Федеральное государственное бюджетное образовательное учреждение
высшего образования
"Дальневосточный государственный университет путей сообщения"
(ДВГУПС)
Факультет среднего профессионального образования –
Хабаровский техникум железнодорожного транспорта

УТВЕРЖДАЮ
И.о. декана ФСПО - ХТЖТ
_____Д.Н. Никитин
«_21_» ___мая_____2021 г

РАБОЧАЯ ПРОГРАММА

дисциплины ПМ.03 Защита информации техническими средствами

Для специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем

Профиль: технический

Составитель(и): Преподаватель Касьяненко А.Ю.

Обсуждена на заседании ПЦК Информационная безопасность автоматизированных систем

Протокол от « 20 » мая 2021 г. № 9

Методист _____Л.В. Петрова

г. Хабаровск
2021 г.

ЛИСТ ДОПОЛНЕНИЙ И ИЗМЕНЕНИЙ (АКТУАЛИЗАЦИИ)

в рабочую программу ПМ.03 Защита информации техническими средствами

наименование структурного элемента ОПОП

10.02.05 Обеспечение информационной безопасности автоматизированных систем

с указанием кода направления подготовки и профиля

На основании

решения заседания кафедры (ПЦК) **Информационная безопасность автоматизированных систем**

полное наименование кафедры (ПЦК)

"26 " мая 2022 г., протокол № 9

на 2022 / 2023 учебный год внесены изменения:

№ / наименование раздела	Новая редакция
	Изменений нет

Заведующий кафедрой (председатель ПЦК)

_____А.Ю. Касьяненко

ЛИСТ ДОПОЛНЕНИЙ И ИЗМЕНЕНИЙ (АКТУАЛИЗАЦИИ)

в рабочую программу ПМ.03 Защита информации техническими средствами

наименование структурного элемента ОПОП

10.02.05 Обеспечение информационной безопасности автоматизированных систем

с указанием кода направления подготовки и профиля

На основании

решения заседания кафедры (ПЦК) **Информационная безопасность автоматизированных систем**

полное наименование кафедры (ПЦК)

"26 " мая 2023 г., протокол № 9

на 2023 / 2024 учебный год внесены изменения:

№ / наименование раздела	Новая редакция
	Изменений нет

Заведующий кафедрой (председатель ПЦК)

_____А.Ю. Касьяненко

Рабочая программа дисциплины ПМ.03 Защита информации техническими средствами

разработана в соответствии с ФГОС, утвержденным приказом Министерства образования и науки Российской Федерации от 09.12.2016 г. № 1553

Квалификация **Техник по защите информации**

Форма обучения **очная**

ОБЪЕМ ДИСЦИПЛИНЫ (МДК, ПМ) В ЧАСАХ С УКАЗАНИЕМ ОБЯЗАТЕЛЬНОЙ И МАКСИМАЛЬНОЙ НАГРУЗКИ ОБУЧАЮЩИХСЯ

Общая трудоемкость **647 ЧАСОВ**

Часов по учебному плану 647

Виды контроля в семестрах:

Дифференцированный зачет: 5
Другие формы промежуточной аттестации: 3,6,7
Зачет: 4
Курсовой проект 8
Экзамен: 8
Экзамен квалификационный: 8

Распределение часов дисциплины (МДК, ПМ) по семестрам (курсам)

Семестр (<Курс>.<Семестр на курсе>)	3 (2.1)		4 (2.2)		5 (3.1)		6 (3.2)		7 (4.1)		8 (4.2)		Итого	
Недель	13 (4)		19 (4)		17		14 2/3 (9)		7 (9)		12 (4)			
Вид занятий	УП	РПД	УП	РПД	УП	РПД	УП	РПД	УП	РПД	УП	РПД	УП	РПД
МДК 03.01														
Лекции, уроки	36	36	40	40	50	50							126	126
Практические занятия	23	23	36	36	35	35							94	94
Лабораторные занятия	6	6											6	6
Итого	65	65	76	76	85	85							226	226
МДК 03.02														
Лекции, уроки							29	29	18	18	46	46	93	93
Практические занятия							10	10	4	4	22	22	36	36
Лабораторные занятия							6	6	6	6	22	22	34	34
Самостоятельная работа											26	26	26	26
Курсовой проект											30	30	30	30
Консультации											6	6	6	6
Промежуточная аттестация (экзамен)											8	8	8	8
Итого							45	45	28	28	160	160	233	233
Учебная практика по ПМ.03, 4 нед*														
Самостоятельная работа			144	144									144	144
Производственная практика по ПМ.03, 1 нед*														
Самостоятельная работа									36	36			36	36
Промежуточная аттестация (экзамен квалификационный)											8	8	8	8
Итого	65	65	220	220	85	85	45	45	64	64	168	168	647	647

*Программа практики приведена в отдельном документе

МДК.03.01 ***Техническая защита информации***

1. АННОТАЦИЯ ДИСЦИПЛИНЫ (МДК, ПМ)	
1.1	Предмет и задачи технической защиты информации. Общие положения защиты информации техническими средствами. Информация как предмет защиты. Технические каналы утечки информации. Методы и средства технической разведки. Физические основы утечки информации по каналам побочных электромагнитных излучений и наводок. Физические процессы при подавлении опасных сигналов. Системы защиты от утечки информации по акустическому каналу. Системы защиты от утечки информации по проводному каналу. Системы защиты от утечки информации по вибрационному каналу. Системы защиты от утечки информации по электромагнитному каналу. Системы защиты от утечки информации по телефонному каналу. Системы защиты от утечки информации по электросетевому каналу. Системы защиты от утечки информации по оптическому каналу. Применение технических средств защиты информации. Эксплуатация технических средств защиты информации.

