Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Дальневосточный государственный университет путей сообщения»

УТВЕРЖДАЮ

Проректор ПО и СП - Директор ХТЖТ
_____ А.Н. Ганус
(подпись, Ф.И.О.)
«_19 » июня_ 2023 г.

ОЦЕНОЧНЫЕ МАТЕРИАЛЫ
итоговой (государственной итоговой) аттестации

по программе подготовки специалистов среднего звена (ППССЗ)
10.02.05 Обеспечение информационной безопасности автоматизированных систем

для специальности
10.02.05 Обеспечение информационной безопасности автоматизированных систем
код и наименование направления подготовки (специальности)

направленность (профиль): нет

Составитель(и) преподаватель Касьяненко А.Ю.
ученая степень, должность Ф.И.О. подпись

Обсуждена на заседании предметно-цикловой комиссии по ППССЗ «Информационная безопасность автоматизированных систем»

« 26 » мая 2023 г., протокол № 9_____

Председатель ПЦК _____Касьяненко А.Ю.
подпись

Старший методист_____Балаганская Н.В.
подпись

Хабаровск
2023

1. Описание показателей и критериев оценивания компетенций, а также шкал оценивания

Перечень компетенций и этапы их формирования в процессе освоения образовательной программы	Описание показателей и критериев оценивания компетенций на различных этапах их формирования, описание шкал оценивания			Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций в процессе освоения образовательной программы	Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта, характеризующих этапы формирования компетенций
Компетенция	Показатель оценивания	Критерий оценивания	Шкала оценивания		
ОК 01. Выбирать способы решения задач профессиональной деятельности применительно к различным контекстам	**Знания.** актуальный профессиональный и социальный контекст, в котором приходится работать и жить; основные источники информации и ресурсы для решения задач и проблем в профессиональном и/или социальном контексте; алгоритмы выполнения работ в профессиональной и смежных областях; методы работы в профессиональной и смежных сферах; структуру плана для решения задач; порядок оценки результатов решения задач профессиональной деятельности **Умения.** распознавать задачу и/или проблему в профессиональном и/или социальном контексте; анализировать задачу и/или проблему и выделять её составные части; определять этапы решения задачи; выявлять и эффективно искать информацию, необходимую для решения задачи и/или проблемы; составить план действия; определить необходимые ресурсы; владеть актуальными методами работы в профессиональной и смежных сферах; реализовать составленный план; оценивать результат и последствия своих действий (самостоятельно или с помощью наставника)	**Демонстрационного экзамена и дипломного проекта (дипломной работы)** 1.Качество ДП (ДР) (качество пояснительной записки; качество иллюстративного материала (чертежей)); Качество защиты ДП (ДР) (качество доклада; качество ответов на вопросы). **2. Демонстрационного экзамена** Охрана труда и техника безопасности. Технологии анализа и защиты сетевого трафика, установка, конфигурирование, компрометация,	**Демонстрационного экзамена и дипломного проекта (работы)** **1. Дипломного проекта (дипломной работы):** **Отлично:** Полное соответствие темы ДП (ДР) направлению или специальности Актуальность темы ДП (ДР) полностью обоснована. Полное соответствие содержания ДП (ДР) сформулированной теме. При выполнении ДП (ДР) использована новая отечественная и литература.	Вопросы к защите ДП (ДР): 1, 2, 5, 6, 9, 15 Вопросы к защите ДП (ДР): 21, 24, 29, 38, 39 Вопросы к защите ДП (ДР): 40, 44, 54, 61, 79, 83	Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности приведены в стандарте ДВГУПС СТ 02-28-21 «Формы, периодичность и порядок текущего контроля успеваемости и промежуточной аттестации».
ОК 02. Осуществлять поиск, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности	**Знания.** номенклатура информационных источников, применяемых в профессиональной деятельности; приемы структурирования информации; формат оформления результатов поиска информации **Умения.** определять задачи для поиска информации; определять необходимые источники информации; планировать процесс поиска; структурировать получаемую информацию; выделять наиболее значимое в перечне информации; оценивать практическую значимость результатов поиска; оформлять результаты поиска			Вопросы к защите ДП (ДР): 2, 3, 4, 7, 8, 11 Вопросы к защите ДП (ДР): 23, 24, 30, 31, 37 Вопросы к защите ДП (ДР): 39, 40, 41, 47, 63	

ОК 03. Планировать и реализовывать собственное профессиональное и личностное развитие	**Знания:** содержание актуальной нормативно-правовой документации; современная научная и профессиональная терминология; возможные траектории профессионального развития и самообразования **Умения**: определять актуальность нормативно-правовой документации в профессиональной деятельности; выстраивать траектории профессионального и личностного развития	межсетевое взаимодействие и туннелирование. *Критерии оценки выполненного демонстрационного экзамена разрабатываются в соответствии с Регламентом «Молодые профессионалы», техническим описанием компетенции «Корпоративная защита от внутренних угроз информационной безопасности»*	В ДП (ДР) использованы современных информационных технологий. Графический материал полностью раскрывает смысл и отвечает ГОСТ, ЕСКД и др. Текст ДП (ДР) читается легко, ошибки отсутствуют. В работе использованы оригинальные программно-технические средства. ДП (ДР) соответствует всем предъявленным требованиям. Во время защиты полностью раскрыта тема ДП (ДР), соблюдён регламент. Ответы точные, высокий уровень эрудиции. Оценка руководителя и рецензента: «отлично». **Хорошо:** Имеют место незначительные погрешности. Имеют место несущественные погрешности в обосновании актуальности темы, незначительные погрешности в формулировке.	Вопросы к защите ДП (ДР): 3, 12, 21, 22, 31, 32 Вопросы к защите ДП (ДР): 40, 44, 45, 48, 57, 61, 66 Вопросы к защите ДП (ДР): 69, 71, 73, 80, 82	
ОК 04. Работать в коллективе и команде, эффективно взаимодействовать с коллегами, руководством, клиентами	**Знания.** психология коллектива; психология личности; основы проектной деятельности **Умения.** организовывать работу коллектива и команды; взаимодействовать с коллегами, руководством, клиентами			Вопросы к защите ДП (ДР): 1, 2, 4, 13, 22, 24, 32 Вопросы к защите ДП (ДР): 41, 50, 59, 63, 67 Вопросы к защите ДП (ДР): 76, 77, 81, 82, 84	
ОК 05. Осуществлять устную и письменную коммуникацию на государственном языке с учетом особенностей социального и культурного контекста	**Знания.** особенности социального и культурного контекста; правила оформления документов.. **Умения.** излагать свои мысли на государственном языке; оформлять документы.			Вопросы к защите ДП (ДР): 10, 14, 18, 19, 25 Вопросы к защите ДП (ДР): 29, 32, 40, 49, 51 Вопросы к защите ДП (ДР): 54, 55, 61, 62, 65	
ОК 06. Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных общечеловеческих ценностей, применять стандарты антикоррупционного поведения	**Знания.** сущность гражданско-патриотической позиции; общечеловеческие ценности; правила поведения в ходе выполнения профессиональной деятельности **Умения.** описывать значимость своей профессии; презентовать структуру профессиональной деятельности по специальности			Вопросы к защите ДП (ДР): 6, 15, 16, 17, 18, 20 Вопросы к защите ДП (ДР): 27, 33, 34, 41, 42 Вопросы к защите ДП (ДР): 51, 52, 56, 64, 69	
ОК 07. Содействовать сохранению окружающей среды, ресурсосбережению, эффективно действовать в чрезвычайных ситуациях	**Знания.** правила экологической безопасности при ведении профессиональной деятельности; основные ресурсы, задействованные в профессиональной деятельности; пути обеспечения ресурсосбережения **Умения.** соблюдать нормы экологической безопасности; определять направления ресурсосбережения в рамках профессиональной			Вопросы к защите ДП (ДР): 1, 5, 9, 16, 19, 20, 25 Вопросы к защите ДП (ДР): 26, 31, 35, 43, 44 Вопросы к защите ДП (ДР):	

