****

КОНКУРСНОЕ ЗАДАНИЕ КОМПЕТЕНЦИИ

«Сетевое и системное администрирование»

*Юниоры*

Итоговый (межрегиональный) этап Чемпионата

по профессиональному мастерству «Профессионалы»

Калужская область, Калуга Технопарк

регион проведения

2024 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 2](#_Toc142037183)

[1.1. Общие сведения о требованиях компетенции 2](#_Toc142037184)

[1.2. Перечень профессиональных задач специалиста по компетенции «Сетевое и системное администрирование» 2](#_Toc142037185)

[1.3. Требования к схеме оценки 7](#_Toc142037186)

[1.4. Спецификация оценки компетенции 7](#_Toc142037187)

[1.5. Конкурсное задание 8](#_Toc142037188)

[1.5.1. Разработка/выбор конкурсного задания 8](#_Toc142037189)

[1.5.2. Структура модулей конкурсного задания (инвариант/вариатив) 8](#_Toc142037190)

[2. СПЕЦИАЛЬНЫЕ ПРАВИЛА КОМПЕТЕНЦИИ 20](#_Toc142037191)

[2.1. Личный инструмент конкурсанта 20](#_Toc142037192)

[2.2.Материалы, оборудование и инструменты, запрещенные на площадке 20](#_Toc142037193)

[3. ПРИЛОЖЕНИЯ 20](#_Toc142037194)

**ИСПОЛЬЗУЕМЫЕ СОКРАЩЕНИЯ**

1. ФГОС – Федеральный государственный образовательный стандарт
2. ПС – Профессиональный стандарт
3. КЗ – Конкурсное задание
4. ИЛ – Инфраструктурный лист

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 (Юниоры)»

*Таблица №1*

**Перечень профессиональных задач специалиста**

|  |  |  |
| --- | --- | --- |
| **№ п/п** | **Раздел** | **Важность в %** |
| **1** | Выполнение работ по выявлению и устранению инцидентов в информационно-коммуникационных системах | **30** |
| - Специалист должен знать и понимать:  Лицензионные требования по настройке и эксплуатации устанавливаемого программного обеспечения  Основы архитектуры, устройства и функционирования вычислительных систем  Принципы организации, состав и схемы работы операционных систем  Стандарты информационного взаимодействия систем  Регламенты проведения профилактических работ на администрируемой информационно-коммуникационной системе  Инструкции по установке администрируемых сетевых устройств  Инструкции по эксплуатации администрируемых сетевых устройств  Инструкции по установке администрируемого программного обеспечения  Инструкции по эксплуатации администрируемого программного обеспечения  Требования 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 установки  Оценивать степень критичности инцидентов при работе прикладного программного обеспечения  Устранять возникающие инциденты  Локализовать отказ и инициировать корректирующие действия  Пользоваться нормативно-технической документацией в области инфокоммуникационных технологий  Производить мониторинг администрируемой информационно-коммуникационной системы  Конфигурировать операционные системы сетевых устройств  Пользоваться контрольно-измерительными приборами и аппаратурой  Документировать учетную информацию об использовании сетевых ресурсов согласно утвержденному графику |
| **2** | Обеспечение работы технических и программных средств информационно-коммуникационных систем | **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; |
| **3** | Реализация схемы резервного копирования, архивирования и восстановления конфигураций технических и программных средств информационно-коммуникационных систем по утвержденным планам | **20** |
| - 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** |  | **А** | **Б** | **В** |  |
| **1** | 30 | 0 | 0 | **30** |
| **2** | 0 | 14,1 | 10,9 | **25** |
| **3** | 0 | 11,5 | 8,5 | **20** |
| **4** | 0 | 9,4 | 15,6 | **25** |
| **Итого баллов за критерий/модуль** | | **30** | **35** | **35** | **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** |
| **А** | **Аудит** | В соответствии с используемыми ОС и Сетевым оборудованием |
| **Б** | **Настройка технических и программных средств информационно-коммуникационных систем** | В соответствии с используемыми ОС и Сетевым оборудованием |
| **В** | **Обеспечение отказоустойчивости** | В соответствии с используемыми ОС и Сетевым оборудованием |

1.5. КОНКУРСНОЕ ЗАДАНИЕ

Общая продолжительность Конкурсного задания[[1]](#footnote-1): 12 ч.

Количество конкурсных дней: 3 дня

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.

1.5.1. Разработка/выбор конкурсного задания

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

1.5.2. Структура модулей конкурсного задания

**Модуль А. *Аудит*. (Инвариант)**

*Время на выполнение модуля 4 часа*

**Задания:**

Вам предложено 15 заявок от пользователей в техническую поддержку, накопившиеся за определенное время. При этом, заведомо известно, что в какой-то момент все работало идеально, однако потом вышло из строя в силу технического сбоя или было повреждено некорректными действиями пользователя или технического персонала.

