

МИНОБРНАУКИ РОССИИ

федеральное государственное бюджетное образовательное учреждение высшего образования
«Кузбасский государственный технический университет имени Т.Ф. Горбачева»

Филиал КузГТУ в г. Новокузнецке

УТВЕРЖДАЮ

заместитель директора по УР,
совмещающая обязанности директора
филиала КузГТУ в г. Новокузнецке

_____ Т.А. Евсина

«27» июня 2024 г.

Фонд оценочных средств

Итоговой аттестации

Специальность

10.02.05 Обеспечение информационной безопасности автоматизированных систем

Присваиваемая квалификация «Техник по защите информации»

Форма обучения очная

Год набора 2022

Срок обучения на базе

среднего общего образования - 2 года 10 месяцев

Новокузнецк 2024 г.

1. ПАСПОРТ ФОНДА ОЦЕНОЧНЫХ СРЕДСТВ ИТОГОВОЙ АТТЕСТАЦИИ

1.1. Область применения

Фонд оценочных средств (далее – ФОС) для проведения итоговой аттестации (далее – ИА) оценивает всю совокупность компетенций, которая установлена федеральным государственным стандартом среднего профессионального образования (далее – ФГОС СПО) для образовательной программы по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем.

Фонд оценочных средств для проведения ИА содержит:

- перечень компетенций, которыми должны овладеть обучающиеся в результате освоения образовательной программы;
- описание критериев оценивания компетенций;
- материалы, необходимые для оценки результатов освоения образовательной программы;
- методические материалы, определяющие процедуры оценивания результатов освоения образовательной программы.

1.2. Результаты, подлежащие проверке на ИА

В результате освоения образовательной программы по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем готовится к следующим видам деятельности:

1. Эксплуатация автоматизированных (информационных) систем в защищённом исполнении;
2. Защита информации в автоматизированных системах программными и программно-аппаратными средствами;
3. Защита информации техническими средствами;
4. Выполнение работ по профессии: "

В результате ИА осуществляется комплексная проверка умений и знаний, а также динамика формирования общих и профессиональных компетенций, предусмотренных ФГОС по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем.

Коды компетенций по ФГОС СПО	Компетенции	Показатели оценки результата обучения	Форма контроля
ОК 01.	Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам.	<p>иметь практический опыт:</p> <ul style="list-style-type: none"> – 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. <p>уметь:</p> <ul style="list-style-type: none"> – 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 	Защита дипломной работы
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.	<p>монтаж, осуществлять диагностику и устранять неисправности компьютерных сетей, работать с сетевыми протоколами разных уровней;</p> <ul style="list-style-type: none"> – настраивать и устранять неисправности программно-аппаратных средств защиты информации в компьютерных сетях по заданным правилам. <p>знать:</p> <ul style="list-style-type: none"> – 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. 	
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 1.4.	Осуществлять проверку технического состояния, техническое обслуживание и текущий ремонт, устранять отказы и восстанавливать работоспособность автоматизированных (информационных) систем в защищенном исполнении.		
ОК 01.	Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам.	иметь практический опыт: <ul style="list-style-type: none"> – 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. 	Защита дипломной работы
ОК 02.	Осуществлять поиск, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности.		
ОК 03.	Планировать и реализовывать собственное профессиональное и личностное развитие.		
		уметь:	

ОК 04.	Работать в коллективе и команде, эффективно взаимодействовать с коллегами, руководством, клиентами.	<ul style="list-style-type: none"> – 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. <p>знать:</p> <ul style="list-style-type: none"> – особенности и способы применения программных и программно-аппаратных средств защиты информации, в том числе, в операционных системах, компьютерных сетях, базах данных; 	
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.	<ul style="list-style-type: none"> – 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. 	
ОК 11.	Использовать знания по финансовой грамотности, планировать предпринимательскую деятельность в профессиональной сфере.		
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.		
ОК 01.	Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам.	<p>иметь практический опыт:</p> <ul style="list-style-type: none"> – 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. <p>уметь:</p> <ul style="list-style-type: none"> – применять средства охранной сигнализации, 	<p>Демонстрационный экзамен;</p> <p>Защита дипломной работы</p>
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.	охранного телевидения и систем контроля и управления доступом;	
ОК 07.	Содействовать сохранению окружающей среды, ресурсосбережению, эффективно действовать в чрезвычайных ситуациях.	– применять технические средства для криптографической защиты информации конфиденциального характера;	
ОК 08.	Использовать средства физической культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и поддержания необходимого уровня физической подготовленности.	– применять технические средства для уничтожения информации и носителей информации, защиты информации в условиях применения мобильных устройств обработки и передачи данных;	
ОК 09.	Использовать информационные технологии в профессиональной деятельности.	– применять инженерно-технические средства физической защиты объектов информатизации.	
ОК 10.	Пользоваться профессиональной документацией на государственном и иностранном языках.	знать:	
ОК 11.	Использовать знания по финансовой грамотности, планировать предпринимательскую деятельность в профессиональной сфере.	– 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;	
ПК 3.1.	Осуществлять установку, монтаж, настройку и техническое обслуживание технических средств защиты информации в соответствии с требованиями эксплуатационной	– 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;	