	деятельности по специальности		Современная отечественная литература. В ряде случаев отсутствуют ссылки на источник информации. Имеют место небольшие погрешности в использовании современных информационных технологий, вычислительной техники. Есть отдельные грамматические ошибки. Современные пакеты программ используются широко. Допущены незначительные погрешности в оформлении ДП (ДР). Есть ошибки в регламенте и использовании чертежей. Есть незначительные погрешности в оформлении. Высокая эрудиция, существенных ошибок в ответах нет. Оценка руководителя и рецензента: «хорошо». **Удовлетворительно:** Имеют место серьёзные нарушения требований,	45, 46, 53, 60, 68	
ОК 08. Использовать средства физической культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и поддержания необходимого уровня физической подготовленности	**Знания.** роли физической культуры в общекультурном, профессиональном и социальном развитии человека; основ здорового образа жизни; условий профессиональной деятельности и зон риска физического здоровья для специальности; средств профилактики перенапряжения **Умения.** использовать физкультурно-оздоровительную деятельность для укрепления здоровья, достижения жизненных и профессиональных целей; применять рациональные приемы двигательных функций в профессиональной деятельности; пользоваться средствами профилактики перенапряжения характерными для данной специальности.			Вопросы к защите ДП (ДР): 2, 8, 10, 17, 18 Вопросы к защите ДП (ДР): 23, 26, 27, 33, 36 Вопросы к защите ДП (ДР): 49, 52, 58, 70	
ОК 09. Использовать информационные технологии в профессиональной деятельности	**Знания.** современные средства и устройства информатизации; порядок их применения и программное обеспечение в профессиональной деятельности **Умения.** применять средства информационных технологий для решения профессиональных задач; использовать современное программное обеспечение			Вопросы к защите ДП (ДР): 7, 9, 11, 12, 13, 14 Вопросы к защите ДП (ДР): 22, 26, 28, 34, 35 Вопросы к защите ДП (ДР): 55, 60, 73, 74, 75, 78	
ОК 10. Пользоваться профессиональной документацией на государственном и иностранном языках	**Знания.** правил построения простых и сложных предложений на профессиональные темы; основных общеупотребительных глаголов (бытовая и профессиональная лексика); лексического минимума, относящегося к описанию предметов, средств и процессов профессиональной деятельности; особенности произношения; правил чтения текстов профессиональной направленности **Умения.** понимать общий смысл четко произнесенных высказываний на известные темы (профессиональные и бытовые), понимать тексты на базовые профессиональные темы; участвовать в диалогах на знакомые общие и профессиональные темы; строить простые высказывания о себе и о своей профессиональной деятельности; кратко обосновывать и объяснить свои действия (текущие и планируемые); писать простые связные сообщения на знакомые или интересующие профессиональные темы			Вопросы к защите ДП (ДР): 7, 28, 36, 37, 38, 42 Вопросы к защите ДП (ДР): 47, 49, 50, 56, 57, 58 Вопросы к защите ДП (ДР): 66, 71, 72, 80, 83	
ОК 11 Использовать знания по финансовой грамотности, планировать	**Знания.** Методы планирования предпринимательской деятельности в профессиональной сфере. **Умения.**			Вопросы к защите ДП (ДР): 7, 28, 36, 37, 38, 42 Вопросы к защите ДП	

предпринимательскую деятельность в профессиональной сфере	Использовать полученные знания и опыт в организации предпринимательской деятельности в профессиональной сфере		предъявляемым к формулировке темы. Имеют место существенные погрешности в обосновании актуальности темы. Отечественная литература. В значительной степени в работе использованы выводы, выдержки из других авторов без ссылок на них. Современные информационные технологий использованы слабо. Допущены серьёзные ошибки в расчётах. Есть отдельные грамматические и стилистические ошибки. Современные пакеты программ используются. Требования, предъявляемые к оформлению ДП (ДР), нарушены. Не соблюден регламент, недостаточно раскрыта тема ДП (ДР). Чертежи не полностью отвечают содержанию доклада, есть ошибки в оформлении и отклонение от ГОСТ, ЕСКД.	(ДР): 47, 49, 50, 56, 57, 58 Вопросы к защите ДП (ДР): 66, 71, 72, 80, 83	
ПК 1.1. Производить установку и настройку компонентов автоматизированных (информационных) систем в защищенном исполнении в соответствии с требованиями эксплуатационной документации	**Уметь**: Обеспечивать работоспособность, обнаруживать и устранять неисправности, осуществлять комплектование, конфигурирование, настройку автоматизированных систем в защищенном исполнении и компонент систем защиты информации автоматизированных систем **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 **Иметь практический опыт:** установка компонентов систем защиты информации автоматизированных информационных систем			Вопросы к защите ДП (ДР): 47, 49, 50, 56, 57, 58 Вопросы к защите ДП (ДР): 66, 71, 72, 80, 83 Вопросы к защите ДП (ДР): 14, 16, 17, 19, 20	Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности приведены в стандарте ДВГУПС СТ 02-28-21 «Формы, периодичность и порядок текущего контроля успеваемости и промежуточной аттестации».
ПК 1.2. Администрировать программные и программно-аппаратные компоненты автоматизированной (информационной) системы в защищенном исполнении	**Уметь**: Производить установку, адаптацию и сопровождение типового программного обеспечения, входящего в состав систем защиты информации автоматизированной системы; организовывать, онфигурировать, производить монтаж, осуществлять диагностику и устранять неисправности компьютерных сетей, работать с сетевыми протоколами разных уровней; **Знать:** теоретические основы компьютерных сетей и их аппаратных компонент, сетевых моделей, протоколов и принципов адресации **Иметь практический опыт:** администрирование автоматизированных систем в защищенном исполнении			Вопросы к защите ДП (ДР): 8, 9, 10, 15, 18 Вопросы к защите ДП (ДР): 21, 22, 23, 24, 25 Вопросы к защите ДП (ДР): 26, 27, 28, 29, 30	
ПК 1.3. Обеспечивать бесперебойную работу автоматизированных (информационных) систем в защищенном исполнении в соответствии с требованиями эксплуатационной документации	**Уметь**: настраивать и устранять неисправности программно-аппаратных средств защиты информации в компьютерных сетях по заданным правилам **Знать**: порядок установки и ввода в эксплуатацию средств защиты информации в компьютерных сетях **Иметь практический опыт**: эксплуатация компонентов систем защиты информации автоматизированных систем, их диагностике, устранении отказов и восстановлении работоспособности.			Вопросы к защите ДП (ДР): 10, 15, 18, 21, 22 Вопросы к защите ДП (ДР): 25, 26, 27, 29, 30 Вопросы к защите ДП (ДР): 31, 32, 38, 39, 40	
ПК 1.4. Осуществлять проверку технического состояния, техническое обслуживание и текущий ремонт, устранять отказы и восстанавливать работоспособность	**Уметь**: обеспечивать работоспособность, обнаруживать и устранять неисправности **Знать:** принципы основных методов организации и проведения технического обслуживания вычислительной техники и других технических средств информатизации **Иметь практический опыт**: диагностика компонентов систем защиты информации автоматизированных систем, устранение отказов и восстановление работоспособности автоматизированных			Вопросы к защите ДП (ДР): 8, 9, 23, 24, 28 Вопросы к защите ДП (ДР): 29, 30, 31, 32, 33 Вопросы к защите ДП (ДР):	

