

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ
ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«ОРЛОВСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
ИМЕНИ И.С. ТУРГЕНЕВА»

Ливенский филиал ОГУ им. И.С. Тургенева

Кафедра информационных технологий и экономики

«Утверждаю»

И.о. проректора

по учебно-методической

деятельности

 Н.С. Лаушкина

**ПРОГРАММА
ГОСУДАРСТВЕННОЙ ИТОГОВОЙ АТТЕСТАЦИИ**

наименование специальности
10.02.05 Обеспечение информационной безопасности
автоматизированных систем

квалификация: техник по защите информации

форма обучения: очная

Ливны - 2024

Программа государственной итоговой аттестации составлена в соответствии с требованиями Федерального государственного образовательного стандарта среднего профессионального образования по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем, утвержденного приказом Министерства образования и науки Российской Федерации №1553 от 09.12.2016 г.

Программа переутверждена (на основе утвержденной НМС филиала протокол № 9 от 20 «мая» 2024 г.) кафедрой информационных технологий и экономики Ливенского филиала ОГУ им. И.С. Тургенева «02» сентября 2024 г. протокол № 2.

И.о. заведующего кафедрой
информационных технологий
и экономики, канд. экон. наук



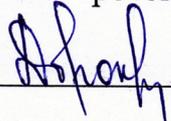
О.В. Псарева

Согласовано с работодателем:
ведущий инженер-программист
отдела информационных технологий
БУЗ Орловской области
«Ливенская центральная районная больница»



О.А. Поздняков

Программа переутверждена на заседании научно-методического совета Ливенского филиала ОГУ им. И.С. Тургенева протокол от «02» сентября 2024 г. №1.

Председатель НМС, канд. пед. наук  Дорохова Г.Д.

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	4
1.4	Требования к результатам освоения основной образовательной программы	5
1.5	Формы проведения государственной итоговой аттестации	7
2	Процедура проведения государственной итоговой аттестации	7
2.1	Состав и порядок работы государственной экзаменационной комиссии	7
2.2	Порядок организации и проведения демонстрационного экзамена	8
2.2.1	Фонд оценочных средств для подготовки и сдачи демонстрационного экзамена	11
2.2.2	Перечень литературы, необходимой для подготовки к сдаче демонстрационного экзамена	17
2.3	Порядок организации и защиты выпускной квалификационной работы	22
2.3.1	Фонд оценочных средств для защиты выпускной квалификационной работы	23
2.3.2	Перечень литературы, необходимой для подготовки выпускной квалификационной работы	26
3	Порядок апелляции по результатам государственной итоговой аттестации	31

1. Общие положения

1.1 Общая характеристика программы государственной итоговой аттестации

Программа государственной итоговой аттестации (далее - Программа) разработана на основании требований Федерального государственного образовательного стандарта среднего профессионального образования по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем, утвержденного приказом Минобрнауки России 9 декабря 2016 г. N 1553.

Программа является частью основной образовательной программы по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем и устанавливает процедуру организации и проведения государственной итоговой аттестации (далее - ГИА) обучающихся.

1.2 Нормативные документы, регламентирующие проведение государственной итоговой аттестации

Нормативно-правовую базу разработки программы государственной итоговой аттестации 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 Минпросвещения России от 08.11.2021 № 800 «Об утверждении Порядка проведения государственной итоговой аттестации по образовательным программам среднего профессионального образования»;
- приказ Министерства просвещения Российской Федерации от 24 августа 2022 г. № 762 «Об утверждении Порядка организации и осуществления образовательной деятельности по образовательным программам среднего профессионального образования»;
- приказ Министерства просвещения Российской Федерации от 22 июня 2023г. № П-291 «О введении в действие Методики организации и проведения демонстрационного экзамена»;
- приказа Министерства просвещения Российской Федерации от 17 апреля 2023 г. № 285 «Об операторе демонстрационного экзамена базового и профильного уровней по образовательным программам среднего профессионального образования»;
- федеральный государственный образовательный стандарт среднего профессионального образования по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем, утвержденный приказом Минобрнауки России 9 декабря 2016 г. N 1553;
- Устав и локальные нормативные акты ОГУ имени И.С. Тургенева.

1.3 Цель и задачи государственной итоговой аттестации

Цель ГИА в соответствии с Федеральным законом от 29 декабря 2012 г. №273-ФЗ «Об образовании в Российской Федерации»:

Цель государственной итоговой аттестации – определение соответствия результатов освоения обучающимися образовательной программы – программы подготовки специалистов среднего звена требованиям ФГОС СПО по 10.02.05 Обеспечение информационной безопасности автоматизированных систем.

Задачи государственной итоговой аттестации:

- проверка сформированности у выпускников общих и профессиональных компетенций, установленных ФГОС СПО;
- определение готовности выпускников к выполнению установленных ФГОС СПО основных видов деятельности согласно получаемой квалификации «Техник по защите информации».

Демонстрационный экзамен предусматривает моделирование реальных производственных условий для решения выпускниками практических задач профессиональной деятельности.

1.4 Требования к результатам освоения основной образовательной программы

Выпускник по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем должен обладать следующими компетенциями:

Таблица 1 -Требования к результатам освоения основной образовательной программы

Коды	Краткое содержание / определение компетенции.
Общие компетенции	
ОК 01	Выбирать способы решения задач профессиональной деятельности применительно к различным контекстам.
ОК 2	Использовать современные средства поиска, анализа и интерпретации информации и информационные технологии для выполнения задач профессиональной деятельности
ОК 3	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 4	Эффективно взаимодействовать и работать в коллективе и команде.
ОК 5	Осуществлять устную и письменную коммуникацию на государственном языке Российской Федерации с учетом особенностей социального и культурного контекста.
ОК 6	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 7	Содействовать сохранению окружающей среды, ресурсосбережению, применять знания об изменении климата, принципы бережливого производства, 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	Пользоваться профессиональной документацией на государственном и иностранных языках.

Профессиональные компетенции	
Эксплуатация автоматизированных (информационных) систем в защищённом исполнении	
ПК 1.1.	Производить установку и настройку компонентов автоматизированных (информационных) систем в защищенном исполнении в соответствии с требованиями эксплуатационной документации.
ПК 1.2.	Администрировать программные и программно-аппаратные компоненты автоматизированной (информационной) системы в защищенном исполнении.
ПК 1.3.	Обеспечивать бесперебойную работу автоматизированных (информационных) систем в защищенном исполнении в соответствии с требованиями эксплуатационной документации.
ПК 1.4.	Осуществлять проверку технического состояния, техническое обслуживание и текущий ремонт, устранять отказы и восстанавливать работоспособность автоматизированных (информационных) систем в защищенном исполнении
Защита информации в автоматизированных системах программными и программно-аппаратными средствами	
ПК 2.1.	Осуществлять установку и настройку отдельных программных, программно-аппаратных средств защиты информации.
ПК 2.2.	Обеспечивать защиту информации в автоматизированных системах отдельными программными, программно-аппаратными средствами.
ПК 2.3.	Осуществлять тестирование функций отдельных программных и программно-аппаратных средств защиты информации.
ПК 2.4.	Осуществлять обработку, хранение и передачу информации ограниченного доступа.
ПК 2.5.	Уничтожать информацию и носители информации с использованием программных и программно-аппаратных средств.
ПК 2.6.	Осуществлять регистрацию основных событий в автоматизированных (информационных) системах, в том числе с использованием программных и программно-аппаратных средств обнаружения, предупреждения и ликвидации последствий компьютерных атак.
Защита информации техническими средствами	
ПК 3.1.	Осуществлять установку, монтаж, настройку и техническое обслуживание технических средств защиты информации в соответствии с требованиями эксплуатационной документации.
ПК 3.2.	Осуществлять эксплуатацию технических средств защиты информации в соответствии с требованиями эксплуатационной документации.
ПК 3.3.	Осуществлять измерение параметров побочных электромагнитных излучений и наводок, создаваемых техническими средствами обработки информации ограниченного доступа.
ПК 3.4.	Осуществлять измерение параметров фоновых шумов, а также физических полей, создаваемых техническими средствами защиты информации.
ПК 3.5.	Организовывать отдельные работы по физической защите объектов информатизации.
Выполнение работ по одной или нескольким профессиям рабочих, должностям служащих	
ПК 4.1	Подготавливать к работе и настраивать аппаратное обеспечение, периферийные устройства, операционную систему персонального компьютера и мультимедийное оборудование
ПК 4.2	Выполнять ввод цифровой и аналоговой информации в персональный компьютер с различных носителей
ПК 4.3	Конвертировать файлы с цифровой информацией в различные форматы
ПК 4.4	Обрабатывать аудио- и визуальный контент средствами звуковых, графических

	и видеоредакторов
ПК 4.5	Создавать и воспроизводить видеоролики, презентации, слайд-шоу, медиафайлы и другую итоговую продукцию из исходных аудио-, визуальных и мультимедийных компонентов средствами персонального компьютера и мультимедийного оборудования
ПК 4.6	Управлять размещением цифровой информации на дисках персонального компьютера, а также дисковых хранилищах локальной и глобальной компьютерной сети
ПК 4.7	Тиражировать мультимедиа-контент на различных съемных носителях информации
ПК 4.8	Публиковать мультимедиа-контент в сети Интернет

1.5 Формы проведения государственной итоговой аттестации

Государственная итоговая аттестация по образовательной программе среднего профессионального образования 10.02.05 Обеспечение информационной безопасности автоматизированных систем в соответствии с федеральным государственным образовательным стандартом среднего профессионального образования проводится в форме демонстрационного экзамена и защиты дипломного проекта.

