МИНИСТЕРСТВО ОБРАЗОВАНИЯ БЕЛГОРОДСКОЙ ОБЛАСТИ
ОБЛАСТНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ПРОФЕССИОНАЛЬНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
«АЛЕКСЕЕВСКИЙ КОЛЛЕДЖ»

СОГЛАСОВАНО:

УТВЕРЖДАЮ:
Директор ОГАПОУ
«Алексеевский колледж»

_____О.В. Афанасьева
_____г.

КОМПЛЕКТ КОНТРОЛЬНО-ОЦЕНОЧНЫХ СРЕДСТВ ПО ПРОФЕССИОНАЛЬНОМУ МОДУЛЮ

ПМ.03 Защита информации техническими средствами

программы подготовки специалистов среднего звена
по специальности СПО

10.02.05 Обеспечение информационной безопасности автоматизированных систем

Алексеевка - 2022

Комплект оценочных средств разработан на основе Федерального государственного образовательного стандарта среднего профессионального образования по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем и рабочей программы ПМ 03. Защита информации техническими средствами.

Разработчик:

ОГАПОУ «Алексеевский колледж»	преподаватель	И.Д. Гадяцкая
(место работы)	(занимаемая должность)	(инициалы, фамилия)

Эксперт:

(место работы)	(занимаемая должность)	(инициалы, фамилия)

1. ОБЩИЕ ПОЛОЖЕНИЯ

Контрольно-оценочные средства (далее – КОС) по профессиональному модулю 03 Защита информации техническими средствами является частью программы подготовки специалистов среднего звена по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем и предназначен для оценки результатов освоения профессионального модуля. Результатом освоения профессионального модуля является готовность обучающегося к выполнению вида деятельности - Защита информации техническими средствами и составляющих его профессиональных компетенций, а также общие компетенции, формирующиеся в процессе освоения ППССЗ в целом.

Форма промежуточной аттестации по ПМ – экзамен по модулю.

Итогом экзамена является однозначное решение: «вид профессиональной деятельности освоен/не освоен».

Условием допуска к экзамену по модулю является успешное освоение обучающимися всех элементов программы профессионального модуля: программы МДК.03.01 Техническая защита информации, МДК.03.02 Инженерно-технические средства физической защиты объектов информатизации, учебной и производственной практики.

Формы промежуточной аттестации по профессиональному модулю

Таблица 1.

Элемент модуля	**Форма контроля и оценивания**	
	Промежуточная аттестация	**Текущий контроль**
МДК.03.01 Техническая защита информации	Экзамен	Экспертное наблюдение выполнения лабораторных работ, экспертное наблюдение выполнения практических работ, оценка решения ситуационных задач, оценка процесса и результатов выполнения видов работ на практике
МДК.03.02 Инженерно-технические средства физической защиты объектов информатизации	Экзамен	Экспертное наблюдение выполнения лабораторных работ, экспертное наблюдение выполнения практических работ, оценка решения ситуационных задач,

		оценка процесса и результатов выполнения видов работ на практике
УП.03 Учебная практика	Дифференцированный зачет	Экспертная оценка в рамках текущего контроля в ходе проведения учебной практики.
ПП.03 Производственная практика	Дифференцированный зачет	Экспертная оценка в рамках текущего контроля в ходе проведения производственной практики.

2. РЕЗУЛЬТАТЫ ОСВОЕНИЯ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ, ПОДЛЕЖАЩИЕ ПРОВЕРКЕ

2.1. Профессиональные и общие компетенции

Целью экзамена по модулю является комплексная проверка готовности к овладению обучающимися видом деятельности и сформированности у них основных профессиональных и общих компетенций по запланированным показателям оценки результата.

Результатом освоения профессионального модуля является овладение обучающимися видом деятельности - Защита информации техническими средствами, в том числе общими компетенции (ОК) и профессиональными компетенциями (ПК):

Таблица 2.

Коды и наименования проверяемых компетенций или их сочетаний	**Показатели оценки результата**
ОК 01. Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам.	– обоснованность постановки цели, выбора и применения методов и способов решения профессиональных задач; - адекватная оценка и самооценка эффективности и качества выполнения профессиональных задач
ОП 02.Осуществлять поиск, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности.	- использование различных источников, включая электронные ресурсы, медиаресурсы, Интернет-ресурсы, периодические издания по специальности для решения профессиональных задач
ОК 03. Планировать и реализовывать собственное профессиональное и личностное развитие.	- демонстрация ответственности за принятые решения - обоснованность самоанализа и коррекция результатов собственной работы;
ОК 04. Работать в коллективе и команде,	- взаимодействие с обучающимися,

эффективно взаимодействовать с коллегами, руководством, клиентами.	преподавателями и мастерами в ходе обучения, с руководителями учебной и производственной практик; - обоснованность анализа работы членов команды (подчиненных)
ОК 05. Осуществлять устную и письменную коммуникацию на государственном языке с учетом особенностей социального и культурного контекста.	-грамотность устной и письменной речи, - ясность формулирования и изложения мыслей
ОК 06. Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных общечеловеческих ценностей.	- соблюдение норм поведения во время учебных занятий и прохождения учебной и производственной практик,
ОК 07. Содействовать сохранению окружающей среды, ресурсосбережению, эффективно действовать в чрезвычайных ситуациях.	- эффективность выполнения правил ТБ во время учебных занятий, при прохождении учебной и производственной практик; - знание и использование ресурсосберегающих технологий в области телекоммуникаций
ОК 08. Использовать средства физической культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и поддержание необходимого уровня физической подготовленности.	- эффективность выполнения правил ТБ во время учебных занятий, при прохождении учебной и производственной практик;
ОК 09. Использовать информационные технологии в профессиональной деятельности.	- эффективность использования информационно-коммуникационных технологий в профессиональной деятельности согласно формируемым умениям и получаемому практическому опыту;
ОК 10. Пользоваться профессиональной документацией на государственном и иностранном языках.	- эффективность использования в профессиональной деятельности необходимой технической документации, в том числе на английском языке.
ПК 3.1 Осуществлять установку, монтаж, настройку и техническое обслуживание технических средств защиты информации в соответствии с требованиями эксплуатационной документации	Демонстрировать умения и практические навыки в установке, монтаже, настройке ипроведении технического обслуживания технических средств защиты информации в соответствии с требованиями эксплуатационной документации
ПК 3.2 Осуществлять эксплуатацию технических средств защиты информации в соответствии с требованиями эксплуатационной документации	Проявлять умения и практического опыта в эксплуатации технических средств защиты информации в соответствии с требованиями эксплуатационной документации

ПК 3.3. Осуществлять измерение параметров побочных электромагнитных излучений и наводок (ПЭМИН), создаваемых техническими средствами обработки информации ограниченного доступа	Проводить работы по измерению параметров побочных электромагнитных излучений и наводок (ПЭМИН), создаваемых техническими средствами обработки информации ограниченного доступа
ПК 3.4 Осуществлять измерение параметров фоновых шумов, а также физических полей, создаваемых техническими средствами защиты информации	Проводить самостоятельные измерения параметров фоновых шумов, а также физических полей, создаваемых техническими средствами защиты информации
ПК 3.5 Организовывать отдельные работы по физической защите объектов информатизации	Проявлять знания в выборе способов решения задач по организации отдельных работ по физической защите объектов информатизации

2.2. Портфолио как контрольно-оценочное средство профессионального модуля

Портфолио обучающихся ОГАПОУ «Алексеевский колледж» - это комплекс документов (грамоты, дипломы, сертификаты, копии приказов, фотодокументы и т.д.), отзывов и продуктов различных видов деятельности: как учебной (диагностические работы, научно-исследовательские и проектные работы, рефераты, результаты самостоятельной работы и т.д.), так и внеурочной (творческие работы, презентации, фото и видеоматериалы).