автоматизированных (информационных) систем в защищенном исполнении	(информационных) систем в защищенном исполнении		Знание основного материала. Оценка руководителя и рецензента: «удовлетворительно».	34, 35, 36, 37, 38	
ПК 2.1. Осуществлять установку и настройку отдельных программных, программно-аппаратных средств защиты информации	**Уметь:** устанавливать, настраивать, применять программные и программно-аппаратные средства защиты информации; **Знать:** особенности и способы применения программных и программно-аппаратных средств защиты информации, в том числе, в операционных системах, компьютерных сетях, базах данных **Иметь практический опыт:** установка, настройка программных средств защиты информации		**Неудовлетворительно:** Полное несоответствие темы ДП (ДР) специальности. Актуальность темы не обоснована. Отечественная литература. Полное несоответствие содержания ДП (ДР) поставленным целям или их отсутствие. Недостаточный анализ литературы. Работа в значительной степени не является самостоятельной. Современные информационные технологии, вычислительная техника не были использованы. Использование ЭВМ отсутствует. Много грамматических и стилистических ошибок. Полное невыполнение требований, предъявляемым к оформлению ДП	Вопросы к защите ДП (ДР): 41, 42, 43, 44, 45 Вопросы к защите ДП (ДР): 46, 47, 48, 49, 50 Вопросы к защите ДП (ДР): 51, 52, 53, 54, 55	
ПК 2.2. Обеспечивать защиту информации в автоматизированных системах отдельными программными, программно-аппаратными средствами.	**Уметь**: устанавливать и настраивать средства антивирусной защиты в соответствии с предъявляемыми требованиями; устанавливать, настраивать, применять программные и программно-аппаратные средства защиты информации; **Знать**: особенности и способы применения программных и программно-аппаратных средств защиты информации, в том числе, в операционных системах, компьютерных сетях, базах данных **Иметь практический опыт**: обеспечение защиты автономных автоматизированных систем программными и программно-аппаратными средствами; использование программных и программно-аппаратных средств для защиты информации в сети			Вопросы к защите ДП (ДР): 41, 42, 43, 44, 45 Вопросы к защите ДП (ДР): 46, 47, 48, 49, 50 Вопросы к защите ДП (ДР): 51, 52, 53, 54, 55	
ПК 2.3. Осуществлять тестирование функций отдельных программных и программно-аппаратных средств защиты информации	**Уметь**: диагностировать, устранять отказы, обеспечивать работоспособность и тестировать функции программно-аппаратных средств защиты информации; **Знать**: методы тестирования функций отдельных программных и программно-аппаратных средств защиты информации **Иметь практический опыт**: тестирование функций, диагностика, устранение отказов и восстановление работоспособности программных и программно-аппаратных средств защиты информации			Вопросы к защите ДП (ДР): 42, 43, 44 Вопросы к защите ДП (ДР): 48, 49, 50 Вопросы к защите ДП (ДР): 56, 57, 58	
ПК 2.4. Осуществлять обработку, хранение и передачу информации ограниченного доступа	**Уметь**: применять программные и программно-аппаратные средства для защиты информации в базах данных; проверять выполнение требований по защите информации от несанкционированного доступа при аттестации объектов информатизации по требованиям безопасности информации; применять математический аппарат для выполнения криптографических преобразований; использовать типовые программные криптографические средства, в том числе электронную подпись **Знать**: особенности и способы применения программных и программно-аппаратных средств защиты информации, в том числе, в операционных системах, компьютерных сетях, базах данных;			Вопросы к защите ДП (ДР): 51, 52, 53 Вопросы к защите ДП (ДР): 56, 57, 58 Вопросы к защите ДП (ДР): 59, 60	

	типовые модели управления доступом, средств, методов и протоколов идентификации и аутентификации; основные понятия криптографии и типовых криптографических методов и средств защиты информации **Иметь практический опыт**: решение задач защиты от НСД к информации ограниченного доступа с помощью программных и программно-аппаратных средств защиты информации; применение электронной подписи, симметричных и асимметричных криптографических алгоритмов и средств шифрования данных		(ДР). В докладе не раскрыта тема ДП (ДР), нарушен регламент. Чертежи не соответствуют содержанию доклада, выполнены на низком уровне. Не может ответить на дополнительные вопросы. Оценка руководителя и рецензента: «неудовлетворительно». **2. Демонстрационного экзамена** Количество баллов от 0 до 30 означает оценку «неудовлетворительно». Количество баллов от 31 до 40 означает оценку «удовлетворительно». Количество баллов от 41 до 50 означает оценку «хорошо». Количество баллов от 51 до 60 означает оценку «отлично».		
ПК 2.5. Уничтожать информацию и носители информации с использованием программных и программно-аппаратных средств	**Уметь**: применять средства гарантированного уничтожения информации **Знать**: особенности и способы применения программных и программно-аппаратных средств гарантированного уничтожения информации **Иметь практический опыт**: учёт, обработка, хранение и передача информации, для которой установлен режим конфиденциальности			Вопросы к защите ДП (ДР): 45, 46, 47 Вопросы к защите ДП (ДР): 54, 55, 56, 57 Вопросы к защите ДП (ДР): 58, 59, 60	
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	**Уметь**: устанавливать, настраивать, применять программные и программно-аппаратные средства защиты информации; 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 **Знать**: типовые средства и методы ведения аудита, средств и способов защиты информации в локальных вычислительных сетях, средств защиты от несанкционированного доступа **Иметь практический опыт**: работа с подсистемами регистрации событий; выявление событий и инцидентов безопасности в автоматизированной системе			Вопросы к защите ДП (ДР): 41, 42, 43 Вопросы к защите ДП (ДР): 48, 49, 50 Вопросы к защите ДП (ДР): 58, 59, 60	
ПК 3.1. Осуществлять установку, монтаж, настройку и техническое обслуживание технических средств защиты информации в соответствии с требованиями эксплуатационной документации	**Уметь**: применять технические средства для защиты информации в условиях применения мобильных устройств обработки и передачи данных **Знать:** порядок технического обслуживания технических средств защиты информации; номенклатуру применяемых средств защиты информации от несанкционированной утечки по техническим каналам **Иметь практический опыт**: установка, монтаж и настройка технических средств защиты информации; техническое обслуживание технических средств защиты информации; применение основных типов технических средств защиты информации			Вопросы к защите ДП (ДР): 61, 62, 63, 64, 65 Вопросы к защите ДП (ДР): 71, 72, 73, 74, 75 Вопросы к защите ДП (ДР): 81, 82, 83, 84	
ПК 3.2. Осуществлять эксплуатацию	**Уметь**: применять технические средства для криптографической защиты информации конфиденциального характера; применять технические средства для уничтожения информации и носителей			Вопросы к защите ДП (ДР): 66, 67, 68, 69, 70	