	документации.	<ul style="list-style-type: none"> – 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. 	
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.		
ОК 01.	Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам.	иметь практический опыт: <ul style="list-style-type: none"> – подключения кабельной системы персонального компьютера, периферийного и мультимедийного оборудования; – настройки параметров функционирования персонального компьютера, периферийного и мультимедийного оборудования; – ввода цифровой и аналоговой информации в персональный компьютер с различных носителей, периферийного и мультимедийного оборудования; 	Защита дипломной работы
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.		
		<ul style="list-style-type: none"> – сканирования, обработки и распознавания документов; – конвертирования медиафайлов в различные форматы, экспорта и импорта файлов в различные программы - редакторы; – обработки аудио - визуального и мультимедийного контента с помощью специализированных программ - редакторов; – создания и воспроизведения видеороликов, презентаций, слайд-шоу, медиафайлов и другой итоговой продукции из исходных аудио, визуальных и мультимедийных компонентов; – осуществления навигации по ресурсам, поиска, ввода и передачи данных с помощью технологий и сервисов сети Интернет. <p>уметь:</p> <ul style="list-style-type: none"> – подключать и настраивать параметры функционирования персонального компьютера, периферийного и мультимедийного оборудования; – настраивать основные компоненты графического интерфейса операционной системы и специализированных программ - редакторов; – управлять файлами данных на локальных, съемных запоминающих устройствах, а также на дисках локальной компьютерной сети и в сети Интернет; – производить распечатку, копирование и тиражирование документов на принтере и других периферийных устройствах вывода; 	

ОК 10.	Пользоваться профессиональной документацией на государственном и иностранном языках.	<ul style="list-style-type: none"> – распознавать сканированные текстовые документы с помощью программ распознавания текста; – вводить цифровую и аналоговую информацию в персональный компьютер с различных носителей, периферийного и мультимедийного оборудования; – создавать и редактировать графические объекты с помощью программ для обработки растровой и векторной графики; – конвертировать файлы с цифровой информацией в различные форматы; – производить сканирование прозрачных и непрозрачных оригиналов; – производить съемку и передачу цифровых изображений с фото- и видеокамеры на персональный компьютер; – обрабатывать аудио, визуальный контент и медиафайлы средствами звуковых, графических и видео - редакторов; – создавать видеоролики, презентации, слайд-шоу, медиафайлы и другую итоговую продукцию из исходных аудио, визуальных мультимедийных компонентов; – воспроизводить аудио, визуальный контент и медиафайлы средствами персонального компьютера и мультимедийного оборудования; 	
ОК 11.	Использовать знания по финансовой грамотности, планировать предпринимательскую деятельность в профессиональной сфере.		
ДПК 4.1	Осуществлять подготовку оборудования компьютерной системы к работе, производить инсталляцию, настройку и обслуживание программного обеспечения		
ДПК 4.2	Создавать и управлять на персональном компьютере текстовыми документами, таблицами, презентациями и содержанием баз данных, работать в графических редакторах.		
ДПК 4.3	Использовать ресурсы локальных вычислительных сетей, ресурсы технологий и сервисов Интернета.		
ДПК 4.4	Обеспечивать применение средств защиты информации в компьютерной системе.		

ДПК 5.1	Подготовка (организация поверки) контрольно-измерительного оборудования для проведения контроля функционирования инфокоммуникационной системы	<ul style="list-style-type: none"> – производить распечатку, копирование и тиражирование документов на принтере и других периферийных устройствах вывода; – использовать мультимедиа - проектор для демонстрации содержимого экранных форм с персонального компьютера; – вести отчетную и техническую документацию. 	
ДПК 5.2	Документирование результатов контроля, включая подготовку протоколов или ввод данных в автоматизированные информационные системы	<p>знать:</p> <ul style="list-style-type: none"> – устройство персональных компьютеров, основные блоки, функции и – технические характеристики; – архитектуру, состав, функции и классификацию операционных систем – персонального компьютера; – виды и назначение периферийных устройств, их устройство и принцип – действия, интерфейсы подключения и правила эксплуатации; – принципы установки и настройки основных компонентов – операционной системы и драйверов периферийного оборудования; – принципы цифрового представления звуковой, графической, видео и – мультимедийной информации в персональном компьютере; – виды и параметры форматов аудио -, графических, видео - и 	

