

Аннотация рабочей программы
ГИА «ГОСУДАРСТВЕННАЯ ИТОГОВАЯ АТТЕСТАЦИЯ»
по специальности 09.02.06 Сетевое и системное администрирование
уровень подготовки – базовый

1. Область применения программы

Рабочая программа государственной итоговой аттестации является частью программы подготовки специалистов среднего звена в соответствии с ФГОС СПО по специальности 09.02.06 Сетевое и системное администрирование.

Государственная итоговая аттестация выпускника образовательного учреждения среднего профессионального образования является обязательной и осуществляется после освоения ППСЗ специальности 09.02.06 Сетевое и системное администрирование (базовой подготовки) в полном объеме.

Необходимым условием допуска к государственной итоговой аттестации является представление документов, подтверждающих освоение обучающимся компетенций при изучении теоретического материала и прохождении практики по каждому из основных видов профессиональной деятельности. В том числе выпускником могут быть представлены отчеты о ранее достигнутых результатах, дополнительные сертификаты, свидетельства (дипломы) олимпиад, конкурсов, творческие работы по специальности, характеристики с мест прохождения преддипломной практики.

2. Область применения программы государственной итоговой аттестации

В соответствии со ст.59 Федерального закона «Об образовании в Российской Федерации» государственная итоговая аттестация (ГИА) обучающихся, завершающих обучение по основным профессиональным образовательным программам среднего профессионального образования, обязательной.

Государственная итоговая аттестация проводится для установления степени готовности обучающихся к самостоятельной деятельности и уровня сформированности у них соответствующих профессиональных компетенций.

Государственная итоговая аттестация выпускника образовательного учреждения среднего профессионального образования является обязательной и осуществляется после освоения ППСЗ специальности 09.02.06 Сетевое и системное администрирование (базовой подготовки) в полном объеме.

Необходимым условием допуска к государственной итоговой аттестации является представление документов, подтверждающих освоение обучающимся компетенций при изучении теоретического материала и прохождении практики по каждому из основных видов профессиональной деятельности. В том числе выпускником могут быть представлены отчеты о ранее достигнутых результатах, дополнительные сертификаты, свидетельства (дипломы) олимпиад, конкурсов, творческие работы по специальности, характеристики с мест прохождения преддипломной практики.

В соответствии с ФГОС СПО по данному направлению подготовки областью профессиональной деятельности выпускников является: сопровождение, настройка и администрирование системного и сетевого программного обеспечения; эксплуатация и обслуживание серверного и сетевого оборудования; диагностика и мониторинг работоспособности программно-технических средств; обеспечение целостности резервирования информации информационной безопасности объектов сетевой инфраструктуры.

Объектами профессиональной деятельности выпускников являются:

- комплексы и системы на основе аппаратных, программных и коммуникационных компонентов информационных технологий;
- средства обеспечения информационной безопасности;
- инструментальные средства для эксплуатации сетевых конфигураций;
- инструментарий поддержки сетевых конфигураций;
- сетевые ресурсы в информационных системах;
- мероприятия технического контроля работоспособности компьютерных сетей;

Виды профессиональной деятельности выпускника:

- выполнение работ по проектированию сетевой инфраструктуры;
- организация сетевого администрирования;
- эксплуатация объектов сетевой инфраструктуры.

3. Цели и задачи государственной итоговой аттестации

Целью государственной итоговой аттестации является установление соответствия уровня освоенности компетенций, обеспечивающих соответствующую квалификацию и уровень образования обучающихся, Федеральному государственному образовательному стандарту среднего профессионального образования. Государственная итоговая аттестация призвана способствовать систематизации и закреплению знаний и умений обучающегося по специальности при решении конкретных профессиональных задач, определять уровень подготовки выпускника к самостоятельной работе.