1. Потерян доступ к веб-интерфейсу FW-X
2. Клиенты из сети X потеряли доступ в интернет
3. Компьютеры в филиале A не могут обращаться по именам к компьютерам в домене
4. Сотрудник за PC-X не может обратиться на сервер Y по внутреннему адресу
5. Сервер Приложения на устройстве APP-L не работает, хотя контейнер запущен.
6. На VDS было два пользователя: user1 и user2. Но при попытке зайти на машину, используя эти два логина ничего не получалось. Файлы и группы пользователей должны быть сохранены.
7. Сотрудник, работающий из дома, не может подключиться к серверам во внутренней инфраструктуре организации.
8. Корпоративный портал открывается с ошибкой сертификата.
9. Не открывается корпоративный портал из сети Интернет
10. Пользователь на NB-Y не может обратиться к сайту <имя-сайта>
11. Пользователь vasya на компьютере PC-Z не может записывать файлы в примонтированную сетевую директорию
12. На сервер логирования не приходят события с сервера K
13. При подключении по FTP пользователь admin не может записывать файлы, хотя ему нужна такая возможность для обслуживание корпоративного портала организации.
14. Устройства в филиале X перестали синхронизировать время с сервером времени этого филиала.
15. Пользователь user на ClientTVR не может установить программу командой sudo apt-get install gimp. Обеспечьте пользователю возможность устанавливать приложения из штатных репозиториев ОС.

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

*Время на выполнение модуля 4 часа.*

**Задания:**

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 интерфейсы loopback на всех FW\* и R\*. Обеспечьте возможность обращаться к этим адресам из всех сетей, если в задании явно не указано иного.
3. Настройте имена всех устройств согласно топологии.
4. Все устройства должны иметь доступ в интернет, если в задании явно не указано иного.
5. Соберите отказоустойчивый vrrp-кластер с условным обозначением R1-KLG из устройств R2-KLG и R3-KLG.
   1. Все устройства должны иметь межсетевую связность в соответствии с другими пунктами данного технического задания, если хотя бы один из роутеров кластера запущен.
   2. При отказе одного из роутеров в кластере, а также при возвращении отказавшего роутера в кластер, межсетевая связность должна восстанавливаться не более чем за 60 секунд.
   3. По умолчанию основным (MASTER) устройством должен быть R2-KLG и если он работает, то весь трафик должен проходить через него.
   4. Информация о интерфейсах, в том числе номера VLAN представлены на схеме сети.
   5. При необходимости, можно дополнительно использовать vlan 2001 для взаимодействия между R2-KLG и R3-KLG.
   6. \* если Вы не готовы собирать отказоустойчивый кластер - то вы можете использовать R2-KLG как самостоятельное устройство и все межсетевые настройки делать только на нем. Однако учитывайте, что Заказчик будет этим недоволен и лишит Вас премии (всех баллов за отказоустойчивый vrrp-кластер), однако примет все остальные задачи, которые выполнены в соответствии с заданием.
6. Настройте OSPFv2 между R1-KLG и FW-KLG
   1. FW-KLG должен узнавать о сетях, подключенных к R1-KLG, через OSPF, при этом если R2-KLG
   2. R1-KLG должен получать маршрут по умолчанию и другие необходимые маршруты от FW-KLG через OSPF.
   3. В таблице маршрутизации могут содержаться дополнительные резервные маршруты, но именно OSPF-маршруты должны быть “выбраны” системой маршрутизации.
   4. Маршруты до loopback интерфейсов также должны распространяться по OSPF.
   5. R1-KLG должен быть защищен от вброса маршрутов с любых интерфейсов, кроме тех, на которых обмен маршрутами явно требуется.
7. В филиале KLG разверните домен klg.jun.profi на базе FreeIPA с контроллером домена на сервере SRV-KLG c центром сертификации (далее - корпоративный центр сертификации). При развертывании учтите, что это устройство будет выполнять функции DNS и DHCP сервера в филиале KLG.
