**МИНИСТЕРСТВО ЦИФРОВОГО РАЗВИТИЯ, СВЯЗИ И МАССОВЫХ КОММУНИКАЦИЙ РОССИЙСКОЙ ФЕДЕРАЦИИ**

**ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ**

**УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ**

**«САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ТЕЛЕКОММУНИКАЦИЙ ИМ. ПРОФ. М.А. БОНЧ-БРУЕВИЧА»**

**(СПбГУТ)**

Институт магистратуры

Кафедра Защищенных систем связи

Дисциплина Технологии обеспечения информационной безопасности больших данных

**ОТЧЕТ ПО ЛАБОРАТОРНОЙ РАБОТЕ № 5**

Falco - инструмент для обнаружения аномалий и мониторинга активности в системе *(тема отчета)*

Направление/специальность подготовки

     10.04.01 - Информационная безопасность

*(код и наименование направления/специальности)*

Студенты:

Фёдорова О.В. ИКТБ-18м

*(Ф.И.О., № группы) (подпись)*

Салита А. С. ИКТБ-18м

*(Ф.И.О., № группы) (подпись)*

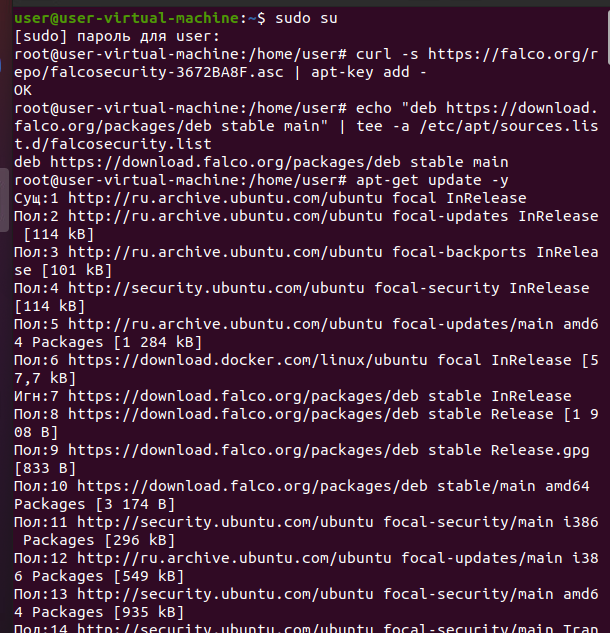
Проверил:

         Виткова Л. А.

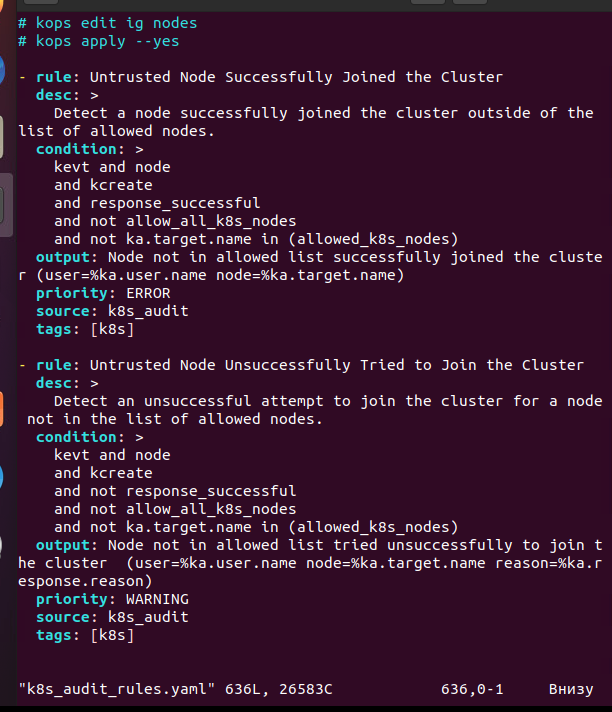
*(Ф.И.О.) (подпись)*

**Ход работы:**

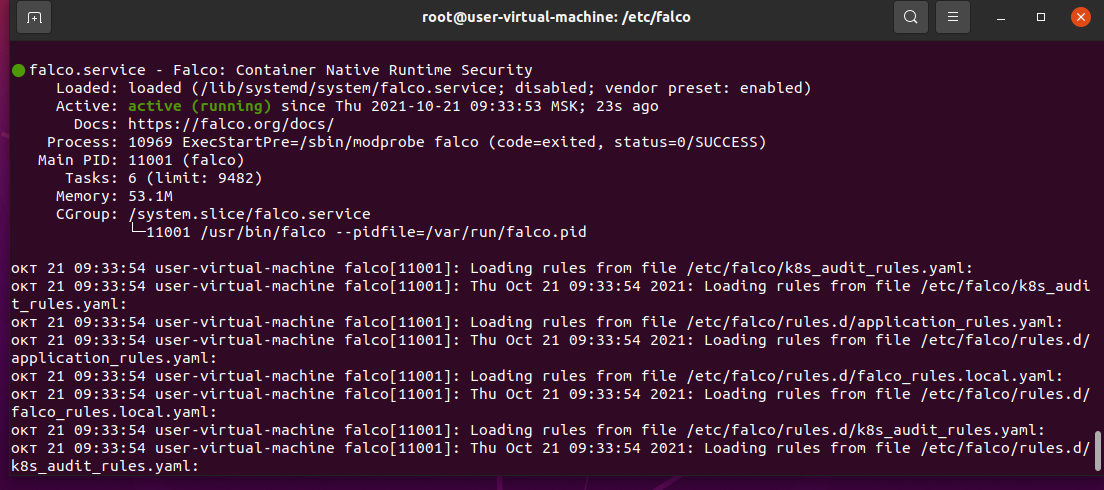
Перед установкой необходимо обновить систему. Также необходимо установить kernel headers.  
Через команду *apt-get install -y falco* устанавливаем falco на нашу машину с докерконтейнерами.



