



**КОМПЛЕКТ ОЦЕНОЧНОЙ ДОКУМЕНТАЦИИ №1.1  
ДЛЯ ДЕМОНСТРАЦИОННОГО ЭКЗАМЕНА ПО  
СТАНДАРТАМ ВОРЛДСКИЛЛС РОССИЯ  
ПО КОМПЕТЕНЦИИ № 39 «СЕТЕВОЕ И СИСТЕМНОЕ  
АДМИНИСТРИРОВАНИЕ»  
(ДАЛЕЕ – ДЕМОНСТРАЦИОННЫЙ ЭКЗАМЕН)**

## СОДЕРЖАНИЕ

Паспорт комплекта оценочной документации (КОД) № 1.1 по компетенции № 39 «Сетевое и системное администрирование» .....	3
Задание для демонстрационного экзамена по комплекту оценочной документации № 1.1 по компетенции № 39 «Сетевое и системное администрирование» (образец) .....	42
Примерный план работы Центра проведения демонстрационного экзамена по КОД № 1.1 по компетенции «Сетевое и системное администрирование».....	84
План застройки площадки для проведения демонстрационного экзамена по КОД № 1.1 по компетенции № 39 «Сетевое и системное администрирование».....	86
ПРИЛОЖЕНИЕ .....	87

## Паспорт комплекта оценочной документации (КОД) № 1.1 по компетенции № 39 «Сетевое и системное администрирование»

Комплект оценочной документации (КОД) № 1.1 разработан в целях организации и проведения демонстрационного экзамена по компетенции № 39 «Сетевое и системное администрирование» и рассчитан на выполнение заданий продолжительностью 6 часов.

КОД № 1.1 может быть рекомендован для оценки освоения основных профессиональных образовательных программ и их частей, дополнительных профессиональных программ и программ профессионального обучения, а также на соответствие уровням квалификации согласно Таблице (Приложение).

**1. Перечень знаний, умений, навыков в соответствии со Спецификацией стандарта компетенции № 39 «Сетевое и системное администрирование» (WorldSkills Standards Specifications, WSSS), проверяемый в рамках комплекта оценочной документации (Таблица 1).**

**Таблица 1.**

Раздел WSSS	Наименование раздела WSSS	Важность (%)
1	<b>Организация работы и управление</b>	<b>0,6</b>
	Специалист должен знать и понимать: <ul style="list-style-type: none"><li>• Регламентирующие документы в области охраны труда и безопасности жизнедеятельности;</li><li>• В каких ситуациях необходимо применять персональные защитные средства;</li><li>• Порядок работы, хранения, и обслуживания оборудования в условиях антистатического окружения;</li><li>• Важность соблюдения техники безопасности и аккуратности при работе с клиентским оборудованием и информацией;</li><li>• Важность безопасной переработки отходов;</li><li>• Методы планирования и определения приоритетов;</li><li>• Важность точной работы, проверки выполненной работы, а также внимания к деталям во всех аспектах своей работы;</li><li>• Важность организации труда в соответствии с методиками;</li></ul>	

	<ul style="list-style-type: none"> <li>• Методы и технологии исследования;</li> <li>• Важность управления собственным профессиональным развитием;</li> <li>• Скорость изменения ИТ-сферы и важности соответствия современному уровню.</li> </ul>	
	<p>Специалист должен уметь:</p> <ul style="list-style-type: none"> <li>• Следовать предписаниям в области охраны труда и безопасности жизнедеятельности;</li> <li>• Поддерживать безопасную рабочую среду;</li> <li>• Определять и применять подходящие персональные защитные средства для организации антистатического окружения;</li> <li>• Выбирать, применять и обслуживать инструментарий и оборудование в соответствии с правилами техники безопасности;</li> <li>• Планировать свою работу для достижения максимальной эффективности и поддерживать чистоту на рабочем месте;</li> <li>• Регулярно планировать и корректировать планы в соответствии с изменяющимися приоритетами;</li> <li>• Работать эффективно и регулярно оценивать результаты своего труда;</li> <li>• Соответствовать различным требованиям таких отраслевых систем сертификаций как Cisco, Microsoft, Linux (со специализацией хотя бы в одной из этих областей);</li> <li>• Соответствовать требованиям, предъявляемым к носителям данной компетенции, соответствовать современному уровню;</li> <li>• Демонстрировать эффективные и всеобъемлющие методы получения знаний;</li> <li>• Демонстрировать энтузиазм в области внедрения новых методов, систем, быть готовым к изменениям;</li> <li>• Эффективно работать в составе команды.</li> </ul>	
<b>2</b>	<b>Коммуникация и общение</b>	<b>1,7</b>
	<p>Специалист должен знать и понимать:</p> <ul style="list-style-type: none"> <li>• Важность умения слушать собеседника как части эффективной коммуникации;</li> <li>• Роли и требования коллег и наиболее эффективные методы коммуникации;</li> </ul>	

	<ul style="list-style-type: none"> <li>• Важность построения и поддержания продуктивных рабочих отношений с коллегами и управляющими;</li> <li>• Методы эффективной командной работы;</li> <li>• Способы разрешения непонимания и конфликтующих требований;</li> <li>• Методы управления стрессом и гневом для разрешения сложных ситуаций.</li> </ul>	
	<p>Специалист должен уметь:</p> <ul style="list-style-type: none"> <li>• Демонстрировать развитые способности слушать и задавать вопросы для более глубокого понимания сложных ситуаций;</li> <li>• Выстраивать эффективное письменное и устное общение с коллегами;</li> <li>• Понимать изменяющиеся требования коллег и адаптироваться к ним;</li> <li>• Активно принимать участие в формировании сильной и эффективной команды;</li> <li>• Обмениваться знаниями и опытом с коллегами и поддерживать атмосферу самосовершенствования в коллективе;</li> <li>• Управлять стрессом и раздражением, давать уверенность окружающим в том, что их проблемы могут быть разрешены.</li> </ul>	
<b>3</b>	<b>Консультирование и поддержка пользователей</b>	<b>1,1</b>
	<p>Специалист должен знать и понимать:</p> <ul style="list-style-type: none"> <li>• Основные возможности определенного круга ИТ-систем для обеспечения качественной поддержки;</li> <li>• Подходы к планированию рабочего процесса с целью обеспечения высокого уровня обслуживания, способного удовлетворить потребности пользователя и организации;</li> <li>• Различные методы демонстрации и презентации для поддержки развития навыков и знаний пользователя;</li> <li>• Различные методы оценки возможностей пользователя с целью удовлетворения его немедленных потребностей и поощрения к саморазвитию;</li> <li>• Различные методики обучения, позволяющие адаптировать процесс обучения с учетом навыков и возможностей пользователей;</li> <li>• Тренды и вызовы современной ИТ-индустрии и способы развития, которые могут быть представлены пользователям;</li> </ul>	

	<ul style="list-style-type: none"> <li>• Способы ведения переговоров для различных ситуаций.</li> </ul>	
	<p>Специалист должен уметь:</p> <ul style="list-style-type: none"> <li>• Заблаговременно поддерживать уровень собственных познаний в сфере информационных технологий;</li> <li>• Своевременно (в установленных регламентом рамках) отвечать на запросы как локальных, так и удаленных пользователей;</li> <li>• Планировать и постоянно актуализировать планы выполнения пользовательских запросов к поддержке для балансировки потребностей пользователей и организации;</li> <li>• Точно определять требования пользователя и оправдывать ожидания;</li> <li>• Подсчитывать время и стоимость выполнения работы;</li> <li>• Выбирать наиболее подходящие способы демонстрации для более точного соответствия подачи материала навыкам и знаниям аудитории;</li> <li>• Эффективно демонстрировать информационные системы пользователям и группам пользователей для предоставления им возможностей к улучшению своих навыков и знаний;</li> <li>• Успешно обучать пользователей очно и заочно для успешного разрешения проблем в области ИТ-инфраструктуры, представления новых продуктов, улучшения пользовательских навыков и знаний;</li> <li>• Определять возможности к улучшению продукта и общей удовлетворенности пользователя;</li> <li>• Формировать точные, своевременные рекомендации в области обновления и приобретения новых ИТ-продуктов и сервисов для улучшения качества принятия решений;</li> <li>• Формировать корректные, отвечающие требованиям и ограничениям, рекомендации на основе запросов и потребностей;</li> <li>• Принимать участие в тендерных и закупочных процедурах.</li> </ul>	
<b>4</b>	<b>Поиск и устранение неисправностей</b>	<b>7,1</b>
	<p>Специалист должен знать и понимать:</p> <ul style="list-style-type: none"> <li>• Важность спокойного и сфокусированного подхода к решению проблемы;</li> </ul>	

	<ul style="list-style-type: none"> <li>• Значимость IT-систем и зависимость пользователей и организаций от их доступности;</li> <li>• Популярные аппаратные и программные ошибки;</li> <li>• Аналитический и диагностический подходы к решению проблем;</li> <li>• Границы собственных знаний, навыков и полномочий;</li> <li>• Ситуации, требующие эскалации инцидентов;</li> <li>• Стандартное время решения наиболее популярных проблем.</li> </ul>	
5	<p>Специалист должен уметь:</p> <ul style="list-style-type: none"> <li>• Подходить к проблеме с необходимым уровнем уверенности для успокоения пользователя в случае необходимости;</li> <li>• Регулярно проверять результаты собственной работы во избежание проблем на последующих этапах;</li> <li>• Уточнять некорректную информацию для предотвращения или минимизации проблем;</li> <li>• Демонстрировать уверенность и упорство в решении проблем</li> <li>• Быстро узнавать и понимать суть неисправностей и разрешать их в ходе самостоятельной управляемой работы</li> <li>• Тщательно расследовать и анализировать сложные, комплексные ситуации и проблемы, применять методики поиска неисправностей;</li> <li>• Выбирать и принимать диагностирующее ПО и инструменты для поиска неисправностей;</li> <li>• Поддерживать пользователей в решении проблем через советы, указания и инструкции;</li> <li>• Искать помощь в тех случаях, когда требуется более тщательная экспертиза, избегать чрезмерного увлечения проблемой;</li> <li>• Уточнять уровень удовлетворенности пользователя после решения проблемы;</li> <li>• Точно описывать инцидент и документировать решение проблемы.</li> </ul> <p style="text-align: center;"><b>Дизайн</b></p>	4,5
	<p>Специалист должен знать и понимать:</p> <ul style="list-style-type: none"> <li>• Сетевые топологии и окружения;</li> </ul>	

	<ul style="list-style-type: none"> <li>• Логические и функциональные диаграммы;</li> <li>• Типы активных сетевых устройств (маршрутизаторов и коммутаторов и т.д.) и требования к их расположению;</li> <li>• Решения в области безопасности и их влияние;</li> <li>• Схемы адресации;</li> <li>• Документацию по настройке оборудования и программ.</li> </ul>	
	<p>Специалист должен уметь:</p> <ul style="list-style-type: none"> <li>• Сетевые топологии и окружения;</li> <li>• Логические и функциональные диаграммы;</li> <li>• Типы активных сетевых устройств (маршрутизаторов и коммутаторов и т.д.) и требования к их расположению;</li> <li>• Решения в области безопасности и их влияние;</li> <li>• Схемы адресации;</li> <li>• Документацию по настройке оборудования и программ.</li> </ul>	
<b>6</b>	<b>Настройка, обновление и конфигурация операционных систем</b>	<b>15</b>
	<p>Специалист должен знать и понимать:</p> <ul style="list-style-type: none"> <li>• Разнообразие операционных систем, их возможности к удовлетворению пользовательских требований;</li> <li>• Процесс выбора подходящих драйверов для разных типов аппаратных средств;</li> <li>• Базовые функции аппаратного обеспечения и процесс начальной загрузки;</li> <li>• Важность следования инструкциям и последствия, цену пренебрежения ими;</li> <li>• Меры предосторожности, рекомендуемые к принятию перед установкой ПО или обновлением системы;</li> <li>• Цель документирования процессов обновления и установки.</li> </ul>	
	<p>Специалист должен уметь:</p> <ul style="list-style-type: none"> <li>• Внимательно слушать и определять пользовательские запросы для удовлетворения ожиданий;</li> <li>• Выбирать операционную систему – проприетарную или открытую;</li> <li>• Точно определять устройство и соответствующий ему драйвер;</li> <li>• Последовательно проверять указанные производителем инструкции при выполнении обновления;</li> </ul>	



	<ul style="list-style-type: none"> <li>• Выбирать роли и возможности операционных систем (такие как Контроллер Домена и т.д.);</li> <li>• Обсуждать предложенные решения для выбранных ролей и возможностей, соглашаться с конструктивными предложениями от пользователей, менеджеров и коллег;</li> <li>• Подготовить технический документ, отражающий принятое решение для согласования и подписи;</li> <li>• Конфигурировать необходимые роли\возможности в соответствии с инструкциями разработчиков или в соответствии с наилучшими практиками;</li> <li>• Тестировать системы, устранять проблемы и проводить контрольные проверки;</li> <li>• Добиваться пользовательского одобрения.</li> </ul>	
<b>7</b>	<b>Конфигурация сетевых устройств</b>	<b>15</b>
	<p>Специалист должен знать и понимать:</p> <ul style="list-style-type: none"> <li>• Сетевое окружение;</li> <li>• Сетевые протоколы;</li> <li>• Процесс построения сети и как сетевые устройства могут быть настроены для эффективного взаимодействия;</li> <li>• Типы сетевых устройств.</li> </ul>	
	<p>Специалист должен уметь:</p> <ul style="list-style-type: none"> <li>• Интерпретировать пользовательские запросы и требования с точки зрения промышленных сертификационных требований;</li> <li>• Применять все типы конфигураций, программные и аппаратные обновления на все типы сетевых устройств, которые могут быть в сетевом окружении;</li> <li>• Проектировать и реализовывать процедуры ликвидации инцидентов;</li> <li>• Поддерживать базу данных конфигураций.</li> </ul>	

## 2. Форма участия

Индивидуальная

## 2. Обобщенная оценочная ведомость.

В данном разделе определяются критерии оценки и количество начисляемых баллов (судейские и объективные) (Таблица 2).

Общее максимально возможное количество баллов задания по всем критериям оценки составляет 45.

**Таблица 2.**

п/п	Критерий	Модуль, в котором используется критерий	Проверяемые разделы WSSS	Баллы		
				Судейская (если это применимо)	Объективная	Общая
1	A Linux Enviroments	A Linux Enviroments	6	0	15	15
2	B Windows Enviroments	B Windows Enviroments	1, 2, 3, 4, 5	0	15	15
3	C Cisco Enviroments	C Cisco Enviroments	7	0	15	15
<b>ИТОГО:</b>					<b>45</b>	<b>45</b>

#### **4. Количество экспертов, участвующих в оценке выполнения задания, и минимальное количество рабочих мест на площадке.**

4.1. Минимальное количество экспертов, участвующих в оценке демонстрационного экзамена по компетенции № 39 «Сетевое и системное администрирование» - 3 чел.

4.2. Минимальное количество рабочих мест составляет 9.

4.3. Расчет количества экспертов исходя из количества рабочих мест и участников осуществляется по схеме согласно Таблице 3:

**Таблица 3.**

Количество постов-рабочих мест	1	2	3	4	5	6	7	8	9
	3	3	3	3	3	3	3	3	3
Количество участников	3	3	3	3	3	3	3	3	3

#### **5. Список оборудования и материалов, запрещенных на площадке (при наличии)**

К проносу запрещаются такие электронные устройства как мобильные телефоны, смартфоны, плееры, наушники, диктофоны, камеры, ноутбуки, планшетные компьютеры и прочие персональные электронные устройства.