Портфолио может содержать материал из внешних источников (отзывы или грамоты, выписки из приказов с практики, с военных сборов и т.д.), дающий дополнительную оценку освоения общих и профессиональных компетенций.

Портфолио является контрольно-оценочным средством профессионального модуля (ПМ) и позволяет оценить сформированность общих и профессиональных компетенций.

Портфолио создается в течение всего обучения в колледже. Портфолио в дальнейшем может служить основой для составления резюме выпускника при поиске работы, при продолжении образования и др.

Цель Портфолио: отслеживание и оценивание формирования общих и профессиональных компетенций в рамках освоения программы подготовки

специалистов среднего звена среднего профессионального образования (ППССЗ СПО).

Задачи Портфолио: отслеживание персональных достижений обучающихся в соответствии с поэтапными требованиями ППССЗ СПО; оценивание сформированности общих компетенций ППССЗ СПО; оценивание сформированности профессиональных компетенций ППССЗ СПО; оценивание освоения видов профессиональной деятельности в соответствии с ФГОС СПО специальности; формирование и совершенствование учебной мотивации, мотивации достижений и мотивации на профессиональную деятельность.

Функции Портфолио: - функция предъявления, фиксации и накопления документально подтвержденных персональных достижений в процессе освоения ОПОП; - функция оценивания сформированности общих и профессиональных компетенций; - функция экспертной оценки освоения видов профессиональной деятельности; - функция формирования личной ответственности за результаты учебно- профессиональной деятельности, профессионально-личностного самосовершенствования, мотивации и интереса.

Участниками работы над портфолио являются студенты, преподаватели, кураторы. Одним из основных условий составления портфолио является установка тесного сотрудничества между всеми участниками и четкое распределение обязанностей между ними.

Обязанности студента: оформляет Портфолио в соответствии с принятой в ОГАПОУ «Алексеевский колледж» структурой; систематически самостоятельно пополняет соответствующие разделы материалами, отражающими успехи и достижения в учебной, производственной и внеучебной деятельности; отвечает за достоверность представленных материалов; при необходимости обращается за помощью к куратору.

Обязанности куратора: направляет всю работу студента по ведению портфолио, консультирует, помогает, дает советы, объясняет правила ведения и заполнения портфолио; совместно со студентами отслеживает и оценивает динамику их индивидуального развития и профессионального роста, поддерживает их образовательную, профессиональную, творческую активность и самостоятельность; выполняет роль посредника между студентом, преподавателями, обеспечивает их постоянное сотрудничество и взаимодействие; осуществляет контроль за заполнением соответствующих разделов Портфолио; помогает сделать электронные копии приказов, распоряжений и т.д. администрации колледжа и внешних организаций.

Обязанности преподавателей: преподаватели проводят экспертизу и оценку представленных работ по дисциплине, междисциплинарному курсу, профессиональному модулю и дают рекомендацию о размещении работы в портфолио (допускается размещение работ, выполненных на оценку не ниже «хорошо»), оформляют сертификат установленного образца; преподаватели/сотрудники администрации, являющиеся организаторами

проведения различных мероприятий в колледже оформляют сертификат установленного образца на участие студента в тех или иных мероприятиях; оформляют заявку на имя заведующего отделением для поощрения студентов за участие в учебной и внеучебной работе: грамоты, дипломы, отзывы, благодарности.

Обязанности администрации: заведующий отделением, руководитель практики, заместители директора по учебной работе, учебно-методической работе, учебно- производственной работе, воспитательной работе, методист осуществляют общий контроль за деятельностью педагогического коллектива по реализации технологии портфолио и оказывают необходимую помощь кураторам в организации сбора документов соответствующих разделов портфолио; собеседование с лицами, поступающими в колледж; по итогам учебного года организует награждение Почетными грамотами лучших студентов в номинациях: за успехи в учебе, за активное участие в общественной работе, за активное участие в культурно-массовой работе, за активное участие в военно-патриотической работе, за активное участие в волонтерском движении и т.д.

Ведение портфолио осуществляется самим студентом в печатном (папка-накопитель с файлами) и электронном виде. Каждый отдельный материал, включенный в портфолио за время обучения в образовательном учреждении, датируется.

Структура портфолио:

1) Титульный лист.

2) Раздел «Официальные документы».

3) Достижения в освоении образовательной программы и программ дополнительного образования. В этом разделе помещаются все имеющиеся у студента сертифицированные документы, подтверждающие его индивидуальные достижения: копии документов (свидетельств), подтверждающих обучение по основной образовательной программе и программам дополнительного образования; информация о наградах, грамотах, благодарственных письмах; копии документов (свидетельств), подтверждающих его участие в различных конкурсах (соревнованиях и т.д.); другие документы по усмотрению автора.

4) Раздел «Итоги прохождения производственной практики» формируется по мере прохождения студентом производственной практики по профессиональным модулям, предусмотренным ППССЗ по специальностям. Формирование данного раздела является обязательным требованием для каждого студента. Раздел включает в следующие материалы: характеристики с места прохождения практики, заверенная подписью общего руководителя производственной практики и печатью учреждения; отзывы, благодарности от руководителей практик, руководства организаций, где студент проходил производственную практику; аттестационные листы.

5) Раздел «Достижения в НИРС и УИРС» формируется в период всего

обучения студента в колледже. В данном разделе допускается представление копий документов. Радел включает следующие материалы: исследовательские работы и рефераты; отзывы на курсовые работы и проекты (возможно в электронном виде); ксерокопии статей или печатные издания со статьями студента; тезисы докладов на конференциях, семинарах и т.д.; все имеющиеся у студента сертифицированные документы, подтверждающие индивидуальные достижения в различных видах деятельности: дипломы об участии в предметных олимпиадах и конкурсах профессионального мастерства, научно-практических конференциях различного уровня, грамоты за участие в конкурсах, сертификаты прохождения курсов дополнительного образования и т.д.

6) Раздел «Дополнительные личные достижения» формируется в период всего обучения студента в колледже. В данный раздел включаются работы и сертифицированные документы, подтверждающие индивидуальные достижения в области искусства, творчества, волонтерства, спорта или официальные документы, подтверждающие участие, достижения во внеучебной деятельности.