Демонстрационный экзамен (далее – ДЭ) направлен на определение уровня освоения выпускником материала, предусмотренного ОП СПО и степени сформированности профессиональных умений и навыков путем проведения независимой экспертной оценки выполненных выпускником практических заданий в условиях реальных или смоделированных производственных процессов.

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

2. Процедура проведения государственной итоговой аттестации

2.1 Состав и порядок работы государственной экзаменационной комиссии

В целях определения соответствия результатов освоения выпускниками ОП СПО соответствующим требованиям ФГОС СПО ГИА проводится государственными экзаменационными комиссиями (далее - ГЭК), создаваемыми филиалом по каждой укрупненной группе специальностей или по отдельным специальностям СПО.

ГЭК формируется из педагогических работников филиала, 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 ДЭ (далее - оператор), обладающих профессиональными знаниями, навыками и опытом в сфере, соответствующей специальности СПО, по которой проводится ДЭ (далее - эксперты).

Состав ГЭК утверждается приказом директора филиала и действует в течение одного календарного года. В состав ГЭК входят председатель ГЭК, заместитель председателя ГЭК и члены ГЭК.

Секретарь ГЭК назначается из числа педагогических работников филиала, не входящих в состав ГЭК.

ГЭК возглавляет председатель, который организует и контролирует её деятельность, обеспечивает единство требований, предъявляемых к выпускникам.

Председатель ГЭК утверждается не позднее 20 декабря текущего года на следующий календарный год (с 1 января по 31 декабря) приказом Министерства науки и высшего образования Российской Федерации.

Председателем ГЭК утверждается, лицо, не работающее в ОГУ имени И.С. Тургенева 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.

Руководитель филиала является заместителем председателя ГЭК. В случае создания в филиале нескольких ГЭК назначается несколько заместителей председателя ГЭК из числа заместителей директора филиала (декана факультета) или педагогических работников.

При проведении демонстрационного экзамена в составе ГЭК создается экспертная группа из числа экспертов (далее - экспертная группа).

Экспертная группа создается по каждой специальности СПО или виду деятельности, по которому проводится ДЭ.

Экспертную группу возглавляет главный эксперт, назначаемый из числа экспертов, включенных в состав ГЭК. Главный эксперт организует и контролирует деятельность возглавляемой экспертной группы, обеспечивает соблюдение всех требований к проведению ДЭ и не участвует в оценивании результатов ГИА.

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.

Результаты проведения ГИА оцениваются с проставлением одной из оценок: «отлично», «хорошо», «удовлетворительно», «неудовлетворительно» - и объявляются в тот же день после оформления протоколов заседаний ГЭК.

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

2.2 Порядок организации и проведения демонстрационного экзамена

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

план или индивидуальный учебный план по осваиваемой образовательной программе СПО.

Демонстрационный экзамен по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем проводится на базовом уровне на основе требований к результатам освоения образовательных программ среднего профессионального образования, установленных ФГОС СПО.

Координатором подготовки и проведения ДЭ в филиале выступает Координационный центр «Молодые профессионалы» ФГБОУ ВО «ОГУ им. И.С. Тургенева» (далее - КЦ «МП»). КЦ «МП» координирует процессы организации демонстрационного экзамена.

Для проведения ДЭ заведующим кафедрой и преподавателями выпускающей кафедры до начала нового учебного года осуществляется выбор компетенций, комплектов оценочной документации, формируется заявка на проведение ДЭ от выпускающей кафедры по конкретным специальностям. Даты проведения ДЭ, представленные в заявке, определяются в соответствии с календарным графиком учебного процесса по конкретной специальности, утвержденным приказом ректора Университета.

Заместитель директора по учебно-методической работе филиала (далее – зам. директора по УМР филиала) формирует единую заявку от филиала по всем специальностям СПО филиала и представляет ее в КЦ «МП».

По запросу КЦ «МП» зам. директора УМР филиала до 1 декабря календарного года в КЦ «МП» предоставляет заявку на проведение демонстрационного экзамена и предполагаемые списки групп обучающихся, которые будут принимать участие в процедуре ДЭ.

Зам. директора по УМР филиала осуществляет сбор согласий обучающихся на обработку персональных данных и предоставляет их КЦ «МП».

Для подготовки обучающихся к участию в ДЭ преподавателями филиала проводятся консультации.

ДЭ проводится в Центре проведения ДЭ (далее - ЦПДЭ), представляющем собой площадку, оборудованную и оснащенную в соответствии с КОД. ЦПДЭ может располагаться на территории Университета, а при сетевой форме реализации образовательных программ - также на территории иной организации, обладающей необходимыми ресурсами для организации ЦПДЭ.

Место расположения ЦПДЭ, дата и время начала проведения ДЭ, 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 «МП» не позднее чем за двадцать календарных дней до даты проведения ДЭ.

Декан факультета знакомит с планом проведения ДЭ выпускников, сдающих ДЭ, и лиц, обеспечивающих проведение ДЭ, в срок не позднее чем за пять рабочих дней до даты проведения экзамена.

Выпускники проходят ДЭ в ЦПДЭ в составе экзаменационных групп.

Выпускникам и лицам, привлекаемым к проведению ГИА, во время ее проведения запрещается иметь при себе и использовать средства связи.

Выпускники знакомятся со своими рабочими местами, под руководством главного эксперта также повторно знакомятся с планом проведения ДЭ, условиями оказания первичной медицинской помощи в ЦПДЭ. Факт ознакомления отражается главным экспертом в протоколе распределения рабочих мест.

Технический эксперт под подпись знакомит главного эксперта, членов экспертной группы, выпускников с требованиями охраны труда и безопасности производства.

В день проведения ДЭ в ЦПДЭ присутствуют:

- директор КЦ «МП», контролирующий процедуру проведения ДЭ (если ДЭ проходит в ЦПДЭ Университета). Представитель филиала из числа педагогических работников, контролирующий процедуру проведения ДЭ (если ДЭ проводится в ЦПДЭ другой образовательной организации);

- не менее одного члена ГЭК, не считая членов экспертной группы;

- члены экспертной группы;

- главный эксперт;

- представители организаций-партнеров (по согласованию с филиалом);

- выпускники;

- технический эксперт;

- представитель из числа педагогических работников филиала, ответственный за сопровождение выпускников к ЦПДЭ (при необходимости);

- тьютор (ассистент), оказывающий необходимую помощь выпускнику из числа лиц с ограниченными возможностями здоровья, детей-инвалидов, инвалидов (далее - тьютор (ассистент)) - при необходимости;

- организаторы, назначенные образовательной организацией (на базе которой аккредитован ЦПДЭ и проводится ДЭ) из числа педагогических работников, оказывающие содействие главному эксперту в обеспечении соблюдения всех требований к проведению ДЭ.

В случае отсутствия в день проведения ДЭ в ЦПДЭ лиц, указанных в настоящем пункте, решение о проведении ДЭ принимается главным экспертом, о чем главным экспертом вносится соответствующая запись в протокол проведения ДЭ.

Допуск выпускников в ЦПДЭ осуществляется главным экспертом на основании документов, удостоверяющих личность.

Выпускники вправе:

- пользоваться оборудованием ЦПДЭ, необходимыми материалами, средствами обучения и воспитания в соответствии с требованиями КОД, задания ДЭ;

- получать разъяснения технического эксперта по вопросам безопасной и бесперебойной эксплуатации оборудования ЦПДЭ;

- получить копию задания демонстрационного экзамена на бумажном носителе.

Выпускники обязаны:

- во время проведения ДЭ не пользоваться и не иметь при себе средства связи, носители информации, средства ее передачи и хранения, если это прямо не предусмотрено КОД;

- во время проведения ДЭ использовать только средства обучения и воспитания, разрешенные КОД;

- во время проведения ДЭ не взаимодействовать с другими выпускниками, экспертами, иными лицами, находящимися в ЦПДЭ, если это не предусмотрено КОД и заданием ДЭ.