Главной задачей по реализации требований Федерального государственного образовательного стандарта является реализация практической направленности подготовки специалистов со средним профессиональным образованием. Это требует перестройки всего учебного процесса, в том числе критериев и подходов к государственной итоговой аттестации студентов. Конечной целью обучения является подготовка специалиста, обладающего не только и не столько совокупностью теоретических знаний, но, в первую очередь, специалиста, готового решать профессиональные задачи. Отсюда коренным образом меняется подход к оценке качества подготовки специалиста. Упор делается на оценку умения самостоятельно решать профессиональные задачи. Поэтому при разработке программы государственной итоговой аттестации учтена степень использования наиболее значимых профессиональных компетенций и необходимых для них знаний и умений.

4. Перечень планируемых результатов освоения СПО

Выпускник, освоивший основную профессиональную образовательную программу среднего профессионального образования по специальности 09.02.06 Сетевое и системное администрирование должен обладать *общими компетенциями, включающими в себя способность:*

ОК 01 Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам.

ОК 02 Осуществлять поиск, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности.

ОК 03 Планировать и реализовывать собственное профессиональное и личностное развитие.

ОК 04 Работать в коллективе и команде, эффективно взаимодействовать с коллегами, руководством, клиентами.

ОК 05 Осуществлять устную и письменную коммуникацию на

государственном языке с учетом особенностей социального и культурного контекста.

ОК 06 Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных общечеловеческих ценностей, применять стандарты антикоррупционного поведения.

ОК 07 Содействовать сохранению окружающей среды, ресурсосбережению, 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 Использовать информационные технологии в профессиональной деятельности.

ОК 10 Пользоваться профессиональной документацией на государственном и иностранном языках.

ОК 11. Использовать знания по финансовой грамотности, планировать предпринимательскую деятельность в профессиональной сфере.

Выпускник должен обладать профессиональными компетенциями, соответствующими основным видам профессиональной деятельности:

Выполнение работ по проектированию сетевой инфраструктуры

ПК 1.1. Выполнять проектирование кабельной структуры компьютерной сети.

ПК 1.2. Осуществлять выбор технологии, инструментальных средств и средств вычислительной техники при организации процесса разработки и исследования объектов профессиональной деятельности.

ПК 1.3. Обеспечивать защиту информации в сети с использованием программно-аппаратных средств.

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.

ПК 1.5. Выполнять требования нормативно-технической документации, иметь опыт оформления проектной документации.

Организация сетевого администрирования

ПК 2.1. Администрировать локальные вычислительные сети и принимать меры по устранению возможных сбоев.

ПК 2.2. Администрировать сетевые ресурсы в информационных системах.

ПК 2.3. Обеспечивать сбор данных для анализа использования и функционирования программно-технических средств компьютерных сетей.

ПК 2.4. Взаимодействовать со специалистами смежного профиля при разработке методов, средств и технологий применения объектов профессиональной деятельности.

Эксплуатация объектов сетевой инфраструктуры

ПК 3.1. Устанавливать, настраивать, эксплуатировать и обслуживать технические и программно-аппаратные средства компьютерных сетей.

ПК 3.2. Проводить профилактические работы на объектах сетевой инфраструктуры и рабочих станциях.

ПК 3.3. Устанавливать, настраивать, эксплуатировать и обслуживать сетевые конфигурации.

ПК 3.4. Участвовать в разработке схемы послеаварийного восстановления

работоспособности компьютерной сети, выполнять восстановление и резервное копирование информации.

ПК 3.5. Организовывать инвентаризацию технических средств сетевой инфраструктуры, осуществлять контроль оборудования после его ремонта.

ПК 3.6. Выполнять замену расходных материалов и мелкий ремонт периферийного оборудования, определять устаревшее оборудование и программные средства сетевой инфраструктуры.

5. Распределение времени на подготовку и проведение государственной итоговой аттестации

Этапы итоговой государственной аттестации	Количество недель
1. Выполнение выпускной квалификационной работы	4
2. Защита выпускной квалификационной работы	2
Всего	6

6. Примерная тематика выпускных квалификационных работ

1. Оценка различных способов повышения достоверности информации в сетях.

2. Эффективность функционирования компьютерных сетей (КС) и пути ее повышения.

3. Организация работы офисной сети под управлением конкретной ОС.

4. Анализ методов и средств администрирования сетей.

5. Методы и средства удаленного доступа.