При оформлении портфолио необходимо соблюдать следующие требования: оформлять в печатном виде отдельными листами формата А4 (в пределах одного бланка или листа, таблицы); предоставлять достоверную информацию; располагать материалы в папке Портфолио в соответствии с принятой в ОГАПОУ «Алексеевский колледж» структурой портфолио. Студент самостоятельно оформляет Разделы. Преподаватель и куратор периодически контролируют и проверяют достоверность информации. Ответственность за сохранность подлинных документов и материалов несет лично студент. На экзамен (квалификационный) по профессиональному модулю студент обязан предоставить подлинные подтверждения своих профессиональных достижений.

3. ОСВОЕНИЕ ЗНАНИЙ, УМЕНИЙ, ПРАКТИЧЕСКОГО ОПЫТА

3.1. Комплект материалов для оценки сформированности знаний, умений, практического опыта по МДК.03.01 Техническая защита информации

Комплект оценочных средств предназначен для оценки результатов освоения МДК.03.01 Техническая защита информации (ПФР) в рамках текущей и промежуточной аттестации.

Форма промежуточной аттестации – экзамен.

С целью овладения указанным видом деятельности и соответствующими профессиональными компетенциями обучающийся в ходе освоения МДК должен:

уметь:

У1 применять технические средства для криптографической защиты информации конфиденциального характера;

У2 применять технические средства для уничтожения информации и носителей информации;

У3 применять нормативные правовые акты, нормативные методические документы по обеспечению защиты информации техническими средствами;

У4 применять технические средства для защиты информации в условиях применения мобильных устройств обработки и передачи данных;

У5 применять средства охранной сигнализации, охранного телевидения и систем контроля и управления доступом;

У6 применять инженерно-технические средства физической защиты объектов информатизации.

знать:

З1 порядок технического обслуживания технических средств защиты информации;

З2 номенклатуру применяемых средств защиты информации от несанкционированной утечки по техническим каналам;

З3 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;

З4 порядок устранения неисправностей технических средств защиты информации и организации ремонта технических средств защиты информации;

З5 методики инструментального контроля эффективности защиты информации, обрабатываемой средствами вычислительной техники на объектах информатизации;

З6 номенклатуру и характеристики аппаратуры, используемой для измерения параметров ПЭМИН, а также параметров фоновых шумов и физических полей, создаваемых техническими средствами защиты информации;

З7 основные принципы действия и характеристики технических средств физической защиты;

З8 основные способы физической защиты объектов информатизации;

З9 номенклатуру применяемых средств физической защиты объектов информатизации.

Критерии оценки результатов освоения МДК.03.01 Техническая защита информации:

- оценка «отлично» выставляется, если студент свободно владеет теоретическим материалом, на все вопросы дает правильные и обоснованные ответы, убедительно защищает свою точку зрения, полно и правильно выполнил практическое задание, хорошо владеет юридической терминологией, полно отвечает на дополнительные вопросы.

- оценка «хорошо» выставляется, если студент твердо владеет теоретическим материалом, может применять его самостоятельно или по указанию преподавателя, на большинство вопросов даны правильные ответы, студент защищает свою точку зрения достаточно обоснованно, правильно выполнил практическое задание, хорошо знает основной материал, но допускает неточности в терминологии и в ответе на дополнительные вопросы.

- оценка «удовлетворительно» выставляется, если студент имеет только основы правовых знаний, может применять их по указанию преподавателя, на некоторые вопросы даны правильные ответы, выполнил практическое задание с допущением неточностей, затрудняется отвечать на дополнительные и уточняющие вопросы.

- оценка «неудовлетворительно» выставляется, если студент имеет неполные знания основного материала, допускает грубые ошибки при ответе, отвечает на дополнительные вопросы не полно, допустил грубые фактические ошибки при выполнении практического задания, не дает ответа на поставленные вопросы, не может отстоять свою точку зрения.

3. 2. Типовые задания для оценки освоения МДК.03.01 Техническая защита информации:

Тестовые задания (ТЗ)

Задание №1

Создание систем и средств предотвращения несанкционированного доступа к обрабатываемой информации и специальных воздействий, вызывающих разрушение, уничтожение, искажение информации, а также изменение штатных режимов функционирования систем и средств информатизации и связи относится к:

1. правовым методам защиты информации
2. организационно-техническим методам защиты информации
3. организационно-распорядительным методам защиты информации

4. экономическим методам защиты информации

Задание №2

Субъект, в полном объеме реализующий полномочия владения, пользования, распоряжения информацией, называется:

1. собственник информации
2. владелец информации
3. пользователь

Задание №3

Форма допуска, требуемая для работы со сведениями особой важности является:

1. первой формой допуска
2. второй формой допуска
3. третьей формой допуска

Задание №4

Форма допуска, требуемая для работы с совершенно секретными сведениями является:

1. первой формой допуска
2. второй формой допуска
3. третьей формой допуска

Задание №5

Форма допуска, требуемая для работы с секретными сведениями является:

1. первой формой допуска
2. второй формой допуска
3. третьей формой допуска

Задание №6

В сфере государственной тайны действует функционально-зональный принцип. Это значит, что:

1. каждый пользователь допускается должностными лицами только к такой информации, которая требуется ему для исполнения должностных обязанностей
2. каждый пользователь допускается должностными лицами только к информации, касающейся зоны его проживания
3. каждый пользователь допускается должностными лицами ко всей информации, к которой у него есть форма допуска

Задание №7

Противоправные процессы утечки, утраты, распространения, разглашения, копирования, тиражирования, фальсификации, хранения с целью передачи, удаления информации называется процессом:

1. незаконного оборота информации
2. взлома информации
3. несанкционированного использования информации

Задание №8

Форма преднамеренного распространения или мнимого разглашения (утечки) неких планов и намерений, которые не отвечают реальным действиям называется:

1. дезинформация
2. легендирование
3. шпионаж

Задание № 9

Какое направление защиты в основном применяется для охраны материальных ценностей?

1. инженерно-техническая
2. организационно-техническая
3. организационно-распорядительная
4. нормативно-правовая
5. экономическая

Задание №10

Что из нижеперечисленного оборудования может выступать в качестве технического канала связи?

1. контроллер жесткого диска, передающий электрические импульсы, считанные магниторезистивной головкой с поверхности магнитного носителя, по шлейфу в системную магистраль для копирования в оперативную память
2. инфракрасный светодиод лазерного принтера, посылающий кратковременные
3. вспышки на электризованную поверхность фоточувствительного барабана
4. модулированный по силе тока поток электронов, засвечивающий в определенном
5. порядке пикселы люминофора электронно-лучевой трубки
6. экран компьютерного монитора и глаза пользователя
7. оптический канал связи
8. все варианты могут быть отнесены к техническим каналам связи

Задание №11

Какой канал утечки информации основан на использовании электромагнитной энергии видимого и инфракрасного диапазона?