2. МЕСТО ДИСЦИПЛИНЫ (МДК, ПМ) В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ	
Код дисциплины:	МДК.03.01
2.1	**Требования к предварительной подготовке обучающегося:**
2.1.1	ПД.2 Информатика
2.1.2	ПД.3 Физика
	МДК изучается в 1,2 семестрах 2 курса и в 1 семестре 3 курса
2.2	**Дисциплины и практики, для которых освоение данной дисциплины (МДК, ПМ) необходимо как предшествующее:**
2.2.1	МДК 03.02 Инженерно-технические средства физической защиты объектов информатизации
2.2.2	МДК 04.01 Выполнение работ по одной или нескольким профессиям рабочих, должностям служащих

3. ПЕРЕЧЕНЬ ПЛАНИРУЕМЫХ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ (МДК, ПМ), СООТНЕСЕННЫХ С ПЛАНИРУЕМЫМИ РЕЗУЛЬТАТАМИ ОСВОЕНИЯ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ
ОК 01: Выбирать способы решения задач профессиональной деятельности применительно к различным контекстам
Знать: актуальный профессиональный и социальный контекст, в котором приходится работать и жить; основные источники информации и ресурсы для решения задач и проблем в профессиональном и/или социальном контексте; алгоритмы выполнения работ в профессиональной и смежных областях; методы работы в профессиональной и смежных сферах; структуру плана для решения задач; порядок оценки результатов решения задач профессиональной деятельности
Уметь: распознавать задачу и/или проблему в профессиональном и/или социальном контексте; анализировать задачу и/или проблему и выделять её составные части; определять этапы решения задачи; выявлять и эффективно искать информацию, необходимую для решения задачи и/или проблемы; составить план действия; определить необходимые ресурсы; владеть актуальными методами работы в профессиональной и смежных сферах; реализовать составленный план; оценивать результат и последствия своих действий (самостоятельно или с помощью наставника)
ОК 02: Осуществлять поиск, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности
Знать: номенклатура информационных источников применяемых в профессиональной деятельности; приемы структурирования информации; формат оформления результатов поиска информации
Уметь: определять задачи для поиска информации; определять необходимые источники информации; планировать процесс поиска; структурировать получаемую информацию; выделять наиболее значимое в перечне информации; оценивать практическую значимость результатов поиска; оформлять результаты поиска
ОК 03: Планировать и реализовывать собственное профессиональное и личностное развитие
Знать: содержание актуальной нормативно-правовой документации; современная научная и профессиональная терминология; возможные траектории профессионального развития и самообразования
Уметь: определять актуальность нормативно-правовой документации в профессиональной деятельности; выстраивать траектории профессионального и личностного развития
ОК 04: Работать в коллективе и команде, эффективно взаимодействовать с коллегами, руководством, клиентами
Знать: психология коллектива; психология личности; основы проектной деятельности
Уметь: организовывать работу коллектива и команды; взаимодействовать с коллегами, руководством, клиентами
ОК 05: Осуществлять устную и письменную коммуникацию на государственном языке с учетом особенностей социального и культурного контекста
Знать: особенности социального и культурного контекста; правила оформления документов.
Уметь: излагать свои мысли на государственном языке; оформлять документы.
ОК 06: Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных общечеловеческих ценностей, применять стандарты антикоррупционного поведения
Знать: сущность гражданско-патриотической позиции; Общечеловеческие ценности; Правила поведения в ходе выполнения профессиональной деятельности
Уметь: описывать значимость своей профессии; Презентовать структуру профессиональной деятельности по

специальности
ОК 07: Содействовать сохранению окружающей среды, ресурсосбережению, эффективно действовать в чрезвычайных ситуациях
Знать: правила экологической безопасности при ведении профессиональной деятельности; основные ресурсы, задействованные в профессиональной деятельности; пути обеспечения ресурсосбережения**.**
Уметь: соблюдать нормы экологической безопасности; определять направления ресурсосбережения в рамках профессиональной деятельности по специальности.
ОК 08: Использовать средства физической культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и поддержание необходимого уровня физической подготовленности
Знать: роль физической культуры в общекультурном, профессиональном и социальном развитии человека; основы здорового образа жизни; условия профессиональной деятельности и зоны риска физического здоровья для специальности; средства профилактики перенапряжения.
Уметь: использовать физкультурно-оздоровительную деятельность для укрепления здоровья, достижения жизненных и профессиональных целей; применять рациональные приемы двигательных функций в профессиональной деятельности; пользоваться средствами профилактики перенапряжения характерными для данной специальности
ОК 09: Использовать информационные технологии в профессиональной деятельности
Знать: современные средства и устройства информатизации; порядок их применения и программное обеспечение в профессиональной деятельности.
Уметь: применять средства информационных технологий для решения профессиональных задач; использовать современное программное обеспечение
ОК 10: Пользоваться профессиональной документацией на государственном и иностранном языках
Знать: правила построения простых и сложных предложений на профессиональные темы; основные общеупотребительные глаголы (бытовая и профессиональная лексика); лексический минимум, относящийся к описанию предметов, средств и процессов профессиональной деятельности; особенности произношения; правила чтения текстов профессиональной направленности
Уметь: понимать общий смысл четко произнесенных высказываний на известные темы (профессиональные и бытовые), понимать тексты на базовые профессиональные темы; участвовать в диалогах на знакомые общие и профессиональные темы; строить простые высказывания о себе и о своей профессиональной деятельности; кратко обосновывать и объяснить свои действия (текущие и планируемые); писать простые связные сообщения на знакомые или интересующие профессиональные темы
ОК 11: Использовать знания по финансовой грамотности, планировать предпринимательскую деятельность в профессиональной сфере
Знать: методы планирования предпринимательской деятельности в профессиональной сфере.
Уметь: использовать полученные знания и опыт в организации предпринимательской деятельности в профессиональной сфере.
ПК 3.1. Осуществлять установку, монтаж, настройку и техническое обслуживание технических средств защиты информации в соответствии с требованиями эксплуатационной документации
Знать: порядок технического обслуживания технических средств защиты информации; номенклатуру применяемых средств защиты информации от несанкционированной утечки по техническим каналам
Уметь: применять технические средства для защиты информации в условиях применения мобильных устройств обработки и передачи данных
Иметь практический опыт: установка, монтаж и настройка технических средств защиты информации; техническое обслуживание технических средств защиты информации; применение основных типов технических средств защиты информации
ПК 3.2. Осуществлять эксплуатацию технических средств защиты информации в соответствии с требованиями эксплуатационной документации
Знать: физические основы, структуру и условия формирования технических каналов утечки информации, способы их выявления и методы оценки опасности, классификацию существующих физических полей и технических каналов утечки информации; порядок устранения неисправностей технических средств защиты информации и организации ремонта технических средств защиты информации; методики инструментального контроля эффективности защиты информации, обрабатываемой средствами вычислительной техники на объектах информатизации; номенклатуру применяемых средств защиты информации от несанкционированной утечки по техническим каналам
Уметь: применять технические средства для криптографической защиты информации конфиденциального характера; применять технические средства для уничтожения информации и носителей информации, защиты информации в условиях применения мобильных устройств обработки и передачи данных; применять нормативные правовые акты, нормативные методические документы по обеспечению защиты информации техническими средствами
Иметь практический опыт: применение основных типов технических средств защиты информации; выявление технических каналов утечки информации; участие в мониторинге эффективности технических средств защиты информации; диагностика, устранение отказов и неисправностей, восстановление работоспособности технических средств защиты информации
ПК 3.3. Осуществлять измерение параметров побочных электромагнитных излучений и наводок, создаваемых техническими средствами обработки информации ограниченного доступа
Знать: номенклатуру и характеристики аппаратуры, используемой для измерения параметров ПЭМИН, а также

