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

ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ

Сертификат:
00BAD2D3875881A40814260BF2E8455588
Владелец: Колякина Елена Анатольевна
Действителен: с 14.07.2023 до 06.10.2024

«Утверждаю»
И.о. проректор
по учебно-методической
деятельности _____ Н.С. Лаушкина

ПРОГРАММА
ГОСУДАРСТВЕННОЙ ИТОГОВОЙ АТТЕСТАЦИИ

наименование специальности
10.02.04 Обеспечение информационной безопасности
телекоммуникационных 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 10.02.04 Обеспечение информационной безопасности телекоммуникационных систем, утверждённого приказом Министерства образования и науки Российской Федерации №1551 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:
директор АО ИРК «Принт-ТВ» _____ Г.И. Карзов

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

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 10.02.04 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 10.02.04 Обеспечение информационной безопасности телекоммуникационных 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 24.08.2022 № 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 10.02.04 Обеспечение информационной безопасности телекоммуникационных систем) от 09.12.2016 г. №1551;

- 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 телекоммуникационных 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».

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 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 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 информационно-телекоммуникационных систем и сетей.
ПК 1.4.	Осуществлять контроль функционирования информационно-телекоммуникационных 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 информационно-телекоммуникационных систем и сетей.
ПК 2.2.	Поддерживать бесперебойную работу программных и программно-аппаратных, 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 информационно-телекоммуникационных 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.

1.5 Формы проведения государственной итоговой аттестации

Государственная итоговая аттестация по образовательной программе среднего профессионального образования 10.02.04 Обеспечение информационной безопасности телекоммуникационных систем в соответствии с федеральным государственным образовательным стандартом среднего профессионального образования проводится в форме 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 10.02.04 Обеспечение информационной безопасности телекоммуникационных 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 10.02.04 Обеспечение информационной безопасности телекоммуникационных 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 10.02.04-2023 (далее - КОД) по специальности 10.02.04 Обеспечение информационной безопасности телекоммуникационных 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://om.firpo.ru/competencies. Задание ДЭ включает комплексную практическую задачу, моделирующую профессиональную деятельность и выполняемую в режиме реального времени.

Пример типового задания для проведения демонстрационного экзамена по специальности 10.02.04 Обеспечение информационной безопасности телекоммуникационных систем по компетенции

Код и наименование профессии (специальности) среднего профессионального образования	**10.02.04 Обеспечение информационной безопасности телекоммуникационных систем**
Наименование квалификации	Техник по защите информации
Федеральный государственный образовательный стандарт среднего профессионального образования по профессии (специальности) среднего профессионального образования (ФГОС СПО):	ФГОС СПО по специальности 10.02.04 Обеспечение информационной безопасности, утвержденный приказом Министерства образования и науки РФ от 09.12.2016 г. № 1551
Код комплекта оценочной документации	КОД 10.02.04-1-2024

Модуль 1: Эксплуатация информационно-коммуникационных систем и сетей

С помощью технологии виртуальных машин для выполнения задания смоделирована корпоративная сеть организации на 2 филиалах (Главный офис — виртуальные машины, Офис филиал — виртуальные машины). При выполнении заданий необходимо ключевые настройки подтверждать скриншотами. В ходе выполнения данного задания нужно установить основное ПО на рабочие станции будущей защищенной сети. Для правильной работы сети надо создать или убедиться в наличии 4 сетей. Необходимо записать все IP адреса, логины и пароли в текстовый файл. В связи с особенностями работы системы на серверных версиях необходимо устанавливать компоненты системы вручную (например, БД, сервер ЦУС, клиент ЦУС) используя пакеты MSI в подпапках дистрибутивов.

Задача 1. Развертывание ПК Administrator в качестве центра сертификации. Установить базу данных на ВМ Net1-DB (незащищенный узел) Установить и настроить рабочее место администратора Certification Authority (на базе виртуальной машины Net1-Admin (ЦО)): Центр управления сетью (серверное приложение ЦУС), Удостоверяющий и ключевой центр (УКЦ); использовать ранее установленную БД. Установить клиент ЦУС на ВМ Net1-DB (незащищенный узел)

Задача 2. Установка ПО VPN Coordinator и ПО VPN Client для Certification Authority

1. Установить ПО Client, рабочее место администратора;
2. Установить и инициализировать ПО Coordinator HW-VA.

