**РОССИЙСКИЙ УНИВЕРСИТЕТ ДРУЖБЫ НАРОДОВ ИМЕНИ ПАТРИСА ЛУМУМБЫ**

**Факультет физико-математических и естественных наук**

**Кафедра теории вероятностей и кибербезопасности**

ОТЧЕТ

по лабораторной работе № 15

Дисциплина «Администрирование сетевых подсистем»

*Тема «Настройка сетевого журналирования»*

Студент: Щербак Маргарита Романовна

Ст. билет: 1032216537

Группа: НПИбд-02-21

**МОСКВА**

2023 г.

# Цель работы

Получение навыков по работе с журналами системных событий.

# Задание

1. Настроить сервер сетевого журналирования событий.
2. Настроить клиент для передачи системных сообщений в сетевой журнал на сервере.
3. Просмотреть журналы системных событий с помощью нескольких программ. При наличии сообщений о некорректной работе сервисов исправить ошибки в настройках соответствующих служб.
4. Написать скрипты для Vagrant, фиксирующие действия по установке и настройке сетевого сервера журналирования.

**Выполнение**

**1. Настройка сервера сетевого журнала**

**2. Настройка клиента сетевого журнала**

**3. Просмотр журнала**

**4. Внесение изменений в настройки внутреннего окружения виртуальных машин**

**Вывод:** таким образом, в ходе выполнения л/р №15 я получила навыки по работе с журналами системных событий.

# Контрольные вопросы

1. Какой модуль rsyslog вы должны использовать для приёма сообщений от journald?
2. Как называется устаревший модуль, который можно использовать для включения приёма сообщений журнала в rsyslog?
3. Чтобы убедиться, что устаревший метод приёма сообщений из journald в rsyslog

не используется, какой дополнительный параметр следует использовать?

1. В каком конфигурационном файле содержатся настройки, которые позволяют вам настраивать работу журнала?
2. Каким параметром управляется пересылка сообщений из journald в rsyslog?
3. Какой модуль rsyslog вы можете использовать для включения сообщений из файла журнала, не созданного rsyslog?
4. Какой модуль rsyslog вам нужно использовать для пересылки сообщений в базу данных MariaDB?
5. Какие две строки вам нужно включить в rsyslog.conf, чтобы позволить текущему журнальному серверу получать сообщения через TCP?
6. Как настроить локальный брандмауэр, чтобы разрешить приём сообщений журнала через порт TCP 514?