КОНКУРСНОЕ ЗАДАНИЕ

Возрастной ценз: **14 лет и более**
Общая продолжительность Конкурсного задания: **12 ч.**
Количество конкурсных дней: **3 дней**

Вне зависимости от количества модулей, КЗ должно включать оценку по каждому из разделов требований компетенции.

Оценка знаний участника должна проводиться через практическое выполнение Конкурсного задания. В дополнение могут учитываться требования работодателей для проверки теоретических знаний/оценки квалификации.

Разработка/выбор конкурсного задания

Конкурсное задание состоит из 3 модулей, включает обязательную к выполнению часть (инвариант) – 2 модулей, и вариативную часть – 1 модуль. Общее количество баллов конкурсного задания составляет 100.

Обязательная к выполнению часть (инвариант) выполняется всеми регионами без исключения на всех уровнях чемпионатов.

Количество модулей из вариативной части, выбирается регионом самостоятельно в зависимости от материальных возможностей площадки соревнований и потребностей работодателей региона в соответствующих специалистах. В случае если ни один из модулей вариативной части не подходит под запрос работодателя конкретного региона, то вариативный (е) модуль (и) формируется регионом самостоятельно под запрос работодателя. При этом, время на выполнение модуля (ей) и количество баллов в критериях оценки по аспектам не меняются.

Описание конкурсного задания

На маршрутизаторе с ОС **VyOS 1.2.9** логин/пароль по умолчанию - **vyos/vyos**.
На компьютерах с ОС **Window 10 Education** - логин/пароль по умолчанию - **admin/P@ssw0rd**.
На компьютерах с ОС **Debian 11, Fedora 37, Ubuntu 22.04.1** логин/пароль по умолчанию - **user/P@ssw0rd** и **root/toor**.
В случае, если в тексте задания не указано иное, все пользовательские учетные записи должны иметь пароль **P@ssw0rd**.

Все проверки работы клиентских технологий (сайтов, клиентских VPN подключений и т.п.) будут выполняться из под пользователя user соответствующих клиентских машин. Сайты будут проверяться через стандартный браузер клиентской **ОС (для Windows - Edge, для Linux - Firefox).**

При выполнении настоящего задания всегда нужно руководствоваться правилом наименьших привилегий. Консольный доступ к виртуальной машине провайдера ISP для участника не предполагается. Следите за тем, чтобы виртуальная машина ISP была включена в течение всего времени выполнения задания.

Модуль А. "Настройка технических и программных средств информационно-коммуникационных систем"

