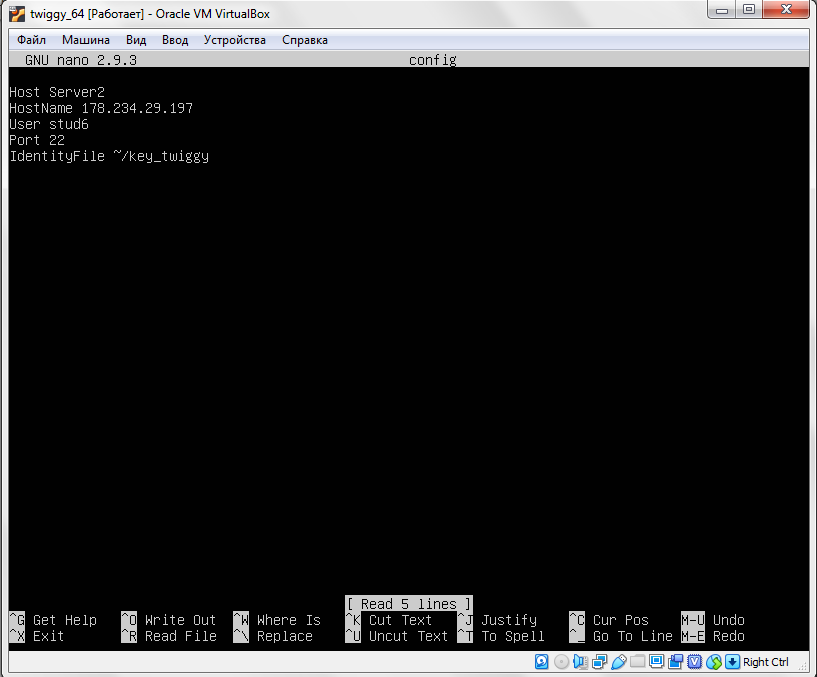
1. Результат выполнения команды ssh-keygen



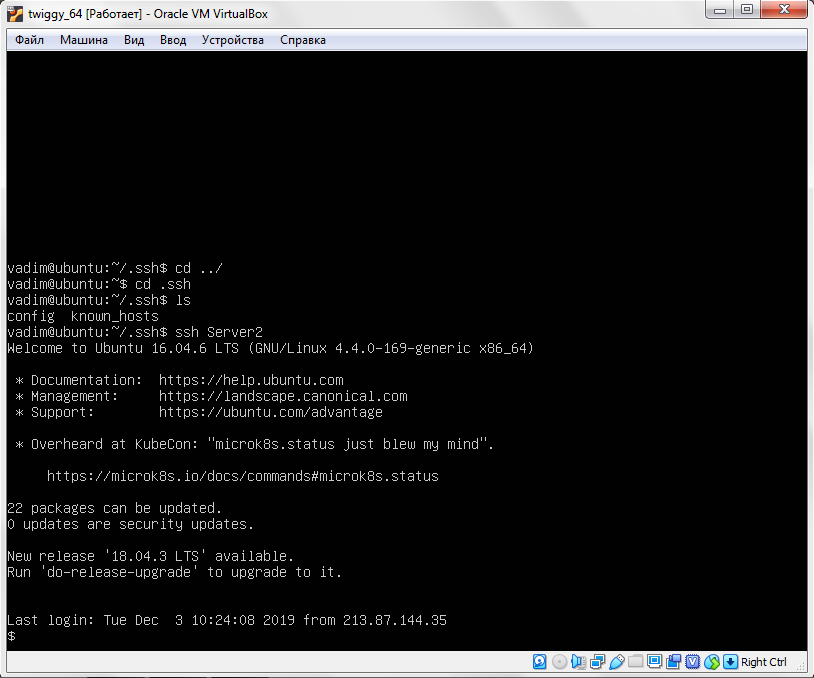
1. Содержимое публичного ключа
2. Скопируем публичный ключ на удаленный хост [www.kurgasov.ru](http://www.kurgasov.ru) командой «cat ~/key\_twiggy.pub | ssh [stud6@www.kurgsov.ru](mailto:stud6@www.kurgsov.ru) “mkdir –p ~/.ssh && cat >> ~/.ssh/authorized\_keys”»
   1. Авторизуемся с помощью логина и пароля на www.kurgasov.ru и найдем созданный файл authorized\_keys, при успешном перемещении публичного ключа на удаленный хост мы можем больше не использовать логин и пароль для авторизации.



1. Результат копирования публичного ключа на удаленный хост
2. После успешного создания ключа и переброса его на удаленный хост мы можем создать файл конфигурации, который избавит нас от необходимости помнить название ключа и логин.



1. Листинг файла конфигураций
   1. Попробуем осуществить авторизацию на сервере [www.kurgasov.ru](http://www.kurgasov.ru), используя файл конфигураций.



1. Пример успешной авторизации

Ответы на контрольные вопросы

1. SSH – зашифрованный протокол, который часто используется для взаимодействия и удаленного управления серверами. Он более удобен для применения, не нужно использовать пароль.
2. С помощью команды «ssh-keygen» можно сгенерировать ключ в ОС Linux. В ОС Windows можно воспользоваться программой PuTTY key Generator для создания ключа ssh.
3. Из публичного ключа можно сгенерировать закрытый и наоборот.
4. Ключи, созданные на одном ПК несколько раз с теми же исходными условиями всегда будут отличаться.
5. Доступные виды ключей:

* RSA
* DSA
* ECDSA
* Ed25519

1. Я думаю, что это можно сделать с различных ОС, но не с различных ПК.
2. С помощью процедуры Putty можно организовать подключение по ключу ssh к системе с ОС Windows, в которой запущен OpenSSh сервер.
3. [www.kurgasov.ru](http://www.kurgasov.ru)

Вывод

Ознакомился с программным обеспечением удаленного доступа к распределённым системам обработки данных.