Липецкий государственный технический университет

Кафедра прикладной математики

Отчет по лабораторной работе № 6
«Авторизация по ключу ssh»
по курсу «ОС Linux»

Студент _____ Гришагин Е.Е.
подпись, дата фамилия, инициалы

Группа ПМ-19-2

Руководитель

_____ _____ Кургасов В.В.
ученая степень, ученое звание подпись, дата фамилия, инициалы

Липецк 2022 г.

Содержание

Задание кафедры

Организовать доступ к удаленному серверу по ssh (без ввода пароля (по ключу)) имея следующие исходные данные:

- IP: 178.234.29.197
- Порт: 22
- Логин: stud2
- Пароль: w549QriOET

1. Ход работы

Запуск анализатора трафика tcpdump для telnet и его логирование.

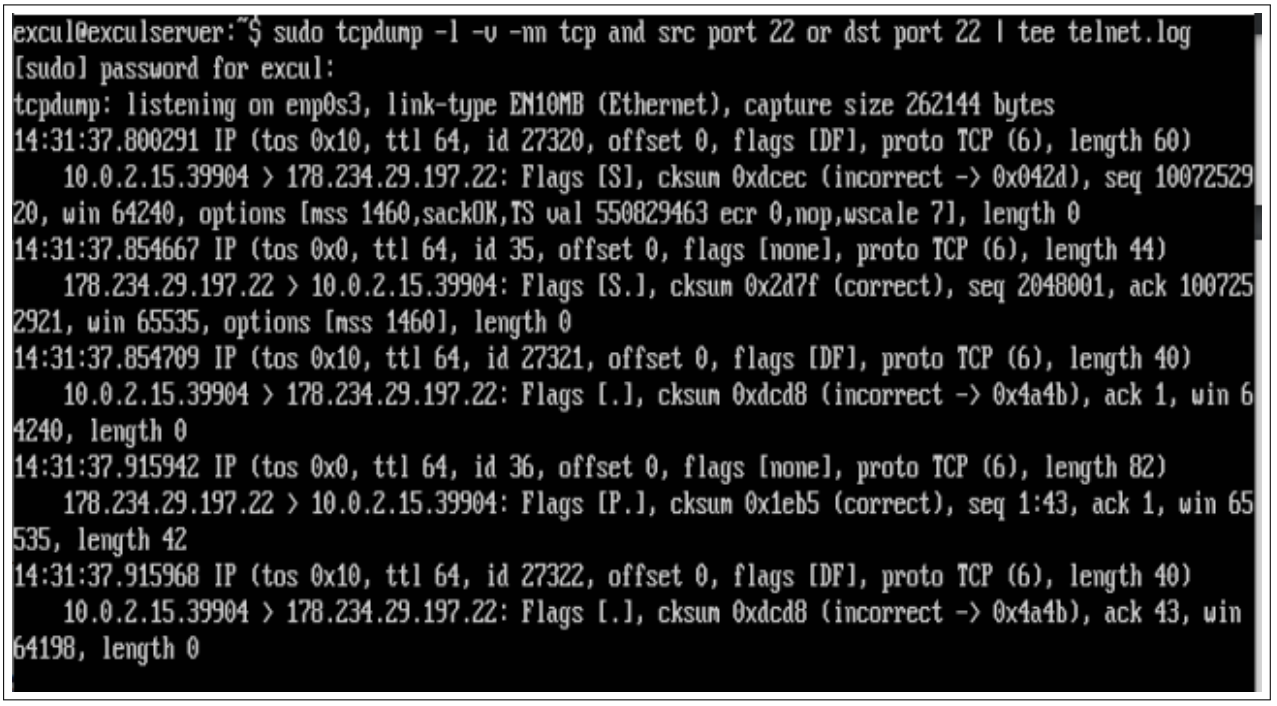

Рисунок 1 - Запуск анализатора трафика

Запуск telnet.

