Министерство цифрового развития, связи и массовых коммуникаций Российской Федерации
Федеральное государственное бюджетное образовательное учреждение высшего образования
«Сибирский государственный университет телекоммуникаций и информатики»
(СибГУТИ)
Уральский технический институт связи и информатики (филиал) в г. Екатеринбурге
(УрТИСИ СибГУТИ)

Утверждаю
Директор УрТИСИ СибГУТИ
_____ Е.А. Минина
«18» 11 2025 г.

ОЦЕНОЧНЫЕ МАТЕРИАЛЫ ГОСУДАРСТВЕННОЙ ИТОГОВОЙ АТТЕСТАЦИИ

для специальности:
09.02.06 Сетевое и системное администрирование

Квалификация: сетевой администратор

Год начала подготовки: 2026

Екатеринбург
2025

Министерство цифрового развития, связи и массовых коммуникаций Российской Федерации
Федеральное государственное бюджетное образовательное учреждение высшего образования
«Сибирский государственный университет телекоммуникаций и информатики»
(СибГУТИ)
Уральский технический институт связи и информатики (филиал) в г. Екатеринбурге
(УрТИСИ СибГУТИ)

Утверждаю
Директор УрТИСИ СибГУТИ
_____ Е.А. Минина
«___» _____ 2025 г.

ОЦЕНОЧНЫЕ МАТЕРИАЛЫ ГОСУДАРСТВЕННОЙ ИТОГОВОЙ АТТЕСТАЦИИ

для специальности:
09.02.06 Сетевое и системное администрирование

Квалификация: сетевой администратор

Год начала подготовки: 2026

Екатеринбург
2025

Оценочные материалы составил:
Тарасов Е.С. - преподаватель ЦК ЭТД кафедры ИТ и МС

Одобрено цикловой комиссией
Электротехнических дисциплин
кафедры Инфокоммуникационных
технологий и мобильной связи.
Протокол 3 от 26.11.2015
Председатель цикловой комиссии
_____ Е.С. Тарасов

Согласовано
Заместитель директора
по учебной работе
_____ А.Н. Белякова

Оценочные материалы составил:
Тарасов Е.С. - преподаватель ЦК ЭТД кафедры ИТ и МС

Одобрено цикловой комиссией
Электротехнических дисциплин
кафедры Инфокоммуникационных
технологий и мобильной связи.
Протокол ___ от _____
Председатель цикловой комиссии
_____ Е.С. Тарасов

Согласовано
Заместитель директора
по учебной работе
_____ А.Н. Белякова

1 Общие положения

Оценочные материалы государственной итоговой аттестации (далее - ГИА) являются частью образовательной программы - программы подготовки специалистов среднего звена в соответствии с ФГОС СПО по специальности 09.02.06 Сетевое и системное администрирование.

Оценочные материалы устанавливают уровень подготовки выпускника к выполнению профессиональных задач и соответствия его подготовки требованиям ФГОС СПО по специальности 09.02.06 Сетевое и системное администрирование.

2 Формы и объем государственной итоговой аттестации

Формами ГИА в соответствии с ФГОС СПО являются:

- демонстрационный экзамен;
- защита дипломного проекта.

Сроки проведения каждой формы ГИА регламентированы календарным графиком учебного процесса на текущий учебный год.

Объем времени на подготовку и проведение ГИА - 6 недель.

3 Компетенции выпускника

В рамках проведения ГИА обучающийся должен показать владение общими и профессиональными компетенциями.

3.1 Общие компетенции.

Общие компетенции указаны в таблице 1.

Таблица 1

Код ОК	Наименование общих компетенций
ОК 01	Выбирать способы решения задач профессиональной деятельности применительно к различным контекстам.
ОК 02	Использовать современные средства поиска, анализа и интерпретации информации, и информационные технологии для выполнения задач профессиональной деятельности.
ОК 03	Планировать и реализовывать собственное профессиональное и личностное развитие, предпринимательскую деятельность в профессиональной сфере, использовать знания по правовой и финансовой грамотности в различных жизненных ситуациях.
ОК 04	Эффективно взаимодействовать и работать в коллективе и команде.
ОК 05	Осуществлять устную и письменную коммуникацию на государственном языке Российской Федерации с учетом особенностей социального и культурного контекста.
ОК 06	Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных российских духовно-нравственных ценностей, в том числе с учетом гармонизации межнациональных и межрелигиозных отношений, применять стандарты антикоррупционного поведения.

ОК 07	Содействовать сохранению окружающей среды, ресурсосбережению, применять знания об изменении климата, принципы бережливого производства, эффективно действовать в чрезвычайных ситуациях.
ОК 08	Использовать средства физической культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и поддержания необходимого уровня физической подготовленности.
ОК 09	Пользоваться профессиональной документацией на государственном и иностранных языках.

3.2 Профессиональные компетенции.

Профессиональные компетенции, соответствующие видам деятельности, указаны в таблице 2.

