Документ подписан простой электронной подписью
Информация о владельце:
ФИО: Нилова Екатерина Викторовна
Должность: Директор
Дата подписания: 05.02.2025 10:00:00
Уникальный программный ключ:
02C8 4F90 008A B230 9845 B4E4 6D85 DDCA 3A
Срок действия: с 20.02.2025 по 20.05.2026

АВТОНОМНАЯ НЕКОММЕРЧЕСКАЯ
ПРОФЕССИОНАЛЬНАЯ ОБРАЗОВАТЕЛЬНАЯ ОРГАНИЗАЦИЯ
«УРЮПИНСКИЙ КОЛЛЕДЖ БИЗНЕСА»

РАССМОТРЕНО
на заседании педагогического совета
АНПОО «Урюпинский колледж бизнеса»
Протокол № 3 от «25» декабря 2024 г.

СОГЛАСОВАНО
Разработчик
АО «БАРС Груп»
С.В. Симонов

УТВЕРЖДЕНО
Директор
АНПОО «Урюпинский колледж бизнеса»
Е.В. Нилова
«26» декабря 2024 г.

ПРОГРАММА
ГОСУДАРСТВЕННОЙ ИТОГОВОЙ АТТЕСТАЦИИ
по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем
на 2024-2025 учебный год

Урюпинск 2024 г.

СОДЕРЖАНИЕ

1. Общие положения 3
2. Форма государственной итоговой аттестации 14
3. Подготовка проведения ГИА 17
3.1. Сроки проведения 17
3.2. Дополнительные сроки 18
3.3. Необходимые материалы для подготовки и проведения ГИА 18
3.4. Кадровое обеспечение ГИА 19
3.5. Условия подготовки государственной итоговой аттестации 20
3.6. Тематика дипломных проектов 21
3.7. Подготовка к демонстрационному экзамену 24
3.8. Требования к дипломному проекту и методика его оценивания 25
3.8.1. Структура дипломного проекта 25
3.8.2. Содержание дипломного проекта 25
4. Проведение государственной итоговой аттестации 28
4.1. Защита дипломного проекта 28
4.2. Процедура проведения демонстрационного экзамена 29
4.3. Обобщенная оценочная ведомость 31
4.4. Модули с описанием работ 32
4.5. Порядок проведения демонстрационного экзамена 36
5. Оценивание результатов ГИА 38
5.1. Критерии оценки текста дипломного проекта 38
5.2. Критерии оценки защиты дипломного проекта 38
5.3. Итоговая оценка сформированности общих и профессиональных компетенций при выполнении и защите дипломного проекта выпускников по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем 39
5.4. Оформление результатов демонстрационного экзамена 40
5.5. Показатели и критерии оценивания компетенций по результатам сдачи демонстрационного экзамена, шкалы их оценивания 41
5.6. Методика перевода результатов демонстрационного экзамена в оценку 41
6. Порядок подачи и рассмотрения апелляций 42
7. Оценивание результатов ГИА Особенности проведения ГИА для выпускников из числа лиц с ограниченными возможностями здоровья, детей-инвалидов и инвалидов 43
8. Материально-техническое обеспечение ГИА 45
9. Хранение дипломных проектов 45
10. Документы, выдаваемые по итогам аттестационных процедур 45
ПРИЛОЖЕНИЯ 46

1. Общие положения

Программа государственной итоговой аттестации выпускников по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем разработана в соответствии с требованиями:

– Федерального закона от 29.12.2012 №273-ФЗ (ред. от 28.12.2024) «Об образовании в Российской Федерации»;

– Приказа Минобрнауки России от 09.12.2016 №1553 (ред. от 03.07.2024) «Об утверждении федерального государственного образовательного стандарта среднего профессионального образования по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем»

– Приказа Минобрнауки России от 09.12.2016 №1553 (ред. от 03.07.2024) «Об утверждении федерального государственного образовательного стандарта среднего профессионального образования по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем» (Зарегистрировано в Минюсте России 26.12.2016 № 44938);

– Приказа Минпросвещения России от 08.11.2021 №800 (ред. от 24.04.2024) «Об утверждении Порядка проведения государственной итоговой аттестации по образовательным программам среднего профессионального образования» (Зарегистрировано в Минюсте России 07.12.2021 № 66211);

– Приказа Минпросвещения России от 05.05.2022 №311 «О внесении изменений в приказ Министерства просвещения Российской Федерации от 8 ноября 2021 г. №800 «Об утверждении Порядка проведения государственной итоговой аттестации по образовательным программам среднего профессионального образования» (Зарегистрировано в Минюсте России 27.05.2022 №68606);

– Приказа Минпросвещения России от 19.01.2023 №37 «О внесении изменений в Порядок проведения государственной итоговой аттестации по образовательным программам среднего профессионального образования, утвержденный приказом Министерства просвещения Российской Федерации от 8 ноября 2021 г. №800» (Зарегистрировано в Минюсте России 03.04.2023 №72843);

– Приказа Минпросвещения России от 24.08.2022 №762 (ред. от 20.12.2022) «Об утверждении Порядка организации и осуществления образовательной деятельности по образовательным программам среднего профессионального образования» (Зарегистрировано в Минюсте России 21.09.2022 №70167);

– Распоряжения Минпросвещения России от 01.04.2020 №Р-36 «О внесении изменений в приложение к распоряжению Министерства просвещения Российской Федерации от 1 апреля 2019 г. №Р-42 «Об утверждении методических рекомендаций о проведении аттестации с использованием механизма демонстрационного экзамена»;

– Приказа Минпросвещения России от 17.03.2020 №103 «Об утверждении временного порядка сопровождения реализации образовательных программ начального общего, основного общего, среднего общего образования, образовательных программ среднего профессионального образования и дополнительных общеобразовательных программ с применением электронного обучения и дистанционных образовательных технологий» (Зарегистрировано в Минюсте России 19.03.2020 №57788);

– «Методических рекомендаций по организации выполнения и защиты выпускной квалификационной работы в образовательных организациях, реализующих образовательные программы среднего профессионального образования по программам подготовки специалистов среднего звена» (направлены письмом Минобрнауки России от 20.07.2015 №06-846);

– Приказа Минпросвещения России от 02.06.2022 №390 (ред. от 27.12.2022) «Об утверждении образцов и описания диплома о среднем профессиональном образовании и приложения к нему» (Зарегистрировано в Минюсте России 12.08.2022 №69621);

– Устава Автономной некоммерческой профессиональной образовательной организации «Урюпинский колледж бизнеса» утверждённого решением Правления (решение учредителя № 1 от 12 декабря 2023 года)

– Приказа ФГБОУ ДПО ИРПО от 22 июня 2023 г. № П-291 «О введении в действие Методики организации и проведения демонстрационного экзамена»);

– Комплекты оценочной документации для проведения в 2025 году государственной итоговой аттестации (промежуточной аттестации) по образовательным программам среднего профессионального образования в форме демонстрационного экзамена базового и профильного уровней по профессии (специальности) среднего профессионального образования 10.02.05 Обеспечение информационной безопасности автоматизированных систем (в редакции от 17.01.2025);

– Профессионального стандарта «Специалист по защите информации в автоматизированных системах» (утв. Приказом Министерства труда и социальной защиты РФ от 15 сентября 2016 г. № 522н).

– Профессионального стандарта «Специалист по защите информации в телекоммуникационных системах и сетях» (утв. приказом Министерства труда и социальной защиты Российской Федерации от 3 ноября 2016 г. №608н);

– Профессионального стандарта «Специалист по безопасности компьютерных систем и сетей» (утв. приказом Министерства труда и социальной защиты Российской Федерации от 1 ноября 2016 г. №598н);

– Профессионального стандарта «Специалист по технической защите информации», (утв. приказом Министерства труда и социальной защиты Российской Федерации от 1 ноября 2016 г. №599н);

– Профессионального стандарта «Специалист по обнаружению, предупреждению и ликвидации последствий компьютерных атак» (утв. приказом Министерства труда и социальной защиты Российской Федерации от 29 декабря 2015 г. № 1179н.)

Программа государственной итоговой аттестации (далее – ГИА) является частью программы подготовки специалистов среднего звена в соответствии с ФГОС СПО по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем 10.00.00 «Информационная безопасность» (квалификация – техник по защите информации, база приема – основное общее образование).

При разработке программы государственной итоговой аттестации определены:

- форма и вид государственной итоговой аттестации;
- объем времени на подготовку и проведение государственной итоговой аттестации;
- сроки проведения государственной итоговой аттестации;
- требования к дипломному проекту;
- условия подготовки и процедура проведения государственной итоговой аттестации;
- критерии оценки уровня и качества подготовки выпускника.

Данная программа доводится до сведения студентов не позднее, чем за шесть месяцев до начала проведения процедур государственной итоговой аттестации.

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

Решение о допуске студентов к государственной итоговой аттестации оформляется приказом директора АНПОО «Урюпинский колледж бизнеса».

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

Техник по защите информации должен быть подготовлен к решению профессиональных задач в соответствии видами профессиональной деятельности:

в области Эксплуатации автоматизированных (информационных) систем в защищенном исполнении

знать:

– состав и принципы работы автоматизированных систем, операционных систем и сред;

– принципы разработки алгоритмов программ, основных приемов программирования;

– модели баз данных;

– принципы построения, физические основы работы периферийных устройств, основных методов организации и проведения технического обслуживания вычислительной техники и других технических средств информатизации;

– теоретические основы компьютерных сетей и их аппаратных компонент, сетевых моделей, протоколов и принципов адресации;

– порядок установки и ввода в эксплуатацию средств защиты информации в компьютерных сетях.

уметь:

– обеспечивать работоспособность, обнаруживать и устранять неисправности, осуществлять комплектование, конфигурирование, настройку автоматизированных систем в защищенном исполнении и компонент систем защиты информации автоматизированных систем;

– производить установку, адаптацию и сопровождение типового программного обеспечения, входящего в состав систем защиты информации автоматизированной системы;

– организовывать, конфигурировать, производить монтаж, осуществлять диагностику и устранять неисправности компьютерных сетей, работать с сетевыми протоколами разных уровней;

– настраивать и устранять неисправности программно-аппаратных средств защиты информации в компьютерных сетях по заданным правилам.

иметь практический опыт в:

– эксплуатации компонентов систем защиты информации автоматизированных систем, их диагностике, устранении отказов и восстановлении работоспособности;

– администрировании автоматизированных систем в защищенном исполнении;

– установке компонентов систем защиты информации автоматизированных информационных систем.

в области Защиты информации в автоматизированных системах программными и программно-аппаратными средствами

знать:

– особенности и способы применения программных и программно-аппаратных средств защиты информации, в том числе, в операционных системах, компьютерных сетях, базах данных;

– типовые модели управления доступом, средств, методов и протоколов идентификации и аутентификации;

– типовые средства и методы ведения аудита, средств и способов защиты информации в локальных вычислительных сетях, средств защиты от несанкционированного доступа;

– основные понятия криптографии и типовых криптографических методов и средств защиты информации.

уметь:

– устанавливать, настраивать, применять программные и программно-аппаратные средства защиты информации;

– диагностировать, устранять отказы, обеспечивать работоспособность и тестировать функции программно-аппаратных средств защиты информации;

– проверять выполнение требований по защите информации от несанкционированного доступа при аттестации объектов информатизации по требованиям безопасности информации;

– использовать типовые программные криптографические средства, в том числе электронную подпись;

– устанавливать и настраивать средства антивирусной защиты в соответствии с предъявляемыми требованиями;

– осуществлять мониторинг и регистрацию сведений, необходимых для защиты объектов информатизации, в том числе с использованием программных и программно-аппаратных средств обнаружения, предупреждения и ликвидации последствий компьютерных атак.

иметь практический опыт в:

– установке и настройке программных средств защиты информации;

– тестировании функций, диагностике, устранении отказов и восстановлении работоспособности программных и программно-аппаратных средств защиты информации;

– учете, обработке, хранении и передаче информации, для которой установлен режим конфиденциальности.

в области Защиты информации техническими средствами

знать:

– физические основы, структуру и условия формирования технических каналов утечки информации, способы их выявления и методы оценки опасности, классификацию существующих физических полей и технических каналов утечки информации;

– номенклатуру и характеристики аппаратуры, используемой для измерения параметров побочных электромагнитных излучений и наводок (далее - ПЭМИН), а также параметров фоновых шумов и физических полей, создаваемых техническими средствами защиты информации;

– основные принципы действия и характеристики, порядок технического обслуживания, устранение неисправностей и организацию ремонта технических средств защиты информации;

– основные способы физической защиты объектов информатизации;

– методики инструментального контроля эффективности защиты информации, обрабатываемой средствами вычислительной техники на объектах информатизации;

– номенклатуру применяемых средств защиты информации от несанкционированной утечки по техническим каналам и физической защиты объектов информатизации.

уметь:

– применять средства охранной сигнализации, охранного телевидения и систем контроля и управления доступом;

– применять технические средства для криптографической защиты информации конфиденциального характера;

– применять технические средства для уничтожения информации и носителей информации, защиты информации в условиях применения мобильных устройств обработки и передачи данных;

– применять инженерно-технические средства физической защиты объектов информатизации.

иметь практический опыт в:

– выявлении технических каналов утечки информации;

– применении, техническом обслуживании, диагностике, устранении отказов, восстановлении работоспособности, установке, монтаже и настройке инженерно-технических средств физической защиты и технических средств защиты информации;

– проведении измерений параметров ПЭМИН, создаваемых техническими средствами обработки информации, для которой установлен режим конфиденциальности, при аттестации объектов информатизации по требованиям безопасности информации;

– проведении измерений параметров фоновых шумов, а также физических полей, создаваемых техническими средствами защиты информации.