Выпускники могут иметь при себе лекарственные средства и питание, прием которых осуществляется в специально отведенном для этого помещении согласно плану проведения ДЭ за пределами ЦПДЭ.

Допуск выпускников к выполнению заданий осуществляется при условии обязательного их ознакомления с требованиями охраны труда и производственной безопасности.

В соответствии с планом проведения ДЭ главный эксперт знакомит выпускников с заданиями, передает им копии заданий ДЭ.

После ознакомления с заданиями ДЭ выпускники занимают свои рабочие места в соответствии с протоколом распределения рабочих мест. После того, как все выпускники и лица, привлеченные к проведению ДЭ, займут свои рабочие места в соответствии с требованиями охраны труда и производственной безопасности, главный эксперт объявляет о начале ДЭ. После объявления главным экспертом начала ДЭ выпускники приступают к выполнению заданий ДЭ.

Время начала ДЭ фиксируется в протоколе проведения ДЭ, составляемом главным экспертом по каждой экзаменационной группе.

ДЭ проводится при неукоснительном соблюдении выпускниками, лицами, привлеченными к проведению ДЭ, требований охраны труда и производственной безопасности, а также с соблюдением принципов объективности, открытости и равенства выпускников.

ЦПДЭ могут быть оборудованы средствами видеонаблюдения, позволяющими осуществлять видеозапись хода проведения ДЭ. Видеоматериалы о проведении ДЭ в случае осуществления видеозаписи подлежат хранению в Университете не менее одного года с момента завершения ДЭ.

Явка выпускника, его рабочее место, время завершения выполнения задания ДЭ подлежат фиксации главным экспертом в протоколе проведения ДЭ.

В случае удаления из ЦПДЭ выпускника, лица, привлеченного к проведению ДЭ, или присутствующего ЦПДЭ, главным экспертом составляется акт об удалении. Результаты ГИА выпускника, удаленного из ЦПДЭ, аннулируются ГЭК, и такой выпускник признается ГЭК не прошедшим ГИА по неуважительной причине.

Главный эксперт сообщает выпускникам о течении времени выполнения задания ДЭ каждые 60 минут, а также за 30 и 5 минут до окончания времени выполнения задания.

После объявления главным экспертом окончания времени выполнения заданий выпускники прекращают любые действия по выполнению заданий ДЭ.

Выпускник по собственному желанию может завершить выполнение задания досрочно, уведомив об этом главного эксперта.

Результаты выполнения выпускниками заданий ДЭ подлежат фиксации экспертами экспертной группы в соответствии с требованиями комплекта оценочной документации и задания ДЭ.

Даты проведения ДЭ определяется календарным учебным графиком учебного плана по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем. Продолжительность демонстрационного экзамена составляет не более 3 часов.

2.2.1 Фонд оценочных средств для подготовки и сдачи демонстрационного экзамена

Демонстрационный экзамен проводится с использованием единых оценочных материалов, включающих в себя конкретные комплекты оценочной

документации, варианты заданий и критерии оценивания, разрабатываемые экспертами организации, наделенной полномочиями по обеспечению прохождения ГИА в форме ДЭ.

Комплект оценочной документации базового уровня КОД 10.02.05-2024 (далее - КОД) по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем 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 <https://bom.firpo.ru/Public/173>

Модуль 1: Эксплуатация автоматизированных (информационных) систем в защищенном исполнении

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

Ниже представлен образец задания по демонстрационному экзамену по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем

Задача. Установка центра регистрации, сервиса публикации и сервиса информирования Certification Authority на соответствующие виртуальные машины

- установить ПО Client;
- установить ПО Publication Service;
- установить ПО Registration Point;
- установить ПО CA Informing.

Задача. Развертывание удостоверяющего центра в составе сети Необходимо использовать рабочее место администратора (созданное ранее) для создания структуры защищенной сети, развернуть с помощью технологии виртуальных машин сеть предприятия и настроить необходимые АРМ в соответствии с заданными ролями.

Схема сети, которую требуется создать, приведена далее.

IP адреса сетей перечислены в начале задания (по названию сетей).

Net1 Certification Authority

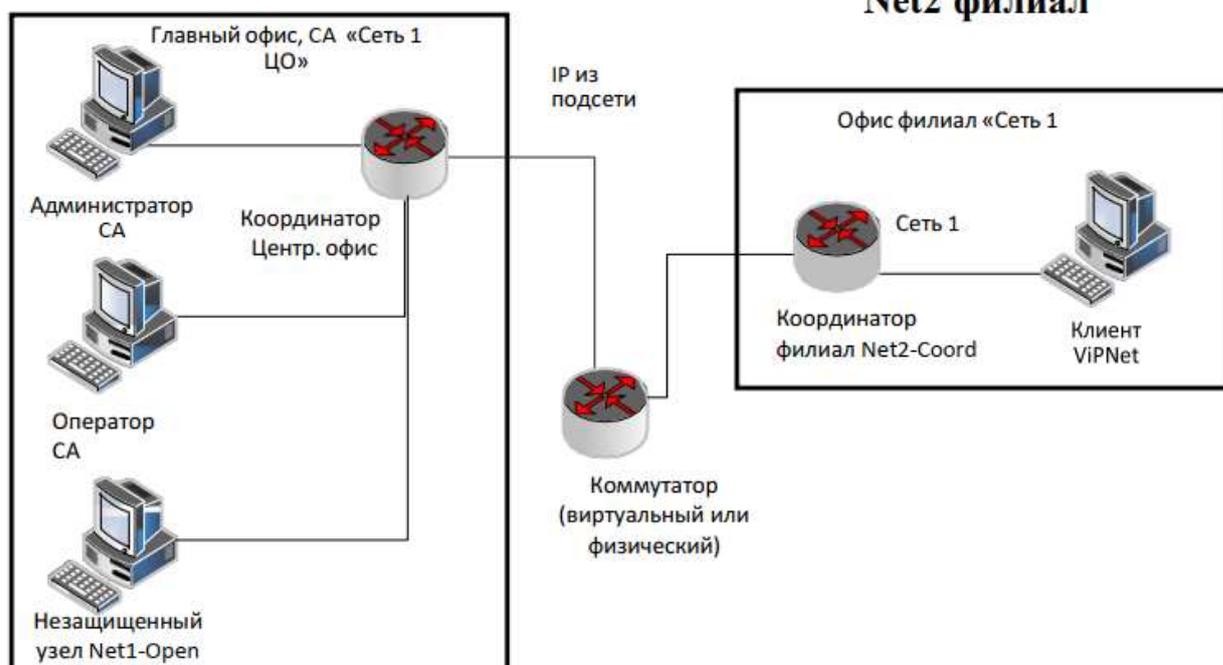


Рисунок 1 Схема защищенной сети

В итоге выполнения задания должны быть развернуты и настроены следующие сетевые узлы защищенной сети (см. таблицу).

Таблица 1 Узлы защищенной сети если УКЦ и ЦУС на одной машине.

Вирт. машина	Название сетевого узла	ПО	ОС сетевого узла	Имя пользователя сетевого узла, уровень полномочий
Net1-AdminCA (ЦО)	Главный администратор (VM)	Administrator (ЦУС клиент и сервер + УКЦ), Client, CA Informing	ОС пользовательская или серверная	AdminCA
Net1-CoordCA (ЦО)	Координатор Центр Офис (VM)	Coordinator	Координатор HW-VA	CoordinatorCA
Net1-OperCA (ЦО)	Оператор УЦ (VM)	Client, Publication Service, Registration Point	ОС пользовательская или серверная	OperCA
Net2-Coord (Филиал)	Координатор Филиал (VM)	Coordinator	Координатор HW-VA	CoordinatorSub
Net2-Client (филиал)	Пользователь_2 Филиал (VM)	Client	ОС пользовательская или серверная	User

Связи между узлами необходимо настроить самостоятельно.