		<ul style="list-style-type: none">– мультимедийных файлов в методы их конвертирования;– назначение, возможности, правила эксплуатации мультимедийного оборудования;– основные типы интерфейсов для подключения мультимедийного оборудования;– основные приемы обработки цифровой информации;– назначение, разновидности и функциональные возможности программ обработки звука;– назначение, разновидности и функциональные возможности программ обработки графических изображений;– назначение, разновидности и функциональные возможности программ обработки видео- и мультимедиа контента;– структуру, виды информационных ресурсов и основные виды услуг в сети Интернет;– назначение, разновидности и функциональные возможности программ для создания веб-страниц;– нормативные документы по охране труда при работе с персональным компьютером, мультимедийным	
--	--	---	--

2. СИСТЕМА КОНТРОЛЯ И ОЦЕНКИ ОСВОЕНИЯ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

В соответствии с требованиями ФГОС СПО ИА по образовательной программе специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем:

- демонстрационный экзамен по КОД: 10.02.05-1-2025;
- подготовку и защиту выпускной квалификационной работы (дипломная работа).

2.1. Демонстрационный экзамен по КОД: 10.02.05-1-2025

Демонстрационный экзамен по КОД: 10.02.05-1-2025 охватывает минимальное содержание данного модуля, установленное в соответствии с требованиями ФГОС СПО по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем.

В содержании Программы демонстрационного экзамена выделяются два основных модуля:

- Эксплуатация автоматизированных (информационных) систем в защищенном исполнении;
- Защита информации в автоматизированных системах программными и программно- аппаратными средствами

Демонстрационный экзамен проводится в форме экзамена базового уровня.

2.1.1. Содержание демонстрационного экзамена по КОД: 10.02.05-1-2025

1. Демонстрационный экзамен проводится с использованием КОД, включенных образовательными организациями в программу ИА.

2. Задания демонстрационного экзамена доводятся до главного эксперта в день, предшествующий дню начала демонстрационного экзамена.

3. Образовательная организация обеспечивает необходимые технические условия для обеспечения заданиями во время демонстрационного экзамена выпускников, членов ГЭК, членов экспертной группы.

4. Демонстрационный экзамен проводится в ЦПДЭ, представляющем собой площадку, оборудованную и оснащенную в

5. ЦПДЭ может располагаться на территории образовательной организации, а при сетевой форме реализации образовательных программ — также на территории иной организации, обладающей необходимыми ресурсами для организации ЦПДЭ.

6. Выпускники проходят демонстрационный экзамен в ЦПДЭ в составе экзаменационных групп.

7. Образовательная организация знакомит с планом проведения демонстрационного экзамена выпускников, сдающих демонстрационный экзамен, и лиц, обеспечивающих проведение демонстрационного экзамена, в срок не позднее чем за 5 рабочих дней до даты проведения экзамена.

8. Количество, общая площадь и состояние помещений, предоставляемых для проведения демонстрационного экзамена, должны обеспечивать проведение демонстрационного экзамена в соответствии с КОД.

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

10. Главным экспертом осуществляется осмотр ЦПДЭ, распределение обязанностей между членами экспертной группы по оценке выполнения заданий демонстрационного экзамена, а также распределение рабочих мест между выпускниками с использованием способа случайной выборки. Результаты распределения обязанностей между членами экспертной группы и распределения рабочих мест между выпускниками фиксируются главным экспертом в соответствующих протоколах.

11. Выпускники знакомятся со своими рабочими местами, под

руководством главного эксперта также повторно знакомятся с планом проведения демонстрационного экзамена, условиями оказания первичной медицинской помощи в ЦПДЭ. Факт ознакомления отражается главным экспертом в протоколе распределения рабочих мест.

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

13. Образовательная организация обязана не позднее чем за один рабочий день до дня проведения демонстрационного экзамена уведомить главного эксперта об участии в проведении демонстрационного экзамена тьютора (ассистента).

2.2. Выпускная квалификационная работа

2.2.1. Содержание ВКР

Формой ВКР по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем является дипломная работа.

Обучающиеся имеют право:

- самостоятельно выбирать тему работы;
- самостоятельно анализировать информацию, обобщать факты, готовить портфолио;
- самостоятельно выбирать методы решения проектной задачи;
- получать консультации руководителя по теме исследования в установленное для этого время.

