



**КОНКУРСНОЕ ЗАДАНИЕ**

Региональный Чемпионат

ЮниорПрофи 2023

Сетевое и системное администрирование

Возрастная группа 14+

Конкурсное задание включает в себя следующие разделы:

1. Формы участия в конкурсе
2. Задание для конкурса
3. Описание Задания
4. Критерии оценки

Количество часов на выполнение задания: 12 ч.

* 1. **ФОРМЫ УЧАСТИЯ В КОНКУРСЕ**

Командный конкурс, команда 2 человека.

* 1. **ЗАДАНИЕ ДЛЯ КОНКУРСА**

Содержанием конкурсного задания является Создание и настройка сетевой инфраструктуры дома или небольшого офиса. Участники соревнований получают инструкцию и топологию сети. Конкурсное задание сквозное и выполняется в течение 3х дней.

Конкурс включает в себя выполнение пуско-наладочных работ сетевого и пользовательского оборудования, а также выполнение работ по поиску и устранению неисправностей.

Окончательные аспекты критериев оценки уточняются оцениваю-щими экспертами. Оценка производится ежедневно по окончании работ. Если участник конкурса не выполняет требования техники безопасности, подвергает опасности себя или других конкурсантов, такой участник может быть отстранен от конкурса.

Время и детали конкурсного задания в зависимости от конкурсных условий могут быть изменены оценивающими экспертами.

#### ОПИСАНИЕ КОНКУРСНОГО ЗАДАНИЯ

#### СХЕМА ОЦЕНКИ

Оцениваемые аспекты имеют разный вес в зависимости от их сложности. Схема оценки построена так, чтобы каждый аспект оценивался только один раз. Например, в задании предписывается настроить корректные имена для всех устройств, данный аспект будет оценен только один раз и повторная оценка данного аспекта проводится не будет.  
Следует также учесть, что для данного задания возможна **автоматическая** оценка результатов.

#### НЕОБХОДИМОЕ ОБОРУДОВАНИЕ, ПРИБОРЫ, ПО И МАТЕРИАЛЫ

Конкурсное задание выполнимо в полном объеме с привлечением оборудования и материалов, указанных в *Инфраструктурном листе*. Для выполнения задания возможно использование виртуальной инфраструктуры.

Используемое ПО:  
BR-GW используют OPNsense 22.7;  
ISP, HQ-GW, HQ-SRV-1, HQ-SRV-2, HQ-CLI-1 используют Debian 11.05;  
BR-SRV, HQ-CLI-2, BR-CLI-2 использует Fedora 37;  
BR-CLI-1 использует Ред ОС 7.3.1 с графическим окружением Mate;  
HQ-RTR-D, HQ-RTR-L использует Ред ОС 7.3.1  
HQ-CLI-3 использует Windows 10 Education/Enterprise;  
HQ-DC, HQ-ROOTCA использует Windows Server 2022;  
REM-CLI использует ArchLinux 2023.01.01.

#### ИНСТРУКЦИИ ДЛЯ УЧАСТНИКОВ

В первую очередь рекомендуется прочитать задание полностью. Следует обратить внимание, что задание составлено не в строгом хронологическом порядке. Для выполнения некоторых пунктов задания может потребоваться выполнение действий из других пунктов, которые изложены в задании ниже. Таким образом, **порядок выполнения задания и распределение временных затрат определяется участниками самостоятельно.**

Участникам разрешено пользоваться Интернетом. Находить и использовать информацию можно исключительно из **открытых источников**. Скачивать, использовать заготовленный перед конкурсом материал, файлы, скрипты, сайты для конкурса **запрещено**.

Рекомендуется тщательно проверять результаты своей работы. Также учтите, что в конце дня Вам необходимо по указанию экспертов **выключить все виртуальные машины**, а затем включить их в желаемом порядке.

Устройства участников могут иметь **предустановленное программное обеспечение**, которое будет применяться при проверке и оценке, его не рекомендуется удалять. Если данное ПО будет преустановленно, то участникам и экспертам будет сообщено о нём перед началом конкурса.

