Согласовано

ООО «Инвест ИТ»

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_/\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_/

 (подпись) (расшифровка)

«\_\_\_\_\_\_» \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ 2023 г.

Утверждено

Главный эксперт компетенции «Сетевое и системное администрирование»

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_/ Топильский А.В. /

«\_\_\_\_\_\_» \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ 2023 г.

КОНКУРСНОЕ ЗАДАНИЕ КОМПЕТЕНЦИИ

«СЕТЕВОЕ И СИСТЕМНОЕ АДМИНИСТРИРОВАНИЕ»

2023 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 3](#_30j0zll)

[1.1. ОБЩИЕ СВЕДЕНИЯ О ТРЕБОВАНИЯХ КОМПЕТЕНЦИИ 3](#_1fob9te)

[1.2. ПЕРЕЧЕНЬ ПРОФЕССИОНАЛЬНЫХ ЗАДАЧ СПЕЦИАЛИСТА ПО КОМПЕТЕНЦИИ «Сетевое и системное администрирование» 3](#_2et92p0)

[1.3. ТРЕБОВАНИЯ К СХЕМЕ ОЦЕНКИ 9](#_kyxgng2spsaw)

[1.4. СПЕЦИФИКАЦИЯ ОЦЕНКИ КОМПЕТЕНЦИИ 9](#_3dy6vkm)

[1.5. КОНКУРСНОЕ ЗАДАНИЕ 9](#_1gjzjscfqbrt)

[1.5.1. Разработка/выбор конкурсного задания 10](#_w4lz5275v6pi)

[1.5.2. Структура модулей конкурсного задания 10](#_1t3h5sf)

[Модуль А. (Аудит) 10](#_tcb573kyrem9)

[Модуль Б. (Настройка технических и программных средств информационно-коммуникационных систем) 12](#_36j88e2dnqyo)

[Модуль Д. (Автоматизация) 18](#_1fbpe1niy30)

[2. СПЕЦИАЛЬНЫЕ ПРАВИЛА КОМПЕТЕНЦИИ 21](#_4d34og8)

[2.1. Личный инструмент конкурсанта 21](#_2s8eyo1)

[2.2. Материалы, оборудование и инструменты, запрещенные на площадке 21](#_17dp8vu)

[3. ПРИЛОЖЕНИЯ 22](#_3rdcrjn)

**ИСПОЛЬЗУЕМЫЕ СОКРАЩЕНИЯ**

*1. ИКС – Информационно коммуникационная система*

*2. КС – Компьютерная сеть*

*3. 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»

*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; |

***Проверить/соотнести с ФГОС, ПС, Отраслевыми стандартами***

## 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** |  | **A** | **Б** | **Д** |  |
| **1** | 5 | 5 | 10 | 20 |
| **2** | 5 | 5 | 10 | 20 |
| **3** | 10 | 10 | 10 | 30 |
| **4** | 10 | 10 | 10 | 30 |
| **Итого баллов за критерий/модуль** | 30 | 30 | 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** |
| --- | --- |
| **А** | **Аудит** | Определяется регионом в соответствии с используемыми ОС и Сетевым оборудованием |
| **Б** | **Настройка технических и программных средств информационно-коммуникационных систем** | Определяется регионом в соответствии с используемыми ОС и Сетевым оборудованием |
| **Д** | **Автоматизация** | Определяется регионом в соответствии с используемыми ОС и Сетевым оборудованием |

## 1.5. КОНКУРСНОЕ ЗАДАНИЕ

Возрастной ценз: от 16 лет.

Общая продолжительность Конкурсного задания[[1]](#footnote-0): 15 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.

### 1.5.1. 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.

### 1.5.2. Структура модулей конкурсного задания

#### Модуль А. (*Аудит*)

*Время на выполнение модуля 5 часов*.

**Задания:**

Руководство компании *“IT сфера”* столкнулось с рядом проблем после увольнения человека, отвечающего за поддержку инфраструктуры офиса. Было принято решение пригласить Вас, как высококлассного специалиста, для решения возникших вопросов.

Перед Вами поставлены несколько задач, описанных в техническом задании, которые нужно решить за очень короткий промежуток времени. К сожалению, поскольку специалиста в организации не осталось, некоторые из требовании могут звучать не очень внятно. Но вы же высококлассный специалист и, конечно, поймёте о чём идёт речь. Да прибудет с Вами сила!

