МИНОБРНАУКИ РОССИИ

федеральное государственное бюджетное образовательное учреждение высшего образования

«Кузбасский государственный технический университет имени Т.Ф. Горбачева»

Филиал КузГТУ в г. Новокузнецке

ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ

Сертификат: 65A182AF55E85519218FE36C1C7FB48A
Владелец: Евсина Татьяна Алексеевна
Действителен: с 16.11.2022 до 09.02.2024

УТВЕРЖДАЮ
Директор филиала КузГТУ
_____ Т.А. Евсина
«29» мая 2023 г.

Фонд оценочных средств Государственной 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
основного общего образования – 3 года 10 месяцев

Новокузнецк 2023 г.

1. ПАСПОРТ ФОНДА ОЦЕНОЧНЫХ СРЕДСТВ ГОСУДАРСТВЕННОЙ ИТОГОВОЙ АТТЕСТАЦИИ

1.1. Область применения

Фонд оценочных средств (далее – ФОС) для проведения государственной итоговой аттестации (далее – ГИА) 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 ГИА 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 ГИА

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:14995 Наладчик технологического оборудования.

В результате ГИА 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.	**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 информационных систем. **уметь:** – обеспечивать работоспособность, обнаруживать и устранять неисправности, осуществлять комплектование, конфигурирование, настройку автоматизированных систем в защищенном исполнении и компонент систем защиты информации автоматизированных систем; – производить установку, адаптацию и сопровождение типового программного обеспечения, входящего в состав систем защиты информации автоматизированной системы; – организовывать, конфигурировать, производить	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.	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. **знать:** – состав и принципы работы автоматизированных систем, операционных систем и сред; – принципы разработки алгоритмов программ, основных приемов программирования; – модели баз данных; – принципы построения, физические основы работы периферийных устройств, основных методов организации и проведения технического обслуживания вычислительной техники и других технических средств информатизации; – теоретические основы компьютерных сетей и их аппаратных компонент, сетевых моделей, протоколов и принципов адресации; – порядок установки и ввода в эксплуатацию средств защиты информации в компьютерных сетях.	
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.		
ОК 01.	Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам.	**иметь практический опыт:** – 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. **уметь:**	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.	– 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. **знать:** – 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.	– 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.	**иметь практический опыт:** – 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. **уметь:** – применять средства охранной сигнализации,	Демонстрационный экзамен; 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.	охранного телевидения и систем контроля и управления доступом; – применять технические средства для криптографической защиты информации конфиденциального характера; – применять технические средства для уничтожения информации и носителей информации, защиты информации в условиях применения мобильных устройств обработки и передачи данных; – применять инженерно-технические средства физической защиты объектов информатизации. **знать:** – физические основы, структуру и условия формирования технических каналов утечки информации, способы их выявления и методы оценки опасности, классификацию существующих физических полей и технических каналов утечки информации; – номенклатуру и характеристики аппаратуры, используемой для измерения параметров побочных электромагнитных излучений и наводок (далее - ПЭМИН), а также параметров фоновых шумов и физических полей, создаваемых техническими средствами защиты информации; – основные принципы действия и характеристики, порядок технического обслуживания, устранение неисправностей и организацию ремонта технических средств защиты информации;	
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 3.1.	Осуществлять установку, монтаж, настройку и техническое обслуживание технических средств защиты информации в соответствии с требованиями эксплуатационной		

	документации.	– 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:** – 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.	– 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. **уметь:** – подключать и настаивать 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 04.	Работать в коллективе и команде, эффективно взаимодействовать с коллегами, руководством, клиентами.		
ОК 05.	Осуществлять устную и письменную коммуникацию на государственном языке с учетом особенностей социального и культурного контекста.		
ОК 06.	Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных общечеловеческих ценностей, применять стандарты антикоррупционного поведения.		
ОК 07.	Содействовать сохранению окружающей среды, ресурсосбережению, эффективно действовать в чрезвычайных ситуациях.		
ОК 08.	Использовать средства физической культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и поддержания необходимого уровня физической подготовленности.		
ОК 09.	Использовать информационные технологии в профессиональной деятельности.		

