Министерство науки и высшего образования Российской Федерации

Федеральное государственное бюджетное образовательное учреждение

высшего образования

**«КУБАНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»**

**(ФГБОУ ВО «КубГУ»)**

**Факультет компьютерных технологий и прикладной математики**

**Кафедра вычислительных технологий**

**ЛАБОРАТОРНАЯ РАБОТА №9**

**Дисциплина: Информационная безопасность**

Работу выполнил: Романов В.В.

Направление подготовки: 02.03.02 Фундаментальная информатика и информационные технологии

Преподаватель: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Шиян В.И.

**Цель:** Получение теоретических и практических навыков работы с песочницами и файловыми антивирусами. Изучить работу почтового сервера, получить практические навыки работы по защите от спама.

**Ход работы:**

Настроим 2 ВМ в облаке. Для этого выполним следующие действия:

1. Войдём в интерфейс управления облачным провайдером (например, Azure);
2. Создадим 2 ВМ с ОС Ubuntu;
3. Укажем минимальные характеристики для каждой ВМ (2 CPU, 4 GB RAM, 20 GB SSD);
4. Настроим сетевые параметры: разрешим доступ по SSH (TCP порт 22), откроем порты, необходимые для работы Mailcow (HTTP: 80, HTTPS: 443, SMTP: 25, IMAP: 993, POP3: 995);
5. Настроим правила безопасности (Security Groups или Firewall Rules), ограничив доступ только с доверенных IP;
6. Убедимся, что обе машины находятся в одной сети или имеют возможность взаимодействия друг с другом.

**Конфигурация Docker на хостах**:

1. Подключился к каждой ВМ через SSH;
2. Выполнил следующие команды для установки Docker:

* sudo apt-get update
* sudo apt-get install -y apt-transport-https ca-certificates curl software-properties-common
* curl -fsSL https://download.docker.com/linux/ubuntu/gpg | sudo gpg --dearmor -o /usr/share/keyrings/docker-archive-keyring.gpg
* echo "deb [arch=amd64 signed-by=/usr/share/keyrings/docker-archive-keyring.gpg] https://download.docker.com/linux/ubuntu focal stable" | sudo tee /etc/apt/sources.list.d/docker.list > /dev/null
* sudo apt-get update

sudo apt-get install -y docker-ce docker-ce-cli containerd.io

1. Настроил Docker для запуска при старте системы:  
   sudo systemctl enable docker.

После этого развернем Mailcow на 2 машинах. Для этого выполним следующее:

1. Подключимся к 1-ой ВМ через SSH.
2. Выполнил команды:
   * git clone https://github.com/mailcow/mailcow-dockerized.git
   * cd mailcow-dockerized
   * sed -i 's/MYSQL/MARIADB/g' docker-compose.yml
   * bash generate\_config.sh
   * docker compose pull && docker compose up –d

Повторим те же действия на 2-ой машине. На рисунках 1-2 представлены окно входа в mailcow и её характеристики нагрузки.