Таблица 2. Схема связей пользователей

Схема связей пользователей	Coordinator Office	Admin	OperCA	Coordinator Sub	User
CoordinatorOffice	×	*	*	*	
Admin	*	×	*		*
OperCA	*	*	×	*	
CoordinatorSub	*		*	×	*
User		*		*	×

Задача. Настройка работы удостоверяющего центра в аккредитованном режиме

Необходимо перевести УКЦ в режим аккредитованного удостоверяющего центра, настроить параметры издания квалифицированных сертификатов, указав:

сведения о средствах УЦ,

средство электронной подписи издателя,

средства удостоверяющего центра,

сертификат на средство электронной подписи издателя,

сертификат на средство удостоверяющего центра,

класс защищенности, которому соответствуют программные средства УЦ,

место хранения контейнеров ключа ЭП и ключа защиты УКЦ. После перевода УКЦ в аккредитованный режим необходимо выпустить:

корневой квалифицированный сертификат,

квалифицированные электронные подписи для пользователей. При формировании сертификатов необходимо заполнить следующие поля:

Имя: <Имя пользователя или узла> Электронная почта

Город Область Организация

Подразделение Почтовый индекс

Создать квалифицированные ключи ЭП и ключи проверки ЭП для пользователей сети. Настроить схему обмена файлами между УКЦ посредством Сервиса Публикации (Publication Service).

Реализовать автоматическую публикацию сертификатов. Посредством Центра Регистрации (Registration Point):

зарегистрировать пользователя;

отправить запрос в УКЦ на выпуск сертификата, удовлетворить запрос;

отправить запрос в УКЦ на аннулирование ранее выпущенного сертификата, удовлетворить запрос.

Посредством Сервиса Информирования (CA Informing): настроить способ выдачи уведомлений и сформировать отчет о выданных за текущие сутки сертификатах, предварительно в настройках указав место хранения отчетов.

Задача. Модификация структуры защищенной сети

Перед началом выполнения сделать HTML выгрузку структуры сети и сделать скриншот ЦУС окна с пользователями.

Модификация структуры сети:

добавить новый сетевой узел и пользователя за координатором (без фактического развертывания его на виртуальной машине). Добавить связь пользователя нового узла с пользователем. На указанных узлах проверить появление нового узла;

добавить пользователя на узле Филиал (Net2-Client филиала 2), связать его со всеми пользователями группы узлов центральный офис.

По результатам проведенной модификации сети для указанного пользователя проверить появление новых связей, отправить письмо по Деловой почте пользователю, отправить текстовое сообщение пользователю.

Необходимо зафиксировать процесс настройки скриншотами ключевых моментов и заполненных форм:

скриншоты деловой почты на отправителе и получателе (при отправке письма);

скриншоты текстового сообщения на отправителе и получателе;

скриншоты журнала IP-пакетов на координаторах, подтверждающие прохождение письма через координаторов, скриншот Удостоверяющего центра со списком изданных сертификатов. Кроме того, необходимо сохранить файл HTML с обновленной структурой защищенной сети, выгруженный из ЦУС.

Модуль 2: Защита информации в автоматизированных системах программными и программно-аппаратными средствами

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. Оригинал протокола проведения ДЭ передается на хранение в КЦ «МП» в составе архивных документов.

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 ДЭ далее передается в ГЭК для выставления оценок по итогам ГИА. Перевод баллов в оценки осуществляется ГЭК с обязательным участием главного эксперта и оформляется протоколом.

Методика перевода результатов ДЭ в оценку устанавливается с учетом специфики компетенции, уровня сложности комплектов оценочной документации по компетенции. Методика перевода баллов в оценки разработана на основании приложения к письму № 1.5/WSR-2062/2017 от 26.12.2017 «Предложения по методике перевода результатов ДЭ в оценку» и представлена в таблице - 2

Максимально возможное количество баллов – 100.

Таблица 2 - Методика перевода результатов проведения демонстрационного экзамена в оценку по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем КОД 10.02.05-1-2024, максимальное количество баллов 50.

Оценка ДЭ	неудовлетворительно	удовлетворительно	хорошо	отлично
Отношение полученного количества баллов к максимально возможному (в%)	0,00%-19,99%	20,00%-39,99%	40,00%-69,99%	70,00%-100,00%
Количество баллов	0-9,99	10-19,99	20-34,99	35-50,00

2.2.2 Перечень литературы, необходимой для подготовки к сдаче демонстрационного экзамена

Основная литература:

1. Беленький, В. Г. Беспроводные сети передачи данных: учебное пособие для СПО / В. Г. Беленький, А. В. Лопшарев. — Саратов: Профобразование, 2022. — 98 с. — ISBN 978-5-4488-1499-0. — Текст: электронный // Цифровой образовательный ресурс IPR SMART: [сайт]. — URL: <https://www.iprbookshop.ru/125572.html>
2. Внуков, А.А. Основы информационной безопасности: защита информации: учебное пособие для среднего профессионального образования/ А. А. Внуков. — 3-е изд., перераб. и доп. — Москва: Издательство Юрайт, 2023. — 161 с. — (Профессиональное образование). — ISBN 978-5-534-13948-8. — Текст: электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/518006>
3. Гостев, И. М. Операционные системы: учебник и практикум для среднего профессионального образования / И. М. Гостев. — 2-е изд., испр. и доп. — Москва: Издательство Юрайт, 2023. — 164 с. — (Профессиональное образование). — ISBN 978-5-534-04951-0. — Текст: электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/514426>
4. Зиангирова, Л. Ф. Инфокоммуникационные системы и сети: учебное пособие для СПО / Л. Ф. Зиангирова. — Саратов: Профобразование, Ай Пи Ар Медиа, 2019. — 128 с. — ISBN 978-5-4488-0302-4, 978-5-4497-0183-1. — Текст: электронный // Цифровой образовательный ресурс IPR SMART: [сайт]. — URL: <https://www.iprbookshop.ru/85806.html>
5. Извозчикова, В. В. Эксплуатация информационных систем : учебное пособие для СПО / В. В. Извозчикова. — Саратов: Профобразование, 2019. — 136 с. — ISBN 978-5-4488-0355-0. — Текст: электронный // Цифровой образовательный ресурс IPR SMART: [сайт]. — URL: <https://www.iprbookshop.ru/86210.html>
6. Ильин, М. Е. Криптографическая защита информации в объектах информационной инфраструктуры: учеб. для студ. учреждений сред. проф. образования / М. Е. Ильин, Т. И. Калинкина, В. Н. Пржегорлинский; под ред. В. Н. Пржегорлинского — Москва: Академия, 2020.— 288 с. — URL: <https://www.academia-moscow.ru/catalogue/4831/444518/>
7. Казарин, О. В. Программно-аппаратные средства защиты информации. Защита программного обеспечения: учебник и практикум для среднего профессионального образования / О. В. Казарин, А. С. Забабурин. — Москва: Издательство Юрайт, 2023. — 312 с. — (Профессиональное образование). — ISBN 978-5-534-13221-2. — Текст: электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/519364>
8. Мэйволд, Э. Безопасность сетей: учебное пособие для СПО / Э. Мэйволд. — Саратов: Профобразование, 2021. — 571 с. — ISBN 978-5-4488-0990-3. — Текст: электронный // Цифровой образовательный ресурс IPR SMART: [сайт]. — URL: <https://www.iprbookshop.ru/102183.html>
9. Организационное и правовое обеспечение информационной безопасности: учебник и практикум для среднего профессионального образования / Т. А. Полякова, А. А. Стрельцов, С. Г. Чубукова, В. А. Ниесов; ответственные редакторы Т. А. Полякова, А. А. Стрельцов. — Москва: Издательство Юрайт, 2023. — 325 с. — (Профессиональное образование). — ISBN 978-5-534-00843-2. —

Текст: электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/512861>

10. Скрипник, Д. А. Общие вопросы технической защиты информации: учебное пособие / Д. А. Скрипник. — 3-е изд. — Москва, Саратов: Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2020. — 424 с. — ISBN 978-5-4497-0336-1. — Текст: электронный // Цифровой образовательный ресурс IPR SMART: [сайт]. — URL: <https://www.iprbookshop.ru/89451.html>

11. Советов, Б. Я. Базы данных: учебник для среднего профессионального образования / Б. Я. Советов, В. В. Цехановский, В. Д. Чертовской. — 3-е изд., перераб. и доп. — Москва: Издательство Юрайт, 2023. — 420 с. — (Профессиональное образование). — ISBN 978-5-534-09324-7. — Текст: электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/514585>

12. Солонская, О. И. Средства защиты информации: учебное пособие для СПО / О. И. Солонская. — Саратов: Профобразование, 2022. — 88 с. — ISBN 978-5-4488-1504-1. — Текст: электронный // Цифровой образовательный ресурс IPR SMART: [сайт]. — URL: <https://www.iprbookshop.ru/125578.html>

13. Технологии защиты информации в компьютерных сетях: учебное пособие для СПО / Н. А. Руденков, А. В. Пролетарский, Е. В. Смирнова, А. М. Суоров. — Саратов: Профобразование, 2021. — 368 с. — ISBN 978-5-4488-1014-5. — Текст: электронный // Цифровой образовательный ресурс IPR SMART: [сайт]. — URL: <https://www.iprbookshop.ru/102207.html>

14. Фороузан, Б. А. Криптография и безопасность сетей: учебное пособие для СПО / Б. А. Фороузан; под редакцией А. Н. Берлина. — Саратов: Профобразование, 2021. — 776 с. — ISBN 978-5-4488-0999-6. — Текст: электронный // Цифровой образовательный ресурс IPR SMART: [сайт]. — URL: <https://www.iprbookshop.ru/102192.html>

Дополнительная литература:

15. Конституция Российской Федерации (с гимном России). Новая редакция. - Москва: Проспект, 2021. - 64 с.

