# Тестовое задание для стажера на позицию

# «Инженер» в ЦНИПР

## Задание №1

1. Создать две виртуальные машины (ВМ) под управлением любого Linux. Гипервизор – любой, работающий под Windows. Связать ВМ при помощи виртуальной сети. Проверить, что ping успешно проходит.
2. На одной ВМ (Клиент) разработать с использованием C/C++ ПО Агент, который будет запускаться автоматически вместе с Клиентом, регулярно собирать какие-либо данные о функционировании Клиента и отправлять их на другую ВМ (Сервер\_ML). Какие собирать данные остается на усмотрение исполнителя, но желательно, чтобы они были важны с точки зрения информационной безопасности. Идеально, если по этим данным можно обнаружить атаку на/компрометацию Клиента.
3. На Сервере\_ML разработать с использованием Python/C/C++ ПО Детектор, который будет регулярно принимать данные от Агента, оцифровывать их и выполнять классификацию или обнаружение аномалий с помощью ML. Механизм Детектора остается на усмотрение исполнителя.
4. Провести тестирование всей системы, демонстрирующее, что при выполнении аномальных операций на Клиенте Сервер\_ML их своевременно (в пределах периода получения данных от Клиента) обнаруживает и выдает сообщение об этом на консоль или в файл.

Примеры подозрительной активности на Клиенте, о которой можно собирать информацию: вход в систему в нерабочее время, повышение привилегий аккаунта, изменение сетевых каталогов, выполнение аномальных для данной системы команд, аномальный трафик или объем трафика и др.

Исполнитель может использовать что-то из перечисленного или придумать любой свой вариант реализации.

## Требования к присылаемым решениям:

Присылаемое решение должно содержать:

* готовый стенд, который, может быть запущен и проверен на любом ПК под управлением Windows, с установленным гипервизором;
* исходный код Агента и Детектора;
* отчет, содержащий: схему и описание стенда, план и результат тестирования стенда.

## Максимальное время на выполнение задания: 3 недели.