Если реализация предполагает использование виртуальных машин, то рекомендуется включать только те машины, которые необходимы для выполнения задания. **Тщательно распределяйте имеющиеся ресурсы.**

Доступ к ОС Opnsense осуществляется через '**root**' с паролем '**opnsense**'.  
Доступ к рабочему столу Ред ОС осуществляется через '**user**' с паролем '**P@ssw0rd**'  
Доступ к ОС Windows 10 и Windows Server 2022 должен быть организован участниками через пользователя '**User**' с паролем '**P@ssw0rd**'.  
Доступ ко всем остальным ОС осуществляется через '**root**' с паролем '**toor**'.

### 

### **ЗАДАНИЕ**

#### НАСТРОЙКИ ПРОВАЙДЕРА

Для связи с Интернетом получите настройки сетевого контроллера через DHCP.

#### НАСТРОЙКИ IP-АДРЕСАЦИИ

##### Таблица 1. Настройка IP-адресации

| Устройство | Сеть | Адрес IPv4/Маска |
| --- | --- | --- |
| ISP | WAN | DHCP |
|  | ISP-REM-Net | 192.168.111.1/24 |
|  | ISP-BR-Net | 10.200.20.1/28 |
|  | ISP-HQ-Net | 10.14.18.1/28 |
| HQ-GW | ISP-HQ-Net | 10.14.18.5/28 |
|  | HQ-ServerNet | 192.168.1.1/24 |
|  | HQ-L-Net | 172.16.20.1/30 |
|  | HQ-R-Net | 172.16.10.1/30 |
| BR-GW | ISP-BR-Net | 10.200.20.1/28 |
|  | BR-ClientNet | 192.168.50.254/24 |
|  | BR-ServerNet | 172.16.10.6/29 |
| HQ-RTR-L | HQ-L-Net | 172.16.20.2/30 |
|  | HQ-WinNet | 192.168.20.1/24 |
| HQ-RTR-D | HQ-D-Net | 172.16.10.1/30 |
|  | HQ-ClientNet | 192.168.10.1/24 |
| HQ-SRV-1 | HQ-ServerNet | 192.168.1.10/24 |
| HQ-SRV-2 | HQ-ServerNet | 192.168.1.20/24 |
| HQ-DC | HQ-WinNet | 192.168.20.10/24 |
| HQ-ROOTCA | HQ-WinNet | 192.168.20.111/24 |
| HQ-CLI-1 | HQ-ClientNet | DHCP [192.168.10.10/24] |
| HQ-CLI-2 | HQ-ClientNet | DHCP |
| HQ-CLI-3 | HQ-WinNet | DHCP [192.168.20.123/24] |
| BR-SRV | BR-ServerNet | 172.16.10.1/29 |
| BR-CLI-1 | BR-ClientNet | DHCP [192.168.50.1/24] |
| BR-CLI-2 | BR-ClientNet | DHCP |
| REM-CLI | ISP-REM-Net | DHCP |

#### День 1. Настройка сетевого взаимодействия и базовых сервисов

##### **Базовая настройка всех устройств**

1. Настройте имена всех устройств и виртуальных машин в соответствии с **Топологией сети.**
2. Настройте IPv4-адресацию на всех сетевых интерфейсах в соответствии с **Настройками IP-адресации**.
3. На всех устройствах должно быть установлено актуальное время и часовой поясу (GMT+3) | (UTC+3). *Рекомендуется использовать часовой пояс Москвы.*
4. Обеспечьте выход в Интернет всех устройств в **Топологии сети.**
   1. Используйте трансляцию сетевых адресов на ISP,HQ-GW, BR-GW.