16. О безопасности. Федеральный закон от 28.12.2010 N 390-ФЗ (ред. от 09.11.2020) // СПС КонсультантПлюс.

17. О персональных данных. Федеральный закон от 27.07.2006 N 152-ФЗ (ред. от 14.07.2022) // СПС КонсультантПлюс.

18. О техническом регулировании. Федеральный закон от 27.12.2002 N 184-ФЗ (ред. от 02.07.2021) (с изм. и доп., вступ. в силу с 23.12.2021) // СПС КонсультантПлюс.

19. Об информации, информационных технологиях и о защите информации. Федеральный закон от 27.07.2006 N 149-ФЗ (ред. от 29.12.2022) (с изм. и доп., вступ. в силу с 09.01.2023) // СПС КонсультантПлюс.

20. Об утверждении Инструкции об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну. Приказ ФАПСИ от 13.06.2001 N 152 (Зарегистрировано в Минюсте РФ 06.08.2001 N 2848) // СПС КонсультантПлюс.

21. Об утверждении Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации

(Положение ПКЗ-2005). Приказ ФСБ РФ от 09.02.2005 N 66 (ред. от 12.04.2010) (Зарегистрировано в Минюсте РФ 03.03.2005 N 6382) // СПС КонсультантПлюс.

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

23. ГОСТ Р ИСО/МЭК 13335-1-2006. Национальный стандарт Российской Федерации. Информационная технология. Методы и средства обеспечения безопасности. Часть 1. Концепция и модели менеджмента безопасности информационных и телекоммуникационных технологий" (утв. и введен в действие Приказом Ростехрегулирования от 19.12.2006 N 317-ст) // СПС КонсультантПлюс.

24. ГОСТ Р 50739-95. Средства вычислительной техники. Защита от несанкционированного доступа к информации. Общие технические требования (принят и введен в действие Постановлением Госстандарта РФ от 09.02.1995 N 49) // СПС КонсультантПлюс.

25. Меры защиты информации в государственных информационных системах. Методический документ (утв. ФСТЭК России 11.02.2014) // СПС КонсультантПлюс.

26. Авдошин, С. М. Технологии и продукты Microsoft в обеспечении информационной безопасности: учебное пособие для СПО / С. М. Авдошин, А. А. Савельева, В. А. Сердюк. — Саратов: Профобразование, 2021. — 431 с. — ISBN 978-5-4488-1015-2. — Текст: электронный // Цифровой образовательный ресурс IPR SMART: [сайт]. — URL: <https://www.iprbookshop.ru/102208.html>

27. Гордеев, С. И. Организация баз данных в 2 ч. Часть 1: учебник для среднего профессионального образования / С. И. Гордеев, В. Н. Волошина. — 2-е изд., испр. и доп. — Москва: Издательство Юрайт, 2023. — 310 с. — (Профессиональное образование). — ISBN 978-5-534-11626-7. — Текст: электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/518510>

28. Гордеев, С. И. Организация баз данных в 2 ч. Часть 2: учебник для среднего профессионального образования / С. И. Гордеев, В. Н. Волошина. — 2-е изд., испр. и доп. — Москва: Издательство Юрайт, 2023. — 513 с. — (Профессиональное образование). — ISBN 978-5-534-11625-0. — Текст: электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/518511>

29. Грошев, А. С. Основы работы с базами данных: учебное пособие для СПО / А. С. Грошев. — Саратов: Профобразование, 2021. — 255 с. — ISBN 978-5-4488-1006-0. — Текст: электронный // Цифровой образовательный ресурс IPR SMART: [сайт]. — URL: <https://www.iprbookshop.ru/102199.html>

30. Дибров, М. В. Компьютерные сети и телекоммуникации. Маршрутизация в IP-сетях в 2 ч. Часть 1: учебник и практикум для среднего профессионального образования / М. В. Дибров. — Москва: Издательство Юрайт, 2023. — 333 с. — (Профессиональное образование). — ISBN 978-5-534-04638-0. — Текст: электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/513518>

31. Дибров, М. В. Компьютерные сети и телекоммуникации. Маршрутизация в IP-сетях в 2 ч. Часть 2: учебник и практикум для среднего профессионального образования / М. В. Дибров. — Москва: Издательство Юрайт, 2023. — 351 с. — (Профессиональное образование). — ISBN 978-5-534-04635-9. — Текст: электронный // Образовательная платформа Юрайт [сайт]. —

URL: <https://urait.ru/bcode/514019>

32. Епишкина, А. В. Нормативное регулирование в области защиты информации. Конспект лекций: учебное пособие / А. В. Епишкина, С. В. Запечников. — Москва: Национальный исследовательский ядерный университет «МИФИ», 2021. — 116 с. — ISBN 978-5-7262-2807-5. — Текст: электронный // Цифровой образовательный ресурс IPR SMART: [сайт]. — URL: <https://www.iprbookshop.ru/125496.html>

33. Илюшечкин, В. М. Основы использования и проектирования баз данных: учебник для среднего профессионального образования / В. М. Илюшечкин. — испр. и доп. — Москва: Издательство Юрайт, 2023. — 213 с. — (Профессиональное образование). — ISBN 978-5-534-01283-5. — Текст: электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/513827>

34. Казарин, О. В. Основы информационной безопасности: надежность и безопасность программного обеспечения: учебное пособие для среднего профессионального образования / О. В. Казарин, И. Б. Шубинский. — Москва: Издательство Юрайт, 2023. — 342 с. — (Профессиональное образование). — ISBN 978-5-534-10671-8. — Текст: электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/518005>

35. Киренберг, А. Г. Информационная безопасность современных операционных систем: учебное пособие / А. Г. Киренберг. — Кемерово: Кузбасский государственный технический университет имени Т.Ф. Горбачева, 2022. — 138 с. — ISBN 978-5-00137-320-9. — Текст: электронный // Цифровой образовательный ресурс IPR SMART: [сайт]. — URL: <https://www.iprbookshop.ru/128393.html>

36. Киренберг, А. Г. Системное администрирование и информационная безопасность сетей ЭВМ: учебное пособие / А. Г. Киренберг. — Кемерово: Кузбасский государственный технический университет имени Т.Ф. Горбачева, 2022. — 119 с. — ISBN 978-5-00137-292-9. — Текст: электронный // Цифровой образовательный ресурс IPR SMART: [сайт]. — URL: <https://www.iprbookshop.ru/128406.html>

37. Молдованова, О. В. Информационные системы и базы данных: учебное пособие для СПО / О. В. Молдованова. — Саратов: Профобразование, 2021. — 177 с. — ISBN 978-5-4488-1177-7. — Текст: электронный // Цифровой образовательный ресурс IPR SMART: [сайт]. — URL: <https://www.iprbookshop.ru/106617.html>

38. Нестеров, С. А. Базы данных: учебник и практикум для среднего профессионального образования / С. А. Нестеров. — Москва: Издательство Юрайт, 2023. — 230 с. — (Профессиональное образование). — ISBN 978-5-534-11629-8. — Текст: электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/518507>

39. Никифоров, С. Н. Методы защиты информации. Защищенные сети: учебное пособие / С. Н. Никифоров. — 2-е изд., стер. — Санкт-Петербург: Лань, 2021. — 96 с. — ISBN 978-5-8114-8123-1. — Текст: электронный // Лань: электронно-библиотечная система. — URL: <https://e.lanbook.com/book/171868>

40. Олифер, В. Г. Основы сетей передачи данных: учебное пособие для СПО / В. Г. Олифер, Н. А. Олифер. — Саратов: Профобразование, 2021. — 219 с. — ISBN 978-5-4488-1007-7. — Текст: электронный // Цифровой образовательный ресурс IPR SMART: [сайт]. — URL: <https://www.iprbookshop.ru/102200.html>