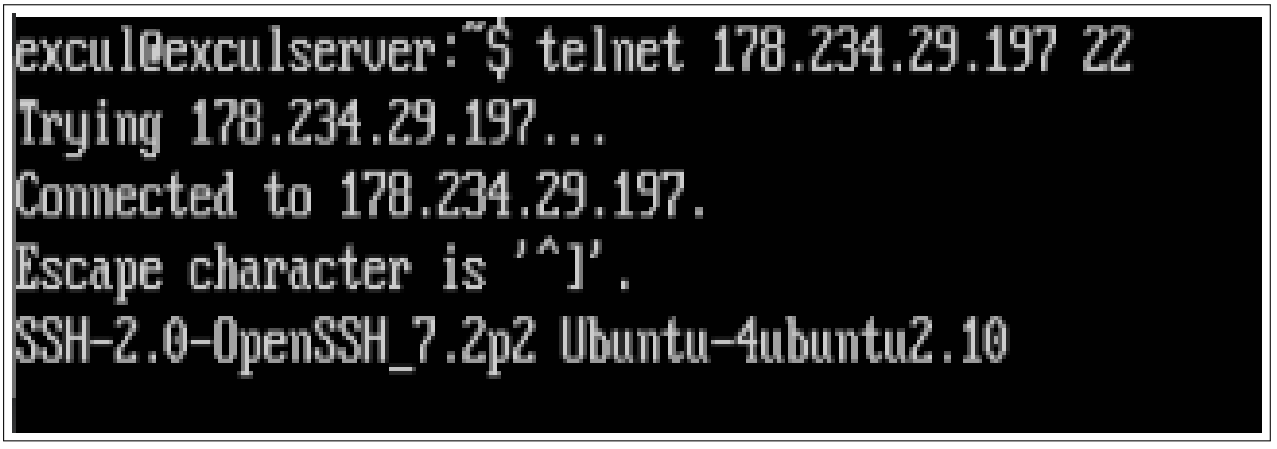

Рисунок 2 - Запуск telnet

Запуск анализатора трафика tcpdump для ssh и его логирование.

Рисунок 3 - Запуск анализатора трафика

Соединение с сервером через ssh при помощи логина и пароля

Рисунок 4 - Соединение с сервером через ssh

Защищённая передача файла с помощью логина и пароля

Рисунок 5 - Защищённая передача файла

Генерация ssh-ключа для безпарольной аутинтефикации.

