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

КОНКУРСНОЕ ЗАДАНИЕ КОМПЕТЕНЦИИ

«Сетевое и системное администрирование» (Юниоры)

Региональный чемпионат по профессиональному мастерству «Профессионалы» в 2025 г.

2025 г.

Конкурсное задание разработано экспертным сообществом и утверждено Менеджером компетенции, в котором установлены нижеследующие правила и необходимые требования владения профессиональными навыками для участия в соревнованиях по профессиональному мастерству.

**Конкурсное задание включает в себя следующие разделы:**

[1. ОСНОВНЫЕ ТРЕБОВАНИЯ КОМПЕТЕНЦИИ 4](#_Toc187830907)

[1.1. ОБЩИЕ СВЕДЕНИЯ О ТРЕБОВАНИЯХ КОМПЕТЕНЦИИ 4](#_Toc187830908)

[1.2. ПЕРЕЧЕНЬ ПРОФЕССИОНАЛЬНЫХ ЗАДАЧ СПЕЦИАЛИСТА ПО КОМПЕТЕНЦИИ «Сетевое и системное администрирование» 4](#_Toc187830909)

[1.3. ТРЕБОВАНИЯ К СХЕМЕ ОЦЕНКИ 9](#_Toc187830910)

[1.4. СПЕЦИФИКАЦИЯ ОЦЕНКИ КОМПЕТЕНЦИИ 9](#_Toc187830911)

[1.5. КОНКУРСНОЕ ЗАДАНИЕ 10](#_Toc187830912)

[1.5.1. Разработка/выбор конкурсного задания 10](#_Toc187830913)

[1.5.2. Структура модулей конкурсного задания 11](#_Toc187830914)

[2. СПЕЦИАЛЬНЫЕ ПРАВИЛА КОМПЕТЕНЦИИ 30](#_Toc187830915)

[2.1. Личный инструмент конкурсанта 30](#_Toc187830916)

[2.2.Материалы, оборудование и инструменты, запрещенные на площадке 30](#_Toc187830917)

[3. Приложения 30](#_Toc187830918)

**ИСПОЛЬЗУЕМЫЕ СОКРАЩЕНИЯ**

1. ФГОС – Федеральный государственный образовательный стандарт
2. ПС – Профессиональный стандарт
3. КЗ – Конкурсное задание
4. ИЛ – Инфраструктурный лист
5. ИКС – Информационно коммуникационная система
6. КС – Компьютерная сеть
7. ОС – Операционная система

1. ОСНОВНЫЕ ТРЕБОВАНИЯ КОМПЕТЕНЦИИ

1.1. ОБЩИЕ СВЕДЕНИЯ О ТРЕБОВАНИЯХ КОМПЕТЕНЦИИ

Требования компетенции (ТК) «Сетевое и системное администрирование» определяют знания, умения, навыки и трудовые функции, которые лежат в основе наиболее актуальных требований работодателей отрасли.

Целью соревнований по компетенции является демонстрация лучших практик и высокого уровня выполнения работы по соответствующей рабочей специальности или профессии.

Требования компетенции являются руководством для подготовки конкурентоспособных, высококвалифицированных специалистов / рабочих и участия их в конкурсах профессионального мастерства.

В соревнованиях по компетенции проверка знаний, умений, навыков и трудовых функций осуществляется посредством оценки выполнения практической работы.

Требования компетенции разделены на четкие разделы с номерами и заголовками, каждому разделу назначен процент относительной важности, сумма которых составляет 100.

1.2. ПЕРЕЧЕНЬ ПРОФЕССИОНАЛЬНЫХ ЗАДАЧ СПЕЦИАЛИСТА ПО КОМПЕТЕНЦИИ «Сетевое и системное администрирование»

*Перечень видов профессиональной деятельности, умений и знаний и профессиональных трудовых функций специалиста (из ФГОС/ПС/ЕТКС..) и базируется на требованиях современного рынка труда к данному специалисту*