в области Выполнения работ по одной или нескольким профессиям рабочих, должностям служащих

знать:

– состав и принципы работы автоматизированных систем, операционных систем и сред;

– принципы построения, физические основы работы периферийных устройств, основных методов организации и проведения технического обслуживания вычислительной техники и других технических средств информатизации;

– теоретические основы компьютерных сетей и их аппаратных компонент, сетевых моделей, протоколов и принципов адресации;

– особенности и способы применения программных и программно-аппаратных средств защиты информации, в том числе, в операционных системах, компьютерных сетях, базах данных;

– типовые модели управления доступом, средств, методов и протоколов идентификации и аутентификации;

– основные способы физической защиты объектов информатизации.

уметь:

– производить установку, адаптацию и сопровождение типового программного обеспечения, входящего в состав систем защиты информации автоматизированной системы;

– организовывать, конфигурировать, производить монтаж, осуществлять диагностику и устранять неисправности компьютерных сетей, работать с сетевыми протоколами разных уровней;

– устанавливать, настраивать, применять программные и программно-аппаратные средства защиты информации;

– диагностировать, устранять отказы, обеспечивать работоспособность и тестировать функции программно-аппаратных средств защиты информации;

– использовать типовые программные криптографические средства, в том числе электронную подпись;

– устанавливать и настраивать средства антивирусной защиты в соответствии с предъявляемыми требованиями;

– осуществлять мониторинг и регистрацию сведений, необходимых для защиты объектов информатизации, в том числе с использованием программных и программно-аппаратных средств обнаружения, предупреждения и ликвидации последствий компьютерных атак;

– применять технические средства для уничтожения информации и носителей информации, защиты информации в условиях применения мобильных устройств обработки и передачи данных.

иметь практический опыт в:

– эксплуатации компонентов систем защиты информации автоматизированных систем, их диагностике, устранении отказов и восстановлении работоспособности;

– установке компонентов систем защиты информации автоматизированных информационных систем;

– установке и настройке программных средств защиты информации;

– тестировании функций, диагностике, устранении отказов и восстановлении работоспособности программных и программно-аппаратных средств защиты информации; учете, обработке, хранении и передаче информации, для которой установлен режим конфиденциальности

в соответствии с Профессиональным стандартом №525н

Трудовые функции:

– Проведение технического обслуживания систем защиты информации автоматизированных систем А/01.5 (таб.1.1);

– Ведение технической документации, связанной с эксплуатацией систем защиты информации автоматизированных систем А/02.5 (таб. 1.2);

– Обеспечение защиты информации при выводе из эксплуатации автоматизированных систем А/03.5 (таб. 1.3).

Таблица 1.1

Трудовая функция

Наименование	Проведение технического обслуживания систем защиты информации автоматизированных систем	Код	А/01.5	Уровень (подуровень) квалификации	5

Трудовые действия	Проверка работоспособности системы защиты информации автоматизированной системы
	Контроль соответствия конфигурации системы защиты информации автоматизированной системы ее эксплуатационной документации
	Контроль стабильности характеристик системы защиты информации автоматизированной системы
Необходимые умения	Конфигурировать параметры системы защиты информации автоматизированной системы в соответствии с ее эксплуатационной документацией
	Обнаруживать и устранять неисправности системы защиты информации автоматизированной системы согласно эксплуатационной документации
	Производить монтаж и диагностику компьютерных сетей
	Использовать типовые криптографические средства защиты информации, в том числе средства электронной подписи
Необходимые знания	Типовые средства и методы защиты информации в локальных и глобальных вычислительных сетях
	Базовой конфигурации системы защиты информации автоматизированной системы

	Особенностей применения программных и программно-аппаратных средств защиты информации в автоматизированных системах
	Типовых средств, методов и протоколов идентификации, аутентификации и авторизации
	Нормативных правовых актов в области защиты информации
	Организационных мер по защите информации

Таблица 1.2

Трудовая функция

Наименование	Ведение технической документации, связанной с эксплуатацией систем защиты информации автоматизированных систем	Код	A/02.5	Уровень (подуровень) квалификации	5

Трудовые действия	Ведение документов учета, обработки, хранения и передачи информации, составляющей тайну
	Информирование персонала об угрозах безопасности информации
	Информирование персонала о правилах эксплуатации системы защиты автоматизированной системы и отдельных средств защиты информации
	Ведение протоколов и журналов учета при изменении конфигурации систем защиты информации автоматизированных систем
	Ведение протоколов и журналов учета при осуществлении мониторинга систем защиты информации автоматизированных систем
	Ведение протоколов и журналов учета при осуществлении аудита систем защиты информации автоматизированных систем
Необходимые умения	Оформлять документацию по регламентации мероприятий и оказанию услуг в области защиты информации
	Оформлять техническую документацию в соответствии с нормативными правовыми актами в области защиты информации
Необходимые знания	Нормативные правовые акты в области защиты информации
	Основные методические и руководящие документы уполномоченных федеральных органов исполнительной власти по защите информации
	Эксплуатационная и проектная документация на автоматизированную систему
	Основные методы организации и проведения технического обслуживания технических средств информатизации
	Организационные меры по защите информации

Таблица 1.3

Трудовые функции

Наименование	Обеспечение защиты информации при выводе из эксплуатации автоматизированных систем	Код	A/03.5	Уровень (подуровень) квалификации	5

Трудовые действия	Уничтожение информации, обрабатываемой автоматизированной системой
	Уничтожение машинных носителей информации, обрабатываемой автоматизированной системой
	Архивирование информации, обрабатываемой автоматизированной системой
Необходимые умения	Использовать программные средства для архивирования информации
	Использовать программные и программно-аппаратные средства для уничтожения информации и носителей информации
	Использовать типовые криптографические средства защиты информации, в том числе электронную подпись
Необходимые знания	Процедуры по архивированию информации, обрабатываемой автоматизированной системой
	Назначение и принципы работы основных узлов современных технических средств информатизации
	Организация ремонтного обслуживания компонентов автоматизированной системы
	Регламент автоматизированной системы по уничтожению информации и машинных носителей информации
	Нормативные правовые акты в области защиты информации
	Основные методические и руководящие документы уполномоченных федеральных органов исполнительной власти по защите информации

в соответствии с Профессиональным стандартом №474н

Трудовые функции:

– Проведение технического обслуживания систем защиты информации автоматизированных систем A/01.5 (таб.1.4);

– Ведение технической документации, связанной с эксплуатацией систем защиты информации автоматизированных систем A/02.5 (таб. 1.5);

– Обеспечение защиты информации при выводе из эксплуатации автоматизированных систем A/03.5 (таб. 1.6).

Таблица 1.4

Трудовая функция

Наименование	Проведение работ по установке, настройке, испытаниям и техническому обслуживанию технических средств защиты информации от	Код	A/01.5	Уровень (подуровень) квалификации	5

	утечки за счет побочных электромагнитных квалификации излучений и наводок				

Трудовые действия	Установка и монтаж технических средств защиты информации от утечки за счет побочных электромагнитных излучений и наводок
	Настройка и испытание технических средств защиты информации от утечки за счет побочных электромагнитных излучений и наводок
	Техническое обслуживание технических средств защиты информации от утечки за счет побочных электромагнитных излучений и наводок
	Устранение неисправностей и организация ремонта технических средств защиты информации от утечки за счет побочных электромагнитных излучений и наводок
Необходимые умения	Проводить установку и монтаж технических средств защиты информации от утечки за счет побочных электромагнитных излучений и наводок в соответствии с техническим проектом, инструкциями по эксплуатации и эксплуатационно-техническими документами
	Проводить настройку и испытание технических средств защиты информации от утечки за счет побочных электромагнитных излучений и наводок в соответствии с инструкциями по эксплуатации и требованиями нормативно-методических документов
	Проводить техническое обслуживание технических средств защиты информации от утечки за счет побочных электромагнитных излучений и наводок в соответствии с инструкциями по эксплуатации и эксплуатационно-техническими документами
	Проводить устранение выявленных неисправностей технических средств защиты информации от утечки за счет побочных электромагнитных излучений и наводок и при необходимости организовывать их ремонт
Необходимые знания	Нормативные правовые акты, методические документы, национальные стандарты в области защиты информации ограниченного доступа и аттестации объектов информатизации на соответствие требованиям по защите информации
	Технические каналы утечки информации, возникающие за счет побочных электромагнитных излучений от основных технических средств, за счет наводок информативных сигналов на цепи электропитания и заземления основных технических средств и систем, вспомогательные технические средства и системы, их кабельные коммуникации, а также создаваемые методом высокочастотного облучения основных технических средств и систем и за счет возможно внедренных электронных

	устройств перехвата информации в основных технических средствах и системах
	Способы и средства защиты информации от утечки за счет побочных электромагнитных излучений и наводок
	Средства и методики контроля эффективности защиты информации от утечки за счет побочных электромагнитных излучений и наводок
	Технические описания и инструкции (руководства) по эксплуатации технических средств защиты информации от утечки за счет побочных электромагнитных излучений и наводок
	Проектная документация на систему защиты объекта информатизации (в части защиты объекта от утечки информации за счет побочных электромагнитных излучений и наводок)
	Порядок технического обслуживания технических средств защиты информации от утечки за счет побочных электромагнитных излучений и наводок
	Порядок устранения неисправностей и организации ремонта средств защиты информации от утечки за счет побочных электромагнитных излучений и наводок

Таблица 1.5

Трудовая функция

Наименование	Проведение работ по установке, настройке, испытаниям и техническому обслуживанию технических средств защиты акустической речевой информации от ее утечки по техническим квалификации каналам	Код	A/02.5	Уровень (подуровень) квалификации	5

Трудовые действия	Установка и монтаж технических средств защиты акустической речевой информации от утечки по техническим каналам
	Настройка и испытания технических средств защиты акустической речевой информации от утечки по техническим каналам
	Техническое обслуживание технических средств защиты акустической речевой информации от утечки по техническим каналам
	Устранение неисправностей и организация ремонта технических средств защиты акустической речевой информации от утечки по техническим каналам
Необходимые умения	Производить установку и монтаж технических средств защиты акустической речевой информации от утечки по техническим каналам в соответствии с техническим проектом, инструкциями

	по эксплуатации и эксплуатационно-техническими документами
	Проводить настройку и испытания технических средств защиты акустической речевой информации от утечки по техническим каналам в соответствии с технической документацией, инструкциями по эксплуатации и эксплуатационно-техническими документами
	Проводить техническое обслуживание технических средств защиты акустической речевой информации от утечки по техническим каналам в соответствии с инструкциями по эксплуатации и эксплуатационно-техническими документами
	Проводить устранение выявленных неисправностей технических средств защиты акустической речевой информации от утечки по техническим каналам и при необходимости организовывать их ремонт
Необходимые знания	Нормативные правовые акты, методические документы, национальные стандарты в области защиты информации ограниченного доступа и аттестации выделенных (защищаемых) помещений на соответствие требованиям по защите информации
	Технические каналы утечки акустической речевой информации (прямые акустические, вибрационные, акустооптические, акустоэлектрические, акустоэлектромагнитные)
	Возможности средств акустической речевой разведки
	Технические каналы утечки акустической речевой информации, создаваемые за счет возможно внедренных электронных устройств перехвата информации в технические средства и (или) помещения
	Основные характеристики электронных устройств перехвата информации
	Способы и средства защиты акустической речевой информации от утечки по техническим каналам
	Средства и методики контроля эффективности защиты акустической речевой информации от утечки по техническим каналам
	Технические описания и инструкции по эксплуатации технических средств защиты речевой информации от утечки по техническим каналам
	Проектная документация на систему защиты выделенного помещения (в части защиты акустической речевой информации от утечки по техническим каналам)
	Порядок технического обслуживания технических средств защиты речевой информации от утечки по техническим каналам
	Порядок устранения неисправностей технических средств защиты акустической речевой информации от утечки по техническим каналам и организация их ремонта

Таблица 1.6

Трудовые функции

Наименование	Проведение работ по установке, настройке, испытаниям и техническому обслуживанию программных (программно-технических) средств защиты информации от несанкционированного доступа	Код	A/03.5	Уровень (подуровень) квалификации	5

Трудовые действия	Установка и настройка программных (программно-технических) средств защиты информации от несанкционированного доступа
	Испытания программных (программно-технических) средств защиты информации от несанкционированного доступа
	Техническое обслуживание программно-технических средств защиты информации от несанкционированного доступа
	Обнаружение и исправление ошибок в программных средствах защиты информации от несанкционированного доступа
	Устранение неисправностей и организация ремонта программно-технических средств защиты информации от несанкционированного доступа
Необходимые умения	Производить установку и настройку программных (программно-технических) средств защиты информации от несанкционированного доступа в соответствии с инструкциями по эксплуатации и эксплуатационно-техническими документами
	Проводить испытания программных (программно-технических) средств защиты информации от несанкционированного доступа в соответствии с инструкциями по эксплуатации и эксплуатационно-техническими документами
	Проводить обнаружение и исправление ошибок в программных средствах защиты информации от несанкционированного доступа
	Проводить техническое обслуживание программно-технических средств защиты информации от несанкционированного доступа в соответствии с инструкциями по эксплуатации и эксплуатационно-техническими документами
	Проводить устранение выявленных неисправностей программно-технических средств защиты информации от несанкционированного доступа и при необходимости организовывать их ремонт
Необходимые знания	Нормативные правовые акты, методические документы, национальные стандарты в области защиты информации от несанкционированного доступа и аттестации

	автоматизированных систем на соответствие требованиям по защите информации
	Способы реализации несанкционированного доступа к информации и специальных программных воздействий на информацию и ее носители в автоматизированных системах
	Методы и средства защиты информации от несанкционированного доступа и специальных программных воздействий на нее
	Средства и методики контроля защищенности информации от несанкционированного доступа и специальных программных воздействий
	Технические описания и инструкции по эксплуатации программных (программно-технических) средств защиты информации от несанкционированного доступа
	Порядок технического обслуживания программно-технических средств защиты информации от несанкционированного доступа и специальных воздействий
	Порядок устранения неисправностей программно-технических средств защиты информации от несанкционированного доступа и специальных воздействий, организации их ремонта

2. Форма государственной итоговой аттестации

Формой государственной итоговой аттестации по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем является защита дипломного проекта и демонстрационного экзамена.