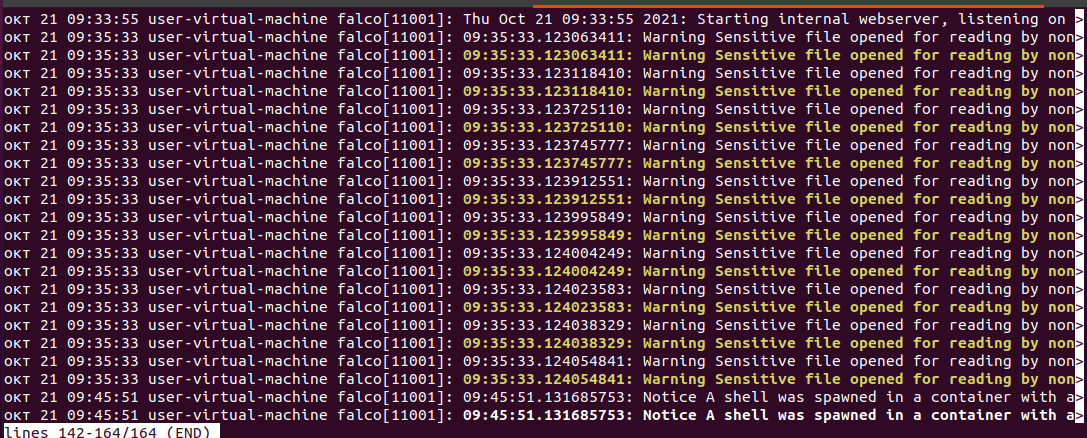
После можно запустить falco и загрузить правила в директорию /etc/falco/rules.d/ :



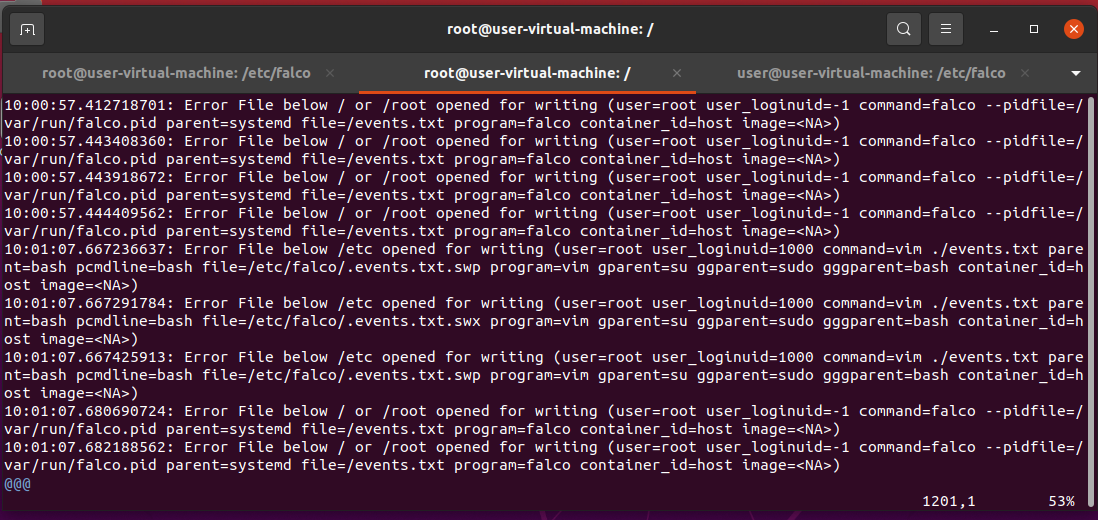
Запускаем Falco и проверяем статус работы:



Falco работает и пишет в syslog.



Также возможна и отдельная запись событий в логфайл. Для этого необходимо включить её в файле falco.yam. По умолчанию файл с логами находится в самой верхней директории (/) и называется events.txt



**Вывод:**

В ходе лабораторной работы была выполнена установка Falco на машину Ubuntu 20.4, была проверена работоспособность данной утилиты.