Таблица соответствия

знаний, умений и практических навыков, оцениваемых в рамках демонстрационного экзамена по компетенции №39 «Сетевое и системное администрирование» по КОД № 1.1 профессиональным компетенциям, основным видам деятельности, предусмотренным ФГОС СПО и уровням квалификаций в соответствии с профессиональными стандартами

Уровень аттестации (промежуточная/ГИА)	Код и наименование ФГОС СПО	Основные виды деятельности ФГОС СПО (ПМ)	Профессиональные компетенции (ПК) ФГОС СПО	Наименование профессионального стандарта (ПС)	Наименование и уровень квалификаций ПС	WSSS/модули/критерии оценки по КОД (по решению разработчика)
Комплект оценочной документации №1.1, продолжительность 6 час., максимально возможный балл - 456.						
ГИА	09.01.02 Наладчик компьютерных сетей	4.3.1. Выполнение работ по монтажу, наладке, эксплуатации и обслуживанию локальных компьютерных сетей. 4.3.2. Выполнение работ по подключению к глобальным компьютерным сетям. 4.3.3. Обеспечение информационной безопасности компьютерных сетей.	ПК 1.1. Осуществлять монтаж кабельной сети и оборудования локальных сетей различной топологии. ПК 1.2. Осуществлять настройку сетевых протоколов серверов и рабочих станций. ПК 1.3. Выполнять работы по эксплуатации и обслуживанию сетевого оборудования. ПК 1.4. Обеспечивать работу системы регистрации и авторизации пользователей сети. ПК 1.5. Осуществлять системное администрирование локальных сетей. ПК 2.1. Устанавливать и настраивать подключения к сети Интернет с помощью различных технологий и специализированного оборудования.		Мониторинг СКС с целью локализации неисправностей, 4	

Уровень аттестации (промежуточная/ГИА)	Код и наименование ФГОС СПО	Основные виды деятельности ФГОС СПО (ПМ)	Профессиональные компетенции (ПК) ФГОС СПО	Наименование профессионального стандарта (ПС)	Наименование и уровень квалификаций ПС	WSSS/модули/критерии оценки по КОД (по решению разработчика)
			<p>ПК 2.2. Осуществлять выбор технологии подключения и тарифного плана у провайдера доступа к сети Интернет.</p> <p>ПК 2.3. Устанавливать специализированные программы и драйверы, осуществлять настройку параметров подключения к сети Интернет.</p> <p>ПК 2.4. Осуществлять управление и учет входящего и исходящего трафика сети.</p> <p>ПК 2.5. Интегрировать локальную сеть в сеть Интернет.</p> <p>ПК 2.6. Устанавливать и настраивать программное обеспечение серверов сети Интернет.</p> <p>ПК 3.1. Обеспечивать резервное копирование данных.</p> <p>ПК 3.2. Осуществлять меры по защите компьютерных сетей от несанкционированного доступа.</p> <p>ПК 3.3. Применять специализированные средства для борьбы с вирусами, несанкционированными рассылками электронной почты, вредоносными программами.</p>			

Уровень аттестации (промежуточная/ ГИА)	Код и наименование ФГОС СПО	Основные виды деятельности ФГОС СПО (ПМ)	Профессиональные компетенции (ПК) ФГОС СПО	Наименование профессионального стандарта (ПС)	Наименование и уровень квалификаций ПС	WSSS/модули/критерии оценки по КОД (по решению разработчика)
			ПК 3.4. Осуществлять мероприятия по защите персональных данных.			
промежуточная/ ГИА	09.02.02 Компьютерные сети	<p>4.3. Техник по компьютерным сетям готовится к следующим видам деятельности:</p> <p>4.3.1. Участие в проектировании сетевой инфраструктуры.</p> <p>4.3.2. Организация сетевого администрирования .</p> <p>4.3.3.Эксплуатация объектов сетевой инфраструктуры.</p> <p>4.3.4.Выполнение работ по одной или нескольким профессиям рабочих, должностям служащих (приложение к</p>	<p>5.2.1. Участие в проектировании сетевой инфраструктуры.</p> <p>ПК 1.1. Выполнять проектирование кабельной структуры компьютерной сети.</p> <p>ПК 1.2. Осуществлять выбор технологии, инструментальных средств и средств вычислительной техники при организации процесса разработки и исследования объектов профессиональной деятельности.</p> <p>ПК 1.3. Обеспечивать защиту информации в сети с использованием программно-аппаратных средств.</p> <p>ПК 1.4. Принимать участие в приемо-сдаточных испытаниях компьютерных сетей и сетевого оборудования различного уровня и в оценке качества и экономической</p>	Приказ Минтруда России от 05.10.2015 N 684н "Об утверждении профессионального стандарта "Системный администратор информационно-коммуникационных систем"	Администрирование прикладного программного обеспечения инфокоммуникационной системы организации, 5 Управление программно-аппаратными средствами информационных служб инфокоммуникационной системы организации, 6	

Уровень аттестации (промежуточная/ГИА)	Код и наименование ФГОС СПО	Основные виды деятельности ФГОС СПО (ПМ)	Профессиональные компетенции (ПК) ФГОС СПО	Наименование профессионального стандарта (ПС)	Наименование и уровень квалификаций ПС	WSSS/модули/критерии оценки по КОД (по решению разработчика)
		<p>настоящему ФГОС СПО).</p> <p>4.4. Специалист по администрированию сети готовится к следующим видам деятельности:</p> <p>4.4.1. Участие в проектировании сетевой инфраструктуры.</p> <p>4.4.2. Организация сетевого администрирования .</p> <p>4.4.3. Эксплуатация объектов сетевой инфраструктуры.</p> <p>4.4.4. Управление сетевыми сервисами.</p>	<p>эффективности сетевой топологии.</p> <p>ПК 1.5. Выполнять требования нормативно-технической документации, иметь опыт оформления проектной документации.</p> <p>5.2.2. Организация сетевого администрирования.</p> <p>ПК 2.1. Администрировать локальные вычислительные сети и принимать меры по устранению возможных сбоев.</p> <p>ПК 2.2. Администрировать сетевые ресурсы в информационных системах.</p> <p>ПК 2.3. Обеспечивать сбор данных для анализа использования и функционирования программно-технических средств компьютерных сетей.</p> <p>ПК 2.4. Взаимодействовать со специалистами смежного</p>		<p>Администрирование сетевой подсистемы инфокоммуникационной системы организации, 6</p> <p>Администрирование системного программного обеспечения инфокоммуникационной системы организации, 7</p> <p>Управление развитием инфокоммуникационной</p>	

Уровень аттестации (промежуточная/ГИА)	Код и наименование ФГОС СПО	Основные виды деятельности ФГОС СПО (ПМ)	Профессиональные компетенции (ПК) ФГОС СПО	Наименование профессионального стандарта (ПС)	Наименование и уровень квалификаций ПС	WSSS/модули/критерии оценки по КОД (по решению разработчика)
		<p>4.4.5. Участие в модернизации сетевой инфраструктуры.</p> <p>4.4.6. Выполнение работ по одной или нескольким профессиям рабочих, должностям служащих (приложение к настоящему ФГОС СПО).</p>	<p>профиля при разработке методов, средств и технологий применения объектов профессиональной деятельности.</p> <p>5.2.3. Эксплуатация объектов сетевой инфраструктуры.</p> <p>ПК 3.1. Устанавливать, настраивать, эксплуатировать и обслуживать технические и программно-аппаратные средства компьютерных сетей.</p> <p>ПК 3.2. Проводить профилактические работы на объектах сетевой инфраструктуры и рабочих станциях.</p> <p>ПК 3.3. Эксплуатация сетевых конфигураций.</p> <p>ПК 3.4. Участвовать в разработке схемы послеаварийного восстановления работоспособности компьютерной сети, выполнять восстановление и резервное копирование информации.</p>		<p>системы организации, 7</p>	

Уровень аттестации (промежуточная/ГИА)	Код и наименование ФГОС СПО	Основные виды деятельности ФГОС СПО (ПМ)	Профессиональные компетенции (ПК) ФГОС СПО	Наименование профессионального стандарта (ПС)	Наименование и уровень квалификаций ПС	WSSS/модули/критерии оценки по КОД (по решению разработчика)
			<p>ПК 3.5. Организовывать инвентаризацию технических средств сетевой инфраструктуры, осуществлять контроль оборудования после его ремонта.</p> <p>ПК 3.6. Выполнять замену расходных материалов и мелкий ремонт периферийного оборудования, определять устаревшее оборудование и программные средства сетевой инфраструктуры.</p> <p>5.4.4. Управление сетевыми сервисами.</p> <p>ПК 4.1. Принимать меры по отслеживанию, предотвращению и устранению нештатных ситуаций.</p> <p>ПК 4.2. Контролировать сетевую инфраструктуру с использованием инструментальных средств эксплуатации сетевых конфигураций.</p> <p>ПК 4.3. Обеспечивать максимальную стабильность</p>			



Уровень аттестации (промежуточная/ГИА)	Код и наименование ФГОС СПО	Основные виды деятельности ФГОС СПО (ПМ)	Профессиональные компетенции (ПК) ФГОС СПО	Наименование профессионального стандарта (ПС)	Наименование и уровень квалификаций ПС	WSSS/модули/критерии оценки по КОД (по решению разработчика)
			<p>предоставляемых сетевых сервисов.</p> <p>ПК 4.4. Предоставлять согласованные с информационно-технологическими подразделениями сетевые сервисы и выполнять необходимые процедуры поддержки.</p> <p>ПК 4.5. Восстанавливать нормальную работу сетевых сервисов в соответствии с требованиями регламентов.</p> <p>ПК 4.6. Вести учет плановой потребности в расходных материалах и комплектующих.</p> <p>5.4.5. Участие в модернизации сетевой инфраструктуры.</p> <p>ПК 5.1. Идентифицировать проблемы в процессе эксплуатации программного обеспечения.</p> <p>ПК 5.2. Разрабатывать предложения по</p>			

Уровень аттестации (промежуточная/ГИА)	Код и наименование ФГОС СПО	Основные виды деятельности ФГОС СПО (ПМ)	Профессиональные компетенции (ПК) ФГОС СПО	Наименование профессионального стандарта (ПС)	Наименование и уровень квалификаций ПС	WSSS/модули/критерии оценки по КОД (по решению разработчика)
			<p>совершенствованию и повышению эффективности работы сетевой инфраструктуры.</p> <p>ПК 5.3. Разрабатывать сетевые топологии в соответствии с требованиями отказоустойчивости и повышения производительности корпоративной сети.</p> <p>ПК 5.4. Составлять отчет по выполненному заданию, участвовать во внедрении результатов разработок.</p> <p>ПК 5.5. Проводить эксперименты по заданной методике, выполнять анализ результатов.</p> <p>5.4.6. Выполнение работ по одной или нескольким профессиям рабочих, должностям служащих.</p>			
ГИА	09.02.06 Сетевое и системное	Выполнение работ по проектированию	3.4.1. Выполнение работ по проектированию сетевой инфраструктуры:	Приказ Минтруда России от 05.10.2015 N 684н	Администрирование прикладного программного	

Уровень аттестации (промежуточная/ГИА)	Код и наименование ФГОС СПО	Основные виды деятельности ФГОС СПО (ПМ)	Профессиональные компетенции (ПК) ФГОС СПО	Наименование профессионального стандарта (ПС)	Наименование и уровень квалификаций ПС	WSSS/модули/критерии оценки по КОД (по решению разработчика)
	администрирование	сетевой инфраструктуры Организация сетевого администрирования Эксплуатация объектов сетевой инфраструктуры Управление сетевыми сервисами Сопровождение модернизации сетевой инфраструктуры	<p>ПК 1.1. Выполнять проектирование кабельной структуры компьютерной сети.</p> <p>ПК 1.2. Осуществлять выбор технологий, инструментальных средств и средств вычислительной техники при организации процесса разработки и исследования объектов профессиональной деятельности.</p> <p>ПК 1.3. Обеспечивать защиту информации в сети с использованием программно-аппаратных средств.</p> <p>ПК 1.4. Принимать участие в приемо-сдаточных испытаниях компьютерных сетей и сетевого оборудования различного уровня и в оценке качества и экономической эффективности сетевой топологии.</p> <p>ПК 1.5. Выполнять требования нормативно-технической документации,</p>	"Об утверждении профессионального стандарта "Системный администратор информационно-коммуникационных систем"	обеспечения инфокоммуникационной системы организации, 5 Управление программно-аппаратными средствами информационных служб инфокоммуникационной системы организации, 6 Администрирование сетевой подсистемы инфокоммуникационной	

Уровень аттестации (промежуточная/ГИА)	Код и наименование ФГОС СПО	Основные виды деятельности ФГОС СПО (ПМ)	Профессиональные компетенции (ПК) ФГОС СПО	Наименование профессионального стандарта (ПС)	Наименование и уровень квалификаций ПС	WSSS/модули/критерии оценки по КОД (по решению разработчика)
			<p>иметь опыт оформления проектной документации.</p> <p>3.4.2. Организация сетевого администрирования:</p> <p>ПК 2.1. Администрировать локальные вычислительные сети и принимать меры по устранению возможных сбоев.</p> <p>ПК 2.2. Администрировать сетевые ресурсы в информационных системах.</p> <p>ПК 2.3. Обеспечивать сбор данных для анализа использования и функционирования программно-технических средств компьютерных сетей.</p> <p>ПК 2.4. Взаимодействовать со специалистами смежного профиля при разработке методов, средств и технологий</p>		<p>системы организации, 6</p> <p>Администрирование системного программного обеспечения инфокоммуникационной системы организации, 7</p> <p>Управление развитием инфокоммуникационной системы организации, 7</p>	

Уровень аттестации (промежуточная/ГИА)	Код и наименование ФГОС СПО	Основные виды деятельности ФГОС СПО (ПМ)	Профессиональные компетенции (ПК) ФГОС СПО	Наименование профессионального стандарта (ПС)	Наименование и уровень квалификаций ПС	WSSS/модули/критерии оценки по КОД (по решению разработчика)
			<p>применения объектов профессиональной деятельности.</p> <p>3.4.3. Эксплуатация объектов сетевой инфраструктуры:</p> <p>ПК 3.1. Устанавливать, настраивать, эксплуатировать и обслуживать технические и программно-аппаратные средства компьютерных сетей.</p> <p>ПК 3.2. Проводить профилактические работы на объектах сетевой инфраструктуры и рабочих станциях.</p> <p>ПК 3.3. Устанавливать, настраивать, эксплуатировать и обслуживать сетевые конфигурации.</p> <p>ПК 3.4. Участвовать в разработке схемы послеаварийного восстановления работоспособности компьютерной сети, выполнять</p>			

Уровень аттестации (промежуточная/ГИА)	Код и наименование ФГОС СПО	Основные виды деятельности ФГОС СПО (ПМ)	Профессиональные компетенции (ПК) ФГОС СПО	Наименование профессионального стандарта (ПС)	Наименование и уровень квалификаций ПС	WSSS/модули/критерии оценки по КОД (по решению разработчика)
			<p>восстановление и резервное копирование информации.</p> <p>ПК 3.5. Организовывать инвентаризацию технических средств сетевой инфраструктуры, осуществлять контроль оборудования после его ремонта.</p> <p>ПК 3.6. Выполнять замену расходных материалов и мелкий ремонт периферийного оборудования, определять устаревшее оборудование и программные средства сетевой инфраструктуры.</p> <p>3.4.4. Управление сетевыми сервисами:</p> <p>ПК 4.1. Принимать меры по отслеживанию, предотвращению и устранению нештатных ситуаций.</p> <p>ПК 4.2. Контролировать сетевую инфраструктуру с использованием инструментальных средств</p>			

Уровень аттестации (промежуточная/ГИА)	Код и наименование ФГОС СПО	Основные виды деятельности ФГОС СПО (ПМ)	Профессиональные компетенции (ПК) ФГОС СПО	Наименование профессионального стандарта (ПС)	Наименование и уровень квалификаций ПС	WSSS/модули/критерии оценки по КОД (по решению разработчика)
			<p>эксплуатации сетевых конфигураций.</p> <p>ПК 4.3. Обеспечивать максимальную стабильность предоставляемых сетевых сервисов.</p> <p>ПК 4.4. Предоставлять согласованные с информационно-технологическими подразделениями сетевые сервисы и выполнять необходимые процедуры поддержки.</p> <p>ПК 4.5. Восстанавливать нормальную работу сетевых сервисов в соответствии с требованиями регламентов.</p> <p>ПК 4.6 Вести учет плановой потребности в расходных материалах и комплектующих.</p> <p>3.4.5. Сопровождение модернизации сетевой инфраструктуры;</p>			