##### **Настройка сети провайдера**

1. Настройте DHCP-сервер на ISP для сети ISP-REM-Net.
   1. Используйте пул адресов **192.168.111.10 - 192.168.111.20**.
   2. В качестве адреса DNS-сервера используется адреса по порядку: ISP, открытый DNS-сервер в Интернете.  
      *Рекомендуется использовать DNS-сервер Google (8.8.8.8 или 8.8.4.4)*
2. Настройте NTP-сервер на ISP.
   1. Используйте NTP сервер на базе Chrony.
   2. NTP-сервера должен иметь стратум 4.
   3. HQ-GW, BR-GW должны синхронизировать время с ISP по NTP.
3. На ISP должен быть настроен DNS-сервер с использование bind9.
   1. DNS-сервер должен обслуживать зону '**isp.local**'.
   2. Сервер должен быть настроен как нерекурсивный DNS-сервер.
   3. Запросы, которые выходят за рамки зоны '**isp.local**', должны пересылаться любому общедоступному DNS-серверу в Интернете.  
      *Рекомендуется использовать DNS-сервер Google (8.8.8.8 или 8.8.4.4)*
   4. Файлы зон должны располагаться в каталоге /var/dns/.
   5. Настройте разрешение имен в соответствии с таблицей:

| Тип записи | Ключ | Значение |
| --- | --- | --- |
| A | isp | 10.200.20.1 |
| A | isp | 10.14.18.1 |
| A | hq-gw | 10.14.18.5 |
| A | br-gw | 10.200.20.7 |
| CNAME | internet | isp |

1. На REM-CLI настройте VPN клиент WireGuard.
   1. Используйте имя туннеля VPN.
   2. Используйте IP адрес туннеля 10.10.10.5/24.
   3. Используйте Persistent keepalive равный 25.
   4. Обеспечьте автоматическое подключение туннеля после перезагрузки устройства.

##### **Настройка сети штаб-квартиры**

1. Настройте DHCP-сервер на HQ-RTR-D для сети HQ-ClientNet.
   1. Используйте пул адресов **192.168.10.5 - 192.168.10.20**.
   2. Адрес **192.168.10.15** должен быть исключён из автоматической выдачи адресов.
   3. IP-адрес **192.168.10.10** должен быть зарезервирован для HQ-CLI-1.
   4. В качестве адреса DNS-сервера используется адрес HQ-DC, ISP.
   5. В качестве доменного имени используется '**hq.local**'.
2. Настройте DHCP-сервер на HQ-DC для сети HQ-WinNet.
   1. Используйте пул адресов **192.168.20.100 - 192.168.20.150**.
   2. Адрес **192.168.10.115** должен быть исключён из автоматической выдачи адресов.
   3. IP-адрес **192.168.10.123** должен быть зарезервирован для HQ-CLI-1.
   4. В качестве адреса DNS-сервера используется адрес HQ-DC, ISP.
   5. В качестве доменного имени используется '**hq.local**'.
3. На устройствах HQ-GW, BR-GW должен быть настроен межсетевой экран.
   1. Разрешение портов должно быть выполнено по принципу **"необходимо и достаточно"**.  
      *Должно быть разрешено только то, что указано в задании - остальное заблокировано.*
   2. Запретите попадание не транслируемого сетевого трафика с внешних сетей во внутренние сети HeadQuarters и Branch.
   3. Разрешите подключение внешних клиентов только к тем портам, которые необходимы для выполнения других пунктов задания.
   4. Устройства внутри локальных сетей HeadQuarters, Branch и ISP **не должны** иметь ограничений по выходу во внешние сети.
   5. Любые подключение внутри туннелей должны быть разрешены.
4. Обеспечьте динамическую маршрутизацию с помощью OSPFv2 на HQ-GW, HQ-RTR-L, HQ-RTR-D.
   1. Для OSPFv2 используйте программный пакет frr на GW.
   2. Используйте область 0.
   3. Настройте на GW раздачу маршрута по умолчанию для области OSPFv2.
   4. Все использующиеся интерфейсы, кроме тех, что используются для распространение  
      маршрутов OSPFv2 между устройствами, должны находиться в пассивном режиме.
5. На HQ-DC должен быть организован Active Directory.
   1. HQ-DC должен быть контроллером домена '**hq.local**'.
   2. Создайте подразделение Clients в домене.
   3. Добавьте в подразделение компьютер HQ-CLI-3.
   4. Создайте две пользовательские учетные записи User1 и User2.
   5. Настройте разрешение имен DNS службы в соответствии с таблицей:

| Тип записи | Ключ | Значение |
| --- | --- | --- |
| A | isp | 10.14.18.1 |
| A | hq-srv-1 | 192.168.1.10 |
| A | hq-srv-2 | 192.168.1.20 |
| A | www | 192.168.20.10 |