Области профессиональной деятельности, согласно ФГОС СПО	Тематика ВКР	Виды ВКР
ПМ.01 Эксплуатация автоматизированных (информационных) систем в защищённом исполнении	<ol style="list-style-type: none">1. Разработка технического решения по внедрению DLP-системы в комплексную систему обеспечения информационной безопасности страховой компании2. Разработка защиты информации с применением межсетевых экранов автоматизированного рабочего места главного инженера (на примере компании...)3. Разработка защиты базы данных Университетского колледжа информационных технологий от несанкционированного доступа4. Обеспечение защиты персональных данных (на примере предприятия ООО...)5. Защита транзакций в интернет-магазине (на примере...)6. Разработка защиты базы данных от несанкционированного доступа к серверу (на примере компании ...)	Дипломная работа

- | | | |
|--|--|--|
| | <ol style="list-style-type: none">7. Обеспечение защищенного документооборота между компанией налогоплательщиком и государственными контролирующими органами8. Организация защищенного сегмента сети научно-исследовательского центра для обработки информации с ограниченным доступом9. Обеспечение безопасности автоматизированной информационной системы (на примере организации ...)10. Разработка защиты базы данных компании от несанкционированного доступа к серверу (на примере ...)11. Обеспечение защиты информации автоматизированного рабочего места финансового директора банка12. Обеспечение защиты от влияния побочных электромагнитных излучений и наводок рабочего места разработчика программного обеспечения13. Обеспечение информационной безопасности автоматизированного рабочего места сотрудников офиса департамента эксплуатации прикладных систем (на примере ...)14. Защита речевой информации от утечки по техническим каналам в Open Space помещении (на примере организации ...)15. Обеспечение защиты от влияния побочных электромагнитных излучений и наводок рабочего места разработчика программного обеспечения16. Комплексное обеспечение информационной безопасности персональных данных в компании индустрии моды и дизайна17. Разработка автоматизированной системы | |
|--|--|--|

	<p>динамического анализа вредоносных файлов на основе технологии «Песочница» (на примере ...)</p> <p>18.Разработка проекта единой системы идентификации и аутентификации (на примере производственного предприятия или завода)</p> <p>19.Разработка политики информационной безопасности для компании ООО ...</p> <p>20.Обеспечение комплексной защиты информации кабинета руководителя издательского дома</p> <p>21.Обеспечение защищенного документооборота между компанией налогоплательщиком и государственными контролирующими органами</p>	
<p>ПМ.02 Защита информации в автоматизированных системах программными и программно-аппаратными средствами</p>	<ol style="list-style-type: none"> 1. Применение программных методов защиты базы данных компании (на примере ООО ...) 2. Применение корпоративных антивирусных решений на предприятии (на примере...) 3. Применение программных средств обеспечения безопасности веб-сайтов на примере обеспечения защиты от XSS атак 4. Обеспечение комплексной антивирусной защиты ИКТ-инфраструктуры производственного предприятия 5. Разработка технического решения по внедрению программно-аппаратных методов защиты электронного документооборота (на примере ООО ...) 6. Разработка технического решения по внедрению программно-аппаратной системы аутентификации пользователей (на примере ООО ...) 7. Разработка программного обеспечения для защиты USB-носителей 	<p>Дипломная работа</p>

	<p>8. Разработка программно-аппаратной защиты информации объекта ИТ-службы (на примере организации...)</p> <p>9. Применение защиты и методов предотвращения DDoS атак на предприятии ...</p> <p>10. Обеспечение программно-аппаратных методов защиты ретроконверсии для ООО ...</p> <p>11. Применение программно-аппаратных методов и средств обеспечения конфиденциальной информации для научно-производственного предприятия (на примере ООО...)</p> <p>12. Применение программно-аппаратных методов и средств обеспечения конфиденциальной информации для избирательного участка</p> <p>13. Разработка технического решения по внедрению программно-аппаратных средств защиты коммерческой тайны (на примере ...)</p> <p>14. Применение программно-аппаратных методов защиты данных от несанкционированного доступа (на примере ГУП ...)</p> <p>15. Разработка программных методов защиты ведомственных баз данных</p> <p>16. Обеспечение комплексной защиты сетей (на примере ...)</p> <p>17. Разработка программных методов защиты ведомственных баз данных</p> <p>18. Разработка методов предоставления работ и услуг по специальной проверке оборудования</p> <p>19. Разработка политики информационной безопасности и моделирования угроз организации (на примере ООО ...)</p> <p>20. Разработка проекта требований безопасности информации, предъявляемых к</p>	
--	--	--

