РОССИЙСКАЯ ФЕДЕРАЦИЯ
РЕСПУБЛИКА ИНГУШЕТИЯ

РОССЕ ФЕДЕРАЦИ
ГІАЛГІАЙ МОХК

Министерство образования и науки Республики Ингушетия
Государственное бюджетное профессиональное образовательное учреждение
“Колледж сервиса и быта”

УТВЕРЖДАЮ:
Директор ГБПОУ «КСИБ»
Зязиков А.А

Цифровая Подпись:Зязиков Аслан Аскабович
DN:CN=Зязиков Аслан Аскабович, SN=Зязиков, G=Аслан Аскабович, E=gpu2@mail.ru, ИНН=060600902961, СНИЛС=14234495752, O="ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ПРОФЕССИОНАЛЬНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ""КОЛЛЕДЖ СЕРВИСА И БЫТА""", T=Директор, L=назрань, S=Республика Ингушетия, C=RU
Дата:2023.05.30 21:09:18 +03:00

# ПРОГРАММА

# ГОСУДАРСТВЕННОЙ ИТОГОВОЙ АТТЕСТАЦИИ

По специальности

**10.02.04 Обеспечение информационной безопасности телекоммуникационных систем**

Квалификация – техник по защите информации

Назрань
2022г.

Данная программа составлена в соответствии с требованиями

Федерального государственного образовательного стандарта среднего профессионального образования по специальности 10.02.04 «Обеспечение информационной безопасности телекоммуникационных систем» (далее – ФГОС СПО), утвержденного приказом Министерства образования и науки от 9 декабря 2016 года № 1553 (зарегистрирован Министерством юстиции Российской Федерации 26 декабря 2016 г. № 44938).

Программа обсуждена на заседании кафедры профессиональных и специальных дисциплин 04.12.2022г., протокол №4

Зав. кафедрой _____Ажигова Р.А

Согласована с работодателем: директор ООО «ИТТ»

_____Зурабов М.М.

Программа утверждена на заседание учебно- методического совета колледжа
От 07.12.2022 г.

**Содержание**

1 Общие положения 4

1.1 Общая характеристика программы государственной итоговой аттестации 4

1.2 Нормативные документы, регламентирующие проведение государственной итоговой аттестации 4

1.3 Цель и задачи государственной итоговой аттестации, формы проведения 5

1.4 Требования к результатам освоения основной образовательной программы 6

2 Процедура проведения государственной итоговой аттестации 8

3 Порядок апелляции по результатам государственной итоговой аттестации 23

## 1 ОБЩИЕ ПОЛОЖЕНИЯ

### 1.1 Общая характеристика программы государственной итоговой аттестации

Программа государственной итоговой аттестации (далее - Программа) разработана на основании требований ФГОС СПО по специальности 10.02.04 Обеспечение информационной безопасности телекоммуникационных систем, утвержденного приказом Минобрнауки России 9 декабря 2016 г. N 1551.

Программа является частью основной образовательной программы по специальности 10.02.04 Обеспечение информационной безопасности телекоммуникационных систем и устанавливает процедуру организации и проведения государственной итоговой аттестации (далее - ГИА) обучающихся.

### 1.2 Нормативные документы, регламентирующие проведение итоговой аттестации

Нормативно-правовую базу разработки программы ГИА по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем составляют:

– Федеральный закон от 29.12.2012 г. № 273-ФЗ «Об образовании в Российской Федерации»;

– приказ Минобрнауки России от 16.08.2013 № 968 «Об утверждении Порядка проведения государственной итоговой аттестации по образовательным программам среднего профессионального образования»;

– приказ Минобрнауки России от 14.06.2013 № 464 «Об утверждении Порядка организации и осуществления образовательной деятельности по образовательным программам среднего профессионального образования»;

– приказ Минобрнауки России от 31.01.2014 № 74 «О внесении изменений в Порядок проведения государственной итоговой аттестации по образовательным программам среднего профессионального образования», утвержденный приказом Министерства образования и науки Российской Федерации от 16.08.2013 г. №968;

– приказ Минобрнауки России от 17.11.2017 № 1138 «О внесении изменений в Порядок проведения государственной итоговой аттестации по образовательным программам среднего профессионального образования», утвержденный приказом Министерства образования и науки Российской Федерации от 16.08.2013 г. №968;

– письмо Министерства образования и науки Российской Федерации от 20.07.2015 № 06-846 «О направлении методических рекомендаций»;

– распоряжение Министерства просвещения Российской Федерации от 01 апреля 2019 № З-42 «Об утверждении методических рекомендаций о проведении аттестации с использованием механизма демонстрационного экзамена»;

– приказ союза «Агентство развития профессиональных сообществ и рабочих кадров «Молодые профессионалы» от 31.01.2019 г № 31.01.2019-1 «Об утверждении Методики организации и проведения демонстрационного экзамена по стандартам «Молодые профессионалы Россия»;

– федеральный государственный образовательный стандарт среднего профессионального образования по специальности 10.02.04 Обеспечение информационной безопасности телекоммуникационных систем) от 09.12.2016 г.;

- положение П-ОГУ 85-05-03-2018 «О порядке организации выполнения и защиты выпускной квалификационной работы обучающимися среднего профессионального образования выпускной квалификационной работе».

### 1.3 Цель и задачи государственной итоговой аттестации

Целью государственной итоговой аттестации является установление соответствия уровня подготовленности выпускника к выполнению профессиональных задач в соответствии с требованиями ФГОС СПО к результатам освоения программы подготовки специалистов среднего звена по специальности 10.02.04 Обеспечение информационной безопасности телекоммуникационных систем.

Задачами ГИА являются:

- установление соответствия результатов освоения обучающимися программы подготовки специалистов среднего звена по специальности 10.02.04 Обеспечение информационной безопасности телекоммуникационных систем соответствующим требованиям ФГОС СПО;
- овладение выпускниками компетенциями, необходимыми для осуществления профессиональной деятельности в соответствии с ФГОС СПО по специальности 10.02.04 Обеспечение информационной безопасности телекоммуникационных систем;
- разработка рекомендаций по совершенствованию подготовки обучающихся соответствующего уровня профессионального образования.

### 1.4 Требования к результатам освоения основной образовательной программы

Выпускник по специальности 10.02.04 Обеспечение информационной безопасности телекоммуникационных систем должен обладать следующими компетенциями:

Таблица 1 -Требования к результатам освоения основной образовательной программы

| Коды | Краткое содержание / определение компетенции. |
|---|---|
| **Общие компетенции** | |
| ОК 1 | Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам. |
| ОК 2 | Осуществлять поиск, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности. |
| ОК 3 | Планировать и реализовывать собственное профессиональное и личностное развитие. |
| ОК 4 | Работать в коллективе и команде, эффективно взаимодействовать с коллегами, руководством, клиентами. |
| ОК 5 | Осуществлять устную и письменную коммуникацию на государственном языке с учетом особенностей социального и культурного контекста. |
| ОК 6 | Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных общечеловеческих ценностей, применять стандарты антикоррупционного поведения. |
| ОК 7 | Содействовать сохранению окружающей среды, ресурсосбережению, эффективно действовать в чрезвычайных ситуациях. |
| ОК 8 | Использовать средства физической культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и поддержания необходимого уровня физической подготовленности. |
| ОК 9 | Использовать информационные технологии в профессиональной деятельности. |
| ОК 10 | Пользоваться профессиональной документацией на государственном и иностранном языке. |
| ОК 11 | Использовать знания по финансовой грамотности, планировать предпринимательскую деятельность в профессиональной сфере. |
| **Профессиональные компетенции** | |
| **Эксплуатация информационно-телекоммуникационных систем и сетей** | |
| ПК 1.1. | Производить монтаж, настройку, проверку функционирования и конфигурирование оборудования информационно-телекоммуникационных систем и сетей |
| ПК 1.2. | Осуществлять диагностику технического состояния, поиск неисправностей и ремонт оборудования информационно-телекоммуникационных систем и сетей. |