   1. CN корневого сертификата “JUN PROFI CA”; страна “RU”.
   2. Создайте пользователей den и alex, поместите их в группу jun-users
   3. Введите компьютер PC-KLG в домен, обеспечьте возможность входа под всеми доменными учетными записями на данный ПК.
   4. Создайте правило, разрешающее доменному пользователю alex использовать sudo на всех компьютерах в домене без ограничения.
   5. Обеспечьте доменному пользователю admin, после успешной авторизации на компьютере PC-KLG, возможность заходить в интерфейс FreeIPA без использования пароля. Для аутентификации и авторизации используйте Kerberos.
8. Настройте инфраструктуру разрешения имен в филиалах следующим образом:
   1. DNS-сервер в филиале KLG располагается на SRV-KLG и интегрирован с доменом FreeIPA.
   2. DNS-сервер в филиале RZN располагается на FW-RZN.
   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 DNS запросов от локальных клиентов на DNS сервер провайдера, указанный в Схеме IP-адресации.
   5. Client\* и VDS должны обращаться с DNS запросами на сервер провайдера, указанный в Схеме IP-адресации.
   6. Настройте для всех устройств филиалов в Красноярске и Владивостоке доменные имена в зонах rzn.jun.profi и klg.jun.profi соответственно.
   7. Все устройства должны быть доступны в локальных сетях всех филиалов по именам в соответствии с топологией в доменах соответствующих филиалов. К примеру srv-rzn.rzn.jun.profi или pc-klg.klg.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 SRV-KLG, чтобы все ip-адреса в филиале KLG расшифровывались в соответствующие им DNS-имена.
9. Настройте DHCP-сервер на FW-RZN для клиентов сети LAN-RZN, а также на SRV-KLG для клиентов сетей LAN-KLG и SEC-KLG. DHCP-сервер должен передавать клиентам все необходимые опции для работы в сети и взаимодействия с другими устройствами и сетями по IP и DNS именам.
   1. Выдаваемый диапазон адресов должен оставлять свободными ровно 10 адресов в начале сети, зарезервированных для дальнейшего использования, все остальные адреса должны предназначаться для выдачи клиентам по DHCP.
   2. DHCP-сервера должны работать на основе ПО “Kea DHCP server”
   3. Настройте необходимые параметры на R1-KLG таким образом, чтобы клиенты PC-KLG и ARM-KLG получали адреса по DHCP.
10. Настройте синхронизацию времени
    1. Сервер точного времени в филиале KLG располагается на SRV-KLG.
    2. Сервер точного времени в филиале RZN располагается на FW-RZN.
    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 по адресу 100.101.102.103.
    6. Настройте часовой пояс на всех устройствах в соответствии с их географическим расположением. Для машины VDS используйте часовой пояс Калуги.
11. Настройте правила межсетевого экранирования для сети DMZ-KLG:
    1. Устройства в сетях DMZ-\* не должны иметь возможности инициировать соединения к устройствам в приватных сетях организации, при этом входящие соединения из всех остальных локальных сетей в сети DMZ-\* должны быть разрешены.
    2. Устройства в сетях DMZ-\* не должны иметь доступа к интернету, за исключением полного IPv4 доступа к серверу VDS, и официальных репозиториев ОС для установки и обновления пакетов.
    3. При необходимости, допускается возможность открывать конкретные дополнительные порты, необходимые для выполнения задания.
12. Настройте защищенный VPN-туннель FW-KLG<=>FW-RZN 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
13. Настройте работу OSPF между R\* и FW\*, чтобы все маршрутизаторы имели полную информацию о маршрутах во все локальные сети всех филиалов.
14. Обеспечьте авторизацию пользователей сети GST-RZN через captive portal.
    1. Для авторизации используйте локального пользователя FW-RZN 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.