Таблица 2

Код ПК	Наименование вида деятельности и профессиональных компетенций
ВД 1	***Настройка сетевой инфраструктуры***
ПК 1.1	Документировать состояния инфокоммуникационных систем и их составляющих в процессе наладки и эксплуатации.
ПК 1.2	Поддерживать работоспособность аппаратно-программных средств устройств инфокоммуникационных систем.
ПК 1.3	Устранять неисправности в работе инфокоммуникационных систем.
ПК 1.4	Проводить приемо-сдаточные испытания компьютерных сетей и сетевого оборудования различного уровня и оценку качества сетевой топологии в рамках своей ответственности.
ПК 1.5	Осуществлять резервное копирование и восстановление конфигурации сетевого оборудования информационно-коммуникационных систем.
ПК 1.6	Осуществлять инвентаризацию технических средств сетевой инфраструктуры, контроль оборудования после проведенного ремонта.
ПК 1.7	Осуществлять регламентное обслуживание и замену расходных материалов периферийного, сетевого и серверного оборудования инфокоммуникационных систем.
ВД 2	***Организация сетевого администрирования операционных систем***
ПК 2.1	Принимать меры по устранению сбоев в операционных системах.
ПК 2.2	Администрировать сетевые ресурсы в операционных системах.
ПК 2.3	Осуществлять сбор данных для анализа использования и функционирования программно-технических средств компьютерных сетей.
ПК 2.4	Осуществлять проведение обновления программного обеспечения операционных систем и прикладного программного обеспечения.
ПК 2.5	Осуществлять выявление и устранение инцидентов в процессе функционирования операционных систем.
ВД 3	***Эксплуатация объектов сетевой инфраструктуры (по выбору)***
ПК 3.1	Осуществлять проектирование сетевой инфраструктуры.
ПК 3.2	Обслуживать сетевые конфигурации программно-аппаратных средств.
ПК 3.3	Осуществлять защиту информации в сети с использованием программно-аппаратных средств.
ПК 3.4	Осуществлять устранение нетипичных неисправностей в работе сетевой инфраструктуры.
ПК 3.5	Модернизировать сетевые устройства информационно-коммуникационных систем.

4 Организация и порядок проведения государственной итоговой аттестации

4.1 Демонстрационный экзамен.

Демонстрационный экзамен проводится в рамках ГИА, направлен на определение уровня освоения выпускником материала, предусмотренного образовательной программой, и степени сформированности профессиональных умений и навыков путём проведения независимой экспертной оценки выполненных выпускником практических заданий в условиях реальных или смоделированных производственных процессов.

Демонстрационный экзамен проводится с использованием единых оценочных материалов, включающих в себя конкретные комплекты оценочной документации (КОД), варианты заданий и критерии оценивания, разрабатываемых оператором.

КОД включает комплекс требований для проведения демонстрационного экзамена, перечень оборудования и оснащения, расходных материалов, средств обучения и воспитания, план застройки площадки демонстрационного экзамена, требования к составу экспертных групп, инструкции по технике безопасности, а также образцы заданий.

Задание демонстрационного экзамена включает комплексную практическую задачу, моделирующую профессиональную деятельность и выполняемую в режиме реального времени.

КОД для проведения демонстрационного экзамена профильного уровня разрабатываются оператором с участием организаций-партнеров, отраслевых и профессиональных сообществ.

Продолжительность демонстрационного экзамена профильного уровня представлена в таблице 3.

Таблица 3

Вид аттестации	Уровень ДЭ	Составная часть КОД (инвариантная/вариативная часть)	Продолжительность ДЭ, час.
ГИА	профильный	инвариантная часть	3:30

Содержательная структура КОД представлена в таблице 4.

Таблица 4

Вид деятельности	Перечень оцениваемых ПК, ОК	Перечень оцениваемых умений, навыков (практического опыта)	ГИА ДЭ ПУ
Настройка сетевой инфраструктуры.	ПК: Устранять неисправности в работе инфокоммуникационных систем.	Умение: устранять неисправности в работе инфокоммуникационных систем.	+
		Умение: документировать состояния инфокоммуникационных систем и их составляющих в процессе наладки и эксплуатации.	+

		Практический опыт: поддерживать работоспособность аппаратно-программных средств устройств инфокоммуникационных систем.	+
	ПК: Проводить приемо-сдаточные испытания компьютерных сетей и сетевого оборудования различного уровня и оценку качества сетевой топологии в рамках своей ответственности.	Умение: оценивать качество сетевой топологии в рамках своей ответственности.	+
		Практический опыт: диагностировать сетевое оборудование различного уровня.	+
	ПК: Осуществлять регламентное обслуживание и замену расходных материалов периферийного, сетевого и серверного оборудования инфокоммуникационных систем.	Умение: осуществлять регламентное обслуживание и замену расходных материалов периферийного, сетевого и серверного оборудования инфокоммуникационных систем.	+
		Практический опыт: использовать инструментальные средства на этапе отладки сетевого и серверного оборудования инфокоммуникационных систем.	+
Организация сетевого администрирования операционных систем операционных систем.	ПК: Администрировать сетевые ресурсы в операционных системах.	Умение: принимать меры по устранению сбоев в операционных системах.	+
		Умение: настраивать конфигурацию компьютерных систем.	+
		Практический опыт: администрировать сетевые ресурсы в операционных системах.	+
	ПК: Осуществлять сбор данных для анализа использования и функционирования программно-технических средств компьютерных сетей.	Уметь: осуществлять сбор данных для анализа использования и функционирования программно-технических средств компьютерных сетей.	+
		Практический опыт: проводить обновления программного обеспечения операционных систем и прикладного программного обеспечения.	+
	ПК: Осуществлять проведение обновления программного обеспечения операционных систем и прикладного программного обеспечения.	Умение: выявление и устранение инцидентов в процессе функционирования операционных систем.	+
		Практический опыт: проводить обновления программного обеспечения операционных систем и прикладного программного обеспечения.	+