| | |
|---|---|
| ПК 1.3. | Проводить техническое обслуживание оборудования информационнотелекоммуникационных систем и сетей. |
| ПК 1.4. | Осуществлять контроль функционирования информационнотелекоммуникационных систем и сетей. |
| **Защита информации в информационно-телекоммуникационных системах и сетях с использованием программных и программно-аппаратных, в том числе криптографических средств защиты** | |
| ПК 2.1. | Производить установку, настройку, испытания и конфигурирование программных и программно-аппаратных, в том числе криптографических средств защиты информации от несанкционированного доступа и специальных воздействий в оборудование информационнотелекоммуникационных систем и сетей. |
| ПК 2.2. | Поддерживать бесперебойную работу программных и программноаппаратных, в том числе криптографических средств защиты информации в информационно-телекоммуникационных системах и сетях. |
| ПК 2.3. | Осуществлять защиту информации от несанкционированных действий и специальных воздействий в информационно-телекоммуникационных системах и сетях с использованием программных и программно-аппаратных, в том числе криптографических средств в соответствии с предъявляемыми требованиями. |
| **Защита информации в информационно-телекоммуникационных системах и сетях с использованием технических средств защиты** | |
| ПК 3.1. | Производить установку, монтаж, настройку и испытания технических средств защиты информации от утечки по техническим каналам в информационнотелекоммуникационных системах и сетях. |
| ПК 3.2. | Проводить техническое обслуживание, диагностику, устранение неисправностей и ремонт технических средств защиты информации, используемых в информационно-телекоммуникационных системах и сетях. |
| ПК 3.3. | Осуществлять защиту информации от утечки по техническим каналам в информационно-телекоммуникационных системах и сетях с использованием технических средств защиты в соответствии с предъявляемыми требованиями. |
| ПК 3.4. | Проводить отдельные работы по физической защите линий связи информационно-телекоммуникационных систем и сетей. |
| **Выполнение работ по одной или нескольким профессиям рабочих, должностям служащих** | |
| ПК 4.1 | Выполнять монтаж и настройку сетей проводного и беспроводного абонентского доступа в соответствии с действующими отраслевыми стандартами; |
| ПК 4.2 | Выполнять монтаж, демонтаж и техническое обслуживание кабелей связи и оконечных структурированных кабельных устройств в соответствии с действующими стандартами; |

| | |
|---|---|
| ПК 4.3 | Выполнять монтаж, демонтаж, первичную инсталляцию, мониторинг, диагностику инфокоммуникационных систем передачи в соответствии с действующими отраслевыми стандартами. |

## 2 . Процедура проведения государственной итоговой аттестации

К государственной итоговой аттестации допускаются обучающиеся, не имеющие академической задолженности и в полном объёме выполнившие учебный план или индивидуальный учебный план.

Для проведения государственной итоговой аттестации в филиале создаются государственные экзаменационные комиссии (далее - ГЭК), которые действуют в течение календарного года. Состав экзаменационных комиссий утверждается приказом директора филиала.

ГЭК формируется из педагогических работников, «КСИБ» лиц, приглашённых из сторонних организаций, в том, числе: педагогических работников, представителей организаций-партнеров, направление деятельности которых соответствует области профессиональной деятельности, к которой готовятся выпускники; экспертов организации, наделенной полномочиями по обеспечению прохождения ГИА в форме демонстрационного экзамена (далее - оператор) (при проведении ГИА в форме демонстрационного экзамена), экспертов организации, обладающих профессиональными знаниями, навыками и опытом в сфере, соответствующей профессии, специальности среднего профессионального образования, по которой проводится демонстрационный экзамен (далее - эксперты). ГЭК возглавляет председатель, который организует и контролирует её деятельность, обеспечивает единство требований, предъявляемых к выпускникам. Председателем ГЭК утверждается, лицо, не работающее в «КСИБ» из числа:

- руководителей или заместителей руководителей организаций, осуществляющих образовательную деятельность, соответствующую области профессиональной деятельности, к которой готовятся выпускники; представителей работодателей или их объединений;
- организаций-партнеров, включая экспертов, при условии, что направление деятельности данных представителей соответствует области профессиональной деятельности, к которой готовятся выпускники.

Для проведения демонстрационного экзамена при государственной экзаменационной комиссии создается экспертная группа, которую возглавляет главный эксперт. Количество экспертов, входящих в состав экспертной группы, определяется на основе условий, указанных в комплекте оценочной документации для проведения демонстрационного экзамена.

Решение ГЭК оформляется протоколом, который подписывается председателем государственной экзаменационной комиссии (в случае отсутствия председателя - его заместителем) и секретарём государственной экзаменационной комиссии и хранится в архиве колледжа.

Результаты защиты выпускной квалификационной работы (дипломного проекта) определяются оценками «отлично», «хорошо», «удовлетворительно», «неудовлетворительно».

Дополнительные заседания ГЭК организуются в установленные филиалом сроки, но не позднее четырёх месяцев после подачи заявления лицом, не проходившим ГИА по уважительной причине.

Для прохождения ГИА лицо, не прошедшее ГИА по неуважительной причине или получившее на ГИА неудовлетворительную оценку, восстанавливается в филиал ОГУ имени И.С. Тургенева на период времени, установленный филиалом в соответствии с календарным учебным графиком для прохождения ГИА соответствующей ОП СПО. Повторное прохождение ГИА для одного лица назначается не более двух раз. В этом случае ГЭК может признать целесообразным повторную защиту обучающимся той же ВКР, либо вынести решение о закреплении за ним нового задания на ВКР и определить срок повторной защиты, но не ранее, чем через шесть месяцев.

Обучающемуся, получившему оценку «неудовлетворительно» при защите ВКР (дипломного проекта) выдается справка об обучении или о периоде обучения по образцу, самостоятельно устанавливаемому «КСИБ».

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

Результаты защиты выпускной квалификационной работы (дипломного проекта) вместе с решением ГЭК о присвоении соответствующей квалификации и выдаче диплома заносится в зачетную книжку обучающегося и подписывается председателем ГЭК.

**Выпускная квалификационная работа (дипломный проект)**

Выпускная квалификационная работа выпускника по специальности 10.02.04 Обеспечение информационной безопасности телекоммуникационных систем предусматривает выполнение дипломного проекта.

Выпускная квалификационная работа (дипломный проект) направлен на систематизацию и закрепление знаний выпускника по специальности, а также определение уровня готовности выпускника к самостоятельной профессиональной деятельности. ВКР (дипломный проект) предполагает самостоятельную подготовку (написание) выпускником проекта, демонстрирующего уровень знаний выпускника в рамках выбранной темы и сформированность его профессиональных умений и навыков.

Выпускнику предоставляется право выбора темы выпускной квалификационной работы (дипломного проекта), в том числе предложения своей темы с необходимым обоснованием целесообразности ее разработки для практического применения. При этом тема ВКР (дипломного проекта) должна соответствовать содержанию одного или нескольких профессиональных модулей, входящих в ОП СПО.

