МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное образовательное учреждение  
высшего образования «Ижевский государственный технический  
университет имени М. Т. Калашникова»

Институт «Информатика и вычислительная техника»

Кафедра «Защита информации в компьютеризированных системах»

**ОТЧЕТ**

по лабораторной работе №2

по дисциплине «Разработка и эксплуатация защищенных автоматизированных систем»

на тему «Установка и настройка средств защиты на периметре локально вычислительной сети программно-аппаратным комплексом UTM Usergate»

Выполнили:  
студент гр. С17-361-1 Буров К.А.

Проверил:  
ст. преп. П. А. Кудашев

Ижевск 2021

# **Содержание**

[**Содержание** 2](#_Toc84785621)

[**Цель работы** 3](#_Toc84785622)

[**Задачи** 3](#_Toc84785623)

[**Ход работы** 4](#_Toc84785624)

[1. Схема сети 4](#_Toc84785625)

[2. Настройка интерфейсов 6](#_Toc84785626)

[3. Настройка маршрутизации. 7](#_Toc84785627)

[4. Настройка DNS 7](#_Toc84785628)

[5. Настройка NTP 8](#_Toc84785629)

[6. Настройка зон 8](#_Toc84785630)

[7. Создание пользователей 8](#_Toc84785631)

[8. Создание групп 9](#_Toc84785632)

[9. Настройка NAT 9](#_Toc84785633)

[10. Настройка правил межсетевого экрана 9](#_Toc84785634)

[11. Настройка правил фильтрации 10](#_Toc84785635)

[12. Тестирование 10](#_Toc84785636)

[**Вывод** 12](#_Toc84785637)

# **Цель работы**

Обеспечить защиту локальной вычислительной сети, посредством создания защищенного периметра на границе с недоверенными участками сети с помощью UTM-решения Usergate.

# **Задачи**

1. Указать схему сети.
2. Настроить интерфейсы.
3. Настроить маршрутизацию.
4. Настроить DNS.
5. Настроить NTP.
6. Настроить зоны.
7. Завести пользователей.
8. Завести группы.
9. Настроить NAT.
10. Настроить правила межсетевого экрана.
11. Настроить правила фильтрации.
12. Протестировать накстроенные правила

# **Ход работы**

## Схема сети

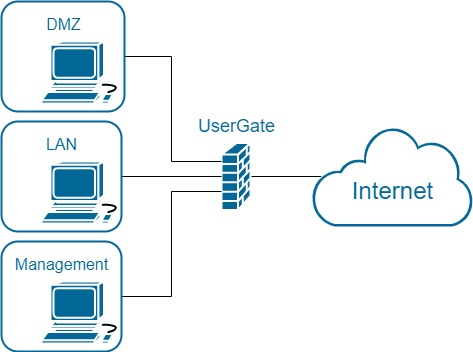


Рисунок 1- Схема сети

Перед выполнение лабораторной работы необходимо настроить стенд. Стенд будет содержать виртуальную машину Usergate, хост в качестве станции администратора и виртуальная машина Kali Linux в качестве рабочей станции пользователя.

Сконфигурируем сетевые адаптеры UTM следующим образом :

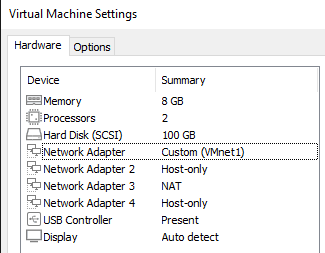


Рисунок 2 - Сетевые адаптеры Usergate

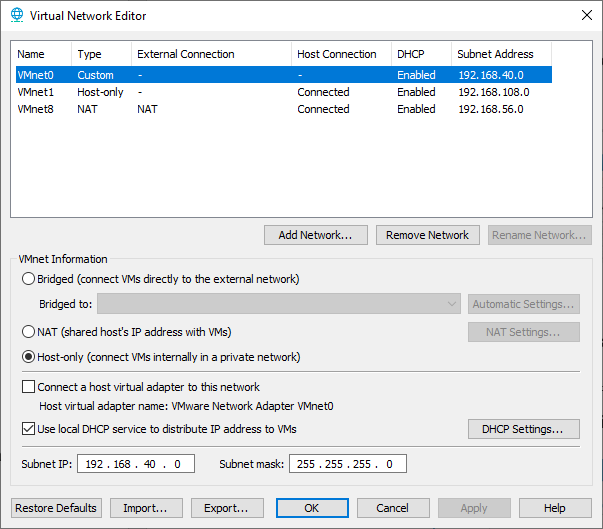


Рисунок 3 - Настройка виртуального адаптера

Запустим UTM – решение и подождем пока интерфейсам будут назначены IP адреса по DHCP.

