Приложение 5

к программе СПО 10.02.04 Обеспечение информационной безопасности телекоммуникационных систем

СОДЕРЖАНИЕ
ГОСУДАРСТВЕННОЙ ИТОГОВОЙ АТТЕСТАЦИИ

по специальности

10.02.04 Обеспечение информационной безопасности телекоммуникационных систем

2026 год

СОДЕРЖАНИЕ

1. **СТРУКТУРА ОЦЕНОЧНЫХ МАТЕРИАЛОВ ДЛЯ ПРОВЕДЕНИЯ ДЕМОНСТРАЦИОННОГО ЭКЗАМЕНА**
2. **КОМПЛЕКС ТРЕБОВАНИЙ И РЕКОМЕНДАЦИЙ ДЛЯ ПРОВЕДЕНИЯ ДЕМОНСТРАЦИОННОГО ЭКЗАМЕНА**

1. СТРУКТУРА ОЦЕНОЧНЫХ МАТЕРИАЛОВ ДЛЯ ПРОВЕДЕНИЯ ДЕМОНСТРАЦИОННОГО ЭКЗАМЕНА

Для выпускников, осваивающих ППССЗ в соответствии с ФГОС СПО проводится в форме демонстрационного экзамена и защиты дипломного проекта (работы).

1.1. Структура оценочных материалов

Оценочные материалы для проведения демонстрационного экзамена включают в себя комплект(ы) оценочной документации, варианты заданий и критерии оценивания.

1.2. Структура комплекта оценочной документации

Комплект оценочной документации (далее – КОД) включает в себя следующие разделы:

1.Комплекс требований для проведения демонстрационного экзамена.
2.Перечень оборудования и оснащения, расходных материалов, средств обучения и воспитания.
3.План застройки площадки демонстрационного экзамена.
4.Требования к составу экспертных групп.
5.Инструкции по технике безопасности.
6.Образец задания.

2. КОМПЛЕКС ТРЕБОВАНИЙ И РЕКОМЕНДАЦИЙ ДЛЯ ПРОВЕДЕНИЯ ДЕМОНСТРАЦИОННОГО ЭКЗАМЕНА

2.1. Организационные требования:

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 соответствии 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 (пять) рабочих дней до даты проведения экзамена.

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

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

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

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

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

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

2.2. Рекомендуемое содержание КОД

Компетенции, рекомендуемые для включения в содержание КОД

Общие компетенции

Код компетенции	Формулировка компетенции	Код	Знания, умения
ОК 01	Выбирать способы решения задач профессиональной деятельности применительно к различным контекстам		**Умения:**
		Уо 01.01	распознавать задачу и/или проблему в профессиональном и/или социальном контексте
		Уо 01.02	анализировать задачу и/или проблему и выделять её составные части
		Уо 01.03	определять этапы решения задачи
		Уо 01.04	выявлять и эффективно искать информацию, необходимую для решения задачи и/или

			проблемы
		Уо 01.05	составлять план действия
		Уо 01.06	определять необходимые ресурсы
		Уо 01.07	владеть актуальными методами работы в профессиональной и смежных сферах
		Уо 01.08	реализовывать составленный план
		Уо 01.09	оценивать результат и последствия своих действий (самостоятельно или с помощью наставника)
			Знания:
		Зо 01.01	актуальный профессиональный и социальный контекст, в котором приходится работать и жить
		Зо 01.02	основные источники информации и ресурсы для решения задач и проблем в профессиональном и/или социальном контексте
		Зо 01.03	алгоритмы выполнения работ в профессиональной и смежных областях
		Зо 01.04	методы работы в профессиональной и смежных сферах
		Зо 01.05	структуру плана для решения задач
		Зо 01.06	порядок оценки результатов решения задач профессиональной деятельности
ОК 02	Использовать современные средства поиска, анализа и интерпретации информации, и информационные технологии для выполнения задач профессиональной деятельности		**Умения:**
		Уо 02.01	определять задачи для поиска информации
		Уо 02.02	определять необходимые источники информации
		Уо 02.03	планировать процесс поиска; структурировать получаемую информацию
		Уо 02.04	выделять наиболее значимое в перечне информации
		Уо 02.05	оценивать практическую значимость результатов поиска
		Уо 02.06	оформлять результаты поиска, применять средства информационных технологий для решения профессиональных задач
		Уо 02.07	использовать современное программное обеспечение
		Уо 02.08	использовать различные цифровые средства для решения профессиональных задач
			Знания:
		Зо 02.01	номенклатура информационных источников, применяемых в профессиональной деятельности
		Зо 02.02	приемы структурирования информации
		Зо 02.03	формат оформления результатов поиска информации, современные средства и устройства информатизации

		Зо 02.04	порядок их применения и программное обеспечение в профессиональной деятельности в том числе с использованием цифровых средств
ОК 03	Планировать и реализовывать собственное профессиональное и личностное развитие, предпринимательскую деятельность в профессиональной сфере, использовать знания по финансовой грамотности в различных жизненных ситуациях		**Умения:**
		Уо 03.01	определять актуальность нормативно-правовой документации в профессиональной деятельности
		Уо 03.02	применять современную научную профессиональную терминологию
		Уо 03.03	определять и выстраивать траектории профессионального развития и самообразования
		Уо 03.04	выявлять достоинства и недостатки коммерческой идеи
		Уо 03.05	презентовать идеи открытия собственного дела в профессиональной деятельности; оформлять бизнес-план
		Уо 03.06	рассчитывать размеры выплат по процентным ставкам кредитования
		Уо 03.07	определять инвестиционную привлекательность коммерческих идей в рамках профессиональной деятельности
		Уо 03.08	презентовать бизнес-идею
		Уо 03.09	определять источники финансирования
			Знания:
		Зо 03.01	содержание актуальной нормативно-правовой документации
		Зо 03.02	современная научная и профессиональная терминология
		Зо 03.03	возможные траектории профессионального развития и самообразования
		Зо 03.04	основы предпринимательской деятельности основы финансовой грамотности
		Зо 03.05	правила разработки бизнес-планов
		Зо 03.06	порядок выстраивания презентации
		Зо 03.07	кредитные банковские продукты
ОК 04	Эффективно взаимодействовать и работать в коллективе и команде		**Умения:**
		Уо 04.01	организовывать работу коллектива и команды
		Уо 04.02	взаимодействовать с коллегами, руководством, клиентами в ходе профессиональной деятельности
			Знания:
		Зо 04.01	психологические основы деятельности коллектива, психологические особенности личности
		Зо 04.02	основы проектной деятельности
ОК 05	Осуществлять устную		**Умения:**

	и письменную коммуникацию на государственном языке Российской Федерации с учетом особенностей социального и культурного контекста	Уо 05.01	грамотно излагать свои мысли и оформлять документы по профессиональной тематике на государственном языке, проявлять толерантность в рабочем коллективе
			Знания:
		Зо 05.01	особенности социального и культурного контекста
		Зо 05.02	правила оформления документов и построения устных сообщений
ОК 06	Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных общечеловеческих ценностей, в том числе с учетом гармонизации межнациональных и межрелигиозных отношений, применять стандарты антикоррупционного поведения		**Умения:**
		Уо 06.01	описывать значимость своей *профессии (специальности)*
		Уо 06.02	применять стандарты антикоррупционного поведения
			Знания:
		Зо 06.01	сущность гражданско-патриотической позиции, общечеловеческих ценностей
		Зо 06.02	значимость профессиональной деятельности по *профессии (специальности)*
		Зо 06.03	стандарты антикоррупционного поведения и последствия его нарушения
ОК 07	Содействовать сохранению окружающей среды, ресурсосбережению, применять знания об изменении климата, принципы бережливого производства, эффективно действовать в чрезвычайных ситуациях	Уо 07.01	**Умения:**
			соблюдать нормы экологической безопасности
		Уо 07.02	определять направления ресурсосбережения в рамках профессиональной деятельности по *профессии (специальности),* осуществлять работу с соблюдением принципов бережливого производства
		Уо 07.03	организовывать профессиональную деятельность с учетом знаний об изменении климатических условий региона
			Знания:
		Зо 07.01	правила экологической безопасности при ведении профессиональной деятельности
		Зо 07.02	основные ресурсы, задействованные в профессиональной деятельности
		Зо 07.03	пути обеспечения ресурсосбережения
		Зо 07.04	принципы бережливого производства
		Зо 07.05	основные направления изменения климатических условий региона
ОК 08	Использовать средства физической культуры для сохранения		**Умения:**
		Уо 08.01	использовать физкультурно-оздоровительную деятельность для укрепления здоровья, достижения жизненных и профессиональных

	и укрепления здоровья в процессе профессиональной деятельности и поддержания необходимого уровня физической подготовленности		целей
		Уо 08.02	применять рациональные приемы двигательных функций в профессиональной деятельности
		Уо 08.03	пользоваться средствами профилактики перенапряжения, характерными для данной *специальности*
			Знания:
		Зо 08.01	роль физической культуры в общекультурном, профессиональном и социальном развитии человека
		Зо 08.02	основы здорового образа жизни
		Зо 08.03	условия профессиональной деятельности и зоны риска физического здоровья для *профессии (специальности)*
		Зо 08.04	средства профилактики перенапряжения
ОК 09	Пользоваться профессиональной документацией на государственном и иностранном языках		**Умения:**
		Уо 09.01	понимать общий смысл четко произнесенных высказываний на известные темы (профессиональные и бытовые), понимать тексты на базовые профессиональные темы
		Уо 09.02	участвовать в диалогах на знакомые общие и профессиональные темы
		Уо 09.03	строить простые высказывания о себе и о своей профессиональной деятельности
		Уо 09.04	кратко обосновывать и объяснять свои действия (текущие и планируемые)
		Уо 09.05	писать простые связные сообщения на знакомые или интересующие профессиональные темы
			Знания:
		Зо 09.01	правила построения простых и сложных предложений на профессиональные темы
		Зо 09.02	основные общеупотребительные глаголы (бытовая и профессиональная лексика)
		Зо 09.03	лексический минимум, относящийся к описанию предметов, средств и процессов профессиональной деятельности
		Зо 09.04	особенности произношения
		Зо 09.05	правила чтения текстов профессиональной направленности