*Таблица №1*

**Перечень профессиональных задач специалиста**

|  |  |  |
| --- | --- | --- |
| **№ п/п** | **Раздел** | **Важность в %** |
| 1 | Выполнение работ по выявлению и устранению инцидентов в информационно-коммуникационных системах | 25 |
| - Специалист должен знать и понимать:Лицензионные требования по настройке и эксплуатации устанавливаемого программного обеспеченияОсновы архитектуры, устройства и функционирования вычислительных системПринципы организации, состав и схемы работы операционных системСтандарты информационного взаимодействия системРегламенты проведения профилактических работ на администрируемой информационно-коммуникационной системеИнструкции по установке администрируемых сетевых устройствИнструкции по эксплуатации администрируемых сетевых устройствИнструкции по установке администрируемого программного обеспеченияИнструкции по эксплуатации администрируемого программного обеспеченияТребования охраны труда при работе с аппаратными, программно-аппаратными и программными средствами администрируемой информационно-коммуникационной системы. |
| - Специалист должен уметь:Идентифицировать инциденты, возникающие при установке программного обеспечения, и принимать решение об изменении процедуры установкиОценивать степень критичности инцидентов при работе прикладного программного обеспеченияУстранять возникающие инцидентыЛокализовать отказ и инициировать корректирующие действияПользоваться нормативно-технической документацией в области инфокоммуникационных технологийПроизводить мониторинг администрируемой информационно-коммуникационной системыКонфигурировать операционные системы сетевых устройствПользоваться контрольно-измерительными приборами и аппаратуройДокументировать учетную информацию об использовании сетевых ресурсов согласно утвержденному графику |
| 2 | Обеспечение работы технических и программных средств информационно-коммуникационных систем | 25 |
| - Специалист должен знать и пониматьИспользовать современные методы контроля производительности информационно-коммуникационной системы; Анализировать сообщения об ошибках в сетевых устройствах и операционных системах; Локализовывать отказ и инициировать корректирующие действия; Применять программно-аппаратные средства для диагностики отказов и ошибок сетевых устройств; Применять штатные программно-аппаратные средства для контроля производительности сетевой инфраструктуры информационно-коммуникационной системы; Применять внешние программно-аппаратные средства для контроля производительности сетевой инфраструктуры информационно-коммуникационной системы; |
| - Специалист должен уметь:Общие принципы функционирования аппаратных, программных и программно-аппаратных средств администрируемой сети; Архитектура аппаратных, программных и программно-аппаратных средств администрируемой сети; Инструкции по установке администрируемых сетевых устройств; Инструкции по эксплуатации администрируемых сетевых устройств; Инструкции по установке администрируемого программного обеспечения; Инструкции по эксплуатации администрируемого программного обеспечения; Протоколы канального, сетевого, транспортного и прикладного уровней модели взаимодействия открытых систем; Базовая эталонная модель взаимодействия открытых систем; Международные стандарты локальных вычислительных сетей; Модели информационно-телекоммуникационной сети «Интернет»; Регламенты проведения профилактических работ на администрируемой информационно-коммуникационной системе; Устройство и принцип работы кабельных и сетевых анализаторов; Средства глубокого анализа информационно-коммуникационной системы; Метрики производительности администрируемой информационно-коммуникационной системы; Регламенты проведения профилактических работ на администрируемой информационно-коммуникационной системе; Требования охраны труда при работе с сетевой аппаратурой администрируемой информационно-коммуникационной системы; |
| 3 | Реализация схемы резервного копирования, архивирования и восстановления конфигураций технических и программных средств информационно-коммуникационных систем по утвержденным планам | 25 |
| - Специалист должен знать и понимать:Общие принципы функционирования аппаратных, программных и программно-аппаратных средств администрируемой информационно-коммуникационной системы; Архитектура аппаратных, программных и программно-аппаратных средств администрируемой информационно-коммуникационной системы; Инструкции по установке администрируемых сетевых устройств информационно-коммуникационной системы; Инструкции по эксплуатации администрируемых сетевых устройств информационно-коммуникационной системы; Инструкции по установке администрируемого программного обеспечения; Инструкции по эксплуатации администрируемого программного обеспечения; Протоколы канального, сетевого, транспортного и прикладного уровней модели взаимодействия открытых систем; Базовая эталонная модель взаимодействия открытых систем для управления сетевым трафиком; Международные стандарты локальных вычислительных сетей Регламенты проведения профилактических работ на администрируемой информационно-коммуникационной системе; Требования охраны труда при работе с сетевой аппаратурой администрируемой информационно-коммуникационной системы; |
| - Специалист должен уметь:Использовать процедуры восстановления данных; определять точки восстановления данных; работать с серверами архивирования и средствами управления операционных систем; Пользоваться нормативно-технической документацией в области инфокоммуникационных технологий; Выполнять плановое архивирование программного обеспечения пользовательских устройств согласно графику; |
| 4 | Внесение изменений в технические и программные средства информационно-коммуникационных систем по утвержденному плану работ | 25 |
| - Специалист должен знать и понимать:Использовать современные методы контроля производительности информационно-коммуникационной системы; Анализировать сообщения об ошибках в сетевых устройствах и операционных системах; Локализовывать отказ и инициировать корректирующие действия; Применять программно-аппаратные средства для диагностики отказов и ошибок сетевых устройств; Применять штатные программно-аппаратные средства для контроля производительности сетевой инфраструктуры информационно-коммуникационной системы; Применять внешние программно-аппаратные средства для контроля производительности сетевой инфраструктуры информационно-коммуникационной системы; |
| - Специалист должен уметь:Общие принципы функционирования аппаратных, программных и программно-аппаратных средств администрируемой сети; Архитектура аппаратных, программных и программно-аппаратных средств администрируемой сети; Инструкции по установке администрируемых сетевых устройств; Инструкции по эксплуатации администрируемых сетевых устройств; Инструкции по установке администрируемого программного обеспечения; Инструкции по эксплуатации администрируемого программного обеспечения; Протоколы канального, сетевого, транспортного и прикладного уровней модели взаимодействия открытых систем; Базовая эталонная модель взаимодействия открытых систем; Международные стандарты локальных вычислительных сетей; Модели информационно-телекоммуникационной сети «Интернет»; Регламенты проведения профилактических работ на администрируемой информационно-коммуникационной системе; Устройство и принцип работы кабельных и сетевых анализаторов; Средства глубокого анализа информационно-коммуникационной системы; Метрики производительности администрируемой информационно-коммуникационной системы; Регламенты проведения профилактических работ на администрируемой информационно-коммуникационной системе; Требования охраны труда при работе с сетевой аппаратурой администрируемой информационно-коммуникационной системы; |

1.3. ТРЕБОВАНИЯ К СХЕМЕ ОЦЕНКИ

Сумма баллов, присуждаемых по каждому аспекту, должна попадать в диапазон баллов, определенных для каждого раздела компетенции, обозначенных в требованиях и указанных в таблице №2.

*Таблица №2*

**Матрица пересчета требований компетенции в критерии оценки**

|  |  |
| --- | --- |
| **Критерий/Модуль** | **Итого баллов за раздел ТРЕБОВАНИЙ КОМПЕТЕНЦИИ** |
| **Разделы** **ТРЕБОВАНИЙ КОМПЕТЕНЦИИ** |  | **Б** | **Г** |  |
| **1** | 25 | 0 | 25 |
| **2** | 25 | 0 | 25 |
| **3** | 5 | 20 | 25 |
| **4** | 5 | 20 | 25 |
| **Итого баллов за критерий/модуль** | 60 | 40 | **100** |

1.4. СПЕЦИФИКАЦИЯ ОЦЕНКИ КОМПЕТЕНЦИИ

Оценка Конкурсного задания будет основываться на критериях, указанных в таблице №3:

*Таблица №3*

**Оценка конкурсного задания**

|  |  |
| --- | --- |
| **Критерий** | **Методика проверки навыков в критерии** |
| **Б** | **Настройка технических и программных средств информационно-коммуникационных систем** | В соответствии с используемыми ОС и Сетевым оборудованием |
| **Г** | **Обеспечение отказоустойчивости** | В соответствии с используемыми ОС и Сетевым оборудованием |

1.5. КОНКУРСНОЕ ЗАДАНИЕ

Общая продолжительность Конкурсного задания: 12 ч.