1. визуально-оптический канал
2. электромагнитный канал
3. виброакустический канал
4. материально-вещественный канал

Задание № 12

Процесс перехвата и фиксации процесса клавиатурного ввода идентифицирующей информации является примером утечки информации:

1. визуально-оптического канала
2. электромагнитного канала
3. виброакустического канала
4. материально-вещественного канала

Задание №13

Какой канал утечки информации включает в себя весь радиодиапазон от сверхнизких до сверхвысокочастотных волн?

1. визуально-оптический канал
2. электромагнитный канал
3. виброакустический канал
4. материально-вещественный канал

Задание №14

Электрические сигналы (напряжения, токи), модулированные по закону передаваемого сообщения, протекающие по проводникам и элементам радиоцепей (линиям связи, антеннам, конденсаторам) и возбуждающие в окружающем пространстве электромагнитную энергию является примером утечки информации:

1. визуально-оптического канала
2. электромагнитного канала
3. виброакустического канала
4. материально-вещественного канала

Задание №16

Какой канал утечки информации представляет собой фактический побочный прием модулированной акустической энергии, распространяющейся в газообразной, жидкой или твердой средах

1. визуально-оптический канал
2. электромагнитный канал
3. виброакустический канал
4. материально-вещественный канал

Задание №17

Примером какого канала утечки информации служит звук голоса человека?

1. визуально-оптического канала
2. электромагнитного канала
3. виброакустического канала
4. материально-вещественного канала

Задание №18

По какому признаку делят на классы средства технической разведки (СТР) ?

1. по дальности канала
2. по форме допуска
3. по мощности
4. по степени финансирования

Задание №19

Портативные устройства для запечатления информации, скрытно проносимые на территорию объекта нарушителем на своем теле относят к …

1. первому классу СРТ
2. второму классу СРТ
3. третьему классу СРТ

Задание №20

Для наблюдения за объектами информатизации из-за пределов их охраняемой или контролируемой территории используются СРТ…

1. первого класса
2. второго класса
3. третьего класса

3.2. Практические задания:

1. Выявить и описать потенциальные каналы утечки информации в помещениях. Указать причины возникновения. Составить модель каналов утечки информации.
2. Для помещений определить основные источники информации и их носители. Классифицируйте и опишите категории помещений.

3. Представлены основные варианты возможной утечки речевой информации из объемов выделенных помещений. Определите группы и виды каналов утечки. Опишите технические средства, с помощью которых может быть осуществлен перехват информации.Опишите возможные каналы утечки информации.
4. Опишите методы и средства технической защиты, которые могут применяться для блокирования угроз, связанных с утечкой информации.
5. Для объекта защиты составьте список потенциальных угроз безопасности.
6. Составьте план защиты объекта с помощью технических средств. Поясните расположение и обоснуйте свой выбор.
7. Для объекта защиты выделите и опишите контролируемы зоны ОТСС.
8. Для помещения (объекта защиты) составить проект технической защиты информации от утечки по акустическому каналу.
9. Для помещения (объекта защиты) составить проект технической защиты информации от утечки по оптическому каналу.

3.3. Комплект материалов для оценки сформированности знаний, умений, практического опыта по МДК.03.02 Инженерно-технические средства физической защиты объектов информатизации

Комплект оценочных средств предназначен для оценки результатов освоения МДК.03.02 Инженерно-технические средства физической защиты объектов информатизации в рамках текущей и промежуточной аттестации.

Форма промежуточной аттестации – экзамен.

С целью овладения указанным видом деятельности и соответствующими профессиональными компетенциями обучающийся в ходе освоения МДК должен:

У1 применять технические средства для криптографической защиты информации конфиденциального характера;

У2 применять технические средства для уничтожения информации и носителей информации;

У3 применять нормативные правовые акты, нормативные методические документы по обеспечению защиты информации техническими средствами;

У4 применять технические средства для защиты информации в условиях применения мобильных устройств обработки и передачи данных;

У5 применять средства охранной сигнализации, охранного телевидения и систем контроля и управления доступом;

У6 применять инженерно-технические средства физической защиты объектов информатизации.

знать:

З1 порядок технического обслуживания технических средств защиты информации;

З2 номенклатуру применяемых средств защиты информации от несанкционированной утечки по техническим каналам;

З3 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;

З4 порядок устранения неисправностей технических средств защиты информации и организации ремонта технических средств защиты информации;

З5 методики инструментального контроля эффективности защиты информации, обрабатываемой средствами вычислительной техники на объектах информатизации;

З6 номенклатуру и характеристики аппаратуры, используемой для измерения параметров ПЭМИН, а также параметров фоновых шумов и физических полей, создаваемых техническими средствами защиты информации;

З7 основные принципы действия и характеристики технических средств физической защиты;

З8 основные способы физической защиты объектов информатизации;

З9 номенклатуру применяемых средств физической защиты объектов информатизации.

Критерии оценки результатов освоения МДК.03.02 Инженерно-технические средства физической защиты объектов информатизации

- оценка «отлично» выставляется, если студент свободно владеет теоретическим материалом, на все вопросы дает правильные и обоснованные ответы, убедительно защищает свою точку зрения, полно и правильно выполнил практическое задание, хорошо владеет юридической терминологией, полно отвечает на дополнительные вопросы.

- оценка «хорошо» выставляется, если студент твердо владеет теоретическим материалом, может применять его самостоятельно или по указанию преподавателя, на большинство вопросов даны правильные ответы, студент защищает свою точку зрения достаточно обоснованно, правильно выполнил практическое задание, хорошо знает основной материал, но

допускает неточности в терминологии и в ответе на дополнительные вопросы.

- оценка «удовлетворительно» выставляется, если студент имеет только основы правовых знаний, может применять их по указанию преподавателя, на некоторые вопросы даны правильные ответы, выполнил практическое задание с допущением неточностей, затрудняется отвечать на дополнительные и уточняющие вопросы.

- оценка «неудовлетворительно» выставляется, если студент имеет неполные знания основного материала, допускает грубые ошибки при ответе, отвечает на дополнительные вопросы не полно, допустил грубые фактические ошибки при выполнении практического задания, не дает ответа на поставленные вопросы, не может отстоять свою точку зрения.

3.4. Типовые задания для оценки освоения МДК.03.02 Инженерно-технические средства физической защиты объектов информатизации.

Тестовые задания (ТЗ)

1. Понятие информации. Проблема обеспечения безопасности в информационных системах, политика информационной безопасности.
2. Устройства защиты от утечки информации по радиоканалам, основные методы обнаружения радиозакладок.
3. Физические средства
4. Аппаратные средства
5. Программные средства
6. Криптографические средства
7. Индикаторы поля, акустическая развязка, дифференциальный индикатор поля.
8. Генераторы шума.
9. Особенности работы и основные характеристики сканирующих радиоприемников.
10. Блок-схема типового сканирующего радиоприемника.
11. Автоматизированные комплексы обнаружения радиозакладок. Методы обнаружения локализации в пространстве закладных устройств.
12. Виды модуляции и кодирования передаваемой информации.
13. Амплитудная модуляция. Амплитудная модуляция с подавлением верхней или нижней боковой частоты. Частотная модуляция. Фазовая модуляция.
14. Кодово-импульсная модуляция. Специальные виды модуляции. Основные требования к специальным системам связи.
15. Использование ШПС и ППРЧ сигналов. Основные характеристики.
16. Обнаружители и подавители диктофонов. Назначение. Принципы работы. Основные характеристики.
17. Принципы работы локаторов нелинейностей. Основные методы обнаружения ложных и истинных соединений.
18. Концепции инженерно-технической защиты информации.
19. Системный подход к защите информации.
20. Основные проблемы инженерно-технической защиты информации.
21. Основные концептуальные положения инженерно-технической защиты информации.