Профессиональные компетенции

Виды деятельности	Код и наименование компетенции	Код	Показатели освоения компетенции

Эксплуатация информационно – телекоммуникационных систем и сетей	ПК1.1. Производить монтаж, настройку и поверку функционирования и конфигурирования оборудования информационно – телекоммуникационных систем и сетей.		**Навыки:**
		Н 1.1.01	монтажа, настройки, проверки функционирования и конфигурирования оборудования информационно-телекоммуникационных систем и сетей (далее –ИТКС)
			Умения:
		У 1.1.01	осуществлять техническую эксплуатацию линейных сооружений связи
		У 1.1.02	производить монтаж кабельных линий и оконечных кабельных устройств
		У 1.1.03	настраивать, эксплуатировать и обслуживать оборудование ИТКС
		У 1.1.04	осуществлять подключение, настройку мобильных устройств и распределенных сервисов ИТКС
		У 1.1.05	производить испытания, проверку и приемку оборудования ИТКС
		У 1.1.06	производить монтаж кабельных линий и оконечных кабельных устройств ИТКС
		У 1.1.07	применять средства измерений характеристик функционирования электрических цепей и сигналов ИТКС
			Знания:
		З 1.1.01	принципов построения и основных характеристик ИТКС
		З 1.1.02	принципов передачи информации в ИТКС

		З 1.1.03	видов и характеристик сигналов в ИТКС
		З 1.1.04	видов помех в каналах связи ИТКС и методов защиты от них
		З 1.1.05	разновидностей линий передач, конструкции и характеристик электрических и оптических кабелей связи
		З 1.1.06	технологий и оборудования удаленного доступа в ИТКС
		З 1.1.07	принципов построения, основные характеристики активного сетевого и коммуникационного оборудования ИТКС
		З 1.1.08	основных характеристик типовых измерительных приборов и правил работы с ними
	ПК 1.2. Осуществлять диагностику технического состояния, поиск неисправностей и ремонт оборудования информационно – телекоммуникационных систем и сетей.		**Навыки:**
		Н 1.2.01	текущего контроля функционирования оборудования ИТКС
		Н 1.2.02	диагностики технического состояния приёмо-передающих устройств и линейных сооружений связи и источников питания
			Умения:
		У 1.2.01	осуществлять подключение, настройку мобильных устройств и распределенных сервисов ИТКС
		У 1.2.02	производить испытания, проверку и приемку оборудования ИТКС
		У 1.2.03	осуществлять диагностику технического состояния ИТКС
		У 1.2.04	применять средства измерений характеристик

			функционирования электрических цепей и сигналов ИТКС
			Знания:
		З 1.2.01	принципов построения и основных характеристик ИТКС
		З 1.2.02	принципы передачи информации в ИТКС
		З 1.2.03	разновидностей линий передач, конструкций и характеристик электрических и оптических кабелей связи
		З 1.2.04	технологий и оборудования удаленного доступа в ИТКС
		З 1.2.05	периодичности выполнения поверок контрольно-измерительной аппаратуры
		З 1.2.06	требований метрологического обеспечения функционирования ИБТКС
	ПК 1.3. Проводить техническое обслуживание оборудования информационно – телекоммуникационных систем и сетей		**Навыки:**
		Н 1.3.01	проведения технического обслуживания, диагностики технического состояния, поиска неисправностей и ремонта оборудования ИТКС
			Умения:
		У 1.3.01	осуществлять техническую эксплуатацию линейных сооружений связи
		У 1.3.02	проверять функционирование, производить регулировку и контроль основных параметров источников питания радиоаппаратуры
		У 1.3.03	производить настройку программного обеспечения коммутационного оборудования защищенных телекоммуникационных систем

		У 1.3.04	производить контроль параметров функционирования ИТКС
			Знания:
		З 1.3.01	принципов построения и основных характеристик ИТКС
		З 1.3.02	видов и характеристик сигналов в ИТКС
		З 1.3.03	разновидностей линий передач, конструкции и характеристик электрических и оптических кабелей связи
		З 1.3.04	принципов построения, основных характеристик активного сетевого и коммуникационного оборудования ИТКС
		З 1.3.05	принципов организации технической эксплуатации ИТКС
	ПК 1.4. Осуществлять контроль функционирования информационно – телекоммуникационных систем и сетей		**Навыки:**
		Н 1.4.01	текущего контроля функционирования оборудования ИТКС
		Н 1.4.02	мониторинга технического состояния и работоспособности приёмо-передающих устройств и линейных сооружений связи и источников питания ИТКС
			Умения:
		У 1.4.01	осуществлять техническую эксплуатацию линейных сооружений связи
		У 1.4.02	настраивать, эксплуатировать и обслуживать оборудование ИТКС
		У 1.4.03	производить испытания, проверку и приемку оборудования ИТКС

		У 1.4.04	проводить работы по техническому обслуживанию, диагностике технического состояния и ремонту оборудования ИТКС
		У 1.4.05	осуществлять техническую эксплуатацию приемо-передающих устройств
		У 1.4.05	оформлять эксплуатационно-техническую документацию
			Знания:
		З 1.4.01	принципов построения и основных характеристик ИТКС
		З 1.4.02	принципов передачи информации в ИТКС
		З 1.4.03	видов и характеристик сигналов в ИТКС
		З 1.4.04	видов помех в каналах связи ИТКС и методов защиты от них
		З 1.4.05	принципов построения, основных характеристик активного сетевого и коммуникационного оборудования ИТКС
		З 1.4.06	спецификацию изделий, комплектующих, запасного имущества и принадлежностей ИТКС
Защита информации в информационно – телекоммуникационных системах и сетях с использованием программно-аппаратных, в том числе криптографических средств защиты	ПК 2.1. Производить установку, настройку, испытания и конфигурирование программных и программно-аппаратных, в том числе криптографических средств защиты		**Навыки:**
		Н 2.1.01	установки, настройки, испытаний и конфигурирования программных и программно-аппаратных (в том числе криптографических) средств защиты информации в оборудовании ИТКС
			Умения:

	информации от несанкционированного доступа и специальных воздействий в оборудование информационно – телекоммуникационных систем и сетей	У 2.1.01	выявлять и оценивать угрозы безопасности информации в ИТКС
		У 2.1.02	настраивать и применять средства защиты информации в операционных системах, в том числе средства антивирусной защиты
		У 2.1.03	проводить установку и настройку программных и программно-аппаратных (в том числе криптографических) средств защиты информации
		У 2.1.04	проводить конфигурирование программных и программно-аппаратных (в том числе криптографических) средств защиты информации
			Знания:
		З 2.1.01	способов защиты информации от несанкционированного доступа (далее – НСД) и специальных воздействий на нее
		З 2.1.02	типовых программных и программно-аппаратных средств защиты информации в ИТКС
		З 2.1.03	криптографических средств защиты информации конфиденциального характера, которые применяются в ИТКС
	ПК 2.2. Поддерживать бесперебойную работу программных и программно-аппаратных, в том числе и криптографических средств защиты		**Навыки:**
		Н 2.2.01	поддержания бесперебойной работы программных и программно-аппаратных (в том числе криптографических) средств защиты информации в ИТКС
			Умения:

	информации в информационно – телекоммуникационных системах и сетях	У 2.2.01	выявлять и оценивать угрозы безопасности информации в ИТКС
		У 2.2.02	проводить контроль показателей и процесса функционирования программных и программно-аппаратных (в том числе криптографических) средств защиты информации
		У 2.2.03	проводить восстановление процесса и параметров функционирования программных и программно-аппаратных (в том числе криптографических) средств защиты информации
		У 2.2.04	проводить техническое обслуживание и ремонт программно-аппаратных (в том числе криптографических) средств защиты информации
			Знания:
		З 2.2.01	возможных угроз безопасности информации в ИТКС
		З 2.2.02	способов защиты информации от НСД и специальных воздействий на нее
		З 2.2.03	порядка тестирования функций программных и программно-аппаратных (в том числе криптографических) средств защиты информации
		З 2.2.04	организации и содержания технического обслуживания и ремонта программно-аппаратных (в том числе криптографических) средств защиты информации

		З 2.2.05	порядка и правил ведения эксплуатационной документации на программные и программно-аппаратные (в том числе криптографические) средства защиты информации
	ПК 2.3. Осуществлять защиту информации от несанкционированных действий и специальных воздействий в информационно – телекоммуникационных системах и сетях с использованием программных и программно-аппаратных, в том числе криптографических средств в соответствии с предъявленными требованиями.		**Навыки:**
		Н 2.3.01	защиты информации от НСД и специальных воздействий в ИТКС с использованием программных и программно-аппаратных (в том числе криптографических) средств защиты в соответствии с предъявляемыми требованиями
			Умения:
		У 2.3.01	выявлять и оценивать угрозы безопасности информации в ИТКС
		У 2.3.02	настраивать и применять средства защиты информации в операционных системах, в том числе средства антивирусной защиты
		У 2.3.03	проводить конфигурирование программных и программно-аппаратных (в том числе криптографических) средств защиты информации
			Знания:
		З 2.3.01	возможных угроз безопасности информации в ИТКС
		З 2.3.02	способов защиты информации НСД и специальных воздействий на нее
		З 2.3.03	типовых программных и программно-аппаратных средств защиты информации в ИТКС