технических средств защиты информации в соответствии с требованиями эксплуатационной документации	информации, защиты информации в условиях применения мобильных устройств обработки и передачи данных; применять нормативные правовые акты, нормативные методические документы по обеспечению 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; порядок устранения неисправностей технических средств защиты информации и организации ремонта технических средств защиты информации; методики инструментального контроля эффективности защиты информации, обрабатываемой средствами вычислительной техники на объектах информатизации; номенклатуру применяемых средств защиты информации от несанкционированной утечки по техническим каналам **Иметь практический опыт**: применение основных типов технических средств защиты информации; выявление технических каналов утечки информации; участие в мониторинге эффективности технических средств защиты информации; диагностика, устранение отказов и неисправностей, восстановление работоспособности технических средств защиты информации			Вопросы к защите ДП (ДР): 76, 77, 78, 79, 80 Вопросы к защите ДП (ДР): 81, 82, 83, 84	
ПК 3.3. Осуществлять измерение параметров побочных электромагнитных излучений и наводок, создаваемых техническими средствами обработки информации ограниченного доступа	**Уметь**: применять технические средства для защиты информации в условиях применения мобильных устройств обработки и передачи данных **Знать:** номенклатуру и характеристики аппаратуры, используемой для измерения параметров ПЭМИН, а также параметров фоновых шумов и физических полей, создаваемых техническими средствами защиты информации; **Иметь практический опыт**: проведение измерений параметров ПЭМИН, создаваемых техническими средствами обработки информации, для которой установлен режим конфиденциальности, при аттестации объектов информатизации по требованиям безопасности информации			Вопросы к защите ДП (ДР): 61, 62, 63, 64, 65 Вопросы к защите ДП (ДР): 68, 69, 70, 71, 72 Вопросы к защите ДП (ДР): 76, 77, 78, 79, 80	
ПК 3.4. Осуществлять измерение параметров фоновых шумов, а также физических полей, создаваемых техническими средствами защиты информации	**Уметь**: применять технические средства для криптографической защиты информации конфиденциального характера **Знать**: номенклатуру применяемых средств защиты информации от несанкционированной утечки по техническим каналам и физической защиты объектов информации **Иметь практический опыт**: проведение измерений параметров фоновых шумов, а также физических полей, создаваемых техническими средствами защиты информации;			Вопросы к защите ДП (ДР): 66, 67, 70 Вопросы к защите ДП (ДР): 73, 74, 75 Вопросы к защите ДП (ДР): 78, 79, 80	
ПК 3.5. Организовывать отдельные работы по физической защите	**Уметь**: применять средства охранной сигнализации, охранного телевидения и систем контроля и управления доступом; применять инженерно-технические средства физической защиты объектов информатизации			Вопросы к защите ДП (ДР): 68, 69, 70 Вопросы к защите ДП	

объектов информатизации	**Знать:** основные принципы действия и характеристики технических средств физической защиты; основные способы физической защиты объектов информатизации; номенклатуру применяемых средств физической защиты объектов информатизации **Иметь практический опыт:** установка, монтаж и настройка, техническое обслуживание, диагностика, устранение отказов и неисправностей, восстановление работоспособности инженерно-технических средств физической защиты			(ДР): 73, 74, 75 Вопросы к защите ДП (ДР): 81, 82, 83, 84	

2. Типовые контрольные задания или иные материалы, необходимые для оценки результатов освоения образовательной программы

2.1 Темы дипломного проекта (работы)

1. Разработка прикладного программного обеспечения деятельности предприятия. (ПМ.01, ПМ.02)
2. Разработка информационной системы предприятия. (ПМ.02, ПМ.03)
3. Разработка справочно-экспертной системы поддержки принятия решений по сопровождению программно-аппаратных комплексов (ПМ.01, ПМ.02, ПМ.03)
4. Разработка программного комплекса для поиска уязвимостей в WEB-приложениях. (ПМ.01, ПМ.02)
5. Разработка профиля защиты информации в информационной системе (ПМ.01, ПМ.02, ПМ.03)
6. Обеспечение информационной безопасности в распределенных информационных системах с использованием облачного сервиса (ПМ.01, ПМ.02, ПМ.03)
7. Разработка профиля защиты информации (ПМ.02, ПМ.03, ПМ.04)
8. Разработка информационной системы электронного голосования на базе «слепой» электронной цифровой подписи (ПМ.01, ПМ.02, ПМ.03)
9. Защита баз данных от инсайдерских атак (ПМ.02, ПМ.03)
10. Защита информации в автоматизированных системах управления производственными и технологическими процессами (ПМ.01, ПМ.02, ПМ.03, ПМ.04)
11. Защита информации в беспроводных сетях стандарта IEEE802.11 (ПМ.02, ПМ.03)
12. Разработка профиля защиты персональных данных (ПМ.01, ПМ.02, ПМ.04)
13. Разработка приложения для фиксации и контроля исходного состояния программного обеспечения (ПМ.01, ПМ.02, ПМ.04)
14. Разработка программно-методического комплекса оценки рисков информационной безопасности (ПМ.01, ПМ.02, ПМ.03, ПМ.04)
15. Разработка сервиса аутентификации по токенам на примере брандмауэра (ПМ.02, ПМ.03)

2.2 Вопросы к защите ДП (ДР)

1. Перечислить и охарактеризовать основные блоки утилиты BIOS SETUP. (ОК 01, ОК 04, ОК 07, ПК 1.1)
2. Описать структурную схему/архитектуру современной операционной системы Windows. (ОК 01, ОК 02, ОК 04, ОК 08, ПК 1.1)
3. Перечислить и охарактеризовать функции ядра операционной системы Windows. (ОК 02, ОК 03, ПК 1.1)
4. Описать структурную схему/архитектуру операционной системы Linux. (ОК 02, ОК 04, ПК 1.1)
5. Дать определение понятию «процесс». Привести классификации процессов. (ОК 01, ОК 07, ПК 1.1)
6. Перечислить и охарактеризовать состояния процесса. Привести диаграмму переходов состояний процесса. (ОК 01, ОК 06, ПК 1.1)
7. Перечислить и охарактеризовать типы адресов и виды адресного пространства вычислительной системы (ОК 02, ОК 09, ОК 10, ОК 11, ПК 1.1)

8. Перечислить и охарактеризовать механизмы реализации виртуальной памяти. (ОК 02, ОК 08, ПК 1.1, ПК 1.2, ПК 1.4)

9. Описать технологию настройки файла подкачки в операционной системе Windows. (ОК 01, ОК 07, ОК 09, ПК 1.2, ПК 1.4)

10. Спектры сигналов. (ОК 05, ОК 08, ПК 1.2, ПК 1.3)

11. Принципы многоканальной связи. (ОК 02, ОК 09, ПК 1.1)

12. Модуляция сигналов ЭС. (ОК 03, ОК 09, ПК 1.1)

13. Среды передачи информации. (ОК 04, ОК 09, ПК 1.1)

14. Классификация и функции сетей. (ОК 05, ОК 09, ПК 1.1)

15. Концентраторы. (ОК 01, ОК 06, ПК 1.2, ПК 1.3)

16. Мосты. (ОК 06, ОК 07, ПК 1.1)

17. Коммутаторы. (ОК 06, ОК 08, ПК 1.1)

18. Сетевые карты. (ОК 05, ОК 06, ОК 08, ПК 1.2, ПК 1.3)

19. Виды локальных сетей. (ОК 05, ОК 07, ПК 1.1)

20. Радиорелейные линии связи. (ОК 06, ОК 07, ПК 1.1)

21. Языки гипертекстовой разметки. (ОК 01, ОК 03, ПК 1.2, ПК 1.3)