Количество конкурсных дней: 3 дня (1 и 2 день – Модуль Б; 3 день – Модуль Г).

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.

1.5.1. Разработка/выбор конкурсного задания

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

1.5.2. Структура модулей конкурсного задания

**Рекомендованное региональное задание
ССА Юниоры 2025**

региональный этап чемпионатов Всероссийского чемпионатного движения по профессиональному мастерству в 2025 году, компетенция “Сетевое и системное администрирование”, возрастная категория Юниоры 14+

***Авторский состав: Рачеев А.В., Золотарёв А.П.***

***[Примечание автора]***

*Здесь и далее курсивом обозначены примечания авторов, предназначенные, в первую очередь, для экспертов, которые планируют организовывать мероприятия по этому заданию или производным от него а также задействованным в этом технических экспертов.*

* 1. **КОНКУРСНОЕ ЗАДАНИЕ**

Формат участия: индивидуальный

Возрастной ценз: от 14 лет

Общая продолжительность Конкурсного задания: 12 ч.

Количество конкурсных дней: 3 дня.

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

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

Конкурсное задание состоит из 3 модулей, общее количество баллов конкурсного задания составляет 100.

Оценка каждого дня осуществляется в соответствующий день.

***[Последовательность выполнения задания и проверки]***

*Модули Б в данном задании сквозной, выполняются на одной и той же инфраструктуре в течение двух соревновательных дней. Модуль Г “Отказоустойчивость и автоматизация” выполняется в третий соревновательный день на отдельных стендах. Задание каждого соревновательного дня подразумевает проверку в день выполнения.*

***[Требования к рабочему месту, среде виртуализации и ресурсам]***

*Задание не подразумевает использование множественных физических рабочих мест, а также физических коммутаторов и маршрутизаторов. Рабочее место участника подразумевает только ПК с доступом к интерфейсу среды виртуализации.*

*Для организации лабораторной инфраструктуры подойдет любая среда виртуализации с поддержкой технологий vlan/trunk и возможностью клонирования виртуальных машин или развертывания ВМ из шаблона.*

*Допустимо использовать рабочее место участника как сервер виртуализации при наличии на нем достаточного объема ресурсов, однако такой подход не рекомендован в силу малой надежности и проблем с обслуживанием.*

*Лабораторный стенд для выполнения данного задания при указанных в соответствующем разделе, предустановленных ОС (например развернутых из образа) имеет следующие требования к ресурсам.*

*Минимальные системные требования:*

* *10 гб ОЗУ*
* *4 процессорных ядра*
* *120 гб SSD-пространства (при использовании “тонких” виртуальных дисков)*
* *интернет на скорости не менее 5 мбит/с*
* *Допускается увеличение объема ресурсов в соответствии с возможностями инфраструктуры, в которой проводится чемпионатное мероприятие, с обеспечением равных условий для всех участников*

***[ISP]***

*В сетевой инфраструктуре функционирует недоступная участникам и не указанная явно в задании виртуальная машина ISP, которая имеет следующие роли:*

1. *Представляет функции провайдеров интернета для филиалов и внешних клиентов.*
2. *Является NAT-шлюзом в реальный интернет, что обеспечивает выполнимость задания.*
3. *При необходимости позволяет контролировать и/или ограничивать доступ машин к реальному интернету, однако данная версия задания подразумевает доступ в интернет для его выполнения.*
4. *Является сервером DNS и провайдером DNS для доменов, необходимых для выполнения задания. Провайдер DNS доступен через веб-интерфейс. Может быть реализован как самодельным решением, так и готовым софтом, например SnitchDNS.*
5. *Является сервером времени (chrony).*
6. *При необходимости, на эту машину можно добавлять другие сервисы необходимые для выполнения производных версий от этого задания.*

*При необходимости получить преднастроенную версию ISP или иные комментарии по его функционированию - можете обратиться в чат компетенции, там Вам, скорее всего, помогут.*

**Операционные системы:**

***[Примечание автора]***

*При разработке задания предполагалась возможность реализовывать его на разных операционных системах.*

*Серверные и клиентские устройства без существенных проблем можно заменить на любую другую ОС общего назначения семейства Linux.*

*ОС межсетевых экранов также возможно заменить на другие, однако функционал различного ПО для межсетевого экранирования может иметь существенные отличия, и для некоторых ОС могут потребоваться изменения в задании вплоть до переноса некоторых задач с фаервола на другие сервера и/или исключения из задания протоколов динамической маршрутизации.*

*Обновления ОС до более новых версий в рамках ближайших нескольких лет не должны привести к невыполнимости задания, т.к. все используемые технологии продолжают развиваться/поддерживаться и не предполагают вывода из эксплуатации в ближайшее время.*

*Конкретное графическое окружение (GUI) ОС Linux не принципиально для выполнения задания, однако там, где указано, графическое окружение должно быть. Обратите внимание, что графическое окружение может существенно влиять на потребность ВМ в ресурсах.*

*В виртуальные машины с ОС семейства Linux рекомендуется предустановить следующие пакеты: компоненты управления используемой среды виртуализации (qemu-guest-agent / open-vm-tools / hyperv-daemons / …), dnsutils / bind-utils, tcpdump и иные компоненты, обусловленные особенностями Вашей инфраструктуры.*