Эксплуатация объектов сетевой инфраструктуры.	ПК: Проектировать сетевые инфраструктуры.	Умение: проектировать сетевую инфраструктуру.	+
		Умение: настраивать конфигурацию программного обеспечения компьютерных систем.	+
		Практический опыт: модернизировать сетевые устройства информационно-коммуникационных систем.	+
	ПК: Обслуживать сетевые конфигурации программно-аппаратных средств.	Умение: обслуживать сетевые конфигурации программно-аппаратных средств.	+
		Практический опыт: настройка отдельных компонентов программного обеспечения компьютерных систем.	+
	ПК: Осуществлять защиту информации в сети с использованием программно-аппаратных средств.	Умение: осуществлять защиту информации в сети с использованием программно-аппаратных средств.	+
		Практический опыт: измерять эксплуатационные характеристики программного обеспечения компьютерных систем на соответствие требованиям.	+

Примерное задание на демонстрационный экзамен:

Модуль 1 Настройка сетевой инфраструктуры:

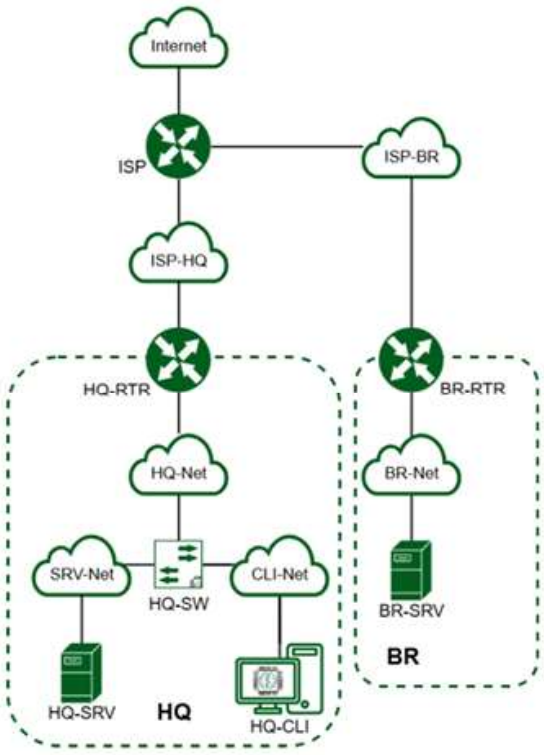

Рисунок 1 - Топология сети

1. Произведите базовую настройку устройств:

1.2 Настройте имена устройств согласно топологии. Используйте полное доменное имя.

1.3 На всех устройствах необходимо сконфигурировать IPv4:

1.3.1 IP-адрес должен быть из приватного диапазона в случае, если сеть локальная, согласно RFC1918.

1.3.2 Локальная сеть в сторону HQ-SRV (VLAN 100) должна вмещать не более 32 адресов.

1.3.3 Локальная сеть в сторону HQ-CLI (VLAN 200) должна вмещать не менее 16 адресов.

1.3.4 Локальная сеть для управления (VLAN 999) должна вмещать не более 8 адресов.

1.3.5 Локальная сеть в сторону BR-SRV должна вмещать не более 16 адресов.

1.4 Сведения об адресах занесите в таблицу 2, в качестве примера используйте Прил_3_О1_КОД 09.02.06-1-2026-М1.

2. Настройте доступ к сети Интернет, на маршрутизаторе ISP:

2.1 Настройте адресацию на интерфейсах. Интерфейс, подключенный к магистральному провайдеру, получает адрес по DHCP.

2.2 Настройте маршрут по умолчанию, если это необходимо.

2.3 Настройте интерфейс, в сторону HQ-RTR, интерфейс подключен к сети 172.16.1.0/28 38.

2.4 Настройте интерфейс, в сторону BR-RTR, интерфейс подключен к сети 172.16.2.0/28.

2.5 На ISP настройте динамическую сетевую трансляцию портов для доступа к сети Интернет HQ-RTR и BR-RTR.

3. Создайте локальные учетные записи на серверах HQ-SRV и BR-SRV:

3.1 Создайте пользователя sshuser.

3.2 Пароль пользователя sshuser с паролем P@ssw0rd.