Уровень аттестации (промежуточная/ГИА)	Код и наименование ФГОС СПО	Основные виды деятельности ФГОС СПО (ПМ)	Профессиональные компетенции (ПК) ФГОС СПО	Наименование профессионального стандарта (ПС)	Наименование и уровень квалификаций ПС	WSSS/модули/критерии оценки по КОД (по решению разработчика)
			<p>ПК 5.1. Идентифицировать проблемы в процессе эксплуатации программного обеспечения.</p> <p>ПК 5.2. Разрабатывать предложения по совершенствованию и повышению эффективности работы сетевой инфраструктуры.</p> <p>ПК 5.3. Разрабатывать сетевые топологии в соответствии с требованиями отказоустойчивости и повышения производительности корпоративной сети.</p> <p>ПК 5.4. Составлять отчет по выполненному заданию, участвовать во внедрении результатов разработок.</p> <p>ПК 5.5. Проводить эксперименты по заданной методике, выполнять анализ результатов.</p>			



Уровень аттестации (промежуточная/ ГИА)	Код и наименование ФГОС СПО	Основные виды деятельности ФГОС СПО (ПМ)	Профессиональные компетенции (ПК) ФГОС СПО	Наименование профессионального стандарта (ПС)	Наименование и уровень квалификаций ПС	WSSS/модули/критерии оценки по КОД (по решению разработчика)
промежуточная/ ГИА	09.02.07 Информационные системы и программирование	Сопровождение и обслуживание программного обеспечения компьютерных систем Сопровождение информационных систем Администрирование информационных ресурсов	<p>3.4.4. Сопровождение и обслуживание программного обеспечения систем:</p> <p>ПК 4.1. Осуществлять инсталляцию, настройку и обслуживание программного обеспечения компьютерных систем.</p> <p>ПК 4.2. Осуществлять измерения эксплуатационных характеристик программного обеспечения компьютерных систем.</p> <p>ПК 4.3. Выполнять работы по модификации отдельных компонент программного обеспечения в соответствии с потребностями заказчика.</p> <p>ПК 4.4. Обеспечивать защиту программного обеспечения компьютерных систем программными средствами.</p>	Приказ Минтруда России от 05.10.2015 N 684н "Об утверждении профессионального стандарта "Системный администратор информационно-коммуникационных систем"	Администрирование прикладного программного обеспечения инфокоммуникационной системы организации, 5	

Уровень аттестации (промежуточная/ГИА)	Код и наименование ФГОС СПО	Основные виды деятельности ФГОС СПО (ПМ)	Профессиональные компетенции (ПК) ФГОС СПО	Наименование профессионального стандарта (ПС)	Наименование и уровень квалификаций ПС	WSSS/модули/критерии оценки по КОД (по решению разработчика)
			<p>3.4.6. Сопровождение информационных систем:</p> <p>ПК 6.1. Разрабатывать техническое задание на сопровождение информационной системы.</p> <p>ПК 6.2. Выполнять исправление ошибок в программном коде информационной системы.</p> <p>ПК 6.4. Оценивать качество и надежность функционирования информационной системы в соответствии с критериями технического задания.</p> <p>ПК 6.5. Осуществлять техническое сопровождение, обновление и восстановление данных информационной системы в соответствии с техническим заданием.</p> <p>3.4.10. Администрирование информационных ресурсов:</p>			

Уровень аттестации (промежуточная/ГИА)	Код и наименование ФГОС СПО	Основные виды деятельности ФГОС СПО (ПМ)	Профессиональные компетенции (ПК) ФГОС СПО	Наименование профессионального стандарта (ПС)	Наименование и уровень квалификаций ПС	WSSS/модули/критерии оценки по КОД (по решению разработчика)
			ПК 10.1. Обрабатывать статический и динамический информационный контент.			
промежуточная	10.02.02 Информационная безопасность телекоммуникационных систем	<p>4.3.1. Техническое обслуживание оборудования защищенных телекоммуникационных систем.</p> <p>4.3.2. Применение программно-аппаратных, инженерно-технических методов и средств обеспечения информационной безопасности телекоммуникационных систем.</p> <p>4.3.3. Участие в организации работ по обеспечению</p>	<p>ПК 1.1. Устанавливать, конфигурировать оборудование защищенных телекоммуникационных систем.</p> <p>ПК 1.2. Эксплуатировать оборудование защищенных телекоммуникационных систем.</p> <p>ПК 2.1. Осуществлять установку (монтаж), настройку (наладку) и запуск в эксплуатацию программно-аппаратных и инженерно-технических средств обеспечения информационной безопасности телекоммуникационных систем.</p> <p>ПК 2.2. Обеспечивать эксплуатацию и содержание в работоспособном состоянии программно-аппаратных и инженерно-технических средств обеспечения информационной безопасности</p>	Приказ Минтруда России от 05.10.2015 N 684н "Об утверждении профессионального стандарта "Системный администратор информационно-коммуникационных систем"	Администрирование сетевой подсистемы инфокоммуникационной системы организации	

Уровень аттестации (промежуточная/ГИА)	Код и наименование ФГОС СПО	Основные виды деятельности ФГОС СПО (ПМ)	Профессиональные компетенции (ПК) ФГОС СПО	Наименование профессионального стандарта (ПС)	Наименование и уровень квалификаций ПС	WSSS/модули/критерии оценки по КОД (по решению разработчика)
		информационной безопасности телекоммуникационных систем.	телекоммуникационных систем, их диагностику, обнаружение отказов, формировать предложения по их устранению. принадлежностей. ПК 3.3. Участвовать во внедрении разработанных технических решений и проектов во взаимодействии с другими специалистами, оказывать техническую помощь исполнителям при изготовлении, монтаже, настройке, испытаниях и эксплуатации технических средств.			
<b>промежуточная/ ГИА</b>	10.02.03 Информационная безопасность автоматизированных систем	4.3.1. Эксплуатация подсистем безопасности автоматизированных систем. 4.3.2. Применение программно-аппаратных средств	ПК 1.1. Участвовать в эксплуатации компонентов подсистем безопасности автоматизированных систем, в проверке их технического состояния, в проведении технического обслуживания и текущего ремонта, устранении отказов и восстановлении работоспособности.	Приказ Минтруда России от 05.10.2015 N 684н "Об утверждении профессионального стандарта "Системный администратор	Администрирование сетевой подсистемы инфокоммуникационной системы организации	

Уровень аттестации (промежуточная/ГИА)	Код и наименование ФГОС СПО	Основные виды деятельности ФГОС СПО (ПМ)	Профессиональные компетенции (ПК) ФГОС СПО	Наименование профессионального стандарта (ПС)	Наименование и уровень квалификаций ПС	WSSS/модули/критерии оценки по КОД (по решению разработчика)
		<p>обеспечения информационной безопасности в автоматизированных системах.</p> <p>4.3.3. Применение инженерно-технических средств обеспечения информационной безопасности.</p>	<p>ПК 1.2. Выполнять работы по администрированию подсистем безопасности автоматизированных систем.</p> <p>ПК 1.3. Производить установку и адаптацию компонентов подсистем безопасности автоматизированных систем.</p> <p>ПК 2.1. Применять программно-аппаратные средства обеспечения информационной безопасности в автоматизированных системах.</p> <p>ПК 2.2. Участвовать в эксплуатации программно-аппаратных средств обеспечения информационной безопасности, в проверке их технического состояния, в проведении технического обслуживания и текущего ремонта, устранении отказов и восстановлении работоспособности.</p> <p>ПК 2.3. Участвовать в мониторинге эффективности применяемых программно-</p>	информационно-коммуникационных систем		

Уровень аттестации (промежуточная/ ГИА)	Код и наименование ФГОС СПО	Основные виды деятельности ФГОС СПО (ПМ)	Профессиональные компетенции (ПК) ФГОС СПО	Наименование профессионального стандарта (ПС)	Наименование и уровень квалификаций ПС	WSSS/модули/критерии оценки по КОД (по решению разработчика)
			аппаратных средств обеспечения информационной безопасности в автоматизированных системах.			
<b>промежуточная/ ГИА</b>	10.02.05 Обеспечение информационной безопасности и автоматизированных систем	Эксплуатация автоматизированных (информационных) систем в защищенном исполнении; Защита информации в автоматизированных системах программными и программно-аппаратными средствами	ПК 2.1. Осуществлять установку и настройку отдельных программных, программно-аппаратных средств защиты информации. ПК 2.2. Обеспечивать защиту информации в автоматизированных системах отдельными программными, программно-аппаратными средствами. ПК 2.4. Осуществлять обработку, хранение и передачу информации ограниченного доступа. ПК 3.2. Осуществлять эксплуатацию технических средств защиты информации в соответствии с требованиями эксплуатационной документации.	06.030 Профессиональный стандарт «Специалист по защите информации в телекоммуникационных системах и сетях», утвержден приказом Министерства труда и социальной защиты Российской Федерации от 3 ноября 2016 г. № 608н (зарегистрирован Министерством юстиции Российской Федерации 25 ноября 2016 г.,	Выполнение комплекса мер по обеспечению функционирования СССЭ исключением сетей связи специального назначения) и средств их защиты от НСД, 5 Обслуживание средств защиты информации в компьютерных	

Уровень аттестации (промежуточная/ГИА)	Код и наименование ФГОС СПО	Основные виды деятельности ФГОС СПО (ПМ)	Профессиональные компетенции (ПК) ФГОС СПО	Наименование профессионального стандарта (ПС)	Наименование и уровень квалификаций ПС	WSSS/модули/критерии оценки по КОД (по решению разработчика)
				<p>регистрационный № 44449) 06.032</p> <p>Профессиональный стандарт «Специалист по безопасности компьютерных систем и сетей», утвержден приказом Министерства труда и социальной защиты Российской Федерации от 1 ноября 2016 г. № 598н (зарегистрирован Министерством юстиции Российской Федерации 28 ноября 2016 г.,</p>	<p>системах и сетях, 5</p> <p>Обслуживание систем защиты информации в автоматизированных системах, 5</p>	

Уровень аттестации (промежуточная/ГИА)	Код и наименование ФГОС СПО	Основные виды деятельности ФГОС СПО (ПМ)	Профессиональные компетенции (ПК) ФГОС СПО	Наименование профессионального стандарта (ПС)	Наименование и уровень квалификаций ПС	WSSS/модули/критерии оценки по КОД (по решению разработчика)
				<p>регистрационный № 44464) 06.033</p> <p>Профессиональный стандарт «Специалист по защите информации в автоматизированных системах», утвержден приказом Министерства труда и социальной защиты Российской Федерации от 15 сентября 2016 г. № 522н (зарегистрирован Министерством юстиции Российской Федерации 28 сентября 2016 г.,</p>		



Уровень аттестации (промежуточная/ГИА)	Код и наименование ФГОС СПО	Основные виды деятельности ФГОС СПО (ПМ)	Профессиональные компетенции (ПК) ФГОС СПО	Наименование профессионального стандарта (ПС)	Наименование и уровень квалификаций ПС	WSSS/модули/критерии оценки по КОД (по решению разработчика)
				регистрационный № 43857)		
промежуточная/ ГИА	10.05.02 Информационная безопасность телекоммуникационных систем	эксплуатационная	<p>способностью выполнять установку, настройку, обслуживание, диагностику, эксплуатацию и восстановление работоспособности телекоммуникационного оборудования и приборов, технических и программно-аппаратных средств защиты телекоммуникационных сетей и систем (ПК-14);</p> <p>способностью проводить инструментальный мониторинг защищенности телекоммуникационных систем, обеспечения требуемого качества обслуживания (ПК-15).</p>	<p>06.030</p> <p>Профессиональный стандарт «Специалист по защите информации в телекоммуникационных системах и сетях», утвержден приказом Министерства труда и социальной защиты Российской Федерации от 3 ноября 2016 г. № 608н (зарегистрирован Министерством юстиции Российской Федерации 25 ноября 2016 г.,</p>	<p>Выполнение комплекса мер по обеспечению функционирования СССЭ исключением сетей связи специального назначения) и средств их защиты от НСД, 5</p> <p>Обслуживание средств защиты информации в компьютерных</p>	

Уровень аттестации (промежуточная/ГИА)	Код и наименование ФГОС СПО	Основные виды деятельности ФГОС СПО (ПМ)	Профессиональные компетенции (ПК) ФГОС СПО	Наименование профессионального стандарта (ПС)	Наименование и уровень квалификаций ПС	WSSS/модули/критерии оценки по КОД (по решению разработчика)
				<p>регистрационный № 44449) 06.032</p> <p>Профессиональный стандарт «Специалист по безопасности компьютерных систем и сетей», утвержден приказом Министерства труда и социальной защиты Российской Федерации от 1 ноября 2016 г. № 598н (зарегистрирован Министерством юстиции Российской Федерации 28 ноября 2016 г.,</p>	<p>системах и сетях, 5</p> <p>Обслуживание систем защиты информации в автоматизированных системах, 5</p>	

Уровень аттестации (промежуточная/ГИА)	Код и наименование ФГОС СПО	Основные виды деятельности ФГОС СПО (ПМ)	Профессиональные компетенции (ПК) ФГОС СПО	Наименование профессионального стандарта (ПС)	Наименование и уровень квалификаций ПС	WSSS/модули/критерии оценки по КОД (по решению разработчика)
				<p>регистрационный № 44464) 06.033</p> <p>Профессиональный стандарт «Специалист по защите информации в автоматизированных системах», утвержден приказом Министерства труда и социальной защиты Российской Федерации от 15 сентября 2016 г. № 522н (зарегистрирован Министерством юстиции Российской Федерации 28 сентября 2016 г.,</p>		

Уровень аттестации (промежуточная/ГИА)	Код и наименование ФГОС СПО	Основные виды деятельности ФГОС СПО (ПМ)	Профессиональные компетенции (ПК) ФГОС СПО	Наименование профессионального стандарта (ПС)	Наименование и уровень квалификаций ПС	WSSS/модули/критерии оценки по КОД (по решению разработчика)
				регистрационный № 43857)		
<b>промежуточная</b>	10.02.04 Обеспечение информационной безопасности и телекоммуникационных систем	4.3.3. Участие в организации работ по обеспечению информационной безопасности телекоммуникационных систем.	ПК 3.3. Участвовать во внедрении разработанных технических решений и проектов во взаимодействии с другими специалистами, оказывать техническую помощь исполнителям при изготовлении, монтаже, настройке, испытаниях и эксплуатации технических средств.	06.030 Профессиональный стандарт «Специалист по защите информации в телекоммуникационных системах и сетях», утвержден приказом Министерства труда и социальной защиты Российской Федерации от 3 ноября 2016 г. № 608н (зарегистрирован Министерством юстиции Российской Федерации 25 ноября 2016 г.,	Выполнение комплекса мер по обеспечению функционирования СССЭ исключением сетей связи специального назначения) и средств их защиты от НСД, 5 Обслуживание средств защиты информации в компьютерных	

Уровень аттестации (промежуточная/ГИА)	Код и наименование ФГОС СПО	Основные виды деятельности ФГОС СПО (ПМ)	Профессиональные компетенции (ПК) ФГОС СПО	Наименование профессионального стандарта (ПС)	Наименование и уровень квалификаций ПС	WSSS/модули/критерии оценки по КОД (по решению разработчика)
				<p>регистрационный № 44449) 06.032</p> <p>Профессиональный стандарт «Специалист по безопасности компьютерных систем и сетей», утвержден приказом Министерства труда и социальной защиты Российской Федерации от 1 ноября 2016 г. № 598н (зарегистрирован Министерством юстиции Российской Федерации 28 ноября 2016 г.,</p>	<p>системах и сетях, 5</p> <p>Обслуживание систем защиты информации в автоматизированных системах, 5</p>	