6. Анализ среды передачи данных в вычислительных сетях.

7. Интеграция разнородных сетей.

8. Организация доступа в Интернет в корпоративных сетях.

9. Стратегия поиска и обмена информацией в Internet.

10. Оценка структур и процессов функционирования спутниковых сетей.

11. Развитие беспроводных технологий в России.

12. Развитие технологии Ethernet.

13. Перспективы развития компьютерных сетей.

14. Построение корпоративных компьютерных сетей (ККС) на базе ОС семейства Windows.

15. Методы и средства защиты информации в сетях.

16. Программные средства защиты информации в сетях.

17. Анализ глобальных сетей с коммутацией каналов.

18. Анализ протоколов канального уровня для выделенных линий.

19. Анализ и реализация облачных систем обработки данных.

20. Состав и характеристика сетевого оборудования ЛВС.

21. Состав и характеристика сетевого оборудования ККС.

22. Проектирование локальных вычислительных сетей.

23. Проектирование структурированных вычислительных сетей.

24. Организация и функционирование виртуальных ЛВС.

25. Обеспечение дуплексного режима работы на основе технологий FDM, NDM и WDM.

26. Повышение качества обслуживания в сетях с коммутацией пакетов.
27. Методы и средства обеспечения синхронной и асинхронной передачи данных в сетях.
28. Применение корпоративных информационных порталов (КИП).
29. Структура и функции системы обеспечения безопасности в ККС.
30. Способы и средства установки и обеспечения связи ЛВС с удаленными абонентами.
31. Технологии криптографической защиты информации.
32. Методы управления средствами сетевой безопасности.
33. Построение системы информационной безопасности ККС.
34. Анализ применения спутниковых систем связи в Интернет.
35. Анализ методов и средств высокоскоростного доступа в Интернет.
36. Технологии администрирования и контроля в компьютерных сетях.
37. Технологии защиты межсетевое обмена данными.
38. Организация доступа в Интернет по сетям кабельного телевидения.
39. Организация удаленного доступа к распределенным базам данных.
40. Обеспечение безопасности сети предприятия на базе ОС Linux.
41. Обеспечение безопасности сети предприятия на базе ОС Windows.
42. Организация беспроводной территориально-распределенной компьютерной сети предприятия.
43. Имитационное моделирование компьютерных сетей.

Образец задания Демонстрационного экзамена

Модуль 1: Выполнение работ по проектированию сетевой инфраструктуры

Задание модуля 1:

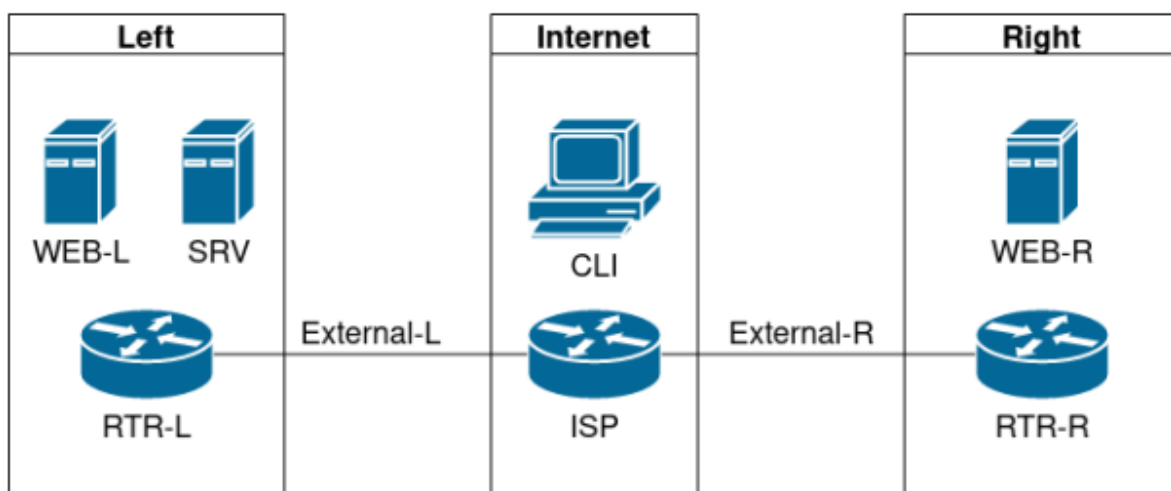


Рисунок 1. Топология

1. Выполнение проектирования кабельной структуры компьютерной сети.