3.3 Идентификатор пользователя 2026.

3.4 Пользователь sshuser должен иметь возможность запускать sudo без ввода пароля.

3.5 Создайте пользователя net_admin на маршрутизаторах HQ-RTR и BR RTR.

3.6 Пароль пользователя net_admin с паролем P@ssw0rd.

3.7 При настройке ОС на базе Linux, запускать sudo без ввода пароля.

3.8 При настройке ОС отличных от Linux пользователь должен обладать максимальными привилегиями.

4. Настройте коммутацию в сегменте HQ следующим образом:

4.1 Трафик HQ-SRV должен принадлежать VLAN 100.

4.2 Трафик HQ-CLI должен принадлежать VLAN 200.

4.3 Предусмотреть возможность передачи трафика управления в VLAN 999.

4.4 Реализовать на HQ-RTR маршрутизацию трафика всех указанных VLAN с использованием одного сетевого адаптера ВМ/физического порта.

4.5 Сведения о настройке коммутации внесите в отчёт.

5. Настройте безопасный удаленный доступ на серверах HQ-SRV и BR SRV:

5.1 Для подключения используйте порт 2026.

5.2 Разрешите подключения исключительно пользователю sshuser.

5.3 Ограничьте количество попыток входа до двух.

5.4 Настройте баннер «Authorized access only».

6. Между офисами HQ и BR, на маршрутизаторах HQ-RTR и BR-RTR необходимо сконфигурировать ip туннель:

6.1 На выбор технологии GRE или IP in IP.

6.2 Сведения о туннеле занесите в отчёт.

7. Обеспечьте динамическую маршрутизацию на маршрутизаторах HQ RTR и BR-RTR сети одного офиса должны быть доступны из другого офиса и наоборот. Для обеспечения динамической маршрутизации используйте link state протокол на усмотрение участника:

7.1 Разрешите выбранный протокол только на интерфейсах ip туннеля.

7.2 Маршрутизаторы должны делиться маршрутами только друг с другом.

7.3 Обеспечьте защиту выбранного протокола посредством парольной защиты.

7.4 Сведения о настройке и защите протокола занесите в отчёт.

8. Настройка динамической трансляции адресов маршрутизаторах HQ RTR и BR-RTR:

8.1 Настройте динамическую трансляцию адресов для обоих офисов в сторону ISP, все устройства в офисах должны иметь доступ к сети Интернет.

9. Настройте протокол динамической конфигурации хостов для сети в сторону HQ-CLI:

9.1 Настройте нужную подсеть.

9.2 В качестве сервера DHCP выступает маршрутизатор HQ-RTR.

9.3 Клиентом является машина HQ-CLI.

9.4 Исключите из выдачи адрес маршрутизатора.

9.5 Адрес шлюза по умолчанию – адрес маршрутизатора HQ-RTR.

9.6 Адрес DNS-сервера для машины HQ-CLI – адрес сервера HQ-SRV.

9.7 DNS-суффикс – au-team.irpo.

9.8 Сведения о настройке протокола занесите в отчёт.

10. Настройте инфраструктуру разрешения доменных имён для офисов HQ и BR:

10.1 Основной DNS-сервер реализован на HQ-SRV.

10.2 Сервер должен обеспечивать разрешение имён в сетевые адреса устройств и обратно.

10.3 В качестве DNS сервера пересылки используйте любой общедоступный DNS сервер (77.88.8.7, 77.88.8.3 или другие).

11. Настройте часовой пояс на всех устройствах (за исключением виртуального коммутатора, в случае его использования) согласно месту проведения экзамена.

Модуль 2 Организация сетевого администрирования:

Топология сети таже.

1. Настройте контроллер домена Samba DC на сервере BR-SRV:

1.1 Имя домена au-team.irpo.

1.2 Введите в созданный домен машину HQ-CLI.

1.3 Создайте 5 пользователей для офиса HQ: имена пользователей формата hquser№ (например, hquser1, hquser2 и т.д.).

1.4 Создайте группу hq, введите в группу созданных пользователей.

1.5 Убедитесь, что пользователи группы hq имеют право аутентифицироваться на HQ-CLI.

1.6 Пользователи группы hq должны иметь возможность повышать привилегии для выполнения ограниченного набора команд: cat, grep, id. Запускать другие команды с повышенными привилегиями пользователи группы права не имеют.

2. Сконфигурируйте файловое хранилище на сервере HQ-SRV:

2.1 При помощи двух подключенных к серверу дополнительных дисков размером 1 Гб сконфигурируйте дисковый массив уровня 0.

2.2 Имя устройства – md0, при необходимости конфигурация массива размещается в файле /etc/mdadm.conf.

2.3 Создайте раздел, отформатируйте раздел, в качестве файловой системы используйте ext4

2.4 Обеспечьте автоматическое монтирование в папку /raid.

3. Настройте сервер сетевой файловой системы (nfs) на HQ-SRV:

3.1 В качестве папки общего доступа выберите /raid/nfs, доступ для чтения и записи исключительно для сети в сторону HQ-CLI.