Время на выполнение модуля 4 часа

Задание

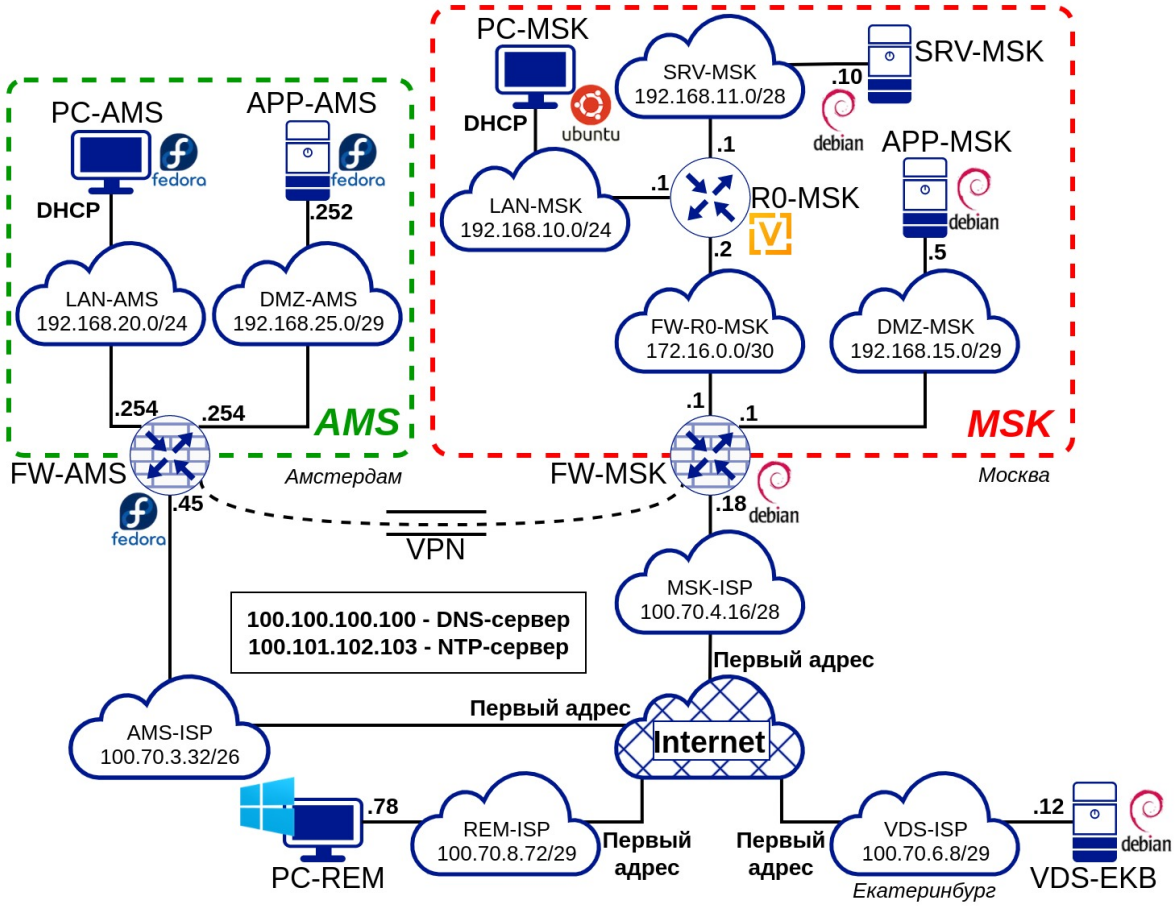
Сеть	Устройство	Адрес/Маска	Шлюз
Internet	PC-REM	100.70.8.72/29	ISP – первый адрес в сети
	FW-AMS	100.70.8.72/29	ISP – первый адрес в сети
	FW-MSK	100.70.4.18/28	ISP – первый адрес в сети
	VDS-EKB	100.70.6.12/29	ISP – первый адрес в сети
	DNS-сервер	100.100.100.100	
	NTP-сервер	100.101.102.103	
FW–R0–MSK	FW-MSK	172.16.0.1/30	
	R0-MSK	172.16.0.2/30	
LAN–MSK	R0–MSK	192.168.10.1/24	
	PC-MSK	DHCP	R0-MSK
SRV–MSK	R0-MSK	192.168.11.1/24	
	SRV–MSK	192.168.11.10/24	R0-MSK
DMZ–MSK	FW-MSK	192.168.15.5/29	
	APP-MSK	192.168.15.5/29	FW-MSK
LAN–AMS	FW–AMS	192.168.20.254	
	PC–AMS	DHCP	FW–AMS
DMZ–AMS	FW–AMS	192.168.25.254/29	
	APP–AMS	192.168.25.252/29	FW–AMS

1. Настройте статичные **IPv4-адреса**, шлюз по умолчанию и описания на интерфейсах **FW*** и **R0** согласно схеме адресации.
2. Настройте статичные **IPv4-адреса** и **шлюз по умолчанию** на всех устройствах, где это требуется, согласно схеме адресации.
3. Настройте **OSPFv2** между **R0-MSK** и **FW-MSK**.
    1. **FW-MSK** должен узнавать о сетях **LAN-MSK** и **SRV-MSK** через OSPF.