		З 2.3.04	криптографических средств защиты информации конфиденциального характера, которые применяются в ИТКС
		З 2.3.05	порядка и правил ведения эксплуатационной документации на программные и программно-аппаратные (в том числе криптографические) средства защиты информации
Защита информации в информационно – телекоммуникационных системах и сетях с использованием технических средств защиты	ПК 3.1. Производить установку, монтаж, настройку и испытания технических средств защиты информации от утечки по техническим каналам в информационно – телекоммуникационных системах и сетях.		**Навыки:**
		Н 3.1.01	установки, монтажа, настройки и испытаний технических средств защиты информации от утечки по техническим каналам
			Умения:
		У 3.1.01	проводить установку, монтаж, настройку и испытание технических средств защиты информации от утечки по техническим каналам
		У 3.1.02	применять нормативные правовые акты и нормативные методические документы в области защиты информации
			Знания:
		З 3.1.01	способов защиты информации от утечки по техническим каналам с использованием технических средств защиты
		З 3.1.02	основных типов технических средств защиты информации от утечки по техническим каналам
		З 3.1.03	законодательства в области информационной безопасности, структуру государственной системы

			защиты информации, нормативных актов уполномоченных органов исполнительной власти, национальных стандартов и других методических документов в области информационной безопасности
	ПК 3.2. Проводить техническое обслуживание, диагностику, устранение неисправностей и ремонт технических средств защиты информации, используемых в информационно – телекоммуникационных системах и сетях		**Навыки:**
		Н 3.2.01	установки, монтажа, настройки и испытаний технических средств защиты информации от утечки по техническим каналам
		Н 3.2.02	проведения технического обслуживания и ремонта технических средств защиты информации от утечки по техническим каналам
			Умения:
		У 3.2.01	проводить установку, монтаж, настройку и испытание технических средств защиты информации от утечки по техническим каналам
		У 3.2.02	проводить техническое обслуживание, устранение неисправностей и ремонт технических средств защиты информации от утечки по техническим каналам
		У 3.2.03	применять нормативные правовые акты и нормативные методические документы в области защиты информации
			Знания:
		З 3.2.01	основных типов технических средств защиты информации от утечки по техническим каналам

		З 3.2.02	организацию и содержание технического обслуживания и ремонта технических средств защиты информации от утечки по техническим каналам
		З 3.2.03	порядка и правил ведения эксплуатационной документации на технические средства защиты информации от утечки по техническим каналам
	ПК 3.3. Осуществлять защиту информации от утечки по техническим каналам в информационно – телекоммуникационных системах и сетях с использованием технических средств защиты в соответствии с предъявляемыми требованиями.		**Навыки:**
		Н 3.3.01	защиты информации от утечки по техническим каналам с использованием технических средств защиты в соответствии с предъявляемыми требованиями
			Умения:
		У 3.3.01	проводить измерение параметров фоновых шумов и ПЭМИН, создаваемых оборудованием ИТКС
		У 3.3.02	проводить измерение параметров электромагнитных излучений и токов, создаваемых техническими средствами защиты информации от утечки по техническим каналам
		У 3.3.03	применять нормативные правовые акты и нормативные методические документы в области защиты информации
			Знания:
		З 3.3.01	способов защиты информации от утечки по техническим каналам с использованием технических

			средств защиты
		З 3.3.02	основных типов технических средств защиты информации от утечки по техническим каналам
		З 3.3.03	методик измерения параметров побочных электромагнитных излучений и наводок (далее – ПЭМИН), а также параметров фоновых шумов и физических полей, создаваемых техническими средствами защиты информации от утечки по техническим каналам
		З 3.3.04	порядка и правил ведения эксплуатационной документации на технические средства защиты информации от утечки по техническим каналам
	ПК 3.4. Проводить отдельные работы по физической защите линий связи информационно – телекоммуникационных систем и сетей		**Навыки:**
		Н 3.4.01	проведение измерений параметров фоновых шумов, а также физических полей, создаваемых техническими средствами защиты информации
		Н 3.4.02	выявление технических каналов утечки информации
			Умения:
		У 3.4.01	применять технические средства для защиты информации в условиях применения мобильных устройств обработки и передачи данных
			Знания:
		З 3.4.01	номенклатуру применяемых средств защиты информации

			от несанкционированной утечки по техническим каналам

2.3.Требования к оцениванию

Максимально возможное количество баллов	**100**

Рекомендуемая схема перевода результатов демонстрационного экзамена из стобалльной шкалы в пятибалльную

Оценка (пятибалльная шкала)	**«2»**	**«3»**	**«4»**	**«5»**
Оценка в баллах (стобалльная шкала)	0,00 – 19,99	20,00 – 39,99	40,00 – 69,99	70,00 – 100,00

2.3. Учет в КОД условий для лиц с ограниченными возможностями здоровья и выпускников из числа детей-инвалидов и инвалидов

Для выпускников из числа лиц с ограниченными возможностями здоровья и выпускников из числа детей-инвалидов и инвалидов в КОД учитываются условия, позволяющие проводить демонстрационный экзамен с учетом особенностей и возможностей такой категории лиц.

2.4. Объем времени на государственную итоговую аттестацию установлен ФГОС СПО– 6 недель, в том числе: 4 недели отведены на подготовку дипломного проекта и подготовку к демонстрационному экзамену и 2 недели на защиту дипломного проекта и проведение демонстрационного экзамена. Сроки проведения государственной итоговой аттестации определены учебным планом и календарным учебным графиком по специальности.

3. Порядок проведения демоэкзамена

Демонстрационный экзамен проводится по компетенции «Корпоративная защита от внутренних угроз информационной безопасности».

КОД 1.1 содержит:

Паспорт КОД с указанием:

- перечня знаний, умений и навыков из Спецификации стандарта компетенции «Корпоративная защита от внутренних угроз информационной безопасности», проверяемых в рамках КОД;
- обобщенной оценочной ведомости;
- количества экспертов, участвующих в оценке выполнения задания;
- списка оборудования и материалов, запрещенных на площадке (при наличии);
- Инструкцию по охране труда и технике безопасности для проведения демонстрационного экзамена;
- Образец задания для демонстрационного экзамена;
- Инфраструктурный лист;
- План проведения демонстрационного экзамена с указанием времени и продолжительности работы участников и экспертов;
- План застройки площадки для проведения демонстрационного экзамена.
- Инструкция по охране труда и технике безопасности для проведения демонстрационного экзамена по компетенции: «Корпоративная защита от внутренних угроз информационной безопасности»

Количество экспертов, участвующих в оценке выполнения задания

Минимальное количество экспертов, участвующих в оценке демонстрационного экзамена по компетенции «Корпоративная защита от внутренних угроз информационной безопасности» - 3 чел.

Дополнительное количество экспертов рассчитывается исходя из количества участников демонстрационного экзамена – 1 эксперт на 12 участников.

4. ОРГАНИЗАЦИЯ И ПРОВЕДЕНИЕ ЗАЩИТЫ ДИПЛОМНОЙ РАБОТЫ (ДИПЛОМНОГО ПРОЕКТА)

Программа организации проведения защиты дипломного проекта (работы) как формы ГИА включает общие положения, тематику, структуру и содержание дипломной работы (проекта), порядок оценки результатов дипломной работы (проекта).

3.1. Общие положения

Дипломный проект (работа) направлен на систематизацию и закрепление знаний выпускника по специальности, а также определение уровня готовности выпускника к самостоятельной профессиональной деятельности. Дипломный проект (работа) предполагает самостоятельную подготовку (написание) выпускником проекта (работы), демонстрирующего уровень знаний выпускника в рамках выбранной темы, а также сформированность его профессиональных умений и навыков.

Тематика дипломных проектов (работ) определяется образовательной организацией. Выпускнику предоставляется право выбора темы дипломного проекта (работы), в том числе предложения своей темы с необходимым обоснованием целесообразности ее разработки для практического применения. Тема дипломного проекта (работы) должна соответствовать содержанию одного или нескольких профессиональных модулей, входящих в образовательную программу среднего профессионального образования.

Для подготовки дипломного проекта (работы) выпускнику назначается руководитель и при необходимости консультанты, оказывающие выпускнику методическую поддержку.

Закрепление за выпускниками тем дипломных проектов (работ), назначение руководителей и консультантов осуществляется распорядительным актом образовательной организации.

3.2. Тематика дипломных работ (проектов) по специальности

Примерные темы дипломных проектов для специальности 10.02.04 Обеспечение информационной безопасности телекоммуникационных систем

1. Разработка информационно-поисковой системы, приложения баз данных: складской учет, библиотечные системы кадровый состав, системы хранения и обработки информации, создание комментариев, руководств пользователей для новых программных средств, адаптация их для конкретной организации, разработка программных средств защиты информационных систем

2. Программирование расчетных задач: задачи моделирования и расчета производственных процессов, разработка программных модулей для бухгалтерских пакетов, корпоративных систем 3. Создание WEB-сайтов, средств дистанционного обучения: создание сайтов организации, создание тематических сайтов, разработка электронных учебников, разработка обучающих игр

4. Проектирование компьютерной сети в соответствии с заданными параметрами

5. Разработка программных средств по защите информации

3.3. Структура и содержание дипломной работы (проекта)

Для обеспечения единства требований к выпускной квалификационной работе студентов устанавливаются общие требования к структуре и объему дипломного проекта.