22. Направления инженерно-технической защиты информации.
23. Показатели эффективности инженерно-технической защиты информации.
24. Теоретические основы инженерно-технической защиты информации.
25. Источники опасных сигналов.
26. Виды побочных опасных электромагнитных излучений.
27. Характеристика технической разведки.
28. Технические каналы утечки информации.
29. Методы инженерно-технической защиты информации.
30. Методы инженерной защиты и технической охраны объекта.
31. Методы скрытия информации и ее носителей.
32. Физические основы защиты информации.
33. Физические основы побочных электромагнитных излучений и наводок.
34. Распространение сигналов в технических каналах утечки информации.
35. Физические процессы подавления опасных сигналов.
36. Технические средства добывания и инженерно-технической защиты.
37. Средства технической разведки.
38. Средства инженерной защиты и технической охраны.
39. Средства предотвращения утечки информации по техническим каналам.
40. Организационные основы инженерно-технической защиты информации.
41. Государственная система защиты информации.
42. Контроль эффективности инженерно-технической защиты информации.
43. Методическое обеспечение инженерно-технической защиты автоматизированных систем от вредоносных программных воздействий.
44. Моделирование инженерно-технической защиты информации.
45. Методические рекомендации по оценке эффективности защиты информации.

Практическое задание (ПЗ)

Инструкция для выполнения задания

Внимательно прочитайте задание.

Время выполнения задания - 45 минут**.**

Текст задания

Промышленное предприятие (условно ОАО «Маяк»), специализирующееся на производстве пластмассовых труб, которые по своим качествам пользуются большим спросом. Охрана и защита коммерческих секретов, связанных с технологией производства труб, находятся в центре внимания руководства и службы безопасности предприятия. Предприятие имеет административную зону, где расположены управленческие структуры, производственную и складскую зоны. Все эти зоны разделены заборами. Предприятие имеет широкий круг партнеров, клиентов (в том числе и за рубежом). В сфере деятельности предприятия часто возникают конфликтные ситуации с конкурентами и спорные вопросы с органами местной власти по земельным и финансовым вопросам.

1. Определите объекты и субъекты системы безопасности предприятия.
2. Выберите и обоснуйте виды охраны предприятия.

3. Разработайте и обоснуйте систему видеонаблюдения административной зоны.

4. ОЦЕНКА ПО УЧЕБНОЙ И ПРОИЗВОДСТВЕННОЙ ПРАКТИКЕ

4.1. Общие положения

Комплект оценочных средств предназначен для оценки результатов освоения учебной и производственной практик профессионального модуля ПМ.03 Защита информации техническими средствами.

Целью текущей и промежуточной аттестации по учебной и производственной практике является комплексная проверка сформированности у обучающихся практических профессиональных умений и навыков в рамках профессионального модуля по основному виду деятельности - Защита информации техническими средствами для освоения профессии, обучения трудовым приемам, операциям и способам выполнения трудовых процессов, характерных для соответствующей профессии и необходимых для последующего освоения ими общих и профессиональных компетенций по избранной специальности.

4.2. Виды работ практики и проверяемые результаты обучения по профессиональному модулю

Виды учебной работы на практике, включая самостоятельную работу студентов	**Проверяемые результаты (ПК, ОК, ПО, У)**	**Форма проверки результатов**
Измерение параметров физических полей.	ПК 3.1. Осуществлять установку, монтаж, настройку и техническое обслуживание технических средств защиты информации в соответствии с требованиями эксплуатационной документации. ПК 3.2. Осуществлять эксплуатацию технических средств защиты информации в соответствии с требованиями эксплуатационной документации. ПК 3.3. Осуществлять измерение параметров побочных электромагнитных излучений и наводок (ПЭМИН), создаваемых техническими средствами обработки информации ограниченного доступа.	Проверка отчета, собеседование, дифференцированный зачет
Определение каналов утечки ПЭМИН.		
Проведение измерений параметров фоновых шумов и физических полей, создаваемых техническими средствами защиты информации.		
Установка и настройка технических средств защиты информации.		
Проведение измерений		

параметров побочных электромагнитных излучений и наводок. Проведение аттестации объектов информатизации. Монтаж различных типов датчиков. Проектирование установки системы пожарно-охранной сигнализации по заданию и ее реализация. Применение промышленных осциллографов, частотомеров и генераторов и другого оборудования для защиты информации. Рассмотрение системы контроля и управления доступом. Рассмотрение принципов работы системы видеонаблюдения и ее проектирование. Рассмотрение датчиков периметра, их принципов работы. Выполнение звукоизоляции помещений системы зашумления. Реализация защиты от утечки по цепям электропитания и заземления. Разработка организационных и технических мероприятий по заданию	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. **иметь практический опыт:** – установки, монтажа и настройки технических средств защиты информации; – технического обслуживания технических средств защиты информации; – применения основных типов технических средств защиты информации; – выявления технических каналов утечки информации; – участия в мониторинге эффективности технических средств защиты информации; – диагностики, устранения отказов и неисправностей, восстановления работоспособности технических средств защиты информации; – проведения измерений параметров ПЭМИН, создаваемых техническими средствами обработки информации при аттестации объектов информатизации, для которой установлен режим конфиденциальности, при аттестации объектов информатизации по требованиям безопасности информации; – проведения измерений параметров фоновых шумов, а также физических полей, создаваемых техническими средствами защиты информации; – установки, монтажа и настройки, технического обслуживания, диагностики, устранения отказов и неисправностей, восстановления работоспособности инженерно-технических средств физической защиты. **уметь:** – применять технические средства	

преподавателя;	для криптографической защиты информации конфиденциального характера; – применять технические средства для уничтожения информации и носителей информации; – применять нормативные правовые акты, нормативные методические документы по обеспечению защиты информации техническими средствами; – применять технические средства для защиты информации в условиях применения мобильных устройств обработки и передачи данных; – применять средства охранной сигнализации, охранного телевидения и систем контроля и управления доступом; – применять инженерно-технические средства физической защиты объектов информатизации. **знать:** – порядок технического обслуживания технических средств защиты информации; – номенклатуру применяемых средств защиты информации от несанкционированной утечки по техническим каналам; – физические основы, структуру и условия формирования технических каналов утечки информации, способы их выявления и методы оценки опасности, классификацию существующих физических полей и технических каналов утечки информации; – порядок устранения неисправностей технических средств защиты информации и организации ремонта технических средств защиты информации; – методики инструментального контроля эффективности защиты информации, обрабатываемой средствами вычислительной техники на объектах информатизации;		
Разработка основной документации по инженерно-технической защите информации.			