Задача 3. Установка центра регистрации, сервиса публикации и сервиса информирования Certification Authority на соответствующие виртуальные машины

1. Установить ПО Client.
2. Установить ПО Publication Service.
3. Установить ПО Registration Point.
4. Установить ПО CA Informing., теги.
5. Произвести проверку работоспособности политик.

Задача 4. Установка ПО Coordinator и ПО Client для организации сети филиала 1. Установить и инициализировать ПО Coordinator HW-VA. 2. Установить ПО Client, рабочее место пользователя.

Задача 5. 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.

Задача 6. Создание структуры защищенной сети ЦУС. Необходимо создать в ЦУС структуру защищенной сети в соответствии с заданной схемой. Создать пользователей узлов, настроить полномочия пользователей и их связи в соответствии со схемой. Провести инициализацию УКЦ. Задать пароли пользователей. Сформировать дистрибутивы ключей для всех сетевых узлов. Создать группы узлов для центрального офиса (удостоверяющего центра) и филиала, настроить пароль администратора группы сетевых узлов для каждой из групп. На всех узлах сети корректно настроить корректность настройки сетевых, проверить доступность соседних узлов. Разнести DST файлы по АРМ, провести первичную инициализацию узлов защищенной сети (координаторов и клиентов), проверить доступность узлов защищенной сети.

Модуль 2: Защита информации в информационно-коммуникационных системах и сетях с использованием программных, программно-аппаратных, в том числе криптографических средств защиты

Задача 7. 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;

• квалифицированную электронную подпись для пользователя;

• квалифицированную электронную подпись для пользователя. 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):

1. зарегистрировать пользователя;

2. отправить запрос в УКЦ на выпуск сертификата, удовлетворить запрос;

3. отправить запрос в УКЦ на аннулирование ранее выпущенного ГИА/ДЭ ПУ 29 сертификата, удовлетворить запрос. Посредством Сервиса Информирования (CA Informing):

4. настроить способ выдачи уведомлений;

5. сформировать отчет о выданных за текущие сутки сертификатах, предварительно в настройках указав место хранения отчетов

Задача 8. Компрометация узла защищенной сети. Произвести компрометацию ключей и восстановление сетевого взаимодействия средствами УКЦ/ЦУС:

1. скомпрометировать ключи пользователя на узле;

2. произвести смену ключей пользователя и сетевых узлов;

3. отправить обновления и произвести процедуру смены ключа пользователя;

4. проверить работу защищенной сети после обновления отправив сообщение от пользователя.

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 10.02.04 - 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. 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.academia-moscow.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.academia-moscow.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-valentina-andreevna-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.: Интернет-Университет 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 c. — 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 c. — 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 c. — 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.academia-moscow.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 c. — 978-5-4488-0015-3. — 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 c. — 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 c. — 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 c. — 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 c. — 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. 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.

35. 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/

36. 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.

2.3 Порядок организации и защиты дипломного проекта

Государственная итоговая аттестация по специальности 10.02.04 Обеспечение информационной безопасности телекоммуникационных 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.

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 10.02.04 Обеспечение информационной безопасности телекоммуникационных 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 чёткую 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 профессиональный 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 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 дипломного проекта 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 дипломного проекта. Проявлена недостаточная профессиональная подготовка.

2.3.1 Фонд оценочных средств для защиты дипломного проекта

Примерный перечень тем 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

2.3.2 Перечень литературы, необходимой для подготовки дипломного проекта

Основная литерат

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.academia-moscow.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.academia-moscow.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-valentina-andreevna-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.: Интернет-Университет 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 c. — 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 c. — 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 c. — 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 c. — 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 c. — 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 c. — 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.academia-moscow.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. — 978-5-4488-0015-3. — 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. - 240с. – 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.