Выпускная квалификационная работа (дипломный проект) является самостоятельной разработкой и решением конкретной комплексной задачи, включающей в себя обзор и критический анализ современного состояния вопроса, выбор и обоснование способа (метода) решения поставленной задачи.

В процессе выполнения и защиты выпускной квалификационной работы (дипломного проекта) обучающийся должен подтвердить свою подготовленность к самостоятельной профессиональной деятельности и право на присвоение ему квалификации техника.

Выпускная квалификационная работа (дипломный проект) (50 листов формата А4) состоит из пояснительной записки, проектной (практической) части и презентационного материала.

Пояснительная записка имеет следующее содержание:

1 Теоретический раздел - дается обзор и теоретические основы рассматриваемой проблемы, динамика развития исследуемой темы, анализ отечественного и международного опыта, накопленного в данной области.

2 Аналитический раздел выполняется с учетом данных, полученных в результате анализа теоретического раздела, включает в себя исследования, расчёты, выводы и обоснования, предложения по улучшению и т.д.

3 Практический раздел включает в себя выполнение практического задания, написание исходного кода программы, сборку модели или устройства, выполнение практических действий по сборке, ремонту, установке и модификации материальных и программных комплексов и т.д.

4 Технико-экономический раздел, включающий в себя расчёт экономической эффективности проекта.

5 Охрана труда и техника безопасности.

В проектной (практической) части выделяются три направления:

- разработка проекта по модернизации программно-аппаратных и инженернотехнических средств защиты информации;
- разработка проекта по организации защиты информации на предприятии;
- разработка программ для шифрования, дешифрования на основе различных алгоритмов;
- проектирование стендов согласно профилю специальности.

Иногда в тематике дипломного проектирования невозможно провести четкую грань между разработкой аппаратных и программных средств, так как задача, поставленная перед дипломником, может быть решена только за счет их совместного применения. Дипломные проекты такого типа ориентированы на комплексную разработку аппаратных и программных средств.

Обоснование решения в виде наглядного представления (схемы алгоритма, диаграммы, циклограммы, информационной или иной модели, блок-схемы и т.д.) должно быть представлено в раздаточном материале.

Программные документы, разработанные в дипломном проекте различных проблемных областей, должны быть оформлены в соответствии с требованиями стандартов Единой системы программной документации.

Графическая часть ВКР (дипломного проекта) должна иллюстрировать постановку задачи, формализацию методов ее решения, реализацию, полученные результаты.

Под презентационной частью ВКР (дипломного проекта) понимают готовые форматные слайды, в одном из общеупотребительных форматах их представления – электронном (ppt, pptx, pdf и т.д.), графическом (плакаты и чертежи), мультимедийные (видеоролики) содержащие конкретную, чётко структурируемую информацию. Презентация представляется в электронном виде, на одном из установленных типов носителей (CD/DVD диск, флэш карта, переносной жёсткий диск и т.д.). Допускается использование студентом своих средств представления презентаций (ноутбуков).

Тематика ВКР (дипломных проектов) разрабатывается преподавателями кафедры ОПиСДи рассматривается на заседании кафедры.

**Примерный перечень тем ВКР (дипломных проектов)**

1 Внедрение дополнительных методов обеспечения безопасности сети ООО …

2 Разработка комплексной системы методов обеспечения безопасности сети ООО …

3 Разработка сайта с реализацией защиты персональных данных

4 Модернизация сайта с реализацией защиты персональных данных

5 Проектирование программной системы зашиты рабочих мест от утечек информации

6 Модернизирование программной системы зашиты рабочих мест от утечек информации

7 Разработка мобильного приложения управления системы контроля и управления доступа на объект

8 Проектирование инженерно-технической системы защиты информации на предприятии от физического проникновения на объект.

9 Анализ и модернизация существующей инженерно-технической системы защиты информации на предприятии от физического проникновения на объект.

10 Обоснование и выбор мест установки средств защиты информации от утечек по техническим каналам связи на предприятии

11 Обоснование и выбор мест установки средств защиты информации от утечек по техническим каналам связи для конфиденциальных переговоров.

12 Обоснование и выбор мест установки средств защиты информации от утечек по техническим каналам связи для организаций, работающих или имеющие отношение к государственной тайне

13 Создание и разработка организационно-правовой системы для защиты информации в предприятии

14 Создание и разработка организационно-правовой системы для защиты информации в банке

15 Создание и разработка организационно-правовой системы для защиты информации в организации работающих с государственной тайной или уровнем секретности.

16 Разработка плана инженерно - технической защиты здания банка

17 Разработка плана инженерно - технической защиты здания с уровнем секретности

18 Разработка плана инженерно - технической защиты здания предприятия

19 Анализ и модернизация инженерно-технической системы защиты информации на предприятии.

20 Проектирование инженерно-технической системы защиты учебного заведения

21 Анализ и модернизация инженерно-технической системы защиты информации здания предприятия

22 Разработка системы защиты веб-сайтов от парсинга

23 Применение программно-аппаратных средств обеспечения информационной безопасности в автоматизированной системе

24 Анализ существующей безопасности базы данных организации, и реализация методов ее повышения

25 Проектирование инженерно-технической системы защиты комнаты переговоров

26 Анализ информационной системы медицинских услуг ЕМИАС

27 Создание программной системы работы СКУДа

28 Анализ и модернизация существующей программной системы работы СКУДа

29 Реализация отказоустойчивости сервера по средствам распределения нагрузки

30 Проектирование и создание аппаратной части работы СКУДа

31 Анализ и модернизация аппаратной части работы СКУДа

32 Анализ и повышение уровня существующей системы защиты информации предприятия

33 Создание технической защиты каналов от утечки информации

34 Анализ и модернизация технической защиты каналов от утечки информации

35 Настройка безопасной авторизации, идентификации и аутентификация при подключении к беспроводной точке доступа для организации

36 Разработка политики информационной безопасности для организации

37 Эксплуатация подсистем безопасности (в защищённом исполнении) автоматизированной системы

38 Проектирование программной системы защиты информации предприятия

39 Разработка корпоративной сети для организации

40 Модернизация корпоративной сети для организации

Закрепление тем выпускных квалификационных работ (дипломных проектов) с указанием руководителей и сроков выполнения за обучающимися оформляется приказом директора колледжа.

К защите выпускной квалификационной работы (дипломного проекта) допускаются студенты, выполнившие работу в полном объеме, получившие отзыв руководителя, подписи всех консультантов, рецензию на работу.

Защита выпускных квалификационных работ (дипломных проектов) проводится на открытом заседании ГЭК по специальности 10.02.04 Обеспечение информационной безопасности телекоммуникационных систем, утвержденной приказом директора колледжа . На защиту выпускной квалификационной работы (дипломного проекта) отводится до 45 мин.

Общую оценку за выпускную квалификационную работу (дипломный проект) выводят члены ГЭК на коллегиальной основе с учетом соответствия содержания заявленной теме, глубины ее раскрытия, соответствия оформления принятым стандартам, проявленной во время защиты способности студента демонстрировать собственное видение проблемы и умение мотивированно его отстоять, владения теоретическим материалом, способности грамотно его излагать и аргументированно отвечать на поставленные вопросы. Оценки выпускным квалификационным работам (дипломным проектам) даются членами ГЭК на закрытом заседании и объявляются выпускникам в тот же день после подписания соответствующего протокола заседания комиссии.