	– номенклатуру и характеристики аппаратуры, используемой для измерения параметров ПЭМИН, а также параметров фоновых шумов и физических полей, создаваемых техническими средствами защиты информации; – основные принципы действия и характеристики технических средств физической защиты; – основные способы физической защиты объектов информатизации; – номенклатуру применяемых средств физической защиты объектов информатизации.	

Критерии оценки результатов освоения учебной практики

- оценка «отлично» выставляется, если студент свободно владеет теоретическим материалом, на все вопросы дает правильные и обоснованные ответы, убедительно защищает свою точку зрения, полно и правильно выполнил практическое задание, хорошо владеет юридической терминологией, полно отвечает на дополнительные вопросы.

- оценка «хорошо» выставляется, если студент твердо владеет теоретическим материалом, может применять его самостоятельно или по указанию преподавателя, на большинство вопросов даны правильные ответы, студент защищает свою точку зрения достаточно обоснованно, правильно выполнил практическое задание, хорошо знает основной материал, но допускает неточности в терминологии и в ответе на дополнительные вопросы.

- оценка «удовлетворительно» выставляется, если студент имеет только основы правовых знаний, может применять их по указанию преподавателя, на некоторые вопросы даны правильные ответы, выполнил практическое задание с допущением неточностей, затрудняется отвечать на дополнительные и уточняющие вопросы.

- оценка «неудовлетворительно» выставляется, если студент имеет неполные знания основного материала, допускает грубые ошибки при ответе, отвечает на дополнительные вопросы не полно, допустил грубые фактические ошибки при выполнении практического задания, не дает ответа на поставленные вопросы, не может отстоять свою точку зрения.

4.2. Производственная практика

Виды учебной работы на практике, включая самостоятельную работу студентов	Проверяемые результаты (ПК, ОК, ПО, У)	Форма проверки результатов
Исследование угроз и методологии оценки уязвимости информации. Оценка информационных рисков. Исследование методов и моделей оценки уязвимости информации. Исследование аналитических моделей для определения базовых показателей уязвимости информации. Участие в проектировании политики безопасности информационного объекта. Проектирование политики безопасности информационного объекта на конкретном примере. Мероприятия по выявлению каналов утечки информации (специальные обследования). Участие в монтаже технических средств защиты информации в телефонных линиях Участие в обслуживании и эксплуатации технических средств защиты информации в телефонных линиях Участие в монтаже, обслуживании и эксплуатации средств инженерной защиты и технической охраны	ПК 3.1. Осуществлять установку, монтаж, настройку и техническое обслуживание технических средств защиты информации в соответствии с требованиями эксплуатационной документации. ПК 3.2. Осуществлять эксплуатацию технических средств защиты информации в соответствии с требованиями эксплуатационной документации. ПК 3.3. Осуществлять измерение параметров побочных электромагнитных излучений и наводок (ПЭМИН), 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. **иметь практический опыт:** – установки, монтажа и настройки технических средств защиты информации; – технического обслуживания технических средств защиты информации; – применения основных типов технических средств защиты информации; – выявления технических каналов утечки информации; – участия в мониторинге эффективности технических средств защиты информации; – диагностики, устранения отказов и неисправностей, восстановления работоспособности технических средств	Проверка отчета, собеседование, дифференцированный зачет

объектов: системы защиты от утечки информации по оптическому каналу Проектирование системы видеонаблюдения за протяженным периметром. Проектирование системы идентификации людей на входе в здание. Проектирование системы видеонаблюдения в транспорте. Проектирование системы видеонаблюдения в школе Участие в монтаже систем видеонаблюдения. Участие в обслуживании систем видеонаблюдения. Эксплуатации систем видеонаблюдения. Участие в монтаже, обслуживании и эксплуатации средств защиты информации от несанкционированного съёма, и утечки по техническим каналам: защита информации от утечки по акустическому каналу пассивными методами Участие в монтаже, обслуживании и эксплуатации средств защиты информации от несанкционированного съёма, и утечки по техническим каналам: системы защиты от утечки информации по электросетевому каналу	защиты информации; – проведения измерений параметров ПЭМИН, создаваемых техническими средствами обработки информации при аттестации объектов информатизации, для которой установлен режим конфиденциальности, при аттестации объектов информатизации по требованиям безопасности информации; – проведения измерений параметров фоновых шумов, а также физических полей, создаваемых техническими средствами защиты информации; – установки, монтажа и настройки, технического обслуживания, диагностики, устранения отказов и неисправностей, восстановления работоспособности инженерно-технических средств физической защиты. **уметь:** – применять технические средства для криптографической защиты информации конфиденциального характера; – применять технические средства для уничтожения информации и носителей информации; – применять нормативные правовые акты, нормативные методические документы по обеспечению защиты информации техническими средствами; – применять технические средства для защиты информации в условиях применения мобильных устройств обработки и передачи данных; – применять средства охранной сигнализации, охранного телевидения и систем контроля и управления доступом; – применять инженерно-технические средства физической защиты объектов информатизации. **знать:** – порядок технического обслуживания технических средств защиты информации;	

	– номенклатуру применяемых средств защиты информации от несанкционированной утечки по техническим каналам; – физические основы, структуру и условия формирования технических каналов утечки информации, способы их выявления и методы оценки опасности, классификацию существующих физических полей и технических каналов утечки информации; – порядок устранения неисправностей технических средств защиты информации и организации ремонта технических средств защиты информации; – методики инструментального контроля эффективности защиты информации, обрабатываемой средствами вычислительной техники на объектах информатизации; – номенклатуру и характеристики аппаратуры, используемой для измерения параметров ПЭМИН, а также параметров фоновых шумов и физических полей, создаваемых техническими средствами защиты информации; – основные принципы действия и характеристики технических средств физической защиты; – основные способы физической защиты объектов информатизации; – номенклатуру применяемых средств физической защиты объектов информатизации.	

Критерии оценки результатов освоения производственной практики

- оценка «отлично» выставляется, если студент свободно владеет теоретическим материалом, на все вопросы дает правильные и обоснованные ответы, убедительно защищает свою точку зрения, полно и правильно

выполнил практическое задание, хорошо владеет юридической терминологией, полно отвечает на дополнительные вопросы.

- оценка «хорошо» выставляется, если студент твердо владеет теоретическим материалом, может применять его самостоятельно или по указанию преподавателя, на большинство вопросов даны правильные ответы, студент защищает свою точку зрения достаточно обоснованно, правильно выполнил практическое задание, хорошо знает основной материал, но допускает неточности в терминологии и в ответе на дополнительные вопросы.

- оценка «удовлетворительно» выставляется, если студент имеет только основы правовых знаний, может применять их по указанию преподавателя, на некоторые вопросы даны правильные ответы, выполнил практическое задание с допущением неточностей, затрудняется отвечать на дополнительные и уточняющие вопросы.