В состав дипломного проекта входит пояснительная записка и файлы, а также схемы, макеты на CD, DVD, Flash-накопителях. Все приложенные файлы должны открываться в режиме offline, как запускаемые файлы или с помощью установленных приложений.

Объём пояснительной записки – не менее 70 страниц рукописного или 40 страниц печатного текста. Пояснительная записка должна быть переплетена и подписана дипломником с указанием даты окончания работы над проектом. В пояснительной записке к дипломному проекту должна быть четко выдержана структура.

Титульный лист является первой страницей, оформляется на типовом бланке.

Задание на дипломный проект является второй страницей и оформляется на бланке установленной формы с указанием даты выдачи задания, сроков выполнения и даты сдачи законченной работы.

Заключение руководителя оформляется на типовом бланке.

Рецензия оформляется на типовом бланке.

Содержание ДП включает названия глав и параграфов с указанием страниц, с которых они начинаются. Пункты содержания соответствуют заголовкам глав и параграфов в тексте работы, представление их в тексте в другой редакции не допускается.

Введение должно содержать общие сведения о работе, ее краткую характеристику. В нем необходимо отразить актуальность выбранной темы, цель и задачи, решаемые в работе, используемые методики и средства разработки, практическую значимость полученных результатов.

Во введении необходимо также перечислить вопросы, которые будут рассмотрены в проекте, выделив вопросы, которые предполагается решить практически.

Основная часть содержит несколько глав, каждая из которых может делиться на необходимое количество разделов.

Содержание глав основной части должно точно соответствовать теме дипломного проекта и полностью его раскрывать. Главы целесообразно завершать краткими выводами. Первая глава посвящена рассмотрению теоретических аспектов исследуемой темы и служит основой для дальнейшего изложения материала. В этой главе рассматривается сущность, содержание, организация исследуемого процесса, его составные элементы. Полученные в результате рассмотрения первой главы выводы должны раскрыть новизну работы, которая формулируется во введении. Приводимые факты и числовой материал должны быть достоверными. При написании дипломной работы собранный во время прохождения студентами производственной и преддипломной практики по исследуемой теме материал дополняется и обновляется.

Содержание и структура глав дипломного проекта могут быть изменены дипломником совместно с руководителем в соответствии с темой дипломного проекта и поставленными задачами.

Глава 2. Практическая часть (наименование главы определяется тематикой дипломной работы, например, Проектирование системы инженерно-технических для защиты). В данной главе должно содержаться пошаговое описание процесса практических мероприятий при решении поставленных задач по защите информации автоматизированных систем. На основе моделирования угроз рассчитывается структура комплекса по защите информации автоматизированных систем. Разрабатывается схема комплексной системы защиты безопасности с расчётом возможностей применяемых инженерно-технических или программно-аппаратных средств.

В заключении могут быть освещены следующие моменты: в заключении кратко и логически последовательно излагаются теоретические и практические выводы и предложения, они должны вытекать из содержания работы и носить обобщающий характер. Из текста заключения должно быть ясно, что цель и задачи дипломного проекта полностью

выполнены. Последовательность изложения выводов должна соответствовать порядку представления материалов в тексте работы. Следует также указать пути внедрения работы (если таковое имеет место), сформулировать перспективные направления развития темы диплома. Заключение представляет собой связный, четкий, компактный текст. Заключение завершается оценкой перспектив исследуемой проблемы в целом. Объем заключения занимает 2 – 3 страницы.

Материалы дипломного проекта должны излагаться четко, ясно, последовательно, соблюдая логичность перехода от одной главы к другой и от одного параграфа к другому. Законченную мысль в тексте необходимо выделять в самостоятельный абзац, применяя для этого «красную строку». Следует использовать принятую научную терминологию, избегать повторений общеизвестных положений, имеющихся в учебниках и учебных пособиях. Уточнять необходимо только понятия малоизвестные или противоречивые, делая ссылку на авторов, высказывающих разные мнения по одному и тому же вопросу. Особое внимание должно быть уделено языку и стилю написания пояснительной записки, свидетельствующей об общем уровне подготовки будущего специалиста, его профессиональной культуре. Стиль написания – безличный монолог, т.е. изложение, ведется от второго лица, множественного числа. Не употребляется форма первого и второго лица местоимений единственного числа.

Во всем дипломном проекте должно быть достигнуто единообразие терминов, обозначений и условных сокращений.

Список литературы (библиографический список) содержит не менее 10 наименований литературных источников, оформляется в соответствии с принятым стандартом (ГОСТ 7.1-2016). В список включаются только те источники, которые использовались при подготовке дипломного проекта и на которые имеются ссылки в основной части работы.

Приложение содержит файлы со всеми компонентами АИС и вспомогательный материал, не включенный в основную часть пояснительной записки (таблицы, схемы, заполненные формы отчетности, инструкции, распечатки, фрагменты нормативных документов и т.д.). Указанный материал включается в приложение с целью сокращения объема основной части, страницы его не входят в подсчет общего объема работы. Конкретный состав приложений, их объем, включая иллюстрационный материал, определяются по согласованию с руководителем дипломного проекта. Объем приложений не ограничивается и не учитывается при определении общего объема работы. Связь приложений с текстом осуществляется с помощью ссылок со словами «смотри», которое сокращается и заключается в круглые скобки.

Файлы с компонентами АИС на CD, DVD, Flash-накопителях. Пояснительная записка дипломного проекта должна быть выполнена машинописным способом с помощью компьютера на одной стороне листа белой бумаги формата А4 (210*297 мм) через полтора межстрочных интервала. Шрифт – 14. Размер полей составляет: левое – 30 мм; правое – 20 мм; верхнее – 20 мм, нижнее – 20 мм. Вписывать в текст отдельные слова, условные знаки допускается только черного цвета, причем плотность вписанного текста должна соответствовать плотности основного текста. Опечатки или графические неточности допускается исправлять путем применения специальных корректирующих средств с последующим внесением исправлений черным цветом. На странице не должно быть более пяти исправлений. Необходимые сноски и подстрочные примечания помещаются в нижней части соответствующей страницы и заканчиваются до границы нижнего поля. Номера страниц проставляются в правом верхнем углу листа, соблюдая сквозную нумерацию по всему тексту работы. Точка в номере страницы не ставится. Титульный лист и задание на дипломное проектирование включаются в общую нумерацию страниц, но номер страницы на них не проставляется. Нумерация начинается с 3-ей страницы – «Содержание». Каждая новая глава и другие структурные элементы работы – введение, заключение, список литературы, приложения, кроме параграфов, входящих в состав глав, начинаются с новой страницы. Фразы, начинающиеся с «красной строки», выделяют абзацным отступом, равным 15 мм (5 печатных знаков).

3.4. Порядок оценки результатов дипломной работы (проекта)

Критерии оценки дипломных проектов Для определения качества выполнения и защиты дипломных проектов предлагаются следующие основные показатели ее оценки:

– соответствие темы исследования сформулированным целям и задачам;

– умение систематизировать и обобщать факты, самостоятельно решать поставленные задачи (в том числе нестандартные) с использованием передовых научных технологий;

– структура дипломной работы и культура ее оформления; последовательность и логичность, завершенность изложения, наличие научно-справочного аппарата, стиль изложения;

– использование в работе научных достижений отечественных и зарубежных исследователей и реального опыта; апробация в среде специалистов-практиков;

– использование современных технологий, применение в работе методов исследования;

– возможность использования результатов в профессиональной практике для решения образовательных задач.

Оценка качества дипломного проекта является комплексной. Государственная экзаменационная комиссия при оценке дипломного проекта обращает внимание на содержание и качество проведенного исследования (проектирования), оформление работы, содержательность ответов студентов на вопросы комиссии, оценку рецензента и отзыв руководителя.

3.5 Порядок оценки защиты дипломной работы (проекта)

Подготовка и защита дипломного проекта студентом позволяет оценить освоение общих и профессиональных компетенций, сформированности личностных результатов. Оценка по результатам защиты дипломного проекта определяется баллами «отлично», «хорошо», «удовлетворительно», «неудовлетворительно».

«отлично»	1. Студент своевременно отчитывался по всем этапам выполнения дипломного проекта 2. Текстовое описание дипломного проекта составлено в полном объеме и аккуратно. 3. Во время защиты студент показал свободное владение темой проекта, знание используемых терминов. Для защиты студент использовал презентацию. 4. Выпускная квалификационная работа соответствует П
«хорошо»	1. Студент своевременно отчитывался по всем этапам выполнения дипломного проекта 2. Текстовое описание дипломного проекта составлено не в полном объеме. 3. Во время защиты студент показал свободное владение темой проекта, знание используемых терминов. Для защиты студент использовал презентацию. 4. Выпускная квалификационная работа соответствует утвержденной теме
«удовлетворительно»	1. Студент несвоевременно отчитывался по всем этапам выполнения дипломного

	проекта 2. Текстовое описание дипломного проекта составлено не в полном объеме и недостаточно аккуратно. 3. Во время защиты студент показал слабые знания по теме проекта. Для защиты студент не использовал презентацию или презентация выполнена на слабом уровне 4. Выпускная квалификационная работа соответствует утвержденной теме
«неудовлетворительно»	1. Студент не выполнил дипломный проект. 2. Студент не владеет темой проекта и не ответил на дополнительные вопросы. 3. Пояснительная записка или выступление студента или приложенные файлы не соответствуют теме проекта.

Пример задания демонстрационного экзамена

Описание модуля А: «Установка, конфигурирование и устранение неисправностей в системе корпоративной защиты от внутренних угроз» Задание выполняется на подготовленных виртуальных машинах: контроллер домена с поднятым DNS и AD, чистая серверная система, чистая клиентская система (2 шт), предустановленный, но не настроенный DLP-сервер (с установленной лицензией).