Качественно выполненная выпускная квалификационная работа (дипломный проект) должна свидетельствовать об умении обучающегося:

- четко формулировать проблему и оценивать степень ее актуальности;
- обосновывать выбранные методы решения поставленных задач;
- самостоятельно работать с необходимым количеством отечественной и зарубежной литературы и другими информационно-справочными материалами;

- отбирать нужные сведения, анализировать их, интерпретировать и представлять в графической или иной иллюстративной форме;
- делать обоснованные выводы, давать практические рекомендации (в соответствующих случаях).

Результаты защиты определяются оценками «отлично», «хорошо», «удовлетворительно», «неудовлетворительно» и объявляются в тот же день после окончания защиты.

«Отлично» – представленная на защиту ВКР (дипломный проект) носит практический и опытно-экспериментальный характер, соответствует структуре ВКР. Графический и текстовый материалы выполнены в соответствии с заданием, нормативными документами и согласуются с требованиями, предъявляемыми к уровню подготовки по специальностям СПО. Отзыв руководителя и рецензия положительные. Выпускник в ходе защиты выпускной квалификационной работы (дипломного проекта) продемонстрировал глубокое и хорошо аргументированное обоснование темы; четкую формулировку и понимание изучаемой проблемы; широкое и правильное использование методов исследования. Содержание исследования и ход защиты указывают на наличие навыков работы выпускника в данной области. В выпускной квалификационной работе (дипломном проекте) представлена расширенная библиография. Защита проведена выпускником грамотно, с четким изложением содержания работы и с достаточным обоснованием самостоятельности ее разработки. Ответы на вопросы членов ГЭК даны в полном объеме. Выпускник в процессе защиты показал высокий уровень освоения профессиональных компетенций, соответствующих основным видам профессиональной деятельности, самостоятельность, творческий подход и ответственность при выполнении проекта, глубину исследования, привел убедительную аргументацию, представил практические результаты проекта. Выпускная квалификационная работа (дипломный проект) соответствует названию работы, ее содержанию, имеет чёткую целевую направленность, логическую последовательность изложения материала, которые базируется на прочных теоретических знаниях по избранной теме. Изложение материала корректно и грамотно оформлено.

«Хорошо» – представленная на защиту ВКР (дипломный проект) носит практический и опытно-экспериментальный характер, соответствует структуре ВКР. Графический и текстовый материалы выполнены в соответствии с заданием, нормативными документами и согласуются с требованиями, предъявляемыми к уровню подготовки по специальностям СПО. Отзыв руководителя и рецензия положительные. Выпускник в ходе защиты выпускной квалификационной работы (дипломного проекта) продемонстрировал хорошо аргументированное обоснование темы; четкую формулировку и понимание изучаемой проблемы. В выпускной квалификационной работе (дипломном проекте) использовано ограниченное число литературных источников, но достаточное для проведения практического и опытно-экспериментального исследования. Содержание исследования и ход защиты указывают на наличие практических навыков работы выпускника в данной области. Ход защиты выпускной квалификационной работы (дипломного проекта) показал достаточный уровень освоения профессиональных компетенций, соответствующих основным видам профессиональной деятельности. Защита проведена выпускником грамотно, с достаточным обоснованием самостоятельности ее разработки, но с неточностями в изложении отдельных положений содержания выпускной квалификационной работы (дипломного проекта). Ответы на некоторые вопросы членов ГЭК даны в неполном объеме.

«Удовлетворительно» – представленная ВКР (дипломный проект) носит практический и опытно-экспериментальный характер, соответствует структуре ВКР. Графический и текстовый материалы в целом выполнены в соответствии с заданием, нормативными документами, но имеют место отклонения от существующих требований. Отзыв руководителя и рецензия положительные, но с замечаниями. Защита проведена выпускником с недочетами в изложении содержания работы и в обосновании самостоятельности ее разработки. На отдельные вопросы членов ГЭК ответы не даны. Выпускник в процессе защиты показал достаточную подготовку к профессиональной деятельности и освоение профессиональный компетенций, но при защите выпускной квалификационной работы (дипломного проекта) отмечены отдельные отступления от требований, предъявляемых к уровню подготовки по специальностям СПО. Ход защиты выпускной квалификационной работы (дипломного проекта) показал достаточную профессиональную подготовку выпускника.

«Неудовлетворительно» – представленный на защиту выпускная квалификационная работа (дипломный проект) выполнен с заметными отступлениями от задания, принятых нормативных документов и не всегда согласуется с требованиями, предъявляемыми к уровню подготовки по специальности среднего профессионального образования. Выпускник в ходе защиты раскрыл тему ВКР в общем виде. Отзыв руководителя и рецензия с существенными замечаниями. Использовано ограниченное число литературных источников. Защита проведена выпускником на низком уровне с ограниченным изложением содержания ВКР и неубедительным обоснованием самостоятельности ее разработки. На большую часть вопросов членов ГЭК не дано ответов или даны неверные ответы. Отмечается шаблонное изложение материала. Во время защиты выпускником проявлена ограниченная эрудиция. В ходе защиты выпускник показал недостаточный уровень освоения профессиональных компетенций, соответствующих основным видам профессиональной деятельности по теме выпускной квалификационной работы (дипломного проекта). Проявлена недостаточная профессиональная подготовка.

**Демонстрационный экзамен**

Демонстрационный экзамен (ДЭ) базового уровня проводится с использованием единых оценочных материалов, включающих в себя конкретные комплекты оценочной документации, варианты заданий и критерии оценивания, разрабатываемых экспертами организации, наделенной полномочиями по обеспечению прохождения ГИА в форме ДЭ.

Комплект оценочной документации 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. Министерство просвещения Российской Федерации обеспечивает размещение разработанных комплектов оценочной документации на официальном сайте оператора в информационно-телекоммуникационной сети «Интернет» (далее – сеть «Интернет») не позднее 1 октября года, предшествующего проведению ГИА.

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

Представление выпускником выполненного практического задания дает возможность оценить качественный уровень овладения им общими компетенциями через демонстрацию понимания сущности своей будущей профессии; оценку эффективности и качества своей работы; принятие решения в стандартных и нестандартных ситуациях; демонстрацию ответственности за принятые решения, результат выполнения задания, владения информационной культурой.

Результаты выполнения практического задания освещаются в определенной логической последовательности, профессиональным языком с комментариями по технике безопасности в условиях производства.

Представление выпускником результата выполнения практического задания может иметь форму самооценки (подробный комментарий процесса выполнения практического задания, исправление обозначенных ошибок и определение степени их влияния на качество конечного результата).

ДЭ проводится в центре проведения демонстрационного экзамена (далее - центр проведения экзамена), представляющем собой площадку, оборудованную и оснащенную в соответствии с комплектом оценочной документации. Место расположения центра проведения ДЭ, дата и время начала проведения, расписание сдачи ДЭ в составе экзаменационных групп, планируемая продолжительность проведения ДЭ, технические перерывы в проведении ДЭ определяются планом проведения ДЭ, утверждаемым ГЭК совместно с КЦ «Молодые профессионалы» не позднее чем за двадцать календарных дней до даты проведения демонстрационного экзамена. Директор колледжа (зам. директора по учебно-производственной работе) знакомит с планом проведения демонстрационного экзамена выпускников, сдающих ДЭ, и лиц, обеспечивающих проведение ДЭ, в срок не позднее чем за пять рабочих дней до даты проведения экзамена.

Не позднее чем за один рабочий день до даты проведения демонстрационного экзамена главным экспертом проводится проверка готовности центра проведения экзамена в присутствии членов экспертной группы, выпускников, а также технического эксперта, назначаемого организацией, на территории которой расположен центр проведения экзамена, ответственного за соблюдение установленных норм и правил охраны труда и техники безопасности. Выпускники проходят ДЭ в центре проведения экзамена в составе экзаменационных групп.

