---

### \*\*🚀 0. Подготовка (30 минут)\*\*

\*\*🎯 Цель\*\*: Создать ВМ и настроить сеть согласно ТЗ.

1. \*\*📥 Скачайте ПО\*\*:

- \*\*Infotecs IDS\*\*: [Установщик](https://www.infotecs.ru/) → `infotecs-ids-5.0.iso`.

- \*\*Базальт СПО\*\*: [ISO](https://basealt.ru/) → `alt-server-10.iso`.

- \*\*Гипервизор\*\*: [VMware Workstation Pro](https://www.vmware.com/).

2. \*\*🖥️ Создайте ВМ\*\*:

- \*\*Названия\*\*: `FW1`, `FW2`, `CHR-1`, `С1`, `С2`, `ALD1`, `R1`, `R2`, `AT1`, `AT2`, `A1-A4`.

- \*\*Сеть\*\*:

- \*\*NAT-сеть 1\*\*: `192.168.1.0/24` (для FW1, CHR-1).

- \*\*NAT-сеть 2\*\*: `192.168.2.0/24` (для FW2, С1).

- \*\*Internal Network\*\*: `10.0.0.0/24` (для ALD1, A1-A4).

3. \*\*🔧 Настройте интерфейсы\*\*:

- \*\*Для FW1\*\*:

```bash

# В терминале FW1:

ip link set eth0 up

ip addr add 192.168.1.1/24 dev eth0

ip link set eth1 up

ip addr add 10.0.0.1/24 dev eth1

```

- \*\*Проверка\*\*:

```bash

ping 192.168.1.2 # CHR-1 должен ответить.

```

---

### \*\*🔥 1. Настройка FW1 (1 час)\*\*

\*\*🎯 Цель\*\*: Активация, DHCP, политики брандмауэра, снэпшот.

#### \*\*Шаг 1.1: Веб-интерфейс (15 мин)\*\*

1. \*\*Установите веб-сервер\*\*:

```bash

apt install apache2 -y

systemctl start apache2

```

2. \*\*Откройте порт 443\*\*:

```bash

ufw allow 443/tcp

systemctl restart ufw

```

3. \*\*Проверка\*\*:

```bash

curl -I https://localhost:443 # Должен быть ответ "200 OK".

```

\*Ошибка\*: Если порт закрыт → `ufw disable && ufw enable`.

---

#### \*\*Шаг 1.2: DHCP-сервер (20 мин)\*\*

1. \*\*Установите `isc-dhcp-server`\*\*:

```bash

apt install isc-dhcp-server -y

```

2. \*\*Настройте `/etc/dhcp/dhcpd.conf`\*\*:

```conf

subnet 192.168.1.0 netmask 255.255.255.0 {

range 192.168.1.100 192.168.1.200;

option routers 192.168.1.1;

option domain-name-servers 8.8.8.8;

}

```

3. \*\*Запустите службу\*\*:

```bash

systemctl restart isc-dhcp-server

```

4. \*\*Проверка\*\*:

- Подключите ВМ к сети FW1 → `ip addr show eth0` → должен получить IP из пула.

\*Ошибка\*: Нет аренды → проверьте `journalctl -u isc-dhcp-server`.

---

#### \*\*Шаг 1.3: Политики брандмауэра (15 мин)\*\*

1. \*\*Разрешите ICMP\*\*:

```bash

ufw allow proto icmp from 192.168.1.0/24

```

2. \*\*Заблокируйте соцсети через iptables\*\*:

```bash

iptables -A OUTPUT -p tcp -d facebook.com -j DROP

iptables -A OUTPUT -p tcp -d twitter.com -j DROP

```

3. \*\*Сохраните правила\*\*:

```bash

iptables-save > /etc/iptables/rules.v4

```

4. \*\*Проверка\*\*:

```bash

ping 192.168.1.1 # Должен работать.

curl https://facebook.com # Должен быть заблокирован.

```

---

#### \*\*Шаг 1.4: Снэпшот (5 мин)\*\*

1. \*\*В VMware\*\*:

- `ПКМ на ВМ → Снэпшот → Создать`.

- Название: `FW1\_Base\_Config`.

---

### \*\*🔥 2. Настройка CHR-1 (1 час)\*\*

\*\*🎯 Цель\*\*: NAT, безопасность SSH, пользователи, бэкап.

#### \*\*Шаг 2.1: NAT (20 мин)\*\*

1. \*\*Включите IP-форвардинг\*\*:

```bash

sysctl -w net.ipv4.ip\_forward=1

```

2. \*\*Добавьте правило iptables\*\*:

```bash

iptables -t nat -A POSTROUTING -o eth0 -j MASQUERADE

```

3. \*\*Проверка\*\*:

- На клиентской ВМ: `ping 8.8.8.8` → должен быть ответ.