В компании «Демо Лаб» возникла необходимость внедрения DLP системы для лучшей защиты разработок и предотвращения утечек прочей информации. Вам необходимо установить и настроить компоненты системы в соответствии с выданным заданием.

Основными каналами потенциальной утечки данных являются электронная почта и различные интернет-ресурсы, если не указано иное.

Серверные компоненты устанавливаются в виртуальной среде, сетевые интерфейсы настроены, но IP адреса (и/или DNS сервер) нужно назначить согласно прилагаемой карточке.

Подготовлены следующие виртуальные машины для дальнейшей работы:

• AD и DNS сервер (контроллер домена)

• DLP сервер установлен (но не настроен), активирована лицензия

• Виртуальная машина для установки сервера агентского мониторинга •

Виртуальные машины «нарушителей» (2 шт)

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

Стоит отметить, что имена всех компьютеров (hostname) должны быть уникальными (проверить и исправить самостоятельно).

При выполнении заданий можно пользоваться разрешенными справочными ресурсами в сети Интернет и документацией на компьютерах и/или в общем сетевом каталоге.

Все дистрибутивы находятся в каталоге, указанном в дополнительной карточке задания. Все логины, пароли, сетевые настройки и прочее указаны в дополнительной карточке задания.

В случае отсутствия необходимых для выполнения задания данных, обратитесь к экспертам.

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) или передаются экспертам иным способом по запросу.

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.

При выполнении модуля А ставятся следующие цели:

1. Настроенный контроллер домена.
2. Работоспособный сервер мониторинга сетевого трафика.
3. Установленный и работоспособный сервер агентского мониторинга.
4. Установленные и работоспособные агенты мониторинга на клиентских устройствах
5. Настроенный компонент контроля сетевых хранилищ.
6. Сгенерированные сертификаты безопасности. Установленные на сервер мониторинга сетевого трафика.

При выполнении данного модуля А ставятся следующие задачи: Задача 1: Настройка контроллера домена

Для удобства работы рекомендуется создать подразделение “Test” в корневом каталоге оснастки “Пользователи и компьютеры” AD сервера.

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

Логин: user1, пароль: xxXX1234, права пользователя домена Логин: user2, пароль: xxXX1234, права пользователя домена Логин: admin1, пароль: xxXX1234, права администратора домена

Логин: user3, пароль: xxXX1234, права пользователя домена Логин:

user4, пароль: xxXX1234, права пользователя домена

Задача 2: Настройка DLP сервера

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

Необходимо синхронизировать каталог пользователей и компьютеров LDAP с домена с помощью ранее созданного пользователя user4.

Для входа в веб-консоль необходимо настроить использование ранее созданного пользователя домена user3 с полными правами офицера безопасности и на администрирование системы, полный доступ на все области видимости.

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

Необходимо ввести сервер в домен, после перезагрузки войти в систему от ранее созданного пользователя admin1 (важно). После входа в систему необходимо переместить введенный в домен компьютер в ранее созданное подразделение “Test” на домене.

Установить базуданных PostgreSQLили функциональный аналог с паролем суперпользователя xxXX1234.

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: officer с паролем xxXX1234

Синхронизировать каталог пользователей и компьютеров с Active Directory или функциональным аналогом.

После синхронизации настроить беспарольный вход в консоль управления от ранее созданного доменного пользователя admin1, установить полный доступ к системе, установить все области видимости.

Проверить работоспособность входа в консоль управления без ввода пароля. Если сервер не введен в домен или работает от другого пользователя, данная опция работать не будет.

Задача 4: Установка агента мониторинга на машине нарушителя

Необходимо ввести клиентскую машину 1 в домен, после перезагрузки войти в систему от ранее созданного пользователя user1.

Необходимо ввести клиентскую машину 2 в домен, после перезагрузки войти в систему от ранее созданного пользователя user2.

После входа в систему необходимо переместить веденные в домен компьютеры в ранее созданное подразделение “Test” на домене.

Установить агент мониторинга:

На машину 1 с помощью задачи первичного распространения с сервера агентского мониторинга.

На машину 2 с помощью групповых политик домена.

Необходимо создавать отдельные объекты групповых политик на каждое Задача и делать снимки экрана для подтверждения создания и выполнения политик.

Ручная установка с помощью переноса на машину нарушителя пакета установки является некорректным выполнением задания

Задача 5: Установка и настройка подсистемы сканирования сетевых ресурсов.

Необходимо установить и настроить подсистему сканирования сетевых ресурсов на сервер с установленным сервером агентского мониторинга с настройками по умолчанию.

Необходимо создать общий каталог Test в корне диска сервера и установить права доступа на запись и чтение для всех пользователей домена.

Необходимо настроить подсистему сканирования сетевых ресурсов на автоматическое ежедневное сканирование только ранее созданного каталога. Для работы подсистемы может потребоваться редактирования конфигурационных файлов (для устранения предупреждения).

Задача 6: 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 некий термин, установить уровень угрозы для всех событий, добавить тег.

Проверить срабатываниевсеми четырьмя возможными способами (передачи, копирования, хранения и буфера обмена, хотя бы 1 событие на каждый тип) с помощью виртуальной машины нарушителя 1 с установленным агентом.

Сделать одну выборку, в которой будет отображено только по одному событию каждого типа, настроив конструктор выборки вручную.

Зафиксировать выполнение скриншотом выполненной выборки или конструктора выборки.

Задача 7: Защита системы с помощью сертификатов

Создайте дерево сертификатов формата PKCS для защиты веб-соединения с DLPсервером по протоколу HTTPS. Сертификат и используемый ключ должен удовлетворять общепринятым на сегодня стандартам и требованиям, 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: 1. корневой root-сертификат (ca)

2. серверный (server) сертификат

3. по желанию допускается использование пользовательского и промежуточного сертификата

Поля сертификата заполняются по вариантам заданий.

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 для доверенного подключения к веб-консоли DLP-системы уровня сети.

Итоговый результат должен включать:

Дерево из 2-3 сертификатов, упакованных в пакет PKCS (.p12), а также представленные в виде отдельных файлов ключей сертификатов, расположенных на рабочем столе. Содержимое команд по генерации ключей и сертификатов в текстовом файле 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»).

Описание модуля E: «Технологии защиты узла и агентского мониторинга»

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 (это всегда указывается отдельно).

При выполнении модуля E ставятся следующие цели:

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.

При выполнении модуля Е ставятся следующие задачи:

Задача 1

Необходимо создать 2 новых группы компьютеров: «Test1» и «Test2», а также создать 2 новых политики: «Test1» и «Test2». Каждая из политик должна применяться только на соответствующие группы. Компьютер 1 необходимо перенести в Test1, а компьютер 2 — в Test2.

Зафиксировать выполнение скриншотом.

Задача 2

Для удобства работы офицера безопасности необходимо установить дополнительную консоль управления сервером агентского мониторинга на другую машину для удаленного доступа к серверу агентского мониторинга.

Задача 3: разработать правила агентского мониторинга. Следующие правила создаются в политике «Test1».

Правило 1

Необходимо запретить пользоваться Microsoft Paint, так как участились случаи подделки печатей компании.

Проверить работоспособность и зафиксировать выполнение скриншотом.

Правило 2

Необходимо запретить создание снимков экрана в табличных процессорах для предотвращения утечки секретных расчетов и баз данных.

Проверить работоспособность и зафиксировать выполнение скриншотом.

Правило 3

Ограничить доступ к определенным облачным хранилищам (по вариантам). Проверить работоспособность и зафиксировать выполнение

Правило 4

Необходимо запретить печать на сетевых принтерах.

Зафиксировать создание политики скриншотом.

Правило 5

Необходимо запретить запись файлов на определенные носители информации, при этом оставить возможность считывания информации.

Проверить работоспособность и зафиксировать выполнение

Правило 6

С учетом ранее созданной блокировки необходимо разрешить использование доверенного носителя информации.

Проверить работоспособность и зафиксировать выполнение

Правило 7

Полностью запретить использование определенного устройства для пользователя.

Проверить работоспособность и зафиксировать выполнение

Правило 8

С учетом ранее выполненного запрета необходимо предоставить временный доступ для определенного устройства не определенное время для пользователя.

Зафиксировать этапы выдачи доступа и работоспособность скриншотами.

Задача 4: разработать правила агентского мониторинга. Следующие правила создаются в политике «Test2».

Правило 9

Необходимо поставить на контроль буфер обмена в блокноте и notepad++. Проверить занесение нескольких событий в WEB-консоль.

Проверить работоспособность и зафиксировать выполнение скриншотом.

Правило 10

Необходимо запретить использовать терминальные сессиидля пользователя.

Проверить работоспособность и зафиксировать выполнение

Правило 11

Необходимо установить контроль за компьютером потенциального нарушителя путем создания снимков экрана каждые 60 секунд или при смене окна.

Проверить работоспособность и зафиксировать выполнение

Правило 12

Запретить передачу файлов определенного типа на съемные носители информации или в сетевое расположение.

Проверить работоспособность и зафиксировать выполнение

Задача 5: разработать и применить групповые политики домена.

Групповые применяются только на компьютер 2, должны быть созданы в домене.

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

Групповая политика 1

Настроить политику паролей и блокировки: Максимальный срок действия пароля,

Минимальная длина пароля, Сложность пароля, Блокировка учетной записи при неверном вводе пароля.

Зафиксировать настройки политики скриншотами.

Групповая политика 2

Запретить запуск приложений по списку (по вариантам задания). Зафиксировать настройки политики и выполнение скриншотами.