41. Операционные системы: учебное пособие для СПО / составители И. В. Винокуров. — Саратов, Москва: Профобразование, Ай Пи Ар Медиа, 2022. — 127 с. — ISBN 978-5-4488-1441-9, 978-5-4497-1444-2. — Текст: электронный // Цифровой образовательный ресурс IPR SMART: [сайт]. — URL: <https://www.iprbookshop.ru/115697.html>
42. Операционные системы. Программное обеспечение: учебник / составитель Т. П. Куль. — Санкт-Петербург: Лань, 2020. — 248 с. — ISBN 978-5-8114-4290-4. — Текст: электронный // Лань: электронно-библиотечная система. — URL: <https://e.lanbook.com/book/131045>
43. Сети и телекоммуникации: учебник и практикум для среднего профессионального образования / К. Е. Самуйлов [и др.]; под редакцией К. Е. Самуйлова, И. А. Шалимова, Д. С. Кулябова. — Москва: Издательство Юрайт, 2023. — 363 с. — (Профессиональное образование). — ISBN 978-5-9916-0480-2. — Текст: электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/517817>
44. Стасышин, В. М. Базы данных: технологии доступа: учебное пособие для среднего профессионального образования / В. М. Стасышин, Т. Л. Стасышина. — 2-е изд., испр. и доп. — Москва: Издательство Юрайт, 2023. — 164 с. — (Профессиональное образование). — ISBN 978-5-534-09888-4. — Текст: электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/516927>
45. Суворова, Г. М. Основы информационной безопасности: учебное пособие для СПО / Г. М. Суворова. — Саратов: Профобразование, 2021. — 135 с. — ISBN 978-5-4488-1294-1. — Текст: электронный // Цифровой образовательный ресурс IPR SMART: [сайт]. — URL: <https://www.iprbookshop.ru/108005.html>
46. Тумбинская, М. В. Комплексное обеспечение информационной безопасности на предприятии: учебник / М. В. Тумбинская, М. В. Петровский. — Санкт-Петербург: Лань, 2022. — 344 с. — ISBN 978-5-8114-3940-9. — Текст: электронный // Лань : электронно-библиотечная система. — URL: <https://e.lanbook.com/book/207095>
47. Тумбинская, М. В. Защита информации на предприятии: учебное пособие / М. В. Тумбинская, М. В. Петровский. — Санкт-Петербург: Лань, 2020. — 184 с. — ISBN 978-5-8114-4291-1. — Текст: электронный // Лань: электронно-библиотечная система. — URL: <https://e.lanbook.com/book/130184>
48. Фомин, Д. В. Информационная безопасность: учебное пособие для СПО / Д. В. Фомин. — Саратов, Москва: Профобразование, Ай Пи Ар Медиа, 2022. — 218 с. — ISBN 978-5-4488-1351-1, 978-5-4497-1565-4. — Текст: электронный // Цифровой образовательный ресурс IPR SMART: [сайт]. — URL: <https://www.iprbookshop.ru/118458.html>
49. Фомин, Д. В. Защита информации: специализированные аттестованные программные и программно-аппаратные средства: практикум / Д. В. Фомин. — Саратов: Вузовское образование, 2021. — 218 с. — ISBN 978-5-4487-0795-7. — Текст: электронный // Цифровой образовательный ресурс IPR SMART: [сайт]. — URL: <https://www.iprbookshop.ru/110329.html>
50. Шаньгин, В. Ф. Информационная безопасность и защита информации / В. Ф. Шаньгин. — 2-е изд. — Саратов: Профобразование, 2019. — 702 с. — ISBN 978-5-4488-0070-2. — Текст: электронный // Цифровой образовательный ресурс IPR SMART: [сайт]. — URL: <https://www.iprbookshop.ru/87995.html>
51. Швецов, В. И. Базы данных: учебное пособие для СПО / В. И. Швецов.

— Саратов: Профобразование, 2019. — 219 с. — ISBN 978-5-4488-0357-4. — Текст: электронный // Цифровой образовательный ресурс IPR SMART: [сайт]. — URL: <https://www.iprbookshop.ru/86192.html>

52. Щербак, А. В. Информационная безопасность: учебник для среднего профессионального образования / А. В. Щербак. — Москва: Издательство Юрайт, 2023. — 259 с. — (Профессиональное образование). — ISBN 978-5-534-15345-3. — Текст: электронный // — URL: <https://urait.ru/bcode/519614>

2.3 Порядок организации и защиты дипломного проекта

Государственная итоговая аттестация по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем предусматривает выполнение дипломного проекта.

Дипломный проект направлен на систематизацию и закрепление знаний выпускника по специальности, а также определение уровня готовности выпускника к самостоятельной профессиональной деятельности. 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 дипломного проекта, в том числе предложения своей темы с необходимым обоснованием целесообразности ее разработки для практического применения. При этом тема дипломного проекта должна соответствовать содержанию одного или нескольких профессиональных модулей, входящих в ОП СПО.

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 дипломного проекта обучающийся должен подтвердить свою подготовленность к самостоятельной профессиональной деятельности и право на присвоение ему квалификации техника по защите информации.

Дипломный проект (70-90 страниц рукописного или 50-80 страниц печатного текста 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 Экономический раздел, включающий в себя расчёт экономической эффективности проекта.

5 Безопасность жизнедеятельности.

В проектной (практической) части выделяются три направления:

- разработка проекта по модернизации программно-аппаратных и инженерно-технических 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 дипломного проекта должна иллюстрировать постановку задачи, формализацию методов ее решения, реализацию, полученные результаты.

Под презентационной частью 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 обучающимся своих средств представления презентаций (ноутбуков).

Тематика дипломных проектов разрабатывается преподавателями кафедры информационных технологий и экономики и рассматривается на заседании кафедры.

2.3.1 Фонд оценочных средств для защиты дипломного проекта

Примерный перечень тем дипломных проектов:

- 1 Проектирование системы защиты компьютерной информации организации.
- 2 Организация программной защиты информации учета кадров на предприятии.
- 3 Защита информации в локальной вычислительной сети организации при использовании сервисов и ресурсов сетей общего пользования.
- 4 Защита информации в локальной вычислительной сети предприятия.
- 5 Организация режима защиты конфиденциальной информации в экономическом отделе предприятия.
- 6 Анализ системы защиты электронного документооборота предприятия.
- 7 Разработка защищённой автоматизированной информационной системы.
- 8 Разработка политики информационной безопасности организации.
- 9 Проектирование системы видеонаблюдения для магазина.
- 10 Защита информации в локальной вычислительной сети предприятия на основе контроллера домена.
- 11 Организация программной защиты информации предприятия в

приложении «1С: Предприятие»

12 Защита информации в локальной вычислительной сети предприятия при использовании сети Интернет.

13 Разработка системы защиты информации АИС «Пропуск» для администрации г. Ливны.

14 Анализ системы обеспечения информационной безопасности АИС «Кадры» и разработка предложений по её совершенствованию.

15 Анализ системы обеспечения информационной безопасности рабочих станций локальной вычислительной сети предприятия.

16 Организация программной защиты информации организации в приложении «1С: Бухгалтерия»

17 Анализ системы обеспечения информационной безопасности учёта продукции для организации товародвижения готовой продукции.

18 Организация системы защиты автоматизированного учёта движения продукции.

19 Организация системы защиты автоматизированной системы пропуск-контроля администрации Ливенского района.

20 Организация системы защиты локальной вычислительной сети организации с модулем Wi-Fi.

21 Анализ системы обеспечения информационной безопасности автоматизированного заполнения первичной документации.

22 Обеспечение безопасности информационной системы тестирования уровня знаний

23 Обеспечение безопасности информационной системы АПС предприятия

24 Обеспечение безопасности информационной системы образовательного учреждения

25 Обеспечение безопасности информационной системы учета средств компьютерной техники

Закрепление тем дипломных проектов с указанием руководителей и сроков выполнения за обучающимися оформляется приказом директора филиала.

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

Защита дипломных проектов проводится на открытом заседании ГЭК по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем, утвержденной приказом директора Ливенского филиала ОГУ имени И.С. Тургенева. На защиту дипломного проекта отводится до 45 мин.

Общую оценку за 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 дипломным проектам даются членами ГЭК на закрытом заседании и объявляются выпускникам в тот же день после подписания соответствующего протокола заседания комиссии.

Качественно выполненный дипломный проект должен свидетельствовать об умении студента:

- 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» – представленный на защиту 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 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 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. Дипломный проект соответствует названию работы, ее содержанию, имеет четкую целевую направленность, логическую последовательность изложения материала, которые базируется на прочных теоретических знаниях по избранной теме. Изложение материала корректно и грамотно оформлено.

«Хорошо» – представленный на защиту 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 дипломного проекта продемонстрировал хорошо аргументированное обоснование темы; четкую формулировку и понимание изучаемой проблемы. В 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 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 дипломного проекта. Ответы на

некоторые вопросы членов ГЭК даны в неполном объеме.