    2. **R0** должен получать маршрут по умолчанию и другие необходимые маршруты от **FW-MSK** через OSPF.
    3. Не используйте статические маршруты до этих сетей. Статические маршруты применимы только в качестве временной меры.
    4. **R0-MSK** должен быть защищен от вброса маршрутов с интерфейсов смотрящих в сторону сетей **LAN-MSK** и **SRV-MSK**
    5. **FW-MSK** должен быть защищен от вброса маршрутов с интерфейса смотрящего в сторону сети **DMZ-MSK**.
4. Обеспечьте выход в Интернет для всех устройств московского и амстердамского офисов.
5. Настройте сервер разрешения имен.
    1. Устройства в локальных сетях должны обращаться с **DNS-запросами** к своим **FW**.
    2. Пограничные маршрутизаторы **FW*** должны выполнять пересылку DNS-запросов от локальных клиентов на DNS-сервер по адресу **100.100.100.100**.
    3. **VDS-EKB** должны обращаться с DNS-запросами к **100.100.100.100**.
6. Настройте имена устройств согласно топологии.
7. Настройте для всех устройств московского и амстердамского офисов доменные имена в зонах **msk.jun39.fpo** и **ams.jun39.fpo** соответственно.
    1. Все устройства должны быть доступны в локальных сетях всех филиалов по именам в соответствии с топологией в доменах соответствующих филиалов. К примеру dmz-ams.ams.jun39.rpo или pc-msk.msk.jun39.rpo.
    2. В рамках каждого филиала короткие имена должны **автоматически дополняться** доменным именем соответствующего филиала.
8. Настройте **DHCP-сервер на SRV–MSK** для клиентов в сети **LAN–MSK** и **DHCP-сервер на FW-AMS** для сети **LAN–AMS**. **DHCP-сервер** должен передавать клиентам следующие опции:
    1. Адрес хоста;
    2. Маску сети;
    3. Адрес шлюза;
    4. Имя домена (msk.jun39.rpo и ams.jun39.rpo соответственно);
    5. Адрес DNS (FW);
    6. Адрес NTP (FW);
    7. Выдаваемый диапазон адресов должен иметь запас в как минимум по 10 адресов в начале и конце сети, но не более 50 суммарного запаса.
9. Настройте **DHCP-Relay** на маршрутизаторе **R0-MSK** таким образом, чтобы клиентам в сети **LAN–MSK** адреса выдавал сервер **SRV–MSK**.
10. Настройте синхронизацию времени.
    1. Устройства в локальных сетях **должны синхронизировать** свое время с **FW***.
    2. Устройства с динамическими адресами должны получать получать информацию о сервере времени от своего **DHCP-сервера** и использовать ее для работы.
    3. Пограничные маршрутизаторы **FW*, REM-PC** и **VDS-EKB** должны синхронизировать свое время с **NTP-сервером** по адресу **100.101.102.103**.
    4. Настройте часовой пояс на всех устройствах в соответствии с их географическим расположением.
11. Настройте правила **firewall** так, чтобы устройства в сетях **DMZ-*** не могли инициировать соединения к клиентам в приватных сетях организации, при этом входящие соединения из всех локальных сетей в сети **DMZ-*** должны быть разрешены и машины в сети **DMZ-*** должны иметь доступ в интернет. При необходимости, допускается возможность штучно открывать дополнительные порты, необходимые для выполнения задания.

12. Настройте сетевое обнаружение по протоколу **LLDP** на всех сетевых устройствах и серверах.
13. Настроить удаленный доступ к **VDS-EKB** и **R0-MSK** по **SSH**.
    1. Устройство **PC-MSK** при входе под пользователем **user** должно иметь доступ к **VDS-EKB** под пользователем **user** с использованием ключей **SSH**, без необходимости ввода пароля.
    2. Подключение к **VDS-EKB** с **PC-MSK** должно осуществляться по имени **“VDS”**.
14. Настройте защищенный **VPN-туннель** между **FW-AMS** <= и => **FW-MSK** со следующими параметрами:
    1. Возможно использовать следующие **VPN** технологии: **Wireguard**, **IPsec**, **OpenVPN**.
    2. Используйте современные надежные протоколы шифрования **AES** и семейство **SHA-2**.
    3. **Не допускается** использование протоколов шифрования и аутентификации с длиной ключа/хеша **менее 256 бит**.
    4. Настройте маршрутизацию, NAT и межсетевой экран таким образом, чтобы трафик для другого офиса **не натировался** и **не блокировался**.
15. Настройте работу **OSPFv2** между **FW***, чтобы устройства из московского офиса имели связанность с устройствами из амстердамского.
16. Обеспечьте подключение клиента **PC-REM** к серверу **VPN** на **FW-MSK**.
    1. Возможно использовать следующие **VPN** технологии: **Wireguard**, **IPsec**, **OpenVPN**.
    2. Клиент должен иметь доступ к серверам в сети **SRV-MSK**.
    3. Соединение должно автоматически устанавливаться при включении компьютера или входе под пользователем **user**.
17. Настройте централизованный сбор журналов **syslog** на **SRV-MSK**.
    1. Журналы должны храниться в файлах **/opt/logs/[hostname]**, где **hostname** - это короткое или полное доменное имя машины, предоставившей соответствующие сообщения.
    2. **PC-MSK** должен записывать сообщения error и более важные.
    3. **FW-*** должны записывать сообщения warning и более важные.
    4. **FW-MSK** должен записывать сообщения от служб ospf и имеющихся на устройстве служб туннелирования (ipsec, openvpn, wireguard и т.д) уровня не менее notice.