Предыдущий специалист имел настолько низкую квалификацию, что за всё время обслуживания существующей локальной сети так и не собрал необходимую сетевую документацию. Это стало серьезной проблемой, когда пользователи стали обращаться с жалобами на некачественную работу некоторых сервисов.

**Ваша первая задача** – составить всю необходимую для обслуживания сети документацию. Самостоятельно разработайте формат документации, который будет удобно использовать, примеры оформления представлены в приложении №5. Необходимо собрать следующую информацию об инфраструктуре:

* Схема подключений
* Схема топологии канального уровня
* Схема топологии сетевого уровня
* Таблица адресации
	+ Имя устройства
	+ Тип устройства
	+ Операционная система, версия
	+ Сетевой интерфейс
	+ IP-конфигурация
* Таблица сетевых сервисов
	+ Имя устройства
	+ Название сервиса
	+ Роль в инфраструктуре

Документ сохраните на рабочем столе компьютера администратора с именем *“Документация к инфраструктуре”* в формате **PDF**.

**Ваша вторая задача** - отреагировать на жалобы пользователей, связанные с работой некоторых приложений. Предыдущий администратор с ними уже пообщался и записал результаты опроса в текстовый документ на рабочем столе компьютера администратора с названием “*ОФИСНЫЕ\_ПРОБЛЕМЫ”*. Определите в чём проблемы, запишите первопричину в тот же файл и попытайтесь устранить её.

В выполнении задания есть один серьезный нюанс – Вы работаете удалённо, поэтому физически обнаружить устройства не представляется возможным, а все операции придется выполнять с компьютера администратора.

Реквизиты доступа к компьютеру администратора выданы Вам перед началом работ.

**Спецификация оценки.**

В рамках данного модуля оцениваются навыки аудита имеющейся сетевой инфраструктуры.

Проверка результатов выполнения задания осуществляется оценивающими экспертами сразу по окончании выделенного на модуль времени. В дальнейшем проверка данного модуля осуществляться не будет.

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

*Время на выполнение модуля 5 часов.*

**Задания:**

Умение работать с системами на основе открытого исходного кода становится все более важным навыком для тех, кто желает построить успешную карьеру в Российском ИТ. Данное задание содержит множество задач, основанных на опыте реальной эксплуатации информационных систем, в основном, интеграции и аутсорсинге. Если вы можете выполнить задание с высоким результатом, то вы точно сможете обслуживать информационную инфраструктуру большого предприятия. Все необходимые диаграммы и таблицы представлены в приложении №5.

**Базовая конфигурация**

1. Задайте имена всех машин в соответствии с сетевой диаграммой
2. Настройте IP-адресацию согласно таблице адресации
3. На клиентской машине **OUT-CLI** создайте скрипты для подключения с помощью удаленного доступа:
	1. Подключение к сетям организаций Left и Right выполняется путем выполнения скриптов *connect\_left* и *connect\_right*
	2. Отключение удаленного доступа (к любой организации) должен выполнять скрипт *disconnect\_any*
	3. Все скрипты должны быть расположены в */opt/vpn*
	4. Скрипты должны вызываться из любого каталога простым введением имени скрипта
4. На клиентских машинах обеих организаций создайте скрипты для подключения соответствующих файловых хранилищ:
	1. Монтирование должно осуществляться через вызов скрипта *mount\_share*
	2. Скрипт должен располагается в */opt/scripts* клиентской машины
	3. Скрипт должен вызываться без указания пути
	4. Вызываться должен экземпляр скрипта, находящийся в */opt/scripts*
5. Выполните установку и базовое конфигурирование системы виртуализации Proxmox
	1. Используйте машину **R-PRX**
	2. Установочный образ находится в хранилище ISO на сервере
	3. При установке для суперпользователя используйте пароль P@ssw0rd
	4. В веб интерфейсе отключите надоедливое окно о подписке на платные сервисы