Виртуальные машины и коммутация

Необходимо выполнить создание и базовую конфигурацию виртуальных машин.

1.1. На основе предоставленных ВМ или шаблонов ВМ создайте отсутствующие виртуальные машины в соответствии со схемой.

- a. Характеристики ВМ установите в соответствии с **Таблицей 1**;
 б. Коммутацию (если таковая не выполнена) выполните в соответствии со схемой сети.

1.2. Имена хостов в созданных ВМ должны быть установлены в соответствии со схемой.

1.3. Адресация должна быть выполнена в соответствии с Таблицей 1;

1.4. Обеспечьте ВМ дополнительными дисками, если таковое необходимо в соответствии с **Таблицей 1**.

Таблица 1. Характеристики ВМ

Имя ВМ	ОС	ОЗУ	Кол- во ядер	IP-адреса	Дополнительно
RTR- L	Debian 11	2 Гб	2	4.4.4.100/24 192.168.200.254/ 24	
	Cisco CSR		4		
RTR- R	Debian 11	2 Гб	2	5.5.5.100/24 172.16.100.254/2 4	
	Cisco CSR	4 Гб	4		
SRV	Debian 11	2 Гб	2		
	Windows Server 2019	4 Гб	4	192.168.200.200/ 24	Дополнительные диски: 2 шт по 2 Гб
WEB- L	Debian 11	2 Гб	2	192.168.200.100/ 24	
WEB- R	Debian 11	2 Гб	2	172.16.100.100/2 4	
ISP	Debian 11	2 Гб	2	4.4.4.1/24 5.5.5.1/24 3.3.3.1/24	
CLI	Windows 10	4	4	3.3.3.10/24	

2. Осуществление выбора технологии, инструментальных средств и средств вычислительной техники при организации процесса разработки и исследования объектов профессиональной деятельности

Сетевая связанность

2.1. Настройте статический маршрут по умолчанию на маршрутизаторах **RTR-L** и **RTR-R**.

2.2. Настройте динамическую трансляцию портов (PAT):

- На маршрутизаторе **RTR-L** настройте динамическую трансляцию портов (PAT) для сети 192.168.200.0/24 в соответствующие адреса исходящего интерфейса

- На маршрутизаторе **RTR-R** настройте динамическую трансляцию портов (PAT) для сети 172.16.100.0/24 в соответствующие адреса исходящего интерфейса.

Конфигурация виртуальных частных сетей

2.3. Между платформами **RTR-L** и **RTR-R** должен быть установлен туннель, позволяющий осуществлять связь между регионами с применением внутренних адресов со

следующими параметрами:

- a) Используйте в качестве VTI интерфейс Tunnel1
- b) Между платформами должен быть установлен туннель, позволяющий осуществлять связь между регионами с применением внутренних адресов

Настройка маршрутизации

2.4. Настройте динамическую маршрутизацию между платформами **RTR-L** и **RTR-R**.

2.5. Трафик, идущий по туннелю между регионами по внутренним адресам, не должен транслироваться.

Модуль 2: Организация сетевого администрирования

Таблица 2. DNS-записи зон

Зона	Тип записи	Ключ	Значение
demo.wsr	A	ISP	3.3.3.1
	A	www	4.4.4.100
	A	www	5.5.5.100
	CNAME	internet	ISP
int.demo.wsr	A	web-l	192.168.200.100
	A	WEB-R	172.16.100.100
	A	SRV	192.168.200.200
	A	rtr-l	192.168.200.254
	A	rtr-r	172.16.100.254
	CNAME	webapp-L	web-l
	CNAME	webapp-R	WEB-R
	CNAME	ntp	SRV
	CNAME	dns	SRV

1. Администрирование локальных вычислительных сетей и принятие мер по устранению возможных сбоев

Сетевая связность.