22. Технология Fast Ethernet. Отличия от классического Ethernet. (ОК 03, ОК 04, ОК 09, ПК 1.2, ПК 1.3)

23. Работа коммутаторов в полудуплексном и полнодуплексном режимах. (ОК 02, ОК 08, ПК 1.2, ПК 1.4)

24. Технологии Gigabit Ethernet и 10Gigabit Ethernet. (ОК 01, ОК 02, ОК 04, ПК 1.2, ПК 1.4)

25. Сетевые утилиты командной строки Windows (ОК 05, ОК 07, ПК 1.2, ПК 1.3)

26. PHP. Обзор возможностей. Краткая характеристика. (ОК 07, ОК 08, ОК 09, ПК 1.2, ПК 1.3)

27. XML. Обзор возможностей. Краткая характеристика. (ОК 06, ОК 08, ПК 1.2, ПК 1.3)

28. Серверное программное обеспечение. (ОК 09, ОК 10, ОК 11, ПК 1.2, ПК 1.4)

29. Инструментальные средства создания приложений PHP. (ОК 01, ОК 05, ПК 1.2, ПК 1.3, ПК 1.4)

30. Инновационные технологии сети Internet. (ОК 02, ПК 1.2, ПК 1.3, ПК 1.4)

31. Основы построения серверной части программного обеспечения. (ОК 02, ОК 03, ОК 07, ПК 1.3, ПК 1.4)

32. Шифры потока и блочные шифры. Основные принципы. Определения. (ОК 03, ОК 04, ОК 05, ПК 1.3, ПК 1.4)

33. Современные блочные шифры. Основные принципы. Определения. (ОК 06, ОК 08, ПК 1.4)

34. Понятие: подстановка, транспозиция и полноразмерный ключевой шифр. (ОК 06, ОК 09, ПК 1.4)

35. Генераторы псевдослучайных чисел. (ОК 07, ОК 09, ПК 1.4)

36. Основные принципы использования генераторов псевдослучайных чисел при потоковом шифровании. (ОК 08, ОК 10, ОК 11, ПК 1.4)

37. Алгебраические структуры. Группа. Циклическая группа. Кольцо. Поле. (ОК 02, ОК 10, ОК 11, ПК 1.4)

38. Конечные поля. Поля Галуа. Полиномы. (ОК 01, ОК 10, ОК 11, ПК 1.3, ПК 1.4)

39. Понятие хеш-функции. Основные требования, предъявляемые к криптографическим хеш-функциям. (ОК 01, ОК 02, ПК 1.3)

40. Компоненты современного блочного шифра. (ОК 01, ОК 02, ОК 03, ОК 05, ПК 1.3)

41. Понятие: P-блоки и S-блоки. Алгоритм. Виды. Назначение. Раунды. (ОК 02, ОК 04, ОК 06, ПК 2.1, ПК 2.2, ПК 2.6)

42. Компоненты современного блочного шифра. Операция циклического сдвига. Операция замены. (ОК 06, ОК 10, ОК 11, ПК 2.1, ПК 2.2, ПК 2.3, ПК 2.6)

43. Компоненты современного блочного шифра. Понятие: P-блоки и S-блоки. Алгоритм. Виды. Назначение. Раунды. (ОК 07, ПК 2.1, ПК 2.2, ПК 2.3, ПК 2.6)

44. Компоненты современного блочного шифра. Операция циклического сдвига. Операция замены. (ОК 01, ОК 03, ОК 07, ПК 2.1, ПК 2.2, ПК 2.3)

45. Разбиение и объединение. Рассеивание и перемешивание. (ОК 03, ОК 07, ПК 2.1, ПК 2.2, ПК 2.5)

46. Шифр Файстеля и шифр не-Файстеля. Основная идея. Алгоритм. Криптоанализ. (ОК 07, ПК 2.1, ПК 2.2, ПК 2.5)

47. Современные шифры потока. Основные принципы. Определения. (ОК 02, ОК 10, ОК 11, ПК 2.1, ПК 2.2, ПК 2.5)

48. Стандарт шифрования данных DES (DATA ENCRYPTION STAND-ARD). Основная идея. Алгоритм. Криптоанализ. (ОК 03, ПК 2.1, ПК 2.2, ПК 2.3, ПК 2.6)

49. Стандарт шифрования данных AES (ADVANCED ENCRYPTION STANDARD). Основная идея. Алгоритм. Криптоанализ. (ОК 05, ОК 08, ОК 10, ОК 11, ПК 2.1, ПК 2.2, ПК 2.3, ПК 2.6)

50. Виды, источники и носители защищаемой информации. (ОК 04, ОК 10, ОК 11, ПК 2.1, ПК 2.2, ПК 2.3, ПК 2.6)

51. Прослушивание информации направленными микрофонами. (ОК 05, ОК 06, ПК 2.1, ПК 2.2, ПК 2.4)

52. Электронные стетоскопы. (ОК 06, ОК 08, ПК 2.1, ПК 2.2, ПК 2.4)

53. Лазерные системы подслушивания. (ОК 07, ПК 2.1, ПК 2.2, ПК 2.4)

54. Гидроакустические преобразователи. (ОК 01, ОК 05, ПК 2.1, ПК 2.2, ПК 2.5)

55. Системы защиты информации от утечки по вибрационному каналу. (ОК 05, ОК 09, ПК 2.1, ПК 2.2, ПК 2.5)

56. Структура канала утечки информации. Характеристика каналов утечки информации. (ОК 06, ОК 10, ОК 11, ПК 2.3, ПК 2.4, ПК 2.5)

57. Классификация существующих физических полей и технических каналов утечки информации. (ОК 03, ОК 10, ОК 11, ПК 2.3, ПК 2.4, ПК 2.5)

58. Радиоэлектронные каналы утечки информации, характеристика. (ОК 08, ОК 10, ОК 11, ПК 2.3, ПК 2.4, ПК 2.5, ПК 2.6)

59. Оптический канал утечки информации, характеристика. (ОК 04, ПК 2.4, ПК 2.5, ПК 2.6)

60. Технические средства акустической разведки. (ОК 07, ОК 09, ПК 2.4, ПК 2.5, ПК 2.6)

61. Технические средства для уничтожения информации и носителей информации, порядок применения. (ОК 01, ОК 03, ОК 05, ПК 3.1, ПК 3.3)

62. Этапы эксплуатации технических средств защиты информации. (ОК 05, ПК 3.1, ПК 3.3)

63. Установка и настройка технических средств защиты информации. (ОК 02, ОК 04, ПК 3.1, ПК 3.3)

64. Классификация демаскирующих признаков (ОК 06, ПК 3.1, ПК 3.3)

65. Телевизионные системы наблюдения. Приборы ночного видения. (ОК 05, ПК 3.1, ПК 3.3)

66. Классификация и принципы действия акустических преобразователей. (ОК 03, ОК 10, ОК 11, ПК 3.2, ПК 3.4)

67. Побочные высокочастотные и низкочастотные излучения технических средств. (ОК 04, ПК 3.2, ПК 3.4)

68. Утечка информации по цепям электропитания и заземления (ОК 07, ПК 3.2, ПК 3.3, ПК 3.5)

69. Виды угроз безопасности информации. (ОК 03, ОК 06, ПК 3.2, ПК 3.3, ПК 3.5)

70. Основные задачи и типовая структура разведки. (ОК 08, ПК 3.2, ПК 3.3, ПК 3.4, ПК 3.5)