параметров фоновых шумов и физических полей, создаваемых техническими средствами защиты информации;
Уметь: применять технические средства для защиты информации в условиях применения мобильных устройств обработки и передачи данных
Иметь практический опыт: проведение измерений параметров ПЭМИН, создаваемых техническими средствами обработки информации, для которой установлен режим конфиденциальности, при аттестации объектов информатизации по требованиям безопасности информации
ПК 3.4. Осуществлять измерение параметров фоновых шумов, а также физических полей, создаваемых техническими средствами защиты информации
Знать: номенклатуру применяемых средств защиты информации от несанкционированной утечки по техническим каналам и физической защиты объектов информации
Уметь: применять технические средства для криптографической защиты информации конфиденциального характера
Иметь практический опыт: проведение измерений параметров фоновых шумов, а также физических полей, создаваемых техническими средствами защиты информации

В результате освоения дисциплины (МДК, ПМ) обучающийся должен

3.1	**Знать:**
	актуальный профессиональный и социальный контекст, в котором приходится работать и жить; основные источники информации и ресурсы для решения задач и проблем в профессиональном и/или социальном контексте; алгоритмы выполнения работ в профессиональной и смежных областях; методы работы в профессиональной и смежных сферах; структуру плана для решения задач; порядок оценки результатов решения задач профессиональной деятельности; номенклатура информационных источников применяемых в профессиональной деятельности; приемы структурирования информации; формат оформления результатов поиска информации; содержание актуальной нормативно-правовой документации; современная научная и профессиональная терминология; возможные траектории профессионального развития и самообразования; психология коллектива; психология личности; основы проектной деятельности; особенности социального и культурного контекста; правила оформления документов; сущность гражданско-патриотической позиции; Общечеловеческие ценности; Правила поведения в ходе выполнения профессиональной деятельности; правила экологической безопасности при ведении профессиональной деятельности; основные ресурсы, задействованные в профессиональной деятельности; пути обеспечения ресурсосбережения; роль физической культуры в общекультурном, профессиональном и социальном развитии человека; основы здорового образа жизни; условия профессиональной деятельности и зоны риска физического здоровья для специальности; средства профилактики перенапряжения; современные средства и устройства информатизации; порядок их применения и программное обеспечение в профессиональной деятельности; правила построения простых и сложных предложений на профессиональные темы; основные общеупотребительные глаголы (бытовая и профессиональная лексика); лексический минимум, относящийся к описанию предметов, средств и процессов профессиональной деятельности; особенности произношения; правила чтения текстов профессиональной направленности; методы планирования предпринимательской деятельности в профессиональной сфере; 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 применяемых средств защиты информации от несанкционированной утечки по техническим каналам; номенклатуру применяемых средств защиты информации от несанкционированной утечки по техническим каналам и физической защиты объектов информации; номенклатуру и характеристики аппаратуры, используемой для измерения параметров ПЭМИН, а также параметров фоновых шумов и физических полей, создаваемых техническими средствами защиты информации.
3.2	**Уметь:**