3.2 На HQ-CLI настройте автомонтирование в папку /mnt/nfs.

3.3 Основные параметры сервера отметьте в отчёте.

4. Настройте службу сетевого времени на базе сервиса chrony на маршрутизаторе ISP:

4.1 Вышестоящий сервер ntp на маршрутизаторе ISP - на выбор участника.

4.2 Стратум сервера – 5.

4.3 В качестве клиентов ntp настройте: HQ-SRV, HQ-CLI, BR-RTR, BR SRV.

5. Сконфигурируйте ansible на сервере BR-SRV:

5.1 Сформируйте файл инвентаря, в инвентарь должны входить HQ-SRV, HQ-CLI, HQ-RTR и BR-RTR.

5.2 Рабочий каталог ansible должен располагаться в /etc/ansible.

5.3 Все указанные машины должны без предупреждений и ошибок отвечать pong на команду ping в ansible посланную с BR-SRV.

6. Разверните веб приложение в docker на сервере BR-SRV:

6.1 Средствами docker должен создаваться стек контейнеров с веб приложением и базой данных.

6.2 Используйте образы site_latestи mariadb_latestpac полагающиеся в директории docker в образе Additional.iso.

6.3 Основной контейнер testapp должен называться tespapp.

6.4 Контейнер с базой данных должен называться db.

6.5 Импортируйте образы в docker, укажите в yaml файле параметры подключения к СУБД, имя БД - testdb, пользователь testc паролем P@ssw0rd, порт приложения 8080, при необходимости другие параметры.

6.6 Приложение должно быть доступно для внешних подключений через порт 8080.

7. Разверните веб приложение на сервере HQ-SRV:

7.1 Используйте веб-сервер apache.

7.2 В качестве системы управления базами данных используйте mariadb.

7.3 Файлы веб приложения и дамп базы данных находятся в директории web образа Additional.iso.

7.4 Выполните импорт схемы и данных из файла dump.sql в базу данных webdb.

7.5 Создайте пользователя webc паролем P@ssw0rd и предоставьте ему права доступа к этой базе данных.

7.6 Файлы index.php и директорию images скопируйте в каталог веб сервера apache.

7.7 В файле index.php укажите правильные учётные данные для подключения к БД.

7.8 Запустите веб сервер и убедитесь в работоспособности приложения Основные параметры отметьте в отчёте.

8. На маршрутизаторах сконфигурируйте статическую трансляцию портов:

8.1 Пробросьте порт 8080в порт приложения testapp BR-SRV на маршрутизаторе BR-RTR, для обеспечения работы приложения testapp извне.

8.2 Пробросьте порт 8080в порт веб приложения на HQ-SRV на маршрутизаторе HQ-RTR, для обеспечения работы веб приложения извне.

8.3 Пробросьте порт 2026на маршрутизаторе HQ-RTR в порт 2026 сервера HQ-SRV, для подключения к серверу по протоколу ssh из внешних сетей.

8.4 Пробросьте порт 2026на маршрутизаторе BR-RTR в порт 2026сервера BR-SRV, для подключения к серверу по протоколу ssh из внешних сетей.

9. Настройте веб-сервер nginx как обратный прокси-сервер на ISP.

9.1 При обращении по доменному имени web.au-team.irpo у клиента должно открываться веб приложение на HQ-SRV.

9.2 При обращении по доменному имени docker.au-team.irpo клиента должно открываться веб приложение testapp.

10. На маршрутизаторе ISP настройте web-based аутентификацию:

10.1 При обращении к сайту web.au-team.irpo клиенту должно быть предложено ввести аутентификационные данные:

10.1.1 В качестве логина для аутентификации выберите WEBc паролем P@ssw0rd.

10.1.2 Выберите файл /etc/nginx/.htpasswd в качестве хранилища учётных записей.

10.1.3 При успешной аутентификации клиент должен перейти на веб сайт.

11. Удобным способом установите приложение Яндекс Браузер на HQ-CLI.

11.1 Установку браузера отметьте в отчёте.

Модуль 3 Эксплуатация объектов сетевой инфраструктуры:

Топология сети таже.

1. Выполните импорт пользователей в домен au-team.irpo:

1.1 В качестве файла источника выберите файл users.csv располагающийся в образе Additional.iso.

1.2 Пользователи должны быть импортированы со своими паролями и другими атрибутами.

1.3 Убедитесь, что импортированные пользователи могут войти на машину HQ-CLI.

2. Выполните настройку центра сертификации на базе HQ-SRV:

2.1 Необходимо использовать отечественные алгоритмы шифрования.

2.2 Сертификаты выдаются на 30дней.

2.3 Обеспечьте доверие сертификату для HQ-CLI.

2.4 Выдайте сертификаты веб серверам.

2.5 Перенастройте ранее настроенный реверсивный прокси nginx на протокол https.

2.6 При обращении к веб серверам https://web.au-team.irpo и https://docker.au-team.irpo у браузера клиента не должно возникать предупреждений.