ОК 10.	Пользоваться профессиональной документацией на государственном и иностранном языках.	– 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	– 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**.** **знать:** – 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	
ДПК 5.2	Документирование результатов контроля, включая подготовку протоколов или ввод данных в автоматизированные информационные системы		

		– 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 оборудованием и оргтехникой	

2. СИСТЕМА КОНТРОЛЯ И ОЦЕНКИ ОСВОЕНИЯ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

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

- демонстрационный экзамен по КОД: 10.02.01-2023;
- подготовку и защиту выпускной квалификационной работы (дипломная работа).

2.1. Демонстрационный экзамен по КОД: 10.02.05-2023

Демонстрационный экзамен по КОД: 10.02.05-2023 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 защищенномисполнении;
- 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: 10.02.05-2023

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

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 уведомитьглавного эксперта об участии в проведении демонстрационного экзамена тьютора (ассистента).

Образец задания

Описание общих требований

В компании «SoC» возникла необходимость внедрения DLP системы для лучшей защиты корпоративной информации и предотвращения утечек данных. Вам необходимо установить и настроить компоненты системы в соответствии с выданным заданием. Серверные компоненты установлены, сетевые интерфейсы настроены.

Подготовлены следующие виртуальные машины для дальнейшей работы:

Контроллер домена;

DLP сервер установлен, активирована лицензия, есть LDAP синхронизация;

Виртуальная машина с установленным сервером агентского мониторинга;

Виртуальная машина «нарушителя» в домене (1 шт).

В компании развернут домен со всеми сотрудниками с указанием ФИО, должности и контактов.

При выполнении заданий можно пользоваться разрешенными справочными ресурсами в сети Интернет и/или документацией на компьютерах и/или в общем сетевом каталоге. Все логины, пароли, сетевые настройки и прочее указаны в дополнительной карточке задания.

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

При выполнении задания модуля необходимо достичь следующих целей:

Настроенный контроллер домена.

Работоспособный сервер мониторинга сетевого трафика.

Установленный и работоспособный сервер агентского мониторинга.

Установленные и работоспособные агент мониторинга на клиентском устройстве.

Если в задании указано сделать скриншот, необходимо называть его по номеру задания, например, «Задание_5_копирование.jpg». Все скриншоты и отчеты сохраняются на рабочий стол физического компьютера в один каталог или документ (важно соблюдать последовательность заданий). При создании снимков экрана необходимо делать либо полный снимок экрана, либо целого окна. Не стоит вырезать только маленький кусочек (например, сообщение о событии), т. к. это не будет являться явным подтверждением работы.

Допускается последующее выделение рамкой, стрелкой или иным способом результата работы.

Задание модуля 1:

Задача 1: Настройка контроллера домена

Создать подразделение “DemoExam” в контроллере домена.

Внутри созданного подразделения “DemoExam” необходимо создать и настроить следующих доменных пользователей с соответствующими правами:

Логин: web-officer, пароль: xxXX3344, права пользователя домена;

Логин: ldap-sync, пароль: xxXX3344, права пользователя домена;

Логин: device-officer, пароль: xxXX3344, права администратора домена илокального администратора;

Логин: violator, пароль xxXX3344, права пользователя домена.

Задача 2: Настройка DLP сервера

DLP-сервер контроля сетевого трафика уже предустановлен, но не настроен:

необходимо узнать IP-адрес сервера через локальную консоль виртуальной машины и проверить настройки DNS на сервере для корректной работы, в случаенесовпадений настроить DNS правильно;

синхронизировать каталог пользователей и компьютеров LDAP с домена с помощью ранее созданного пользователя ldap-sync;

для входа в веб-консоль необходимо настроить использование ранее созданного пользователя домена web-officer с полными правами системы.