Топология



Модуль Б. "Развертывание и сопровождение сетевой инфраструктуры"

Время на выполнение модуля 4 часа

Задание

Сеть	Устройство	Адрес/Маска	Шлюз
Internet	PC-REM	100.70.8.78/29	ISP – первый адрес в сети
	FW-AMS	100.70.3.45/29	ISP – первый адрес в сети
	FW-MSK	100.70.4.18/28	ISP – первый адрес в сети
	VDS-EKB	100.70.6.12/29	ISP – первый адрес в сети
	DNS-сервер	100.100.100.100	
	NTP-сервер	100.101.102.103	
FW–R0–MSK	FW-MSK	172.16.0.1/30	
	R0-MSK	172.16.0.2/30	
LAN–MSK	R0–MSK	192.168.10.1/24	
	PC-MSK	DHCP	R0-MSK
SRV–MSK	R0-MSK	192.168.11.1/24	
	SRV–MSK	192.168.11.10/24	R0-MSK

Сеть	Устройство	Адрес/Маска	Шлюз
DMZ–MSK	FW-MSK	192.168.15.12/29	
	APP-MSK	192.168.15.5/29	FW-MSK
LAN–AMS	FW–AMS	192.168.20.254	
	PC–AMS	DHCP	FW–AMS
DMZ–AMS	FW–AMS	192.168.25.254/29	
	APP–AMS	192.168.25.252/29	FW–AMS
LAN-IKT	FW-IKT	192.168.30.128/24	
	PC-IKT	DHCP	FW-IKT
	SRV-IKT	192.168.30.254/24	FW-IKT
DMZ-IKT	FW-IKT	192.168.35.129/29	
	APP-IKT	192.168.35.130/29	FW-IKT

В связи с большим спросом на наши услуги на Дальнем востоке, для обеспечения качественного соединения и разумного уровня задержек по передачи данных, руководство приняло решение открыть новый филиал в Сибири. Создайте необходимую инфраструктуру для нового филиала в Иркутске.

1. **Разверните необходимые машины** из шаблонов и назначьте им параметры стандартные параметры шаблона.
2. Создайте виртуальные сети и соедините устройства согласно топологии.
3. Настройте **IPv4-адресацию** на устройствах в иркутском филиале и обеспечьте выход в интернет.
4. Настройте сервер разрешения имен.
    1. Устройства в локальных сетях должны обращаться с **DNS-запросами** к своему **FW**.
    2. **FW–IKT** должен выполнять пересылку DNS-запросов от локальных клиентов на DNS-сервер по адресу **100.100.100.100**.
5. Настройте для всех новых устройств соответствующие им имена и доменное имя **ikt.jun39.rpo**.
6. Как исправить ошибку Minecraft GLFW 65542 (драйвер не поддерживает OpenGL)? Настройте синхронизацию времени аналогично другим филиалам.
7. Настройте защищенные **VPN-туннели FW-IKT**<= и => **FW-MSK** со следующими параметрами:
    1. Возможно использовать следующие **VPN** технологии: **Wireguard**, **IPsec**, **OpenVPN**.
    2. Используйте современные надежные протоколы шифрования **AES** и семейство **SHA-2**.
    3. **Не допускается** использование протоколов шифрования и аутентификации с длиной ключа/хеша **менее 256 бит**.
    4. Настройте NAT и межсетевой экран таким образом, чтобы трафик для другого офиса **не натировался** и не **блокировался**.
    5. Настройка тоннеля не должна помешать функционированию тоннеля между AMS и MSK.