	распознавать задачу и/или проблему в профессиональном и/или социальном контексте; анализировать задачу и/или проблему и выделять её составные части; определять этапы решения задачи; выявлять и эффективно искать информацию, необходимую для решения задачи и/или проблемы; составить план действия; определить необходимые ресурсы; владеть актуальными методами работы в профессиональной и смежных сферах; реализовать составленный план; оценивать результат и последствия своих действий (самостоятельно или с помощью наставника); определять задачи для поиска информации; определять необходимые источники информации; планировать процесс поиска; структурировать получаемую информацию; выделять наиболее значимое в перечне информации; оценивать практическую значимость результатов поиска; оформлять результаты поиска; определять актуальность нормативно-правовой документации в профессиональной деятельности; выстраивать траектории профессионального и личностного развития; организовывать работу коллектива и команды; взаимодействовать с коллегами, руководством, клиентами; излагать свои мысли на государственном языке; оформлять документы; описывать значимость своей профессии; Презентовать структуру профессиональной деятельности по специальности; соблюдать нормы экологической безопасности; определять направления ресурсосбережения в рамках профессиональной деятельности по специальности; использовать физкультурно-оздоровительную деятельность для укрепления здоровья, достижения жизненных и профессиональных целей; применять рациональные приемы двигательных функций в профессиональной деятельности; пользоваться средствами профилактики перенапряжения характерными для данной специальности; применять средства информационных технологий для решения профессиональных задач; использовать современное программное обеспечение; понимать общий смысл четко произнесенных высказываний на известные темы (профессиональные и бытовые), понимать тексты на базовые профессиональные темы; участвовать в диалогах на знакомые общие и профессиональные темы; строить простые высказывания о себе и о своей профессиональной деятельности; кратко обосновывать и объяснить свои действия (текущие и планируемые); писать простые связные сообщения на знакомые или интересующие профессиональные темы; использовать полученные знания и опыт в организации предпринимательской деятельности в профессиональной сфере; применять технические средства для защиты информации в условиях применения мобильных устройств обработки и передачи данных; применять технические средства для криптографической защиты информации конфиденциального характера; применять технические средства для защиты информации в условиях применения мобильных устройств обработки и передачи данных; применять технические средства для криптографической защиты информации конфиденциального характера.
3.3	**Иметь практический опыт:**
	установка, монтаж и настройка технических средств защиты информации; техническое обслуживание технических средств защиты информации; применение основных типов технических средств защиты информации; применение основных типов технических средств защиты информации; выявление технических каналов утечки информации; участие в мониторинге эффективности технических средств защиты информации; диагностика, устранение отказов и неисправностей, восстановление работоспособности технических средств защиты информации; проведение измерений параметров ПЭМИН, создаваемых техническими средствами обработки информации, для которой установлен режим конфиденциальности, при аттестации объектов информатизации по требованиям безопасности информации; проведение измерений параметров фоновых шумов, а также физических полей, создаваемых техническими средствами защиты информации

4. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (МДК, ПМ), СТРУКТУРИРОВАННОЕ ПО ТЕМАМ (РАЗДЕЛАМ) С УКАЗАНИЕМ ОТВЕДЕННОГО НА НИХ КОЛИЧЕСТВА АКАДЕМИЧЕСКИХ ЧАСОВ И ВИДОВ УЧЕБНЫХ ЗАНЯТИЙ

Код занятия	Наименование разделов и тем /вид занятия/	Семестр / Курс	Часов	Компетенции	Литература	Примечание
	Раздел 1. Лекционные занятия					
1.1	Предмет и задачи технической защиты информации.	3/2	2	ОК 01, ОК 02, ОК 03, ОК 04, ОК 05, ОК 06, ОК 07, ОК 08, ОК 09, ОК 10, ОК 11, ПК 3.1, ПК 3.2, ПК 3.3, ПК 3.4	Л1.1, Л1.2, Л2.1, Л2.2, Э1, Э2, Э3	

1.2	Предмет и задачи технической защиты информации.	3/2	2	ОК 01, ОК 02, ОК 03, ОК 04, ОК 05, ОК 06, ОК 07, ОК 08, ОК 09, ОК 10, ОК 11, ПК 3.1, ПК 3.2, ПК 3.3, ПК 3.4	Л1.1, Л1.2, Л2.1, Л2.2, Э1, Э2, Э3		
1.3	Предмет и задачи технической защиты информации.	3/2	2	ОК 01, ОК 02, ОК 03, ОК 04, ОК 05, ОК 06, ОК 07, ОК 08, ОК 09, ОК 10, ОК 11, ПК 3.1, ПК 3.2, ПК 3.3, ПК 3.4	Л1.1, Л1.2, Л2.1, Л2.2, Э1, Э2, Э3		
1.4	Предмет и задачи технической защиты информации.	3/2	2	ОК 01, ОК 02, ОК 03, ОК 04, ОК 05, ОК 06, ОК 07, ОК 08, ОК 09, ОК 10, ОК 11, ПК 3.1, ПК 3.2, ПК 3.3, ПК 3.4	Л1.1, Л1.2, Л2.1, Л2.2, Э1, Э2, Э3		
1.5	Общие положения защиты информации техническими средствами.	3/2	2	ОК 01, ОК 02, ОК 03, ОК 04, ОК 05, ОК 06, ОК 07, ОК 08, ОК 09, ОК 10, ОК 11, ПК 3.1, ПК 3.2, ПК 3.3, ПК 3.4	Л1.1, Л1.2, Л2.1, Л2.2, Э1, Э2, Э3		
1.6	Общие положения защиты информации техническими средствами.	3/2	2	ОК 01, ОК 02, ОК 03, ОК 04, ОК 05, ОК 06, ОК 07, ОК 08, ОК 09, ОК 10, ОК 11, ПК 3.1, ПК 3.2, ПК 3.3, ПК 3.4	Л1.1, Л1.2, Л2.1, Л2.2, Э1, Э2, Э3		
1.7	Общие положения защиты информации техническими средствами.	3/2	2	ОК 01, ОК 02, ОК 03, ОК 04, ОК 05, ОК 06, ОК 07, ОК 08, ОК 09, ОК 10, ОК 11, ПК 3.1, ПК 3.2, ПК 3.3, ПК 3.4	Л1.1, Л1.2, Л2.1, Л2.2, Э1, Э2, Э3		