Запишите IP-адреса, токен, логины и пароли от учетных записей, а также все прочие нестандартные данные (измененные вами) вашей системы в текстовом файле «отчет.txt»на рабочем столе компьютера.

Задача 3: Установка и настройка сервера агентского мониторинга

Используя виртуальную машину агентского мониторинга:

необходимо ввести сервер в домен, после перезагрузки войти в систему от ранее созданного пользователя device-officer (важно);

после входа в систему необходимо переместить введенный в домен компьютер в ранее созданное подразделение “DemoExam” на домене;

установить базу данных PostgreSQL или функциональный аналог с паролем суперпользователя QWEasd123;

установить сервер агентского мониторинга с параметрами по умолчанию, подключившись к ранее созданной БД;

при установке сервера агентского мониторинга необходимо установить соединение с DLP-сервером по IP-адресу и токену, но можно сделать это и после установки. При установке настроить локального пользователя консоли управления: web-officer с паролем QWEasd123;

синхронизировать каталог пользователей и компьютеров с контроллером домена. Запишите IP-адреса, логины и пароли от учетных записей, а также все прочие данные, измененные вами, в текстовом файле «отчет.txt» с на рабочем столе компьютера.

Задача 4: Установка агента мониторинга на машине нарушителя

Используя виртуальную машину нарушителя:

необходимо ввести клиентскую машину в домен, после перезагрузки войти в систему от ранее созданного пользователя violator;

после входа в систему необходимо переместить введённый в домен компьютер в ранее созданное подразделение “DemoExam” на домене.

На машину нарушителя (violator) средствами групповых политик или сервера мониторинга установить агент мониторинга. Необходимо учесть, что установка осуществляется только с правами администратора (доменного или локального).

Ручная установка с помощью создания и переноса любым способом пакета установки является некорректным выполнением задания.

В случае проблем при установке компонентов стоит проверить настройки брандмауэра иDNS.

Задача 5: Защита системы с помощью сертификатов

Создайте дерево сертификатов формата PKCS для защиты веб-соединения с DLP- сервером по протоколу HTTPS. Сертификат и используемый ключ должен удовлетворять общепринятым на сегодня стандартам и требованиям (по длительности не более 1 года, длине ключа не менее 2048 бит и т. п.), параметры сертификата должны соответствовать

атрибутам компании. Утилита для создания сертификата — на выбор участника из доступных в операционных системах и дистрибутивах (openssl или аналоги).

Дерево сертификатов должно включать: корневой root-сертификат (ca); серверный (server) сертификат;

по желанию допускается использование пользовательского и промежуточного сертификата.

Дополнительная информация сертификатов должна включать в себя: Страна: RU.

Город: Moscow.

Компания (и иные дополнительные поля): DemoExam. Отдел: SoC.

Пароли ключей (если применимо): QWEasd123.

Остальные поля заполняются самостоятельно.

После генерации сертификатов необходимо установить серверный сертификат на веб- сервер DLP-системы, а также установить корневой сертификат как доверенный в контроллер домена для использования на всех компьютерах в сети.

В случае невозможности — это сделать, установить сертификат на машину домена и отобразить это в отчете.

Итоговый результат должен включать:

Дерево из сертификатов, упакованных в пакет PKCS (.p12), а также представленные в виде отдельных файлов ключей и сертификатов, расположенных на рабочем столе в каталоге «Сертификаты».

Содержимое команд по генерации ключей и сертификатов в текстовом файле

«сертификаты.txt» на рабочем столе с комментариями.

Скриншоты успешного подключения к консоли сервера DLP без ошибок сертификата, скриншоты окон просмотра сертификата в системе с помощью оснастки «Сертификаты» операционной системы (вкладки «Общие», «Путь сертификации»).

Сертификаты не должны содержать ошибок, предупреждений (warnings), неверной информации и т. п.

Модуль 2: Защита информации в автоматизированных системах программными и

программно-аппаратными средствами

При выполнении задания модуля необходимо достичь следующих целей:

1) Настройка сервера агентского мониторинга для правильной работы системы.