Уровень аттестации (промежуточная/ГИА)	Код и наименование ФГОС СПО	Основные виды деятельности ФГОС СПО (ПМ)	Профессиональные компетенции (ПК) ФГОС СПО	Наименование профессионального стандарта (ПС)	Наименование и уровень квалификаций ПС	WSSS/модули/критерии оценки по КОД (по решению разработчика)
				<p>регистрационный № 44464) 06.033</p> <p>Профессиональный стандарт «Специалист по защите информации в автоматизированных системах», утвержден приказом Министерства труда и социальной защиты Российской Федерации от 15 сентября 2016 г. № 522н (зарегистрирован Министерством юстиции Российской Федерации 28 сентября 2016 г.,</p>		

Уровень аттестации (промежуточная/ГИА)	Код и наименование ФГОС СПО	Основные виды деятельности ФГОС СПО (ПМ)	Профессиональные компетенции (ПК) ФГОС СПО	Наименование профессионального стандарта (ПС)	Наименование и уровень квалификаций ПС	WSSS/модули/критерии оценки по КОД (по решению разработчика)
				регистрационный № 43857)		
<b>промежуточная/ ГИА</b>	11.02.11 Сети связи и системы коммутации	<p>4.3.1. Техническая эксплуатация информационно-коммуникационных сетей связи.</p> <p>4.3.2. Обеспечение информационной безопасности телекоммуникационных систем и информационно-коммуникационных сетей связи.</p> <p>4.3.3. Техническая эксплуатация телекоммуникационных систем.</p>	<p>ПК 1.1. Выполнять монтаж и производить настройку сетей проводного и беспроводного абонентского доступа.</p> <p>ПК 1.2. Осуществлять работы с сетевыми протоколами.</p> <p>ПК 1.4. Выполнять монтаж и первичную инсталляцию компьютерных сетей.</p> <p>ПК 1.6. Производить администрирование сетевого оборудования.</p> <p>ПК 2.1. Использовать программно-аппаратные средства защиты информации в телекоммуникационных системах и сетях связи.</p> <p>ПК 2.2. Применять системы анализа защищенности для обнаружения уязвимости в сетевой инфраструктуре,</p>	Приказ Минтруда России от 05.10.2015 N 684н "Об утверждении профессионального стандарта "Системный администратор информационно-коммуникационных систем"	Администрирование прикладного программного обеспечения инфокоммуникационной системы организации, 5 Управление программно-аппаратными средствами информационных служб инфокоммуникационной системы организации, 6	

Уровень аттестации (промежуточная/ГИА)	Код и наименование ФГОС СПО	Основные виды деятельности ФГОС СПО (ПМ)	Профессиональные компетенции (ПК) ФГОС СПО	Наименование профессионального стандарта (ПС)	Наименование и уровень квалификаций ПС	WSSS/модули/критерии оценки по КОД (по решению разработчика)
			<p>выдавать рекомендации по их устранению.</p> <p>ПК 2.3. Обеспечивать безопасное администрирование телекоммуникационных систем и информационно-коммуникационных сетей связи.</p> <p>ПК 3.1. Выполнять монтаж оборудования телекоммуникационных систем.</p> <p>ПК 3.2. Проводить мониторинг и диагностику телекоммуникационных систем.</p> <p>ПК 3.3. Управлять данными телекоммуникационных систем.</p> <p>ПК 3.4. Устранять аварии и повреждения оборудования телекоммуникационных систем, выбирать методы восстановления его работоспособности.</p> <p>ПК 3.5. Выполнять монтаж и обеспечивать работу линий абонентского доступа и</p>		<p>Администрирование сетевой подсистемы инфокоммуникационной системы организации, 6</p> <p>Администрирование системного программного обеспечения инфокоммуникационной системы организации, 7</p> <p>Управление развитием инфокоммуникационной</p>	



Уровень аттестации (промежуточная/ГИА)	Код и наименование ФГОС СПО	Основные виды деятельности ФГОС СПО (ПМ)	Профессиональные компетенции (ПК) ФГОС СПО	Наименование профессионального стандарта (ПС)	Наименование и уровень квалификаций ПС	WSSS/модули/критерии оценки по КОД (по решению разработчика)
			<p>оконечных абонентских устройств.</p> <p>ПК 3.6. Решать технические задачи в области эксплуатации телекоммуникационных систем.</p>		<p>системы организации, 7</p>	



**Задание для демонстрационного экзамена по комплекту  
оценочной документации № 1.1 по компетенции № 39  
«Сетевое и системное администрирование» (образец)**

Задание включает в себя следующие разделы:

1. Формы участия
2. Модули задания, критерии оценки и необходимое время
3. Необходимые приложения

Продолжительность выполнения задания: 6 ч.

# 1. ФОРМЫ УЧАСТИЯ

Индивидуальный.

## 2. ЗАДАНИЕ

Содержанием экзаменационного задания являются работы по пуско-наладке сетевой инфраструктуры на базе современного сетевого оборудования и операционных систем семейства Windows и Linux. Участники экзамена получают инструкцию, сетевые диаграммы и методические рекомендации по выполнению. Экзаменационное задание имеет несколько модулей, выполняемых последовательно.

Задание демонстрационного экзамена является утвержденным. В нем присутствуют 3 из 5 модулей, т.е. возможно набрать максимально 45 из 100 баллов

Экзамен включает в себя Пуско-наладку инфраструктуры на основе ОС семейства Linux; Пуско-наладку инфраструктуры на основе ОС семейства Windows; Пуско-наладку телекоммуникационного оборудования.

Окончательная методика проверки уточняются членами жюри. Оценка производится в отношении работы модулей. Если участник экзамена не выполняет требования техники безопасности, подвергает опасности себя или других участников, такой участник может быть отстранен от экзамена.

Время и детали экзаменационного задания в зависимости от Экзаменационных условий могут быть изменены членами жюри, по согласованию с менеджером компетенции.

Экзаменационное задание должно выполняться по модульно, циклически по модулям А-В-С. Оценка каждого модуля происходит Ежедневно.

Задания разработаны и протестированы группой сертифицированных экспертов:

### 3. МОДУЛИ ЗАДАНИЯ И НЕОБХОДИМОЕ ВРЕМЯ

Модули и время приедены в таблице 1

Таблица 1 – Время выполнение модуля

п/п	Критерий	Модуль, в котором используется критерий	Время на выполнения модуля	Проверяемые разделы WSSS	Баллы		
					Судейская (если это применимо)	Объективная	Общая
1	A Linux Environments	A Linux Environments	2 часа	6	0	15	15
2	B Windows Environments	B Windows Environments	2 часа	1, 2, 3, 4, 5	0	15	15
3	C Cisco Environments	C Cisco Environments	2 часа	7	0	15	15
<b>Итого =</b>					<b>0</b>	<b>45</b>	<b>45</b>

#### **Модуль А: «Пусконаладка инфраструктуры на основе ОС семейства Linux»**

##### **ВВЕДЕНИЕ**

Умение работать с системами на основе открытого исходного кода становится все более важным навыком для тех, кто желает построить успешную карьеру в ИТ. Данное Экзаменационное 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.

##### **ОПИСАНИЕ ЭКЗАМЕНАЦИОННОГО ЗАДАНИЯ**

Данное Экзаменационное задание разработано с использованием различных открытых технологий, с которыми вы должны быть знакомы по сертификационным курсам LPIC и Red Hat. Задания поделены на следующие секции:

- Базовая конфигурация
- Конфигурация сетевой инфраструктуры
- Службы централизованного управления и журналирования
- Конфигурация служб удаленного доступа
- Конфигурация веб-служб

- Конфигурация служб хранения данных
- Конфигурация параметров безопасности и служб аутентификации

Секции независимы друг от друга, но вместе они образуют достаточно сложную инфраструктуру. Некоторые задания достаточно просты и понятны, некоторые могут быть неочевидными. Можно заметить, что некоторые технологии должны работать в связке или поверх других технологий. Например, динамическая маршрутизация должна выполняться поверх настроенного между организациями туннеля. Важно понимать, что если вам не удалось настроить полностью технологический стек, то это не означает, что работа не будет оценена. Например, для удаленного доступа необходимо настроить IPsec-туннель, внутри которого организовать GRE-туннель. Если, например, вам не удалось настроить IPsec, но вы смогли настроить GRE, то вы все еще получите баллы за организацию удаленного доступа.

## **ИНСТРУКЦИИ ДЛЯ УЧАСТНИКА**

В первую очередь необходимо прочитать задание полностью. Следует обратить внимание, что задание составлено не в хронологическом порядке. Некоторые секции могут потребовать действий из других секций, которые изложены ниже. На вас возлагается ответственность за распределение своего рабочего времени. Не тратьте время, если у вас возникли проблемы с некоторыми заданиями. Вы можете использовать временные решения (если у вас есть зависимости в технологическом стеке) и продолжить выполнение других задач. Рекомендуется тщательно проверять результаты своей работы.

Доступ ко всем виртуальным машинам настроен по аккаунту root:toor.

Если Вам требуется установить пароль, (и он не указан в задании) используйте: “P@ssw0rd”.

Виртуальная машина ISP преднастроена. Управляющий доступ участника к данной виртуальной машине для выполнения задания не предусмотрен. При попытке его сброса возникнут проблемы.

Организация LEFT включает виртуальные машины: L-SRV, L-FW, L-RTR-A, L-RTR-B, L-CLI-A, L-CLI-B.

Организация RIGHT включает виртуальные машины: R-SRV, R-FW, R-RTR, R-CLI.

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

Ожидается, что Экзаменационное задание выполнимо Участником с привлечением оборудования и материалов, указанных в Инфраструктурном Листе.

В качестве системной ОС в организации **LEFT** используется **Debian**

В качестве системной ОС в организации **RIGHT** используется **CentOS**

Вам доступен диск CentOS-7-x86\_64-Everything-1810.iso

Вам доступен диск debian-10.0.0-amd64-BD-1.iso

Вам доступен диск debian-10.0.0-amd64-BD-2.iso

Вам доступен диск debian-10.0.0-amd64-BD-3.iso

Вам доступен диск debian-10.0.0-amd64-BD-4.iso

Вам доступен диск Additional.iso, на котором располагаются недостающие RPM пакеты

Внимание! Все указанные компоненты предоставляются участникам в виде ISO-файлов на локальном или удаленном хранилище.

Участники не имеют права пользоваться любыми устройствами, за исключением находящихся на рабочих местах устройств, предоставленных организаторами.

Участники не имеют права приносить с собой на рабочее место заранее подготовленные текстовые материалы.

В итоге участники должны обеспечить наличие и функционирование в соответствии с заданием служб и ролей на указанных виртуальных машинах. При этом участники могут самостоятельно выбирать способ настройки того или иного компонента, используя предоставленные им ресурсы по своему усмотрению.

### СХЕМА ОЦЕНКИ

Каждый субкритерий имеет приблизительно одинаковый вес. Пункты внутри каждого критерия имеют разный вес, в зависимости от сложности пункта и количества пунктов в субкритерии.

Схема оценка построена таким образом, чтобы каждый пункт оценивался только один раз. Например, в секции «Базовая конфигурация» предписывается настроить имена для всех устройств, однако этот пункт будет проверен только на одном устройстве и оценен только 1 раз. Одинаковые пункты могут быть проверены и оценены больше чем 1 раз, если для их выполнения применяются разные настройки или они выполняются на разных классах устройств.

Подробное описание методики проверки должно быть разработано экспертами, принимавшими участие в оценке экзаменационного задания, и вынесено в

отдельный документ. Данный документ, как и схема оценки, является объектом внесения 30% изменений.

### Конфигурация хостов

- 1) Настройте имена хостов в соответствии с Диаграммой.
- 2) Установите следующее ПО на ВСЕ виртуальные машины:
  - a) Tcprdump
  - b) Net-tools
  - c) Curl
  - d) Vim
  - e) Lynx
  - f) Dhclient
  - g) Bind-utils
  - h) Nfs-utils
  - i) Cifs-utils
  - j) Sshpass
- 3) На хостах сформируйте файл /etc/hosts в соответствии с Диаграммой (кроме адреса хоста L-CLI-A). Данный файл будет применяться во время проверки в случае недоступности DNS-сервисов. Проверка по IP-адресам выполняться не будет.
- 4) В случае корректной работы DNS-сервисов ответы DNS должны иметь более высокий приоритет.
- 5) Все хосты должны быть доступны аккаунту root по SSH на стандартном(22) порту

### Конфигурация сетевой инфраструктуры

- 1) Настройте IP-адресацию на ВСЕХ хостах в соответствии с Диаграммой.
- 2) Настройте сервер протокола динамической конфигурации хостов для L-CLI-A и L-CLI-B
- 3) В качестве DHCP-сервера организации LEFT используйте L-RTR-A.
  - a) Используйте пул адресов 172.16.100.65 — 172.16.100.75 для сети L-RTR-A

- b) Используйте пул адресов 172.16.200.65 — 172.16.200.75 для сети L-RTR-B
- 4) Используйте адрес L-SRV в качестве адреса DNS-сервера.
- 5) Настройте DHCP-сервер таким образом, чтобы L-CLI-B всегда получал фиксированный IP-адрес в соответствии с Диаграммой.
  - a) В качестве шлюза по умолчанию используйте адрес интерфейса соответствующего маршрутизатора в локальной сети.
- 6) Используйте DNS-суффикс skill39.wsr.
  - a) DNS-записи типа A и PTR соответствующего хоста должны обновляться при получении им адреса от DHCP-сервера.
- 7) На L-SRV настройте службу разрешения доменных имен
  - a) Сервер должен обслуживать зону skill39.wsr.
  - b) Сопоставление имен организовать в соответствии с Таблицей 1.
  - c) Запросы, которые выходят за рамки зоны skill39.wsr должны пересылаться DNS-серверу ISP. Для проверки используйте доменное имя ya.ru.
  - d) Реализуйте поддержку разрешения обратной зоны.
  - e) Файлы зон располагать в /opt/dns/
- 8) На L-FW и R-FW настройте интернет-шлюзы для организации коллективного доступа в Интернет.
  - a) Настройте трансляцию сетевых адресов из внутренней сети в адрес внешнего интерфейса.
  - b) Организуйте доступность сервиса DNS на L-SRV по внешнему адресу L-FW.
  - c) Сервер L-FW должен перенаправлять внешние DNS запросы от OUT-CLI на L-SRV. www.skill39.wsr должен преобразовываться во внешний адрес R-FW.

#### Службы централизованного управления и журналирования

- 1) Разверните LDAP-сервер для организации централизованного управления учетными записями
  - a) В качестве сервера выступает L-SRV.
  - b) Учетные записи создать в соответствии с Таблицей 2.
  - c) Группы(LDAP) и пользователей создать в соответствии с Таблицей 2.



- d) L-CLI-A, L-SRV и L-CLI-B должны аутентифицироваться через LDAP.
- 2) На L-SRV организуйте централизованный сбор журналов с хостов L-FW, L-SRV.
  - a) Журналы должны храниться в директории /opt/logs/.
  - b) Журналирование должно производиться в соответствии с Таблицей 3.

#### Конфигурация служб удаленного доступа

1) На L-FW настройте сервер удаленного доступа на основе технологии OpenVPN:

- a) В качестве сервера выступает L-FW
- b) Параметры туннеля.
  - i) Устройство TUN.
  - ii) Протокол UDP.
  - iii) Применяется сжатие.
  - iv) Порт сервера 1122.
- c) Ключевая информация должна быть сгенерирована на R-FW.
- d) В качестве адресного пространства подключаемых клиентов использовать сеть 5.5.5.0/27.
- e) Хранение всей необходимой (кроме конфигурационных файлов) информации организовать в /opt/vpn.
- f) Подключившийся клиент должен быть автоматически сконфигурирован на использование DNS-инфраструктуры предприятия.