1.8	Общие положения защиты информации техническими средствами.	3/2	2	ОК 01, ОК 02, ОК 03, ОК 04, ОК 05, ОК 06, ОК 07, ОК 08, ОК 09, ОК 10, ОК 11, ПК 3.1, ПК 3.2, ПК 3.3, ПК 3.4	Л1.1, Л1.2, Л2.1, Л2.2, Э1, Э2, Э3		
1.9	Общие положения защиты информации техническими средствами.	3/2	2	ОК 01, ОК 02, ОК 03, ОК 04, ОК 05, ОК 06, ОК 07, ОК 08, ОК 09, ОК 10, ОК 11, ПК 3.1, ПК 3.2, ПК 3.3, ПК 3.4	Л1.1, Л1.2, Л2.1, Л2.2, Э1, Э2, Э3		
1.10	Информация как предмет защиты.	3/2	2	ОК 01, ОК 02, ОК 03, ОК 04, ОК 05, ОК 06, ОК 07, ОК 08, ОК 09, ОК 10, ОК 11, ПК 3.1, ПК 3.2, ПК 3.3, ПК 3.4	Л1.1, Л1.2, Л2.1, Л2.2, Э1, Э2, Э3		
1.11	Информация как предмет защиты.	3/2	2	ОК 01, ОК 02, ОК 03, ОК 04, ОК 05, ОК 06, ОК 07, ОК 08, ОК 09, ОК 10, ОК 11, ПК 3.1, ПК 3.2, ПК 3.3, ПК 3.4	Л1.1, Л1.2, Л2.1, Л2.2, Э1, Э2, Э3		
1.12	Информация как предмет защиты.	3/2	2	ОК 01, ОК 02, ОК 03, ОК 04, ОК 05, ОК 06, ОК 07, ОК 08, ОК 09, ОК 10, ОК 11, ПК 3.1, ПК 3.2, ПК 3.3, ПК 3.4	Л1.1, Л1.2, Л2.1, Л2.2, Э1, Э2, Э3		
1.13	Информация как предмет защиты.	3/2	2	ОК 01, ОК 02, ОК 03, ОК 04, ОК 05, ОК 06, ОК 07, ОК 08, ОК 09, ОК 10, ОК 11, ПК 3.1, ПК 3.2, ПК 3.3, ПК 3.4	Л1.1, Л1.2, Л2.1, Л2.2, Э1, Э2, Э3		

1.14	Технические каналы утечки информации.	3/2	2	ОК 01, ОК 02, ОК 03, ОК 04, ОК 05, ОК 06, ОК 07, ОК 08, ОК 09, ОК 10, ОК 11, ПК 3.1, ПК 3.2, ПК 3.3, ПК 3.4	Л1.1, Л1.2, Л2.1, Л2.2, Э1, Э2, Э3		
1.15	Технические каналы утечки информации.	3/2	2	ОК 01, ОК 02, ОК 03, ОК 04, ОК 05, ОК 06, ОК 07, ОК 08, ОК 09, ОК 10, ОК 11, ПК 3.1, ПК 3.2, ПК 3.3, ПК 3.4	Л1.1, Л1.2, Л2.1, Л2.2, Э1, Э2, Э3		
1.16	Технические каналы утечки информации.	3/2	2	ОК 01, ОК 02, ОК 03, ОК 04, ОК 05, ОК 06, ОК 07, ОК 08, ОК 09, ОК 10, ОК 11, ПК 3.1, ПК 3.2, ПК 3.3, ПК 3.4	Л1.1, Л1.2, Л2.1, Л2.2, Э1, Э2, Э3		
1.17	Технические каналы утечки информации.	3/2	2	ОК 01, ОК 02, ОК 03, ОК 04, ОК 05, ОК 06, ОК 07, ОК 08, ОК 09, ОК 10, ОК 11, ПК 3.1, ПК 3.2, ПК 3.3, ПК 3.4	Л1.1, Л1.2, Л2.1, Л2.2, Э1, Э2, Э3		
1.18	Технические каналы утечки информации.	3/2	2	ОК 01, ОК 02, ОК 03, ОК 04, ОК 05, ОК 06, ОК 07, ОК 08, ОК 09, ОК 10, ОК 11, ПК 3.1, ПК 3.2, ПК 3.3, ПК 3.4	Л1.1, Л1.2, Л2.1, Л2.2, Э1, Э2, Э3		
1.19	Методы и средства технической разведки.	4/2	2	ОК 01, ОК 02, ОК 03, ОК 04, ОК 05, ОК 06, ОК 07, ОК 08, ОК 09, ОК 10, ОК 11, ПК 3.1, ПК 3.2, ПК 3.3, ПК 3.4	Л1.1, Л1.2, Л2.1, Л2.2, Э1, Э2, Э3		