2) Разработка политик и правил безопасности, предотвращающих утечки или попытку использования устройств и сервисов пользователями.

3) Разработка групповых политик домена для ограничения пользовательских действий.

4) Проверка работоспособности политик и правил безопасности

Задания выполняются только с помощью компонентов DLP системы или групповых политик (указано в задании).

Все сценарии заданий (где применимо) необходимо воспроизвести и зафиксировать результат. Называйте созданные вами разделы/политики/группы и т. п. в соответствии с заданием, например, «Политика 1» или «Правило 1.2» и т. д., иначе проверка заданий может быть невозможна.

Выполнение отдельных заданий необходимо подтвердить скриншотом. В этом случае необходимо протоколировать свои результаты с помощью двух и более скриншотов для каждого задания (скриншот заданной политики и скриншот ее работы). Для некоторых заданий необходимо после фиксации результатов в виде скриншотов удалить заданную политику, что будет оговорено отдельно в тексте задания. Все скриншоты необходимо сохранить в папке «Модуль 2».

Формат названия скриншотов политик:

Пример 1 для сохранения скриншота созданной политики: CR-1.jpg где CR – сокращение от англ. creating a rule, 1 – номер задания

Пример 2 для сохранения скриншота работающей политики: RW-1.jpg где RW – сокращение от англ. rule work, 1 – номер задания.

Пример 3 для сохранения нескольких скриншотов одной работающей политики: RW-1- 2.jpg где RW – сокращение от англ. rule1 work, 1 – номер задания; 2 – номер скриншота для задания 1.

Задание модуля 2:

Задача 1: Проверка работоспособности системы

Необходимо создать проверочную политику на правило передачи, копирования, хранения и буфера обмена (или работы в приложениях), все 4 варианта срабатывания событий для данных, содержащих термин «Проверка системы» (в любом регистре), установить низкий уровень угрозы для всех событий, добавить тег «Проверка». Для

отработки правил через сервер агентского мониторинга необходимо создавать правила в отдельной политике «Модуль 2». После отработки политик необходимо оставить политику и открепить ее от групп компьютеров или выключить правила, но не удалять. Проверить срабатывание всеми четырьмя возможными способами (передачи, копирования, хранения и буфера обмена, хотя бы 1 событие на каждый тип) с помощью виртуальной машины нарушителя с установленным агентом. Сделать одну выборку, в которой будет отображено только по одному событию каждого типа (суммарно 4 события: передачи, копирования, хранения и буфера обмена), настроив конструктор выборки вручную.

Задача 2: подготовка сервера агентского мониторинга

Необходимо создать новую группу компьютеров: «DemoGroup», а также создать новую политику: «DemoPolicy». Политика должна применяться на ранее созданную группу компьютеров. Компьютер нарушителя необходимо переместить в группу «DemoGroup» Зафиксировать выполнение скриншотом.

Задача 3: смена пароля удаления агента

Необходимо установить (сменить) пароль для удаления агента мониторинга на всех машинах нарушителей с помощью средств сервера агентского мониторинга (удаленно). Пароль: QWEasd123

Зафиксировать выполнение скриншотом.

Следующие правила создаются в политике «DemoPolicy».Правило 1

Запретить печать документов на сетевых принтерах. Также необходимо отдельнымправилом разрешить печать на локальных принтерах.

Зафиксировать факт настройки правил (политик) скриншотами.

Правило 2

Необходимо полностью запретить использование облачного сервиса GoogleDrive, разрешить полное использование сервиса YandexDisk, остальные сервисы настроить только в режиме чтения (разрешить скачивание).

Зафиксировать факт настройки правил (политик) скриншотами.

Правило 3

Запретить запуск приложения wordpad или Libre/Open office Writer.

Проверить работоспособность, зафиксировать факт настройки правил (политик) и ихработоспособность скриншотами.

Правило 4

Необходимо запретить создание снимков экрана в текстовых редакторах дляпредотвращения утечки.