Групповая политика 3

Запретить использование элементов системы стандартными политиками.

Зафиксировать настройки политики и выполнение скриншотами.

Групповая политика 4

Запретить пользователю самостоятельно менять параметры системы (по вариантам задания).

Зафиксировать настройки политики и выполнение скриншотами.

Групповая политика 5

Настроить дополнительные параметры системы, которые должны применяться для пользователя или компьютера (по вариантам задания).

Зафиксировать настройки политики и выполнение скриншотами.

Описание модуля С: «Разработка политик безопасности в системе корпоративной защиты информации от внутренних угроз»

Создайте в DLP-системе политики безопасности согласно

нижеперечисленным заданиям. Политики должны автоматически блокировать трафик и/или предупреждать о нарушении в соответствии с заданием. Способ, которым создана корректная политика, оставлен на усмотрение самого экзаменуемого.

При выявлении уязвимости DLP-система должна автоматически устанавливать уровень угрозы в соответствии с заданием. После создания всех политик может быть запущен автоматический «генератор трафика», который передаст поток данных, содержащих как утечки, так и легальную информацию.

При правильной настройке политики должны автоматически выявить (илиблокировать) и маркировать инциденты безопасности. Не должно быть ложных срабатываний. Не должно быть неправильной маркировки. Должны быть выявлены все инциденты безопасности.

Для некоторых политик могут понадобиться дополнительные файлы, расположение которых можно узнать из карточки задания или у экспертов.

Выполнение отдельных заданий необходимо подтвердить скриншотом (это всегда указывается отдельно). Скриншоты необходимо сохранить в папке «Модуль 3».

Скриншоты необходимо называть в соответствии с номером задания и типом задания

(Например Политика 2, Задание 1–1 и т. д.)

Задания на разработку политик можно выполнять в любом порядке. Наиболее сложные политики находятся в конце.

При разработке политик стоит учитывать, что все политики трафика могут передаваться как через веб-сообщения, так и черезпочтовые сообщения. Вслучае, если данный пункт не соблюден, то проверка заданий может быть невозможной.

Списки сотрудников, занимаемые позиции и отделы сотрудников представлены в разделе «Персоны» по результатам LDAP-синхронизации.

Список тегов для политик:

Политика 1, Политика 2, Политика 3, …

При выполнении модуля С ставятся следующие цели:

1. Настроить систему предотвращения утечек для правильного функционирования политик безопасности.

2. Произвести настройку технологий, используемых в политиках безопасности, а именно: лингвистический анализ, регулярные выражения, эталонные документы, графические объекты, выгрузки из баз данных.

3. Произвести верную настройку объектов защиты, верно выстроить логику срабатывания.

4. Разработать политики безопасности для корректного срабатывания политик, указать направления передачи, уровень нарушений, вердикты, теги.

5. Произвести проверку работоспособности политик.

При выполнении модуля С ставятся следующие задачи: Задача 1.1

Необходимо выключить или удалить стандартные политики и отключить стандартные каталоги объектов защиты.

Задача 1.2

Создайте локальную группу пользователей и добавьте в нее пользователей.

Задача 1.3

Создать список веб-ресурсов. Добавить в список следующие сайты: Site.ru, domain.com,

Задача 1.4

Для работы системы необходимо настроить периметр компании: Почтовый домен, список веб ресурсов, группа персон, исключить из перехвата.

Задача 2

Для контроля за движением документов необходимо вести наблюдение за передачей шаблона документа за пределы компании. Стоит учесть, что содержимое документа может изменяться в пределах определенного уровня.

Вердикт: разрешить Уровень нарушения: низкий Тег: Задача 2

Задача 3

У генерального директора компании недавно появился котик и его фото утекло в сеть компании. Теперь сотрудники обмениваются смешными картинками с подписями и масками внутри компании и выкладывают их в социальные сети. Директор решил, что его котик вызвал снижение качества работы сотрудников из-за повышенной милоты картинок и хочет запретить обмен фотографией котика. Необходимо запретить обмен фотографией и немного измененной фотографией котика.

Вердикт: блокировать Уровень нарушения: низкий

Задача 4

Необходимо отслеживать документы, содержащие печать компании всем сотрудникам, кроме отдела (по вариантам) и определенного сотрудника. Они могут обмениваться документами внутри и за пределами компании без контроля.

Вердикт: разрешить Уровень нарушения: низкий

Задача 5

В последнее время возникла необходимость обработки текстовых данных, а также сканов и фото кредитных карт. Необходимо отслеживать передачу всех возможных данных кредитных карт (в том числе сканов) за пределы компании.

Вердикт: разрешить

Уровень нарушения: средний Тег: Задача 5

Задача 6

Сотрудники заподозрены в сливе баз данных клиентов. Необходимо настроить мониторинг выгрузок из БД для контроля движения данных из базы данных страховых компаний только при отправке из определенного отдела, для остальных контролировать не нужно.

Критичными данными в выгрузке являются определенные поля и в 1 документе присутствует более 1 строчки. Для настройки используйте файл примера.

Вердикт: разрешить

Уровень нарушения: средний Тег: Задача 6

Задача 7

Некая компания попросила обеспечить защиту от утечки важных данных.

Необходимо создать политику на контроль правила передачи содержащие слова «один», «два», «три» в 1 сообщении или документе одновременно. Если в Документе встречается только по 1 слову из перечисленных —Задача срабатывать не должна.

Правило должно срабатывать на сообщения, которые отправляются за пределы компании всеми пользователями, кроме определенного отдела, который может отсылать информацию свободно.

Вердикт: разрешить

Уровень нарушения: средний Тег: Задача 7

Задача 8

Для мониторинга движения анкет необходимо вести наблюдение за анкетами компании за пределы компании, запрещая любую внешнюю передачу документов в пустых и заполненных бланках.

Генеральный директор и совет директоров могут обмениваться данной информацией совершенно свободно. Вердикт: разрешить Уровень нарушения: средний

Задача 9

Пользователи стали часто обмениваться ссылками и файлами, в связи с этим необходимо блокировать передачу (а где это невозможно — просто контролировать) файлов, например формата.mp4 и ссылок определенного формата (содержит уникальную последовательность, например urlname). Ложных срабатываний быть не должно.

Вердикт: Заблокировать Уровень нарушения: средний Тег: Задача 9

Задача 10

Было замечено, что сотрудники компании стали получать множество рекламных сообщений электронной почты, из-за чего возникла необходимость отследить утечку баз email адресов сотрудников. В связи с этим необходимо детектировать сообщения, содержащие адреса электронной почты.

Важно, чтобы в одном сообщении содержалось минимум 2 адреса (т. к. в противном случае будут детектироваться все почтовые сообщения)!

Возможные домены первого уровня: ru, org и прочие. Детектирование только частей адресов (например @mail.ru) недопустимо.

Вердикт: разрешить

Уровень нарушения: высокий Тег: Задача 10

Задача 11

В связи с разгильдяйством сотрудников, передающих свои пароли коллегам с помощью почты и сообщений, необходимо предотвратить передачу любых

стандартизированных паролей для информационной системы в открытом виде любыми отправителями и получателями как внутри, так и за пределы компании.

Стоит учесть, что пароли могут передаваться любым указанным способом: социальные сети и прочие ресурсы (в браузере), мессенджеры, почта, флешки. Необходимо также контролировать наличие паролей в сетевых каталогах.

Стоит учесть, что отдел так как генерацией паролей занимается отдел ИТ, то пользователи отдела могут рассылать пароли пользователям совершенно свободно, но только внутри компании.

Стандартизированные форматы паролей (кириллица):
6 букв – 1 знак !?#$^/_& – 2-4 цифры – 4 буквы – 2-3 знака !?#$^/_& (например, ПаРолЬ#67рКнЕ!?)

Вердикт: разрешить

Уровень нарушения: средний Тег: Задача 11

Задача 12

Необходимо контролировать передачу определенных типов файлов только за пределы компании.

Вердикт: разрешить Уровень нарушения: низкий Тег: Задача 12

Задача 13

В связи с тем, что компания является оператором обработки персональных данных,

необходимо запретить всем сотрудникам кроме отдела (по вариантам) отправлять документы, содержащие информацию о паспортных данных за пределы компании. Отдел (по вариантам) может отправлять файлы без ограничений.

Вердикт: разрешить Уровень нарушения: низкий Тег: Задача 13

Описание модуля F: «Предотвращение инцидентов и управление событиями информационной безопасности»

Необходимо настроить виджеты и отчеты в системе предотвращения утечек.

При выполнении модуля F ставятся следующие цели: 1. Настройка контроля доступа к системе.

2. Разработка виджетов и отчетов, отображающих определенные события и инциденты безопасности.

При выполнении модуля F ставятся следующие задачи: Задача 1: Контроль доступа

Необходимо создать пользователя DLP системы с определенными правами просмотра и редактирования.

Задача 2: Сводки

Создайте новые вкладки сводки в разделе «Сводка»

Задача 3: Виджеты

Создайте в сводке 4 виджета:

9. Выборка по событиям за период

10. Выборка по политикам с технологиями за период 11. Статистика за период

12. По нарушителям за период

Задача 4

Необходимо создать виджет отображающий события определенного типа (с определенного устройства и т. п.) за период.

Зафиксировать скриншотом конструктора выборки.

Задача 5

Необходимо создать виджет отображающий события определенного уровня (определенных политик и т. п.) за период. Инструкция по охране труда и технике безопасности для проведения демонстрационного экзамена

1.1. Программа инструктажа по охране труда и технике безопасности

Инструктаж по охране труда и технике безопасности должен включать: Общие сведения о месте проведения экзамена, расположении компетенции, времени трансфера до

места проживания, расположении транспорта для площадки, особенности питания участников и экспертов, месторасположении санитарно-бытовых помещений, питьевой воды, медицинского пункта, аптечки первой помощи, средств первичного пожаротушения.