1.20	Методы и средства технической разведки.	4/2	2	ОК 01, ОК 02, ОК 03, ОК 04, ОК 05, ОК 06, ОК 07, ОК 08, ОК 09, ОК 10, ОК 11, ПК 3.1, ПК 3.2, ПК 3.3, ПК 3.4	Л1.1, Л1.2, Л2.1, Л2.2, Э1, Э2, Э3		
1.21	Методы и средства технической разведки.	4/2	2	ОК 01, ОК 02, ОК 03, ОК 04, ОК 05, ОК 06, ОК 07, ОК 08, ОК 09, ОК 10, ОК 11, ПК 3.1, ПК 3.2, ПК 3.3, ПК 3.4	Л1.1, Л1.2, Л2.1, Л2.2, Э1, Э2, Э3		
1.22	Методы и средства технической разведки.	4/2	2	ОК 01, ОК 02, ОК 03, ОК 04, ОК 05, ОК 06, ОК 07, ОК 08, ОК 09, ОК 10, ОК 11, ПК 3.1, ПК 3.2, ПК 3.3, ПК 3.4	Л1.1, Л1.2, Л2.1, Л2.2, Э1, Э2, Э3		
1.23	Физические основы утечки информации по каналам побочных электромагнитных излучений и наводок.	4/2	2	ОК 01, ОК 02, ОК 03, ОК 04, ОК 05, ОК 06, ОК 07, ОК 08, ОК 09, ОК 10, ОК 11, ПК 3.1, ПК 3.2, ПК 3.3, ПК 3.4	Л1.1, Л1.2, Л2.1, Л2.2, Э1, Э2, Э3		
1.24	Физические основы утечки информации по каналам побочных электромагнитных излучений и наводок.	4/2	2	ОК 01, ОК 02, ОК 03, ОК 04, ОК 05, ОК 06, ОК 07, ОК 08, ОК 09, ОК 10, ОК 11, ПК 3.1, ПК 3.2, ПК 3.3, ПК 3.4	Л1.1, Л1.2, Л2.1, Л2.2, Э1, Э2, Э3		
1.25	Физические основы утечки информации по каналам побочных электромагнитных излучений и наводок.	4/2	2	ОК 01, ОК 02, ОК 03, ОК 04, ОК 05, ОК 06, ОК 07, ОК 08, ОК 09, ОК 10, ОК 11, ПК 3.1, ПК 3.2, ПК 3.3, ПК 3.4	Л1.1, Л1.2, Л2.1, Л2.2, Э1, Э2, Э3		

1.26	Физические основы утечки информации по каналам побочных электромагнитных излучений и наводок.	4/2	2	ОК 01, ОК 02, ОК 03, ОК 04, ОК 05, ОК 06, ОК 07, ОК 08, ОК 09, ОК 10, ОК 11, ПК 3.1, ПК 3.2, ПК 3.3, ПК 3.4	Л1.1, Л1.2, Л2.1, Л2.2, Э1, Э2, Э3		
1.27	Физические процессы при подавлении опасных сигналов.	4/2	2	ОК 01, ОК 02, ОК 03, ОК 04, ОК 05, ОК 06, ОК 07, ОК 08, ОК 09, ОК 10, ОК 11, ПК 3.1, ПК 3.2, ПК 3.3, ПК 3.4	Л1.1, Л1.2, Л2.1, Л2.2, Э1, Э2, Э3		
1.28	Физические процессы при подавлении опасных сигналов.	4/2	2	ОК 01, ОК 02, ОК 03, ОК 04, ОК 05, ОК 06, ОК 07, ОК 08, ОК 09, ОК 10, ОК 11, ПК 3.1, ПК 3.2, ПК 3.3, ПК 3.4	Л1.1, Л1.2, Л2.1, Л2.2, Э1, Э2, Э3		
1.29	Физические процессы при подавлении опасных сигналов.	4/2	2	ОК 01, ОК 02, ОК 03, ОК 04, ОК 05, ОК 06, ОК 07, ОК 08, ОК 09, ОК 10, ОК 11, ПК 3.1, ПК 3.2, ПК 3.3, ПК 3.4	Л1.1, Л1.2, Л2.1, Л2.2, Э1, Э2, Э3		
1.30	Физические процессы при подавлении опасных сигналов.	4/2	2	ОК 01, ОК 02, ОК 03, ОК 04, ОК 05, ОК 06, ОК 07, ОК 08, ОК 09, ОК 10, ОК 11, ПК 3.1, ПК 3.2, ПК 3.3, ПК 3.4	Л1.1, Л1.2, Л2.1, Л2.2, Э1, Э2, Э3		
1.31	Системы защиты от утечки информации по акустическому каналу.	4/2	2	ОК 01, ОК 02, ОК 03, ОК 04, ОК 05, ОК 06, ОК 07, ОК 08, ОК 09, ОК 10, ОК 11, ПК 3.1, ПК 3.2, ПК 3.3, ПК 3.4	Л1.1, Л1.2, Л2.1, Л2.2, Э1, Э2, Э3		
1.32	Системы защиты от утечки информации по акустическому каналу.	4/2	2	ОК 01, ОК 02, ОК 03, ОК 04, ОК 05, ОК 06, ОК 07, ОК 08, ОК 09, ОК 10, ОК 11, ПК 3.1,	Л1.1, Л1.2, Л2.1, Л2.2, Э1, Э2, Э3		

				ПК 3.2, ПК 3.3, ПК 3.4			
1.33	Системы защиты от утечки информации по акустическому каналу.	4/2	2	ОК 01, ОК 02, ОК 03, ОК 04, ОК 05, ОК 06, ОК 07, ОК 08, ОК 09, ОК 10, ОК 11, ПК 3.1, ПК 3.2, ПК 3.3, ПК 3.4	Л1.1, Л1.2, Л2.1, Л2.2, Э1, Э2, Э3		
1.34	Системы защиты от утечки информации по акустическому каналу.	4/2	2	ОК 01, ОК 02, ОК 03, ОК 04, ОК 05, ОК 06, ОК 07, ОК 08, ОК 09, ОК 10, ОК 11, ПК 3.1, ПК 3.2, ПК 3.3, ПК 3.4	Л1.1, Л1.2, Л2.1, Л2.2, Э1, Э2, Э3		
1.35	Системы защиты от утечки информации по проводному каналу.	4/2	2	ОК 01, ОК 02, ОК 03, ОК 04, ОК 05, ОК 06, ОК 07, ОК 08, ОК 09, ОК 10, ОК 11, ПК 3.1, ПК 3.2, ПК 3.3, ПК 3.4	Л1.1, Л1.2, Л2.1, Л2.2, Э1, Э2, Э3		
1.36	Системы защиты от утечки информации по проводному каналу.	4/2	2	ОК 01, ОК 02, ОК 03, ОК 04, ОК 05, ОК 06, ОК 07, ОК 08, ОК 09, ОК 10, ОК 11, ПК 3.1, ПК 3.2, ПК 3.3, ПК 3.4	Л1.1, Л1.2, Л2.1, Л2.2, Э1, Э2, Э3		
1.37	Системы защиты от утечки информации по проводному каналу.	4/2	2	ОК 01, ОК 02, ОК 03, ОК 04, ОК 05, ОК 06, ОК 07, ОК 08, ОК 09, ОК 10, ОК 11, ПК 3.1, ПК 3.2, ПК 3.3, ПК 3.4	Л1.1, Л1.2, Л2.1, Л2.2, Э1, Э2, Э3		
1.38	Системы защиты от утечки информации по проводному каналу.	4/2	2	ОК 01, ОК 02, ОК 03, ОК 04, ОК 05, ОК 06, ОК 07, ОК 08, ОК 09, ОК 10, ОК 11, ПК 3.1, ПК 3.2, ПК 3.3, ПК 3.4	Л1.1, Л1.2, Л2.1, Л2.2, Э1, Э2, Э3		