- оценка «неудовлетворительно» выставляется, если студент имеет неполные знания основного материала, допускает грубые ошибки при ответе, отвечает на дополнительные вопросы не полно, допустил грубые фактические ошибки при выполнении практического задания, не дает ответа на поставленные вопросы, не может отстоять свою точку зрения.

5. КОНТРОЛЬНО-ОЦЕНОЧНЫЕ МАТЕРИАЛЫ (КОМ) ДЛЯ ЭКЗАМЕНА КВАЛИФИКАЦИОННОГО

5.1.Общие положения

КОМ предназначены для контроля и оценки результатов освоения профессионального модуля ПМ.03 Защита информации техническими средствами в рамках промежуточной аттестации по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем.

5.2. Задания для экзаменующихся

Теоретические вопросы к экзамену по ПМ. 03 Защита информации техническими средствами:

1. Инженерно-техническая защита информации. Задачи государственной системы защиты информации защиты
2. Структура государственной системы защиты информации. Направления работ по защите информации.
3. Органы государственной системы защиты информации

4. Виды информации, защищаемой техническими средствами. Свойства информации, влияющие на возможности ее защиты.

5. Понятие о демаскирующих признаках объектов защиты.

6. Характеристики и особенности семантической (смысловой) информации и информации о демаскирующих признаках объекта

7. Классификация демаскирующих признаков. Опознавательные признаки и признаки деятельности объектов.

8. Видовые, сигнальные и вещественные демаскирующие признаки.

9. Основные видовые демаскирующие признаки объектов наблюдения. Особенности видовых признаков в оптическом и радиодиапазона.

10. Определение основных характеристик аналоговых и дискретных (импульсных) электрических сигналов, средств связи, радиолокационных станций, лазерных и других излучений.

11. Изучение основных признаков, характеризующие физические и химические свойства материальных тел. Понятие о демаскирующих объектах, сигналах и веществах.

12. Технические каналы утечки информации.

13. Понятие об опасных сигналах и их источниках.

14. Диагностика основных и вспомогательных технических средств и систем

15. Побочные электромагнитные излучения и наводки.

16. Акустоэлектрические преобразователи, их виды и принципы работы.

17. Принципы высокочастотного навязывания. Высокочастотные и низкочастотные побочные излучения технических средств и систем (ТСС).

18. Паразитная генерация усилителей. Виды паразитных связей между цепями ТСС.

19. Исследование паразитных наводок в цепях электропитания, заземления, в токопроводящих конструкциях помещений и зданий

20. Характеристики каналов утечки информации.

21. Структура технических каналов утечки информации.

22. Виды технических каналов утечки информации.

23. Основные характеристики технических каналов утечки информации.

24. Способы комплексного использования злоумышленниками технических каналов утечки информации

25. Оптические каналы утечки информации. Структура оптического канала утечки информации.

26. Характеристики среды распространения оптических лучей. Основные показатели оптоэлектронных линий связи и способы снятия с них информации.

27. Радиоэлектронные каналы утечки информации. Особенности радиоэлектронных каналов утечки информации. Виды и структура радиоэлектронных каналов утечки информации.

28. Особенности распространения радиоволн различных диапазонов частот. Способы повышения дальности передачи информации в ультракоротком диапазоне радиоволн.

29. Классификация и характеристики помех в радиоэлектронных каналах утечки информации

30. Диагностика акустических каналов утечки информации.

31. Структура акустического канала утечки информации.

32. Отражение и поглощение акустических волн в среде распространения.

33. Понятие о реверберации и влияние времени реверберации на разборчивость речи.

34. Материально-вещественные каналы утечки информации.

35. Анализ способов утечки демаскирующих веществ в твердом, жидком и газообразном виде.

36. Виды потенциальных угроз безопасности информации. Преднамеренные и случайные воздействия на источники информации
37. Технические каналы утечки речевой информации. Технические каналы утечки информации припередачи ее по каналам связи
38. Электрические каналы утечки информации. Электромагнитные каналы утечки информации
39. Средства нейтрализации угроз и управления физической защитой
40. Средства инженерной защиты. Инженерные конструкции
41. Ограждения территорий, зданий, помещений. Двери, окна, ворота. Металлические сейфы, хранилища. Запирающие устройства
42. Устройства ввода идентификационных признаков. Магнитные карты доступа. Проксимити-карты
43. Биометрические характеристики человека.
44. Устройства управления и исполнения. Турникеты, шлагбаумы, шлюзовые кабины, блокираторы
45. Направленные микрофоны, виды, сравнение характеристик. Диктофоны и стетоскопы.
46. Сканирующие приемники. Нелинейные локаторы. Подавители сигналов
47. Приемно-контрольные приборы. Ретрансляторы.
48. Пульты централизованной охраны.
49. Радиоканальные системы охраны и оповещения. GSM, Internet оповещение
50. Принципы функционирования средств видеонаблюдения. Определение характеристик используемых камер и объективов.
51. Средства отображения видеоинформации. Средства регистрации, хранения и архивации данных. Освещение
52. Системы охранно-тревожной сигнализации. Система пожарной сигнализации
53. Звукоизоляция и звукопоглощение.
54. Диагностика побочных преобразований акустической волны в электрический сигнал.
55. Средства обнаружения, локализации и подавления радиоизлучающих устройств.
56. Средства контроля проводных систем передачи информации.

Билет №1

Практическое задание

Научно-внедренческого предприятия «Звезда» занимается прокладкой компьютерных сетей и разработкой программных комплексов для организаций нашего города. Численность работников в «Звезде» – примерно 80 человек. Одновременно находится в разработке до 30 проектов. Один разработчик может участвовать в нескольких проектах одновременно, степень секретности для каждого проекта индивидуальна. Одна организация может заказать в «Звезде» несколько разработок. В связи с больший востребованностью создаваемых программных продуктов, а также с появлением новых конкурирующих фирм, предоставляющих аналогичные услуги, охране и защите коммерческих секретов уделено усиленное внимание.

1. Определите объекты и субъекты системы безопасности предприятия.
2. Выберите и обоснуйте виды охраны предприятия.

3. Составьте схему классификации в виде графа-структуры, нулевой (верхний) уровень иерархии который соответствует понятию "защищаемая информация", а n-ый (нижний) - элементам информации одного источника из перечня источников организации. Основные требования к схеме классификации: общий признак и полнота классификации, отсутствие пересечений между элементами классификации одного уровня (одна и та же информация не должна указываться в разных элементах классификации).
4. Создайте модель защиты в CorelDRAW.

Билет №2

Практическое задание

Судоходной компании «Балтика» занимается перевозками грузов между континентами. В ее собственности несколько десятков судов различного класса и грузоподъемности. К услугам этой компании обращаются тысячи клиентов из различных стран мира. Судно следует по маршруту. Маршрут разрабатывается главным менеджером компании и проходит через несколько портов. В очередном порту назначения производится лишь частичная погрузка и выгрузка грузов, и судно следует дальше. Компания имеет в своей собственности складские зоны. Все эти зоны разделены между собой. В связи с большим количеством конкурирующих фирм, охране и защите коммерческих секретов, связанных со статусом груза и маршрутом следования, уделено усиленное внимание.