**Конфигурация маршрутизации и виртуальных частных сетей**

1. Настройте GRE-туннель между машинами **L-FW** и **R-FW**:
	1. Используйте следующую адресацию внутри GRE-туннеля:
		1. **L-FW**: 10.5.5.1/30
		2. **R-FW**: 10.5.5.2/30
2. Настройте защиту GRE туннеля между машинами **L-FW** и **R-FW** с помощью технологии IPSEC:
	1. Параметры политики первой фазы IPSec
		1. Проверка целостности SHA-1
		2. Шифрование 3DES
		3. Группа Диффи-Хеллмана — 7
		4. Аутентификация по сертификатам
	2. Параметры преобразования трафика для второй фазы IPSec:
		1. Протокол ESP
		2. Шифрование DES
		3. Проверка целостности SHA-1
	3. В качестве трафика, разрешенного к передаче через IPsec-туннель, должен быть указан только GRE-трафик между машинами машинами **L-FW** и **R-FW**
3. Настройте динамическую маршрутизацию по протоколу OSPF:
	1. Анонсируйте все сети, необходимые для достижения полной связности
	2. Используйте зону с номером 0
	3. Применение статических маршрутов не допускается
	4. В обмене маршрутной информацией участвуют машины **L-RTR-X**, **L-RTR-A**, **L-RTR-B**, **R-RTR**, **L-FW** и **R-FW**
	5. Соседство и обмен маршрутной информацией между машинами **L-FW** и **R-FW** должно осуществляться исключительно через настроенный туннель
4. Настройте удаленный доступ к организациям Left и Right по технологии OpenVPN.
	1. Используйте общие настройки для обеих организаций:
		1. Сгенерируйте необходимую ключевую информацию на сервере **L-SRV**
		2. Используйте TLS шифрование
		3. Используйте сжатие
	2. Для организации Left:
		1. В качестве сервера выступает машина **L-SRV**
		2. Используйте протокол TCP
		3. Тип устройства TAP
		4. Порт 4747
		5. Используйте пул IP-адресов для подключаемых клиентов 10.2.2.0/24
		6. Необходимо обеспечить достижимость службы OpenVPN для внешних клиентов
	3. Для организации Right:
		1. В качестве сервера выступает машина **R-FW**
		2. Используйте протокол UDP
		3. Тип устройства TUN
		4. Порт 4747
		5. Используйте пул IP-адресов для подключаемых клиентов 10.9.8.0/24
	4. Обеспечьте возможность удаленного доступа с машины **OUT-CLI** до сетей организаций Right и Left, ключевая информация должна быть встроена в конфигурационные файлы.

**Конфигурация сетевых сервисов**

1. Настройте службу DHCP на машинах **L-RTR-A**, **R-RTR** в соответствии с требованиями:
	1. Клиентам сетей **L-CLI-A**, **L-CLI-B**, **R-CLI**, **R-SRV** динамически назначаются сетевые адреса
		1. Диапазон от 50 до 150 соответствующей сети
		2. Домен соответствующей организации
		3. Шлюз по умолчанию через интерфейс роутера в данной сети
		4. Адрес DNS-сервера организации
		5. Автоматическое обновление записей DNS-сервера организации при выдаче адреса
	2. Для узла **R-SRV** средствами службы DHCP должен быть зарезервирован статический адрес в соответствии с таблицей.
2. Настройте службу DNS для организации Left и Right на сервере **L-SRV**:
	1. Задайте имя зон left.rzce.ru и right.rzce.ru
	2. Разместите файлы зон в */opt/prof/*
	3. Обеспечьте прямое и обратное разрешение имен
	4. На всех внутренних машинах организаций реализуйте автоматическое разрешение имен в соответствии с таблицей из приложения.
3. Настройте трансляцию сетевых адресов в соответствии.
	1. Настройте трансляцию портов для всех машин каждой организации во внешний адрес соответствующего межсетевого экрана
	2. Обеспечьте достижимость VPN-шлюза организации Left из сети ISP путем трансляции соответствующего порта на **L-FW**
	3. Обеспечьте достижимость веб интерфейса гипервизора **R-PRX** по внешнему адресу ближайшего роутера на соответствующем порту