2) На OUT-CLI настройте клиент удаленного доступа на основе технологии OpenVPN:

- a) Запуск удаленного подключения должен выполняться скриптом start\_vpn.sh
  - i) Отключение VPN-туннеля должно выполняться скриптом stop\_vpn.sh.
  - ii) Скрипты должны располагаться в /opt/vpn.
  - iii) Скрипты должны вызываться из любого каталога без указания пути.
  - iv) Используйте следующий каталог для расположения файлов скриптов /opt/vpn/.

3) Настройте защищенный канал передачи данных между L-FW и R-FW с помощью технологии IPSEC:

a) Параметры политики первой фазы IPsec:

- i) Проверка целостности SHA-1
- ii) Шифрование 3DES
- iii) Группа Диффи-Хеллмана — 14 (2048)
- iv) Аутентификация по общему ключу WSR-2019

b) Параметры преобразования трафика для второй фазы IPsec:

- i) Протокол ESP
- ii) Шифрование AES
- iii) Проверка целостности SHA-2

c) В качестве трафика, разрешенного к передаче через IPsec-туннель, должен быть указан только GRE-трафик между L-FW и R-FW

4) Настройте GRE-туннель между L-FW и R-FW:

a) Используйте следующую адресацию внутри GRE-туннеля:

- i) L-FW: 10.5.5.1/30
- ii) R-FW: 10.5.5.2/30

5) Настройте динамическую маршрутизацию по протоколу OSPF с использованием пакета FRR:

a) Анонсируйте все сети, необходимые для достижения полной связности.

b) Применение статических маршрутов не допускается.

c) В обмене маршрутной информацией участвуют L-RTR-A, L-RTR-B, R-RTR, L-FW и R-FW.

d) Соседство и обмен маршрутной информацией между L-FW и R-FW должно осуществляться исключительно через настроенный GRE-туннель.

e) Анонсируйте сети локальных интерфейсов L-RTR-A и L-RTR-B.

6) На L-FW настройте удаленный доступ по протоколу SSH:

a) Доступ ограничен пользователями ssh\_p, root и ssh\_c

i) В качестве пароля пользователь (кроме root) использовать ssh\_pass.

ii) root использует стандартный пароль

b) SSH-сервер должен работать на порту 22

7) На OUT-CLI настройте клиент удаленного доступа SSH:

a) Доступ к L-FW из под локальной учетной записи root под учетной записью ssh\_r должен происходить с помощью аутентификации на основе открытых ключей.

### Конфигурация веб-служб

- 1) На R-SRV установите и настройте веб-сервер apache:
  - a) Настройте веб-сайт для внешнего пользования www.skill39.wsr.
    - i) Используйте директорию /var/www/html/out.
    - ii) Используйте порт 80.
    - iii) Сайт предоставляет доступ к двум файлам.
  - 2) Документ index.html должен содержать:
    - a) "Hello, www.skill39.wsr is here!"
  - 3) Документ date.php (исполняемый PHP-скрипт) должен содержать:
    - a) Вызов функции date('Y-m-d H:i:s')

### Конфигурация служб хранения данных

- 1) Реализуйте синхронизацию каталогов на основе демона rsyncd.
  - a) В качестве сервера синхронизации используется L-SRV.
    - i) Для работы синхронизации создайте специального пользователя mrsync
  - 2) В качестве пароля используйте тоор.
    - a) Домашний каталог данного пользователя должен быть расположен в /opt/sync/. Данный каталог используйте как каталог синхронизации
    - b) Домашний каталог не должен содержать никакой посторонней информации.
    - c) Для выполнения синхронизации создайте rsync-пользователя sync с паролем parol666.
    - d) Подключение к rsyncd должны быть разрешены исключительно от клиентов L-CLI-A и L-CLI-B
  - 3) В качестве клиентов используются L-CLI-A и L-CLI-B
    - a) Синхронизируемый каталог располагается по адресу /root/sync/
    - b) Каталоги должны быть зеркально идентичны по содержимому.
    - c) Реализуйте синхронизацию в виде скрипта:
      - i) Скрипт находится по адресу /root/sync.sh

ii) Автоматизация скрипта реализована средствами cron пользователя root.

iii) Выполнение производится каждую минуту.

### Конфигурация параметров безопасности и служб аутентификации

- 1) Настройте CA на R-FW, используя OpenSSL.
  - a) Используйте /etc/ca в качестве корневой директории CA
  - b) Атрибуты CA должны быть следующими:
    - i) Страна RU
    - ii) Организация WorldSkills Russia
    - iii) CN должен быть установлен как WSR CA
  - c) Создайте корневой сертификат CA
  - d) Все клиентские операционные системы должны доверять CA
- 2) Настройте межсетевой экран iptables на L-FW и firewalld на R-FW
  - a) Запретите прямое попадание трафика из сетей в Internal
  - b) Разрешите удаленные подключения с использованием OpenVPN на внешний интерфейс маршрутизатора L-FW
  - c) Разрешите необходимый трафик для создания IPSec и GRE туннелей между организациями
  - d) Разрешите SSH подключения на соответствующий порт
  - e) Для VPN-клиентов должен быть предоставлен полный доступ к сети Internal
  - f) Разрешите необходимый трафик к серверам L-SRV и R-SRV для работы настроенных сервисов.
  - g) Остальные сервисы следует запретить.
  - h) В отношении входящих (из внешней сети) ICMP запросов поступать по своему усмотрению

Хост	DNS-имя
L-CLI-A	A,PTR: l-cli-a.skill39.wsr
L-CLI-B	A,PTR: l-cli-b.skill39.wsr
L-SRV	A,PTR: l-srv.skill39.wsr CNAME: server.skill39.wsr
L-FW	A: l-fw.skill39.wsr
R-FW	A: r-fw.skill39.wsr CNAME: www.skill39.wsr
R-SRV	A,PTR: r-srv.skill39.wsr

Таблица 2 – Учетные записи LDAP

Группа	CN	Пароль
Admin	tux	toor
Guest	user	P@ssw0rd

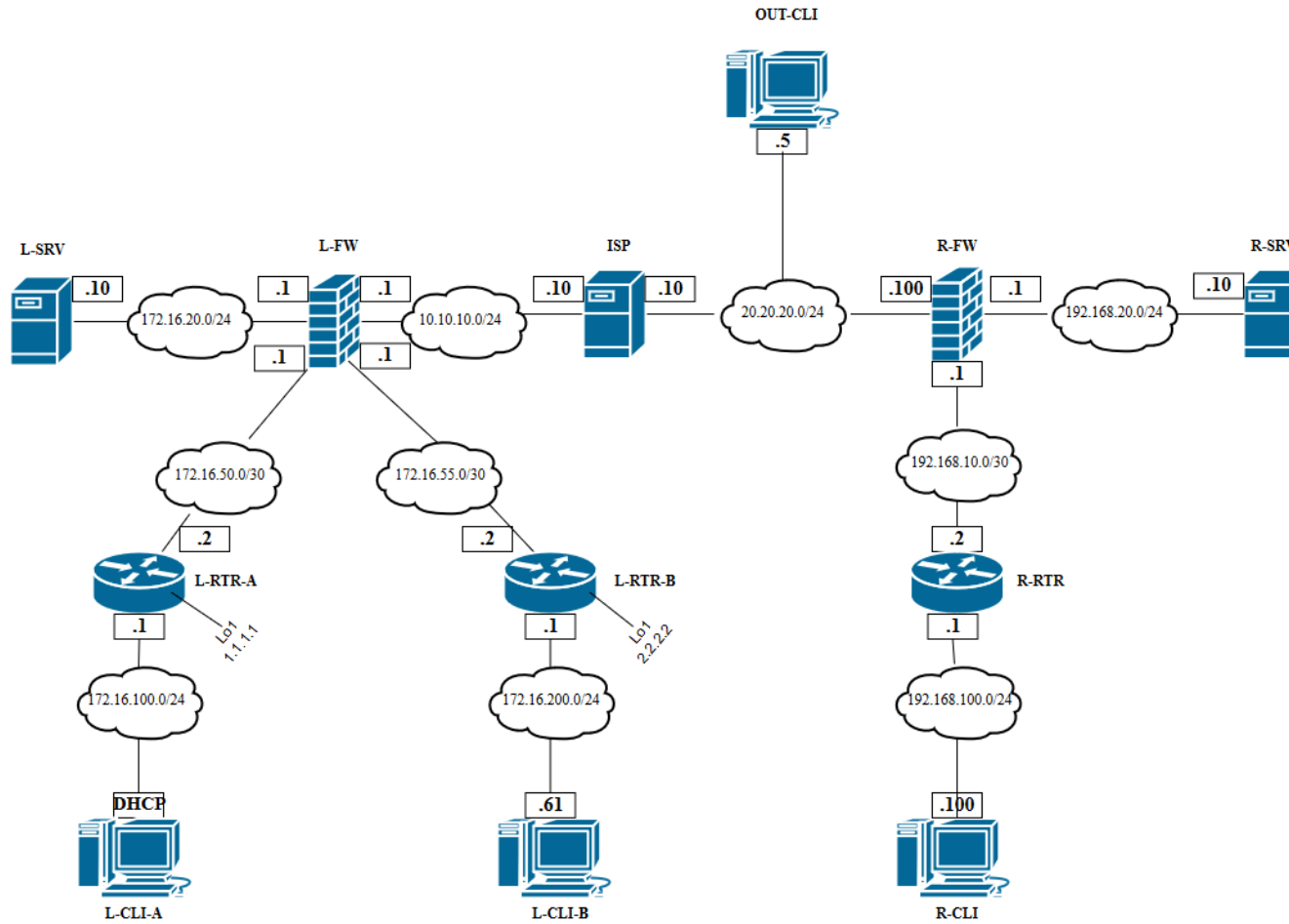
Таблица 3 – Правила журналирования

Источник	Уровень журнала (строгое соответствие)	Файл
L-SRV	auth.*	/opt/logs/<HOSTNAME>/auth.log
L-FW	*.err	/opt/logs/<HOSTNAME>/error.log

\*<HOSTNAME> - название директории для журналируемого хоста

\*\*В директории /opt/logs не должно быть файлов, кроме тех, которые указаны в таблице

# ДИАГРАММА ВИРТУАЛЬНОЙ СЕТИ



Модуль В: «Пусконаладка инфраструктуры на основе ОС семейства Windows»

Версия 2 от 31.07.19.

## **ВВЕДЕНИЕ**

На выполнение задания отводится ограниченное время – подумайте, как использовать его максимально эффективно. Составьте план выполнения работ. Вполне возможно, что для полной работоспособности системы в итоге действия нужно выполнять не строго в той последовательности, в которой они описаны в данном Экзаменационном задании.

В рамках легенды экзаменационного задания Вы – системный администратор компании, находящейся в городе Казань. В главном офисе вы управляете доменом *Kazan.wsr*. Вам необходимо настроить сервисы в локальной сети головного офиса.

Компания, в которой вы работаете, хочет выйти на рынки северной Европы. Для этого она устанавливает партнерские отношения с одной из компаний, находящейся в Санкт-Петербурге. Вам нужно помочь администратору партнерской компании с настройкой своего домена (*SPB.wse*), а потом настроить между доменами доверие.

Также Вам предстоит настроить канал связи между офисами с помощью статических маршрутов.

Внимательно прочтите задание от начала до конца – оно представляет собой целостную систему. При первом доступе к операционным системам либо следуйте указаниям мастера, либо используйте следующие реквизиты: *Administrator/P@ssw0rd*.

Если предоставленные виртуальные машины начнут самопроизвольно отключаться в процессе работы, попробуйте выполнить на них команду *slmgr /rearm* или обратитесь к техническому эксперту.

## **КОМПЛЕКТАЦИЯ ЭКЗАМЕНАЦИОННОГО ЗАДАНИЯ**

### **1. Текстовые файлы:**

- данный файл с Экзаменационным заданием;
- файл дополнений к Экзаменационному заданию, содержащий: описание вида предустановок, описание используемых операционных систем, а также рекомендации по выделению ресурсов для виртуальных машин.

## 2. Программное обеспечение:

- Windows10.ADMX.

Участники не имеют права пользоваться любыми устройствами, за исключением находящихся на рабочих местах устройств, предоставленных организаторами.

Участники не имеют права приносить с собой на рабочее место заранее подготовленные текстовые материалы.

В итоге участники должны обеспечить наличие и функционирование в соответствии с заданием служб и ролей на указанных виртуальных машинах. При этом участники могут самостоятельно выбирать способ настройки того или иного компонента, используя предоставленные им ресурсы по своему усмотрению.



## **Настройка DC1**

### **Базовая настройка**

- 1) переименуйте компьютер в DC1;
- 2) в качестве адреса DC1 используйте первый возможный адрес из подсети 172.16.19.64/26;
- 3) обеспечьте работоспособность протокола ICMP (для использования команды ping), при этом Windows Firewall должен быть включен для всех сетевых профилей.

### **Active Directory**

- 1) сделайте сервер контроллером домена Kazan.wsr.

### **DHCP**

- 1) настройте протокол DHCP для автоконфигурации клиентов – в качестве диапазона выдаваемых адресов используйте все незанятые серверами адреса в подсети;
- 2) настройте failover: mode – Load balancer, partner server – SRV1, state switchover – 5 min;
- 3) настройте дополнительные свойства области (адреса DNS-серверов и основного шлюза).

### **DNS**

- 1) настройте необходимые зоны прямого и обратного просмотра;
- 2) создайте все необходимые записи типа A и PTR для серверов домена и необходимых web-сервисов;
- 3) обеспечьте разрешение имен сайтов обеих компаний.

### **GPO**

- 1) запретите анимацию при первом входе пользователей в систему на всех клиентских компьютерах домена;
- 2) члены группы IT должны быть членами группы локальных администраторов на всех клиентских компьютерах домена;

3) в браузерах IE Explorer и Microsoft Edge должна быть настроена стартовая страница – [www.kazan.wsr](http://www.kazan.wsr);

4) пользователи домена при обращении к общим папкам, на доступ которым у них нет разрешений, должны получать вместо стандартного уведомления следующего вида: «You do not have permissions to use this path - [путь к папке]! Do not try it again!».

## **Элементы доменной инфраструктуры**

1) создайте подразделения: IT и Sales;

2) в соответствующих подразделениях создайте одноименные доменные группы.

3) в каждой группе создайте с помощью скрипта по 30 пользователей. Все учетные записи должны иметь возможность входа в домен с логином, созданным по следующему шаблону *НазваниеГруппы\_ПорядковыйНомерПользователя@kazan.wsr*. В качестве пароля используйте P@ssw0rdX, где X – номер пользователя. Все учетные записи пользователей должны быть включены. Вход в систему должен быть обеспечен для всех пользователей со всех клиентских компьютеров домена и рядовых серверов.

4) для каждого пользователя, члена группы IT, создайте автоматически подключаемую в качестве диска U:\ домашнюю папку внутри папки по адресу SRV1→*d:\shares\IT*;

5) все пользователи при первом входе в домен с компьютера CL11 должны видеть на рабочем столе ярлык программы *Калькулятор*.

## **Настройка SRV1**

### **Базовая настройка**

1) переименуйте компьютер в SRV1;

2) в качестве адреса SRV1 используйте второй возможный адрес из подсети 172.16.19.64/26;

3) обеспечьте работоспособность протокола ICMP (для использования команды ping), при этом Windows Firewall должен быть включен для всех сетевых профилей.

4) с помощью дополнительных жестких дисков создайте RAID-5 массив; назначьте ему букву D:\.

## **Active Directory**

- 1) сделайте сервер дополнительным контроллером домена Kazan.wsr;
- 2) сервер должен быть контроллером домена только для чтения.

## **DHCP**

- 1) настройте протокол DHCP для автоконфигурации клиентов;
- 2) настройте failover: mode – Load balancer, partner server – DC1, state switchover – 5 min.