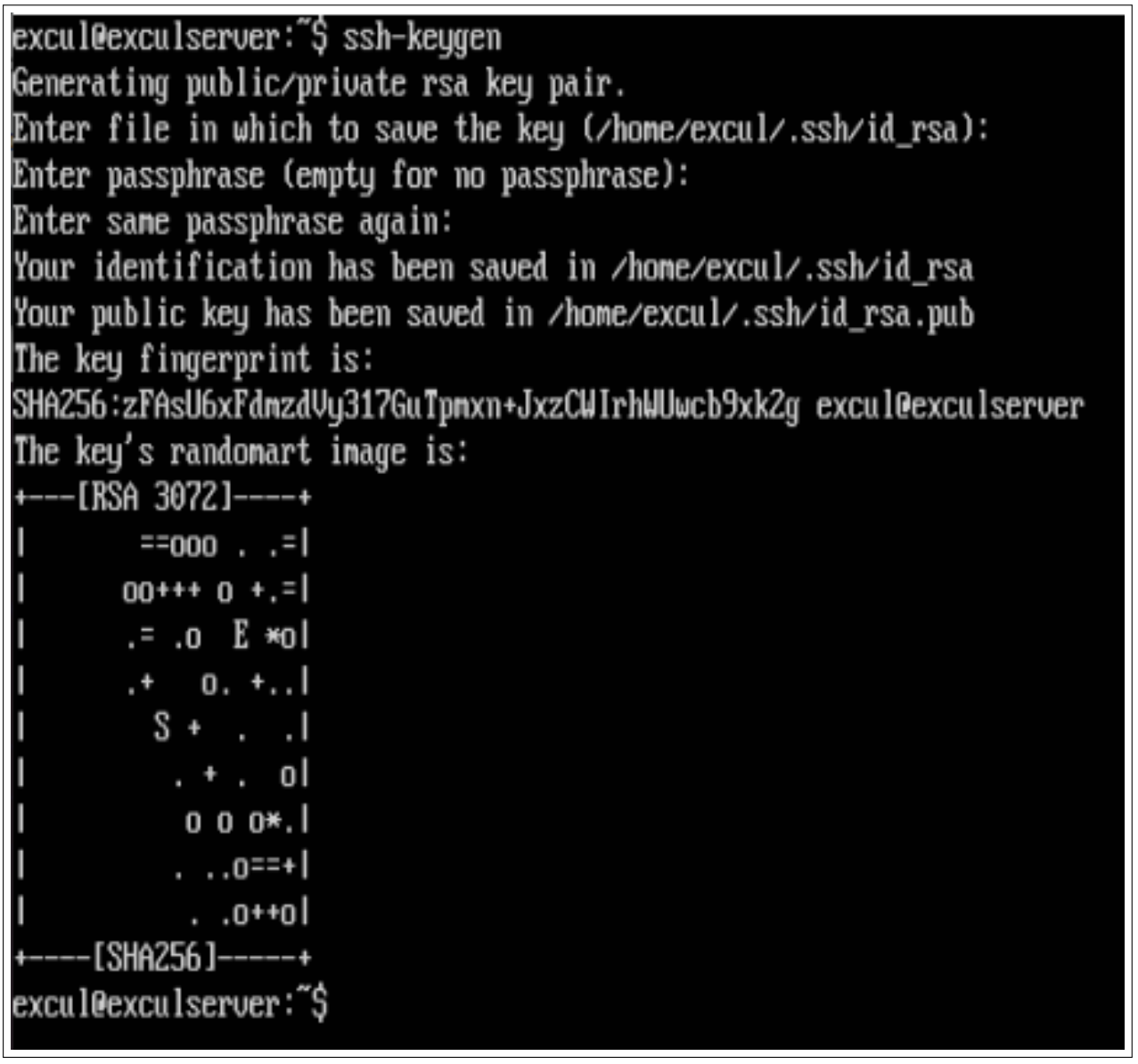

Рисунок 6 - Генерация ssh-ключа

Копирование публичной части сгенерированного ssh-ключа на сервер.