	<p>средствам управления мобильными приложениями</p> <p>21. Разработка комплексной защиты информации кабинета директора производственного предприятия или завода</p> <p>22. Обеспечение информационной безопасности архива (на примере организации ...)</p> <p>23. Обеспечение безопасности мобильной сети оператора сотовой связи</p> <p>24. Разработка проекта единой системы идентификации и аутентификации на предприятии (на примере ...)</p> <p>25. Обеспечение комплексной защиты информации предприятия (на примере ...)</p> <p>26. Обеспечение комплексной защиты информации кабинета руководителя издательского дома (на примере ...)</p> <p>27. Обеспечение информационной безопасности отдела кадров на предприятии (на примере ...)</p>	
<p>ПМ.03 Защита информации техническими средствами</p>	<p>1. Разработка технического решения системы видеонаблюдения (на примере ...)</p> <p>2. Разработка технических решений по защите корпоративной сети (на примере ...)</p> <p>3. Разработка технического решения по внедрению программных средств защиты интернет-аукциона (на примере ...)</p> <p>4. Применение технических средств защиты информации для обеспечения безопасности конференц-зала (на примере...)</p> <p>5. Применение охранных радиолучевых средств на объекте производственного предприятия</p> <p>6. Разработка мобильного инженерно-</p>	<p>Дипломная работа</p>

технического комплекса защиты помещения для ведения коммерческих переговоров (на примере ООО ...)

7. Разработка инженерно-технических методов защиты акустического канала утечки информации автоматизированного рабочего места главного инженера компании (на примере ООО ...)

8. Применение инженерно-технических средств защиты информации для обеспечения безопасности административного здания (на примере компании ООО ...)

9. Применение технических средств защиты информации автоматизированного рабочего места начальника отдела безопасности (на примере ООО ...)

10. Применение инженерно-технических методов защиты кабинета главного инженера компании (на примере ООО ...)

11. Разработка технического решения по внедрению технических средств защиты кабинета руководителя банка

12. Применение технических средств защиты информации для обеспечения безопасности конференц-зала (на примере ООО ...)

13. Применение технических средств защиты информации для обеспечения безопасности лаборатории

14. Разработка защиты техническими средствами помещения серверной (на примере ООО ...)

15. Комплексная защита кабинета для совещаний (на примере ООО ...)

16. Разработка технического решения по внедрению инженерно-технических средств защиты кабинета главного бухгалтера (на примере ...)

- | | | |
|--|--|--|
| | <ol style="list-style-type: none">17. Разработка инженерно-технической защиты отдела IT-разработок (на примере организации ...)18. Разработка инженерно-технической защиты данных на предприятии (на примере производственного предприятия или завода)19. Разработка инженерно-технической защиты информации в бизнес-центре20. Разработка технического решения для конфигураций сетевых устройств (на примере ...)21. Применение технических средств защиты информации для обеспечения безопасности образовательного учреждения | |
|--|--|--|

2.2.2. Формы оценивания поэтапного выполнения ВКР

Текущую оценку подготовки ВКР в письменной форме осуществляет руководитель, определяя процент готовности работы в соответствии с выданным заданием. На основных этапах оценивания оценка ставится на просмотре членами предметно-цикловой комиссии.

Этапы	Виды работ	Формы оценивания
1 этап – Постановка проблемы (планирование)	Подготовка студентами предложений по теме ВКР. Выбор и утверждение тем ВКР. Уточнение объема и структуры дипломной работы. Разработка и выдача индивидуальных заданий на дипломные работы.	Оценка руководителя
2 этап – Сбор материала, анализ и оценка собранных данных по теме исследования	Изучаем особенности объекта исследования. Получение, сбор и анализ исходных данных и необходимых материалов.	Оценка руководителя
3 этап – Разработка рекомендаций и предложений по теме дипломной работы	Формулирование итоговых выводов и оценок по результатам проведенного исследования. Определение необходимых мероприятий по улучшению анализируемой деятельности (разработка рекомендаций и предложений). Подготовка заключения, корректировка введения (цели, задачи исследования). Оформление итогового варианта дипломной работы.	Оценка руководителя Контроль заведующего отделения
4 этап - Защита работы	Написание отзыва руководителем дипломной работы. Рецензирование дипломных работ. Предзащита дипломных работ Защита ВКР	Защита перед ГАК

Предварительная защита

В целях усиления контроля за выполнением дипломных работ, для завершения проверки содержания пояснительной записки, укрепления

динамичности процесса защиты рекомендуется проведение предварительной защиты. Предзащита позволяет руководителю дипломного проекта проверить состояние дипломного проекта накануне его рецензирования и защиты, а также соответствие содержания требованиям государственной итоговой аттестации, зафиксированным в ФГОС СПО, и рекомендациях по подготовке и проведению итоговой государственной аттестации, рассмотренной на заседании методической комиссии и утвержденной на заседании педагогического совета.