После этого подключаемся к веб-консоли по назначенному адресу https://192.168.108.129:8001. И производим первоначальную инициализацию продукта.

Далее авторизуемся под учетной записью Admin

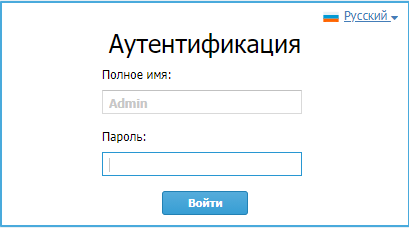


Рисунок 4 - Авторизация в веб-консоли

## Настройка интерфейсов

Для настройки интерфейсов необходимо в веб-консоли перейти на вкладку «Сеть» и выбрать «интерфейсы».

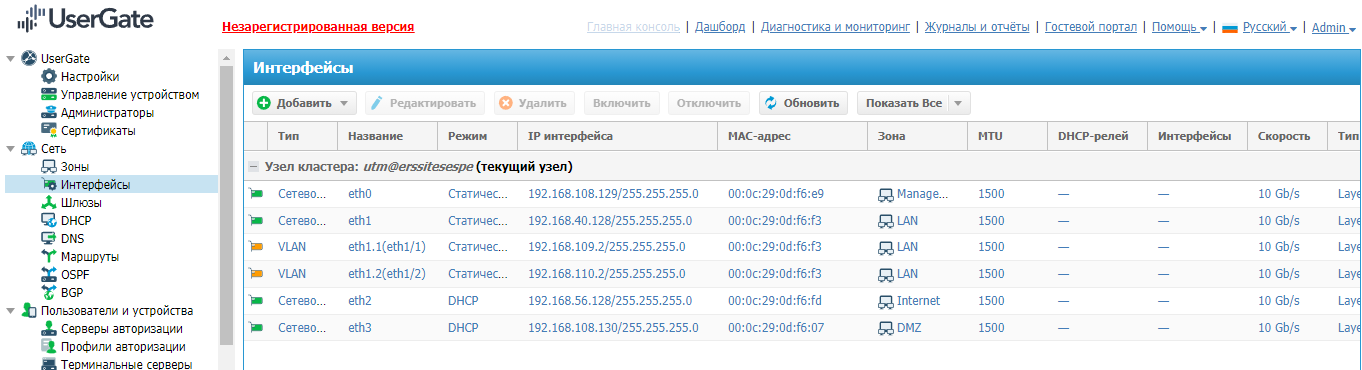


Рисунок 5 - Настройка интерфейсов

Выбираем нужный адаптер и включаем его. Далее в окне «Свойства интерфейса» выбираем режим (статический) и добавляем ip адрес.

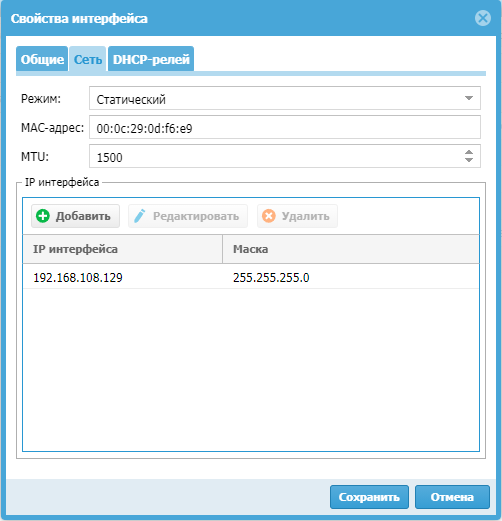


Рисунок - Свойства интерфейса

## Настройка маршрутизации.

Зададим ip адрес шлюза. При корректной настройке слева будет гореть зеленая лампочка.