71. Классификация органов технической разведки. (ОК 03, ОК 10, ОК 11, ПК 3.1, ПК 3.3)

72. Утечка информации. Типовая структура технического канала утечки информации. (ОК 10, ОК 11, ПК 3.1, ПК 3.3)

73. Классификация технических каналов утечки информации. (ОК 03, ОК 09, ПК 3.1, ПК 3.4, ПК 3.5)

74. Средства противодействия утечки информации по оптическим каналам. (ОК 09, ПК 3.1, ПК 3.4, ПК 3.5)

75. Структура и виды радиоэлектронных каналов утечки информации. (ОК 09, ПК 3.1, ПК 3.4, ПК 3.5)

76. Классификация и особенности распространения радиоволн. (ОК 04, ПК 3.2, ПК 3.3)

77. Распространение информативных сигналов в радиоэлектронных каналах утечки информации. (ОК 04, ПК 3.2, ПК 3.3)

78. Классификация помех. (ОК 09, ПК 3.2, ПК 3.3, ПК 3.4)

79. Характер распространения звука в различных средах. Реверберация. (ОК 01, ПК 3.2, ПК 3.3, ПК 3.4)

80. Структура акустического канала утечки информации. (ОК 03, ОК 10, ОК 11, ПК 3.2, ПК 3.3, ПК 3.4)

81. Классификация методов инженерно-технической защиты информации. (ОК 04, ПК 3.1, ПК 3.2, ПК 3.5)

82. Характеристика методов физической защиты информации. (ОК 03, ОК 04, ПК 3.1, ПК 3.2, ПК 3.5)

83. Структура системы инженерной защиты и охраны объектов. (ОК 01, ОК 10, ОК 11, ПК 3.1, ПК 3.2, ПК 3.5)

84. Структура комплексов управления и доступом людей и транспорта. (ОК 04, ПК 3.1, ПК 3.2, ПК 3.5)

2.3 Структура задания для процедуры демонстрационного экзамена

Задания демонстрационного экзамена для обучающихся, участвующих в процедурах итоговой (государственной итоговой) аттестации в образовательной организации, реализующей программы среднего профессионального образования разрабатываются, исходя из требований, приведенных в данных оценочных материалах для проведения итоговой (государственной итоговой) аттестации по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем.

Программа итоговой (государственной итоговой) аттестации, задания, критерии их оценивания, продолжительность демонстрационного экзамена утверждаются образовательной организацией и доводятся до сведения обучающихся не позднее, чем за шесть месяцев до начала итоговой (государственной итоговой) аттестации.

Рабочие места для выполнения демонстрационного экзамена каждому обучающемуся определяются методом случайного выбора в начале демонстрационного экзамена. Время, отводимое на выполнение заданий демонстрационного экзамена, определено в данных оценочных материалах.

3. Типовые задания для демонстрационного экзамена

Содержанием заданий являются работы по анализу и защите сетевого трафика, установке, конфигурированию, компрометации, межсетевого взаимодействия и туннелирования. Обучающиеся получают задания с необходимой сопроводительной документацией. Задания должны выполняться помодульно в утвержденном порядке.

Окончательные аспекты критериев оценки уточняются экспертами. Оценка производится по результатам выполнения каждого модуля демонстрационного экзамена, а в отношении соблюдения правил охраны труда, техники безопасности, электробезопасности, технологии выполнения работ в процессе выполнения задания.

Перечень знаний, умений, навыков в соответствии со Спецификацией стандарта компетенции № F7 «Корпоративная защита от внутренних угроз информационной безопасности» («Молодые профессионалы» Standards Specifications, WSSS).

Таблица 1.

Раздел WSSS	Наименование раздела WSSS	Важность (%)
1	Организация работы и управление	5
2	Установка, конфигурирование и устранение неисправностей	14
5	Технологии анализа и защиты сетевого трафика	41

Форма участия: Индивидуальная

Общее максимально возможное количество баллов задания по всем критериям оценки составляет 60.

Таблица 2.

№ п/п	Критерий	Модуль, в котором используется критерий	Проверяемые разделы WSSS	Баллы	
				Объек-тивная	Общая
1	A. Организация работы и управление	Все модули	1	5	5
3	C. Технологии анализа и защиты сетевого трафика, установка и конфигурирование	1. Технологии анализа и защиты сетевого трафика, установка и конфигурирование	2. Установка, конфигурирование и устранение неисправностей 5. Технологии анализа и защиты сетевого трафика	29	29
5	D. Технологии анализа и защиты сетевого трафика, компрометация, межсетевое взаимодействие и туннелирование	2. Технологии анализа и защиты сетевого трафика, компрометация, межсетевое взаимодействие и туннелирование	2. Установка, конфигурирование и устранение неисправностей 5. Технологии анализа и защиты сетевого трафика	26	26
Итого =				60	60

Минимальное количество экспертов, участвующих в оценке демонстрационного экзамена по компетенции № F7 «Корпоративная защита от внутренних угроз информационной безопасности» — 3 чел.

Минимальное количество рабочих мест составляет 5.

Модули задания, критерии оценки и необходимое время

Таблица 3.

№ п/п	Критерий	Модуль, в котором используется критерий	Время на выполнение модуля	Проверяемые разделы WSSS	Баллы	
					Объективная	Общая
1	A. Организация работы и управление	Все	—	1	5	5
2	C. Технологии анализа и защиты сетевого графика, установка и конфигурирование	1. Технологии анализа и защиты сетевого трафика, установка и конфигурирование	3 часа	2, 5	29	29
3	D. Технологии анализа и защиты сетевого трафика, компрометация, межсетевое взаимодействие и туннелирование	2. Технологии анализа и защиты сетевого трафика, компрометация, межсетевое взаимодействие и туннелирование	2,5 часа	2, 5	26	26
Итого =					60	60

Модуль 1: Технологии анализа и защиты сетевого трафика, установка и конфигурирование.

Участник выполняет следующие действия с использованием VPN-систем корпоративного класса (Virtual Private Network):

– Развёртывание, настройка и проверка работоспособности VPN-сети на существующей и вычислительной инфраструктуре.

– Администрирование узлов и пользователей.

– Внедрение централизованных политик безопасности. Обеспечение защиты рабочих мест.

При выполнении задания необходимо:

– Настроить сетевую инфраструктуру.

– Развернуть структуру защищенной сети согласно схеме с помощью дистрибутивов.

– Произвести настройку пользователей и узлов защищенной сети.

– Установить ключевую информацию.

– Произвести проверку связи между узлами защищенной сети.

– Произвести модификацию защищенной сети.

– Составить отчет о работе.

При работе могут использоваться различные операционные системы.

Модуль 2: Технологии анализа и защиты сетевого трафика, компрометация, межсетевое взаимодействие и туннелирование.

Участник выполняет следующие действия с использованием VPN-систем корпоративного класса (Virtual Private Network):

– Развёртывание, настройка и проверка работоспособности VPN-сети на существующей и вычислительной инфраструктуре во второй сети

– Выполнение компрометации узлов, ключей, пользователей. Восстановление связи. Обновление ключевой информации.

– Организацию межсетевого взаимодействия и туннелирования.