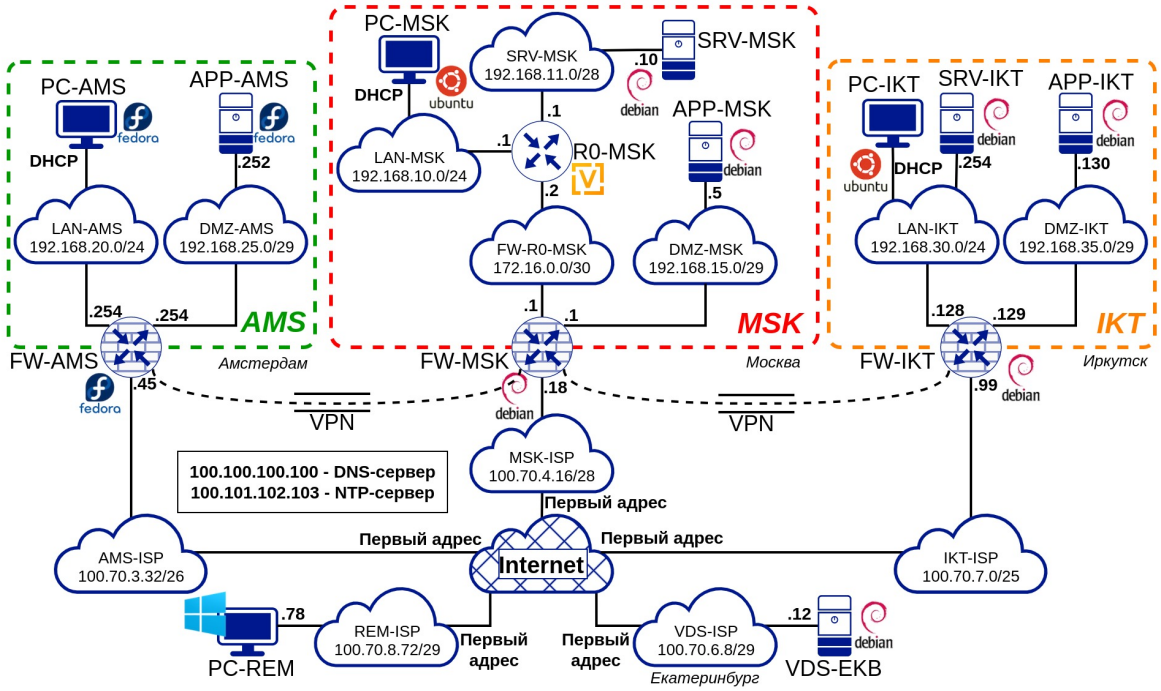
6. Настройте работу **OSPFv2**, чтобы устройства из иркутского филиала имели связанность с устройствами из московского и амстердамского.
7. Настройте инфраструктуру DNS, чтобы устройства из иркутского филиала имели могли обратиться к устройствам других филиалов по доменным именам.