Процедура оценивания результатов выполнения заданий ДЭ осуществляется членами экспертной группы по 100-балльной системе в соответствии с требованиями комплекта оценочной документации. Баллы выставляются в протоколе проведения ДЭ, 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.

Критерии оценки выполнения демонстрационного экзамена:

«Отлично» ставится, если обучающийся по результатам демонстрационного задания набрал более 24 баллов и продемонстрировал высокий уровень освоения теоретических знаний и владения профессиональными компетенциями, соответствующими виду профессиональной деятельности; высокий уровень специальной подготовки, способность и умение применять теоретические знания при выполнении конкретного практического задания сферы профессиональной деятельности; четкое выполнение практического задания; аргументированность при обозначении профессиональных выводов.

«Хорошо» ставится, если студент по результатам демонстрационного экзамена набрал 20 до 23 балла и продемонстрировал достаточный уровень освоения теоретических знаний и владения профессиональными компетенциями, соответствующими виду профессиональной деятельности; способность и умение в целом применять теоретические знания при выполнении конкретного практического задания сферы профессиональной деятельности с допущением незначительных неточностей, не влияющих на результат выполнения практического задания; частичную аргументированность при обозначении профессиональных выводов.

«Удовлетворительно» ставится, если студент по результатам демонстрационного экзамена набрал от 16 до 19 баллов и продемонстрировал необходимый уровень освоения теоретических знаний и владения профессиональными компетенциями, соответствующими виду профессиональной деятельности; недостаточно высокий уровень специальной подготовки, способности применять теоретические знания при выполнении практического задания сферы профессиональной деятельности; недостаточную аргументированность профессиональных выводов; а также допустил ряд ошибок при выполнении практического задания.

«Неудовлетворительно» ставится, если студент по результатам демонстрационного экзамена набрал менее 16 баллов и не продемонстрировал необходимый уровень освоения теоретических знаний и владения профессиональными компетенциями, соответствующими виду профессиональной деятельности; способность и умение применять теоретические знания при выполнении практического задания сферы профессиональной деятельности; допустил принципиальные ошибки, влияющие на результат выполнения практического задания; не сформулировал или не аргументировал профессиональные выводы.

Перевод баллов в оценку осуществляется согласно таблице 2.

Таблица 2 - Перевод баллов в оценку

| **Оценка ГИА** | **неудовлетворительно** | **удовлетворительно** | **хорошо** | **отлично** |
|---|---|---|---|---|
| Отношение полученного количества баллов к максимальному количеству баллов (в процентах) | 0,00%-19,99% | 20,00%-39,99% | 40,00%-69,99% | 70,00%-100,00% |

Пересчет итогового рейтингового балла в 4-х бальную оценку (макс. 30):

| Итоговый рейтинговый балл | 4-х бальная оценка |
|---|---|
|  24 | отлично |
| 20-23 | хорошо |
| 16-19 | удовлетворительно |
|  16 | неудовлетворительно |

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

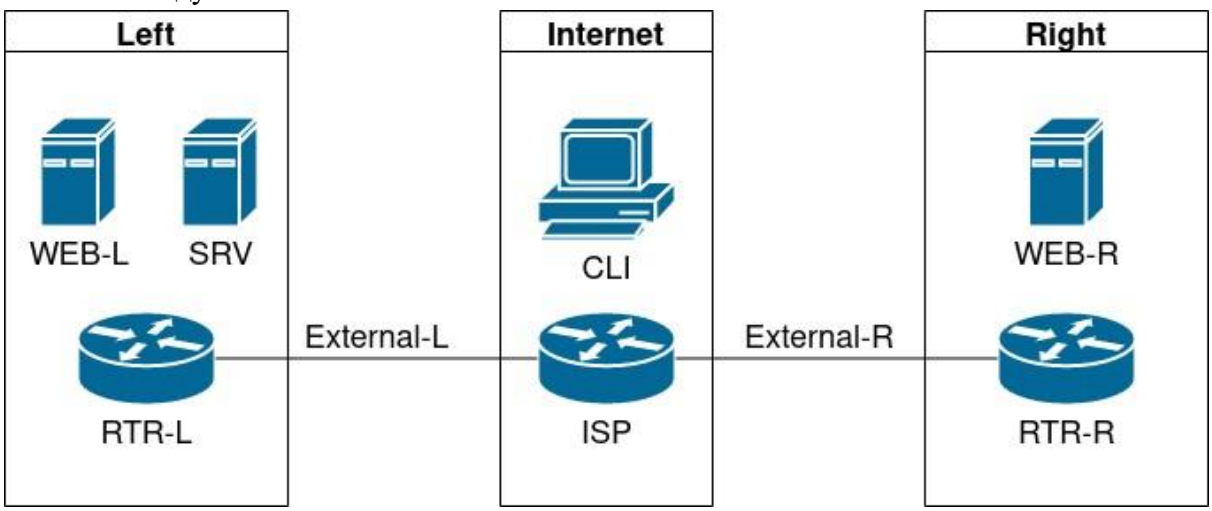
Итоговая оценка по процедуре ГИА выставляется как среднее арифметическое целое число в соответствии с правилами математического округления с учетом результатов сдачи ДЭ и защиты дипломного проекта (работы).

Пример типового задания для проведения демонстрационного экзамена по специальности 10.02.04 Обеспечение информационной безопасности телекоммуникационных систем по компетенции «Сетевое и системное администрирование».

| | |
|---|---|
| **Номер компетенции** | 39 |
| **Название компетенции** | Сетевое и системное администрирование |
| **Номер КОД** | 1.1 |

Описание задания

Описание модуля 1




Виртуальные машины и коммутация

Необходимо выполнить создание и базовую конфигурацию виртуальных машин.

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

Характеристики ВМ установите в соответствии с **Таблицей 1;**

Коммутацию (если таковая не выполнена) выполните в соответствии со схемой сети.

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

Адресация должна быть выполнена в соответствии с Таблицей 1;

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

Сетевая связность

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

Сети, подключенные к ISP, считаются внешними:

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

Платформы контроля трафика, установленные на границах регионов, должны выполнять трансляцию трафика, идущего из соответствующих внутренних сетей во внешние сети стенда и в сеть Интернет.

Трансляция исходящих адресов производится в адрес платформы, расположенный во внешней сети.

Между платформами должен быть установлен защищенный туннель, позволяющий осуществлять связь между регионами с применением внутренних адресов.

Трафик, проходящий по данному туннелю, должен быть защищен:

Платформа ISP не должна иметь возможности просматривать содержимое пакетов, идущих из одной внутренней сети в другую.

Туннель должен позволять защищенное взаимодействие между платформами управления трафиком по их внутренним адресам

Взаимодействие по внешним адресам должно происходит без применения туннеля и шифрования.