При выполнении задания необходимо:

– Произвести компрометацию ключей пользователей сети и восстановить работоспособность

– Настроить сетевую инфраструктуру второй сети

– Развернуть структуру защищенной сети согласно схеме с помощью дистрибутивов

– Установить межсетевое взаимодействие между разными сетями

– Произвести перенастройку пользователей и узлов защищенной сети

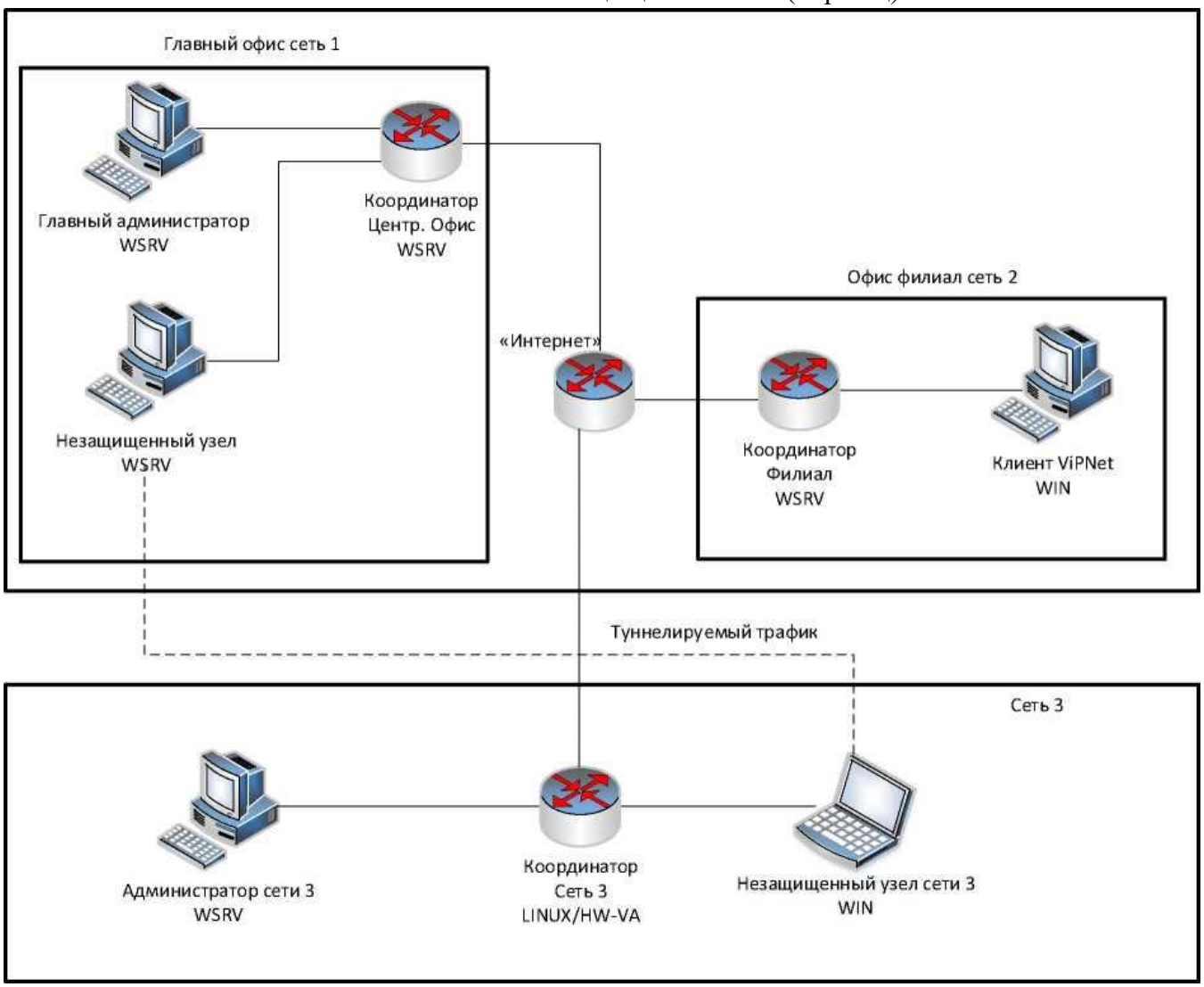
– Произвести проверку связи между узлами различных защищенных сетей

– Произвести настройку туннелирования между незащищенными узлами поверх защищенной сети

– Составить отчет о работе

При работе могут использоваться различные операционные системы.

Типовая схема защищенной сети (образец):



Примерный план работы Центра проведения демонстрационного экзамена по компетенции «Корпоративная защита от внутренних угроз информационной безопасности»

Подготовительный день	Примерное время	Мероприятие
	08:00	Получение главным экспертом задания демонстрационного экзамена
	08:00-09:00	Проверка готовности проведения демонстрационного экзамена, заполнение Акта о готовности / неготовности
	09:00-09:15	Распределение обязанностей по проведению экзамена между членами Экспертной группы, заполнение Протокола о распределении
	09:15-09:30	Инструктаж Экспертной группы по охране труда и технике безопасности, сбор подписей в Протоколе об ознакомлении
	09:30-09:45	Регистрация участников демонстрационного экзамена
	09:45-10:15	Инструктаж участников по охране труда и технике безопасности, сбор подписей в Протоколе об ознакомлении
	10:15-12:00	Распределение рабочих мест (жеребьевка) и ознакомление участников с рабочими местами, оборудованием, графиком работы, иной документацией и заполнение Протокола
День 1	08:50-09:10	Ознакомление с заданием и правилами
	09:10-09:30	Брифинг
	09:30-12:30	Выполнение модуля 1
	12:30-13:30	Обед
	13:30-16:00	Выполнение модуля 2
	16:00-19:00	Работа экспертов, заполнение форм и оценочных ведомостей
	19:00-20:00	Подведение итогов, внесение главным экспертом баллов в CIS, блокировка, сверка баллов, заполнение итогового протокола

Порядок перевода баллов в систему оценивания.

Перевод в оценку баллов, полученных за демонстрационный экзамен, рекомендуется проводить следующим образом:

– Количество баллов от 0 до 30 означает оценку «неудовлетворительно».
– Количество баллов от 31 до 40 означает оценку «удовлетворительно».
– Количество баллов от 41 до 50 означает оценку «хорошо».
– Количество баллов от 51 до 60 означает оценку «отлично».

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

Целью итоговой (государственной итоговой) аттестации в форме защиты демонстрационного экзамена и дипломного проекта (работы) является оценка теоретических знаний обучающегося, способности применять эти знания при решении конкретных практических задач, навыков ведения самостоятельной работы, применения методик исследования и эксперимента при решении разрабатываемых в ДП (ДР) проблем и вопросов в соответствии с требованиями ФГОС и образовательной программы в разделах, характеризующих области, объекты и виды профессиональной деятельности обучающегося по специальности 10.02.05 «Обеспечение информационной безопасности автоматизированных систем»

Регламентирует проведение процедуры итоговой (государственной итоговой) стандарт ДВГУПС СТ 02-13-16 «Итоговая (государственная итоговая) аттестация обучающихся по основным профессиональным образовательным программам.

Защита ДП (ДР) проводится в установленное время на заседании ГЭК по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем. Кроме членов

экзаменационной комиссии на защите ДП (ДР) желательно присутствие руководителя, консультантов и рецензента, в случае проведения открытой защиты ДП (ДР) также возможно присутствие других обучающихся, преподавателей и администрации.

Порядок защиты ДП (ДР) на заседании ГЭК:

Перед началом защиты секретарь ГЭК даёт краткую информацию по личному делу обучающегося.

Защита начинается с доклада обучающего по теме ДП (ДР). Продолжительность доклада зависит от уровня образовательной профессиональной программы, завершающим этапом которой является ДП (ДР). На доклад по ДП (ДР) отводится 10-12 минут.