 Время начала и окончания проведения экзаменационных заданий, нахождение посторонних лиц на площадке.

 Контроль требований охраны труда участниками и экспертами.

 Вредные и опасные факторы во время выполнения экзаменационных заданий и нахождение на территории проведения экзамена.

 Общие обязанности участника и экспертов по охране труда, общие правила поведения во время выполнения экзаменационных заданий и на территории.

 Основные требования санитарии и личной гигиены.

 Средства индивидуальной и коллективной защиты, необходимость их использования.

 Порядок действий при плохом самочувствии или получении травмы. Правила оказания первой помощи.

 Действия при возникновении чрезвычайной ситуации, ознакомление со схемой эвакуации и пожарными выходами.

1.2. Инструкция по охране труда для участников

1.2.1. Общие требования охраны труда

• К самостоятельному выполнению заданий экзамена по стандартам «WorldSkills» допускаются участники:

• прошедшие инструктаж по охране труда по «Программе инструктажа по охране труда и технике безопасности»;

• ознакомленные с инструкцией по охране труда;

• имеющие необходимые навыки по эксплуатации инструмента, приспособлений совместной работы на оборудовании;

• не имеющие противопоказаний к выполнению заданий по состоянию здоровья.

• При работе с ПК рекомендуется организация перерывов на через каждые 45 минут работы.

• При работе на ПК могут воздействовать опасные и вредные производственные факторы:

• физические: повышенный уровень электромагнитного излучения; повышенный уровень статического электричества; повышенная яркость светового изображения; повышенный уровень пульсации светового потока; повышенное значение напряжения в электрической цепи, замыкание которой может произойти через тело человека; повышенный или пониженный уровень освещенности; повышенный уровень прямой и отраженной блескости;

• психофизиологические: напряжение зрения и внимания; интеллектуальные и эмоциональные нагрузки; длительные статические нагрузки; монотонность труда.

• Запрещается находиться возле ПК в верхней одежде, принимать пищу и курить, употреблять во время выполнения задания алкогольные напитки, а также приходить на площадку в состоянии алкогольного, наркотического или другого опьянения.

• Участник экзамена должен знать месторасположение первичных средств пожаротушения.

• О каждом несчастном случае пострадавший или очевидец несчастного случая немедленно должен известить ближайшего эксперта. • В помещении экспертов находится аптечка первой помощи, укомплектованная изделиями медицинского назначения, ее необходимо использовать для оказания первой помощи, самопомощи в случаях получения травмы.

• В случае возникновения несчастного случая или болезни участника, об этом

немедленно уведомляются Главный эксперт и линейные Эксперты. Главный эксперт принимает решение о назначении дополнительного времени для участия. В случае отстранения участника от дальнейшего участия в экзамене ввиду болезни или несчастного случая, он получит баллы за любую завершенную работу.

• Вышеуказанные случаи подлежат обязательной регистрации в Форме регистрации несчастных случаев и в Форме регистрации перерывов в работе. Знаки безопасности, используемые на рабочем месте, для обозначения присутствующих опасностей:

• F 04 Огнетушитель

• E 22 Указатель выхода

• E 23 Указатель запасного выхода

• EC 01 Аптечка первой медицинской помощи

• При работе с ПК участники экзамена должны соблюдать правила личной гигиены.

• Работа на площадке разрешается исключительно в присутствии эксперта.

Запрещается присутствие на площадке посторонних лиц. • По всем вопросам, связанным с работой компьютера, следует обращаться к техническому эксперту.

• Участники, допустившие невыполнение или нарушение инструкции по охране труда, привлекаются к ответственности в соответствии с Регламентом.

• Несоблюдение норм безопасности может привести к временному или перманентному отстранению аналогично апелляции

1.2.2. Требования охраны труда перед началом выполнения работ

• В подготовительный день все участники должны ознакомиться с инструкцией по технике безопасности, с планами эвакуации при возникновении пожара, местами расположения санитарно-бытовых помещений, медицинскими кабинетами, питьевой воды, подготовить рабочее место в соответствии с Техническим описанием компетенции

• По окончании ознакомительного периода, участники подтверждают свое ознакомление со всеми процессами, подписав лист прохождения инструктажа по работе на оборудовании по форме, определенной Оргкомитетом.

• Подготовить рабочее место:

• Осмотреть и привести в порядок рабочее место, убрать все посторонние предметы, которые могут отвлекать внимание и затруднять работу.

• Проверить правильность установки стола, стула, подставки под ноги, угол наклона экрана монитора, положения клавиатуры в целях исключения неудобных поз и длительных напряжений тела. Особо обратить внимание на то, что дисплей должен находиться на расстоянии не менее 50 см от глаз (оптимально 60-70 см).

• Проверить правильность расположения оборудования.

• Кабели электропитания, удлинители, сетевые фильтры должны находиться с тыльной тороны рабочего места, сетевые фильтры не должны лежать на полу.

• Убедиться в отсутствии засветок, отражений и бликов на экране монитора.

• Убедиться в том, что на устройствах ПК (системный блок, монитор, клавиатура) не располагаются сосуды с жидкостями, сыпучими материалами (чай, кофе, сок, вода и пр.).

• Включить электропитание в последовательности, установленной инструкцией по эксплуатации на оборудование; убедиться в правильном выполнении процедуры загрузки оборудования, правильных настройках. Участнику запрещается приступать к выполнению задания при обнаружении неисправности оборудования. О замеченных недостатках и неисправностях немедленно сообщить Эксперту и до устранения неполадок к заданию не приступать.

1.2.3. Требования охраны труда во время выполнения работ

• В течение всего времени выполнения задания со средствами компьютерной и оргтехники участник экзамена обязан: • содержать в порядке и чистоте рабочее место;

• следить за тем, чтобы вентиляционные отверстия устройств ничем не были закрыты;

• выполнять требования инструкции по эксплуатации оборудования;

• соблюдать, установленные расписанием, перерывы в выполнении задания, выполнять рекомендованные физические упражнения.

• Участнику запрещается во время выполнения задания:

• отключать и подключать интерфейсные кабели периферийных устройств если это не указано в задании;

• класть на устройства средств компьютерной и оргтехники бумаги, папки и прочие посторонние предметы;

• прикасаться к задней панели системного блока (процессора) при включенном питании;

• отключать электропитание во время выполнения программы, процесса;

• допускать попадание влаги, грязи, сыпучих веществ на устройства средств компьютерной и оргтехники;

• производить самостоятельно вскрытие и ремонт оборудования;

• работать со снятыми кожухами устройств компьютерной и оргтехники;

• располагаться при работе на расстоянии менее 50 см от экрана монитора.

• При работе с текстами на бумаге, листы надо располагать как можно ближе к экрану, чтобы избежать частых движений головой и глазами при переводе взгляда.

• Рабочие столы следует размещать таким образом, чтобы экран монитора был ориентирован боковой стороной к световым проемам, чтобы естественный свет падал преимущественно слева.

• Освещение не должно создавать бликов на поверхности экрана.

• Продолжительность работы на ПК без регламентированных перерывов не должна превышать 1-го часа. Во время регламентированного перерыва с целью снижения нервноэмоционального напряжения, утомления зрительного аппарата, необходимо выполнять комплексы физических упражнений.

• При неисправности инструмента и оборудования – прекратить выполнение задания и сообщить об этом Эксперту, а в его отсутствие заместителю главного Эксперта.

1.2.4. Требования охраны труда в аварийных ситуациях

• При обнаружении неисправности в работе электрических устройств, находящихся под напряжением (повышенном их нагреве, появления искрения, запаха гари, задымления и т. д.), участнику следует немедленно сообщить о случившемся Экспертам. Выполнение задания продолжить только после устранения возникшей неисправности.

• В случае возникновения у участника плохого самочувствия или получения травмы сообщить об этом эксперту.

• При поражении участника электрическим током немедленно отключить электросеть, оказать первую помощь (самопомощь) пострадавшему, сообщить Эксперту, при необходимости обратиться к врачу.

• При несчастном случае или внезапном заболевании необходимо в первую очередь отключить питание электрооборудования, сообщить о случившемся Экспертам, которые должны принять мероприятия по оказанию первой помощи пострадавшим, вызвать скорую медицинскую помощь, при необходимости отправить пострадавшего в ближайшее лечебное учреждение.

• При возникновении пожара необходимо немедленно оповестить Главного эксперта и экспертов. При последующем развитии событий следует руководствоваться указаниями

Главного эксперта или эксперта, заменяющего его. Приложить усилия для исключения состояния страха и паники.

• При обнаружении очага возгорания на площадке необходимо любым возможным способом постараться загасить пламя в "зародыше" с обязательным соблюдением мер личной безопасности.

• При возгорании одежды попытаться сбросить ее. Если это сделать не удается, упасть на пол и, перекатываясь, сбить пламя; необходимо накрыть горящую одежду куском плотной ткани, облиться водой, запрещается бежать – бег только усилит интенсивность горения.

• В загоревшемся помещении не следует дожидаться, пока приблизится пламя.

Основная опасность пожара для человека – дым. При наступлении признаков удушья лечь на пол и как можно быстрее ползти в сторону эвакуационного выхода.