*На указанных ОС задание выполнимо на 100%.*

*В данной таблице указаны ОС для модуля Б (1й и 2й соревновательные дни).*

|  |  |  |  |
| --- | --- | --- | --- |
| **ВМ** | **ОС** | **Ресурсы (примерно)** | **GUI** |
| ISP | - | 0.5Gb; 1CPU | - |
| FW-RND | OPNsense 24.7 | 1Gb; 1CPU | - |
| DC-RND | Alt Server 10.2 | 2Gb; 2CPU | - |
| PC-RND | Alt Workstation 10.4 | 1Gb; 1CPU | MATE |
| NB-RND | Alt Workstation 10.4 | 1Gb; 1CPU | MATE |
| FW-KRD | OPNsense 24.7 | 1Gb; 1CPU | - |
| SRV-KRD | Alt Server 10.2 | 1Gb; 1CPU | - |
| PC-KRD | Alt Workstation 10.4 | 1Gb; 1CPU | MATE |
| CLIENT-EXT | Alt Workstation 10.4 | 1Gb; 1CPU | MATE |

**Стек технологий, знание которых требуется для выполнения задания и возможных изменений в задании в рамках 30% изменений:**

*Вариативная и расширенная вариативная часть стека не подразумевает использование всех технологий в конкретном чемпионатном мероприятии, однако если вы используете задание как основу для своего образовательного процесса или планируете подготовку для мероприятий межрегионального и федерального уровня, то данные разделы могут быть Вам полезны.*

**Инвариативная часть:**

* Настройка IPv4 адресации
* DHCPv4
* NAT, PAT, Проброс портов
* Статическая маршрутизация
* Туннелирование/VPN (Site-to-Site)
* Пользователи и группы
* Работа с дисками (разметка, монтирование)
* Реализация дискреционной модели прав доступа к файловой системе
* Установка программного обеспечения
* DNS (прямой просмотр)
* Веб-сервер
* NTP/Chrony
* SSH
* Контейнеры Docker
	+ Установка и запуск контейнеров;
	+ Проброс портов;
	+ Связь между контейнерами;
	+ Управление контейнерами.

**Вариативная часть:**

* Loopback-интерфейсы
* Динамическая маршрутизация
* Туннелирование/VPN (Site-to-Client)
* DNS (обратный просмотр)
* Доменные инфраструктуры (FreeIPA)
* Базы данных (Postgresql/Mariadb)
* Центр сертификации, SSL
* FTP
* Централизованная система журналирования (syslog, rsyslog и т.п.)
* Работа с дисками (LVM, RAID, квотирование, шифрование)
* Системы мониторинга ресурсов (Zabbix)
* Отказоустойчивость и/или балансировка нагрузки
* Настройка автоматизированного рабочего места
* Работа с юнитами systemd (управление юнитами, создание простого юнита)
* Работа с системным загрузчиком GRUB

**Расширенная вариативная часть:**

* Авторизация пользователей для получения доступа к ЛВС.
* AAA
* Кластеризованные сетевые и серверные системы
* Резервные провайдеры интернет
* Защищенные сетевые сегменты (специализированные VLAN, отдельные провайдеры с ограниченным доступом, VPN-туннель в закрытый сегмент)
* Автоматизации настройки и развертывания программного обеспечения

**ЗАДАНИЕ**

***[примечание автора]***

*Далее идет та часть, предназначенная для выдачи участникам, однако в ее содержании, в основном в преамбуле, есть определенные моменты, которые могут зависеть от преднастроя и реализации машин в конкретной инфраструктуре виртуализации. Сразу отмечу, что преамбула является неотъемлемой частью задания и содержит моменты, непосредственно влияющие на проверку задания и его выполнимость.*

**Преамбула: Техническое описание лабораторной инфраструктуры и общие требования к реализации.**

В случае, если в тексте задания не указано иное, все учетные записи должны иметь пароль P@ssw0rd

Если для выполнения определенного действия вам требуется указать имя пользователя, которое не указано в задании и система не имеет пользователя по умолчанию, или система имеет повышенные требования к паролю и P@ssw0rd использовать невозможно, укажите необходимые данные для входа около соответствующего пункта задания.

Все проверки работы клиентских технологий (сайтов, клиентских VPN подключений и т.п.), если в задании не указано иного, будут выполняться из под пользователя user соответствующих клиентских машин.

При выполнении настоящего задания всегда нужно руководствоваться правилом наименьших привилегий, в особенности при настройке внешних интерфейсов пограничных шлюзов.

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.

Обратите внимание, что провайдерская адресация 100.64.0.0/10 относится к серому (частотному) диапазону адресов, что может потребовать дополнительных настроек на граничных сетевых устройствах межсетевого экранирования. Однако, в терминологии задания, сеть 100.64.0.0/10 относится к внешним (“белым”) сетям, наряду с “белыми” сетями из реального интернета.

Знак \* (звёздочка, астериск) в задании является подстановочным знаком заменяет произвольную последовательность символов от начала строки или пробельного символа до другого пробельного символа или конца строки. К примеру, при указании на устройство FW\* имеются ввиду все устройства в задании, название которых начинается с FW, например FW1, FW-MSK, FWabc и т.п., а при указании сетей \*MSK имеются в виду все сети в задании, название которых заканчивается на MSK, например LAN1-MSK, SRV-MSK, dmzMSK и т.п.

Операционная система OPNsense в интерфейсе при названии некоторых объектов не допускает использование символа “-”, в таком случае его можно заменять на знак “\_”, но только там, где указать “-” невозможно.

В инфраструктуре функционирует DNS-провайдер (расположенный на ВМ ISP), его интерфейс доступен по адресу https://ns.ext/. Учетная запись: jun

При настройке FreeIPA FQDN в обязательном порядке требуется указывать в нижнем регистре.

vSW на схеме не является отдельным устройством или виртуальной машиной. Данный функционал обеспечивается сетевой подсистемой используемой среды виртуализации.