## **DNS**

- 1) сделайте сервер дополнительным DNS-сервером в домене Kazan.wsr;
- 2) загрузите с DC1 все зоны прямого и обратного просмотра;

## **Общие папки**

1) создайте общие папки для подразделений (IT, Sales) по адресу SRV1→*d:\shares\departments*. Просматривать и редактировать файлы в папках могут только члены соответствующей группы.

2) обеспечьте привязку общей папки подразделения к соответствующей группе пользователей в качестве диска G:\.

## **Квоты/Файловые экраны**

1) установите максимальный размер в 2 Gb для каждой домашней папки пользователя (U:\);

2) запретите хранение в домашних папках пользователей файлов с расширениями .mp3 и .wav; учтите, что файлы остальных типов пользователи вправе хранить в домашних папках.

## **IIS**

1) создайте сайт компании со стартовой страницей следующего содержания:

<html>

Welcome to Kazan!

</html>;

2) сайт должен быть доступен по имени `www.kazan.wsr` по протоколам `http` и `https` в обоих сетевых сегментах с использованием сертификатов, выданных DCA.

## Настройка DCA

### Базовая настройка

- 1) переименуйте компьютер в DCA;
- 2) в качестве адреса DCA используйте третий возможный адрес из подсети `172.16.19.64/26`;
- 3) обеспечьте работоспособность протокола ICMP (для использования команды `ping`), при этом Windows Firewall должен быть включен для всех сетевых профилей;
- 4) присоедините компьютер к домену `Kazan.wsr`.

### Службы сертификации

- 1) установите службы сертификации;
- 2) настройте основной доменный центр сертификации;
- 3) имя центра сертификации – `RootKazanCA`;
- 4) срок действия сертификата – 8 лет;
- 5) настройте шаблон выдаваемого сертификата для клиентских компьютеров `ClientComps`: `subject name=common name`, автозапрос только для компьютера R1;
- 6) настройте шаблон выдаваемого сертификата `ITUsers`: `subject name=common name`, автозапрос только для пользователей – членов группы IT.

## Настройка CLI1

### Базовая настройка

- 1) переименуйте компьютер в CLI1;

2) обеспечьте работоспособность протокола ICMP (для использования команды ping), при этом Windows Firewall должен быть включен для всех сетевых профилей;

3) присоедините компьютер к домену *Kazan.wsr*;

4) запретите использование «спящего режима» таким образом, чтобы пользователи домена не могли изменить эту настройку без участия администратора домена;

5) используйте компьютер для тестирования настроек в домене *Kazan.wsr*: пользователей, общих папок, групповых политик.

## **Настройка DC2**

### **Базовая настройка**

1) переименуйте компьютер в DC2;

2) в качестве адреса DC2 используйте первый возможный адрес из подсети 172.16.20.96/27;

3) обеспечьте работоспособность протокола ICMP (для использования команды ping), при этом Windows Firewall должен быть включен для всех сетевых профилей.

### **Active Directory**

1) сделайте сервер контроллером домена *SPB.wse*;

2) настройте двустороннее доверие доменом *Kazan.wsr*.

### **DHCP**

1) настройте протокол DHCP для автоконфигурации клиентов – в качестве диапазона выдаваемых адресов используйте все незанятые серверами адреса в подсети.

### **DNS**

1) настройте необходимые зоны прямого и обратного просмотра;

2) создайте вручную все необходимые записи типа A и PTR для серверов домена и необходимых web-сервисов;

- 3) обеспечьте разрешение имен сайтов обеих компаний.

## **Элементы доменной инфраструктуры**

- 1) создайте учетную запись пользователя домена *User1\P@ssw0rd*, используйте группу по умолчанию – *Domain Users*.
- 2) для всех пользовательских учетных записей в домене используйте перемещаемые профили;
- 3) для хранения профилей пользователей используйте общую папку по адресу *SRV2→c:\profiles*;
- 4) каждый пользователь должен иметь доступ к файлам только своего профиля; при обращении к указанной общей папке средствами программы *Проводник* пользователь должен видеть в списке только папку со своим профилем.

## **GPO**

- 1) настройте необходимые политики, обеспечивающие использование сервера *DCA.kazan.wsr* в качестве доверенного центра сертификации.

## **Настройка SRV2**

### **Базовая настройка**

- 1) переименуйте компьютер в *SRV2*;
- 2) в качестве адреса *SRV1* используйте второй возможный адрес из подсети *172.16.20.96/27*;
- 3) обеспечьте работоспособность протокола *ICMP* (для использования команды *ping*), при этом *Windows Firewall* должен быть включен для всех сетевых профилей;
- 4) присоедините компьютер к домену *SPB.wse*.

## **IIS**

- 1) создайте сайт компании со стартовой страницей следующего содержания:

<html>

*Welcome to Saint-Petersburg!*

</html>;

2) сайт должен быть доступен по имени [www.spb.wse](http://www.spb.wse), по протоколам http https в обоих сетевых сегментах с использованием сертификатов, выданных DCA.

## **Настройка CLI2**

### **Базовая настройка**

- 1) переименуйте компьютер в CLI2;
- 2) обеспечьте работоспособность протокола ICMP (для использования команды ping), при этом Windows Firewall должен быть включен для всех сетевых профилей;
- 3) присоедините компьютер к домену *SPB.wse*.
- 4) запретите использование «спящего режима» таким образом, чтобы пользователи домена не могли изменить эту настройку без участия администратора домена;
- 5) используйте компьютер для тестирования настроек в домене *SPB.wse*.

## **Настройка R2**

### **Базовая настройка**

- 1) переименуйте компьютер в R2;
- 2) задайте настройки сети следующим образом: для сетевого интерфейса, подключенного к коммутатору ISP, используйте адрес 200.100.100.1/30; для сетевого адреса в подсети *SPB.wse* используйте последний возможный адрес из используемого адресного пространства;
- 3) обеспечьте работоспособность протокола ICMP (для использования команды ping), при этом Windows Firewall должен быть включен для всех сетевых профилей;
- 4) присоедините компьютер к домену *SPB.wse*.

## **Настройка RRAS**

- 1) установите службу RRAS;
- 2) настройте статические маршруты для связи с сетевым сегментом в Казани.

## **Настройка R1**

### **Базовая настройка**

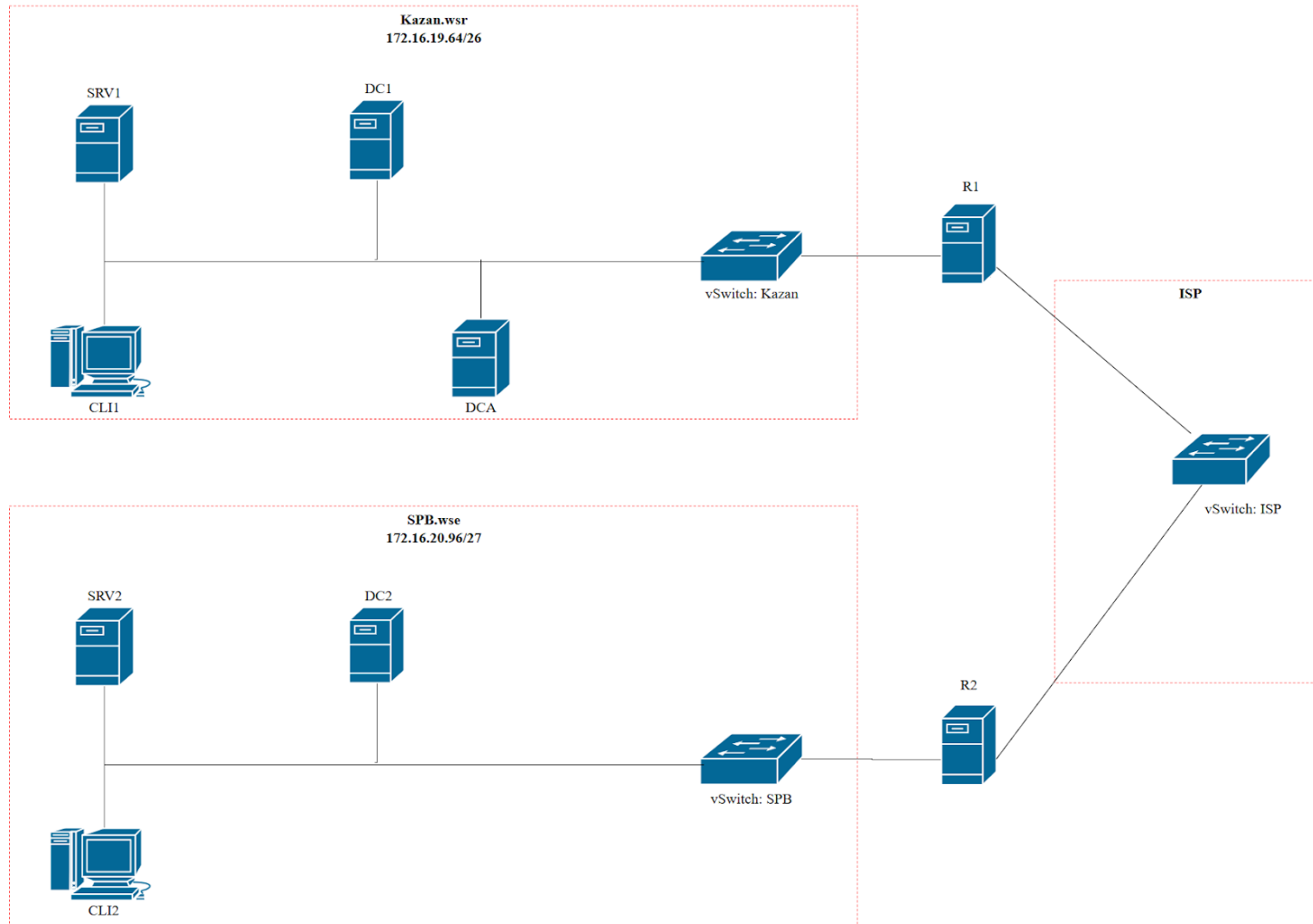
- 1) переименуйте компьютер в R1;
- 2) задайте настройки сети следующим образом: для сетевого интерфейса, подключенного к подключенного к коммутатору ISP, используйте адрес 200.100.100.2/30; для сетевого адреса в подсети Kazan.wsr используйте последний возможный адрес из используемого адресного пространства;
- 3) обеспечьте работоспособность протокола ICMP (для использования команды ping), при этом Windows Firewall должен быть включен для всех сетевых профилей;
- 4) присоедините компьютер к домену Kazan.wsr.

## **Настройка RRAS**

- 1) установите службу RRAS;
- 2) настройте статические маршруты для связи с сетевым сегментом в Санкт-Петербурге.



# ДИАГРАММА ВИРТУАЛЬНОЙ СЕТИ



## **Модуль С: «Пусконаладка телекоммуникационного оборудования»**

### **Версия 5 от 24.09.19.**

#### **ВВЕДЕНИЕ**

Знание сетевых технологий на сегодняшний день становится незаменимым для тех, кто хочет построить успешную карьеру в области ИТ. Данное Экзаменационное 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.

#### **ОПИСАНИЕ ЭКЗАМЕНАЦИОННОГО ЗАДАНИЯ**

Данное Экзаменационное задание разработано с учетом различных сетевых технологий, соответствующих уровням сертификации CCNA R/S. Задание разбито на следующие секции:

- Базовая настройка
- Настройка коммутации
- Настройка подключений к глобальным сетям
- Настройка маршрутизации
- Настройка служб
- Настройка механизмов безопасности
- Настройка параметров мониторинга и резервного копирования
- Конфигурация виртуальных частных сетей

Все секции являются независимыми друг от друга, но вместе образуют достаточно сложную сетевую инфраструктуру. Некоторые задания достаточно просты и понятны, некоторые могут быть неочевидными. Можно заметить, что некоторые технологии должны работать в связке или поверх других технологий. Например, может подразумеваться, что IPv6 маршрутизация должна работать поверх настроенной виртуальной частной сети, которая, в свою очередь, должна работать поверх IPv4 маршрутизации, которая, в свою очередь, должна работать поверх PPPoE и Multilink и т.д. Очень важно понимать, что если вам не удастся решить какую-либо из задач по середине такого технологического стека, это

не значит, что решенные задачи не будут оценены. Например, если вы не можете настроить динамическую маршрутизацию IPv4, которая необходима для работы виртуальной частной сети, вы можете использовать статическую маршрутизацию и продолжать работу над настройкой виртуальной частной сети и всем что должно работать поверх нее. В этом случае вы не получите баллы за динамическую маршрутизацию, но вы получите баллы за всё что должно работать поверх нее (в случае если функциональные тесты пройдены успешно).

### **ИНСТРУКЦИИ ДЛЯ УЧАСТНИКА**

В первую очередь необходимо прочитать задание полностью и составить алгоритм выполнения работы. Вам предстоит вносить изменения в действующую, преднастроенную сетевую инфраструктуру предприятия, состоящую из головного офиса HQ и удаленного офиса BR1. Офисы имеют связь через провайдеров ISP1 и ISP2. Вы не имеете доступа к оборудованию провайдеров, оно полностью настроено и не требует дополнительного конфигурирования. Вам необходимо настраивать оборудование предприятия, а именно: SW1, SW2, SW3, HQ1, FW1 и BR1.

У вас отсутствует консольный доступ к устройствам, будьте очень внимательны при выполнении задания! В случае потери связи с оборудованием, вы будете виноваты сами. Разрешается перезагрузка оборудования – только техническими экспертами. Например, применили неправильный ACL, который закрыл доступ по telnet, но вы не успели сохранить конфигурацию.

Руководствуйтесь пословицей: Семь раз отмерь, один раз отрежь. Для выполнения задания у вас есть одна физическая машина (PC1 с доступом по Telnet и установленным ASDM), которую вы должны использовать в качестве:

PC2 Виртуальный ПК, Windows 10, Putty. Пользователь User пароль P@ssw0rd

SRV1 Виртуальный ПК, Debian пользователь root пароль toor, с предустановленными сервисами

1) SysLog папка для проверки /Cisco\_Log

2) RADIUS - FreeRadius

3) SNMP – для проверки используется пакет Net-SNMP используйте команду snmp\_test

4) NTP

5) TFTP папка для проверки /Cisco\_TFTP

Следует обратить внимание, что задание составлено не в хронологическом порядке. Некоторые секции могут потребовать действий из других секций, которые изложены ниже. Например, задание 3 в секции «Настройка служб» предписывает вам настроить службу протокола автоматической конфигурации хостов, которая, разумеется, не будет работать пока не будут выполнены необходимые настройки в секции «Конфигурация коммутации». На вас возлагается ответственность за распределение своего рабочего времени.

Не тратьте время, если у вас возникли проблемы с некоторыми заданиями. Вы можете использовать временные решения (если у вас есть зависимости в технологическом стеке) и продолжить выполнение других задач. Рекомендуется тщательно проверять результаты своей работы.

Убедитесь в том, что ваши настройки на всех устройствах функционируют после перезагрузки всего оборудования.