• При обнаружении взрывоопасного или подозрительного предмета не подходите близко к нему, предупредите о возможной опасности находящихся поблизости экспертов или обслуживающий персонал. • При происшествии взрыва необходимо спокойно уточнить обстановку и действовать по указанию экспертов, при необходимости эвакуации возьмите с собой документы и предметы первой необходимости, при передвижении соблюдайте осторожность, не трогайте поврежденные конструкции, оголившиеся электрические провода.

В разрушенном или поврежденном помещении не следует пользоваться открытым огнем (спичками, зажигалками и т. п.). 1.2.5. Требование охраны труда по окончании работ

• По окончании работы участник экзамена обязан соблюдать следующую последовательность отключения оборудования:

• произвести завершение всех выполняемых на ПК задач; • отключить питание в последовательности, установленной инструкцией по эксплуатации данного оборудования.

• Убрать со стола рабочие материалы и привести в порядок рабочее место. • Обо всех замеченных неполадках сообщить эксперту. • Сообщить эксперту о выявленных во время выполнения заданий неполадках и неисправностях оборудования, и других факторах, влияющих на безопасность выполнения задания.

1.3. Инструкция по охране труда для экспертов

1.3.1. Общие требования охраны труда

• К работе в качестве эксперта Компетенции «Корпоративная защита от внутренних угроз информационной безопасности» допускаются Эксперты, прошедшие специальное обучение и не имеющие противопоказаний по состоянию здоровья.

• Эксперт с особыми полномочиями, на которого возложена обязанность за проведение инструктажа по охране труда, должен иметь действующие удостоверение «О проверке знаний требований охраны труда».

• В процессе контроля выполнения заданий и нахождения на площадке Эксперт обязан четко соблюдать:

• инструкции по охране труда и технике безопасности;

• правила пожарной безопасности, знать места расположения первичных средств пожаротушения и планов эвакуации.

• расписание и график проведения задания, установленные режимы труда и отдыха.

• При работе на персональном компьютере и копировально множительной технике на Эксперта могут воздействовать следующие вредные и (или) опасные производственные факторы:

• электрический ток;

• статическое электричество, образующееся в результате трения движущейся бумаги с рабочими механизмами, а также при некачественном заземлении аппаратов;

• шум, обусловленный конструкцией оргтехники;

• химические вещества, выделяющиеся при работе оргтехники;

• зрительное перенапряжение при работе с ПК.

• При несчастном случае пострадавший или очевидец несчастного случая обязан немедленно сообщить о случившемся Главному Эксперту. В помещении Экспертов Компетенции «Корпоративная защита от внутренних угроз информационной безопасности» находится аптечка первой помощи, укомплектованная изделиями медицинского назначения, ее необходимо использовать для оказания первой помощи, самопомощи в случаях получения травмы. В случае возникновения несчастного случая или болезни Эксперта, об этом немедленно уведомляется Главный эксперт.

• Эксперты, допустившие невыполнение или нарушение инструкции по охране труда, привлекаются к ответственности в соответствии с Регламентом, а при необходимости

согласно действующему законодательству.

1.3.2. Требования охраны труда перед началом работы

• Перед началом работы Эксперты должны выполнить следующее:

• В подготовительный день, Эксперт с особыми полномочиями, ответственный за охрану труда, обязан провести подробный инструктаж по «Программе инструктажа по охране труда и технике безопасности», ознакомить экспертов и участников с инструкцией по технике безопасности, с планами эвакуации при возникновении пожара, с местами расположения санитарно-бытовых помещений, медицинскими кабинетами, питьевой воды, проконтролировать подготовку рабочих мест участников в соответствии с Техническим описанием компетенции.

• Ежедневно, перед началом работ на площадке и в помещении экспертов необходимо:

• осмотреть рабочие места экспертов и участников;

• привести в порядок рабочее место эксперта;

• проверить правильность подключения оборудования в электросеть;

• Эксперту запрещается приступать к работе при обнаружении неисправности оборудования. О замеченных недостатках и неисправностях немедленно сообщить Техническому Эксперту и до устранения неполадок к работе не приступать.

1.3.3. Требования охраны труда во время работы

• Изображение на экранах видеомониторов должно быть стабильным, ясным и предельно четким, не иметь мерцаний символов и фона, на экранах не должно быть бликов и отражений светильников, окон и окружающих предметов.

• Суммарное время непосредственной работы с персональным компьютером и другой оргтехникой в течение дня должно быть не более 6 часов. Продолжительность непрерывной работы с персональным компьютером и другой оргтехникой без регламентированного перерыва не должна превышать 2-х часов. Через каждый час работы следует делать регламентированный перерыв продолжительностью 15 мин.

• Во избежание поражения током запрещается:

• прикасаться к задней панели персонального компьютера и другой оргтехники, монитора при включенном питании;

• допускать попадания влаги на поверхность монитора, рабочую поверхность клавиатуры, дисководов, принтеров и других устройств;

• производить самостоятельно вскрытие и ремонт оборудования;

• переключать разъемы интерфейсных кабелей периферийных устройств при включенном питании;

• загромождать верхние панели устройств бумагами и посторонними предметами;

• допускать попадание влаги на поверхность системного блока, монитора, рабочую поверхность клавиатуры, дисководов, принтеров и др. устройств;

• При выполнении модулей задания участниками, Эксперту необходимо быть внимательным, не отвлекаться посторонними разговорами и делами без необходимости, не отвлекать других Экспертов и участников.

• Эксперту во время работы с оргтехникой:

• обращать внимание на символы, высвечивающиеся на панели оборудования, не игнорировать их;

• не снимать крышки и панели, жестко закрепленные на устройстве. В некоторых компонентах устройств используется высокое напряжение или лазерное излучение, что может привести к поражению электрическим током или вызвать слепоту;

• не производить включение/выключение аппаратов мокрыми руками;

• не ставить на устройство емкости с водой, не класть металлические предметы;

• не эксплуатировать аппарат, если он перегрелся, стал дымиться, появился посторонний запах или звук;

• не эксплуатировать аппарат, если его уронили или корпус был поврежден;

• вынимать застрявшие листы можно только после отключения устройства из сети;

• запрещается перемещать аппараты включенными в сеть;

• все работы по замене картриджей, бумаги можно производить только после отключения аппарата от сети;

• обязательно мыть руки теплой водой с мылом после каждой чистки картриджей, узлов и т. д.;

• просыпанный тонер, носитель немедленно собрать пылесосом или влажной ветошью.

• Включение и выключение персонального компьютера и оргтехники должно проводиться в соответствии с требованиями инструкции по эксплуатации.

• Запрещается:

• устанавливать неизвестные системы паролирования и самостоятельно проводить переформатирование диска;

• иметь при себе любые средства связи;

• пользоваться любой документацией кроме предусмотренной заданием. • При неисправности оборудования – прекратить работу и сообщить об этом Техническому эксперту, а в его отсутствие заместителю главного Эксперта.

• При нахождении на площадке Эксперту:

• одеть необходимые средства индивидуальной защиты;

• передвигаться по площадке не спеша, не делая резких движений, смотря под ноги.

1.3.4. Требования охраны труда в аварийных ситуациях

• При обнаружении неисправности в работе электрических устройств, находящихся под напряжением (повышенном их нагреве, появления искрения, запаха гари, задымления и т.д.),

Эксперту следует немедленно отключить источник электропитания и принять меры к устранению неисправностей, а также сообщить о случившемся Техническому Эксперту.

Выполнение задания продолжать только после устранения возникшей неисправности.

• В случае возникновения зрительного дискомфорта и других неблагоприятных субъективных ощущений следует ограничить время работы с персональным компьютером и другой оргтехникой, провести коррекцию длительности перерывов для отдыха или провести смену деятельности на другую, не связанную с использованием персонального компьютера и другой оргтехники.

• При поражении электрическим током немедленно отключить электросеть, оказать первую помощь (самопомощь) пострадавшему, сообщить Главному Эксперту, при необходимости обратиться к врачу.

• При возникновении пожара необходимо немедленно оповестить Главного эксперта.

При последующем развитии событий следует руководствоваться указаниями Главного эксперта или должностного лица, 20 заменяющего его. Приложить усилия для исключения состояния страха и паники.

• При обнаружении очага возгорания на площадке необходимо любым возможным способом постараться загасить пламя в «зародыше» с обязательным соблюдением мер личной безопасности.

• При возгорании одежды попытаться сбросить ее. Если это сделать не удается, упасть на пол и, перекатываясь, сбить пламя; необходимо накрыть горящую одежду куском плотной ткани, облиться водой, запрещается бежать – бег только усилит интенсивность горения.

• В загоревшемся помещении не следует дожидаться, пока приблизится пламя.

Основная опасность пожара для человека – дым. При наступлении признаков удушья лечь на пол и как можно быстрее ползти в сторону эвакуационного выхода.

• При обнаружении взрывоопасного или подозрительного предмета не подходить близко к нему, предупредить о возможной опасности находящихся поблизости ответственных лиц.

• При происшествии взрыва необходимо спокойно уточнить обстановку и действовать по указанию должностных лиц, при необходимости эвакуации, эвакуировать участников и

других экспертов, и площадки, взять те с собой документы и предметы первой необходимости, при передвижении соблюдать осторожность, не трогать поврежденные конструкции, оголившиеся электрические провода. В разрушенном или поврежденном помещении не следует пользоваться открытым огнем (спичками, зажигалками и т. п.).

1.3.5. Требование охраны труда по окончании выполнения работы

• После окончания дня Эксперт обязан:

• Отключить электрические приборы, оборудование, инструмент и устройства от источника питания.

• Привести в порядок рабочее место Эксперта и проверить рабочие места участников.

• Сообщить Техническому эксперту о выявленных во время выполнения заданий неполадках и неисправностях оборудования, и других факторах, влияющих на безопасность труда