«Удовлетворительно» – представленный 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 профессиональных компетенций, но при защите дипломного проекта отмечены отдельные отступления от требований, предъявляемых к уровню подготовки по специальностям СПО. Ход защиты дипломного проекта показал достаточную профессиональную подготовку выпускника.

«Неудовлетворительно» – представленный на защиту 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 (дипломного проекта) 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 неудовлетворительным 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.

2.3.2 Перечень литературы, необходимой для подготовки дипломного проекта

Основная литература:

1. Беленький, В. Г. Беспроводные сети передачи данных: учебное пособие для СПО / В. Г. Беленький, А. В. Лошкарёв. — Саратов: Профобразование, 2022. — 98 с. — ISBN 978-5-4488-1499-0. — Текст: электронный // Цифровой образовательный ресурс IPR SMART: [сайт]. — URL: <https://www.iprbookshop.ru/125572.html>

2. Внуков, А. А. Основы информационной безопасности: защита информации: учебное пособие для среднего профессионального образования / А. А. Внуков. — 3-е изд., перераб. и доп. — Москва: Издательство Юрайт, 2023. — 161 с. — (Профессиональное образование). — ISBN 978-5-534-13948-8. — Текст: электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/518006>

3. Гостев, И. М. Операционные системы: учебник и практикум для среднего профессионального образования / И. М. Гостев. — 2-е изд., испр. и доп. — Москва: Издательство Юрайт, 2023. — 164 с. — (Профессиональное образование). — ISBN 978-5-534-04951-0. — Текст: электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/514426>

4. Зиангирова, Л. Ф. Инфокоммуникационные системы и сети: учебное пособие для СПО / Л. Ф. Зиангирова. — Саратов: Профобразование, Ай Пи Ар Медиа, 2019. — 128 с. — ISBN 978-5-4488-0302-4, 978-5-4497-0183-1. — Текст: электронный // Цифровой образовательный ресурс IPR SMART: [сайт]. — URL: <https://www.iprbookshop.ru/85806.html>
5. Извозчикова, В. В. Эксплуатация информационных систем : учебное пособие для СПО / В. В. Извозчикова. — Саратов: Профобразование, 2019. — 136 с. — ISBN 978-5-4488-0355-0. — Текст: электронный // Цифровой образовательный ресурс IPR SMART: [сайт]. — URL: <https://www.iprbookshop.ru/86210.html>
6. Ильин, М. Е. Криптографическая защита информации в объектах информационной инфраструктуры: учеб. для студ. учреждений сред. проф. образования / М. Е. Ильин, Т. И. Калинкина, В. Н. Пржегорлинский ; под ред. В. Н. Пржегорлинского. — Москва: Академия, 2020. — 288 с. — URL: <https://www.academia-moscow.ru/catalogue/4831/444518/>
7. Казарин, О. В. Программно-аппаратные средства защиты информации. Защита программного обеспечения: учебник и практикум для среднего профессионального образования / О. В. Казарин, А. С. Забабурин. — Москва: Издательство Юрайт, 2023. — 312 с. — (Профессиональное образование). — ISBN 978-5-534-13221-2. — Текст: электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/519364>
8. Мэйволд, Э. Безопасность сетей: учебное пособие для СПО / Э. Мэйволд. — Саратов: Профобразование, 2021. — 571 с. — ISBN 978-5-4488-0990-3. — Текст: электронный // Цифровой образовательный ресурс IPR SMART: [сайт]. — URL: <https://www.iprbookshop.ru/102183.html>
9. Организационное и правовое обеспечение информационной безопасности: учебник и практикум для среднего профессионального образования / Т. А. Полякова, А. А. Стрельцов, С. Г. Чубукова, В. А. Ниесов; ответственные редакторы Т. А. Полякова, А. А. Стрельцов. — Москва: Издательство Юрайт, 2023. — 325 с. — (Профессиональное образование). — ISBN 978-5-534-00843-2. — Текст: электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/512861>
10. Скрипник, Д. А. Общие вопросы технической защиты информации: учебное пособие / Д. А. Скрипник. — 3-е изд. — Москва, Саратов: Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2020. — 424 с. — ISBN 978-5-4497-0336-1. — Текст: электронный // Цифровой образовательный ресурс IPR SMART: [сайт]. — URL: <https://www.iprbookshop.ru/89451.html>
11. Советов, Б. Я. Базы данных: учебник для среднего профессионального образования / Б. Я. Советов, В. В. Цехановский, В. Д. Чертовской. — 3-е изд., перераб. и доп. — Москва: Издательство Юрайт, 2023. — 420 с. — (Профессиональное образование). — ISBN 978-5-534-09324-7. — Текст: электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/514585>
12. Солонская, О. И. Средства защиты информации: учебное пособие для СПО / О. И. Солонская. — Саратов: Профобразование, 2022. — 88 с. — ISBN 978-5-4488-1504-1. — Текст: электронный // Цифровой образовательный ресурс IPR SMART: [сайт]. — URL: <https://www.iprbookshop.ru/125578.html>
13. Технологии защиты информации в компьютерных сетях: учебное пособие для СПО / Н. А. Руденков, А. В. Пролетарский, Е. В. Смирнова, А. М.

Суоров. — Саратов: Профобразование, 2021. — 368 с. — ISBN 978-5-4488-1014-5. — Текст: электронный // Цифровой образовательный ресурс IPR SMART: [сайт]. — URL: <https://www.iprbookshop.ru/102207.html>

14. Фороузан, Б. А. Криптография и безопасность сетей: учебное пособие для СПО / Б. А. Фороузан; под редакцией А. Н. Берлина. — Саратов: Профобразование, 2021. — 776 с. — ISBN 978-5-4488-0999-6. — Текст: электронный // Цифровой образовательный ресурс IPR SMART: [сайт]. — URL: <https://www.iprbookshop.ru/102192.html>

Дополнительная литература:

15. Конституция Российской Федерации (с гимном России). Новая редакция. - Москва: Проспект, 2021. - 64 с.

16. О безопасности. Федеральный закон от 28.12.2010 N 390-ФЗ (ред. от 09.11.2020) // СПС КонсультантПлюс.

17. О персональных данных. Федеральный закон от 27.07.2006 N 152-ФЗ (ред. от 14.07.2022) // СПС КонсультантПлюс.

18. О техническом регулировании. Федеральный закон от 27.12.2002 N 184-ФЗ (ред. от 02.07.2021) (с изм. и доп., вступ. в силу с 23.12.2021) // СПС КонсультантПлюс.

19. Об информации, информационных технологиях и о защите информации. Федеральный закон от 27.07.2006 N 149-ФЗ (ред. от 29.12.2022) (с изм. и доп., вступ. в силу с 09.01.2023) // СПС КонсультантПлюс.

20. Об утверждении Инструкции об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну. Приказ ФАПСИ от 13.06.2001 N 152 (Зарегистрировано в Минюсте РФ 06.08.2001 N 2848) // СПС КонсультантПлюс.

21. Об утверждении Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005). Приказ ФСБ РФ от 09.02.2005 N 66 (ред. от 12.04.2010) (Зарегистрировано в Минюсте РФ 03.03.2005 N 6382) // СПС КонсультантПлюс.

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

23. ГОСТ Р ИСО/МЭК 13335-1-2006. Национальный стандарт Российской Федерации. Информационная технология. Методы и средства обеспечения безопасности. Часть 1. Концепция и модели менеджмента безопасности информационных и телекоммуникационных технологий" (утв. и введен в действие Приказом Ростехрегулирования от 19.12.2006 N 317-ст) // СПС КонсультантПлюс.

24. ГОСТ Р 50739-95. Средства вычислительной техники. Защита от несанкционированного доступа к информации. Общие технические требования (принят и введен в действие Постановлением Госстандарта РФ от 09.02.1995 N 49) // СПС КонсультантПлюс.

25. Меры защиты информации в государственных информационных системах. Методический документ (утв. ФСТЭК России 11.02.2014) // СПС КонсультантПлюс.

26. Авдошин, С. М. Технологии и продукты Microsoft в обеспечении информационной безопасности: учебное пособие для СПО / С. М. Авдошин, А. А.