### ПОДКЛЮЧЕНИЕ К УСТРОЙСТВАМ

Для первоначального подключения используйте протокол Telnet. Для подключения к FW1 используете учетную запись с логином: cisco и паролем: cisco, для входа в привилегированный режим используйте пароль cisco. Для подключения к остальным сетевым устройствам используйте пароль: cisco и пароль для привилегированного режима: cisco

Для подключения к устройствам в главном офисе HQ, подключите рабочую станцию к порту F0/10 коммутатора SW2 и настройте адрес в соответствии с диаграммой L3, устройства доступны по следующим адресам:

SW1 – 192.168.254.10

SW2 – 192.168.254.20

SW3 – 192.168.254.30

HQ1 – 192.168.254.1

FW1 – 192.168.254.2

BR1 – 192.168.254.3

### ОЦЕНКА

Оценка осуществляется по SSH или Telnet с устройства PC1. Проверочная группа не осуществляет перекоммутацию на стенде, поэтому будьте предельно внимательны, перед завершением выполнения экзаменационного задания и верните коммутацию в исходное состояние. А также убедитесь, что устройства доступны по

следующим адресам, по SSH или Telnet с учетными записями соответствующим экзаменационному заданию:

SW1 – 10.100.100.10 или 192.168.254.10

SW2 – 10.100.100.20 или 192.168.254.20

SW3 – 10.100.100.30 или 192.168.254.30

HQ1 – 30.78.21.1 или 192.168.254.1

FW1 – 30.78.87.2 или 192.168.254.2

BR1 – 172.16.3.3 или 172.16.1.2 или 3.3.3.3 или 192.168.254.3

### **Базовая настройка**

- 1) Задайте имя всех устройств в соответствии с топологией.
- 2) Назначьте для всех устройств доменное имя worldskills.ru
- 3) Создайте на всех устройствах пользователей wsruser с паролем network
  - a) Пароль пользователя должен храниться в конфигурации в виде результата хэш-функции.
  - b) Пользователь должен обладать максимальным уровнем привилегий.
- 4) На всех устройствах установите пароль wsg на вход в привилегированный режим.
  - a) Пароль должен храниться в конфигурации в виде результата хэш-функции.
- 5) Настройте режим, при котором все пароли в конфигурации хранятся в зашифрованном виде. На FW1 используйте шифрование AES.
- 6) Для всех устройств реализуйте модель AAA.
  - a) Аутентификация на линиях виртуальных терминалов с 0 по 15 должна производиться с использованием локальной базы учётных записей. (кроме маршрутизатора HQ1)
  - b) После успешной аутентификации при удалённом подключении пользователи сразу должны получать права, соответствующие их уровню привилегий или роли (кроме межсетевого экрана FW1).
  - c) Настройте необходимость аутентификации на локальной консоли.
  - d) При успешной аутентификации на локальной консоли пользователи должны сразу должны получать права, соответствующие их уровню привилегий или роли.

- 7) На устройствах, к которым разрешен доступ, в соответствии с топологиями L2 и L3, создайте виртуальные интерфейсы, подинтерфейсы и интерфейсы типа петля, назначьте IP-адреса.
- 8) На маршрутизаторе HQ1 на виртуальных терминальных линиях с 0 по 15 настройте аутентификацию с использованием RADIUS-сервера.
  - a) Используйте на линиях vty с 0 по 15 отдельный список методов с названием `method_map`
  - b) Порядок аутентификации:
    - i) По протоколу RADIUS
    - ii) Локальная
  - c) Используйте общий ключ `cisco`
  - d) Используйте номера портов 1812 и 1813 для аутентификации и учета соответственно
  - e) Адрес RADIUS-сервера 172.16.20.20
  - f) Настройте авторизацию при успешной аутентификации
  - g) Проверьте аутентификацию по протоколу RADIUS при удаленном подключении к маршрутизатору HQ1, используя учетную запись `radius` с паролем `cisco`
- 9) Все устройства должны быть доступны для управления по протоколу SSH версии 2.

### Настройка коммутации

- 1) Для централизованного конфигурирования VLAN в коммутируемой сети предприятия используйте протокол VTP.
  - a) В качестве сервера VTP настройте SW1.
  - b) Коммутаторы SW2 и SW3 настройте в качестве VTP клиента.
  - c) Таблица VLAN должна содержать следующие сети:
    - i) VLAN100 с именем MGT.
    - ii) VLAN200 с именем DATA.
    - iii) VLAN300 с именем OFFICE.
    - iv) VLAN500 с именем NATIVE.
    - v) VLAN600 с именем SHUTDOWN.

- 2) Между всеми коммутаторами настройте транки с использованием протокола IEEE 802.1q.
  - a) Порты F0/10 коммутаторов SW2 и SW3, а также порт F0/1 коммутатора SW1 должны работать без использования согласования. Отключите протокол DTP явным образом.
  - b) Транк между коммутаторами SW2 и SW3 должен быть настроен без использования согласования. Отключите протокол DTP явным образом.
  - c) Транки между коммутаторами SW1 и SW2, а также между SW1 и SW3, должны быть согласованы по DTP, коммутатор SW1 должен инициировать создание транка, а коммутаторы SW2 и SW3 должны ожидать начала согласования параметров от соседа, но сами не инициировать согласование.
  - d) Для всех магистральных каналов назначьте native vlan 500.
  - e) Запретите пересылку по магистральным каналам все неиспользуемые VLAN, в том числе VLAN1
- 3) Настройте агрегирование каналов связи между коммутаторами.
  - a) Номера портовых групп:
    - i) 1 – между коммутаторами SW1 (F0/5-6) и SW2 (F0/5-6);
    - ii) 2 – между коммутаторами SW1 (F0/3-4) и SW3 (F0/3-4);
  - b) Агрегированный канал между SW1 и SW2 должен быть организован с использованием протокола согласования LACP. SW1 должен быть настроен в активном режиме, SW2 в пассивном.
  - c) Агрегированный канал между SW1 и SW3 должен быть организован с использованием протокола согласования PAgP. SW1 должен быть настроен в предпочтительном, SW3 в автоматическом.
- 4) Конфигурация протокола остовного дерева:
  - a) Используйте протокол PVST.
  - b) Коммутатор SW1 должен являться корнем связующего дерева в сетях VLAN 100, 200 и 300, в случае отказа SW1, корнем должен стать коммутатор SW2.
  - c) Настройте порт F0/1 коммутатора SW1, таким образом, что при включении он сразу переходил в состояние forwarding не дожидаясь пересчета остовного дерева.

- 5) Настройте порты F0/10 коммутаторов SW2 и SW3 в соответствии с L2 диаграммой. Порты должны быть настроены в режиме доступа.
- 6) Между HQ1 и FW1 настройте взаимодействие по протоколу IEEE 802.1Q.
- 7) Отключите интерфейс F0/24 коммутатора SW1 и E5 межсетевого экрана FW1, которые использовались для первоначального конфигурирования сетевой инфраструктуры офиса HQ.
- 8) На всех устройствах, отключите неиспользуемые порты.
- 9) На всех коммутаторах, неиспользуемые порты переведите во VLAN 600.

### **Настройка подключений к глобальным сетям**

- 1) Подключение FW1 к ISP1 и ISP2 осуществляется с помощью IPoE, настройте интерфейсы в соответствии с диаграммами L2 и L3.
  - a) Передача данных между FW1 и ISP1 осуществляется не тегированным трафиком.
  - b) Передача данных между FW1 и ISP2 осуществляется тегированным трафиком с использованием VLAN 901.
- 2) ISP3 предоставляет L2 VPN между офисами HQ и BR1.
  - a) Настройте передачу между HQ1, FW1 и BR1 тегированного трафика.
  - b) Взаимодействие должно осуществляться по VLAN 10.
- 3) Настройте подключение BR1 к провайдеру ISP1 с помощью протокола PPP.
  - a) Настройте Multilink PPP с использованием двух Serial-интерфейсов.
  - b) Используйте 1 номер интерфейса.
  - c) Не используйте аутентификацию.
  - d) BR1 должен автоматически получать адрес от ISP1.
- 4) Настройте подключение BR1 к провайдеру ISP2 с помощью протокола HDLC.



## Настройка маршрутизации

**ВАЖНО!** При настройке протоколов динамической маршрутизации, будьте предельно внимательны и анонсируйте подсети в соответствии с диаграммой маршрутизации, иначе не получите баллы за протокол, в котором отсутствует необходимая подсеть, и за тот протокол, в котором эта подсеть оказалась лишней.

Также, стоит учесть, что провайдеры фильтруют маршруты полученные по BGP, если они не соответствуют диаграмме маршрутизации.

1) В офисе HQ, на устройствах HQ1 и FW1 настройте протокол динамической маршрутизации OSPF.

a) Включите в обновления маршрутизации сети в соответствии с Routing-диаграммой.

b) HQ1 и FW1 между собой должны устанавливать соседство, только в сети 172.16.3.0/24.

c) Отключите отправку обновлений маршрутизации на всех интерфейсах, где не предусмотрено формирование соседства.

2) Настройте протокол динамической маршрутизации OSPF в офисе BR1 с главным офисом HQ.

a) Включите в обновления маршрутизации сети в соответствии с Routing-диаграммой.

b) Используйте магистральную область для GRE туннелей.

c) Соседства между офисами HQ и BR1 должны устанавливаться, как через канал L2 VPN, так и через защищенный туннель.

d) Убедитесь в том, что при отказе выделенного L2 VPN, трафик между офисами будет передаваться через защищённый GRE туннель.

e) Отключите отправку обновлений маршрутизации на всех интерфейсах, где не предусмотрено формирование соседства.

3) Настройте протокол BGP в офисах HQ и BR1 для взаимодействия с провайдерами ISP1 и ISP2.

a) На устройствах настройте протокол динамической маршрутизации BGP в соответствии с таблицей 1

Таблица 1 – BGP AS

Устройство	AS
HQ1	65000
FW1	65000
ISP1	65001
ISP2	65002
BR1	65010

b) Настройте автономные системы в соответствии с Routing-диаграммой.

4) Маршрутизаторы HQ1 и FW1 должны быть связаны с помощью iBGP. Используйте для этого соседства, интерфейсы, которые находятся в подсети 30.78.87.0/29.

5) Включите в обновления маршрутизации сети в соответствии с Routing-диаграммой.

6) Настройте протокол динамической маршрутизации EIGRP поверх защищенного туннеля и выделенного канала L2 VPN между маршрутизаторами HQ1 и BR1.

a) Включите в обновления маршрутизации сети в соответствии с Routing-диаграммой.

b) Используйте номер автономной системы 6000.

### Настройка служб

1) В сетевой инфраструктуре сервером синхронизации времени является SRV1. Все остальные сетевые устройства должны использовать его в качестве сервера времени.

a) Передача данных между осуществляется без аутентификации.

b) Настройте временную зону с названием MSK, укажите разницу с UTC +3 часов.

c) Убедитесь, в том, что есть все необходимые маршруты, иначе проверить корректность настроенной трансляции портов, будет невозможно.

2) Настройте протокол динамической конфигурации хостов со следующими характеристиками:

a) На маршрутизаторе HQ1 для подсети OFFICE:

- i) Адрес сети – 30.78.21.0/24.
  - ii) Адрес шлюза по умолчанию интерфейс роутера HQ1.
  - iii) Адрес TFTP-сервера 172.16.20.20.
  - iv) Компьютер PC1 должен получать адрес 30.78.21.10.
- 3) В офисе BR1 используется аутентификация клиентов с помощью протокола PPPoE. Для этого настройте сервер PPPoE на BR1.
- a) Аутентификация PC2 на сервере PPPoE должна осуществляться по логину pc2user и паролю pc2pass.
  - b) PC2 должен получать ip адрес от PPPoE сервера автоматически.

### Настройка механизмов безопасности

- 1) На маршрутизаторе BR1 настройте пользователей с ограниченными правами.
- a) Создайте пользователей user1 и user2 с паролем cisco
  - b) Назначьте пользователю user1 уровень привилегий 5. Пользователь должен иметь возможность выполнять все команды пользовательского режима, а также выполнять перезагрузку, а также включать и отключать отладку с помощью команд debug.
  - c) Создайте и назначьте view-контекст sh\_view на пользователя user2
    - i) Команду show cdp neighbor
    - ii) Все команды show ip \*
    - iii) Команду ping
    - iv) Команду traceroute
  - d) Убедитесь, что пользователи не могут выполнять другие команды в рамках присвоенных контекстов и уровней привилегий.
- 2) На порту F0/10 коммутатора SW2, включите и настройте Port Security со следующими параметрами:
- a) не более 2 адресов на интерфейсе
  - b) адреса должны динамически определяться, и сохраняться в конфигурации.
  - c) при попытке подключения устройства с адресом, нарушающим политику, на консоль должно быть выведено уведомление, порт не должен быть отключен.

## Настройка параметров мониторинга и резервного копирования

1) На маршрутизаторе HQ1 и межсетевом экране FW1 настройте журналирование системных сообщений на сервер SRV1, включая информационные сообщения.

2) На маршрутизаторе HQ1 и межсетевом экране FW1 настройте возможность удаленного мониторинга по протоколу SNMP v3.

a) Задайте местоположение устройств MSK, Russia

b) Задайте контакт admin@wsr.ru

c) Используйте имя группы WSR.

d) Создайте профиль только для чтения с именем RO.

e) Используйте для защиты SNMP шифрование AES128 и аутентификацию SHA1.

f) Используйте имя пользователя: snmpuser и пароль: snmprpass

g) Для проверки вы можете использовать команду snmp\_test на SRV1.

3) На маршрутизаторе HQ1 настройте резервное копирование конфигурации

a) Резервная копия конфигурации должна сохраняться на сервер SRV1 по протоколу TFTP при каждом сохранении конфигурации в памяти устройства

b) Для названия файла резервной копии используйте шаблон <hostname>-<time>.cfg

## Конфигурация частных виртуальных сетей

1) Между HQ1 и BR1 настройте GRE туннель со следующими параметрами:

a) Используйте в качестве VTI интерфейс Tunnel1

b) Используйте адресацию в соответствии с L3-диаграммой

c) Режим — GRE

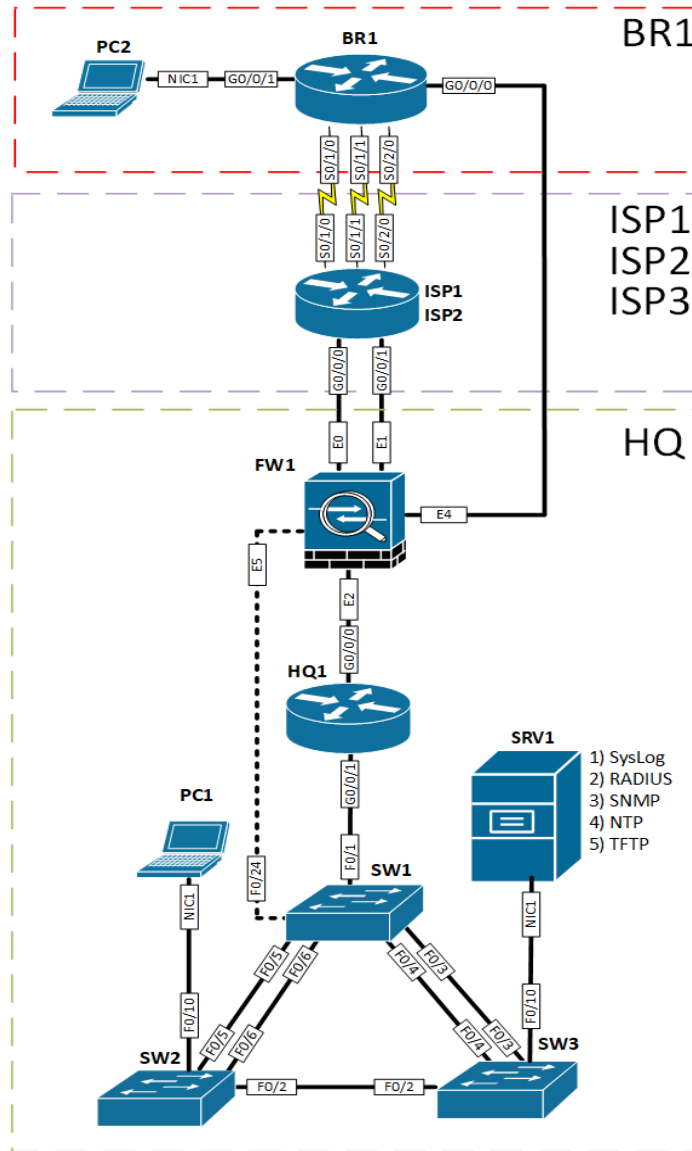
d) Интерфейс-источник — Loopback-интерфейс на каждом маршрутизаторе.