8. Создайте пользователя **admin** с паролем **P@ssw0rd** на **SRV–IKT**, и добавьте в группу sudo.
9. Настройте общий доступ к файлам на **SRV–IKT** по протоколу **NFS**.
    1. Каталог для хранения файлов **/opt/nfs/rw** должен быть доступен для чтения и записи.
    2. Каталог для хранения файлов **/opt/nfs/ro** должен быть доступен только для чтения.
    3. **NFS** должен быть доступен для клиентов в сети **LAN-IKT**.
10. Настройте клиент **NFS** на **PC–IKT**.
    1. Путь **/opt/nfs/rw** на **SRV–IKT** должен быть смонтирован в каталог **/home/user/Desktop/nfs_rw** на **PC–IKT**.
    2. Путь **/opt/nfs/ro** на **SRV–IKT** должен быть смонтирован в каталог **/home/user/Desktop/nfs_ro** на **PC–IKT**.
    3. Монтирование **должно восстанавливаться** при перезагрузке виртуальной машины.
11. Настройте права доступа для каталога **/opt/nfs/** на **SRV–IKT**.
    1. Пользователь **admin** должен иметь права на чтение и запись в каталог **/opt/nfs** и все его подкаталоги.
12. На каждом из серверов **APP-*** должен быть развернут **WEB-сервер**.
    1. Сайт должен открываться по адресу **web.jun39.rpo** по протоколу HTTP на стандартном порте и должен быть доступен из сети интернет.
    2. Сайт должен содержать следующий текст: “Welcome to Minecraft server mc.jun39.rpo site in **XX** region”, где **XX** заменено на “European”, “Central”, “Siberian” соответственно региональному расположению.
13. На сервере **VDS-EKB** разверните сервер **DNS**.
    1. Сервер должен расшифровывать зону **jun39.rpo**.
    2. Имя **jun39.rpo** для клиентов в сети интернет должно расшифровываться в адрес сервера **VDS-EKB**.
    3. Имя **web.jun39.rpo** для для клиентов в сети интернет должно расшифровываться во внешний адрес **FW-*** в ближайшем к клиенту регионе.
    4. Не забудьте проконтролировать, что клиенты **PC-REM** обращаются с **DNS-запросами** к **VDS-EKB**.
14. Внутри филиалов имя **web.jun39.rpo** должно расшифровываться и в локальный адрес **APP-*** в соответствующем регионе и по нему должен открываться соответствующий сайт.
15. Настройте **CA** на **SRV-MSK** со следующими параметрами
    1. Используйте **/opt/ca** в качестве корневой директории CA;
    2. Страна RU;
    3. Организация RPO;
    4. CN должен быть установлен как RPO CA;
    5. Создайте корневой сертификат CA;
    6. SRV-MSK и PC-MSK должны доверять CA.
16. На сервере **SRV-MSK** должен быть развернут **WEB-сервер**:
    1. .Сайт должен открываться по адресу **corp.msk.jun39.rpo**.
    2. Сайт должен содержать следующий текст “Welcome to secure corporate portal jun39.rpo”
    3. Сайт должен функционировать по протоколу **HTTPS**. При обращении по протоколу HTTP должен происходить **автоматическая переадресация** на HTTPS.

4. **WEB-сервер** должен иметь **сертификат**, подписанный корпоративным центром сертификации.
5. Сайт должен открываться с **PC-MSK** без ошибок и предупреждений.

17. Обеспечьте подключение удаленного сотрудника с компьютера **PC-REM** к корпоративному порталу https://corp.msk.jun39.rpo посредством **VPN-подключения**. При этом открытие портала не должно вызывать ошибок и предупреждений безопасности.
18. На **VDS-EKB** разверните сервер Minecraft. Для этого непосредственно перед началом развертывания сервера выделите виртуальной машине побольше ресурсов, а именно **3 VCPU** и **4 GB** оперативной памяти. После этого, разверните сервер Minecraft со следующими параметрами:
    1. Имя сервера: Jun39;
    2. Ограничение кол-ва игроков: 12;
    3. Порт: по умолчанию (25565);
    4. Проверка аккаунтов пользователей: отключена;
    5. Сервер должен быть запущен в виде контейнера Docker;
    6. Контейнер должен автоматически запускаться после перезагрузки компьютера;
    7. Для проверки можете использовать **tlauncher** расположенный на VDS-EKBвашем операторском рабочем месте. Подключение осуществляется по внешнему адресу ISP (в сети 172.16.0.0), можно получить в интерфейсе среды виртуализации.
19. На сервере **APP-MSK** разверните сервер облачного хранения данных. Для этого непосредственно перед началом развертывания сервера выделите виртуальной машине побольше ресурсов, а именно **2 VCPU** и **2 GB** оперативной памяти. После этого, разверните сервер со следующими параметрами:
    1. Файловый сервер: **NextCloud**;
    2. База данных: **MariaDB**;
    3. Веб интерфейс БД: **phpMyAdmin**;
    4. Порт NextCloud: **8080**;
    5. Порт phpMyAdmin: **8888**;
    6. Все сервисы должны быть запущены в виде контейнеров **Docker**;
    7. Все контейнеры должны автоматически запускаться после **перезагрузки компьютера**.
20. Обеспечьте подключение удаленного сотрудника с компьютера **PC-REM** к корпоративному облачному хранилищу на **APP-MSK** посредством имеющегося **VPN-подключения**.

Топология



Примерные задержки передачи данных между клиентами и филиалами.

RTT	AMS	MSK	SPB	EKB	IKT	REM
AMS	-	44	44	70	124	170
MSK	44	-	10	24	74	110
EKB	70	24	30	-	40	90
IKT	124	74	74	40	-	50
REM	170	110	120	90	50	-

Модуль B. "Поиск и устранение неисправностей"

Время на выполнение модуля 4 часа

Секретное задание