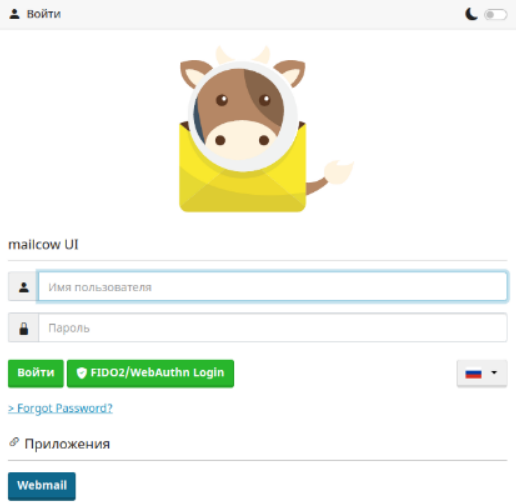


Рисунок 1 – Окно входа в админ-панель mailcow

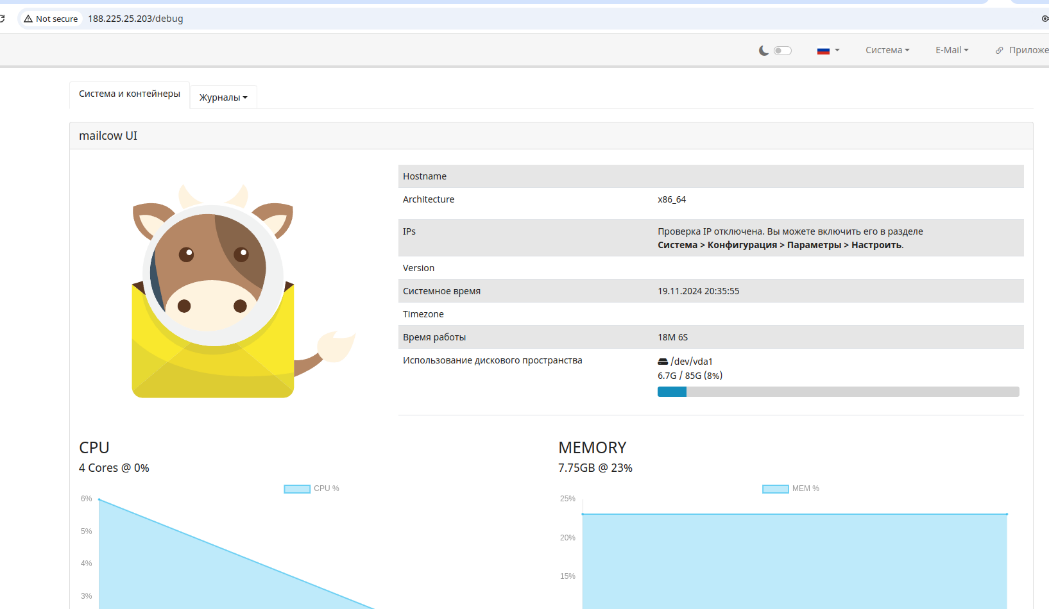


Рисунок 2 – Характеристики нагрузки Mailcow

Теперь настроим домен и почтовый ящик. Для этого зарегистрируем доменное имя и в панели управления DNS добавим следующие записи для домена:

1. A – запись для указания IP-адреса Mailcow-сервера;
2. MX – запись для обработки почтового трафика;
3. SPF – запись для авторизации отправки почты;
4. DKIM – запись для шифрования;
5. DMARC – запись для политики обработки почты.

После вышеперечисленного войдём в административный интерфейс Mailcow и настроим почтовые ящики. На рисунке 3 представлен результат.