e) Обеспечьте работу туннеля с обеих сторон через провайдера ISP1

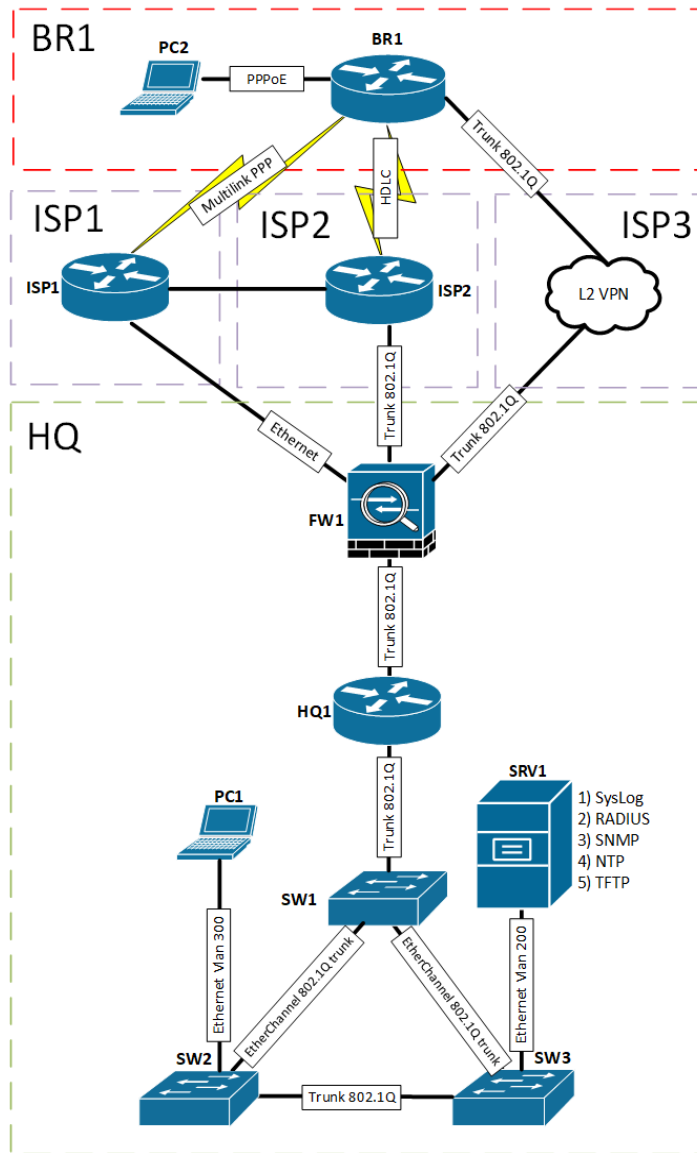
2) Защита туннеля должна обеспечиваться с помощью IPsec между BR1 и FW1.

- a) Обеспечьте шифрование только GRE трафика.
- b) Используйте аутентификацию по общему ключу.
- c) Параметры IPsec произвольные.

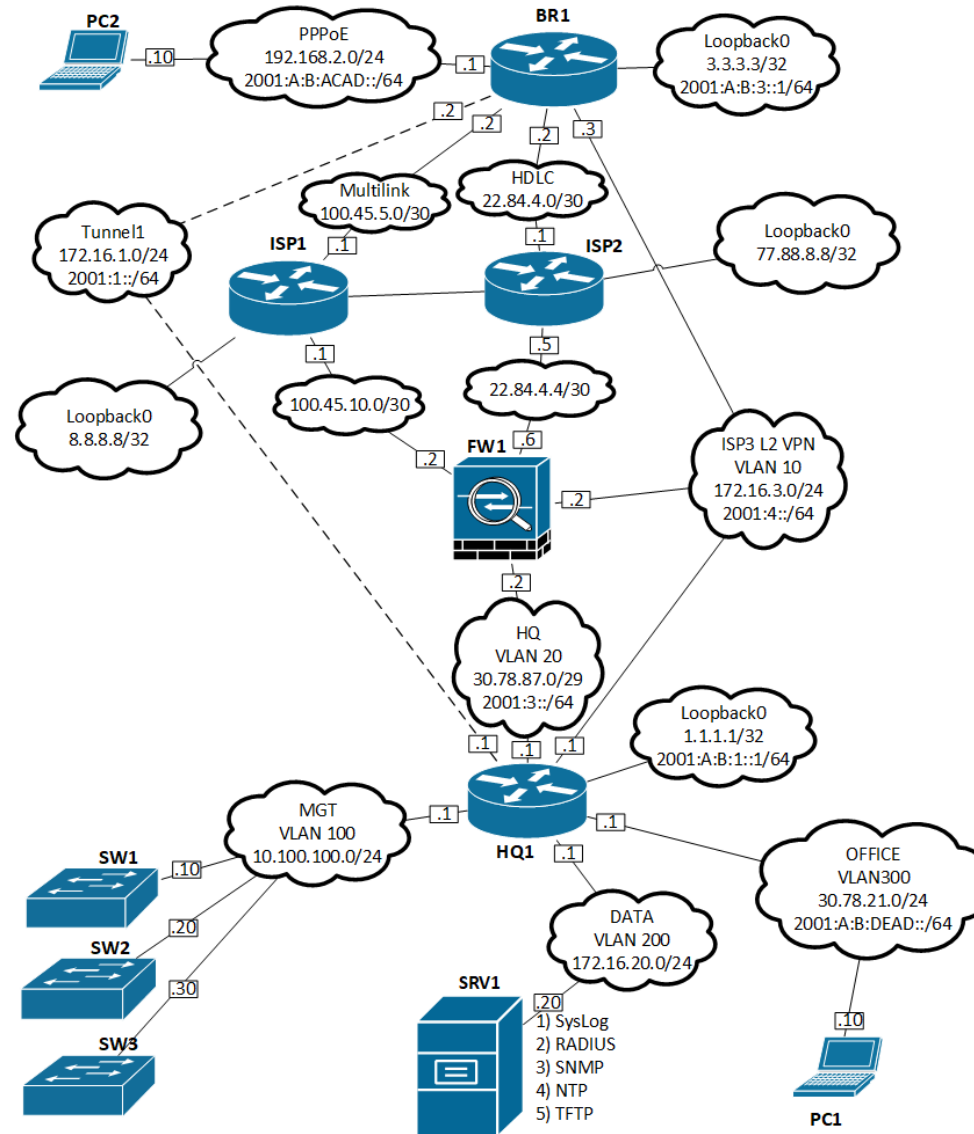
# ТОПОЛОГИЯ L1



# ТОПОЛОГИЯ L2

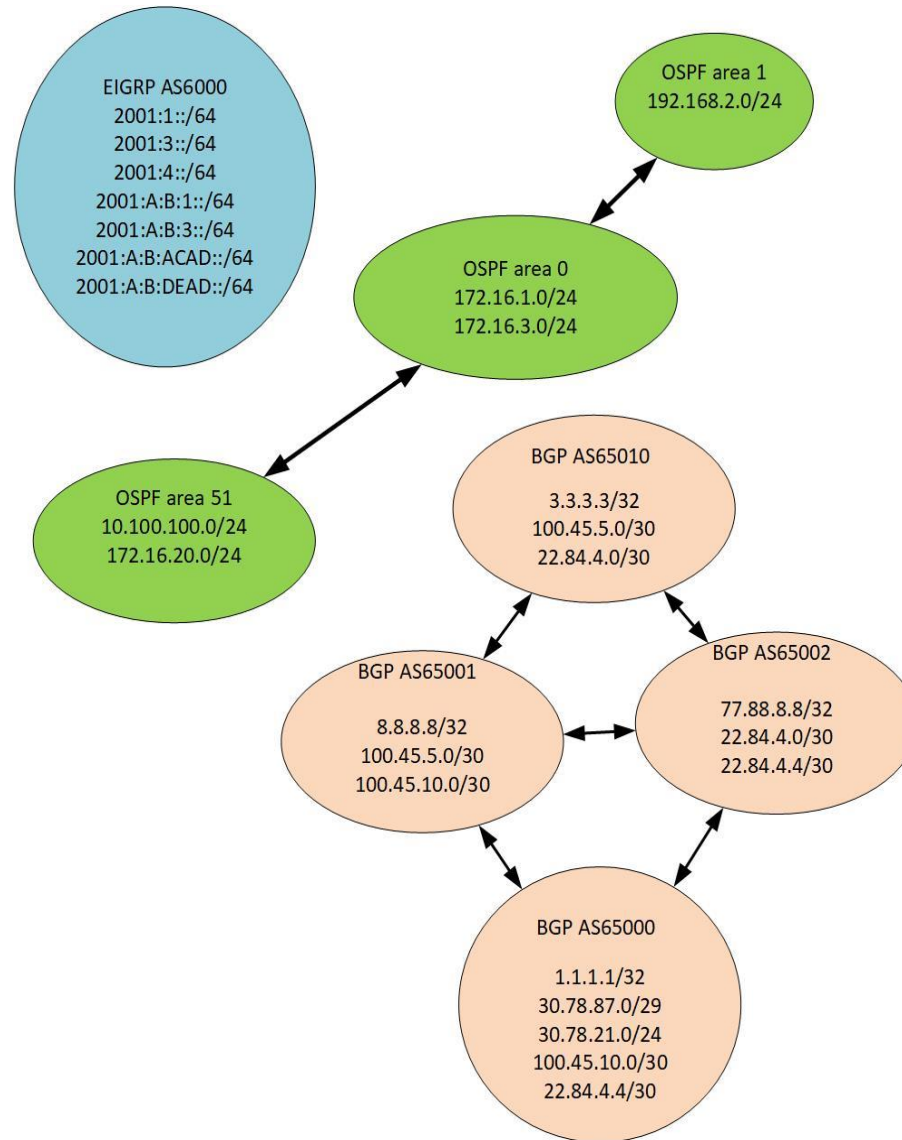


# ТОПОЛОГИЯ L3





# ROUTING-ДИАГРАММА



## **5. ПРИЛОЖЕНИЯ К ЗАДАНИЮ**

*1 Приложение 1 Дополнительные настройки модуля В*

## Дополнительные настройки модуля В

### ПРИЛОЖЕНИЕ

**ВВЕДЕНИЕ.** Настоящие дополнения содержат описание вида предустановок, описание используемых операционных систем, рекомендации по выделению ресурсов для виртуальных машин.

#### ОПИСАНИЕ ПРЕДУСТАНОВОК

1. На SRV1 должно быть установлено четыре (или пять) жестких диска: один не менее – 25 Gb, три (четыре) – 5 Gb .
2. Все остальные жесткие диски всех виртуальных машин должны иметь объем не менее 25 Gb.
3. После установки на всех виртуальных машинах необходимо выполнить сценарий *Sysprep* с опцией *generalize*.
4. После выполнения работ перезагрузка стендов остается на усмотрение экспертов.

#### ОПИСАНИЕ ПРИМЕНЯЕМЫХ ОПЕРАЦИОННЫХ СИСТЕМ

Имя компьютера	Операционная система
DC2	Windows Server 2019 GUI
CLI2	Windows 10 Enterprise
SRV2	Windows Server 2019 Core
R2	Windows 2019 GUI
DC1	Windows 2019 GUI
SRV1	Windows Server 2019 Core
R1	Windows Server 2019 Core
CLI1	Windows 10 Enterprise
DCA	Windows Server 2019 GUI

Задание протестировано на 100% следующих сборках ОС:

- Server 2019 – 17763.379.190312-0539;
- Win 10 Ent – 18362.30.190401-1528

**Примерный план работы Центра проведения демонстрационного экзамена по КОД № 1.1 по компетенции «Сетевое и системное администрирование»**

	<b>Примерное время</b>	<b>Мероприятие</b>
<b>Подготовительный день</b>	08:00	Получение главным экспертом задания демонстрационного экзамена
	08:00 – 08:20	Проверка готовности проведения демонстрационного экзамена, заполнение Акта о готовности/не готовности
	08:20 – 08:30	Распределение обязанностей по проведению экзамена между членами Экспертной группы, заполнение Протокола о распределении
	08:30 – 08:40	Инструктаж Экспертной группы по охране труда и технике безопасности, сбор подписей в Протоколе об ознакомлении
	08:40 – 09:00	Регистрация участников демонстрационного экзамена
	09:00 – 09:30	Инструктаж участников по охране труда и технике безопасности, сбор подписей в Протоколе об ознакомлении
	09:30 – 11:00	Распределение рабочих мест (жеребьевка) и ознакомление участников с рабочими местами, оборудованием, графиком работы, иной документацией и заполнение Протокола
	<b>День 1</b>	09:00 – 09:30
09:30 – 10:00		Брифинг экспертов

	10:00 – 12:00	Выполнение модуля А
	12:30 – 14:30	Выполнение модуля В
	14:30 – 15:30	Обед
	15:30 – 17:30	Выполнение модуля С
	17:30 – 19:30	Работа экспертов, заполнение форм и оценочных ведомостей
	19:30 – 20:30	Подведение итогов, внесение главным экспертом баллов в CIS, блокировка, сверка баллов, заполнение итогового протокола

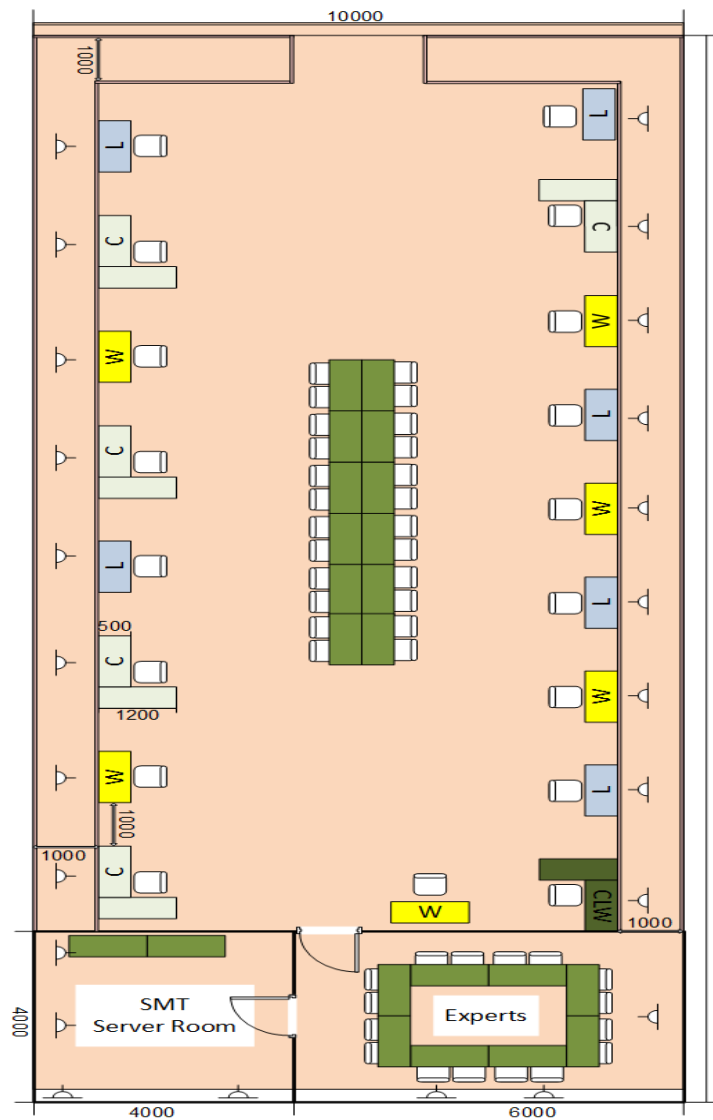
**План застройки площадки для проведения демонстрационного экзамена  
по КОД № 1.1 по компетенции № 39 «Сетевое и системное  
администрирование»**

Компетенция: Сетевое и системное администрирование

Номер компетенции: 39

Общая площадь площадки: 250 м<sup>2</sup>

План застройки площадки:



## **ПРИЛОЖЕНИЕ**

Инфраструктурный лист для КОД № 1.1