3. Перенастройте ip-туннель с базового до уровня туннеля, обеспечивающего шифрование трафика.

3.1 Настройте защищенный туннель между HQ-RTR и BR-RTR.

3.2 Внесите необходимые изменения в конфигурацию динамической маршрутизации, протокол динамической маршрутизации должен возобновить работу после перенастройки туннеля.

3.3 Выбранное программное обеспечение, обоснование его выбора и его основные параметры, изменения в конфигурации динамической маршрутизации отметьте в отчёте.

4. Настройте межсетевой экран на маршрутизаторах HQ-RTR и BR-RTR на сеть в сторону ISP.

4.1 Обеспечьте работу протоколов http, https, dns, ntp, icmp или дополнительных нужных протоколов.

4.2 Запретите остальные подключения из сети Интернет во внутреннюю сеть.

5. Настройте принт-сервер cups на сервере HQ-SRV:

5.1 Опубликуйте виртуальный pdf-принтер.

5.2 На клиенте HQ-CLI подключите виртуальный принтер как принтер по умолчанию.

6. Реализуйте логирование при помощи rsyslog на устройствах HQ-RTR, BR-RTR, BR-SRV:

6.1 Сервер сбора логов расположен на HQ-SRV, убедитесь, что сервер не является клиентом самому себе.

6.2 Приоритет сообщений должен быть не ниже warning.

6.3 Все журналы должны находиться в директории /opt. Для каждого устройства должна выделяться своя поддиректория, которая совпадает с именем машины.

6.4 Реализуйте ротацию собранных логов на сервере HQ-SRV:

6.4.1 Ротируются все логи, находящиеся в директории и поддиректориях /opt.

6.4.2 Ротация производится один раз в неделю.

6.4.3 Логи необходимо сжимать.

6.4.4 Минимальный размер логов для ротации - 10МБ.

7. На сервере HQ-SRV реализуйте мониторинг устройств с помощью открытого программного обеспечения.

7.1 Обеспечьте доступность по URL - http://mon.au-team.irpo для сетей офиса Q, внесите изменения в инфраструктуру разрешения доменных имён.

7.2 Мониторить нужно устройства HQ-SRV и BR-SRV.

7.3 В мониторинге должны визуально отображаться нагрузка на ЦП, объем занятой ОП и основного накопителя.

7.4 Логин и пароль для службы мониторинга admin P@ssw0rd.

7.5 Организуйте доступ к мониторингу для HQ-CLI, без внешнего доступа.

7.6 Выбор программного обеспечения, основание выбора и основные параметры с указанием порта, на котором работает мониторинг, отметьте в отчёте.

8. Реализуйте механизм инвентаризации машин HQ-SRV и HQ-CLI через Ansible на BR-SRV:

8.1 Плейбук должен собирать информацию о рабочих местах:

8.1.1 Имя компьютера.

8.1.2 IP-адрес компьютера.

8.2 Плейбук, должен быть размещен в директории /etc/ansible, отчёты в поддиректории PC-INFO, в формате .yml. Файлы должны называется именем компьютера, который был инвентаризирован.

8.3 Файл плейбука располагается в образе Additional.iso в директории playbook.

9. На HQ-SRV настройте программное обеспечение fail2ban для защиты ssh.

9.1 Укажите порт ssh.

9.2 При 3 неуспешных авторизациях адрес атакующего попадает в бан.

9.3 Бан производится на 1 минуту.

10. Настройка резервного копирования директории сервера HQ-SRV:

10.1 На HQ-SRV развернуть программное обеспечение для резервного копирования и восстановления данных с защитой от вирусов шифровальщиков.

10.2 В качестве решения рекомендуется использовать программное обеспечение Кибер Бэкап версии 17.4 или аналог.

10.3 Настройте организацию irpo.

10.4 Настройте пользователя с правами администратора на сервере HQ-SRV, имя пользователя irpoadmin с паролем P@ssw0rd.

10.5 Установите на HQ-CLI агент с функциями узла хранилища и подключите его к серверу управления.

10.6 На узле хранилища HQ-CLI создайте директорию /backup и выберите её в качестве устройства хранения.

10.7 Создайте два плана резервного копирования для сервера HQ-SRV.

10.7.1 План для резервного копирования директории /etc и всех её поддиректорий.

10.7.2 План для резервного копирования базы данных webdb типа mysql.

10.8 Выполните резервное копирование директории /etc и всех её поддиректорий сервера HQ-SRV на узел хранения HQ-CLI.

10.9 Выполните резервное копирование базы данных webdb сервера HQ-SRV на узел хранения HQ-CLI.

4.2 Дипломный проект.

Дипломный проект - это комплексная самостоятельная работа обучающегося, главной целью и содержанием которой является всесторонний анализ, исследование и разработка актуальных задач и вопросов как теоретического, так и прикладного характера по профилю специальности.

Тематика дипломных проектов, включенных в программу государственной итоговой аттестации, соответствует содержанию одного или нескольких профессиональных модулей (Таблица 5).