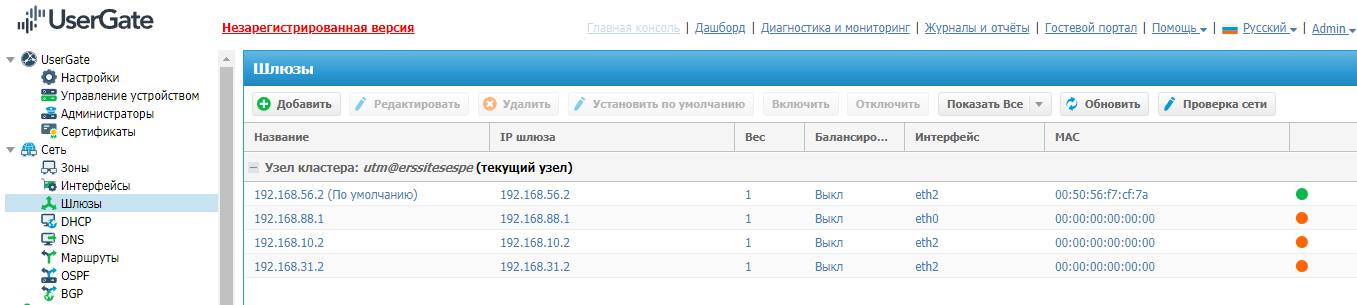


Рисунок 7 - Настройка шлюза

## Настройка DNS

Установим адрес DNS-сервера. Для этого откроем на вкладке «сеть» параметр «DNS». В открывшемся окне нажимаем кнопку добавить.

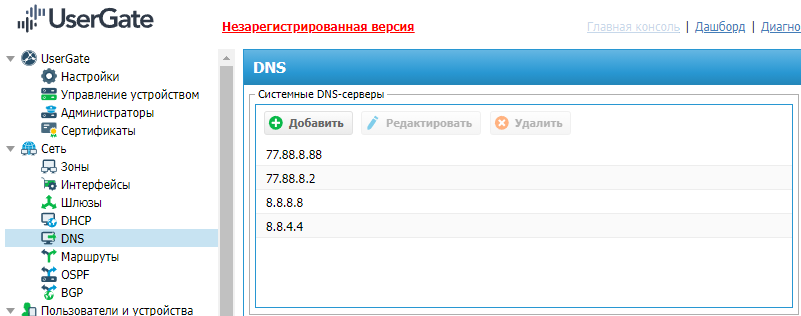


Рисунок 8 - Настройка DNS

Проверим корректность нашей настройки. Для этого в административном интерфейсе перейдем на вкладку «Диагностика и мониторинг» в узле Сеть выберем Ping и попытаемся обратиться к домену google.com

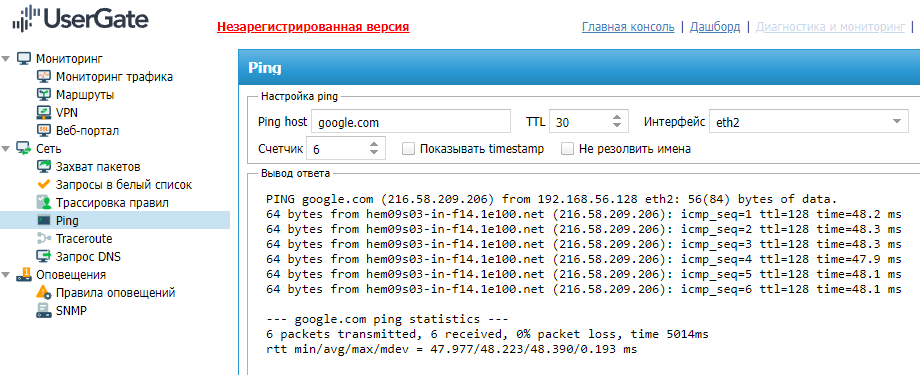


Рисунок 9 - Проверка DNS

## Настройка NTP

Для работы NTP достаточно обеспечить интерфейсу eth2 доступ к Интернету. Корректно работающий NTP будет иметь следующий вид:

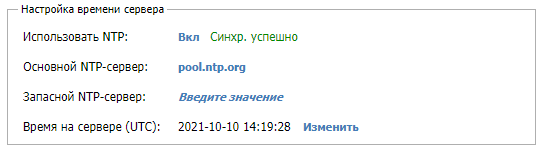


Рисунок 10 - Активный NTP

## Настройка зон

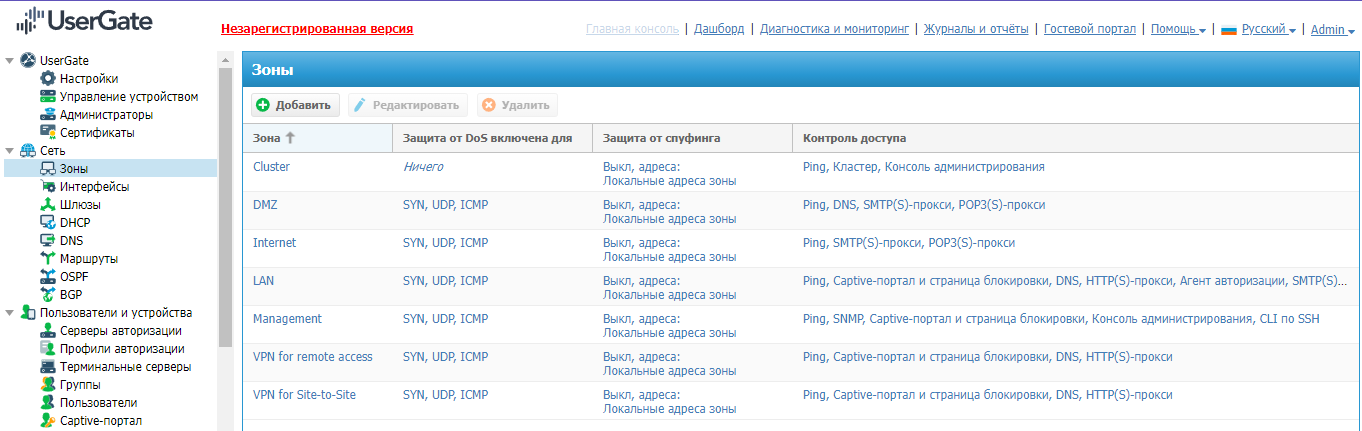


Рисунок 11 - Настроенные зоны

## Создание пользователей

Создадим пользователей при помощи подразделов «Группы» и «Пользователи» раздела «Пользователи и устройства» и добавим их к соответствующим группам.

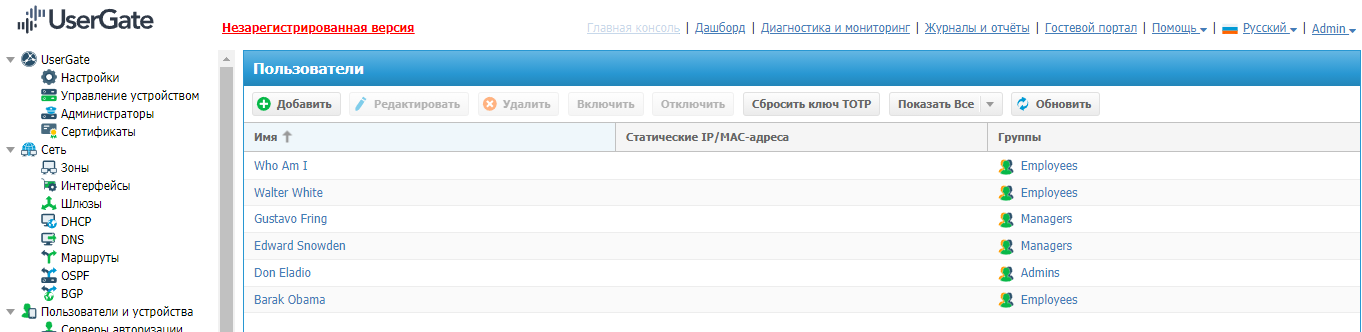


Рисунок 12 - Пользователи

## Создание групп

Создадим группы пользователей при помощи подразделов «Группы» и «Пользователи» раздела «Пользователи и устройства»