Проверить работоспособность, зафиксировать факт настройки правил (политик) и ихработоспособность скриншотами.

Правило 5

Необходимо запретить запись файлов на все съемные носители информации (флешки), оставив возможность чтения и копирования с них. В случае отсутствия USB-накопителей создать правило на сетевые расположения.

Проверить работоспособность, зафиксировать факт настройки правил (политик) и их работоспособность скриншотами.

Правило 6

С учетом ранее созданной блокировки необходимо разрешить копирование только наодин доверенный USB-накопитель.

Проверить работоспособность, зафиксировать факт настройки правил (политик) и ихработоспособность скриншотами.

Правило 7

Полностью заблокируйте доступ к CD/DVD на клиентском компьютере (виртуальной машине). В случае отсутствия CD/DVD привода его необходимо создать.

Проверить работоспособность, зафиксировать факт настройки правил (политик) и ихработоспособность скриншотами.

Правило 8

Осуществить выдачу временного доступа (30 минут) клиенту до заблокированногоCD/DVD привода.

Проверить работоспособность, зафиксировать факт настройки правил (политик) и их работоспособность скриншотами. Необходимо зафиксировать основные шаги выдачи доступа (например, ввод кода).

Правило 9

Необходимо установить контроль за компьютером потенциального нарушителя в случаеиспользования браузера путем создания снимков экрана каждые 30 секунд или при переходе в другое окно.

Проверить работоспособность, зафиксировать факт настройки правил (политик) и их работоспособность скриншотами. Также необходим скриншот сохраненных снимков экрана в системе

Правило 10

Запретить передачу файлов документов типа PDF на съемные носители информации и всетевые каталоги.

Проверить работоспособность любым из правил, зафиксировать факт настройки правил(политик) и их работоспособность скриншотами.

Групповые политики домена

Групповые применяются только на компьютер нарушителя (violator), должны быть созданы в домене, необходимо создать или 1 общий объект для всех политик и применить его к группе компьютеров/пользователей (или к конкретному компьютеру/пользователю), или по 1 объекту на каждую политику и применить их к группе компьютеров/пользователей (или к конкретному компьютеру/пользователю).

Зафиксировать настройку политик скриншотами, при возможности проверки зафиксировать скриншотами проверку политик (например, запрет запуска).

Использование компонентов DLP будет считаться некорректным выполнением задания.

Групповая политика 1

Настроить политику паролей и блокировки:

Максимальный срок действия пароля: 47 дней

Минимальная длина пароля: 8 символов

Блокировка пользователя при неправильном вводе пароля: 5

Блокировка учетной записи при вводе пароля: 20 минутЗафиксировать настройки политики скриншотами.

Групповая политика 2

Отключить анимацию первого входа в систему

Зафиксировать настройки политики скриншотами

Групповая политика 3

Запретить использование командной строки (терминала) пользователем стандартной политикой запрета (не с помощью списка, при наличии).

Зафиксировать настройки политики и выполнение скриншотами.

Групповая политика 4

Запретить пользователю самостоятельный запуск панели управления. Зафиксировать настройки политики и выполнение скриншотами.

Групповая политика 5

Изменить изображение рабочего стола пользователя групповыми политиками.

Изображение необходимо создать самостоятельно, должно содержать в себе названиекомпании («DemoExam») текстом в картинке.

Изменение изображения вручную не будет считаться корректным выполнением задания.