Защита дипломного проекта и демонстрационного экзамена, является обязательным завершающим этапом среднего профессионального образования, предоставляют возможности для самореализации и творческого самовыражения. Его успешное прохождение является необходимым условием присвоения выпускникам квалификации дипломированного специалиста – «техник по защите информации» по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем.

Демонстрационный экзамен направлен на определение уровня освоения выпускником материала, предусмотренного образовательной программой, 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, способствует систематизации и закреплению знаний выпускника по специальности при решении конкретных задач, а также выяснению уровня подготовки выпускника к самостоятельной работе.

Ориентируясь на достижение общих целей образования в целом и целей среднего профессионального образования в частности, дипломный проект и демонстрационный экзамен, имеет свои специфические особенности, связанные с её основной функцией – итоговым контролем и оценкой качества образовательного процесса. При этом предъявляются требования к качеству выполнения и защиты дипломного проекта, а также выделяются умения, определяющие уровень профессиональной подготовки студента:

– умение четко формулировать рассматриваемую задачу, определять ее актуальность и значимость, структурировать решаемую задачу;

– обоснованно выбирать и корректно использовать наиболее эффективные методы решения задач;

– уметь генерировать и анализировать альтернативные варианты и принимать оптимальные решения с учетом множественности критериев, влияющих факторов и характера информации;

– использовать в работе современные информационные технологии, средства компьютерной техники и их программное обеспечение;

– уметь осуществлять поиск научно-технической информации и работать со специальной литературой;

– грамотно, с использованием специальной терминологии и лексики, четко, в логической последовательности излагать содержание выполненных разработок.

Дипломный проект и демонстрационный экзамен предусматривает моделирование реальных производственных условий для решения выпускниками практических задач профессиональной деятельности. Задания демонстрационного экзамена разрабатываются на основе профессиональных стандартов и с учетом оценочных материалов (при наличии), ФГБОУ ДПО ИРПО (далее - ИРПО).

Демонстрационный экзамен профильного уровня проводится по решению Колледжа на основании заявлений выпускников на основе требований к результатам освоения образовательных программ среднего профессионального образования, установленных ФГОС СПО, с учетом положений федерального государственного бюджетного образовательного учреждения дополнительного профессионального образования Институт развития дополнительного профессионального образования (далее - ИРПО), а также квалификационных требований, заявленных организациями, работодателями, заинтересованными в подготовке кадров соответствующей квалификации, в том числе являющимися стороной договора о сетевой форме реализации образовательных программ и (или) договора о практической подготовке обучающихся (далее - организации-партнеры).

Дипломный проект, являясь этапом образовательного процесса, преследует цели пополнения, закрепления и развития знаний, умений, приобретенных на предшествующих этапах обучения. Подготовка дипломного проекта предполагает высокую степень самостоятельности студента, предоставляет возможности для самореализации и творческого самовыражения. Ориентируясь на достижение общих целей образования в целом, формирование и развитие креативного (созидательного, инновационного) типа мышления и целей среднего профессионального образования в частности, выпускная квалификационная работа направлена на выполнение основных требований к результатам освоения основной профессиональной образовательной программы, по которым производится оценка уровня профессиональной подготовленности студента. Интегрально эти основные требования сводятся к следующему:

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

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

ОК 03. Планировать и реализовывать собственное профессиональное и личностное развитие.

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

ОК 05. Осуществлять устную и письменную коммуникацию на государственном языке с учетом особенностей социального и культурного контекста.

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

ОК 07. Содействовать сохранению окружающей среды, ресурсосбережению, эффективно действовать в чрезвычайных ситуациях.

ОК 08. Использовать средства физической культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и поддержания необходимого уровня физической подготовленности.

ОК 09. Использовать информационные технологии в профессиональной деятельности.

ОК 10. Пользоваться профессиональной документацией на государственном и иностранном языках.

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

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.

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.

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.

3. Подготовка проведения ГИА

Объем времени на подготовку и проведение государственной итоговой аттестации студентов, установлен федеральным государственным образовательным стандартом среднего профессионального образования и рабочим учебным планом по специальности 10.02.05

Обеспечение информационной безопасности автоматизированных систем квалификация «техник по защите информации».

Учебным планом по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем квалификация «техник по защите информации» на подготовку и проведение государственной итоговой аттестации отведено: 4 недели – на подготовку выпускной квалификационной работы и 2 – недели на работу государственной экзаменационной комиссии (далее – ГЭК).

3.1. Сроки проведения

В соответствии с календарным учебным графиком на 2024-2025учебный год государственная итоговая аттестация проводится в сроки:

Таблица 1

Содержание и объем государственной итоговой аттестации

Структура ГИА	Количество часов	Продолжительность в неделях	Сроки проведения
Подготовка дипломного проекта	144	4	19.05.2025-14.06.2025
Подготовка к демонстрационному экзамену			
Защита дипломного проекта	72	2	16.06.2025-30.06.2025
Проведение демонстрационного экзамена			23.06.2025-26.06.2025
ИТОГО	216	6	

3.2. Дополнительные сроки

Обучающиеся, непрошедшие ГИА или получившие на ГИА неудовлетворительные результаты, проходят ГИА не ранее чем через шесть месяцев после прохождения ГИА впервые.

Для прохождения ГИА лицо, не прошедшее ГИА по неуважительной причине или получившее на ГИА неудовлетворительную оценку, восстанавливается в АНПОО «Урюпинский колледж бизнеса» на период времени, установленный образовательной организацией самостоятельно, но не менее предусмотренного календарным учебным графиком для прохождения ГИА соответствующей образовательной программы СПО.

Повторное прохождение ГИА для одного лица назначается АНПОО «Урюпинский колледж бизнеса» не более двух раз.

3.3. Необходимые материалы для подготовки и проведения ГИА

В соответствии с Порядком проведения государственной итоговой аттестации по образовательным программам среднего профессионального образования выпускников, обучающихся по ФГОС СПО на заседания государственной экзаменационной комиссии предоставляются следующие документы:

– ФГОС СПО по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем;

– Программа государственной итоговой аттестации выпускников по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем;

– Документация по оценке сформированности элементов общих и профессиональных компетенций, оценочные листы;

– Сводная ведомость результатов освоения основной профессиональной образовательной программы выпускниками по специальности;

– Приказ о закреплении тематики дипломных проектов по специальности;

– Приказ Комитета образования, науки и молодежной политики Волгоградской области о назначении председателя ГЭК;

– Приказ директора АНПОО «Урюпинский колледж бизнеса» об утверждении состава государственной экзаменационной и апелляционной комиссии;

– Приказ директора АНПОО «Урюпинский колледж бизнеса» о допуске к защите дипломных проектов выпускников специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем, успешно завершивших обучение по ППССЗ на заседании ГЭК по специальности;

– Приказ директора АНПОО «Урюпинский колледж бизнеса» об утверждении тем дипломных проектов (с указанием сроков исполнения) и назначении руководителей дипломных проектов и консультантов;

– Индивидуальное задание, разработанное руководителем дипломного проекта по утвержденной теме;

– График защиты дипломного проекта;

– Протоколы заседаний ГЭК по специальности;

– Зачетные книжки студентов;

– Выполненные дипломные проекты студентов с письменными отзывом руководителя дипломного проекта и рецензией установленной формы;

– Оценочные материалы для проведения демонстрационного экзамена, разработанные ИРПО;

– Методические рекомендации по выполнению дипломных проектов по специальности.

3.4. Кадровое обеспечение ГИА

3.1. Для проведения ГИА в Колледже создаются государственные экзаменационные комиссии (далее — ГЭК) по каждой образовательной программе среднего профессионального образования, реализуемой Колледжем, и апелляционная комиссия (далее вместе — комиссии).

3.2. ГЭК формируется из числа педагогических работников Колледжа, лиц, приглашенных из сторонних организаций, в том числе:

– педагогических работников;

– представителей организаций-партнеров, направление деятельности которых соответствует области профессиональной деятельности, к которой готовятся выпускники;

– экспертов организации, наделенной полномочиями по обеспечению прохождения ГИА в форме демонстрационного экзамена (далее - оператор) (при проведении ГИА в форме демонстрационного экзамена), обладающих профессиональными знаниями, навыками и опытом в сфере, соответствующей профессии, специальности среднего профессионального образования, по которой проводится демонстрационный экзамен (далее - эксперты).

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

3.4. Состав ГЭК утверждается приказом Колледжа и действует в течение одного

календарного года. В состав ГЭК входят председатель ГЭК, заместитель председателя ГЭК и члены ГЭК.

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

Председателями ГЭК утверждаются не позднее 20 декабря текущего года на следующий календарный год (с 1 января по 31 декабря) по представлению Колледжа Комитетом образования, науки и молодежной политики Волгоградской области.

Председателями ГЭК Колледжа утверждаются лица, не работающее в Колледже, 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.

3.6. Директор Колледжа является заместителем председателя ГЭК. В случае создания в Колледже нескольких ГЭК назначается несколько заместителей председателя ГЭК из числа заместителей директора Колледжа или педагогических работников.

3.7. Экспертная группа создается по каждой профессии, специальности среднего профессионального образования или виду деятельности, по которому проводится демонстрационный экзамен.

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 демонстрационного экзамена и не участвует в оценивании результатов ГИА.

3.5. Условия подготовки государственной итоговой аттестации

Государственная итоговая аттестация выпускников, завершающих обучение в колледже, является обязательной.

К государственной итоговой аттестации допускаются студенты, предоставившие документы, подтверждающие освоение компетенций при изучении теоретического материала и прохождении практики по каждому из основных видов профессиональной деятельности по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем (базовой подготовки), характеристики с мест прохождения производственной и преддипломной практики. В том числе выпускником могут быть предоставлены отчеты о ранее достигнутых результатах, дополнительные сертификаты, свидетельства (дипломы) олимпиад, конкурсов, творческие работы по специальности, которые свидетельствуют об уровне и качестве освоения профессиональных и общих компетенций. Допуск студентов к государственной итоговой аттестации производится приказом по колледжу.

Программа государственной итоговой аттестации доводится до сведения студентов не позднее, чем за 6 месяцев до начала государственной итоговой аттестации.

Для закрепления выбранной темы дипломного проекта и назначения руководителя работы, выпускник обязан написать заявление на имя директора колледжа. Окончательное закрепление тем дипломного проекта оформляется приказом по колледжу.

Выполнение дипломного проекта студенты осуществляют в течение 4 недель под консультационным сопровождением руководителя.

Основные функции руководителя дипломного проекта:

– разработка задания на подготовку дипломного проекта;

– разработка совместно со студентом содержания дипломного проекта;

– оказание помощи студенту в разработке индивидуального графика работы на весь период выполнения дипломного проекта;

– консультирование студента по вопросам содержания и последовательности выполнения дипломного проекта;

– оказание помощи студенту в подборе необходимых источников;

– контроль хода выполнения дипломного проекта в соответствии с установленным графиком в форме регулярного обсуждения руководителем и студентом хода работ;

– оказание помощи (консультирование студента) в подготовке презентации и доклада для защиты дипломного проекта;

– предоставление письменного отзыва на дипломный проект.

Консультации проводятся согласно графику, утверждаемому на кафедре экономики и информационных дисциплин.

Руководитель дипломного проекта составляется график проверки хода выполнения дипломного проекта, который утверждается на заседании кафедры экономики и информационных дисциплин (Приложение 5).

Руководители дипломного проекта проводят консультации по выполнению и оформлению работы в соответствии с графиком.

По завершении работы руководитель дипломного проекта проверяет ее оформление, подписывает ее и с письменным отзывом (Приложение 4) передает на кафедру для согласования и направления на рецензирование (Приложение 3). Готовая работа переплетается в переплете в колледже и сдается на кафедру экономики и информационных дисциплин не позднее семи дней до защиты для подготовки необходимых материалов на заседание ГЭК и допуска работы к защите заместителем директора по учебной работе. Работа, не соответствующая предъявляемым требованиям, к защите не допускается.

3.6. Тематика дипломных проектов

Тематика дипломных проектов разрабатывается преподавателями кафедры экономики и информационных дисциплин и согласовывается со специалистами организаций или предприятий производственного профиля, где проходили преддипломную практику или временно работали студенты.

Обязательным требованием является – соответствие тематики дипломного проекта содержанию одного или нескольких профессиональных модулей.

Темы дипломных проектов имеют практико-ориентированный характер и соответствуют содержанию:

ПМ.01 Эксплуатация автоматизированных (информационных) систем в защищенном исполнении

ПМ.02 Защита информации в автоматизированных системах программными и программно-аппаратными средствами

ПМ. 03 Защита информации техническими средствами.

При разработке тематики учитывают особенности развития Волгоградской области и выполняются по предложениям организаций различных сфер деятельности.