**Конфигурация файловых и веб служб**

1. На машине **R-SRV** установите и настройте веб-сервер apache:
	1. Организуйте структуру файлов и соответствующих URL в соответствии с таблицей из приложения.
	2. Настройте права доступа и содержание веб страниц в соответствии с таблицей из приложения.
	3. При доступности SSL-соединения настройте автоматический переход по протоколу HTTPS при попытке доступа по протоколу HTTP.
	4. Используйте сертификат, подписанный удостоверяющим центром **L-SRV**. При доступе по протоколу HTTPS с клиентских машин каждой организации сертификат должен рассматриваться как доверенный.
	5. Настройте веб-сервер таким образом, чтобы из ответов сервера нельзя было узнать версию веб-сервера и ОС.
2. На машине **R-SRV** создайте дисковый массив:
	1. Массив должен иметь максимально возможную скорость
	2. В случае отказа дисков сохранность данных не важна
	3. Для массива используйте самую популярную файловую систему в linux
	4. Массив должен быть смонтирован по пути */opt/storage*
	5. Обеспечьте автоматическое монтирование раздела при загрузке системы
3. На машине **R-SRV** настройте общее хранилище по протоколу NFS:
	1. Для хранения файлов используется каталог */opt/storage/nfs/*
	2. Настройте доступ на чтение и запись только для машины **R-PRX**
	3. Всем остальным машинам доступ должен быть запрещён
4. На машине **L-SRV** настройте общее хранилище по протоколу Samba:
	1. Для хранения файлов используется каталог */opt/samba/*
	2. Создать разделяемый ресурс с именем *Share*
	3. Разрешить доступ учетной записи (логин smbuser, пароль smbpass) с правами на чтение и запись
	4. Файлы должны создаваться с маской *0700*
5. Настройте клиентские машины каждой организации
	1. Все машины должны иметь доступ к файловому хранилищу Samba
	2. Хранилище должно монтироваться в */opt/share* соответствующей клиентской машины вызовом скрипта *mount\_share*

**Конфигурация служб мониторинга и журналирования**

1. На сервере **R-SRV** настройте сбор системных сообщений с помощью пакета rsyslog
	1. Настроить сбор сообщений о подключении OpenVPN клиентов с соответствующих серверов в файл по пути */opt/logs/vpn\_audit.log*
	2. Настроить сбор сообщений о входе пользователей на веб интерфейс гипервизора **R-PRX** в файл по пути */opt/logs/prx\_audit.log*

**Конфигурация параметров безопасности и служб аутентификации**

1. Настройте CA на **L-SRV**, используя OpenSSL
	1. Используйте директорию */etc/ca* в качестве корневой директории CA
	2. Создайте корневой сертификат CA
	3. Атрибуты CA должны быть следующими:
		1. Страна RU
		2. Организация Rce Russia
		3. CN должен быть установлен как PROF CA
	4. Все клиентские операционные системы должны доверять CA
	5. Используйте этот CA для выпуска всех необходимых клиентских и серверных сертификатов
2. Для клиентских машин организации Left:
	1. Настройте sudo следующим образом:
		1. Для пользовательских учетных записей запретите запуск команды visudo через sudo
		2. Ввод всех остальных команд через sudo должен быть разрешен с вводом пароля
	2. Запретите вход под учетной записью суперпользователя на первой консоли с 18-00 до 07-00

**Конфигурация системы виртуализации**

1. На машине **R-PRX** настройте систему виртуализации
	1. Подключите сетевое хранилище NFS в качестве хранилища образов виртуальных машин
	2. Веб-интерфейс гипервизора должен работать по 443 порту, соединение должно быть защищенным и доверенным
	3. Создайте виртуальную машину с именем **V-SRV**
		1. Используйте минимально возможные аппаратные характеристики для запуска операционной системы debian
		2. Диск объёмом не менее 200GB, располагается на сетевом хранилище
		3. Не устанавливайте операционную систему

**Спецификация оценки.**

В рамках данного модуля оцениваются навыки настройки сетевых и серверных служб на прилагаемой инфраструктуры.

Проверка результатов выполнения задания осуществляется оценивающими экспертами сразу по окончании выделенного на модуль времени. В дальнейшем проверка данного модуля осуществляться не будет.

#### Модуль Д. (*Автоматизация*)

*Время на выполнение модуля 5 часов.*

**Задания:**

Вам поставили задачу: компания переезжает, необходимо в новом дата центре автоматизировать развертывание обновленной версии веб приложения, которым пользуются ваши клиенты. Исходный код приложения и все необходимые инструкции находятся на git репозитории, ссылка на который в выданном Вам документе. Было решено отработать на локальном стенде сценарий автоматической настройки инфраструктуры с использованием программного обеспечение Ansible.

В вашем распоряжении тестовый стенд состоящий из 3 виртуальных машин под управлением Linux: **node\_worker1**, **node\_worker2** и **node\_balancer**. Топология сети представлена в приложении № 5.