Требования к оцениванию

Максимально возможное количество баллов	**100**

№ п/п	**Модуль задания** (вид деятельности, вид профессиональной деятельности)	**Критерий оценивания**[5]	**Баллы**
1	2	3	4
1	Эксплуатация автоматизированных (информационных) систем в защищенном исполнении	Установка и настройка компонентов автоматизированных (информационных) систем в защищенном исполнении в соответствии с требованиями эксплуатационной документации. Администрирование программных и программно-аппаратных компонентов автоматизированной (информационной) системы в защищенном исполнении	50
2	Защита информации в автоматизированных системах программными и	Установка и настройка отдельных программных, программно- аппаратных	50

	программно- аппаратными средствами	средств защиты информации Обеспечение защиты информации в автоматизированных системах отдельными программными, программно-аппаратными средствами. Тестирование функций отдельных программных и программно- аппаратных средств защиты информации.	
Итого			**100**

2.1.2. Критерии оценки результат демонстрационного экзамена по КОД: 10.02.05-2023

Критерии оценки	Компетенции	ЗУНы	Уровень оценки			
			Повышенный уровень - оценка «отлично»	Высокий уровень - оценка «хорошо»	Базовый уровень - оценка «удовлетвори тельно»	Недостаточный уровень - оценка «неудовлетвор и тельно»
Эксплуатация автоматизированных (информационных) систем в защищенном исполнении	ПК 1.1 – ПК 1.4	**иметь практический опыт**: установки и настройки компонентов систем защиты информации автоматизированных (информационных) систем; администрирования автоматизированных систем в защищенном исполнении; эксплуатации компонентов систем защиты информации автоматизированных	на высоком уровне проводит установку и настройку автоматизированных (информационных) систем в защищенном исполнении в соответствии с требованиями эксплуатационной документации. в полном объёме проводит администрирование программных и программно-аппаратных	обнаруживает знание учебного материала, но допускает несущественные ошибки в изложении теоретического материала	ответ имеет репродуктивный характер	обнаруживает незнание или непонимание большей или наиболее существенной части содержания учебного материала

		систем; диагностики компонентов систем защиты информации автоматизированных систем, устранения отказов и восстановления работоспособности автоматизированных (информационных) систем в защищенном исполнении **уметь:** осуществлять комплектование, конфигурирование, настройку автоматизированных систем в защищенном исполнении компонент систем защиты информации автоматизированных систем; организовывать, конфигурировать,	компонентов автоматизированной (информационной) системы в защищенном исполнении			

		производить монтаж, осуществлять диагностику и устранять неисправности компьютерных сетей, работать с сетевыми протоколами разных уровней; осуществлять конфигурирование, настройку компонент систем защиты информации автоматизированных систем; производить установку, адаптацию и сопровождение типового программного обеспечения, входящего в состав систем защиты информации автоматизированной системы настраивать и устранять				

		неисправности программно-аппаратных средств защиты информации в компьютерных сетях по заданным правилам; обеспечивать работоспособность, обнаруживать и устранять неисправности **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; 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; принципы основных методов организации и проведения технического обслуживания вычислительной техники и других технических средств информатизации.				
Защита информации в автоматизированных системах программными и	ПК 2.1 – ПК 2.6	**иметь практический опыт:** установки, настройки	на высоком уровне проводит установку и настройку отдельных программных,	обнаруживает знание учебного материала, но допускает несущественные	ответ имеет репродуктивный характер	обнаруживает незнание или непонимание большей или наиболее существенной

программно-аппаратными средствами		программных средств защиты информации в автоматизированной системе; обеспечения защиты автономных автоматизированных систем программными и программно-аппаратными средствами; тестирования функций, диагностика, устранения отказов и восстановления работоспособности программных и программно-аппаратных средств защиты информации; решения задач защиты от НСД к информации ограниченного доступа с помощью программных и программно-	программно-аппаратных средств защиты информации в полном объеме обеспечивает защиту информации в автоматизированных системах отдельными программными, программно-аппаратными средствами в полном объеме проводит тестирование функций отдельных программных и программно-аппаратных средств защиты информации	ошибки в изложении теоретического материала		части содержания учебного материала

		аппаратных средств защиты информации; применения электронной подписи, симметричных и асимметричных криптографических алгоритмов и средств шифрования данных; учёта, обработки, хранения и передачи информации, для которой установлен режим конфиденциальности; работы с подсистемами регистрации событий; выявления событий и инцидентов безопасности в автоматизированной системе. **уметь:** устанавливать,				