1.39	Системы защиты от утечки информации по вибрационному каналу.	5/3	2	ОК 01, ОК 02, ОК 03, ОК 04, ОК 05, ОК 06, ОК 07, ОК 08, ОК 09, ОК 10, ОК 11, ПК 3.1, ПК 3.2, ПК 3.3, ПК 3.4	Л1.1, Л1.2, Л2.1, Л2.2, Э1, Э2, Э3		
1.40	Системы защиты от утечки информации по вибрационному каналу.	5/3	2	ОК 01, ОК 02, ОК 03, ОК 04, ОК 05, ОК 06, ОК 07, ОК 08, ОК 09, ОК 10, ОК 11, ПК 3.1, ПК 3.2, ПК 3.3, ПК 3.4	Л1.1, Л1.2, Л2.1, Л2.2, Э1, Э2, Э3		
1.41	Системы защиты от утечки информации по вибрационному каналу.	5/3	2	ОК 01, ОК 02, ОК 03, ОК 04, ОК 05, ОК 06, ОК 07, ОК 08, ОК 09, ОК 10, ОК 11, ПК 3.1, ПК 3.2, ПК 3.3, ПК 3.4	Л1.1, Л1.2, Л2.1, Л2.2, Э1, Э2, Э3		
1.42	Системы защиты от утечки информации по электромагнитному каналу.	5/3	2	ОК 01, ОК 02, ОК 03, ОК 04, ОК 05, ОК 06, ОК 07, ОК 08, ОК 09, ОК 10, ОК 11, ПК 3.1, ПК 3.2, ПК 3.3, ПК 3.4	Л1.1, Л1.2, Л2.1, Л2.2, Э1, Э2, Э3		
1.43	Системы защиты от утечки информации по электромагнитному каналу.	5/3	2	ОК 01, ОК 02, ОК 03, ОК 04, ОК 05, ОК 06, ОК 07, ОК 08, ОК 09, ОК 10, ОК 11, ПК 3.1, ПК 3.2, ПК 3.3, ПК 3.4	Л1.1, Л1.2, Л2.1, Л2.2, Э1, Э2, Э3		
1.44	Системы защиты от утечки информации по электромагнитному каналу.	5/3	2	ОК 01, ОК 02, ОК 03, ОК 04, ОК 05, ОК 06, ОК 07, ОК 08, ОК 09, ОК 10, ОК 11, ПК 3.1, ПК 3.2, ПК 3.3, ПК 3.4	Л1.1, Л1.2, Л2.1, Л2.2, Э1, Э2, Э3		

1.45	Системы защиты от утечки информации по телефонному каналу.	5/3	2	ОК 01, ОК 02, ОК 03, ОК 04, ОК 05, ОК 06, ОК 07, ОК 08, ОК 09, ОК 10, ОК 11, ПК 3.1, ПК 3.2, ПК 3.3, ПК 3.4	Л1.1, Л1.2, Л2.1, Л2.2, Э1, Э2, Э3		
1.46	Системы защиты от утечки информации по телефонному каналу.	5/3	2	ОК 01, ОК 02, ОК 03, ОК 04, ОК 05, ОК 06, ОК 07, ОК 08, ОК 09, ОК 10, ОК 11, ПК 3.1, ПК 3.2, ПК 3.3, ПК 3.4	Л1.1, Л1.2, Л2.1, Л2.2, Э1, Э2, Э3		
1.47	Системы защиты от утечки информации по телефонному каналу.	5/3	2	ОК 01, ОК 02, ОК 03, ОК 04, ОК 05, ОК 06, ОК 07, ОК 08, ОК 09, ОК 10, ОК 11, ПК 3.1, ПК 3.2, ПК 3.3, ПК 3.4	Л1.1, Л1.2, Л2.1, Л2.2, Э1, Э2, Э3		
1.48	Системы защиты от утечки информации по телефонному каналу.	5/3	2	ОК 01, ОК 02, ОК 03, ОК 04, ОК 05, ОК 06, ОК 07, ОК 08, ОК 09, ОК 10, ОК 11, ПК 3.1, ПК 3.2, ПК 3.3, ПК 3.4	Л1.1, Л1.2, Л2.1, Л2.2, Э1, Э2, Э3		
1.49	Системы защиты от утечки информации по электросетевому каналу.	5/3	2	ОК 01, ОК 02, ОК 03, ОК 04, ОК 05, ОК 06, ОК 07, ОК 08, ОК 09, ОК 10, ОК 11, ПК 3.1, ПК 3.2, ПК 3.3, ПК 3.4	Л1.1, Л1.2, Л2.1, Л2.2, Э1, Э2, Э3		
1.50	Системы защиты от утечки информации по электросетевому каналу.	5/3	2	ОК 01, ОК 02, ОК 03, ОК 04, ОК 05, ОК 06, ОК 07, ОК 08, ОК 09, ОК 10, ОК 11, ПК 3.1, ПК 3.2, ПК 3.3, ПК 3.4	Л1.1, Л1.2, Л2.1, Л2.2, Э1, Э2, Э3		
1.51	Системы защиты от утечки информации по электросетевому каналу.	5/3	2	ОК 01, ОК 02, ОК 03, ОК 04, ОК 05, ОК 06, ОК 07, ОК 08, ОК 09, ОК 10, ОК 11, ПК 3.1, ПК 3.2, ПК 3.3, ПК 3.4	Л1.1, Л1.2, Л2.1, Л2.2, Э1, Э2, Э3		