В рамках данного модуля требуется обеспечить сетевую связность между регионами работы приложения, а также обеспечить выход ВМ в имитируемую сеть “Интернет”.

1.1. Сети, подключенные к **ISP**, считаются внешними:

- Запрещено прямое попадание трафика из внутренних сетей во внешние и наоборот;

1.2. Обеспечьте настройку служб SSH региона Left:

a. Подключения со стороны внешних сетей по протоколу к платформе управления трафиком **RTR-L** на порт 2244 должны быть перенаправлены на ВМ **Web-L**;

b. Подключения со стороны внешних сетей по протоколу к платформе управления трафиком **RTR-R** на порт 2222 должны быть перенаправлены на ВМ **WEB-R**.

2. Администрирование сетевых ресурсов в информационных системах

Инфраструктурные службы.

В рамках данного модуля необходимо настроить основные инфраструктурные службы и настроить представленные ВМ на применение этих служб для всех основных функций.

2.1. Выполните настройку первого уровня DNS-системы стенда:

a. Используется ВМ **ISP**;

b. Обслуживается зона demo.wsr.

- Наполнение зоны должно быть реализовано в соответствии с Таблицей 2;

c. Сервер делегирует зону int.demo.wsr на **SRV**;

- Поскольку **SRV** находится во внутренней сети западного региона, делегирование происходит на внешний адрес маршрутизатора данного региона.

- Маршрутизатор региона должен транслировать соответствующие порты DNS-службы в порты сервера **SRV**.

d. Внешний клиент **CLI** должен использовать DNS-службу, развернутую на **ISP**, по умолчанию;

2.2. Выполните настройку второго уровня DNS-системы стенда;

a. Используется ВМ **SRV**;

b. Обслуживается зона int.demo.wsr;

- Наполнение зоны должно быть реализовано в соответствии с Таблицей 2;

c. Обслуживаются обратные зоны для внутренних адресов регионов

- Имена для разрешения обратных записей следует брать из Таблицы 2;

d. Сервер принимает рекурсивные запросы, исходящие от адресов внутренних регионов;

- Обслуживание клиентов(внешних и внутренних), обращающихся к к зоне int.demo.wsr, должно производиться без каких либо ограничений по адресу источника;

e. Внутренние хосты регионов (равно как и платформы управления трафиком) должны использовать данную DNS-службу для разрешения всех запросов имен;

2.3. Выполните настройку первого уровня системы синхронизации времени:

a. Используется сервер **ISP**.

b. Сервер считает собственный источник времени верным, stratum=3;

c. Сервер допускает подключение только через внешний адрес соответствующей платформы управления трафиком;

- Подразумевается обращение **SRV** для синхронизации времени;

d. Клиент **CLI** должен использовать службу времени **ISP**;

e. Выполните конфигурацию службы второго уровня времени на **SRV**.

a. Сервер синхронизирует время с хостом **ISP**;

- Синхронизация с другими источникам запрещена;

b. Сервер должен допускать обращения внутренних хостов регионов, в том числе и платформ управления трафиком, для синхронизации времени;

c. Все внутренние хосты(в том числе и платформы управления трафиком) должны синхронизировать свое время с **SRV**;

2.5. Реализуйте файловый SMB-сервер на базе **SRV**

a. Сервер должен предоставлять доступ для обмена файлами серверам **WEB-L** и **WEB-R**;

b. Сервер, в зависимости от ОС, использует следующие каталоги для хранения файлов:

– /mnt/storage для система на базе Linux;

– Диск R:\ для систем на базе Windows;

c. Хранение файлов осуществляется на диске (смонтированном по указанным выше адресам), реализованном по технологии RAID типа “Зеркало”;

2.6. Сервера **WEB-L** и **WEB-R** должны использовать службу, настроенную на **SRV**, для обмена файлами между собой:

a. Служба файлового обмена должна позволять монтирование в виде стандартного каталога Linux;