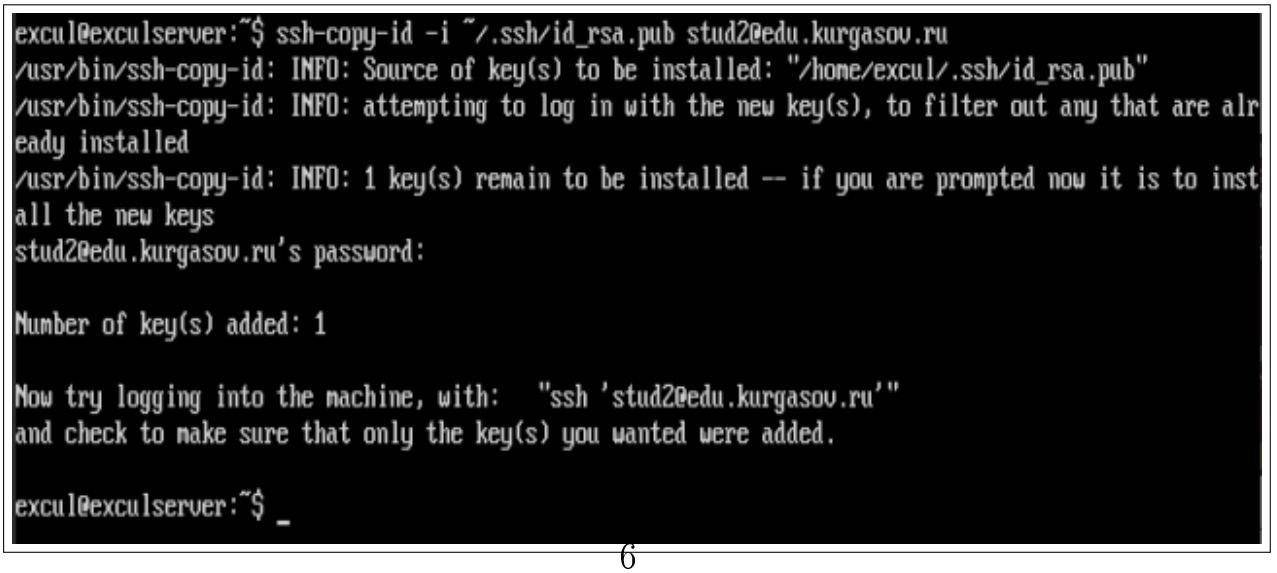

Рисунок 7 - Передача ключа на сервер

Соединение с сервером через ssh при помощи логина и ключа.

Рисунок 8 - Соединение с сервером через ssh

Лог telnet.