		настраивать, применять программные и программно-аппаратные средства защиты информации; устанавливать и настраивать средства антивирусной защиты в соответствии с предъявляемыми требованиями; диагностировать, устранять отказы, обеспечивать работоспособность и тестировать функции программно-аппаратных средств защиты информации; 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; применять средства гарантированного уничтожения информации; 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:** особенности и способы применения программных и программно-аппаратных средств защиты информации, в том				

		числе, в операционных системах, компьютерных сетях, базах данных; методы тестирования функций отдельных программных и программно-аппаратных средств защиты информации; типовые модели управления доступом, средств, методов и протоколов идентификации и аутентификации; основные понятия криптографии и типовых криптографических методов и средств защиты информации; особенности и способы применения программных и программно-				

		аппаратных средств гарантированного уничтожения информации; типовые средства и методы ведения аудита, средств и способов защиты информации в локальных вычислительных сетях, средств защиты от несанкционированного доступа.				

На основании представленных критериев формируется итоговая оценка полноты формирования компетенции (Приложение 1).

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	1. Разработка технического решения по внедрению DLP-системы в комплексную систему обеспечения информационной безопасности страховой компании 2. Разработка защиты информации с применением межсетевого экрана автоматизированного рабочего места главного инженера (на примере компании...) 3. Разработка защиты базы данных Университетского колледжа информационных технологий от несанкционированного доступа 4. 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

	7. Обеспечение защищенного документооборота между компанией налогоплательщиком и государственными контролирующими органами 8. Организация защищенного сегмента сети научно-исследовательского центра для обработки информации с ограниченным доступом 9. 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 банка 12. Обеспечение защиты от влияния побочных электромагнитных излучений и наводок рабочего места разработчика программного обеспечения 13. Обеспечение информационной безопасности автоматизированного рабочего места сотрудников офиса департамента эксплуатации прикладных систем (на примере ...) 14. Защита речевой информации от утечки по техническим каналам в OpeNo Space помещении (на примере организации ...) 15. Обеспечение защиты от влияния побочных электромагнитных излучений и наводок рабочего места разработчика программного обеспечения 16. Комплексное обеспечение информационной безопасности персональных данных в компании индустрии моды и дизайна 17. Разработка автоматизированной системы	

	динамического анализа вредоносных файлов на основе технологии «Песочница» (на примере ...) 18.Разработка проекта единой системы идентификации и аутентификации (на примере производственного предприятия или завода) 19.Разработка политики информационной безопасности для компании ООО ... 20.Обеспечение комплексной защиты информации кабинета руководителя издательского дома 21.Обеспечение защищенного документооборота между компанией налогоплательщиком и государственными контролирующими органами	
ПМ.02 Защита информации в автоматизированных системах программными и программно-аппаратными средствами	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	Дипломная работа

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

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

	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 ...)	

	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-центре 20. 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 зашиты 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 «удовлетвори тельно»	Недостаточный уровень - оценка «неудовлетвори тельно»
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; ДПК 5.1 – ДПК 5.3 ДПК 6.1 – ДПК 6.4	**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. Использованы 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

		информационных систем. установке и настройке программных средств защиты информации; тестировании функций, диагностике, устранении отказов и восстановлении работоспособности программных и программно-аппаратных средств защиты информации; учете, обработке, хранении и передаче информации, для которой установлен режим конфиденциальности. выявлении технических каналов утечки информации; применении, техническом обслуживании, диагностике, устранении отказов,				й безопасности.
Практическая значимость разработанных рекомендаций (предложенных мероприятий)			Практическая часть ВКР выполнена на высоком профессиональном уровне (может быть рекомендована для	Практическая часть ВКР выполнена на хорошем профессиональном уровне.	Практическая часть ВКР выполнена на удовлетворительном профессиональном	Практическая часть не содержит самостоятельно разработанных и надлежаще обоснованных

		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 сформулированны	Отсутствует презентация, доклад не отражает выводы и оценки содержащиеся в ВКР.