Сетевые параметры были сконфигурированы предварительно инженером нашей компании, но **учтите**, что ваш плейбук будет запускаться на инфраструктуре, адресация которой Вам неизвестна. Каждая машина может иметь доступ в Интернет только через хост **node\_balancer**.

Необходимо реализовать Ansible playbook для автоматизации базовой конфигурации виртуальных машин. Контролирующим хостом является **node\_balancer**. На виртуальной машине предустановлены пакеты ansible, sshpass, git, lynx.

Виртуальная машина **node\_balancer** доступна с вашего рабочего места по протоколу SSH. Все необходимые данные для подключения выданы Вам перед началом работ. Машины **node\_worker\*** доступны только из внутренней сети, логин **root** пароль **toor**.

На хосте **node\_balancer** настройте файл доменных имен **hosts**:

<IP-адрес node\_worker1> node\_worker1

<IP-адрес node\_worker2> node\_worker2

Ansible playbook должен выполнять следующие задачи конфигурации:

* Выполнить клонирование Git-репозитория в корневую директорию на узле **node\_balancer**
* Обновить списки пакетов, выполнить установку утилиты curl и брандмауэра ufw
* Активировать межсетевой экран, настроить правила:
	+ На хостах **node\_worker\***:
		- Разрешить доступ к порту веб приложения и службе SSH только с адреса хоста **node\_balancer**
	+ На хосте **node\_balancer**:
		- Правило трансляции внутренних сетевых адресов в адрес внешнего интерфейса
		- Разрешить доступ к порту службы балансировщика HTTP трафика с любого хоста
		- Разрешить доступ к порту SSH только с адреса Вашего рабочего компьютера
	+ Остальной входящий трафик - запретить
* Изменить конфигурационный файл SSH:
	+ Порт подключения должен быть 4747
	+ Разрешить авторизацию по публичному ключу
* Создать пользователей для доступа к виртуальным машинам
	+ Список пользователей - в защищенном файле Ansible Vault по пути *Users/privvars.yml*
		- Для временной расшифровки используйте пароль **gK2VEOxxEK9n**
	+ Для каждого пользователя необходимо разместить публичный ключ
* Перезапустить службу SSH
* Выполнить установку пакета Docker
* Установить docker-compose необходимой версии
* На хостах **node\_worker\*** создать директорию */web-app*, скопируйте файлы необходимые для сборки образов и запуска контейнеров, а также файл *index.html*
* Выполните сборку необходимых образов на соответствующих виртуальных машинах, используя Dockerfile в директории *web-app*
* Запустить соответствующий файл конфигурации docker-compose
* С хоста **node\_balancer** проверить доступность развернутого веб-приложения, записать полученный ответ в файл */opt/testresult.log*
* Выполнить перезагрузку виртуальных машин

После выполнения задания, вам требуется собрать все файлы, которые необходимы для выполнения задания и отправить плейбук с зависимостями на GitHub аккаунт, логин и пароль от которого были выданы Вам перед началом работы.

Создайте отдельный репозиторий с именем *“ISMIG\_<номер рабочего места>”*, тип репозитория - Private. Создайте в вашем репозитории файл Readme.md и укажите инструкцию по запуску Вашего плейбука.

**Спецификация оценки.**

В рамках данного модуля оцениваются навыки развертывания различных сетевых сервисов и приложений, а также знание основ сетевой безопасности.

Проверка результатов выполнения задания осуществляется оценивающими экспертами сразу по окончании выделенного на модуль времени. В дальнейшем проверка данного модуля осуществляться не будет.

#

# 2. СПЕЦИАЛЬНЫЕ ПРАВИЛА КОМПЕТЕНЦИИ

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

* Внешние системы контроля версий
* Общения с живыми людьми посредством форумов, мессенджеров и иных средств коммуникации
* Ресурсы, которые требуют авторизацию пользователя
* Нейросетевые модели обработки текстов

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

Возможно использование личных устройств клавиатура и мышь, не поддерживаемых программирование.

## 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 Критерии оценки

Приложение №4 Инструкция по охране труда и технике безопасности по компетенции «Сетевое и системное администрирование»

Приложение № 5 Чертежи, технологические карты, алгоритмы, схемы и т.д.

1. Указывается суммарное время на выполнение всех модулей КЗ одним конкурсантом. [↑](#footnote-ref-0)