Требования к содержанию, объему и структуре дипломного проекта определяются колледжем на основании порядка проведения государственной итоговой аттестации выпускников по программам СПО, утвержденного федеральным органом исполнительной власти, осуществляющим функции по выработке государственной политики и нормативно-правовому регулированию в сфере образования, определенного в соответствии со статьей 59 Закона «Об образовании в Российской Федерации» от 29.12.2012 г. № 273-ФЗ и п.10 Порядка проведения государственной итоговой аттестации по образовательным программам среднего профессионального образования: - тематика дипломного проекта должна соответствовать

содержанию одного или нескольких профессиональных модулей, входящих в образовательную программу среднего профессионального образования и отвечать современным требованиям развития науки, техники, производства, экономики, культуры и образования:

– темы дипломных проектов рассматриваются на кафедре экономики и информационных дисциплин, а затем согласовываются с предприятиями (базами преддипломной практики), если дипломный проект выполняется по заказу предприятия (организации), то тема дипломного проекта разрабатывается на основании технического задания заказчика;

– студенту предоставляется право выбора темы дипломного проекта, в том числе предложения своей тематики с необходимым обоснованием целесообразности ее разработки для практического применения;

– после согласования тематики дипломного проекта приказом директора проходит утверждение и закрепление за студентами темы дипломного проекта (с указанием сроков исполнения) и назначении руководителей дипломного проекта из числа работников отраслевых предприятий и организаций, ведущих преподавателей кафедры экономики и информационных дисциплин, а также консультантов по разделам дипломного проекта и проведения нормоконтроля не позднее 01 марта 2024 года;

– требования к содержанию, объему и структуре дипломного проекта представлены в Методических указаниях по выполнению выпускных квалификационных работ по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем.

Тематика дипломных проектов представлена в таблице 2.1.

Таблица 2.1

Тематика выпускных квалификационных работ

№ п/п	Тема дипломного проекта	Общие компетенции	Профессиональные компетенции
1.	Разработка и обоснование требований и процедур по защите базы данных на предприятии (на примере …).	ОК.1-ОК.11	ПК 2.1-2.6 ПК 3.1-3.5
2.	Организация безопасного удаленного доступа к ЛВС предприятия (на примере …).	ОК.1-ОК.11	ПК 1.1-1.4
3.	Построение защищенной виртуальной сети на базе специализированного программного обеспечения на предприятии (на примере …).	ОК.1-ОК.11	ПК 2.1-2.6 ПК 1.1-1.4
4.	Обоснование и разработка требований и процедур по защите информации ограниченного доступа на предприятии (на примере …).	ОК.1-ОК.11	ПК 1.1-1.4
5.	Разработка защищенной базы данных на предприятии (на примере …).	ОК.1-ОК.11	ПК 3.1-3.5
6.	Разработка методов и форм работы с персоналом предприятия, допущенным к конфиденциальной информации (на примере …).	ОК.1-ОК.11	ПК 1.1-1.4
7.	Разработка и анализ эффективности внедрения мер по защите информации объектов, подключенных к глобальной сети (на примере …).	ОК.1-ОК.11	ПК 2.1-2.6 ПК 3.1-3.5
8.	Разработка системы защиты информации при межсетевом взаимодействии в организации (на примере …).	ОК.1-ОК.11	ПК 2.1-2.6 ПК 1.1-1.4

9.	Разработка виртуальной защищенной сети на базе программного обеспечения ViPNet (на примере …).	ОК.1-ОК.11	ПК 2.1-2.6 ПК 1.1-1.4
10.	Обоснование и разработка мероприятий по защите персональных данных сотрудников (на примере …).	ОК.1-ОК.11	ПК 2.1-2.6 ПК 3.1-3.5
11.	Разработка организационно-технических мероприятий по обеспечению безопасности функционирующей информационно-вычислительной системы (на примере …).	ОК.1-ОК.11	ПК 3.1-3.5
12.	Автоматизация учета конфиденциальных документов на предприятии (на примере …).	ОК.1-ОК.11	ПК 1.1-1.4
13.	Организация процессов мониторинга конфиденциального документооборота на предприятии (на примере …).	ОК.1-ОК.11	ПК 1.1-1.4
14.	Разработка комплексной системы защиты предприятия (на примере …).	ОК.1-ОК.11	ПК 2.1-2.6 ПК 3.1-3.5
15.	Организация системы планирования и контроля функционирования КСЗИ на предприятии (на примере …).	ОК.1-ОК.11	ПК 2.1-2.6 ПК 3.1-3.5
16.	Разработка структурно-функциональной модели управления КСЗИ предприятия (на примере …).	ОК.1-ОК.11	ПК 2.1-2.6 ПК 1.1-1.4
17.	Разработка системы программно-аппаратной защиты информации предприятия (на примере …).	ОК.1-ОК.11	ПК 2.1-2.6 ПК 1.1-1.4
18.	Разработка изолированной программно-аппаратной среды в Windows 10 (Linux) (на примере …).	ОК.1-ОК.11	ПК 2.1-2.6 ПК 1.1-1.4
19.	Методы применения антивирусных средств защиты информации (на примере ….).	ОК.1-ОК.11	ПК 2.1-2.6 ПК 1.1-1.4
20.	Организация защиты персональных данных предприятия (на примере …).	ОК.1-ОК.11	ПК 2.1-2.6 ПК 3.1-3.5
21.	Разработка рекомендаций по созданию комплексной системы защиты информации на предприятии (на примере …).	ОК.1-ОК.11	ПК 2.1-2.6 ПК 3.1-3.5
22.	Разработка комплексной системы защиты информации с разработкой подсистемы видеонаблюдения (на примере …).	ОК.1-ОК.11	ПК 3.1-3.5
23.	Разработка комплексной системы защиты информации с разработкой подсистемы охранно-пожарной системы (на примере …).	ОК.1-ОК.11	ПК 3.1-3.5
24.	Разработка комплексной системы защиты информации с разработкой подсистемы защищенной связи (на примере …).	ОК.1-ОК.11	ПК 3.1-3.5
25.	Разработка комплексной системы защиты информации с разработкой виброакустической защиты выделенного помещения (на примере …).	ОК.1-ОК.11	ПК 3.1-3.5
26.	Оценка защищенности помещения хозяйствующего субъекта от утечки речевой конфиденциальной информации по акустическому и виброакустическому каналам (на примере …).	ОК.1-ОК.11	ПК 3.1-3.5
27.	Разработка комплекса рекомендаций по технической защите конфиденциальной информации хозяйствующего субъекта (на примере …).	ОК.1-ОК.11	ПК 3.1-3.5

28.	Разработка и обоснование требований и процедур по защите конфиденциальной информации, обрабатываемой средствами вычислительной техники (на примере …).	ОК.1-ОК.11	ПК 1.1-1.4
29.	Разработка методов передачи и защиты информации в каналах связи (на примере …).	ОК.1-ОК.11	ПК 1.1-1.4
30.	Организация порядка установления внутриобъектного режима на объекте информатизации (на примере …).	ОК.1-ОК.11	ПК 3.1-3.5
31.	Обоснование и разработка требований и процедур по защите конфиденциальной информации, обрабатываемой средствами вычислительной техники и информационными системами (на примере …).	ОК.1-ОК.11	ПК 2.1-2.6
32.	Комплексная оценка защищенности помещения хозяйствующего субъекта от утечки конфиденциальной информации по техническим каналам (на примере …).	ОК.1-ОК.11	ПК 3.1-3.5
33.	Методы применения средств межсетевого экранирования (на примере …).	ОК.1-ОК.11	ПК 2.1-2.6
34.	Разработка комплекса мероприятий (рекомендаций) по защите информации, циркулирующей в защищаемых помещениях хозяйствующего субъекта (на примере …).	ОК.1-ОК.11	ПК 3.1-3.5 ПК 2.1-2.6
35.	Разработка системы программно-аппаратной защиты государственной информационной системы (на примере …).	ОК.1-ОК.11	ПК 2.1-2.6
36.	Разработка системы программно-аппаратной защиты информационной системы персональных данных (на примере …).	ОК.1-ОК.11	ПК 2.1-2.6
37.	Организация безопасного удаленного доступа в локальной вычислительной сети предприятия (на примере …).	ОК.1-ОК.11	ПК 2.1-2.6
38.	Организация процессов мониторинга конфиденциального документооборота образовательной организации (на примере …).	ОК.1-ОК.11	ПК 2.1-2.6
39.	Автоматизация процесса проверок наличия конфиденциальных документов на предприятии (на примере …).	ОК.1-ОК.11	ПК 2.1-2.6
40.	Обоснование и разработка мер организационной защиты конфиденциальной информации при взаимодействии сотрудников предприятия со сторонними организациями (на примере …).	ОК.1-ОК.11	ПК 2.1-2.6
41.	Разработка предложений по проведению аудита информационной безопасности образовательного учреждения (на примере …).	ОК.1-ОК.11	ПК 2.1-2.6

3.7. Подготовка к демонстрационному экзамену

Задания демонстрационного экзамена разрабатываются на основе профессиональных стандартов и с учетом оценочных материалов, разработанных федерального государственного бюджетного образовательного учреждения дополнительного профессионального образования Институт развития дополнительного профессионального образования.

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

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

Демонстрационный экзамен проводится с использованием комплектов оценочной документации (далее - КОД), представляющих собой комплекс требований стандартизированной формы к выполнению заданий определенного уровня, оборудованию, оснащению и застройке площадки, составу экспертных групп. В составе КОД включается демонстрационный вариант задания (образец).

Задания, по которым проводится оценка на демонстрационном экзамене, определяются методом автоматизированного выбора из банка заданий в электронной системе интернет мониторинга и доводятся до главного эксперта за 1 день до экзамена.

КОД, включая демонстрационный вариант задания, разрабатываются ежегодно не позднее 1 декабря в соответствии с требованиями и порядком, установленным ИРПО, и размещаются в специальном разделе на официальном сайте https://de.firpo.ru

Колледж обеспечивает проведение предварительного инструктажа выпускников непосредственно в месте проведения демонстрационного экзамена.

3.8. Требования к дипломному проекту и методика его оценивания

Материалы дипломного проекта формируются на основе материала и данных, полученных при прохождении производственных и преддипломной практик.

3.8.1. Структура дипломного проекта

Дипломный проект состоит из текстовой части.

Структурными элементами текстовой части дипломного проекта являются:

- титульный лист;
- задание;
- содержание;
- введение;
- теоретическая часть;
- аналитическая (практическая) часть;
- разработанные мероприятия по повышению информационной безопасности;
- заключение;
- список использованной литературы;
- приложения (в т. ч. электронная презентация);
- отзыв руководителя дипломного проекта;
- рецензия на дипломный проект.

Рекомендуемый объем текстовой части дипломного проекта – 60-70 страниц печатного текста (без приложений). Соотношение частей работы должно быть выдержано по объему. Объем приложений не ограничивается.

Дипломный проект имеет следующую структуру:

- введение (до 5% общего объема работы);
- теоретический раздел (15-20%);
- практический раздел (70-75%);
- заключение (5%);
- список использованной литературы (не менее 20 источников);
- приложения.

3.8.2. Содержание дипломного проекта

Содержание дипломного проекта определяется спецификой специальности и темой дипломного проекта.

Во введении приводится краткое обоснование актуальности выбранной темы, а также цели, задачи, объект, предмет исследования, методы и направления раскрытия темы дипломного проекта.

Теоретическая часть

Задачами теоретической части являются раскрытие понятий и сущности изучаемых явлений или процессов и обоснование на этой основе мер и методов по обеспечению защиты информации выбранного объекта.

В теоретической части на основе обзора отечественной и зарубежной литературы, достижений в области информатизации и по другим источникам обосновывается выбор применяемых методов, описывается их суть, принципы их использования. Здесь также возможно рассмотреть тенденции развития тех или иных социальных, экономических, информационных процессов на предприятии в результате реализации предлагаемых решений.

Для задач, решаемых на основе программно-аппаратной защитой информации объектов, необходимо рассмотреть модели компьютерных систем, модели безопасного взаимодействия и управления безопасностью в информационных системах, модели сетевых средств безопасности, методы декомпозиции моделей угроз, обосновать выбор методов и средств защиты информации выбранного объекта на аппаратном и/или программном уровнях.

Для задач, связанных с защитой и обработкой конфиденциальных документов, необходимо рассмотреть типовой состав технологических стадий входного, выходного и внутреннего документопотоков, провести анализ несанкционированного получения документированной информации, каналов практической реализации возможных угроз, принципов защиты документопотоков, обосновать выбор защищенной технологии и уровень ее автоматизации.

Для задач, решаемых с правовым обеспечением защиты информации на предприятиях, в телекоммуникационных и информационных сетях, организациях, а также информации, составляющих государственную, коммерческую и другие

тайны, интеллектуальную собственность, должны быть рассмотрены и проанализированы соответствующие законодательные акты, виды, условия и порядок их применения. Должен быть выбран и обоснован комплекс правовых мер и мероприятий, обеспечивающих защиту выбранного объекта.

Для задач, решаемых на основе инженерно-технической защиты информации выбранного объекта, необходимо провести анализ существующих методов, способов и средств его инженерно-технической охраны в соответствии с видами угроз, основ организации и методического обеспечения такой защиты, выбрать и обосновать комплекс организационно-распорядительных мероприятий по защите объекта.

Для задач, решаемых с использованием криптографических систем защиты объектов, необходимо обосновать выбор криптосистем, требования к ним, характеристики, режимы их применения, определить алгоритмы их реализации в виде блок-схем или пошагового описания, соответствующего языка программирования, рассмотреть модели таких систем с позиций надежности защиты и экономики.

Для задач, решаемых на основе применения организационных мер по защите информации выбранного объекта, необходимо рассмотреть совокупность нормативных и распорядительных документов, определяющих политику информационной безопасности объектов, обладающих конфиденциальной информацией, принципы и задачи ограничения и разграничения доступа к такого рода информации, обосновать необходимость применения такого рода мер, разработать модель их использования.

Для решения задач комплексной защиты информации на предприятии должен быть проведен системный анализ основ защиты информации, должны быть рассмотрены модели комплексной системы защиты информации (КСЗИ): функциональная, информационная, организационная, потенциального нарушителя, на основе которых может быть определен технический и/или рабочий проект организации КСЗИ с технико-экономическим обоснованием. Указанное обоснование необходимо представить в виде аналитического описания или в виде алгоритмической интерпретации. Могут быть описаны средства, обеспечивающие функционирование КСЗИ с учетом различных ситуаций.