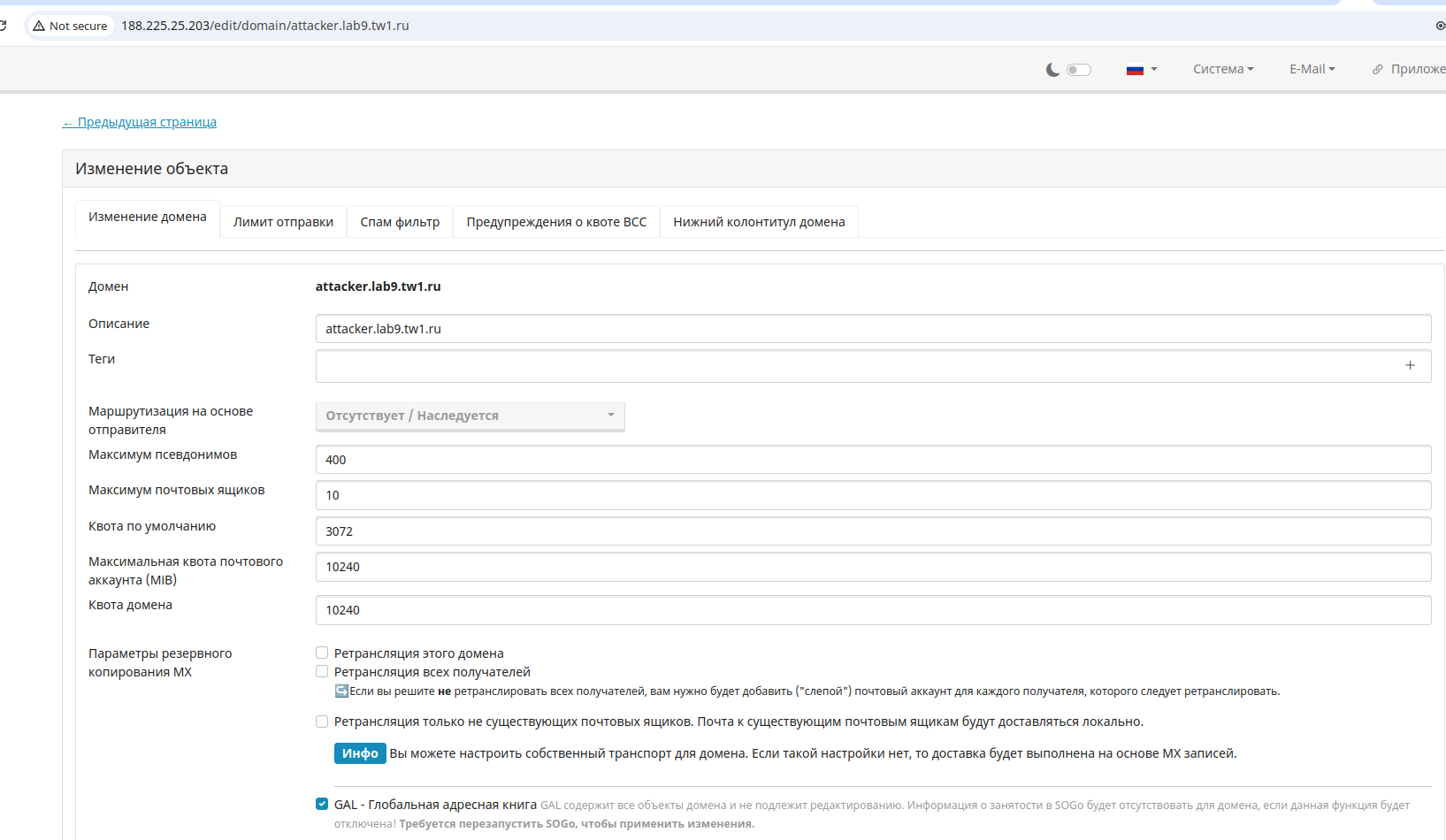


Рисунок 3 – Настройка сервера MailCow

Развернем Anti-Spam Proxy Server (ASSP) на 2-ой ВМ. Для этого выполним следующие действия:

1. Подключился ко 2-ой ВМ через SSH;
2. Выполнил команды для установки ASSP:

git clone https://github.com/fametec/assp.git

cd assp

docker compose pull && docker compose up -d

Проверил доступность интерфейса ASSP по адресу http://<ip\_address>:55555.

Логин: root

Пароль: nospam4me

На рисунке 4 представлен результат.