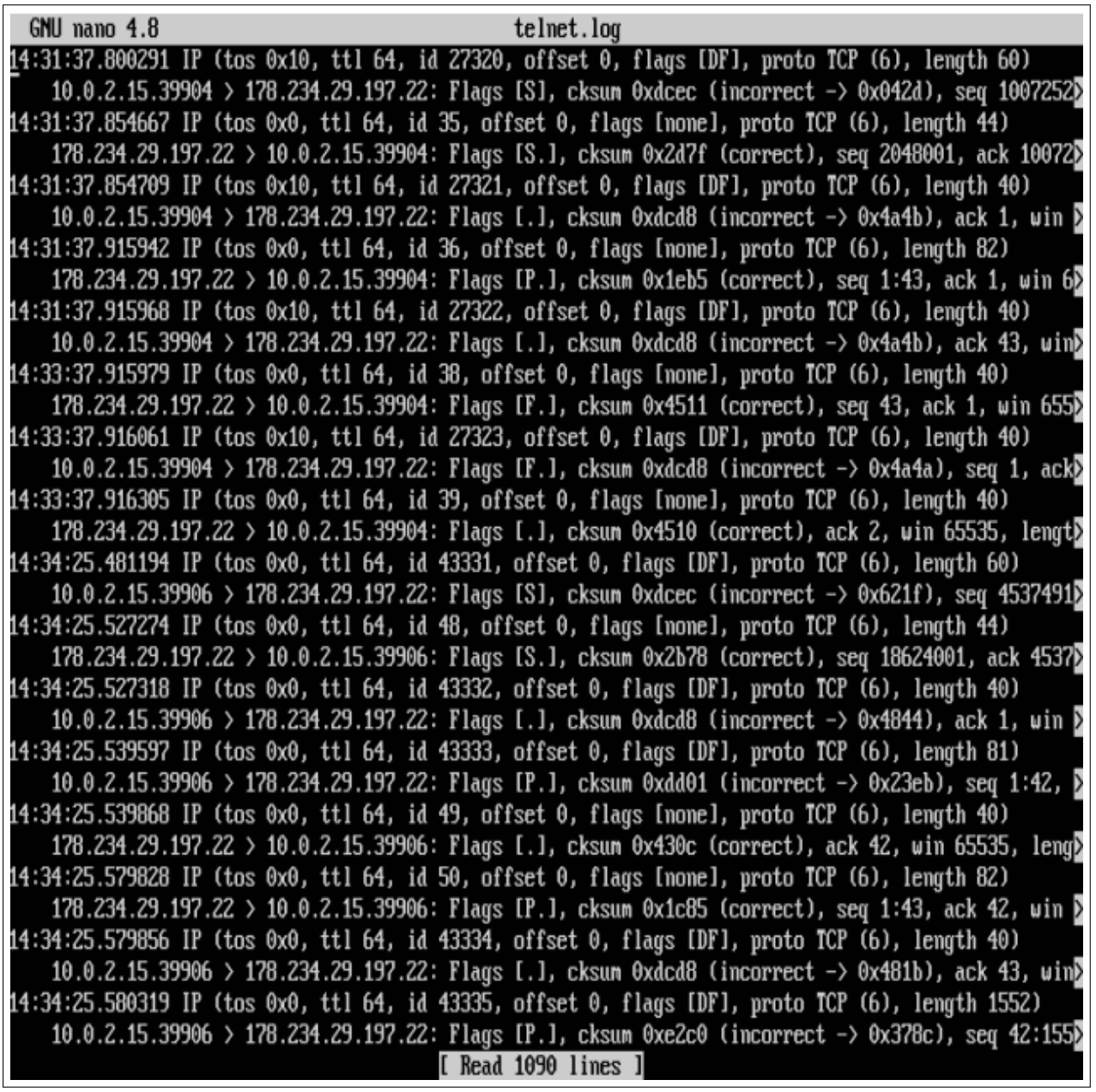

Рисунок 9 - Лог telnet.

Лог ssh.