Таблица 5

Код ПМ	Наименование профессионального модуля
ПМ.01	Настройка сетевой инфраструктуры
ПМ.02	Организация сетевого администрирования операционных систем
ПМн.03	Эксплуатация объектов сетевой инфраструктуры.

Защита дипломного проекта производится на открытом заседании ГЭК с участием не менее двух третей ее состава. Решения ГЭК принимаются на закрытых заседаниях простым большинством голосов членов комиссии, участвующих в заседании, при обязательном присутствии председателя комиссии ГЭК или его заместителя. При равном числе голосов голос председательствующего на заседании ГЭК является решающим.

На защиту дипломного проекта отводится до 30 минут.

Процедура защиты дипломного проекта включает доклад обучающегося (10-15 минут) с демонстрацией презентации, разбор отзыва руководителя и рецензии, вопросы членов комиссии, ответы обучающегося. Допускается выступление руководителя дипломного проекта, а также рецензента, если они присутствуют на защите.

Решение ГЭК оформляется протоколом, который подписывается председательствующим ГЭК, секретарем и членами комиссии ГЭК. В протоколе указываются оценка дипломного проекта, присуждение квалификации и особые мнения членов комиссии.

5 Показатели и критерии оценивания дипломного проекта и демонстрационного экзамена

5.1 Дипломный проект.

Основные требования и показатели, по которым производится оценка выполнения и защиты дипломного проекта и уровня профессиональной подготовленности обучающегося:

- соответствие темы исследования специальности, требованиям общепрофессиональной (специальной) подготовки, сформулированным целям и задачам;
- профессиональная компетентность, умение систематизировать и обобщать факты, самостоятельно решать поставленные задачи (в том числе и нестандартные) с использованием передовых научных технологий;
- структура работы и культура ее оформления; последовательность и логичность, завершенность изложения, наличие научно-справочного аппарата, стиль изложения;
- достоверность и объективность результатов дипломного проекта, использование в работе научных достижений отечественных и зарубежных исследователей, собственных исследований и реального опыта; логические аргументы; апробация в среде специалистов - практиков, преподавателей, исследователей и т.п.;
- использование современных информационных технологий, способность применять в работе математические методы исследований и вычислительную технику;
- выполнение и демонстрация практических результатов работы, позволяющие вести профессиональную деятельность в области профессиональной деятельности;
- возможность использования результатов в профессиональной практике для решения научных, творческих, организационно-управленческих, образовательных задач.

При оценке дипломного проекта дополнительно должны быть учтены качество сообщения, отражающего основные моменты дипломного проекта, и ответы выпускника на вопросы, заданные по теме его работы.

При определении окончательной оценки по защите дипломного проекта учитываются:

- доклад выпускника по каждому разделу;
- ответы на вопросы;
- оценка рецензента;
- отзыв руководителя.

Результаты защиты определяются оценками *«отлично», «хорошо», «удовлетворительно», «неудовлетворительно».*

«Отлично» выставляется за дипломный проект, который имеет положительные отзывы руководителя и рецензента. При его защите выпускник показывает глубокое знание вопросов темы, свободно оперирует данными исследования, вносит обоснованные предложения, во время доклада использует наглядные пособия, легко отвечает на поставленные вопросы.

«Хорошо» выставляется за дипломный проект, который имеет положительный отзыв руководителя и рецензента. При его защите выпускник показывает знания вопросов темы, оперирует данными исследования, вносит предложения по теме исследования, во время доклада использует наглядные пособия, без особых затруднений отвечает на поставленные вопросы.

«Удовлетворительно» выставляется за дипломный проект, в отзывах руководителя и рецензента которой имеются замечания по содержанию работы и методике анализа. При его защите выпускник проявляет неуверенность, показывает слабое знание вопросов темы, не всегда дает исчерпывающие аргументированные ответы на заданные вопросы.

«Неудовлетворительно» выставляется за дипломный проект, который не отвечает требованиям, изложенным в методических указаниях. В отзывах руководителя и рецензента имеются критические замечания. При защите дипломного проекта выпускник затрудняется отвечать на поставленные вопросы по теме, не знает теории вопроса, при ответе допускает существенные ошибки. К защите не подготовлены наглядные пособия.

Результаты проведения защиты дипломных проектов объявляются в тот же день после оформления протоколов (приложение) заседаний ГЭК.

5.2 Демонстрационный экзамен.

Процедура оценивания результатов выполнения заданий демонстрационного экзамена осуществляется членами экспертной группы по балльной системе в соответствии с требованиями комплекта оценочной документации.

Требования к оцениванию. Распределение значений максимальных баллов приведено в таблице 6.

Таблица 6

Вид аттестации	Уровень ДЭ	Составная часть КОД (инвариантная часть)	Максимальный балл
ГИА	ДЭ ПУ	инвариантная часть	75 из 75

Распределение баллов по критериям оценивания для ДЭ ПУ (инвариантная часть КОД) в рамках ГИА представлено в таблице 7.