Теоретическая часть должна заканчиваться выводами по рассмотренным вопросам с обоснованием решений по главным направлениям работы.

Практическая часть

Задачей практической части ВКР является реализация и описание предложенных разработок в рамках выбранной темы и с учетом специфики конкретного объекта и аспектов исследования, подходов, методов и средств решения конкретных задач.

В рамках разработок могут включаться задачи совершенствования (улучшения) существующих систем обеспечения безопасности выбранного объекта. При этом на основе принятых проектных предложений следует определить и указать в работе имеющиеся системы защиты информации, указать их конкретную конфигурацию, схему применения и дополнить комплексом мер, улучшающим безопасность объекта.

Практическая часть должна содержать материал, соответствующий исключительно конкретным особенностям объекта и задачам разработки. В соответствии с поставленными задачами могут быть представлены:

- модели безопасности объектов;
- алгоритмы решения поставленных задач по защите выбранного объекта;
- схемы алгоритмов основных программных модулей, их взаимосвязи и описания;
- программные модули, их взаимосвязи и описания;
- информационные модели защищаемой информации;
- комплексы инженерно-технических средств по обеспечению безопасности объекта;
- структуры аппаратных защитных средств;
- криптографические средства и их ключи;
- правовые меры, ориентированные на защиту выбранного объекта;
- организационные меры по защите исследуемого объекта;
- комплекс организационно-технических мероприятий по внедрению предложенных в ВКР решений.

Практическую часть желательно закончить кратким перечнем основных предложенных в работе проектных решений.

В заключении делаются выводы в соответствии с задачами, которые необходимо было решить в дипломном проекте, дается оценка их выполнения, описываются возможности

внедрения результатов дипломного проекта на предприятии и необходимость дальнейшего их развития.

В приложения помещают материалы, которые носят вспомогательный, поясняющий характер или имеющие большой объем (документы, используемые в организации по рассматриваемым вопросам, тексты программ, примеры распечаток полученных результатов, табличный и иллюстративный материал по отдельным показателям или по интегрированным оценкам, которые использованы в качестве дополнительной аргументации, более подробные блок-схемы по отдельным частям разработанных программ).

В приложения следует выносить вспомогательный материал, который более детально раскрывает смысл основных разделов, но при включении его в основной текст приведет к необоснованному увеличению объема дипломного проекта. Материалы приложения должны иметь порядковые номера.

Объем приложения не лимитируется.

Требования к содержанию и оформлению дипломного проекта подробно представлены в методических указаниях по выполнению дипломного проекта для специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем.

Дипломный проект в обязательном порядке направляется на внешнюю рецензию. Внешнее рецензирование дипломного проекта проводится с целью обеспечения объективности оценки труда выпускника. Выполненные работы рецензируются специалистами по тематике дипломного проекта из государственных органов власти, сферы труда и образования, научно-исследовательских институтов и др. К рецензированию допускаются дипломные проекты, имеющие отзыв на оценку не ниже «удовлетворительно».

Рецензенты дипломного проекта определяются не позднее, чем за месяц до защиты. Рецензия содержит (Приложение 4):

– заключение о соответствии дипломного проекта заданию;

– оценку качества выполнения каждого раздела дипломного проекта;

– оценку степени разработки новых вопросов, оригинальности решений (предложений), теоретической и практической значимости работы.

В рецензии, как и в отзыве, указывается конкретная отметка, которой достойна работа (проект). Содержание рецензии доводится до сведения студента не позднее, чем за 1 день до защиты дипломного проекта.

Внесение изменений в работу после получения рецензии не допускается.

Студенту рекомендуется подготовить презентацию, выполненную с применением информационных технологий.

Выпускная квалификационная работа позволяет членам ГЭК обоснованно оценить приобретенные знания, профессиональные навыки и умения выпускников для их использования в практической деятельности.

4. Проведение государственной итоговой аттестации

4.1. Защита дипломного проекта

Заместитель директора по учебной работе после ознакомления с отзывом руководителя и рецензией решает вопрос о допуске студента к защите дипломного проекта в государственной экзаменационной комиссии.

Студент, получивший допуск к защите, должен подготовить доклад (5-7 минут), в котором четко и кратко изложить положения дипломного проекта, оформляет наглядные пособия, готовит свое выступление в форме презентации, продумывает ответы на замечания рецензента. Он должен не только написать высококачественную работу, но и уметь защитить ее, т.к. иногда высокая оценка руководителя снижается из-за плохой защиты.

Примерная структура доклада на защите дипломного проекта:

– представление темы дипломного проекта;
– актуальность выбранной темы;
– цель, задачи проекта, объект исследования;
– краткий обзор основного содержания дипломного проекта;
– основные выводы и рекомендации по исследуемой проблеме.

На защиту дипломного проекта каждому студенту отводится не более 45 мин.

Процедура защиты дипломного проекта:

– представление работы секретарем комиссии;
– доклад выпускника (5-7 мин);
– демонстрация модели информационной безопасности, разработанной в ходе работы над дипломным проектом;
– ответы выпускника на вопросы членов комиссии;
– представление отзыва и рецензии;
– может быть выступление руководителя выпускной квалификационной работы, а также рецензента, если они присутствуют на заседании государственной экзаменационной комиссии.

Члены ГЭК задают вопросы, как по теме дипломного проекта, так и для выявления профессиональной подготовленности студента. Защита дипломного проекта проводится на открытом заседании ГЭК согласно расписанию, утверждаемому директором колледжа.

Защита дипломного проекта проводится на открытом заседании государственной экзаменационной комиссии с участием не менее 2/3 ее состава. Ход заседания государственной экзаменационной комиссии протоколируется.

В протоколе фиксируются:

– итоговая оценка защиты дипломного проекта;
– вопросы и ответы студентов;
– особое мнение членов комиссии.

Результаты защиты дипломного проекта обсуждаются на закрытом заседании ГЭК и оцениваются простым большинством голосов членов ГЭК, участвующих в заседании, при обязательном присутствии председателя комиссии или его заместителя. При равном числе голосов мнение председателя является решающим.

Протоколы подписываются председателем, заместителем председателя, ответственным секретарем и членами комиссии.

При определении окончательной оценки дипломного проекта учитываются:

– доклад выпускника;
– ответы на вопросы;
– оценка рецензента;
– отзыв руководителя.

Результаты защиты дипломного проекта (определяются оценками «отлично», «хорошо», «удовлетворительно», «неудовлетворительно») и решение о присвоении квалификации по специальности объявляются в тот же день.

Результаты защиты дипломного проекта объявляются в тот же день после оформления в установленном порядке протоколов заседаний ГЭК.

4.2. Процедура проведения демонстрационного экзамена

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

Деятельность ГЭК осуществляется в следующем порядке:

Председатели комиссий организуют и контролируют их деятельность, обеспечивают единство требований, предъявляемых к студентам при проведении ГИА, рассмотрении апелляций, проводят заседания комиссий. Заместитель председателя ГЭК исполняет его обязанности в его отсутствие.

Протоколы заседаний комиссий ведут секретари комиссий. Секретарь ГЭК представляет необходимые материалы в апелляционную комиссию.

Протокол заседания ГЭК подписываются председателем ГЭК (в случае отсутствия председателя — его заместителем), членами комиссии и секретарем ГЭК.

Процедура оценивания результатов выполнения заданий демонстрационного экзамена осуществляется членами экспертной группы по 100-балльной системе в соответствии с требованиями комплекта оценочной документации.

Перевод баллов в оценки осуществляется на основе таблицы:

Оценка ГИА	«2»	«3»	«4»	«5»
Отношение полученного количества баллов к максимально возможному (в процентах)	0,00%-10,79%	10,80%-21,59%	21,60%-37,79%	37,80%-54,00%

Баллы выставляются в протоколе проведения демонстрационного экзамена, который подписывается каждым членом экспертной группы и утверждается главным экспертом после завершения экзамена для экзаменационной группы.

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

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

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

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

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

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

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

В случае отсутствия на аттестационном испытании по уважительной причине студент или его законный представитель должен проинформировать структурное подразделение о причине отсутствия до выставления ГЭК оценок по результатам аттестационного испытания и представить в соответствующее структурное подразделение оригинал документа, подтверждающий причину его отсутствия на аттестационном испытании, в течение 3 дней с момента получения такого документа. В случае невозможности предоставления оригинала документа в установленный срок, может быть предоставлена его копия, в том числе

электронная, с последующим предоставлением оригинала до истечения установленного срока обучения.

Лицам, не проходившим ГИА по уважительной причине, предоставляется возможность пройти ГИА без отчисления из Колледжа.

Дополнительные заседания ГЭК организуются в установленные структурным подразделением сроки, но не позднее четырех месяцев после подачи заявления лицом, не проходившим ГИА по уважительной причине (примерная форма заявления приведена в Приложении № 3 к Положению о проведении государственной итоговой аттестации по образовательным программам среднего профессионального образования).

Студент, не прошедший аттестационное испытание по уважительной причине, допускается к сдаче следующего аттестационного испытания (при его наличии).

Выпускники, не прошедшие ГИА по неуважительной причине, в том числе не явившиеся для прохождения ГИА без уважительных причин (далее - выпускники, не прошедшие ГИА по неуважительной причине), и выпускники, получившие на ГИА неудовлетворительные результаты, могут быть допущены Колледжем для повторного участия в ГИА не более двух раз (примерная форма заявления приведена в Приложении № 4 к Положению о проведении государственной итоговой аттестации по образовательным программам среднего профессионального образования).

Выпускники, не прошедшие ГИА по неуважительной причине, и выпускники, получившие на ГИА неудовлетворительные результаты, отчисляются из Колледжа и проходят ГИА не ранее чем через шесть месяцев после прохождения ГИА впервые.

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

График проведения (даты начала и окончания) ГИА определяется календарным учебным графиком.

Для проведения ГИА заинтересованными кафедрами готовится программа ГИА.

Программа ГИА, включая методику оценивания результатов, требования к дипломным проектам, задания и продолжительность государственных экзаменов определяются с учетом примерной основной образовательной программы СПО и утверждаются после их обсуждения на заседании педагогического совета с участием председателей ГЭК.

Программа ГИА размещается на официальном сайте Колледжа в информационно-телекоммуникационной сети «Интернет» (далее — официальный сайт Колледжа). Программа ГИА доводится до сведения студентов, не позднее чем за шесть месяцев до начала ГИА.

Расписание аттестационных испытаний (далее расписание) утверждается распоряжением уполномоченного руководителя структурного подразделения и не позднее, чем за 30 календарных дней до начала ГИА доводится до сведения студентов, председателей, заместителей председателей (для ГЭК), членов и секретарей ГЭК и апелляционной комиссии, а также руководителей ВКР посредством размещения на официальном сайте Колледжа и на информационном стенде. В расписании указываются виды аттестационных испытаний, форма проведения государственного экзамена, даты, время проведения аттестационных испытаний.

4.3. Распределение баллов по критериям оценивания

Распределение баллов по критериям оценивания для ДЭ ПУ (инвариантная часть КОД) в рамках ГИА представлена в таблице 4.1.

Общее максимально возможное количество баллов задания по всем критериям оценки составляет 80.

Таблица 4.1

№ п/п	**Модуль задания** (вид деятельности, вид профессиональной деятельности)	**Критерий оценивания**	**Баллы**
1.	Эксплуатация автоматизированных (информационных) систем в защищенном исполнении	Администрирование программных и программно-аппаратных компонентов автоматизированной (информационной) системы в защищенном исполнении	4,00
		Использование информационных технологий в профессиональной деятельности	2,00
2.	Защита информации в автоматизированных системах программными и программно-аппаратными средствами	Осуществление установки и настройки отдельных программных, программно-аппаратных средств защиты информации	6,00
		Обеспечение защиты информации в автоматизированных системах отдельными программными, программно-аппаратными средствами	12,00
		Осуществление тестирования функций отдельных программных и программно-аппаратных средств защиты информации	2,00
3.	Эксплуатация автоматизированных (информационных) систем в защищенном исполнении	Производство установки и настройки компонентов автоматизированных (информационных) систем в защищенном исполнении в соответствии с требованиями эксплуатационной документации	4,00
		Администрирование программных и программно-аппаратных компонентов автоматизированной (информационной) системы в защищенном исполнении	6,00
		Осуществление проверки технического состояния, технического обслуживания и текущего ремонта, устранение отказов и восстановление работоспособности автоматизированных (информационных) систем в защищенном исполнении	10,00
4.	Защита информации в автоматизированных системах программными и программно-аппаратными средствами	Осуществление обработки, хранения и передачи информации ограниченного доступа	4,00
5.	Эксплуатация автоматизированных (информационных) систем в защищенном исполнении	Администрирование программных и программно-аппаратных компонентов автоматизированной (информационной) системы в защищенном исполнении	3,00
		Обеспечение бесперебойной работы автоматизированных (информационных) систем в	5,00

		защищенном исполнении в соответствии с требованиями эксплуатационной документации	
6.	Защита информации в автоматизированных системах программными и программно-аппаратными средствами	Осуществление установки и настройки отдельных программных, программно-аппаратных средств защиты информации	6,00
		Осуществление тестирования функций отдельных программных и программно-аппаратных средств защиты информации	6,00
		Осуществление обработки, хранения и передачи информации ограниченного доступа	10,00
		ИТОГО (инвариативная часть)	**80,00**

4.4. Образцы задания

Модуль 1:

Эксплуатация автоматизированных (информационных) систем в защищенном исполнении

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 при помощи текстового редактора, сформировать отчет, в котором представить скриншоты ключевых настроек.