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

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

Разрешаются подключения к портам DNS, HTTP и HTTPS для всех клиентов; Порты необходимо для работы настраиваемых служб

Разрешается работа выбранного протокола организации защищенной связи;

Разрешение портов должно быть выполнено по принципу “необходимо и достаточно”

Разрешается работа протоколов ICMP;

Разрешается работа протокола SSH;

Прочие подключения запрещены;

Для обращений в платформам со стороны хостов, находящихся внутри регионов, ограничений быть не должно;

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

Разрешаются подключения к портам HTTP и HTTPS для всех клиентов;

Порты необходимо для работы настраиваемых служб

Разрешается работа выбранного протокола организации защищенной связи;

Разрешение портов должно быть выполнено по принципу “необходимо и достаточно”

Разрешается работа протоколов ICMP;

Разрешается работа протокола SSH;

Прочие подключения запрещены;

Для обращений в платформам со стороны хостов, находящихся внутри регионов, ограничений быть не должно;

Обеспечьте настройку служб SSH регионов:

Подключения со стороны внешних сетей по протоколу к платформе управления трафиком RTR-L на порт 2222 должны быть перенаправлены на BM Web-L;

Подключения со стороны внешних сетей по протоколу к платформе управления трафиком RTR-R на порт 2244 должны быть перенаправлены на BM Web-R;

Инфраструктурные службы

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

Выполните настройку первого уровня DNS-системы стенда:

Используется ВМ ISP;

Обслуживается зона demo.wsr.

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

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.

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

Выполните настройку второго уровня DNS-системы стенда;

Используется ВМ SRV;

Обслуживается зона int.demo.wsr;

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

Обслуживаются обратные зоны для внутренних адресов регионов

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

Сервер принимает рекурсивные запросы, исходящие от адресов внутренних регионов;

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

Внутренние хосты регионов (равно как и платформы управления трафиком) должны использовать данную DNS-службу для разрешения всех запросов имен; Выполните настройку первого уровня системы синхронизации времени:

Используется сервер ISP.

Сервер считает собственный источник времени верным, stratum=3;

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

Подразумевается обращение SRV для синхронизации времени;

Клиент CLI должен использовать службу времени ISP;

Выполните конфигурацию службы второго уровня времени на SRV.

Сервер синхронизирует время с хостом ISP;

Синхронизация с другими источникам запрещена;

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

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

Реализуйте iSCSI Target на базе SRV

Сервер должен предоставлять доступ для подключения диска по протоколу iSCSI только и исключительно для WEB-L;

Используется диск на базе подключенного дополнительного диска согласно **Табл.1**;

На WEB-L iSCSI-раздел должен быть смонтирован по адресу /mnt/iscsi и быть отформатирован в ext4;

Выполните настройку центра сертификации на базе SRV:

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

Выдаваемые сертификаты должны иметь срок жизни не менее 300 дней; Параметры выдаваемых сертификатов:

Страна RU;

Организация DEMO.WSR;

Прочие поля (за исключением CN) должны быть пусты;

Инфраструктура веб-приложения

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

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

Выполните установку приложения AppDocker0;

Пакеты для установки Docker расположены на дополнительном ISO-образе;

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

Необходимо реализовать следующую инфраструктуру приложения.

Клиентом приложения является CLI (браузер Edge);

Хостинг приложения осуществляется на ВМ WEB-L и WEB-R;

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

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

При необходимости, для доступа к приложению допускается реализовать реверспрокси или трансляцию портов;

Доступ к приложению должен быть защищен с применением технологии TLS;

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

Незащищенное соединение должно переводиться на защищенный канал автоматически;

Необходимо обеспечить отказоустойчивость приложения;

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

Отказ одной из ВМ Web

Отказ одной из ВМ управления трафиком.

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<br>192.168.106.254/24 | |
| | Cisco CSR | | 4 | | |
| RTR-R | Debian 11 | 2 Гб | 2 | 5.5.5.100/24<br>172.16.106.254/24 | |
| | Cisco CSR | | 4 | | |

| | | | | | |
|---|---|---|---|---|---|
| SRV | Debian 11 | 2 Гб | 2 | 192.168.106.200/24 | Дополнительные диски: 2 шт по 2 Гб |
| | Windows Server 2019 | 4 Гб | 4 | | Дополнительные диски: 2 шт по 2 Гб |
| WEB-L | Debian 11 | 2 Гб | 2 | 192.168.106.100/24 | |
| WEB-R | Debian 11 | 2 Гб | 2 | 172.16.106.100/24 | |
| ISP | Debian 11 | 2 Гб | 2 | 4.4.4.1/24<br>5.5.5.1/24<br>3.3.3.1/24 | |
| CLI | Windows 10 | 4 | 4 | 3.3.3.10/24 | |

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 | 192.168.106.100 |
| | A | web-r | 172.16.106.100 |
| | A | srv | 192.168.106.200 |
| | A | rtr-l | 192.168.106.254 |
| | A | rtr-r | 172.16.106.254 |
| | CNAME | ntp | srv |
| | CNAME | dns | srv |

**Перечень литературы, необходимой для подготовки ВКР Основная литература:**

1. Батаев А. В. Операционные системы и среды: учебник для учреждений СПО / А. В. Батаев, Н. Ю. Налютин, С. В. Синицын. – Москва : Академия, 2018. – 272 с. – Режим доступа: http://www.academia-moscow.ru/catalogue/4891/401793/

2. Белева, Л. Ф. Программирование на языке С++ [Электронный ресурс] : учебное пособие / Л. Ф. Белева. — Электрон. текстовые данные. — Саратов : Ай Пи Эр Медиа, 2018. — 81 с. — 978-5-4486-0253-5. — Режим доступа: http://www.iprbookshop.ru/72466.html

3. Гребенюк Е. И. Технические средства информатизации: учебник для учреждений СПО / Е. И. Гребенюк, Н. А. Гребенюк. – Москва : Академия, 2017. - 352 с. – Режим доступа: http://www.academia-moscow.ru/catalogue/4831/294815/

4. Драчева Е. Л. Менеджмент : учебник для учреждений СПО / Е. Л. Драчева, Л. И. Юликов. – Москва : Академия, 2017. - 304 с. – Режим доступа:http://www.academiamoscow.ru/catalogue/4831/295171/

5. Еременко, В. Т. Инженерно-техническая защита объектов инфокоммуникаций : учеб. пособие / В. Т. Еременко ; П. Н. Рязанцев ; А. П.Фисун . - Орел : Изд-во ОГУ , 2016. - 156 с. – Режим доступа: http://elib.oreluniver.ru/media/attach/note/2016/eremenko_ing_tekn_zaschita.pdf

6. Фисун А.П.. – Орел: ФГБОУ ВПО «Госуниверситет - УНПК», 2015. – 165 с. – Режим доступа: http://elib.oreluniver.ru/media/attach/note/2015/Eremenko_progr_apparatn_sredstva.pdf 7. Еременко, В.Т. Техническая защита информации : учеб. пособие / В. Т. Еременко ; А.П. Фисун; П. Н. Рязанцев . - Орел : Изд-во ОГУ , 2016. - 131 с. – Режим доступа: http://elib.oreluniver.ru/media/attach/note/2016/eremenko_ing_tekn_zaschita_BdIqWw1.pdf

8. Жигулин, Г. П. Организационное и правовое обеспечение информационной безопасности [Электронный ресурс] : учебное пособие / Г. П. Жигулин. — Электрон. текстовые данные. — СПб. : Университет ИТМО, 2014. — 174 с. — 2227-8397. — Режим доступа: http://www.iprbookshop.ru/67451.html

9. Косолапова Н.В. Безопасность жизнедеятельности : учебник для учреждений СПО / Н.В.Косолапова, Н.А.Прокопенко, Е.Л. Побежимова. - 8-е изд., стер. – Москва : Академия, 2017. - 288 с. – Режим доступа: http://www.academiamoscow.ru/catalogue/4831/325569/