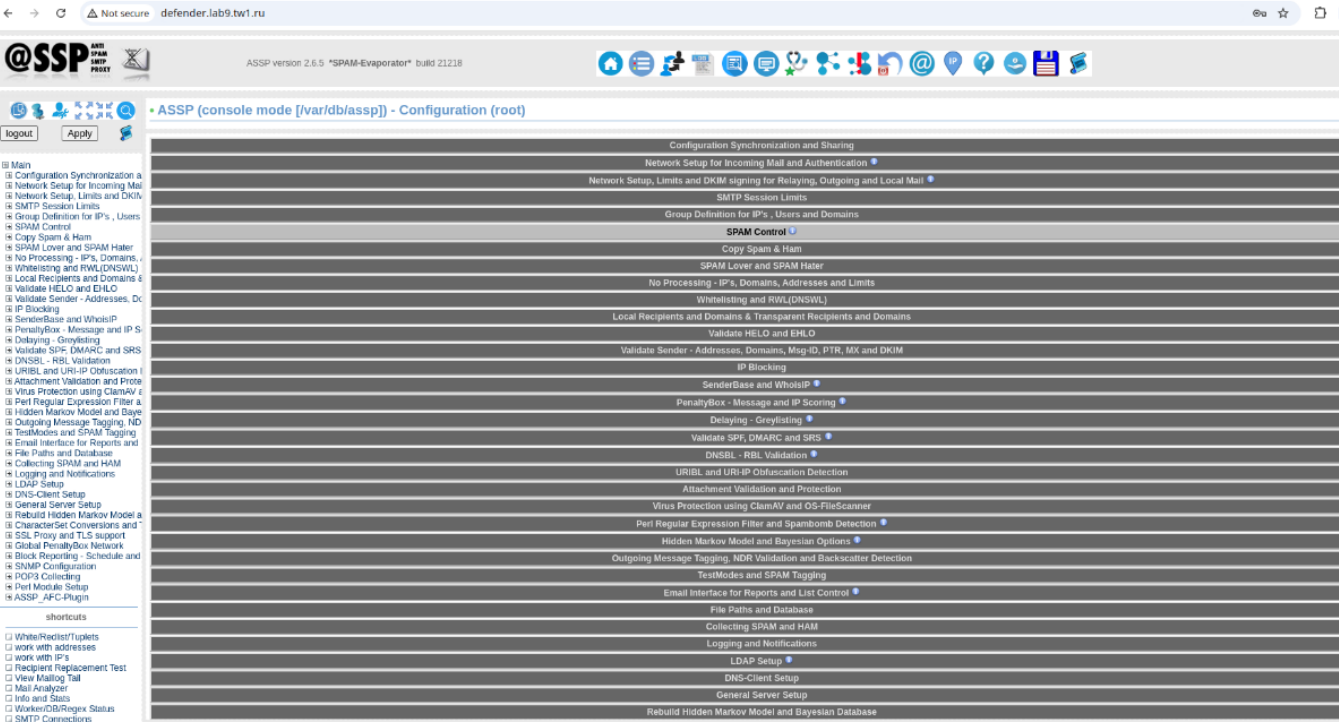


Рисунок 4 – Настройка прокси-антиспама

После чего настроим проксирование через ASSP на Mailcow. Для этого выполним следующие действия:

1. Войдём в веб-интерфейс ASSP (http://<ip\_address>:55555).
2. Настроим параметры проксирования, чтобы перенаправлять входящий почтовый трафик на сервер Mailcow.
3. Проверим соединение, отправив тестовые сообщения через ASSP на Mailcow.

На рисунке 5 представлен результат.

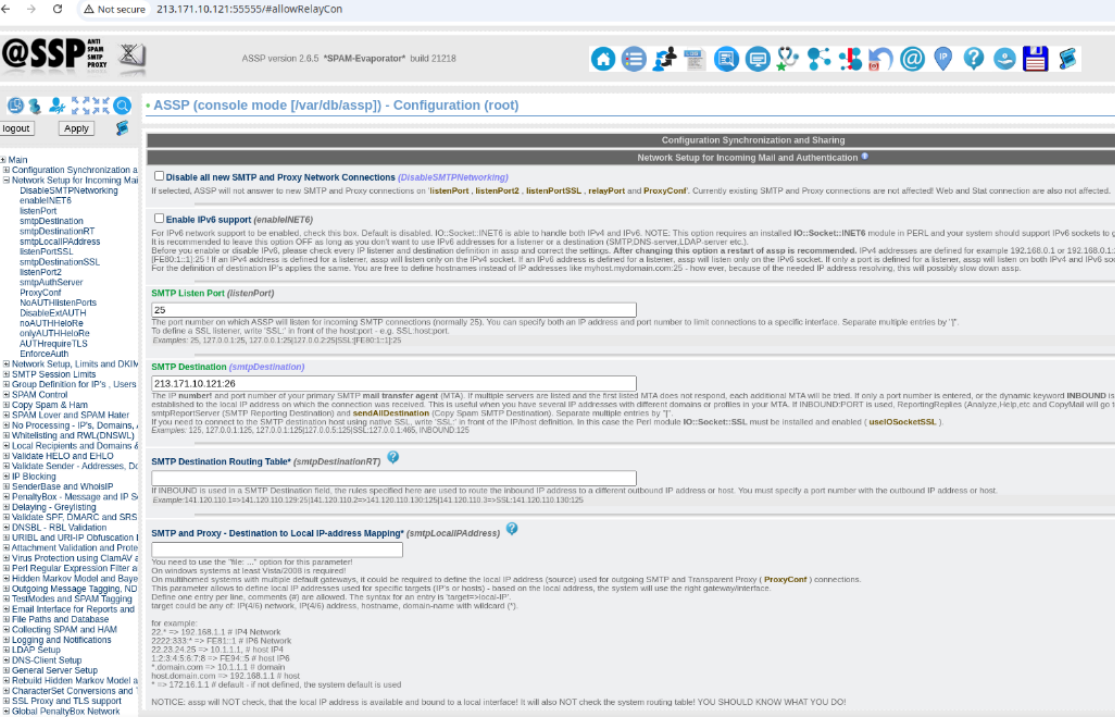


Рисунок 5 – Настройка антиспам-прокси сервера

**Вывод**: изучил и применил на практике технологии настройки почтового сервера и антиспамовых фильтров. А также реализовал процесс развертывания Mailcow и Anti-Spam SMTP Proxy Server на ВМ и настроил взаимодействие между ними. Кроме того, получил навыки работы с доменными записями и сетевыми настройками.