		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;	проведенного исследования.	результатам проведенного исследования.	е предложения по результатам проведенного исследования.	

		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. **уметь:** обеспечивать работоспособность, обнаруживать и устранять неисправности, осуществлять комплектование, конфигурирование, настройку автоматизированных систем в защищенном исполнении и компонент систем защиты информации автоматизированных систем; производить установку, адаптацию и сопровождение типового программного обеспечения, входящего в состав систем защиты информации автоматизированной системы;				

		организовывать, конфигурировать, производить монтаж, осуществлять диагностику и устранять неисправности компьютерных сетей, работать с сетевыми протоколами разных уровней; настраивать и устранять неисправности программно-аппаратных средств защиты информации в компьютерных сетях по заданным правилам. 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. применять средства охранной сигнализации, охранного телевидения и систем контроля и управления доступом; применять технические средства для криптографической защиты информации конфиденциального характера; применять технические средства для уничтожения				

		информации и носителей информации, защиты информации в условиях применения мобильных устройств обработки и передачи данных; применять инженерно-технические средства физической защиты объектов информатизации. подключать и настаивать 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; 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; 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. **знать:** состав и принципы работы автоматизированных систем, операционных систем и сред; принципы разработки алгоритмов программ, основных приемов программирования; модели баз данных; принципы построения, физические основы работы периферийных устройств, основных методов организации и проведения технического обслуживания вычислительной техники и других технических средств информатизации;				

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

		методы ведения аудита, средств и способов защиты информации в локальных вычислительных сетях, средств защиты от несанкционированного доступа; основные понятия криптографии и типовых криптографических методов и средств защиты информации. физические основы, структуру и условия формирования технических каналов утечки информации, способы их выявления и методы оценки опасности, классификацию существующих физических полей и технических каналов утечки информации; номенклатуру и характеристики				

		аппаратуры, используемой для измерения параметров побочных электромагнитных излучений и наводок (далее - ПЭМИН), а также параметров фоновых шумов и физических полей, создаваемых техническими средствами защиты информации; основные принципы действия и характеристики, порядок технического обслуживания, устранение неисправностей и организацию ремонта технических средств защиты информации; основные способы физической защиты объектов информатизации; методики инструментального контроля				

		эффективности защиты информации, обрабатываемой средствами вычислительной техники на объектах информатизации; номенклатуру применяемых средств защиты информации от несанкционированной утечки по техническим каналам и физической защиты объектов информатизации. 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 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, периферийным, мультимедийным оборудованием и компьютерной оргтехникой.				

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;
- Положение о формировании фонда оценочных средств ГИА;
- Программа ГИА по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем.

Приложение 1

ОТЗЫВ О ВЫПУСКНОЙ КВАЛИФИКАЦИОННОЙ РАБОТЕ

_____

_____

_____

(тема работы)

Основное содержание работы

_____

_____

_____

_____

_____

_____

Основные достоинства работы

_____

_____

_____

_____

_____

_____

Основные недостатки работы

_____

_____

_____

_____

_____

_____

Оценка_____

Руководитель ВКР _____

«___»_____20__г

Приложение 2

ОЦЕНОЧНЫЙ ЛИСТ РЕЗУЛЬТАТОВ ДЕМОНСТРАЦИОННОГО ЭКЗАМЕНА

ФИО обучающегося	Критерии оценки							Итого

Приложение 3

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

Приложение 4

СВОДНЫЙ ОЦЕНОЧНЫЙ ЛИСТ РЕЗУЛЬТАТОВ ЗАЩИТЫ ВЫПУСКНОЙ КВАЛИФИКАЦИОННОЙ РАБОТЫ

ФИО студента	Председатель ГЭК ФИО	Зам. председателя ГЭК ФИО	Член ГЭК ФИО	Член ГЭК ФИО	Член ГЭК ФИО	Член ГЭК ФИО	Итоговая оценка