По результатам предварительной защиты решается вопрос о допуске выпускника к рецензированию и защите дипломной работы.

Предварительная защита проводится не позднее, чем за 10 дней до даты официальной защиты. К этому моменту представляются готовая дипломная работа (дипломный проект) в материале и окончательный вариант текста пояснительной записки. Результаты предварительной защиты дипломных работ выпускников протоколируются.

По результатам предварительной защиты издается приказ о допуске выпускников к проведению рецензирования и защите дипломной работы.

Порядок защиты выпускной квалификационной работы

Защита ВКР проводится на открытом заседании государственной экзаменационной комиссии (ГЭК). На защиту дипломной работы отводится до 30 минут. Процедура защиты устанавливается председателем ГЭК по согласованию с членами комиссии и, как правило, включает:

- доклад обучающегося, в котором присутствует обоснование выбранной темы и ее значения в профессиональной деятельности, постановку цели и задач дипломного проекта, объяснение хода работы над своим проектом (не более 10 минут);

- чтение рецензии;
- вопросы членов комиссии;
- ответы обучающегося.

2.2.4. Критерии оценки качества ВКР

Критерии оценки	Компетенции	ЗУНЫ	Уровень оценки			
			Повышенный уровень - оценка «отлично»	Высокий уровень - оценка «хорошо»	Базовый уровень - оценка «удовлетворительно»	Недостаточный уровень - оценка «неудовлетворительно»
Обоснованность и логичность выводов и оценок ВКР	ОК 1 – ОК 11; ПК 1.1 – ПК 1.4; ПК 2.1 – ПК 2.6; ПК 3.1 – ПК 3.5; ПК 4.1 – ПК 4.4;	иметь практический опыт: 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	ВКР выполнена на актуальную тему, цель и задачи исследования четко определены и конкретны, теме полностью соответствуют. Суть проблемы раскрыта на высоком уровне с использованием профессиональных знаний и навыков, полученных в результате обучения в области информационной безопасности.	ВКР выполнена на актуальную тему. Цель и задачи исследования сформулированы, теме соответствуют. Суть проблемы в целом раскрыта. Используются профессиональные знания и навыки, полученные в результате обучения в области информационной безопасности.	ВКР выполнена на актуальную тему, цель и задачи исследования сформулированы, однако, суть проблемы раскрыта не полностью. Слабо использованы профессиональные знания и навыки, полученные в результате обучения в области информационной безопасности.	ВКР выполнена на актуальную тему, цель и задачи исследования сформулированы, однако работой не решены. Практически не использованы профессиональные знания и навыки, полученные в результате обучения в области информационно

		<p>информационных систем.</p> <p>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. выявлении технических каналов</p>				й безопасности.
<p>Практическая значимость разработанных рекомендаций (предложенных мероприятий)</p>		<p>утечки информации; применении, техническом обслуживании, диагностике, устранении отказов,</p>	<p>Практическая часть ВКР выполнена на высоком профессиональном уровне (может быть рекомендована для</p>	<p>Практическая часть ВКР выполнена на хорошем профессиональном уровне.</p>	<p>Практическая часть ВКР выполнена на удовлетворительном профессиональном</p>	<p>Практическая часть не содержит самостоятельно разработанных и надлежаще обоснованных</p>

		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,	внедрения).		уровне, во многих аспектах имеет поверхностное предложение или решение.	рекомендаций.
Актуальность и достаточность использованных источников и литературы			В работе присутствует актуальный и обширный список использованных источников и литературы.	В работе присутствует актуальный и достаточный список использованных источников и литературы.	В работе присутствует не вполне актуальный и ограниченный список использованных источников и литературы.	Список использованных источников и литературы не вполне актуальный и достаточный для достижения цели работы и решения поставленных задач.
Наличие таблиц, графиков и рисунков			Присутствуют в достаточном объеме, самостоятельно сформированные.	Присутствуют.	Присутствуют частично заимствованные из других источников.	Отсутствуют совсем или присутствуют полностью заимствованные из других источников.
Представление ВКР на защите			Наличие презентации (доклада) отражающей все основные выводы и разработанные рекомендации по результатам	Наличие презентации (доклада) отражающей некоторые (основные) выводы и разработанные рекомендации по	Отсутствует презентация, доклад не в полной мере отражает полученные выводы и сформулированы	Отсутствует презентация, доклад не отражает выводы и оценки содержащиеся в ВКР.