10. Лапонина, О. Р. Основы сетевой безопасности. Криптографические алгоритмы и протоколы взаимодействия [Электронный ресурс] / О. Р. Лапонина. — Электрон. текстовые данные. — М. : Интернет-Университет Информационных Технологий (ИНТУИТ), 2016. — 242 с. — 5-9556-00020-5. — Режим доступа: http://www.iprbookshop.ru/52217.html

11. Лобанова, В.А. Операционные системы и базы данных: учебное пособие / В.А. Лобанова, О.А. Воронина, Н.Г. Лобанова. – Орел: ОГУ имени И.С. Тургенева, 2016. – 198 с. – Режим доступа: http://elib.oreluniver.ru/uchebniki-i-uch-posobiya/lobanova-valentinaandreevna-operacionnye-sistemy-.html

12. Мезенцев К. Н. Автоматизированные информационные системы :учебник для учреждений СПО / К. Н. Мезенцев. – 6 – изд., стер. – Москва : Академия, 2016. – 176 с. – Режим доступа:http://www.academia-moscow.ru/catalogue/4831/331837/ 13. Ожиганов, А. А. Криптография [Электронный ресурс] : учебное пособие / А. А. Ожиганов. — Электрон. текстовые данные. — СПб. : Университет ИТМО, 2016. — 142 с. — 2227-8397. — Режим доступа: http://www.iprbookshop.ru/67231.html

14. Семакин И. Г. Основы алгоритмизации и программирования : учебник для учреждений СПО / И. Г.Семакин, А. П. Шестаков. – Москва : Академия, 2017. - 304 с. – Режим доступа: http://www.academia-moscow.ru/catalogue/4831/296437/

15. Скрипник, Д. А. Общие вопросы технической защиты информации [Электронный ресурс] / Д. А. Скрипник. — Электрон. текстовые данные. — М.:

ИнтернетУниверситет Информационных Технологий (ИНТУИТ), 2016. — 424 с. — 2227-8397. —
Режим доступа: http://www.iprbookshop.ru/52161.html

16. Сычев, Ю. Н. Стандарты информационной безопасности. Защита и обработка конфиденциальных документов [Электронный ресурс] : учебное пособие / Ю. Н. Сычев. — Электрон. текстовые данные. — Саратов: Вузовское образование, 2018. — 195 с. — 978-5-
4487-0128-3. — Режим доступа: http://www.iprbookshop.ru/72345.html

17. Чащина Е. А. Обслуживание аппаратного обеспечения персональных компьютеров, серверов, периферийных устройств, оборудования и компьютерной оргтехники : учебник для учреждений СПО / Е.А. Чащина. – Москва : Академия, 2016. - 208 с. – Режим доступа: http://www.academia-moscow.ru/catalogue/4831/183606/ 18. Шаньгин, В. Ф. Защита компьютерной информации. Эффективные методы и средства [Электронный ресурс] / В. Ф. Шаньгин. — Электрон. текстовые данные. — Саратов : Профобразование, 2017. — 544 с. — 978-5-4488-0074-0. — Режим доступа: http://www.iprbookshop.ru/63592.html

19. Эксплуатация объектов сетевой инфраструктуры: учебник для учреждений
СПО / А. В. Назаров [и др.] ; под ред. А. В. Назарова. – Москва : Академия, 2018. - 368 с. – Режим доступа: http://www.academia-moscow.ru/catalogue/4831/345939/

**Дополнительная литература:**

20. ГОСТ Р 50922-2006. Национальный стандарт Российской Федерации. Защита информации. Основные термины и определения (утв. и введен в действие Приказом Ростехрегулирования от 27.12.2006 N 373-ст) // СПС КонсультантПлюс

21. ГОСТ Р 52447-2005. Защита информации. Техника защиты информации. Номенклатура показателей качества" (утв. Приказом Ростехрегулирования от 29.12.2005 N
448-ст) // СПС КонсультантПлюс

22. Кодекс Российской Федерации об административных правонарушениях [Электронный ресурс] / . — Электрон. текстовые данные. — : Электронно-библиотечная система IPRbooks, 2017. — 567 с. — 2227-8397. — Режим доступа: http://www.iprbookshop.ru/1249.html

23. Агешкина, Н. А. Комментарий к Федеральному закону от 27 декабря 2002 г. N 184-ФЗ «О техническом регулировании» [Электронный ресурс] / Н. А. Агешкина, В. Ю. Коржов. — 3-е изд. — Электрон. текстовые данные. — Саратов : Ай Пи Эр Медиа, 2018. — 151 с. — 978-5-4486-0292-4. — Режим доступа: http://www.iprbookshop.ru/73978.html 24. Бехроуз, А. Криптография и безопасность сетей [Электронный ресурс] :
учебное пособие / Фороузан А. Бехроуз ; под ред. А. Н. Берлин. — Электрон. текстовые данные. — Москва, Саратов : Интернет-Университет Информационных Технологий (ИНТУИТ), Вузовское образование, 2017. — 782 с. — 978-5-4487-0143-6. — Режим доступа: http://www.iprbookshop.ru/72337.html

25. Бондаренко, И. С. Методы и средства защиты информации [Электронный ресурс] : лабораторный практикум / И. С. Бондаренко, Ю. В. Демчишин. — Электрон.

текстовые данные. — М. : Издательский Дом МИСиС, 2018. — 32 с. — 2227-8397. — Режим доступа: http://www.iprbookshop.ru/84413.html

26. Бубнов А. А. Основы информационной безопасности : учебник для учреждений СПО / А. А. Бубнов, В. Н. Пржегорлинский, О. А. Савинкин. – Москва : Академия, 2018. - 256 с. – Режим доступа:http://www.academiamoscow.ru/catalogue/4831/302888/

27. Вичугова, А. А. Инструментальные средства разработки компьютерных систем и комплексов [Электронный ресурс] : учебное пособие для СПО / А. А. Вичугова. — Электрон. текстовые данные. — Саратов : Профобразование, 2017. — 135 с. — 978-5-44880015-3. — Режим доступа: http://www.iprbookshop.ru/66387.html

28. Галас, В. П. Вычислительные системы, сети и телекоммуникации. Часть 1.
Вычислительные системы [Электронный ресурс] : электронный учебник / В. П. Галас. — Электрон. текстовые данные. — Владимир : Владимирский государственный университет им. А.Г. и Н.Г. Столетовых, 2016. — 232 с. — 2227-8397. — Режим доступа: http://www.iprbookshop.ru/57363.html 29. Галас, В. П. Вычислительные системы, сети и телекоммуникации. Часть 2.
Сети и телекоммуникации [Электронный ресурс] : электронный учебник / В. П. Галас. — Электрон. текстовые данные. — Владимир : Владимирский государственный университет им. А.Г. и Н.Г. Столетовых, 2016. — 311 с. — 2227-8397. — Режим доступа: http://www.iprbookshop.ru/57364.html

30. Гатченко, Н. А. Криптографическая защита информации [Электронный ресурс] / Н. А. Гатченко, А. С. Исаев, А. Д. Яковлев. — Электрон. текстовые данные. — СПб. : Университет ИТМО, 2012. — 142 с. — 2227-8397. — Режим доступа: http://www.iprbookshop.ru/68658.html

31. Каторин, Ю. Ф. Защита информации техническими средствами [Электронный ресурс] : учебное пособие / Ю. Ф. Каторин, А. В. Разумовский, А. И. Спивак ; под ред. Ю. Ф. Каторин. — Электрон. текстовые данные. — СПб. : Университет ИТМО, 2012. — 417 с. —
2227-8397. — Режим доступа: http://www.iprbookshop.ru/66445.html