**Модуль В. *Обеспечение отказоустойчивости*. (Вариатив)**

*Время на выполнение модуля 4 часа*.

**Задания:**

1. Обеспечьте подключение клиента ClientTVR к серверу VPN на FW-KLG.
   1. Технология VPN на ваш выбор: IPsec, OpenVPN, WireGuard.
   2. Клиент должен иметь доступ к серверам в сети SRV-KLG и DMZ-KLG.
   3. Соединение должно автоматически устанавливаться при включении компьютера или входе под пользователем user.
2. Для хранения важных данных в сервер VDS 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/cms/data/ для дальнейшего использования.
3. На сервере VDS должен быть развернут WEB-сервер корпоративного портала организации:
   1. При развертывании корпоративного портала не используйте технологии контейнеризации
   2. Для портала разверните на веб-сервере CMS Joomla актуальной стабильной версии
   3. В качестве базы данных используйте Postgresql.
      1. Подключение CMS к базе данных должно осуществляться под отдельным пользователем cms, с доступом только к базе данных с именем cms
   4. Веб интерфейс БД: PgAdmin, порт интерфейса 8080
      1. Подключите PgAdmin к созданному серверу БД с полным административным доступом под пользователем pgadm@jun.profi
   5. Файлы сайта должны располагаться в директории /opt/cms/data
   6. Сайт должен открываться по адресу corp.jun.profi
   7. Обращение к сайту из внутренних сетей организации должно происходить только по внутренним каналам связи, однако сайт должен также быть доступен и внешним клиентам по тому же адресу.
   8. Для работоспособности портала из внешнего мира, передайте необходимые настройки хостинг-провайдеру DNS.
   9. При необходимости, допускается использовать дополнительные компоненты, необходимые для выполнения задания, однако все они должны функционировать в контейнерной среде.
   10. Обеспечьте наличие на главной странице текста “Добро пожаловать на корпоративный портал ЗАО Калуга СетСервТрансМаш” и логотипа чемпионатного движения “Профессионалы”, при этом логотип требуется сохранить на сервере Портала, вставка по ссылке недопустима.
   11. Сайт должен функционировать по протоколу HTTPS. При обращении по протоколу HTTP должен происходить автоматический редирект на HTTPS.
   12. WEB-сервер должен иметь сертификат, подписанный корпоративным центром сертификации
   13. Сайт должен открываться с PC-KLG и PC-RZN без ошибок и предупреждений.
   14. При обращении к серверу по ip-адресу или любому другому DNS-имени, кроме адреса корп.портала, сервер должен выдавать ошибку 404.
4. Создайте пользователя webdev на VDS, и добавьте его в группу ftpusers.
5. Настройте права доступа для каталога /opt/cms/data на VDS следующим образом:
   1. пользователь webdev 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 необходимые права для работы сайта, при этом права на запись допустимы только в те папки, в которые это явно требуется.
6. Настройте общий доступ к файлам на VDS по протоколу FTP.
   1. Доступ должен быть только у пользователя webdev.
   2. FTP-сервер должен предоставлять доступ только к содержимому папки /opt/cms/data и вложенных в нее папок.
7. Настройте клиент FTP на Client-TVR.
   1. Установите ПО Filezilla актуальной стабильной версии и проверьте возможность подключения к корпоративному FTP-серверу. Для удобства, создайте ярлык Filezilla на рабочем столе
   2. Под пользователем user в установленном клиенте сделайте закладку “Corp portal data” с подключением к созданному FTP-серверу и заполненными сигнатурами доступа
8. Обеспечьте веб-интерфейс FW-RZN сертификатом HTTPS, подписанным корпоративным центром сертификации, обеспечивающим доверенное соединение при обращении к FW-RZN по полному и сокращенному DNS-имени и IP-адресу loopback с PC-RZN.
9. Обеспечьте возможность подключения к FW-RZN 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-RZN авторизация SSH должна осуществляться по ключу без необходимости ввода пароля.
10. Настроить удаленный доступ к VDS по SSH
    1. На сервере VDS сервис SSH должен функционировать на порте 2202
    2. Устройство PC-KLG при входе под пользователем user должно иметь доступ к VDS под пользователем user c использованием SSH ключей, без необходимости ввода пароля.
    3. Пользователь user на VDS должен иметь возможность выполнять команды через sudo без ввода пароля.
    4. Подключение к VDS с PC-KLG должно осуществляться командой “ssh VDS” без дополнительных параметров.
11. На сервере APP-KLG разверните сервер облачного хранения данных:
    1. При развертывании используйте технологии контейнеризации
    2. Файловый сервер: NextCloud
    3. База данных: PostgreSQL
    4. Порт NextCloud: 80
    5. Обеспечьте работоспособность сервера NextCloud и возможность входа под пользователем user с паролем "jun.profi\_pass".
    6. Обеспечьте работоспособность сервера по адресу cloud.jun.profi в локальных сетях и для внешних клиентов.
12. Обеспечьте подключение удаленного сотрудника с компьютера ClientTVR к корпоративному порталу https://cloud.jun.profi следующим образом:
    * 1. посредством VPN-подключения, когда оно активно.
      2. посредством доступа по внешнему адресу, когда vpn-соединение неактивно.
13. На сервере SRV-RZN разверните сервер мониторинга и настройте его следующим образом:
    1. При развертывании не используйте технологии контейнеризации
    2. Сервер: Zabbix LTS
    3. Веб-интерфейс: на основе Nginx
    4. Основной адрес: mon.jun.profi
    5. Порт веб-интерфейса: 80(HTTP), 443(HTTPS)
    6. Автоматическая переадресация на безопасный протокол
    7. Сертификат подписан корпоративным ЦС
    8. Сайт открывается с PC-NVR без ошибок и предупреждений безопасности.
    9. Добавьте на сервер мониторинга все устройства филиала RZN и сервер VDS
    10. Обеспечьте сбор показателей со всех подключенных устройств с помощью стандартных шаблонов используемых ОС

2. СПЕЦИАЛЬНЫЕ ПРАВИЛА КОМПЕТЕНЦИИ*[[2]](#footnote-2)*

* + - 1. Участникам при выполнении всех модулей можно использовать интернет-ресурсы, за исключением:
* Систем контроля версий
* Общения посредством форумов/мессенджеров/иных средств коммуникации – Видеохостингов
  + - 1. 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 и т.д.

1. *Указывается суммарное время на выполнение всех модулей КЗ одним конкурсантом.* [↑](#footnote-ref-1)
2. *Указываются особенности компетенции, которые относятся ко всем возрастным категориям и чемпионатным линейкам без исключения.* [↑](#footnote-ref-2)