		<p>создаваемых техническими средствами защиты информации. подключения кабельной системы персонального компьютера, периферийного и мультимедийного оборудования; настройки параметров функционирования персонального компьютера, периферийного и мультимедийного оборудования; ввода цифровой и аналоговой информации в персональный компьютер с различных носителей, периферийного и мультимедийного оборудования; сканирования, обработки и распознавания документов;</p>	<p>проведенного исследования.</p>	<p>результатам проведенного исследования.</p>	<p>е предложения по результатам проведенного исследования.</p>	
--	--	--	-----------------------------------	---	--	--

		конвертирования медиафайлов в различные форматы, экспорта и импорта файлов в различные программы - редакторы; обработки аудио - визуального и мультимедийного контента с помощью специализированных программ - редакторов; создания и воспроизведения видеороликов, презентаций, слайд- шоу, медиафайлов и другой итоговой продукции из исходных аудио, визуальных и мультимедийных компонентов; осуществления навигации по ресурсам, поиска, ввода и передачи данных с помощью технологий и				
--	--	--	--	--	--	--

		<p>сервисов сети Интернет.</p> <p>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;</p>				
--	--	--	--	--	--	--

		<p>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. устанавливать, настраивать, применять программные и программно- аппаратные средства защиты информации; диагностировать, устранять отказы, обеспечивать работоспособность и</p>				
--	--	---	--	--	--	--

		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				
--	--	---	--	--	--	--

		<p>сведений, необходимых для защиты объектов информатизации, в том числе с использованием программных и программно- аппаратных средств обнаружения, предупреждения и ликвидации последствий компьютерных атак. 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</p>				
--	--	--	--	--	--	--

		<p>информации и носителей информации, защиты информации в условиях применения мобильных устройств обработки и передачи данных;</p> <p>применять инженерно-технические средства физической защиты объектов информатизации.</p> <p>подключать и настраивать параметры функционирования персонального компьютера, периферийного и мультимедийного оборудования;</p> <p>настраивать основные компоненты графического интерфейса операционной системы и специализированных программ - редакторов;</p>				
--	--	--	--	--	--	--

		<p>управлять файлами данных на локальных, съемных запоминающих устройствах, а также на дисках локальной компьютерной сети и в сети Интернет;</p> <p>производить распечатку, копирование и тиражирование документов на принтере и других периферийных устройствах вывода;</p> <p>распознавать сканированные текстовые документы с помощью программ распознавания текста;</p> <p>вводить цифровую и аналоговую информацию в персональный компьютер с различных носителей, периферийного и мультимедийного оборудования;</p> <p>создавать и</p>				
--	--	--	--	--	--	--

		<p>редактировать графические объекты с помощью программ для обработки растровой и векторной графики; конвертировать файлы с цифровой информацией в различные форматы; производить сканирование прозрачных и непрозрачных оригиналов; производить съемку и передачу цифровых изображений с фото- и видеокамеры на персональный компьютер; обрабатывать аудио, визуальный контент и медиафайлы средствами звуковых, графических и видео-редакторов; создавать видеоролики, презентации, слайд-шоу, медиафайлы и</p>				
--	--	---	--	--	--	--

		другую итоговую продукцию из исходных аудио, визуальных мультимедийных компонентов; воспроизводить аудио, визуальный контент и медиафайлы средствами персонального компьютера и мультимедийного оборудования; производить распечатку, копирование и тиражирование документов на принтере и других периферийных устройствах вывода; использовать мультимедиа - проектор для демонстрации содержимого экранных форм с персонального компьютера;				
--	--	---	--	--	--	--

		<p>вести отчетную и техническую документацию.</p> <p>знать:</p> <p>состав и принципы работы автоматизированных систем, операционных систем и сред;</p> <p>принципы разработки алгоритмов программ, основных приемов программирования;</p> <p>модели баз данных;</p> <p>принципы построения, физические основы работы периферийных устройств, основных методов организации и проведения технического обслуживания вычислительной техники и других технических средств информатизации;</p>				
--	--	---	--	--	--	--

		<p>теоретические основы компьютерных сетей и их аппаратных компонент, сетевых моделей, протоколов и принципов адресации;</p> <p>порядок установки и ввода в эксплуатацию средств защиты информации в компьютерных сетях.</p> <p>особенности и способы применения программных и программно-аппаратных средств защиты информации, в том числе, в операционных системах, компьютерных сетях, базах данных;</p> <p> типовые модели управления доступом, средств, методов и протоколов идентификации и аутентификации;</p> <p> типовые средства и</p>				
--	--	--	--	--	--	--