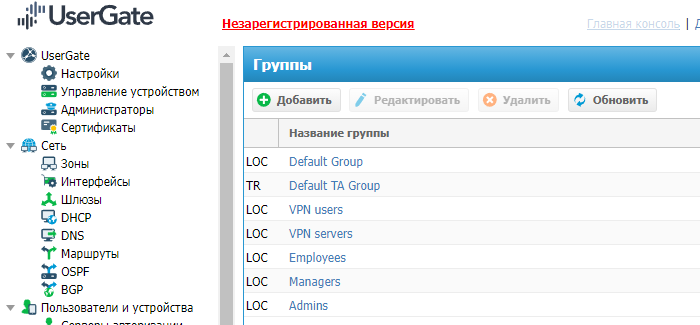


Рисунок 13 - Группы

## Настройка NAT

Сформируем правило NAT в разделе «Политика и сети», «NAT и маршрутизация»

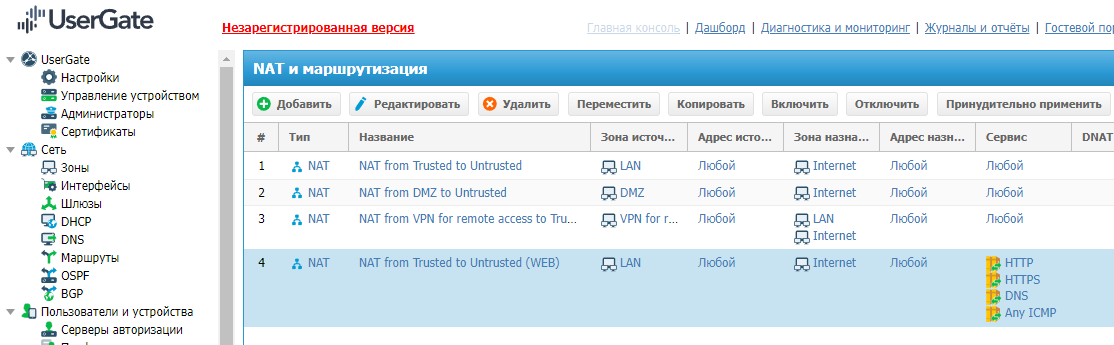


Рисунок 14 - Настройка NAT

## Настройка правил межсетевого экрана

Межсетевой экран настраивается c помощью правил, которые задаются во вкладке «Политики сети - Межсетевой экран». Для группы Преподаватели разрешим только http и https активность из доверенной зоны в не доверенную.