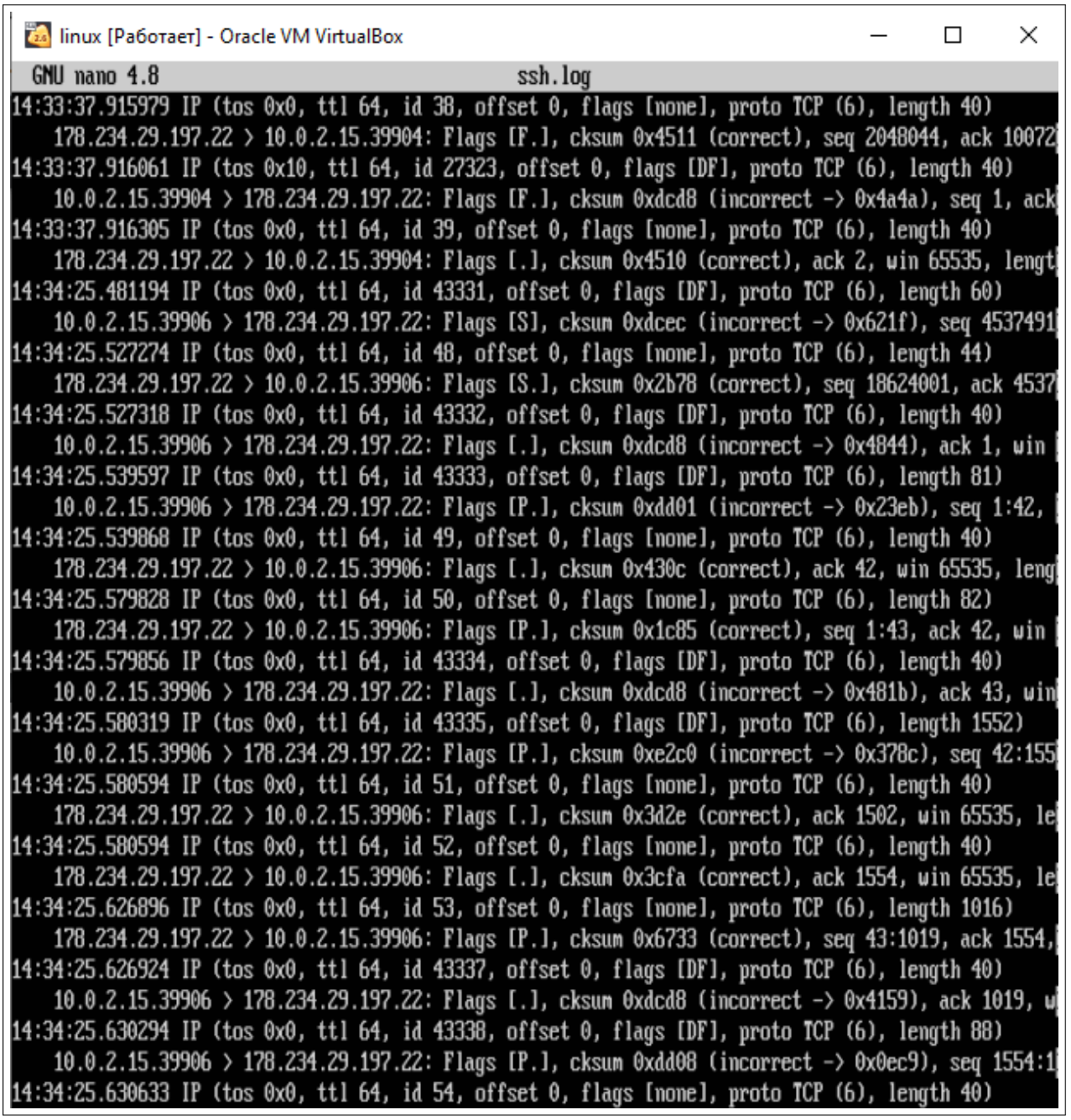

Рисунок 10 - Лог ssh.

2. Контрольные вопросы

1. Вопрос: Определите основные цели и задачи решаемые с помощью ПО удаленного доступа?
   Ответ: ПО удаленного доступа дает пользователю возможность подключаться к компьютеру с помощью другого устройства через интернет. Для создания удаленного подключения используют специальные программы. Обязательное условие — наличие постоянного доступа в интернет, компьютеров, обладающих определенными характеристиками и сервера. Такое ПО делает возможным подключение к другому компьютеру из любой точки мира. Программы позволяют видеть рабочий стол и выполнять все действия на удаленном устройстве, изменять настройки ПО, обмениваться файлами, шифровать передаваемые данные, проводить конференции, подключать веб-камеры, удаленные проекторы и прочие сетевые устройства.

2. Вопрос: Выделите отличительные особенности между режимами работы удаленного доступа по протоколам TELNET и SSH?
   Ответ:

   - Доступ к командной строке удаленного хоста одинаков для обоих протоколов, но основное различие этих протоколов зависит от меры безопасности каждого из них. SSH более защищен, чем TELNET.
   - По умолчанию SSH использует порт 22, а TELNET использует порт 23 для связи, и оба используют стандарт TCP.
   - SSH отправляет все данные в зашифрованном формате, а TELNET отправляет данные в виде обычного текста. Поэтому SSH использует безопасный канал для передачи данных по сети, а TELNET использует обычный способ подключения к сети и связи.
   - SSH использует шифрование с открытым ключом для аутентификации удаленных пользователей, а TELNET не использует механизмов аутентификации. 19
   - SSH больше подходит для использования в общедоступных сетях, а TELNET больше подходит для частных сетей.

•

3. Вопрос: Опишите способы установления соединения при использовании протокола SSH? Охарактеризуйте положительные и отрицательные аспекты приведенных методов.
   Ответ:

   - Значения параметров (высокий, средний, низкий) носят относительный характер и служат только для сравнения показателей.
   - Расход ресурсов сервера (процессор, диск, сетевой канал) на обработку запросов, обычно идущих на 22-й порт.
   - Произвести взлом, если для авторизации используются RSAключи, сложно, однако неограниченное количество попыток авторизации делает это возможным.
   - Количество попыток авторизации ограничено, но серверу приходится обрабатывать их от большого количества злоумышленников.

•

4. Вопрос: Основываясь на заданиях лабораторной работы, приведите практический пример использования систем удаленного доступа?
   Ответ: Системы удаленного доступа нужны тем компаниям, где большинство сотрудников находится за пределами офиса, на частичном фрилансе, аутсорсинге или в командировках, но при этом они нуждаются в обновлении рабочей информации, просмотре корпоративной почты и др. Им не нужно будет скачивать все необходимые для работы данные на внешний носитель или отправлять их по почте – достаточно связаться с офисным компьютером. Удаленный доступ используют системные администраторы для управления системой и устранения сбоев в ее работе, и руководители, желающие проконтролировать процесс выполнения задачи своими подчиненными.

5. Вопрос: Перечислите распространенные сетевые службы, основанные на использовании шифрованного соединения по протоколу SSH? Приведите пример использования службы передачи файлов по безопас-

ному туннелю?

Ответ: Распространенные сетевые службы, основанные на использовании шифрованного соединения по протоколу SSH: OpenSSH, PuTTY/KiTTY, SecureCRT, Xshell. Службы передачи файлов по безопасному туннелю можно использовать для передачи паролей.