		<p>методы ведения аудита, средств и способов защиты информации в локальных вычислительных сетях, средств защиты от несанкционированного доступа;</p> <p>основные понятия криптографии и типовых криптографических методов и средств защиты информации.</p> <p>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</p>				
--	--	---	--	--	--	--

		<p>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</p>				
--	--	--	--	--	--	--

		<p>эффективности защиты информации, обрабатываемой средствами вычислительной техники на объектах информатизации;</p> <p>номенклатуру применяемых средств защиты информации от несанкционированной утечки по техническим каналам и физической защиты объектов информатизации.</p> <p>устройство персональных компьютеров, основные блоки, функции и технические характеристики; архитектуру, состав, функции и классификацию операционных систем персонального компьютера;</p> <p>виды и назначение</p>				
--	--	--	--	--	--	--

		<p>периферийных устройств, их устройство и принцип действия, интерфейсы подключения и правила эксплуатации;</p> <p>принципы установки и настройки основных компонентов операционной системы и драйверов периферийного оборудования;</p> <p>принципы цифрового представления звуковой, графической, видео и мультимедийной информации в персональном компьютере;</p> <p>виды и параметры форматов аудио -, графических, видео - и мультимедийных файлов в методы их конвертирования;</p> <p>назначение, возможности, правила</p>				
--	--	---	--	--	--	--

		<p>эксплуатации мультимедийного оборудования;</p> <p>основные типы интерфейсов для подключения мультимедийного оборудования;</p> <p>основные приемы обработки цифровой информации;</p> <p>назначение, разновидности и функциональные возможности программ обработки звука;</p> <p>назначение, разновидности и функциональные возможности программ обработки графических изображений;</p> <p>назначение, разновидности и функциональные возможности программ обработки видео- и</p>				
--	--	--	--	--	--	--

		<p>мультимедиа контента; структуру, виды информационных ресурсов и основные виды услуг в сети Интернет; назначение, разновидности и функциональные возможности программ для создания веб- страниц; нормативные документы по охране труда при работе с персональным компьютером, периферийным, мультимедийным оборудованием и компьютерной оргтехниккой.</p>				
--	--	---	--	--	--	--

По данным критериям каждый член комиссии выставляет оценки и на основании обозначенных оценок по каждому критерию выводит итоговую оценку. Наивысшей оценкой является оценка «5» (отлично). После обсуждения сопоставляются итоговые оценки всех членов комиссии, и принимается решение об окончательном варианте итоговой оценки. По каждому обучающемуся продумывается мотивация выставленной оценки, в которой отмечаются сильные и слабые стороны дипломной работы.

При определении окончательной оценки по ВКР учитываются: качество доклада студента, качество ответов на вопросы, отзыв руководителя ВКР, отзыв рецензента, соответствующие качеству представленных проектов.

В том случае, когда защита ВКР признается неудовлетворительной, ГЭК устанавливает, может ли выпускник представить к вторичной защите ту же работу с соответствующей доработкой, определяемой комиссией, или же выпускник обязан разработать новую тему, которая должна быть определена после первой защиты ВКР.

2.3. Методические материалы, определяющие процедуры оценивания результатов освоения образовательной программы

Методические материалы, определяющие процедуры оценивания результатов освоения ППССЗ:

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

- образовательная программа по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем;

- Программа ИА по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем.

ОТЗЫВ О ВЫПУСКНОЙ КВАЛИФИКАЦИОННОЙ РАБОТЕ

(тема работы)

Основное содержание работы

Основные достоинства работы

Основные недостатки работы

Оценка _____

Руководитель ВКР _____

« ____ » _____ 20__ г

ОЦЕНОЧНЫЙ ЛИСТ РЕЗУЛЬТАТОВ ДЕМОНСТРАЦИОННОГО ЭКЗАМЕНА

ФИО обучающегося	Критерии оценки							Итого

ОЦЕНОЧНЫЙ ЛИСТ РЕЗУЛЬТАТОВ ЗАЩИТЫ ВЫПУСКНОЙ КВАЛИФИКАЦИОННОЙ РАБОТЫ

ФИО студента	Критерии оценки					
	Обоснованность и логичность выводов и оценок ВКР	Практическая значимость разработанных рекомендаций (предложенных мероприятий)	Актуальность и достаточность использованных источников и литературы	Наличие таблиц, графиков и рисунков	Представление ВКР на защите	Итоговая оценка