В ходе выполнения данного задания нужно установить основное ПО на рабочие станции будущей защищенной сети, задать пароли пользователей и администраторов сети.

Для правильной работы сети надо создать или убедиться в наличии 4 сетей: Host only или внутренняя сеть адаптер для сети центрального офиса Host only или внутренняя сеть адаптер для сети филиала

- Host only или внутренняя сеть адаптер для сети межсетевого взаимодействия;
- Host only адаптер, NAT или Bridge для виртуального «Интернета».

IP адреса защищенных сетей:

- Центральный офис «Сеть 1 ЦО»: 172.16.224.224/27
- Офис филиал «Сеть 1 Филиал»: 10.10.20.128/25
- Офис сеть 2 «Сеть 2 Офис»: 192.168.88.64/26
- «Интернет» для всех координаторов: 10.8.248.0/24

Адреса выбираются самостоятельно из указанного диапазона.

В связи с особенностями работы системы на различных версиях пользовательских или серверных ОС, может потребоваться установка компонентов системы вручную.

Задача 1.1 Установить SQL-сервер, входящий в комплект дистрибутивов программного комплекса, на виртуальную машину Net1-Open (незащищенный узел).

Необходимые приложения: отсутствуют.

Модуль 2:

Защита информации в автоматизированных системах программными и программно-аппаратными средствами

Задача 2.1 Развертывание ПК Administrator в качестве центра сертификации Установить и настроить рабочее место администратора (на базе виртуальной машины Net1-AdminCA (ЦО)): Центр управления сетью (серверное приложение ЦУС), Удостоверяющий и ключевой центр (УКЦ); использовать ранее установленный SQL-сервер. Установить клиент ЦУС на ВМ Net1-Open (незащищенный узел).

Задача 2.2. Инициализация VPN Coordinator и установка ПО VPN Client на виртуальной машине Net1-AdminCA (ЦО) установить ПО Client (Пользовательская или серверная ОС), рабочее место администратора, на виртуальной машине Net1-Coord (ЦО) инициализировать Coordinator HW-VA. Задача 2.3. Инициализация VPN Coordinator и установка ПО VPN Client для организации сети филиала

На виртуальной машине Net2-Coord (филиал) инициализировать Coordinator HW-VA, на виртуальной машине Net2-Client (филиал) установить ПО Client, рабочее место пользователя. В отчете необходимо зафиксировать процесс установки скриншотами форм.

Задача 2.4 Развертывание удостоверяющего центра в составе защищенной 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.

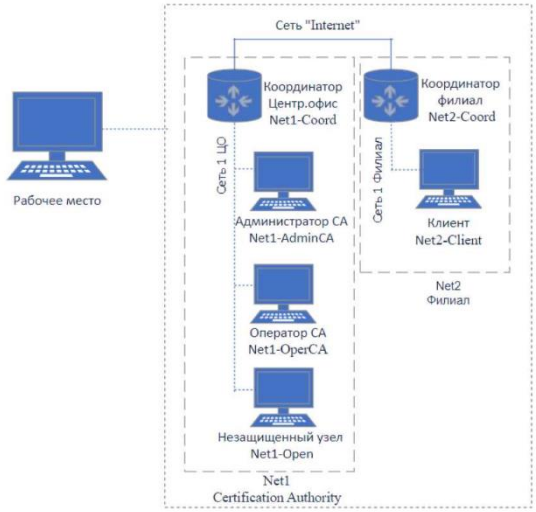


Рис. 1. Схема защищенности сети

В итоге выполнения задания должны быть развернуты и настроены следующие сетевые узлы защищенной сети (таблица 1).

Задача 2.5 Создание структуры защищенной сети

Необходимо создать в ЦУС структуру защищенной сети в соответствии с заданной схемой, представленной на рисунке 1. Создать пользователей узлов, настроить полномочия пользователей и их связи в соответствии со схемой связей, представленной в таблице 2.

Таблица 1 - Узлы защищенной сети

Вирт. машина	Название сетевого узла	ПО	ОС сетевого узла	Имя пользователя сетевого узла, уровень полномочий
Netl-AdminCA (ЦО)	Администратор ИБ	Administrator (ЦУС сервер, УКЦ), Client, CA Informing	Пользовательская или серверная ОС	AdminS
Netl-CoordCA (ЦО)	Корневой координатор	Coordinator	HW-VA	Root_ Coordinator

Netl-OperCA (ЦО)	Узел ЦР	Client, Publication Service, Registration Point	Пользовательская или серверная ОС	Node_CR
Net2-Coord (Филиал)	Подчиненный координатор	Coordinator	HW-VA	Sub_Coordinator
Net2-Client (филиал)	Удаленный клиент	Client	Пользовательская или серверная	Rem_Client

Таблица 2 - Схема связей пользователей

Пользователь	Root_ Coordinator	AdminS	Node_CR	Sub_Coordinator	Rem_Client
Root_Coordinator	X	*	*	*	
AdminS	*	X	*		*
Node_CR	*	*	X	*	
Sub_Coordinator	*		*	X	*
Rem_Client		*		*	X

Провести инициализацию УКЦ, сохранить контейнер ключей администратора в общей папке, поменять тип паролей для пользователей («собственный»). Сформировать дистрибутивы ключей для всех сетевых узлов. Разнести дистрибутивы ключей по АРМ, провести первичную инициализацию узлов защищенной сети, проверить доступность узлов защищенной сети и сделать скриншоты работоспособности узлов.

Задача 2.6 Отправить письмо по Деловой почте пользователю Rem_Client с узла AdminS, отправить текстовое сообщение пользователю AdminS от пользователя Rem_Client. В отчете необходимо представить скриншоты текстового сообщения и деловой почты на отправителе и получателе (при отправке письма), а также скриншоты журнала IP-пакетов на координаторах, подтверждающие прохождение письма через координаторы.

Необходимые приложения: отсутствуют.

Модуль 1:

Эксплуатация автоматизированных (информационных) систем в защищенном исполнении

Задача 1.2 Установка центра регистрации, сервиса публикации и сервиса информирования Certification Authority на соответствующие виртуальные машины

На виртуальной машине Net1-OperCA (ЦО) установить ПО Client, Сервис публикации. На виртуальной машине Net1-OperCA (ЦО) установить ПО Центр регистрации. На виртуальной машине Net1-AdminCA (ЦО) установить ПО Сервис информирования.

Модуль № 1:

Эксплуатация автоматизированных (информационных) систем в защищенном исполнении

Задача 1.3 Настройка работы удостоверяющего центра в аккредитованном режиме

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

После перевода УКЦ в аккредитованный режим необходимо выпустить:

- корневой квалифицированный сертификат, назначить текущим,
- квалифицированную электронную подпись для пользователя AdminS, выдать с новым дистрибутивом ключей,
- квалифицированную электронную подпись для пользователя Rem_Client, сохранить электронные ключи в файл.

Создать квалифицированные ключи ЭП и ключи проверки ЭП для пользователей сети. Настроить схему обмена файлами между УКЦ посредством Сервиса Публикации. Настроить переход в автоматический режим: передачу на публикацию и обновление CRL с периодичностью 1 день. Реализовать автоматическую публикацию сертификатов издателей на FTP- сервере.

Посредством Центра Регистрации: зарегистрировать пользователя Rem_Client, отправить запрос в УКЦ на выпуск сертификата, удовлетворить запрос. Отправить запрос в УКЦ на аннулирование ранее выпущенного сертификата, удовлетворить запрос.

Посредством Сервиса Информирования настроить способ выдачи уведомлений, сформировать отчет о выданных за текущие сутки сертификатах.

Задача 1.4. Компрометация пользователя

Произвести компрометацию ключей и восстановление сетевого взаимодействия средствами УКЦ/ЦУС: скомпрометировать ключи пользователя Rem_Client на узле Удаленный клиент, произвести смену ключей пользователя и сетевых узлов, отправить обновления и произвести процедуру смены ключа пользователя на узле Удаленный клиент, проверить работу защищенной сети после обновления отправив сообщение от пользователя Rem_Client администратору. В отчете необходимо зафиксировать процесс настройки скриншотами.

Задача 1.5 Настроить агрегированный канал связи (интерфейс) на Net2-Coord в сторону внешней сети Inet (задействовать eth0 и eth1). Применить режим, который используется для балансировки нагрузки на подчиненных физических интерфейсах и защищает от сбоев (преимущественно применим в сетях с простой топологией).

Необходимые приложения: отсутствуют.

Модуль № 2:

Защита информации в автоматизированных системах программными и программно-аппаратными средствами.

Задача 2.7. Реализовать межсетевое взаимодействие защищённых сетей (со связями «все со всеми»), развернув на виртуальной машине Net3-Admin рабочее место Администратора партнёрской сети.

Схема межсетевого взаимодействия представлена на рисунке 2.

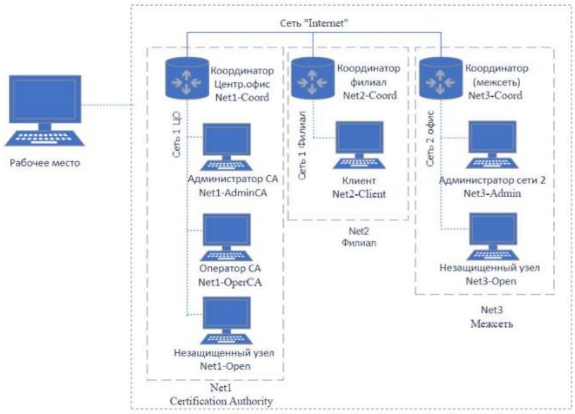


Рис. 2. Схема межсетевого взаимодействия

Создать структуру второй сети: рабочее место администратора на виртуальной машине Net3-Admin (БД, ЦУС, УКЦ, Client), координатор (Net3-Coord-HW- VA). Установить и настроить необходимое ПО. Настроить межсетевое взаимодействие, с использованием ассиметричных межсетевых ключей, между двумя защищёнными сетями, сделать скриншоты всех этапов установки межсетевого взаимодействия. Проверить взаимодействие узлов, отправив сообщение чата и деловой почты с узла Администратор сети (Net1- AdminCA) на Admin (Net3-Admin).

Необходимые приложения: отсутствуют.

4.5. Порядок проведения демонстрационного экзамена

Подготовительный этап

Регистрация студентов, информирование о сроках и порядке проведения демонстрационного экзамена осуществляется центром проведения демонстрационного экзамена (ЦПДЭ).

ЦПДЭ организует регистрацию всех заявленных студентов в системе, а также обеспечивает заполнение всеми студентами личных профилей не позднее, чем за два месяца до начала экзамена. При этом обработка и хранение персональных данных осуществляется в соответствии с Федеральным законом от 27.07.2006 года №152-ФЗ «О персональных данных».

За день до начала ДЭ:

– осуществляется распределение рабочих мест студентов на площадке в соответствии с жеребьевкой. Жеребьевка проводится в присутствии всех студентов способом, исключающим спланированное распределение рабочих мест или оборудования. Итоги жеребьевки фиксируются отдельным документом;

– техническим экспертом проводится инструктаж по охране труда и технике безопасности (далее - ОТ и ТБ) для студентов и членов Экспертной группы под роспись. В случае отсутствия студента на инструктаже по ОТ и ТБ, он не допускается к ДЭ;

– студентам предоставляется время 10 минут для ознакомления с рабочим местом, проверки инструментов, ознакомления с оборудованием;

– студенты информируются о регламенте проведения экзамена с обозначением обеденных перерывов и времени завершения экзаменационных заданий/модулей, ограничениях времени и условий допуска к рабочим местам, включая условия, разрешающие студентам покинуть рабочие места и площадку, информацию о времени и способе проверки оборудования, информацию о пунктах и графике питания, оказании медицинской помощи, о характере и диапазоне санкций, которые могут последовать в случае нарушения регламента проведения экзамена.

Проведение экзамена

Студент в день сдачи демонстрационного экзамена должен иметь при себе студенческий билет, паспорт и полис ОМС.

К демонстрационному экзамену допускаются студенты, прошедшие инструктаж по ОТ и ТБ, а также ознакомившиеся с рабочими местами. Экзаменационные задания на каждый модуль выдаются студентам непосредственно перед началом экзамена. На изучение материалов и дополнительные вопросы выделяется время, которое не включается в общее время проведения экзамена. Минимальное время, отводимое на ознакомление с информацией, составляет 15 минут, которые не входят в общее время проведения экзамена. Ознакомление происходит перед началом каждого модуля. По завершению процедуры ознакомления с заданием экзаменуемые подписывают протокол, форма которого устанавливается ИРПО.

К выполнению экзаменационных заданий студенты приступают после указания Главного эксперта. В случае опоздания к началу выполнения заданий по уважительной причине, студент допускается, но время на выполнение заданий не добавляется. В ходе

проведения экзамена студентам запрещаются контакты с другими студентами или членами Экспертной группы без разрешения Главного эксперта.

В случае возникновения несчастного случая или болезни экзаменуемого Главным экспертом незамедлительно принимаются действия по привлечению ответственных лиц от ЦПДЭ для оказания медицинской помощи. В случае отстранения экзаменуемого от дальнейшего участия в экзамене ввиду болезни или несчастного случая, ему начисляются баллы за любую завершенную работу.

В случае поломки оборудования и его замены (не по вине студента) студенту предоставляется дополнительное время. Факт несоблюдения студентом указаний или инструкций по ОТ и ТБ влияет на итоговую оценку результата ДЭ. Постоянное нарушение норм безопасности может привести к временному или окончательному отстранению участника от выполнения экзаменационных заданий. В случае возникновения несчастного случая или болезни участника, об этом немедленно уведомляется Главный эксперт, которым, при необходимости, принимается решение о назначении дополнительного времени для участника.

