**ДИПЛОМНОЕ ИССЛЕДОВАНИЕ**

на тему:

**Анализ защищенности информационных систем от внешних угроз**

Выполнил:

Анохин Николай Егорович, 10 класс «И»

Руководитель

Коняхин Александр Валерьевич

подпись \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Содержание

[**Введение**](#_k0wz1jw32hp9) **3**

[**Пособие**](#_8h9r0gez8zb1) **4**

[**Вывод**](#_steevf11w8d3) **6**

[**Источники**](#_7hgnxq46hc4j) **7**

# Введение

Некоммерческая ассоциация WorldSkills была основана в 1953 году с целью привлечения молодых людей к рабочим профессиям и улучшения профессионального образования. Основная деятельность организации – проведение конкурсов профессионального мастерства для школьников и студентов по всему миру. На сегодняшний в движении участвуют 76 стран, в том числе и Россия. Участники соревнуются в двух возрастных категориях –14-16 лет в 72 компетенциях и 16-20 лет в 91 компетенции. Соревнования проводятся по 72 компетенциям для младших участников и по 91 компетенции для старших.

В своей работе я хочу рассмотреть задания компетенции «Анализ защищенности информационных систем от внешних угроз».

Анализ защищенности ИС от внешних угроз - важное направление, потому что крупные компании часто сталкиваются с проблемой различных атак извне. Задача специалистов - находить и своевременно устранять бреши в системах безопасности. Однако зачастую проблем в системах безопасности на уровне железа и даже программного обеспечения нет. Угрозу могут загрузить в сеть сотрудники, поэтому расследование инцидентов тоже ложится на плечи специалистов.

## Пособие

На соревнованиях участникам были предоставлены стандартные средства kali linux. Kali linux был развернут на виртуальной машине с помощью приложения virtualbox. Для корректного взаимодействия между машинами необходимо правильно настроить тип сети virtualbox. Выбираем сеть NAT. NAT (Network Address Translation — «преобразование сетевых адресов») — это механизм в сетях TCP/IP, позволяющий преобразовывать IP-адреса транзитных пакетов. (транзитным пакетом называется пакет, который передается между двумя узлами сети). В первом модуле нужно было найти уязвимости виртуальной машины. Для этого нужно было просканировать порты с помощью встроенной в kali linux утилиты - “Nmap” в терминале вводим “nmap localhost” и получаем вывод открытых портов если открыт 445/tcp, или 139/tcp, или 137/udp, или 135/tcp, то система уязвима. Поскольку в рамках задания у нас нет root доступа к виртуальной машине, все сводится к тому, что необходимо правильно настроить virtualbox.

Во втором задании требовалось настроить web сервер с использованием apache и css. Проблема была в опять же в переносе данных с windows на виртуальную машину, чтобы это сделать в настройках виртуальной машины выбираем пункт общие папки и добавляем папку с данными. Также необходимо уметь настраивать apache. Надо настроить виртуальный хост. Настроить права доступа к директориям, и указать там общую папку, которую мы указывали до этого в настройках виртуальной машины. Коротко о настройках apache:

 Файл /etc/apache2/apache2.conf отвечает за основные настройки

/etc/apache2/conf-available/\* - дополнительные настройки веб-сервера

/etc/apache2/mods-available/\* - настройки модулей

/etc/apache2/sites-available/\* - настройки виртуальных хостов

/etc/apache2/ports.conf - порты, на которых работает apache

 В третьем задании необходимо было расследовать инцидент и восстановить работоспособность системы. Надо просканировать порты при помощи nmap, однако все порты закрыты. Затем с помощью команды “sudo apt get upgrade” можно просмотреть список пакетов, которые можно обновить, какие-то недостающие пакеты скачаются заново. Также в процессе выполнения команды можно посмотреть, какие пакеты система будет обновлять. Также можно просканировать систему на наличие вирусов с помощью camscan - встроенного в kali linux антивируса. Запускаем антивирусное сканирование командой “sudo clamscan -r /”.

В задании все свелось к отсутствию файла конфигурации apache. Он установлен заново после “sudo apt upgrade”.

### Вывод

Для успешного выступления на соревнованиях необходимо изучать linux, потому что для большинства задач используется linux. Также я бы рекомендовал посещать курсы подготовки к соревнованиям. Важно не волноваться больше чем надо и описывать свои действия. Внимательно читайте задания, не стесняйтесь обращаться к техническому специалисту. Перед соревнованиями попробуйте разобраться с virtualbox.

#### Источники

1. Worldskills Russia Moscow 2018
<https://worldskills.ru/o-nas/dvizhenie-worldskills/czel-i-missiya.html>
2. Конкурсное задание компетенции анализ защищенности информационных систем от внешних угроз
<https://ocm18.worldskills.moscow/kompetentsii/#comp_list>
3. Статья про настройку apache
<https://losst.ru/ustanovka-i-nastrojka-servera-apache>