Савельева, В. А. Сердюк. — Саратов: Профобразование, 2021. — 431 с. — ISBN 978-5-4488-1015-2. — Текст: электронный // Цифровой образовательный ресурс IPR SMART: [сайт]. — URL: <https://www.iprbookshop.ru/102208.html>

27. Гордеев, С. И. Организация баз данных в 2 ч. Часть 1: учебник для среднего профессионального образования / С. И. Гордеев, В. Н. Волошина. — 2-е изд., испр. и доп. — Москва: Издательство Юрайт, 2023. — 310 с. — (Профессиональное образование). — ISBN 978-5-534-11626-7. — Текст: электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/518510>

28. Гордеев, С. И. Организация баз данных в 2 ч. Часть 2: учебник для среднего профессионального образования / С. И. Гордеев, В. Н. Волошина. — 2-е изд., испр. и доп. — Москва: Издательство Юрайт, 2023. — 513 с. — (Профессиональное образование). — ISBN 978-5-534-11625-0. — Текст: электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/518511>

29. Грошев, А. С. Основы работы с базами данных: учебное пособие для СПО / А. С. Грошев. — Саратов: Профобразование, 2021. — 255 с. — ISBN 978-5-4488-1006-0. — Текст: электронный // Цифровой образовательный ресурс IPR SMART: [сайт]. — URL: <https://www.iprbookshop.ru/102199.html>

30. Дибров, М. В. Компьютерные сети и телекоммуникации. Маршрутизация в IP-сетях в 2 ч. Часть 1: учебник и практикум для среднего профессионального образования / М. В. Дибров. — Москва: Издательство Юрайт, 2023. — 333 с. — (Профессиональное образование). — ISBN 978-5-534-04638-0. — Текст: электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/513518>

31. Дибров, М. В. Компьютерные сети и телекоммуникации. Маршрутизация в IP-сетях в 2 ч. Часть 2: учебник и практикум для среднего профессионального образования / М. В. Дибров. — Москва: Издательство Юрайт, 2023. — 351 с. — (Профессиональное образование). — ISBN 978-5-534-04635-9. — Текст: электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/514019>

32. Епишкина, А. В. Нормативное регулирование в области защиты информации. Конспект лекций: учебное пособие / А. В. Епишкина, С. В. Запечников. — Москва: Национальный исследовательский ядерный университет «МИФИ», 2021. — 116 с. — ISBN 978-5-7262-2807-5. — Текст: электронный // Цифровой образовательный ресурс IPR SMART: [сайт]. — URL: <https://www.iprbookshop.ru/125496.html>

33. Илюшечкин, В. М. Основы использования и проектирования баз данных: учебник для среднего профессионального образования / В. М. Илюшечкин. — испр. и доп. — Москва: Издательство Юрайт, 2023. — 213 с. — (Профессиональное образование). — ISBN 978-5-534-01283-5. — Текст: электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/513827>

34. Казарин, О. В. Основы информационной безопасности: надежность и безопасность программного обеспечения: учебное пособие для среднего профессионального образования / О. В. Казарин, И. Б. Шубинский. — Москва: Издательство Юрайт, 2023. — 342 с. — (Профессиональное образование). — ISBN 978-5-534-10671-8. — Текст: электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/518005>

35. Киренберг, А. Г. Информационная безопасность современных операционных систем: учебное пособие / А. Г. Киренберг. — Кемерово: Кузбасский государственный технический университет имени Т.Ф. Горбачева, 2022. — 138 с. — ISBN 978-5-00137-320-9. — Текст: электронный // Цифровой образовательный ресурс IPR SMART: [сайт]. — URL: <https://www.iprbookshop.ru/128393.html>
36. Киренберг, А. Г. Системное администрирование и информационная безопасность сетей ЭВМ: учебное пособие / А. Г. Киренберг. — Кемерово: Кузбасский государственный технический университет имени Т.Ф. Горбачева, 2022. — 119 с. — ISBN 978-5-00137-292-9. — Текст: электронный // Цифровой образовательный ресурс IPR SMART: [сайт]. — URL: <https://www.iprbookshop.ru/128406.html>
37. Молдованова, О. В. Информационные системы и базы данных: учебное пособие для СПО / О. В. Молдованова. — Саратов: Профобразование, 2021. — 177 с. — ISBN 978-5-4488-1177-7. — Текст: электронный // Цифровой образовательный ресурс IPR SMART: [сайт]. — URL: <https://www.iprbookshop.ru/106617.html>
38. Нестеров, С. А. Базы данных: учебник и практикум для среднего профессионального образования / С. А. Нестеров. — Москва: Издательство Юрайт, 2023. — 230 с. — (Профессиональное образование). — ISBN 978-5-534-11629-8. — Текст: электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/518507>
39. Никифоров, С. Н. Методы защиты информации. Защищенные сети: учебное пособие / С. Н. Никифоров. — 2-е изд., стер. — Санкт-Петербург: Лань, 2021. — 96 с. — ISBN 978-5-8114-8123-1. — Текст: электронный // Лань: электронно-библиотечная система. — URL: <https://e.lanbook.com/book/171868>
40. Олифер, В. Г. Основы сетей передачи данных: учебное пособие для СПО / В. Г. Олифер, Н. А. Олифер. — Саратов: Профобразование, 2021. — 219 с. — ISBN 978-5-4488-1007-7. — Текст: электронный // Цифровой образовательный ресурс IPR SMART: [сайт]. — URL: <https://www.iprbookshop.ru/102200.html>
41. Операционные системы: учебное пособие для СПО / составители И. В. Винокуров. — Саратов, Москва: Профобразование, Ай Пи Ар Медиа, 2022. — 127 с. — ISBN 978-5-4488-1441-9, 978-5-4497-1444-2. — Текст: электронный // Цифровой образовательный ресурс IPR SMART: [сайт]. — URL: <https://www.iprbookshop.ru/115697.html>
42. Операционные системы. Программное обеспечение: учебник / составитель Т. П. Куль. — Санкт-Петербург: Лань, 2020. — 248 с. — ISBN 978-5-8114-4290-4. — Текст: электронный // Лань: электронно-библиотечная система. — URL: <https://e.lanbook.com/book/131045>
43. Сети и телекоммуникации: учебник и практикум для среднего профессионального образования / К. Е. Самуйлов [и др.]; под редакцией К. Е. Самуйлова, И. А. Шалимова, Д. С. Кулябова. — Москва: Издательство Юрайт, 2023. — 363 с. — (Профессиональное образование). — ISBN 978-5-9916-0480-2. — Текст: электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/517817>
44. Стасышин, В. М. Базы данных: технологии доступа: учебное пособие для среднего профессионального образования / В. М. Стасышин, Т. Л. Стасышина. — 2-е изд., испр. и доп. — Москва: Издательство Юрайт, 2023. — 164 с. — (Профессиональное образование). — ISBN 978-5-534-09888-4. —

Текст: электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/516927>

45. Суворова, Г. М. Основы информационной безопасности: учебное пособие для СПО / Г. М. Суворова. — Саратов: Профобразование, 2021. — 135 с. — ISBN 978-5-4488-1294-1. — Текст: электронный // Цифровой образовательный ресурс IPR SMART: [сайт]. — URL: <https://www.iprbookshop.ru/108005.html>

46. Тумбинская, М. В. Комплексное обеспечение информационной безопасности на предприятии: учебник / М. В. Тумбинская, М. В. Петровский. — Санкт-Петербург: Лань, 2022. — 344 с. — ISBN 978-5-8114-3940-9. — Текст: электронный // Лань: электронно-библиотечная система. — URL: <https://e.lanbook.com/book/207095>

47. Тумбинская, М. В. Защита информации на предприятии: учебное пособие / М. В. Тумбинская, М. В. Петровский. — Санкт-Петербург: Лань, 2020. — 184 с. — ISBN 978-5-8114-4291-1. — Текст: электронный // Лань: электронно-библиотечная система. — URL: <https://e.lanbook.com/book/130184>

48. Фомин, Д. В. Информационная безопасность: учебное пособие для СПО / Д. В. Фомин. — Саратов, Москва: Профобразование, Ай Пи Ар Медиа, 2022. — 218 с. — ISBN 978-5-4488-1351-1, 978-5-4497-1565-4. — Текст: электронный // Цифровой образовательный ресурс IPR SMART: [сайт]. — URL: <https://www.iprbookshop.ru/118458.html>

49. Фомин, Д. В. Защита информации: специализированные аттестованные программные и программно-аппаратные средства: практикум / Д. В. Фомин. — Саратов: Вузовское образование, 2021. — 218 с. — ISBN 978-5-4487-0795-7. — Текст: электронный // Цифровой образовательный ресурс IPR SMART: [сайт]. — URL: <https://www.iprbookshop.ru/110329.html>

50. Щербак, А. В. Информационная безопасность: учебник для среднего профессионального образования / А. В. Щербак. — Москва: Издательство Юрайт, 2023. — 259 с. — (Профессиональное образование). — ISBN 978-5-534-15345-3. — Текст: электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/519614>

3. Порядок апелляции по результатам государственной 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 филиала, 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 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.