В случае отстранения участника от дальнейшего участия в экзамене ввиду болезни или несчастного случая, ему начисляются баллы за любую завершенную работу. При этом, ЦПДЭ должны быть предприняты все меры к тому, чтобы способствовать возвращению участника к процедуре сдачи экзамена и к компенсированию потерянного времени.

Вышеуказанные случаи подлежат обязательной регистрации в установленном порядке. Все вопросы по студентам, обвиняемым в нечестном поведении или чье поведение мешает процедуре проведения экзамена, передаются Главному эксперту и рассматриваются Экспертной группой с привлечением председателя апелляционной комиссии.

Процедура проведения демонстрационного экзамена проходит с соблюдением принципов честности, справедливости и информационной открытости. Вся информация и инструкции по выполнению экзамена от членов Экспертной группы, в том числе с целью оказания необходимой помощи, должны быть четкими и недвусмысленными, не дающими преимущества тому или иному студенту. Вмешательство иных лиц, которое может помешать студентам завершить экзаменационное задание, не допускается.

5. Оценивание результатов ГИА

5.1. Критерии оценки текста дипломного проекта

Критерии оценки текста дипломного проекта:

– актуальность и новизна темы;

– практическая значимость дипломного проекта;

– соотнесенность цели и задач, поставленных в проекте, с полученными результатами и выводами;

– профессиональная компетентность, умение систематизировать и обобщать факты, самостоятельно решать поставленные задачи (в том числе и нестандартные) с использованием передовых научно-правовых практик;

– структура проекта и культура его оформления; последовательность и логичность, завершенность изложения, наличие научно-справочного аппарата, стиль изложения;

– достоверность и объективность результатов дипломного проекта, использование в работе научных достижений отечественных и зарубежных исследователей, собственных исследований и реального опыта; логические аргументы; апробация в среде специалистов-практиков, преподавателей, исследователей и т.п.;

– достаточность и актуальность использованной литературы;

– обоснованность привлечения тех или иных методов решения поставленных задач;

– глубина и обоснованность анализа и интерпретации полученных результатов;

– соответствие оформления дипломного проекта требованиям ГОСТ 7.32—2017 и методическим рекомендациям по оформлению дипломного проекта.

При оценке дипломного проекта дополнительно учитывается качество сообщения, отражающего основное содержание дипломного проекта, и ответы выпускника на вопросы, заданные как по теме дипломного проекта, так и из сферы его будущей профессиональной деятельности.

5.2. Критерии оценки защиты дипломного проекта

Критерии оценки защиты дипломного проекта:

– четкость и внятность доклада, отражающего актуальность, новизну, цель, задачи, краткое содержание, основные выводы и результаты проекта;

– четкость, внятность, глубина ответов на вопросы членов ГЭК и присутствующих на защите;

– обоснованность, логичность, глубина ответов на замечания, содержащиеся в рецензии;

– использование технических средств, сопровождающих доклад.

При определении окончательной оценки учитываются материалы портфолио выпускника, характеризующие уровень освоенности профессиональных и общих компетенций.

Итоговая оценка сформированности общих и профессиональных компетенций при выполнении и защите дипломного проекта выпускников по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем выставляется по результатам выполнения (оценка руководителя и рецензента) и публичной защиты дипломного проекта.

5.3. Итоговая оценка сформированности общих и профессиональных компетенций при выполнении и защите дипломного проекта выпускников по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем

Итоговая оценка определяются оценками «отлично», «хорошо», «удовлетворительно», «неудовлетворительно».

Оценка «Отлично» выставляется за дипломный проект, который соответствует следующим требованиям:

– проект по тематике актуален и соответствует одному из профессиональных модулей, выполнен студентом самостоятельно;

– разработанная модель безопасности по тематике проекта, актуальна и может быть применена на предприятии или в организации;

– по своему стилистическому содержанию, форме и объему проекта соответствует требованиям методических рекомендаций;

– выполнена презентация для защиты дипломного проекта с использованием информационных технологий;

– студент свободно оперирует данными исследования;

– выступление студента при защите и ответы на вопросы и критические замечания проведены в полном объеме;

– отзыв на дипломный проект содержит минимальные замечания и отмечен оценкой «отлично»;

– рецензия на дипломный проект содержит минимальные замечания и отмечен оценкой «отлично»;

– при защите студент демонстрирует высокий уровень освоения общих и профессиональных компетенций;

– портфолио выпускника содержит материалы, которые свидетельствуют об уровне и качестве освоения профессиональных и общих компетенций.

Оценка «Хорошо» выставляется в случае, если:

– проект актуален, выполнен самостоятельно;

– разработанная модель безопасности по тематике проекта актуальна и может быть применена на предприятии или в организации;

– по своему стилистическому содержанию, форме и объему проект соответствует требованиям методических рекомендаций;

– выпускник показывает знания вопросов темы, оперирует данными исследования;

– выполнена презентация для дипломного проекта с использованием информационных технологий;

– отзыв на дипломный проект содержит незначительные замечания и отмечен оценкой «хорошо»;

– рецензия на дипломный проект содержит незначительные замечания и отмечен оценкой «хорошо»;

– выступление студента при защите и ответы на вопросы и критические замечания проведены в недостаточно полном объеме;

– при защите студент демонстрирует хороший уровень освоения общих и профессиональных компетенций;

– портфолио выпускника содержит материалы, которые свидетельствуют об уровне и качестве освоения профессиональных и общих компетенций.

Оценка «Удовлетворительно» выставляется в случае, если:

– проект соответствует заявленной теме;

– разработанная модель безопасности по тематике проекта актуальна, но имеет ряд замечаний и с поправками может быть применена на предприятии или в организации;

– по своему стилистическому содержанию, объему и форме проект не соответствует требованиям методических рекомендаций;

– студент проявляет неуверенность, показывает слабое знание вопросов темы;

– отзыв на дипломный проект содержит значительные замечания и отмечен оценкой «удовлетворительно»;

– рецензия на дипломный проект содержит значительные замечания и отмечен оценкой «удовлетворительно»;

– выступление студента при защите и ответы на вопросы и критические замечания слабые, не в полном объеме.

– при защите студент демонстрирует средний уровень освоения общих и профессиональных компетенций;

– портфолио выпускника содержит недостаточное количество материалов, которые свидетельствуют об уровне и качестве освоения профессиональных и общих компетенций.

Оценка «Неудовлетворительно» выставляется в том случае, если:

– содержание дипломного проекта не соответствует теме;

– не разработана модель безопасности по тематике проекта или разработана с критическими замечаниями, не позволяющими рекомендовать ее для применения на предприятии или в организации;

– не носит исследовательского характера;

– предложения автора четко не сформулированы;

– в отзывах руководителя и рецензента имеются существенные критические замечания;

– при защите дипломного проекта студент не смог сделать доклад по защите проекта, не ответил на поставленные вопросы по теме проекта, не знает теории вопроса, при ответе допускает существенные ошибки;

– портфолио выпускника содержит материалы, которые свидетельствуют о низком уровне и качестве освоения профессиональных и общих компетенций.

5.4. Оформление результатов демонстрационного экзамена

Оформление результатов экзамена осуществляется в соответствии с порядком, принятым Федеральным государственным бюджетным образовательным учреждением дополнительного профессионального образования Институт развития дополнительного профессионального образования. Баллы, выставленные членами Экспертной группы, переносятся из рукописных оценочных ведомостей в систему CIS по мере осуществления процедуры оценки. После выставления баллов во все оценочные ведомости, запись о выставленных баллах в системе CIS блокируется.

Результатом работы Экспертной комиссии является итоговый протокол заседания Экспертной комиссии, в котором указывается общий список студентов, сумма баллов по каждому студенту за выполненное задание экзамена, все необходимые бланки и формы формируются через систему CIS.

Формирование итогового документа о результатах выполнения экзаменационных заданий по каждому студенту выполняется автоматизировано с использованием систем CIS и цифровой платформы. Посредством указанных сервисов осуществляется автоматизированная обработка внесенных баллов, синхронизация с персональными данными, содержащимися в личных профилях студентов, и формируется электронный файл по каждому студенту, прошедшему демонстрационный экзамен в виде таблицы с указанием результатов экзаменационных заданий в разрезе выполненных модулей.

Студент может ознакомиться с результатами выполненных экзаменационных заданий в личном профиле на цифровой платформе. Также, право доступа к результатам экзамена может быть предоставлено предприятиям партнерам ИРПО в соответствии с подписанными соглашениями с соблюдением норм федерального законодательства о защите персональных данных.

5.5. Показатели и критерии оценивания компетенций по результатам сдачи демонстрационного экзамена, шкалы их оценивания

Оценка за демонстрационный экзамен выставляется в соответствии с утвержденными критериями. Баллы за выполнение заданий демонстрационного экзамена выставляются в соответствии со схемой начисления баллов, приведенной в комплекте оценочной документации.

Уровни сформированности компетенций по бальной шкале необходимо осуществить перевод полученного количества баллов в оценки «отлично», «хорошо», «удовлетворительно», «неудовлетворительно». Итоговая оценка за демонстрационный экзамен выставляется по традиционной системе оценивания в соответствии с таблицей.

Максимальное количество баллов, которое возможно получить за выполнение задания демонстрационного экзамена, принимается за 100%.

Таблица 4

Перевод баллов в оценку

Оценка ГИА	«2»	«3»	«4»	«5»
Отношение полученного количества баллов к	0,00%-10,79%	10,80%-21,59%	21,60%-37,79%	37,80%-54,00%

максимально возможному (в процентах)				

5.6. Методика перевода результатов демонстрационного экзамена в оценку

Решение государственной экзаменационной комиссии принимается на закрытом заседании простым большинством голосов членов комиссии, участвующих в заседании, при обязательном присутствии председателя комиссии или его заместителя. При равном числе голосов голос председательствующего на заседании государственной экзаменационной комиссии является решающим.

Результаты государственной итоговой аттестации в виде демонстрационного экзамена определяются оценками «отлично», «хорошо», «удовлетворительно», «неудовлетворительно» и объявляются в тот же день после оформления в установленном порядке протоколов заседаний государственных экзаменационных комиссий.

Баллы за выполнение заданий демонстрационного экзамена выставляются в соответствии со схемой начисления баллов, приведенной в комплекте оценочной документации.

Необходимо осуществить перевод полученного количества баллов в оценки «отлично», «хорошо», «удовлетворительно», «неудовлетворительно».

Перевод полученного количества баллов в оценки осуществляется государственной экзаменационной комиссией с обязательным участием главного эксперта.

6. Порядок подачи и рассмотрения апелляций

По результатам ГИА выпускник, участвовавший в ГИА, имеет право подать письменное апелляционное заявление о нарушении, по его мнению, установленного порядка проведения ГИА, в том числе дистанционно, и (или) несогласии с ее результатами (далее - апелляция).

Апелляция подается лично выпускником или родителями (законными представителями) несовершеннолетнего выпускника в апелляционную комиссию образовательной организации.

Апелляция о нарушении Положения подается непосредственно в день проведения ГИА, в том числе до выхода из центра проведения экзамена.

Апелляция о несогласии с результатами ГИА подается не позднее следующего рабочего дня после объявления результатов ГИА.

Апелляция рассматривается апелляционной комиссией не позднее трех рабочих дней с момента ее поступления.

Результаты рассмотрения апелляции оформляются протоколом.

Состав апелляционной комиссии утверждается Колледжем 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 Колледжа, 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 при себе иметь документы, удостоверяющие личность.

Рассмотрение апелляции не является пересдачей ГИА.

При рассмотрении апелляции о нарушении Положения апелляционная комиссия устанавливает достоверность изложенных в ней сведений и выносит одно из следующих решений:

– об отклонении апелляции, если изложенные в ней сведения о нарушениях Положения не подтвердились и (или) не повлияли на результат ГИА;

– об удовлетворении апелляции, если изложенные в ней сведения о допущенных нарушениях Положения 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 Колледжем без отчисления такого выпускника из Колледжа в срок не более четырех месяцев после подачи апелляции.

В случае 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).

В случае рассмотрения апелляции о несогласии с результатами ГИА, полученными при защите дипломного проекта, секретарь ГЭК не позднее следующего рабочего дня с момента поступления апелляции направляет в апелляционную комиссию дипломный проект, 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 Колледжа.

7. Оценивание результатов ГИА Особенности проведения ГИА для выпускников из числа лиц с ограниченными возможностями здоровья, детей-инвалидов и инвалидов

Для выпускников из числа лиц с ограниченными возможностями здоровья и выпускников из числа детей-инвалидов и инвалидов проводится ГИА с учетом особенностей психофизического развития, индивидуальных возможностей и состояния здоровья таких выпускников (далее - индивидуальные особенности).

При проведении ГИА обеспечивается соблюдение следующих общих требований:

– проведение ГИА для выпускников с ограниченными возможностями здоровья, выпускников из числа детей-инвалидов и инвалидов в одной аудитории совместно с выпускниками, не имеющими ограниченных возможностей здоровья, если это не создает трудностей для выпускников при прохождении ГИА;

– присутствие в аудитории, центре проведения экзамена тьютора, ассистента, оказывающих выпускникам необходимую техническую помощь с учетом их индивидуальных особенностей (занять рабочее место, передвигаться, прочитать и оформить задание, общаться с членами ГЭК, членами экспертной группы);

– пользование необходимыми выпускникам техническими средствами при прохождении ГИА с учетом их индивидуальных особенностей;

– обеспечение возможности беспрепятственного доступа выпускников в аудитории, туалетные и другие помещения, а также их пребывания в указанных помещениях (наличие пандусов, поручней, расширенных дверных проемов, при отсутствии лифтов аудитория должна располагаться на первом этаже, наличие специальных кресел и других приспособлений).