Во вступительной части доклада необходимо очень четко сформулировать цель, поставленные задачи ДП (ДР) и обосновать актуальность избранной темы, кратко осветить состояние вопроса (20 % отведенного времени).

В основной части доклада нужно кратко рассмотреть возможные подходы к решению поставленной задачи и более подробно представить подход, выбранный автором ДП (ДР), объяснить, как решалась задача, и обосновать правильность принимаемого решения, обращая особое внимание на наиболее важные разделы и интересные результаты, критические сопоставления и оценки, практическую ценность материала дипломного проекта.

Заключительная часть доклада строится по тексту заключения ДП (ДР), перечисляются общие выводы из её текста без повторения частных обобщений, сделанных при характеристике глав основной части, собираются воедино основные рекомендации (10 % отведенного времени). Обучающемуся рекомендуется излагать основное содержание своей ДП (ДР) свободно, не читая письменного текста.

Структура доклада может конкретизироваться и изменяться в зависимости от особенностей и содержания работы, полученных результатов и представленных демонстрационных материалов.

Рекомендуется в процессе доклада использовать заранее подготовленный наглядный графический материал, иллюстрирующий основные положения работы (чертежи, выполненные в соответствии с ЕСКД, таблицы, схемы). Все материалы, выносимые на наглядную графику, должны быть оформлены так, чтобы обучающийся мог демонстрировать их без особых затруднений, и они были видны всем присутствующим в аудитории. В среднем насыщенность одного плаката (слайда) информацией должна быть эквивалентна 10-15 строкам текста, не более. Плакаты (слайды) нумеруются в левом верхнем углу. Весь плакат (слайд) или его части должны иметь заголовок-название: Постановка задачи, Структурная схема системы и т.д. Обычно плакаты (слайды) соответствуют разделам или подразделам ДП (ДР). Число слайдов должно быть достаточным для полного представления ДП (ДР), но не превышать 20. Для удобства работы членов ГЭК необходимо подготовить раздаточный материал, дублирующий представляемые слайды.

После завершения доклада члены ГЭК задают обучающемуся вопросы, как непосредственно связанные с темой ДП (ДР), так и близко к ней относящиеся. При ответах на вопросы обучающийся имеет право пользоваться своей работой.

После ответов обучающегося на вопросы слово предоставляется руководителю. В конце своего выступления руководитель даёт свою оценку ДП (ДР). В случае отсутствия последнего на заседании ГЭК его отзыв зачитывает секретарь ГЭК.

После выступления руководителя слово предоставляется рецензенту. В конце своего выступления рецензент даёт свою оценку работе. В случае отсутствия последнего на заседании ГЭК его отзыв зачитывает секретарь ГЭК.

После выступления рецензента начинается обсуждение работы или дискуссия. В дискуссии могут принять участие как члены ГЭК, так и присутствующие заинтересованные лица. Продолжительность обсуждения работы и дискуссии не должна превышать 7-10 минут. В случае спорной ситуации отведённое время регламентируется председателем ГЭК (или его заместителем в случае отсутствия председателя ГЭК).

После окончания дискуссии обучающемуся может быть предоставлено заключительное слово. В своём заключительном слове обучающийся должен ответить на замечания рецензента,

соглашаясь с ними или давая обоснованные возражения. Время, отводимое для заключительного слова и ответов на вопросы, регламентируется 3-5 минутами.

Решения ГЭК о результатах защиты ВКР в виде дипломной работы (дипломного проекта) и демонстрационного экзамена, о присвоении квалификации и выдаче диплома принимаются на закрытых заседаниях простым большинством голосов членов комиссии при обязательном присутствии председателя комиссии (или его заместителя, в случае отсутствия председателя ГЭК и оформляются протоколами. При равном числе голосов председательствующий обладает правом решающего голоса. Особые мнения членов комиссии фиксируются в протоколе комиссии. Протоколы заседаний ГЭК оформляются в день проведения заседания комиссии, подписываются председателем (или его заместителем в случае отсутствия председателя ГЭК и секретарём ГЭК, и хранятся согласно номенклатуре дел. К протоколам приобщаются материалы членов комиссии.

Требования к содержанию, объему и структуре демонстрационного экзамена образовательная организация определяет самостоятельно в части выбора компетенций, комплектов оценочной документации.

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».

Результаты победителей и призеров чемпионатов профессионального мастерства, проводимых союзом либо международной организацией «Молодые профессионалы», осваивающих образовательные программы среднего профессионального образования, засчитываются в качестве оценки «отлично» по демонстрационному экзамену.

Условием учёта результатов, полученных в конкурсных процедурах, является признанное образовательной организацией содержательное соответствие компетенции результатам освоения образовательной программы в соответствии с ФГОС СПО, а также отсутствие у студента академической задолженности. Перечень чемпионатов утвержден приказом союза.

Результаты итоговой (государственной итоговой) аттестации определяются оценками "отлично", "хорошо", "удовлетворительно", "неудовлетворительно" и объявляются в тот же день после оформления в установленном порядке протоколов заседаний государственных экзаменационных комиссий и фиксируются в учебной карточке и зачетной книжке студента.

ГЭК принимает решение о выдаче диплома с отличием выпускнику, достигшему особых успехов в освоении ОПОП, если будут соблюдены следующие условия:

– все указанные в приложении к диплому оценки по дисциплинам (модулям), практикам, оценки за курсовые работы (проекты) являются оценками "отлично" и "хорошо";

– все оценки по результатам итоговой (государственной итоговой) аттестации являются оценками "отлично";

– количество указанных в приложении к диплому оценок "отлично", включая оценки по результатам итоговой (государственной итоговой) аттестации, составляет не менее 75% от общего количества оценок, указанных в приложении к диплому.

Студенты, не защитившие ВКР по неуважительной причине в установленный для них срок, отчисляются как не выполнившие обязанности по добросовестному освоению образовательной программы и выполнению учебного плана. Таким студентам выдается справка об обучении и предоставляется право повторной защиты не ранее чем через шесть месяцев.

Оглашение итоговых оценок осуществляется по завершении заседания Государственной экзаменационной комиссии.

Регламентирующие документы:

4.1. Программа ГИА

4.2. Методические рекомендации по разработке дипломных проектов (дипломных работ) для специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем

4.3. Федеральные законы и нормативные документы:

- Федеральный государственный образовательный стандарт среднего профессионального образования по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем утвержденного приказом Министерства образования и науки Российской Федерации от 09 декабря 2016 года № 1553.

- Приказ Министерства образования и науки РФ от 08 октября 2021 г. № 800 «Об утверждении порядка проведения государственной итоговой аттестации по образовательным программам среднего профессионального образования, утвержденный приказом Министерства образования и науки РФ».

- Стандарт ДВГУПС СТ 02-16-17 «Требования к содержанию и оформлению выпускных квалификационных работ».

- Стандарт ДВГУПС СТ 02-13-16 «Итоговая (государственная итоговая) аттестация студентов по основным профессиональным образовательным программа».

- Стандарт ДВГУПС СТ 02-28-21 «Формы, периодичность и порядок текущего контроля успеваемости и промежуточной аттестации».

- Стандарт ДВГУПС СТ 02-37-19 «Проектирование основной профессиональной образовательной программы направления подготовки (специальности) и ее элементов на основе федерального государственного образовательного стандарта»

4.4. Заключение председателя государственной экзаменационной комиссии о соблюдении процедуры проведения ГИА.