Согласно политике Организации, все службы и технологии, необходимые для выполнения задания, должны запускаться автоматически и функционировать в соответствии с заданием при запуске операционных систем, если в задании явно не указано иного.

**Предыстория:**

Рады приветствовать Вас на юге нашей необъятной родины в логистическом и индустриальном центре, городе Ростов-на-Дону! Не поверите, как сложно найти компетентного специалиста, который умеет администрировать отечественные операционные системы, да еще и в сетях разбирается! Мы очень рады что Вы теперь с нами в логистической компании “Destination Reachable” (далее Компания). Следуя потребностям наших клиентов, Компания старается, по возможности, использовать отечественные аппаратные и программные решения. Здесь, в Ростове, располагается наш основной филиал (внутреннее обозначение RND), также, следуя динамике развития регионов, мы, с Вашей помощью, будем открывать новый филиал в Краснодаре (KRD). Наши клиенты располагаются по всей России, поэтому часть наших сервисов предоставляются и внешним пользователям. Все оборудование только что распаковано, операционные системы предустановлены, в соответствии с техническим заданием. Для доступа к сети Интернет нашей компанией заключены договора с провайдерами интернета для обоих филиалов с предоставлением “белых” ip-адресов \*(подробнее в разделе “Техническое описание лабораторной инфраструктуры и общие требования к реализации”).

“ Destination Reachable – Доставку обеспечат Профессионалы! ”

**Схема IP-адресации и схема подключений.**

Схема адресации локальных сетей в задании разрабатывается участниками, однако требуется придерживаться следующих условий:

1. Для локальных сетей используется только приватная адресация из стандартных приватных диапазонов.
2. Все сети, соединяющие маршрутизаторы между собой, включая сети туннелей site-to-site должны иметь маску сети /30 или /29 (там где необходимо).
3. Все остальные локальные сети, включая клиентские VPN-сети, должны иметь адресацию с маской /24. При этом шлюзом по умолчанию в таких сетях должен быть первый или последний адрес в сети, после принятия решения по адресации шлюзов по умолчанию, используйте аналогичные (только первые или только последние) адреса для шлюзов во всей инфраструктуре.
4. При выполнении задания впишите адреса выданные устройствам в столбец “Адрес/Маска” рядом со словом “STATIC”

|  |  |  |  |
| --- | --- | --- | --- |
| Сеть  | Устройство  | Адрес/Маска  | Шлюз |
| INTERNET | FW-RND | 100.67.32.80/26 | ISP – первый адрес в сети |
|  | FW-KRD | 100.127.90.57/27 | ISP – первый адрес в сети |
|   | Client-EXT | 100.108.128.45/28 | ISP – первый адрес в сети |
|  | DNS-сервер  | 100.100.100.100 |  |
|  | NTP-сервер | 100.101.102.103 |  |
| SRV-RND (vl2000) | FW-RND | STATIC |   |
|   | DC-RND | STATIC | FW-RND |
| LAN-RND (vl2010) | FW-RND | STATIC |   |
|   | PC-RND | DHCP | FW-RND |
| GST-RND (vl2020) | FW-RND | STATIC |   |
|   | NB-RND | DHCP | FW-RND |
| SRV-KRD | FW-KRD | STATIC |   |
|   | SRV-KRD | STATIC | FW-KRD |
| LAN-KRD | FW-KRD | STATIC |   |
|   | PC-KRD | DHCP | FW-KRD |