- Разделяемый каталог должен быть смонтирован по адресу /opt/share;

b. Каталог должен позволять удалять и создавать файлы в нем для всех пользователей;

2.7. Выполните настройку центра сертификации на базе **SRV**:

b. В случае применения решения на базе Linux используется центр сертификации типа OpenSSL и располагается по адресу /var/ca;

c. Выдаваемые сертификаты должны иметь срок жизни не менее 300 дней;

d. Параметры выдаваемых сертификатов:

- Страна RU;

- Организация DEMO.WSR;

- Прочие поля (за исключением CN) должны быть пусты;

3. Взаимодействие со специалистами смежного профиля при разработке методов, средств и технологий применения объектов профессиональной деятельности

Инфраструктура веб-приложения.

Данный блок подразумевает установку и настройку доступа к веб-приложению, выполненному в формате контейнера Docker.

3.1. Образ Docker (содержащий веб-приложение) расположен на ISO-образе дополнительных материалов;

a. Выполните установку приложения AppDocker0;

3.2. Пакеты для установки Docker расположены на дополнительном ISO-образе;

3.3. Инструкция по работе с приложением расположена на дополнительном ISO-образе;

3.4. Необходимо реализовать следующую инфраструктуру приложения.

a. Клиентом приложения является **CLI** (браузер Edge);

b. Хостинг приложения осуществляется на **VM WEB-L** и **WEB-R**;

c. Доступ к приложению осуществляется по DNS-имени www.demo.wsr;

- Имя должно разрешаться во “внешние” адреса VM управления трафиком в обоих регионах;

- При необходимости, для доступа к приложению допускается реализовать реверс-прокси или трансляцию портов;

d. Доступ к приложению должен быть защищен с применением технологии TLS;

- Необходимо обеспечить корректное доверие сертификату сайта, без применения “исключений” и подобных механизмов;

e. Незащищенное соединение должно переводиться на защищенный канал автоматически;

3.5. Необходимо обеспечить отказоустойчивость приложения;

a. Сайт должен продолжать обслуживание (с задержкой не более 25 секунд) в следующих сценариях:

- Отказ одной из VM Web

- Отказ одной из ВМ управления трафиком.

Модуль 3: Эксплуатация объектов сетевой инфраструктуры

Задание модуля 3:

1. Установка, настройка, эксплуатация и обслуживание технических и программно-аппаратных средств компьютерных сетей

Конфигурация виртуальных частных сетей

1.1. Защита туннеля должна обеспечиваться с помощью **IPsec** между платформами **RTR-L** и **RTR-R**.

- a) Используйте аутентификацию по общему ключу.
- b) Параметры **IPsec** произвольные.

2. Установка, настройка, эксплуатация и обслуживание сетевых конфигураций.

Настройка списков контроля доступа

2.1. Платформа управления трафиком **RTR-R** выполняет контроль входящего трафика согласно следующим правилам:

- a. Разрешаются подключения к портам HTTP и HTTPS для всех клиентов;
- b. Разрешаются подключения к портам HTTP и HTTPS для всех клиентов;
- Порты необходимо для работы настраиваемых служб
- c. Разрешается работа выбранного протокола организации защищенной связи;
- Разрешение портов должно быть выполнено по принципу “необходимо и достаточно”
- d. Разрешается работа протоколов ICMP;
- e. Разрешается работа протокола SSH;
- f. Прочие подключения запрещены;
- g. Для обращений в платформам со стороны хостов, находящихся внутри регионов, ограничений быть не должно;

2.2. Платформа управления трафиком **RTR-L** выполняет контроль входящего трафика согласно следующим правилам:

- a. Разрешаются подключения к портам DNS, HTTP и HTTPS для всех клиентов;
-Порты необходимо для работы настраиваемых служб
- b. Разрешается работа выбранного протокола организации защищенной связи;
- Разрешение портов должно быть выполнено по принципу “необходимо и достаточно”
- c. Разрешается работа протоколов ICMP;
- d. Разрешается работа протокола SSH;
- e. Прочие подключения запрещены;
- f. Для обращений к платформам со стороны хостов, находящихся внутри регионов, ограничений быть не должно.