---

#### \*\*Шаг 2.2: SSH (15 мин)\*\*

1. \*\*Измените порт SSH\*\*:

```bash

nano /etc/ssh/sshd\_config # Port 2222

systemctl restart sshd

```

2. \*\*Проверка\*\*:

```bash

ssh user@localhost -p 2222 # Должен подключиться.

```

\*Ошибка\*: Если нет → `ufw allow 2222/tcp`.

---

#### \*\*Шаг 2.3: Пользователь и группа (15 мин)\*\*

1. \*\*Создайте пользователя\*\*:

```bash

useradd -m -s /bin/bash user2

passwd user2 # Пароль: P@ssw0rd\_2023!

```

2. \*\*Создайте группу `admin`\*\*:

```bash

groupadd admin

usermod -aG admin user2

```

3. \*\*Проверка\*\*:

```bash

groups user2 # Должна быть группа admin.

```

---

#### \*\*Шаг 2.4: Бэкап (10 мин)\*\*

1. \*\*Создайте архив\*\*:

```bash

tar -czvf /backup\_chr1.tar.gz /etc/ssh /etc/network

```

2. \*\*Установите пароль\*\*:

```bash

openssl rand -base64 12 # Используйте вывод как пароль: e.g., "xT9!kL3@qZ#r".

```

---

### \*\*🛠️ 3. Настройка ALD1 (1 час)\*\*

\*\*🎯 Цель\*\*: Установка ALD, домен, пользователи, подключение A1-A2.

#### \*\*Шаг 3.1: Установка ALD (20 мин)\*\*

1. \*\*Установите пакеты\*\*:

```bash

apt install ald-server ald-client -y

```

2. \*\*Создайте домен\*\*:

```bash

ald-domain-create corp.local

```

3. \*\*Добавьте пользователей\*\*:

```bash

ald-user-add admin -p P@ssw0rd! -d corp.local

ald-user-add user1 -p P@ssw0rd! -d corp.local

```

---

#### \*\*Шаг 3.2: Подключение A1/A2 (20 мин)\*\*

1. \*\*На A1\*\*:

```bash

ald-join corp.local -u admin -p P@ssw0rd!

```

2. \*\*Проверка\*\*:

```bash

ald-list-users # Должны отображаться admin и user1.

```

---

### \*\*🔐 4. IDS Group (1 час)\*\*

\*\*🎯 Цель\*\*: Соединение сенсоров, базы сигнатур, TIAS.

#### \*\*Шаг 4.1: Соединение IDS HS ↔ MC (20 мин)\*\*

1. \*\*В веб-интерфейсе IDS MC\*\*:

- Перейдите: `https://192.168.1.1:8443`.

- Логин: `admin`, Пароль: `P@ssw0rd!`.

- Добавьте IDS HS: `IP: 192.168.1.2`, Порт: `514`.

2. \*\*Проверка\*\*:

- В разделе \*\*Сенсоры\*\* → статус "Online".

---

#### \*\*Шаг 4.2: Базы сигнатур (15 мин)\*\*

1. \*\*Обновите базы\*\*:

```bash

ids-ns --update-signatures

```

2. \*\*Проверка\*\*:

```bash

tail -n 50 /var/log/ids-ns.log # Должны быть записи "Signatures updated".

```

---

### \*\*📊 5. Отчет (30 мин)\*\*

\*\*🎯 Цель\*\*: Документирование всех шагов, скриншоты, таблица критериев.

1. \*\*Структура отчета\*\*:

- \*\*Титульный лист\*\*: Название проекта, дата, ФИО.

- \*\*Скриншоты\*\*:

- Снэпшоты ВМ.

- Настройки DHCP (пул адресов).

- Политики брандмауэра.

- \*\*Таблица критериев\*\*:

| Критерий | Статус | Комментарий |

|-----------------------------------|--------|----------------------|

| FW1: DHCP настроен | ✅ Да | Пул: 100-200 |

| CHR-1: Создан пользователь user2 | ✅ Да | Группа: admin |

2. \*\*Цифровая гигиена\*\*:

- Все пароли: `openssl rand -base64 12` (например, `xT9!kL3@qZ#r`).

- Логи хранятся в `/var/log/`, доступ только для root.

---

### \*\*❗ Типичные ошибки и решения\*\*

- \*\*Проблема\*\*: DHCP не раздает адреса.

\*\*Решение\*\*:

```bash

systemctl status isc-dhcp-server # Проверьте статус службы.

journalctl -u isc-dhcp-server -n 50 # Ищите ошибки в логах.

```

- \*\*Проблема\*\*: Веб-интерфейс недоступен.

\*\*Решение\*\*:

```bash

ufw status # Проверьте открытые порты.

netstat -tuln | grep 443 # Убедитесь, что порт слушается.

```

---