**Схема сети приведена в отдельном файле!**

**Модуль Б. (Настройка технических и программных средств информационно-коммуникационных систем) (инвариант)**

Время на выполнение модуля: 8 часов

**Часть 1 (1-й день - 4 часа)**

1. Настройте IPv4-адреса согласно схеме адресации:
	1. Настройте адреса шлюза по умолчанию, где это требуется;
	2. На FW\* настройте описания интерфейсов, согласно схеме сети
2. Настройте имена всех устройств согласно топологии.
3. Все устройства должны иметь доступ в интернет, если в задании явно не указано иного.
4. Подготовьте PC-RND к работе пользователя:
	1. Установите на АРМ офисный пакет (МойОфис / Р7 Офис) и создайте на него ярлык на рабочем столе.
	2. Установите Яндекс-браузер и создайте на него ярлык на рабочем столе.
5. В филиале RND разверните домен rnd.jun.profi на базе FreeIPA с контроллером домена на DC-RND. При развертывании учтите, что это устройство будет выполнять функции DNS и DHCP сервера в филиале RND.
	1. Создайте пользователей и группы в домене:
		1. группу jun-users, добавьте в нее пользователей: den и alex
		2. группу jun-sec, добавьте в нее пользователей: alex и serg и admin
	2. Введите компьютер PC-RND в домен, обеспечьте возможность входа под всеми доменными учетными записями на данный ПК.
	3. Создайте правило, разрешающее доменному пользователю admin использовать sudo на всех компьютерах в домене без ограничения.
	4. Обеспечьте доменному пользователю admin, после успешной авторизации на компьютере PC-RND, возможность заходить в интерфейс FreeIPA без использования пароля. Для аутентификации и авторизации используйте Kerberos.
6. Настройте инфраструктуру разрешения имен в филиалах следующим образом:
	1. DNS-сервер в филиале RND располагается на DC-RND и интегрирован с доменом FreeIPA.
	2. DNS-сервер в филиале KRD располагается на FW-KRD.
	3. Все устройства в локальных сетях должны обращаться с DNS запросами к DNS-серверам соответствующих филиалов. Исключение допустимо только для гостевых сетей, при наличии технической необходимости.
	4. Указанные DNS-сервера должны выполнять пересылку “внешних” DNS запросов от локальных клиентов на DNS сервер провайдера, указанный в Схеме IP-адресации.
	5. CLIENT-EXT должен обращаться с DNS запросами на сервер провайдера, указанный в Схеме IP-адресации.
	6. Настройте для всех устройств филиалов доменные имена в зонах rnd.jun.profi и krd.jun.profi в соответствии с их расположением.
	7. Все устройства должны быть доступны в локальных сетях всех филиалов по именам в соответствии с топологией в доменах соответствующих филиалов. К примеру srv-krd.krd.jun.profi или pc-rnd.rnd.jun.profi
	8. В рамках каждого филиала короткие имена должны автоматически дополняться доменным именем соответствующего филиала.
	9. Создайте обратную зону(ы) DNS в доменном DNS-сервере DC-RND, чтобы все ip-адреса в филиале RND расшифровывались в соответствующие им DNS-имена.
7. Настройте DHCP-сервера:
	1. на FW-KRD для клиентов сети LAN-KRD
	2. на DC-RND для клиентов сетей LAN-RND и GST-RND
	3. DHCP-сервера должны передавать клиентам все необходимые опции для работы в сети и взаимодействия с другими устройствами и сетями по IP и DNS именам.
	4. Выдаваемые по DHCP адреса не должны пересекаться с зарезервированными, служебными и прочими “занятыми” адресами, необходимыми для выполнения задания.
	5. DHCP-сервера должны работать на основе ПО “Kea DHCP server”
8. Настройте синхронизацию времени:
	1. Сервер точного времени в филиале RND располагается на DC-RND.
	2. Сервер точного времени в филиале KRD располагается на FW-KRD.
	3. Все устройства в локальных сетях должны использовать указанные сервера.
	4. Все сервера и клиенты, которые поддерживают Chrony должны использовать данную реализацию протокола. На устройствах, которые не поддерживают Chrony допускается использовать стандартный NTP.
	5. Указанные сервера времени, а также сервера и клиенты во внешних сетях должны синхронизировать свое время с NTP сервером, указанным в схеме IP-адресации.
	6. Настройте часовой пояс на всех устройствах в соответствии с их географическим расположением. Для машины CLIENT-EXT используйте часовой пояс Москвы.
9. Настройте защищенный VPN-туннель FW-RND<=>FW-KRD со следующими параметрами:
	1. Технология VPN на ваш выбор: IPsec, OpenVPN, WireGuard.
	2. Используйте современные надежные протоколы шифрования AES, SHA-2 или ChaCha20.
	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 подвергался трансляции адресов и не блокировался. На текущем этапе все устройства в локальных сетях филиалов должны иметь возможность взаимодействовать между собой без ограничений, кроме сегментов и устройств, для которых в задании явно указано иное.
10. Настройте OSPFv2 по защищенному туннелю между FW-RND и FW-KRD так, чтобы FW\* имели полную информацию о маршрутах во все локальные сети всех филиалов.
	1. FW\* должны быть защищены от вброса маршрутов с любых интерфейсов, кроме тех, на которых обмен маршрутами явно требуется.
	2. ⚠ В таблицах маршрутизации могут содержаться дополнительные резервные маршруты, но именно OSPF-маршруты должны быть “выбраны” системой маршрутизации.
11. Обеспечьте авторизацию пользователей в гостевой сети GST-RND через captive portal.
	1. Для авторизации используйте локального пользователя FW-RND с именем guest.
	2. Доступ к сетевым ресурсам должен появляться только после авторизации.
	3. Пользователи данной сети должны иметь доступ в интернет и не иметь доступа к локальным ресурсам, кроме необходимых для выполнения задания.
	4. Для удобства пользователя создайте на рабочем столе ярлык на открытие страницы captive portal.

**Часть 2 (2-й день - 4 часа)**

1. Настройте правила межсетевого экранирования для взаимодействия между филиалами через VPN-туннель:
	1. Клиентские рабочие места должны иметь возможность обращаться к серверам в другом филиале по стандартным портам протоколов http и https.
	2. Сервера должны иметь возможность обращаться к серверам и клиентам другого филиала без ограничений.
	3. Все устройства в локальных сетях филиалов должны иметь возможность отправлять друг друг ping-сообщения, кроме тех случаев, когда в задании явно указано иное.
	4. Все остальные взаимодействия между устройствами в разных филиалах должны быть запрещены.
	5. ⚠ Данный раздел не распространяется на гостевые сети, они должны продолжать функционировать так, как указано в соответствующих гостевым сетям пунктах задания.
	6. ⚠ Допускается открывать конкретные дополнительные порты, необходимые для выполнения задания.
	7. ⚠ При настройке межсетевого экранирования учитывайте, что правила должны распространяться на сети, а не на конкретные устройства, при этом по политике организации нахождение в одной сети одновременно клиентов и серверов недопустимо.
2. Для хранения важных данных в сервер SRV-KRD установлено два дополнительных диска. Объедините их в зеркальный отказоустойчивый массив используя технологию md raid. На полученном резервированном носителе создайте файловую систему XFS и подключите раздел по пути /opt/data/ для дальнейшего использования.
3. На сервере SRV-KRD должен быть развернут WEB-сервер корпоративного портала организации:
	1. При развертывании портала не используйте технологии контейнеризации
	2. Файлы сайта должны располагаться в директории /opt/data/
	3. Сайт должен работать на адресе corp.jun.profi на стандартном HTTP-порте
	4. Обеспечьте наличие на главной странице текста “Добро пожаловать на корпоративный портал компании Destination Reachable” и логотипа чемпионатного движения “Профессионалы”, при этом логотип требуется сохранить на сервере Портала, вставка по ссылке недопустима.
	5. При обращении к серверу по ip-адресу или любому другому DNS-имени, кроме адреса корп.портала, сервер должен выдавать ошибку 404.
	6. Для работоспособности портала из внешнего мира, внесите необходимые данные через веб-интерфейс DNS-провайдера.
4. Настройте права доступа для каталога /opt/data на SRV-KRD следующим образом:
	1. пользователь webdev (его требуется создать) должен иметь полные права на чтение и запись в указанный каталог и все его подкаталоги.
	2. обычные пользователи не должны иметь доступа в данный каталог
	3. службы настроенного ранее веб-сервера должны иметь минимально-необходимые права для работы сайта.
	4. ⚠ При назначении прав учитывайте, что для папки задача обеспечить “чтение” подразумевает также возможность перечисления содержимого папки и возможность зайти в эту директорию с помощью команды cd.
5. Обеспечьте возможность подключения к FW-KRD под пользователем fwadm:
	1. посредством веб-интерфейса с полным доступом к настройкам;
	2. посредством протокола SSH с доступом к выполнению команд через sudo;
	3. при подключении с компьютера PC-KRD авторизация SSH должна осуществляться по ключу без необходимости ввода пароля.
	4. Парольный доступ по SSH должен быть запрещен.
6. Настроить удаленный доступ к SRV-KRD по SSH
	1. На сервере SRV-KRD сервис SSH должен функционировать на порте 2202
	2. Устройство PC-KRD при входе под пользователем user должно иметь доступ к SRV-KRD под пользователем user c использованием SSH ключей, без необходимости ввода пароля.
	3. Пользователь user на SRV-KRD должен иметь возможность выполнять команды через sudo без ввода пароля.
	4. Подключение к SRV-KRD с PC-KRD из под пользователя user должно осуществляться командой “ssh SRV” без дополнительных параметров.
7. На сервере SRV-KRD разверните сервер мониторинга и настройте его следующим образом:
	1. При развертывании не используйте технологии контейнеризации
	2. Сервер: Zabbix LTS
	3. База данных: PostgreSQL
	4. Веб-интерфейс: на основе Nginx
	5. Основной адрес: mon.jun.profi
	6. Порт веб-интерфейса: 80(HTTP)\*
	7. Подключите к серверу мониторинга все устройства организации
	8. Обеспечьте сбор показателей со всех подключенных устройств с помощью стандартных шаблонов используемых ОС
	9. ⚠ Подключение устройств в гостевых и внешних сетях не требуется
	10. ⚠ \*Обратите внимание, что на сервере также располагается сайт корпоративного портала. Оба сервиса должны работать на порту 80 на соответствующих именах. В крайнем случае, Zabbix допускается запустить на порте 8080 с потерей части баллов.