1. Определите объекты и субъекты системы безопасности предприятия.
2. Выберите и обоснуйте виды охраны предприятия.
3. Составьте схему классификации в виде графа-структуры, нулевой (верхний) уровень иерархии который соответствует понятию "защищаемая информация", а n-ый (нижний) - элементам информации одного источника из перечня источников организации. Основные требования к схеме классификации: общий признак и полнота классификации, отсутствие пересечений между элементами классификации одного уровня (одна и та же информация не должна указываться в разных элементах классификации).
4. Создайте модель защиты в CorelDRAW.

Билет №3

Практическое задание

ООО «Киновидеопрокат», является почти полным монополистом относительно посреднических услуг в сфере кинобизнеса. Отдел маркетинга, изучив ситуацию на рынке кинофильмов, принимает решение о покупке

тех или иных кинолент. Отдел закупок претворяет эти решения в жизнь,

причем лента может быть куплена как у производителя, так и у посредника. Отдел аренды «Киновидеопроката» сдает закупленные фильмы кинотеатрам города в аренду. В

связи с возникающей больший конкуренцией охране и защите коммерческих секретов уделено усиленное внимание.

1. Определите объекты и субъекты системы безопасности предприятия.
2. Выберите и обоснуйте виды охраны предприятия.
3. Составьте схему классификации в виде графа-структуры, нулевой (верхний) уровень иерархии который соответствует понятию "защищаемая информация", а n-ый (нижний) - элементам информации одного источника из перечня источников организации. Основные требования к схеме классификации: общий признак и полнота классификации, отсутствие пересечений между элементами классификации одного уровня (одна и та же информация не должна указываться в разных элементах классификации).
4. Создайте модель защиты в CorelDRAW.

Билет №4

Практическое задание

Торгово-посредническая фирма «Столица». Бизнес этого предприятия предельно прост: «покупай дешевле – продавай дороже», или состыкуй продавца и покупателя и получи «комиссионные». Основной упор фирма делает на закупки продуктов питания в других регионах страны и за рубежом – там, где они производятся и стоят дешевле, чем в нашем регионе. Часть продукции может быть закуплена и у местных продавцов. В этом случае фирма получает прибыль за счет того, что крупные партии товара стоят дешевле, чем мелкие. Так как в данной сфере количество фирм на сегодняшний день увеличивается, то маркетинговой политики предприятия охраняется как службой безопасности, так и лично руководством.

1. Определите объекты и субъекты системы безопасности предприятия.
2. Выберите и обоснуйте виды охраны предприятия.
3. Составьте схему классификации в виде графа-структуры, нулевой (верхний) уровень иерархии который соответствует понятию "защищаемая информация", а n-ый (нижний) - элементам информации одного источника из перечня источников организации. Основные требования к схеме классификации: общий признак и полнота классификации, отсутствие пересечений между элементами классификации одного уровня (одна и та же информация не должна указываться в разных элементах классификации).
4. Создайте модель защиты в CorelDRAW.

Билет №5

Практическое задание

Рассмотреть работу отдела кадров университета, в которой находятся данные всех сотрудников: от преподавателя до ректора, и их трудовой деятельности. Также в отделе

кадров хранится информация о трудовой деятельности сотрудника: о предыдущих местах работы, сроке работы и предприятии. Отдел кадров занимается подготовкой трудовых договоров с преподавателями после избрания их по конкурсу на очередной срок.

Также в его ведении находятся сведения о наложении взысканий на сотрудников и их поощрениях, часть данных не имеет общего права доступа. Взыскания в трудовую книжку не заносятся, а хранятся в электронном виде.

1. Определите объекты и субъекты системы безопасности предприятия.
2. Выберите и обоснуйте виды охраны предприятия.
3. Составьте схему классификации в виде графа-структуры, нулевой (верхний) уровень иерархии который соответствует понятию "защищаемая информация", а n-ый (нижний) - элементам информации одного источника из перечня источников организации. Основные требования к схеме классификации: общий признак и полнота классификации, отсутствие пересечений между элементами классификации одного уровня (одна и та же информация не должна указываться в разных элементах классификации).
4. Создайте модель защиты в CorelDRAW.

5.3. Критерии оценки результатов освоения профессионального модуля

Коды и наименования проверяемых компетенций или их сочетаний	**Показатели оценки результата**	**Оценка (да / нет)**
ПК 3.1 Осуществлять установку, монтаж, настройку и техническое обслуживание технических средств защиты информации в соответствии с требованиями эксплуатационной документации	Демонстрировать умения и практические навыки в установке, монтаже, настройке ипроведении технического обслуживания технических средств защиты информации в соответствии с требованиями эксплуатационной документации	
ПК 3.2 Осуществлять эксплуатацию технических средств защиты информации в соответствии с требованиями эксплуатационной документации	Проявлять умения и практического опыта в эксплуатации технических средств защиты информации в соответствии с требованиями эксплуатационной документации	
ПК 3.3. Осуществлять измерение параметров побочных электромагнитных излучений и наводок (ПЭМИН), создаваемых	Проводить работы по измерению параметров побочных электромагнитных излучений и наводок (ПЭМИН), создаваемых	

техническими средствами обработки информации ограниченного доступа	техническими средствами обработки информации ограниченного доступа	
ПК 3.4 Осуществлять измерение параметров фоновых шумов, а также физических полей, создаваемых техническими средствами защиты информации	Проводить самостоятельные измерения параметров фоновых шумов, а также физических полей, создаваемых техническими средствами защиты информации	
ПК 3.5 Организовывать отдельные работы по физической защите объектов информатизации	Проявлять знания в выборе способов решения задач по организации отдельных работ по физической защите объектов информатизации	

Итогом экзамена является однозначное решение: «вид профессиональной деятельности освоен/не освоен».

Решение «вид профессиональной деятельности освоен» принимается если:

1) задание выполнено в полном объеме;
2) работа отличается глубиной проработки всех вопросов содержательной части;
3) студент свободно владеет теоретическим материалом, на все вопросы дает правильные и обоснованные ответы либо студент твердо владеет теоретическим материалом, может применять его самостоятельно или по указанию преподавателя и на большинство вопросов даны правильные ответы;
4) студент убедительно защищает свою точку зрения либо студент защищает свою точку зрения достаточно обоснованно;
5) студент обращался в ходе выполнения задания к нормативно-правовым актам;
6) студент рационально распределил время на выполнение задания по этапам: ознакомление с заданием и планирование работы, распределение времени на выполнение элементов задания; получение и поиск необходимой информации; демонстрация последовательности выполнения работы;
7) осуществлялась рефлексия выполнения задания и коррекция подготовленных документов перед сдачей;
8) задания выполнены самостоятельно и своевременно (в соответствии с установленным лимитом времени).

Решение «вид профессиональной деятельности не освоен» принимается

если студент допустил грубые фактические ошибки при выполнении задания, не дает ответа на поставленные вопросы, не может отстоять свою точку зрения.