Дополнительно при проведении ГИА обеспечивается соблюдение следующих требований в зависимости от категорий выпускников с ограниченными возможностями здоровья, выпускников из числа детей-инвалидов и инвалидов:

а) для слепых:

– задания для выполнения, а также инструкция о порядке ГИА, комплект оценочной документации, задания демонстрационного экзамена оформляются рельефно-точечным шрифтом по системе Брайля или в виде электронного документа, доступного с помощью компьютера со специализированным программным обеспечением для слепых, или зачитываются ассистентом;

– письменные задания выполняются на бумаге рельефно-точечным шрифтом по системе Брайля или на компьютере со специализированным программным обеспечением для слепых, или надиктовываются ассистенту;

– выпускникам для выполнения задания при необходимости предоставляется комплект письменных принадлежностей и бумага для письма рельефно-точечным шрифтом Брайля, компьютер со специализированным программным обеспечением для слепых;

б) для слабовидящих:

– обеспечивается индивидуальное равномерное освещение не менее 300 люкс;

– выпускникам для выполнения задания при необходимости предоставляется увеличивающее устройство;

– задания для выполнения, а также инструкция о порядке проведения государственной аттестации оформляются увеличенным шрифтом;

в) для глухих и слабослышащих, с тяжелыми нарушениями речи:

– обеспечивается наличие звукоусиливающей аппаратуры коллективного пользования, при необходимости предоставляется звукоусиливающая аппаратура индивидуального пользования;

– по их желанию государственный экзамен может проводиться в письменной форме;

г) для лиц с нарушениями опорно-двигательного аппарата (с тяжелыми нарушениями двигательных функций верхних конечностей или отсутствием верхних конечностей):

– письменные задания выполняются на компьютере со специализированным программным обеспечением или надиктовываются ассистенту;

– по их желанию государственный экзамен может проводиться в устной форме;

д) также для выпускников из числа лиц с ограниченными возможностями здоровья и выпускников из числа детей-инвалидов и инвалидов создаются иные специальные условия проведения ГИА в соответствии с рекомендациями психолого-медико-педагогической комиссии (далее - ПМПК), справкой, подтверждающей факт установления инвалидности, выданной федеральным государственным учреждением медико-социальной экспертизы (далее - справка).

Выпускники или родители (законные представители) несовершеннолетних выпускников не позднее чем за 3 месяца до начала ГИА подают в образовательную организацию письменное заявление о необходимости создания для них специальных условий при проведении ГИА с приложением копии рекомендаций ПМПК, а дети-инвалиды, инвалиды - оригинала или заверенной копии справки, а также копии рекомендаций ПМПК при наличии.

8. Материально-техническое обеспечение ГИА

Для защиты дипломного проекта отводится специально подготовленный кабинет.

Оснащение кабинета для защиты дипломного проекта:

– рабочее место для членов государственной экзаменационной комиссии;

– компьютер, мультимедийный проектор, экран;

– лицензионное программное обеспечение общего и специального назначения.

Оснащение кабинета для защиты дипломного проекта в виде демонстрационного экзамена согласно инфраструктурного листа в оценочной документации.

9. Хранение дипломных проектов

Выполненные дипломные проекты хранятся после их защиты в архиве Колледжа. Срок хранения определяется в соответствии с номенклатурой дел Колледжа.

Списание дипломных проектов оформляется соответствующим актом.

Лучшие дипломные проекты, представляющие учебно-методическую ценность, могут быть использованы Колледжем в качестве учебных пособий в ходе ведения образовательной деятельности.

Хранение ведомостей с баллами.

10. Документы, выдаваемые по итогам аттестационных процедур

На основании решения государственной экзаменационной комиссии лицам, успешно прошедшим государственную итоговую аттестацию, выдаются документы об образовании и о квалификации.

Документом установленного образца об уровне среднего профессионального образования по профессии/специальности с присвоением квалификации по образованию является диплом о среднем профессиональном образовании.

Лицам, прошедшим процедуру демонстрационного экзамена с применением оценочных материалов, разработанных союзом, выдается паспорт компетенций (Скиллс паспорт), подтверждающий полученный результат, выраженный в баллах.

Решение ГЭК о присвоении квалификации выпускникам, прошедшим государственную итоговую аттестацию, и выдаче соответствующего документа об образовании, оформляется приказом директора колледжа.

ПРИЛОЖЕНИЕ 1

АВТОНОМНАЯ НЕКОММЕРЧЕСКАЯ ПРОФЕССИОНАЛЬНАЯ ОБРАЗОВАТЕЛЬНАЯ ОРГАНИЗАЦИЯ «УРЮПИНСКИЙ КОЛЛЕДЖ БИЗНЕСА»

Специальность _____

_____
(шифр, наименование)

Курс _____ Группа _____

ДИПЛОМНЫЙ ПРОЕКТ

Тема _____

Студент _____
(Фамилия И.О.)

Руководитель _____ _____ _____
(звание, должность) (подпись) (Фамилия И.О.)

Рецензент _____ _____ _____
(звание, должность) (подпись) (Фамилия И.О.)

Работа допущена к защите:
Заведующий кафедрой экономики и информационных дисциплин
_____
(наименование кафедры)

_____ **Мирошниченко Г.И.**
(подпись) (Фамилия И.О.)

Дата защиты «__» __июня_____ 2025 г.
Оценка _____

Урюпинск 2025

ПРИЛОЖЕНИЕ 2

СОГЛАСОВАНО
Директор …
_____Ф.И.О.
«___» _____2025 г.

УТВЕРЖДАЮ
Заместитель директора по учебной работе АНПОО
«Урюпинский колледж бизнеса»
_____ Л.А.Дьякова
«___» _____ 2025 г.

Индивидуальное задание на дипломный проект

Студента ___ курса _____ группы
специальности _____
_____
Тема дипломного проекта: _____
Исходные данные: первичная документация предприятия.

Законченный дипломный проект должен состоять из: титульного листа, задания на дипломный проект, содержания, введения, основной части, заключения, списка использованной литературы и необходимых приложений.

Текстовая часть проекта записывается на диск. Оформляется по формату, условным обозначениям, цифрам, масштабам должны соответствовать требованиям ГОСТ Р 7.0.97-2016 , ГОСТ 7.32-2017, ГОСТ 7.0.1-2003.

Все разделы дипломного проекта следует излагать по возможности кратко, чтобы размер в целом не превышал при печатном тексте 70 страниц, шрифт 14, Times New Roman.

План дипломного проекта

Примерный баланс времени при выполнении выпускником дипломного проекта (указать распределение времени по этапам выполнения в днях):
Введение - 3 дня
1. Глава 1 – 10 дней
2. Глава 2 – 10 дней
3. Глава 3 – 10 дней
Заключение - 2 дня
3. Рецензирование дипломного проекта – 5 дней.
Наименование организации (учреждения), на котором проходит преддипломную практику
Наименование предприятия
Фамилия и должность руководителя дипломного проекта
Ф.И.О. руководителя дипломного проекта, преподаватель кафедры экономики и информационных дисциплин
Дата выдачи дипломного проекта «__» ___ 20 г.
Срок окончания дипломного проекта «»_июня_ 20 г.
Рассмотрено на заседании кафедры экономики и информационных дисциплин «» _____ 20 г
Протокол №

Руководитель дипломного проекта Ф.И.О.

Заведующий кафедры экономики и информационных дисциплин Мирошниченко Г.И.

ПРИЛОЖЕНИЕ 3

АВТОНОМНАЯ НЕКОММЕРЧЕСКАЯ
ПРОФЕССИОНАЛЬНАЯ ОБРАЗОВАТЕЛЬНАЯ ОРГАНИЗАЦИЯ
«УРЮПИНСКИЙ КОЛЛЕДЖ БИЗНЕСА»

Р Е Ц Е Н З И Я
на дипломный проект

Тема _____

Студент _____
(фамилия, имя, отчество)

Специальность _____

Курса _____ Группы _____

1. Актуальность тематики дипломного проекта _____

2. Анализ содержания темы дипломного проекта _____

3. Критические замечания _____

4. Заключения о теоретическом и практическом значении выводов и предложений, возможности их внедрения в производство _____

5. Оценка соответствия дипломного проекта предъявляемым требованиям _____

Рецензент _____
(фамилия, имя, отчество, ученая степень, звание, должность, организация)

_____
(подпись рецензента, заверенная печатью)

« » июня 20__ г.

ПРИЛОЖЕНИЕ 4

АВТОНОМНАЯ НЕКОММЕРЧЕСКАЯ
ПРОФЕССИОНАЛЬНАЯ ОБРАЗОВАТЕЛЬНАЯ ОРГАНИЗАЦИЯ
«УРЮПИНСКИЙ КОЛЛЕДЖ БИЗНЕСА»

О Т З Ы В
на дипломный проект

Тема _____

_____

Студент _____
(фамилия, имя, отчество)

Специальности _____

Курса _____ Группы _____

1. Актуальность тематики дипломного проекта, его практическая значимость и новизна

_____

_____

2. Характеристика методов решения задач, представленных в проекте _____

_____

3. Анализ взаимосвязи всех разделов работ, соответствие их содержанию и степень его раскрытия _____

_____

4. Основные достоинства проекта, иллюстративность и качество его оформления

_____

5. Значимость выводов и предложений _____

_____

6. Положительные и отрицательные стороны дипломного проекта

_____

_____

7. Оценка соответствия дипломного проекта предъявляемым требованиям

_____

_____

(оценка по пятибалльной системе)

Руководитель _____
(фамилия, имя, отчество, ученая степень, звание, должность, организация)

_____
(подпись руководителя, заверенная печатью)

«__» июня 20__ г.

ПРИЛОЖЕНИЕ 5

ГРАФИК ВЫПОЛНЕНИЯ ДИПЛОМНОГО ПРОЕКТА

№ п/п	Наименование этапа написания дипломного проекта	Плановая дата	Дата выполнения	Подпись руководителя
1.	Выбор темы и подача заявления студентом.			
2.	Утверждение списка основных информационных источников. Подготовка структуры (оглавления) дипломного проекта и ее утверждение.			
3.	Подготовка текста введения дипломного проекта. Устранение замечаний, отмеченных руководителем дипломного проекта, по тексту введения.			
4.	Подготовка текста I главы дипломного проекта, согласование его с руководителем.			
5.	Устранение замечаний, отмеченных руководителем дипломного проекта, по I главе.			
6.	Разработка модели информационной безопасности по тематике дипломного проекта			
7.	Устранение замечаний, отмеченных руководителем дипломного проекта, по модели безопасности			
8.	Подготовка текста II главы дипломного проекта, согласование его с руководителем.			
9.	Устранение замечаний, отмеченных руководителем дипломного проекта, по II главе.			
10.	Подготовка содержания приложений дипломного проекта. Устранение замечаний, отмеченных руководителем дипломного проекта, по тексту приложений.			
11.	Подготовка текста заключения дипломного проекта. Устранение замечаний, отмеченных руководителем дипломного проекта, по тексту заключения.			
12.	Оформление списка основных информационных источников, используемых при написании дипломного проекта.			
13.	Предоставление руководителю полного текста дипломного проекта. Окончательное редактирование дипломного проекта.			
14.	Предоставление руководителю готового дипломного проекта (в типографском переплете).			
15.	Предоставление руководителю текста выступления на защите дипломного проекта и мультимедийной презентации.			

16.	Предварительная защита дипломного проекта.			
17.	Подготовка руководителем отзыва на дипломный проект.			
18.	Подготовка рецензии на дипломный проект и ознакомление ее содержания студентом.			
19.	Предоставление дипломного проекта заместителю директора по учебной работе для утверждения допуска к защите.			
20.	Защита дипломного проекта.			

ПРИЛОЖЕНИЕ 6

АВТОНОМНАЯ НЕКОММЕРЧЕСКАЯ
ПРОФЕССИОНАЛЬНАЯ ОБРАЗОВАТЕЛЬНАЯ ОРГАНИЗАЦИЯ
УРЮПИНСКИЙ КОЛЛЕДЖ БИЗНЕСА

ЛИСТ ОЗНАКОМЛЕНИЯ

Обучающихся группы **3Оиб11, 4Оиб9** курса **3,4**

Специальность: *10.02.05 Обеспечение информационной безопасности автоматизированных систем*

Форма обучения: очная

Год проведения государственной итоговой аттестации: 2025 г.

Настоящим подтверждается, что с Программой государственной итоговой аттестации, требованиями к дипломному проекту, критериям оценки знаний, размещёнными в электронной информационно-образовательной среде, ознакомлены следующие обучающиеся:

№ п/п	Ф.И.О. обучающегося	Дата	Подпись обучающегося
1.	Бармина Анжелика Дмитриевна		
2.	Бочаров Сергей Николаевич		
3.	Букин Денис Павлович		
4.	Бурков Артем Алексеевич		
5.	Гуськов Дмитрий Александрович		
6.	Завозин Данил Сергеевич		
7.	Иванов Роман Евгеньевич		
8.	Казьмин Вячеслав Юрьевич		
9.	Карабутов Андрей Юрьевич		
10.	Клюшин Илья Васильевич		
11.	Кобзарь Егор Денисович		
12.	Крюков Владислав Алексеевич		
13.	Кукушкин Даниил Сергеевич		
14.	Мартынов Александр Сергеевич		
15.	Мурашкин Николай Алексеевич		
16.	Поляков Кирилл Андреевич		
17.	Порублев Сергей Михайлович		
18.	Родимин Илья Вячеславович		
19.	Светличкин Кирилл Алексеевич		
20.	Сологубов Мирослав Михайлович		
21.	Сюлюков Игорь Макарович		
22.	Черноносов Данил Юрьевич		
23.	Юматов Александр Сергеевич		

Лист ознакомления составлен «13» декабря 2024 г.

Заведующий кафедрой ЭиИД Г.И. Мирошниченко