**Модуль Г: Обеспечение отказоустойчивости (3-й день, 4 часа)**

Для бесперебойного функционирования корпоративной инфраструктуры, а также качественного предоставления сервиса внешним клиентам, руководство приняло решение организовать отказоустойчивый кластер высокой доступности и разместить в нем систему Helpdesk.

Оборудование уже подключено, операционные системы установлены.

⚠ Компьютер CLIENT-EXT не подразумевает внесения дополнительных настроек, помимо IP-адресации и DNS-параметров и используется только для проверки доступности сервисов Компании из внешних сетей.

**Операционные системы:**

|  |  |  |  |
| --- | --- | --- | --- |
| **ВМ** | **ОС** | **Ресурсы (примерно)** | **GUI** |
| ISP | - | 0.5Gb; 1CPU | - |
| CL-GW1 | OPNsense 24.7 | 1Gb; 1CPU | - |
| CL-GW2 | OPNsense 24.7 | 1Gb; 1CPU | - |
| CL-FRONT1 | Alt Server 10.4 | 1Gb; 1CPU | - |
| CL-FRONT2 | Alt Server 10.4 | 1Gb; 1CPU | - |
| CL-BACK | Alt Server 10.4 | 1Gb; 1CPU | - |
| MGMT-PC | Alt Workstation 10.4 | 1Gb; 1CPU | MATE |
| CLIENT-EXT | Alt Workstation 10.4 | 1Gb; 1CPU | MATE |

**Схема IP-адресации и схема подключений.**

Схема адресации локальных сетей в задании разрабатывается участниками, однако требуется придерживаться следующих условий:

1. Для локальных сетей используется только приватная адресация из стандартных приватных диапазонов.
2. Все сети, соединяющие маршрутизаторы между собой, включая сети туннелей site-to-site должны иметь маску сети /30 или /29 (там где необходимо).
3. Все остальные локальные сети, включая клиентские VPN-сети, должны иметь адресацию с маской /24. При этом шлюзом по умолчанию в таких сетях должен быть первый или последний адрес в сети, после принятия решения по адресации шлюзов по умолчанию, используйте аналогичные (только первые или только последние) адреса для шлюзов во всей инфраструктуре.
4. При выполнении задания впишите адреса выданные устройствам в столбец “Адрес/Маска” рядом со словом “STATIC”

|  |  |  |  |
| --- | --- | --- | --- |
| Сеть  | Устройство  | Адрес/Маска  | Шлюз |
| INTERNET | Client-EXT | 100.108.128.45/28 | ISP – первый адрес в сети |
|  | DNS-сервер  | 100.100.100.100 |  |
|  | NTP-сервер | 100.101.102.103 |  |
| CL-WAN | <СЕТЬ> | 100.99.90.96/28 |  |
|  | ISP | первый адрес в сети |  |
|  | CL-GW1 | STATIC | ISP |
|  | CL-GW2 | STATIC | ISP |
|   | CL-GW(VIP) | STATIC | ISP |
| CL-LAN | CL-CL-GW1 | STATIC |   |
|   | CL-GW2 | STATIC |  |
|  | CL-GW(VIP) | STATIC |  |
|  | CL-FRONT1 | STATIC | CL-GW |
|  | CL-FRONT2 | STATIC | CL-GW |
|  | CL-FRONT(VIP) | STATIC | CL-GW |
|  | CL-BACK | STATIC | CL-GW |
|  | MGMT-PC | DHCP | CL-GW |
| SYNC | CL-GW1 | STATIC |  |
|  | CL-GW2 | STATIC |  |