32. Лазицкас, Е. А. Базы данных и системы управления базами данных [Электронный ресурс]: учебное пособие / Е. А. Лазицкас, И. Н. Загумённикова, П. Г. Гилевский. — Электрон. текстовые данные. — Минск : Республиканский институт профессионального образования (РИПО), 2016. — 268 с. — 978-985-503-558-0. — Режим доступа: http://www.iprbookshop.ru/67612.html

33. Немцова, Т. И. Программирование на языке высокого уровня.
Программирование на языке С++ [Текст]: учеб. пособие для сред. спец. учеб. заведений и вузов. - М. : ИД «ФОРУМ», 2018. - 512 с. + Доп. материалы

34. Прохорова, О. В. Информационная безопасность и защита информации [Электронный ресурс] : учебник / О. В. Прохорова. — Электрон. текстовые данные. — Самара : Самарский государственный архитектурно-строительный университет, ЭБС АСВ,
2014. — 113 с. — 978-5-9585-0603-3. — Режим доступа: http://www.iprbookshop.ru/43183.html
35. Сельвесюк, Н.И. Методология анализа защищенности автоматизированных систем

обработки информации [Электронный ресурс] / Н.И. Сельвесюк, А.С. Островский, В.Д. Сливинский. // Информатика и системы управления. — Электрон. дан. — 2016. — № 2. — С. 17-24. — Режим доступа: https://e.lanbook.com/journal/issue/300657 . — Загл. с экрана.

36. Сенкевич А.В.Архитектура аппаратных средств : учебник для учреждений СПО / А.В. Сенкевич. - Москва : Академия, 2017. - 240 с. – Режим доступа: http://www.academia-moscow.ru/catalogue/4831/295228/

37. Торстейнсон, П. Криптография и безопасность в технологии. NET [Электронный ресурс] / П. Торстейнсон, Г.А. Ганеш ; под ред. С. М. Молявко ; пер. с англ. В. Д. Хорева. — Электрон. дан. — Москва : Издательство «Лаборатория знаний», 2015. — 428 с. — Режим доступа: https://e.lanbook.com/book/70724 . — Загл. с экрана. 38. Федорова Г. Н. Основы проектирования баз данных : учебник для учреждений СПО / Г. Н. Федорова.- 2-е изд., стер. – Москва : Академия, 2018. - 224 с. – Режим доступа: http://www.academia-moscow.ru/catalogue/4831/401009/

## 3 Порядок апелляции по результатам итоговой аттестации

По результатам ГИА выпускник, участвовавший в ГИА, имеет право подать в апелляционную комиссию письменное апелляционное заявление о нарушении, по его мнению, установленного порядка ГИА и (или) несогласии с ее результатами (далее - апелляция). Апелляция подается лично выпускником или родителями (законными представителями) несовершеннолетнего выпускника в апелляционную комиссию филиала. Апелляция о нарушении порядка проведения ГИА подается непосредственно в день проведения ГИА. Апелляция о несогласии с результатами ГИА подаётся не позднее следующего рабочего дня после объявления результатов государственной итоговой аттестации. Апелляция рассматривается апелляционной комиссией не позднее трех рабочих дней с момента ее поступления.

Состав апелляционной комиссии утверждается приказом директором филиала одновременно с утверждением состава ГЭК.

Апелляционная комиссия состоит из председателя апелляционной комиссии, не менее пяти членов апелляционной комиссии и секретаря апелляционной комиссии из числа педагогических работников образовательной организации, не входящих в данном учебном году в состав ГЭК. Председателем апелляционной комиссии может быть назначено лицо из числа руководителей или заместителей руководителей организаций, осуществляющих образовательную деятельность, соответствующую области профессиональной деятельности, к которой готовятся выпускники, представителей организаций-партнеров или их объединений, включая экспертов, при условии, что направление деятельности данных представителей соответствует области профессиональной деятельности, к которой готовятся выпускники, при условии, что такое лицо не входит в состав ГЭК. Апелляция рассматривается на заседании апелляционной комиссии с участием не менее двух третей ее состава.

На заседание апелляционной комиссии приглашается председатель соответствующей ГЭК, а также главный эксперт при проведении ГИА в форме демонстрационного экзамена.

При проведении ГИА в форме демонстрационного экзамена по решению председателя апелляционной комиссии к участию в заседании комиссии могут быть также привлечены члены экспертной группы, технический эксперт.

По решению председателя апелляционной комиссии заседание апелляционной комиссии может пройти с применением средств видео, конференц-связи, а равно посредством предоставления письменных пояснений по поставленным апелляционной комиссией вопросам.

Выпускник, подавший апелляцию, имеет право присутствовать при рассмотрении апелляции. С несовершеннолетним выпускником имеет право присутствовать один из родителей (законных представителей). Указанные лица должны иметь при себе документы, удостоверяющие личность. Рассмотрение апелляции не является пересдачей ГИА.

При рассмотрении апелляции о нарушении порядка проведения ГИА апелляционная комиссия устанавливает достоверность изложенных в ней сведений и выносит одно из решений:

- об отклонении апелляции, если изложенные в ней сведения о нарушениях порядка проведения ГИА выпускника не подтвердились и/или не повлияли на результат ГИА;
- об удовлетворении апелляции, если изложенные в ней сведения о допущенных нарушениях порядка проведения ГИА выпускника подтвердились и повлияли на результат ГИА.

В последнем случае результаты проведения ГИА подлежат аннулированию, в связи, с чем протокол о рассмотрении апелляции не позднее следующего рабочего дня передается в ГЭК для реализации решения апелляционной комиссии. Выпускнику предоставляется возможность пройти ГИА в дополнительные сроки, установленные ОГУ имени И.С. Тургенева (филиала) без отчисления такого выпускника из университета (филиала) в срок не более четырех месяцев после подачи апелляции.

Для рассмотрения апелляции о несогласии с результатами ГИА, полученными при прохождении демонстрационного экзамена, секретарь ГЭК не позднее следующего рабочего дня с момента поступления апелляции направляет в апелляционную комиссию протокол заседания ГЭК, протокол проведения демонстрационного экзамена, письменные ответы выпускника (при их наличии), результаты работ выпускника, подавшего апелляцию, видеозаписи хода проведения демонстрационного экзамена (при наличии).

Для рассмотрения апелляции о несогласии с результатами ГИА, полученными при защите дипломного проекта (работы), секретарь ГЭК не позднее следующего рабочего дня с момента поступления апелляции направляет в апелляционную комиссию дипломный проект (работу), протокол заседания ГЭК.

В результате рассмотрения апелляции о несогласии с результатами ГИА апелляционная комиссия принимает решение об отклонении апелляции и сохранении результата ГИА либо об удовлетворении апелляции и выставлении иного результата ГИА. Решение апелляционной комиссии не позднее следующего рабочего дня передается в ГЭК. Решение апелляционной комиссии является основанием для аннулирования ранее выставленных результатов ГИА выпускника и выставления новых результатов в соответствии с мнением апелляционной комиссии.

Решение апелляционной комиссии принимается простым большинством голосов. При равном числе голосов голос председательствующего на заседании апелляционной комиссии является решающим. Решение апелляционной комиссии доводится до сведения подавшего апелляцию выпускника в течение трех рабочих дней со дня заседания апелляционной комиссии.

Решение апелляционной комиссии является окончательным и пересмотру не подлежит.

Решение апелляционной комиссии оформляется протоколом, который подписывается председателем (заместителем председателя) и секретарем апелляционной комиссии и хранится в архиве в архиве филиала.