1. Введите устройство HQ-CLI-3 и HQ-ROOTCA в домен '**hq.local**'.
2. На HQ-CLI-3 должна быть только одна встроенная локальная учетная запись пользователя Administrator с паролем P@ssw0rd.
3. На HQ-ROOTCA должен быть организован корневой доменный центр сертификации.
   1. Используйте имя WSR CA.
   2. Срок действия корневого сертификата 10 лет.
   3. Сохраните корневой сертификат на рабочем столе HQ-ROOTCA.
   4. Все клиентские операционные системы должны доверять этому центру сертификации.
   5. Все устройства в сети штаб-квартиры должны иметь в качестве адреса DNS-сервера следующий порядок адресов: HQ-DC, ISP.
4. На HQ-DC должен быть организован веб-сервер IIS.
5. На HQ-GW настройте VPN сервер WireGuard.
   1. Используйте имя WG.
   2. Используйте порт 51820.
   3. Используйте для сети WireGuard сетевой диапазон 10.10.10.0/24.
   4. Используйте IP адрес туннеля 10.10.10.1/24.
   5. Настройте конечные точки (клиенты) для возможности подключения с BR-GW и REM-CLI.
   6. Обеспечьте клиентам доступ к локальным сетям HQ-ServerNet, HQ-WinNet, HQ-ClientNet.
6. Настройте **openssh-server** на HQ-GW, HQ-RTR-L, HQ-RTR-D, HQ-SRV-1,   
   HQ-SRV-2.
   1. Создайте пользователя '**ssh-user**' с паролем '**P@ssw0rd**' для подключения по ssh.
   2. Созданный пользователь должен иметь возможность повышать свои права до суперпользователя, используя **sudo**.
   3. По ssh имеет право подключиться только пользователь '**ssh-user**'.

##### **Настройка сети филиала**

1. Настройте DHCP-сервер на BR-GW для сети BR-ClientNet.
   1. Используйте пул адресов **192.168.50.1 - 192.168.50.100**.
   2. Адрес **192.168.10.50** должен быть исключён из автоматической выдачи адресов.
   3. IP-адрес **192.168.10.1** должен быть зарезервирован для BR-CLI-1.
   4. В качестве адреса DNS-сервера используется адрес BR-SRV, ISP.
   5. В качестве доменного имени используется '**br.local**'.
2. Все устройства в сети филиала должны иметь в качестве адреса DNS-сервера следующий порядок адресов: BR-SRV, ISP.
3. На BR-GW настройте VPN клиент WireGuard.
   1. Используйте имя туннеля VPN.
   2. Используйте IP адрес туннеля 10.10.10.2/24.
   3. Используйте Persistentkeepalive равный 25.
   4. Обеспечьте автоматическое подключение туннеля после перезагрузки устройства.
   5. Обеспечьте доступ к локальным сетям BR-ServerNet и BR-ClientNet.