**Схема сети приведена в отдельном файле!**

1. Настройка DNS в соответствии с таблицей
	1. Настройте DNS-сервер на межсетевых экранах CL-GW1 и CL-GW2
	2. Для работоспособности портала из внешнего мира, внесите необходимые данные через веб-интерфейс DNS-провайдера.

|  |  |  |  |
| --- | --- | --- | --- |
| Устройства | тип | имя | адрес |
| CL-GW(CL-GW1 и CL-GW2) | А | helpdesk.jun.profi | CL-FRONT(VIP) |
| DNS-провайдер ns.ext | A | helpdesk.jun.profi | CL-GW (WAN VIP) |

1. Настройка отказоустойчивого кластера маршрутизации
	1. Обеспечьте наличие доступа в интернет со всех устройств в сети CL-LAN
	2. Настройте CARP на CL-GW1 как основной сервер и GW2 как подчинённый сервер
	3. Назначьте номер группы 1 для внешнего интерфейса и номер группы 2 для внутреннего
	4. Проверьте, что при отключении CL-GW1 доступ к сети WAN сохраняется через CL-GW2
	5. Убедитесь, что внешний и внутренний адреса переключаются на CL-GW2 при сбое
	6. Проверьте, что при включении CL-GW1 он восстанавливает свои адреса и повторно становится основным
	7. Обеспечьте автоматизированную репликацию конфигурации и состояний CL-GW1 на CL-GW2 посредством pfSync и XMLRPC-sync
	8. Настройте дополнительные параметры для обеспечения корректной работы кластера маршрутизации
2. Настройка кластера DHCP
	1. Настройте DHCP-сервер на CL-GW1 как основной
	2. Настройте DHCP-сервер на CL-GW2 как запасной
	3. Настройте механизм DHCP failover между CL-GW1 и CL-GW2
	4. Обеспечьте синхронизацию данных между основным и запасным серверами
	5. Настройте CL-GW2 для выдачи IP-адресов в случае сбоя CL-GW1
	6. Проверьте работоспособность кластера при отключении CL-GW1
	7. Убедитесь в корректной работе DHCP на обоих шлюзах после перезагрузки
	8. В качестве DHCP-сервера используйте программную реализацию Kea
3. Перенаправление внешнего порта
	1. Настройте перенаправление трафика с внешнего порта 80 на внутренний порт 80, в общий ip-адрес CL-FRONT1 и CL-FRONT2
	2. Убедитесь, что все запросы корректно обрабатываются на целевом адресе
4. Установка и настройка контейнера на сервере CL-BACK
	1. На сервере CL-BACK разверните сервер системы HelpDesk при помощи технологии контейнеризации docker. Необходимые файлы контейнера разместите в директории /opt/zammad/
	2. Приложение: Helpdesk система Zammad
	3. Порт Helpdesk - 9090
	4. База данных - postgresql
	5. Обеспечьте автоматический запуск контейнера
	6. Обеспечьте работоспособность сервера helpdesk и возможность входа под пользователем hdadmin@jun.profi с паролем "P@ssw0rdP@ssw0rd"
	7. Создайте в системе заявку от пользователя junuser@jun.profi, в теме заявки укажите - "трассировка", к заявке прикрепите снимок экрана трассировки маршрута от компьютера CLIENT-EXT до хоста helpdesk.jun.profi
5. Настройка веб служб на серверах CL-FRONT1 и CL-FRONT2
	1. Настройте программное обеспечение nginx на CL-FRONT1 и CL-FRONT2 как обратный прокси для приложения Zammad на CL-BACK
	2. Настройте nginx на порт 80, убедитесь что порт доступен из внешней сети
	3. При обращении по доменному имени helpdesk.jun.profi из внешних сетей или с MGMT-PC происходит обратное проксирование на CL-BACK в порт 9090
	4. При обращении по ip загружается локальная страница-заглушка с идентификацией сервера, на странице размером <h1> написано имя хоста, отдавшего страницу
6. Настройка отказоустойчивости веб служб
	1. Создайте группу серверов keepalived со следующими параметрами:
	2. Иерархия группы - CL-FRONT1 -> CL-FRONT2
	3. Идентификатор группы – 80
	4. Приоритет - 110 и 100 соответственно
	5. Виртуальный адрес группы - CL-FRONT(VIP)
	6. Интервал рассылки сообщений - 3 секунды
	7. Время, после которого сервер с более высоким приоритетом заберет обратно себе роль мастера – 30 секунд
	8. Настройте keepalived таким образом, чтобы при отключении службы nginx на CL-FRONT1 общий ip адрес передавался CL-FRONT2, при включении общий ip адрес снова возвращался CL-FRONT1
7. Настройка доступа к контейнеру на сервере CL-BACK
	1. Настройте межсетевой экран для ограничения доступа к порту 9090 только для серверов CL-FRONT1 и CL-FRONT2
	2. Убедитесь, что другие источники не могут подключаться к указанным портам

2. СПЕЦИАЛЬНЫЕ ПРАВИЛА КОМПЕТЕНЦИИ

1. Участникам при выполнении всех модулей можно использовать интернет-ресурсы, за исключением:

– Систем контроля версий

– Общения посредством форумов/мессенджеров/иных средств коммуникации – видеохостингов

2. Участники имеют право задавать уточняющие вопросы экспертам (кроме эксперта наставника) и вправе получить ответ, если вопрос не предполагает получения информации о реализации конкретной технологии

2.1. Личный инструмент конкурсанта

Нулевой - нельзя ничего привозить.

2.2.Материалы, оборудование и инструменты, запрещенные на площадке

Мобильные устройства, устройства фото-видео фиксации, носители информации.

3. Приложения

Приложение 1. Инструкция по заполнению матрицы конкурсного задания

Приложение 2. Матрица конкурсного задания

Приложение 3. Инструкция по охране труда

Приложение 4. Чертежи, технологические карты, алгоритмы, схемы