Таблица 7

Вид деятельности	Критерий оценивания	Баллы
Выполнение работ по проектированию сетевой инфраструктуры	Участие в Баллы приемо-сдаточных испытаниях компьютерных сетей и сетевого оборудования различного уровня и в оценке качества и экономической эффективности сетевой топологии	1,00
	Осуществление выбора технологии, инструментальных 1,00 средств и средств вычислительной техники при организации процесса разработки и исследования объектов профессиональной деятельности	14,00
	Выполнение 14,00 проектирования кабельной структуры компьютерной сети	7,00
	Обеспечение защиты информации в сети с использованием программно-аппаратных средств	2,00
	Осуществление поиска, анализа и интерпретации информации, необходимой для выполнения задач профессиональной деятельности	3,00
Организация сетевого администрирования	Администрирование локальных вычислительных сетей и принятие мер по устранению возможных сбоев	21,00
	Администрирование ресурсов сетевых в системах информационных.	3,00
Эксплуатация объектов сетевой инфраструктуры	Проведение профилактических работ на объектах сетевой инфраструктуры и рабочих станциях	10,00
	Установка, настройка, эксплуатация и обслуживание сетевых конфигураций	4,00
	Участие в разработке схемы послеаварийного восстановления работоспособности компьютерной сети, выполнение восстановления и резервного копирования информации	4,00
	Установка, настройка, эксплуатация и обслуживание технических и программно-аппаратных средств компьютерных сетей.	6,00
	ИТОГО (инвариантная часть)	75,00

Схема перевода результатов демонстрационного экзамена из семидесяти пятибальной шкалы в пятибалльную представлена в таблице 8.

Таблица 8

Оценка (пятибалльная шкала)	«Неудовлетворительно»	«Удовлетворительно»	«Хорошо»	«Отлично»
Оценка в баллах (семидесяти пятибальная шкала)	0,0 – 37,4	37,5 – 48,6	48,7 – 67,4	67,5 - 75,0

Баллы выставляются в протоколе проведения демонстрационного экзамена (приложение), который подписывается каждым членом экспертной группы и

утверждается главным экспертом после завершения экзамена для экзаменационной группы.

При выставлении баллов присутствует член ГЭК, не входящий в экспертную группу, присутствие других лиц запрещено.

Подписанный членами экспертной группы и утвержденный главным экспертом протокол проведения демонстрационного экзамена далее передается в ГЭК для выставления оценок по итогам ГИА.

Оригинал протокола проведения демонстрационного экзамена передается на хранение в образовательную организацию в составе архивных документов.

Статус победителя, призера чемпионатов профессионального мастерства, проведенных Агентством (Союзом "Агентство развития профессиональных сообществ и рабочих кадров "Молодые профессионалы"), и участника национальной сборной России по профессиональному мастерству выпускника по профилю осваиваемой образовательной программы среднего профессионального образования засчитывается в качестве оценки "отлично" по демонстрационному экзамену в рамках проведения ГИА по данной образовательной программе среднего профессионального образования.

В случае досрочного завершения ГИА выпускником по независящим от него причинам результаты ГИА оцениваются по фактически выполненной работе, или по заявлению такого выпускника ГЭК принимается решение об аннулировании результатов ГИА, а такой выпускник признается ГЭК не прошедшим ГИА по уважительной причине.

Решения ГЭК принимаются на закрытых заседаниях простым большинством голосов членов ГЭК, участвующих в заседании, при обязательном присутствии председателя комиссии или его заместителя. При равном числе голосов голос председательствующего на заседании ГЭК является решающим.

Решение ГЭК оформляется протоколом, который подписывается председателем ГЭК, в случае его отсутствия заместителем ГЭК и секретарем ГЭК и хранится в архиве образовательной организации.

Выпускникам, не прошедшим ГИА по уважительной причине, в том числе не явившимся для прохождения ГИА по уважительной причине (далее - выпускники, не прошедшие ГИА по уважительной причине), предоставляется возможность пройти ГИА без отчисления из образовательной организации.

Выпускники, не прошедшие ГИА по неуважительной причине, в том числе не явившиеся для прохождения ГИА без уважительных причин (далее - выпускники, не прошедшие ГИА по неуважительной причине), и выпускники, получившие на ГИА неудовлетворительные результаты, могут быть допущены образовательной организацией для повторного участия в ГИА не более двух раз.

Дополнительные заседания ГЭК организуются в установленные образовательной организацией сроки, но не позднее четырех месяцев после подачи заявления выпускником, не прошедшим ГИА по уважительной причине.

Выпускники, не прошедшие ГИА по неуважительной причине, и выпускники, получившие на ГИА неудовлетворительные результаты, отчисляются из

образовательной организации и проходят ГИА не ранее чем через шесть месяцев после прохождения ГИА впервые.

Для прохождения ГИА выпускники, не прошедшие ГИА по неуважительной причине, и выпускники, получившие на ГИА неудовлетворительные результаты, восстанавливаются в образовательной организации на период времени, установленный образовательной организацией самостоятельно, но не менее предусмотренного календарным учебным графиком для прохождения ГИА соответствующей образовательной программы среднего профессионального образования.