#### День 2. Настройка инфраструктурных служб

##### **Настройка сети штаб-квартиры**

1. В качестве центра сертификации используйте устройство HQ-ROOTCA.
   1. Используйте центр сертификации для создания клиентских сертификатов.
   2. Создайте сертификат для сайта.
      1. Используйте имя [**www.hq.local**](file:///C:\Users\123\Downloads\Telegram%20Desktop\www.hq.local)**.**
      2. Срок действия сертификата 2 года.
      3. Сохраните сертификат на рабочем столе HQ-ROOTCA.
   3. Созданный сертификаты должны быть валидны при использовании браузера  
      Microsoft Edge.
2. В качестве веб-хостинга используйте устройство HQ-SRV-1.
3. Веб-хостинг должен в себя включать реверс-прокси Nginx, веб-сервер Apache с Веб-сервер Apache должен работать на порту 8080.
   1. По умолчанию должна открываться стартовая страница index.php.
   2. Реверс-прокси Nginx должен работать на порту 80 и 443.
   3. Настройки, связанные с Nginx, должны содержаться в отдельном конфигурационном файле /etc/nginx/conf.d/site.conf
   4. Пользователь root сервера баз данных должен иметь пароль P@ssw0rd.
4. Развертывание сайта на локальном веб-хостинге.
   1. Создание локальной копии удаленного репозитория.
   2. Сайт находится в Git репозитории по адресу (Полученный во время задания)
   3. Локальная копия репозитория должна быть создана в каталоге /var/www/html.
   4. Импорт базы данных сайта.
      1. Имя дампа базы данных bd.sql.
      2. Файл дампа базы располагается в локальной копии репозитория.
5. На HQ-SRV-2 настройте RAID массив.
   1. Уровень дискового массива RAID 1.
   2. Используйте имя дискового массива md0.
   3. Используйте два неразмеченных жестких диска.
   4. Используйте файловую систему xfs.
   5. Организуйте автоматическое монтирование дискового массива.
   6. Точка монтирования /opt/docker.
6. В качестве сервера Docker используйте HQ-SRV-2.
   1. Установите Docker-ce и плагин Docker Compose.
   2. Пользователь user должен выполнять команды Docker без sudo.
   3. Используя Docker или плагин Docker Compose разверните сервер баз данных Postgres.
   4. В качестве имени контейнера используйте имя postgres.
      1. Сервер баз данных должен работать на стандартном для Postgres порту.
      2. Файлы баз данных должны располагаться локально в папке /opt/docker/postgres.
      3. Обеспечьте запуск сервера баз данных после перезагрузки компьютера.
      4. Используйте суперпользователя postgres с паролем P@ssw0rd.
      5. Создайте базу данных nextcloud.
   5. Используя Docker или плагин Docker Compose разверните файловое хранилище NextCloud.
   6. В качестве имени контейнера используйте имя nextcloud.
   7. Приложение должно работать на порту 8088.
   8. Обеспечьте связь с сервером баз данных.
   9. Обеспечьте запуск приложения после перезагрузки компьютера.
   10. Файлы приложения должны располагаться локально в папке /opt/docker/nextcloud.
   11. Используйте базу данных nextcloud.

##### **Настройка сети филиала**

1. Настройка системы мониторинга.
   1. В качестве сервера системы мониторинга используйте BR-SRV.
   2. В качестве системы мониторинга используйте Zabbix.
   3. Везде, где необходимо, используйте пароль P@ssw0rd.
   4. Используйте имя сервера zabbix.
   5. Администратором системы мониторинга должен быть пользователь Admin с паролем  
      P@ssw0rd.
   6. Настройте возможность использования русского языка.
   7. Для внешних клиентов на RTR-K настройте проброс соответствующего порта.
   8. Настройка узлов сети системы мониторинга Zabbix.
   9. В качестве узлов сети используйте BR-CLI-1, BR-CLI-2.
   10. Имя узла сети должна соответствовать имени устройства.
   11. Для узлов сети используйте Группу Linux Clients.
   12. Шаблон Linux by Zabbix agent.
   13. Для узла сети BR-CLI-1 используйте шаблон FreeBSD by Zabbix agent.
   14. Для узла сети BR-CLI-1 используйте агента системы мониторинга Zabbix agent.

#### День 3. Поиск и устранение неисправности

В этот день будет предложено выполнить работу по поиску и устранению неисправностей в  
сетевой инфраструктуре (Секретное задание).

#### 

#### ТОПОЛОГИЯ