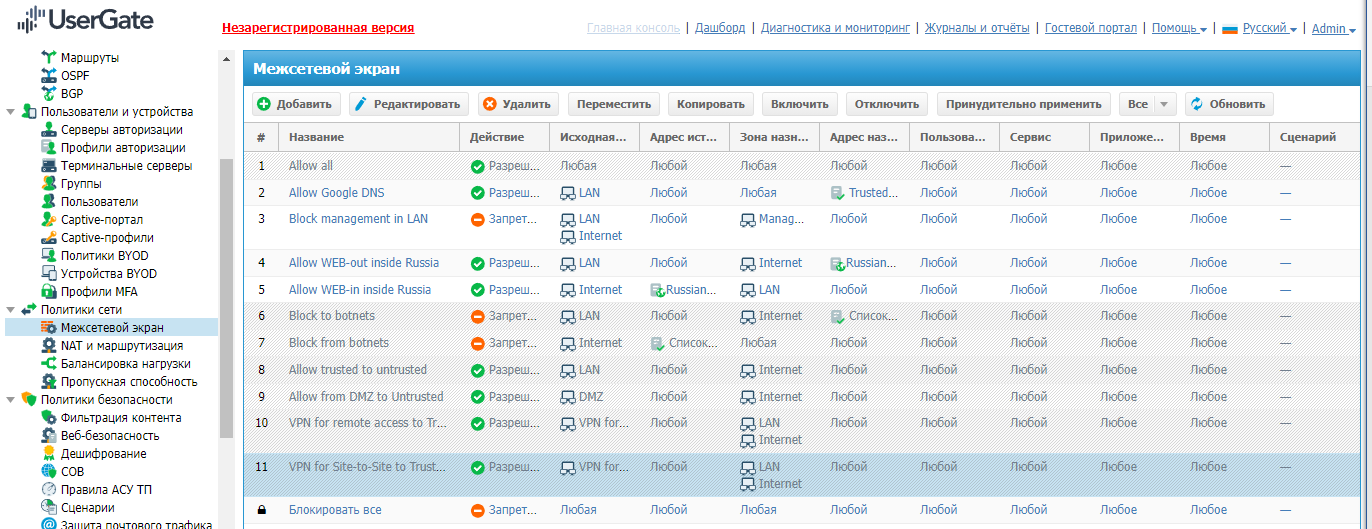


Рисунок 15 - Правила межсетевого экрана

## Настройка правил фильтрации

Для пользователей, имеющих доступ к интернету, создадим фильтрацию контента.

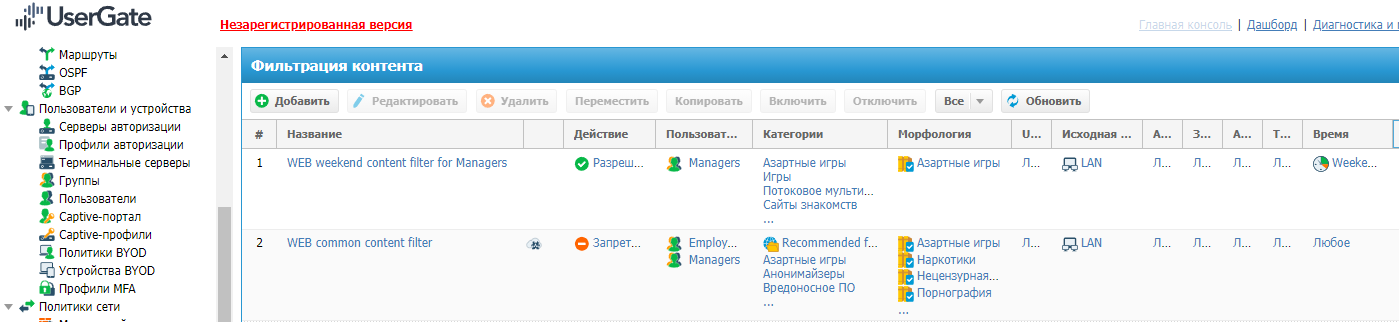


Рисунок 16 - Правила фильтрации контента

## 12. Тестирование

Перед тестированием необходимо настроить пользовательскую машину для работы. Тестовая машина будет находится в зоне LAN. Внесем изменения в файл /etc/network/interfaces

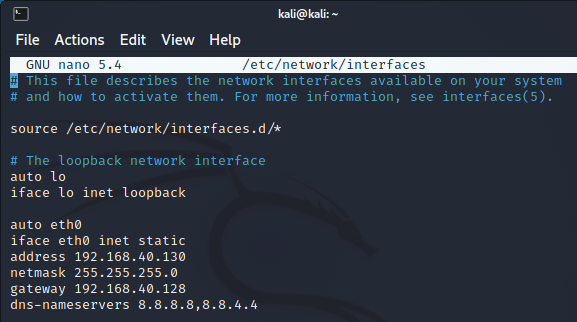


Рисунок 17 - Настройка интерфейса

Настроим адрес DNS сервера:

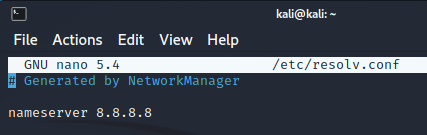


Рисунок 18 - Настройка DNS

Проверим работу интернета:

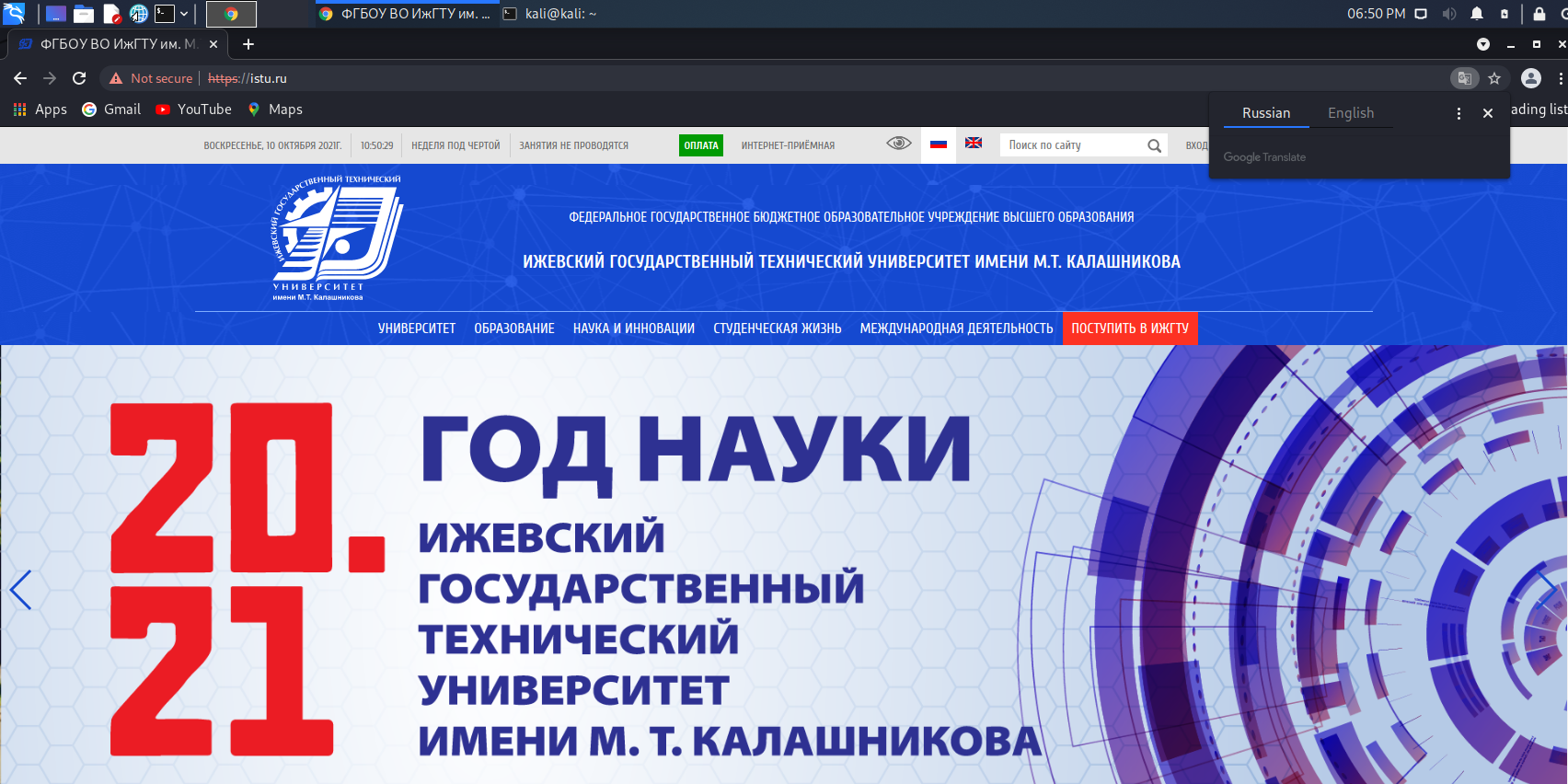


Рисунок 19 - Проверка интернета

Попытаемся зайти на зарубежный сайт:

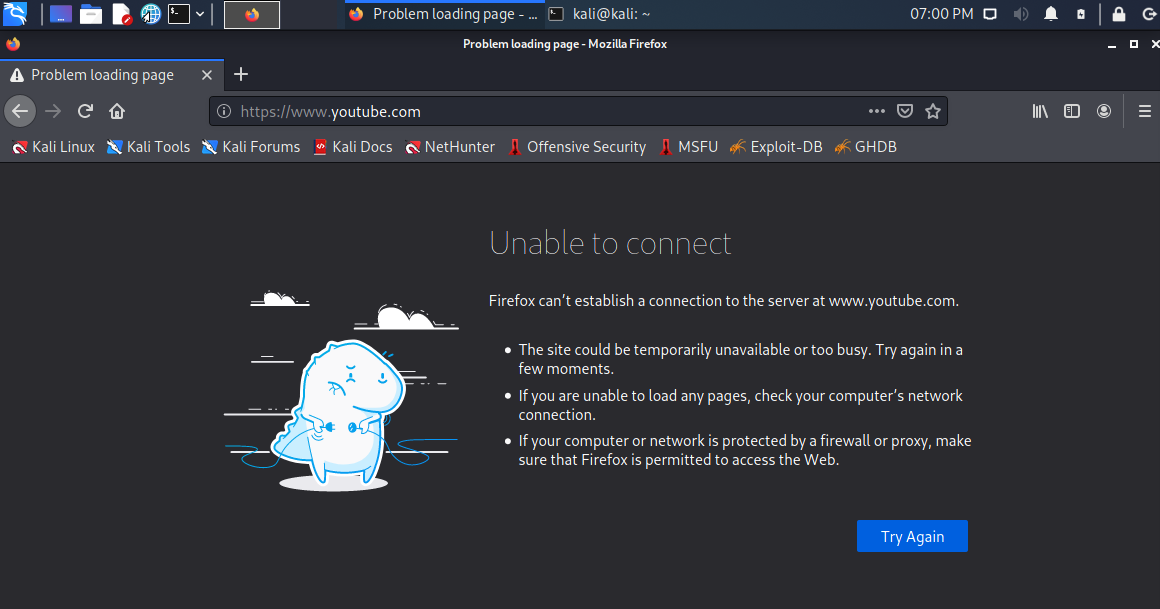


Рисунок 20 - Проверка доступа на зарубежные сайты

Попытаемся зайти на сайт с азартными играми:

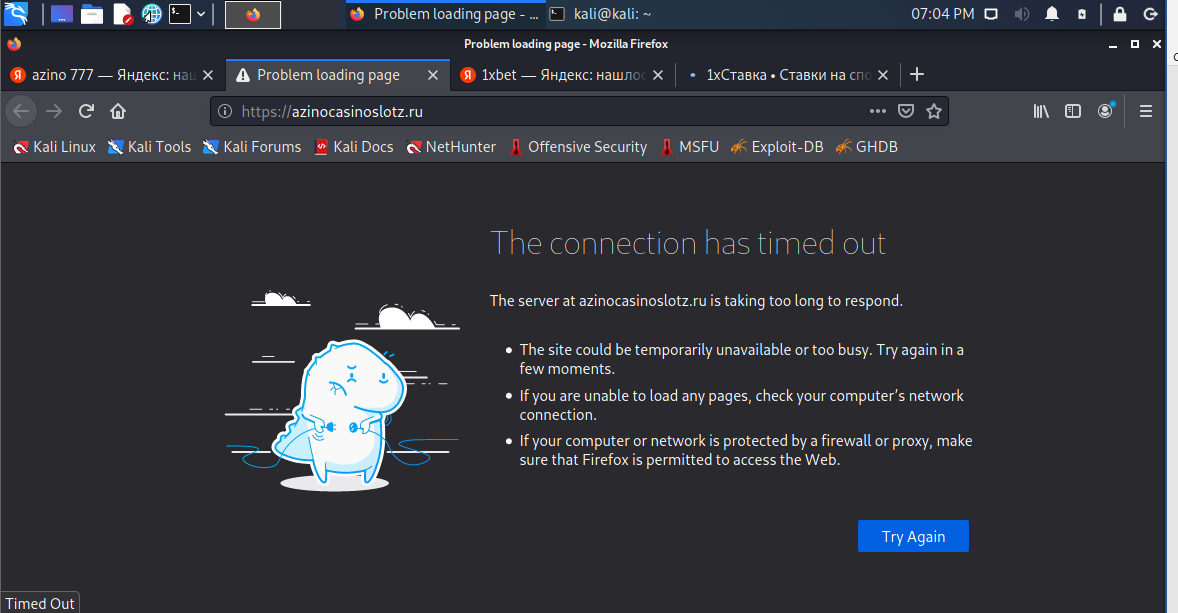


Рисунок 21 - Попытка зайти на запрещенный ресурс

# **Вывод**

В ходе выполнения лабораторной работы был создан безопасный периметр между небезопасной сетью и локальной вычислительной сетью. Был получен опыт работы с UTM-решением Usergate: настройка правил маршрутизации, правил межсетевого экрана, правил фильтрации контента, создания групп и пользователей.