1.52	Системы защиты от утечки информации по оптическому каналу.	5/3	2	ОК 01, ОК 02, ОК 03, ОК 04, ОК 05, ОК 06, ОК 07, ОК 08, ОК 09, ОК 10, ОК 11, ПК 3.1, ПК 3.2, ПК 3.3, ПК 3.4	Л1.1, Л1.2, Л2.1, Л2.2, Э1, Э2, Э3		
1.53	Системы защиты от утечки информации по оптическому каналу.	5/3	2	ОК 01, ОК 02, ОК 03, ОК 04, ОК 05, ОК 06, ОК 07, ОК 08, ОК 09, ОК 10, ОК 11, ПК 3.1, ПК 3.2, ПК 3.3, ПК 3.4	Л1.1, Л1.2, Л2.1, Л2.2, Э1, Э2, Э3		
1.54	Системы защиты от утечки информации по оптическому каналу.	5/3	2	ОК 01, ОК 02, ОК 03, ОК 04, ОК 05, ОК 06, ОК 07, ОК 08, ОК 09, ОК 10, ОК 11, ПК 3.1, ПК 3.2, ПК 3.3, ПК 3.4	Л1.1, Л1.2, Л2.1, Л2.2, Э1, Э2, Э3		
1.55	Применение технических средств защиты информации.	5/3	2	ОК 01, ОК 02, ОК 03, ОК 04, ОК 05, ОК 06, ОК 07, ОК 08, ОК 09, ОК 10, ОК 11, ПК 3.1, ПК 3.2, ПК 3.3, ПК 3.4	Л1.1, Л1.2, Л2.1, Л2.2, Э1, Э2, Э3		
1.56	Применение технических средств защиты информации.	5/3	2	ОК 01, ОК 02, ОК 03, ОК 04, ОК 05, ОК 06, ОК 07, ОК 08, ОК 09, ОК 10, ОК 11, ПК 3.1, ПК 3.2, ПК 3.3, ПК 3.4	Л1.1, Л1.2, Л2.1, Л2.2, Э1, Э2, Э3		
1.57	Применение технических средств защиты информации.	5/3	2	ОК 01, ОК 02, ОК 03, ОК 04, ОК 05, ОК 06, ОК 07, ОК 08, ОК 09, ОК 10, ОК 11, ПК 3.1, ПК 3.2, ПК 3.3, ПК 3.4	Л1.1, Л1.2, Л2.1, Л2.2, Э1, Э2, Э3		
1.58	Применение технических средств защиты информации.	5/3	2	ОК 01, ОК 02, ОК 03, ОК 04, ОК 05, ОК 06, ОК 07, ОК 08, ОК 09, ОК 10, ОК 11, ПК 3.1, ПК 3.2, ПК 3.3, ПК 3.4	Л1.1, Л1.2, Л2.1, Л2.2, Э1, Э2, Э3		

1.59	Эксплуатация технических средств защиты информации.	5/3	2	ОК 01, ОК 02, ОК 03, ОК 04, ОК 05, ОК 06, ОК 07, ОК 08, ОК 09, ОК 10, ОК 11, ПК 3.1, ПК 3.2, ПК 3.3, ПК 3.4	Л1.1, Л1.2, Л2.1, Л2.2, Э1, Э2, Э3		
1.60	Эксплуатация технических средств защиты информации.	5/3	2	ОК 01, ОК 02, ОК 03, ОК 04, ОК 05, ОК 06, ОК 07, ОК 08, ОК 09, ОК 10, ОК 11, ПК 3.1, ПК 3.2, ПК 3.3, ПК 3.4	Л1.1, Л1.2, Л2.1, Л2.2, Э1, Э2, Э3		
1.61	Эксплуатация технических средств защиты информации.	5/3	2	ОК 01, ОК 02, ОК 03, ОК 04, ОК 05, ОК 06, ОК 07, ОК 08, ОК 09, ОК 10, ОК 11, ПК 3.1, ПК 3.2, ПК 3.3, ПК 3.4	Л1.1, Л1.2, Л2.1, Л2.2, Э1, Э2, Э3		
1.62	Эксплуатация технических средств защиты информации.	5/3	2	ОК 01, ОК 02, ОК 03, ОК 04, ОК 05, ОК 06, ОК 07, ОК 08, ОК 09, ОК 10, ОК 11, ПК 3.1, ПК 3.2, ПК 3.3, ПК 3.4	Л1.1, Л1.2, Л2.1, Л2.2, Э1, Э2, Э3		
	Раздел 2. Практические занятия						
2.1	Источники опасных сигналов.	3/2	2	ОК 01, ОК 02, ОК 03, ОК 04, ОК 05, ОК 06, ОК 07, ОК 08, ОК 09, ОК 10, ОК 11, ПК 3.1, ПК 3.2, ПК 3.3, ПК 3.4	Л1.1, Л1.2, Л2.1, Л2.2, Э1, Э2, Э3		
2.2	Основные и вспомогательные технические средства и системы.	3/2	2	ОК 01, ОК 02, ОК 03, ОК 04, ОК 05, ОК 06, ОК 07, ОК 08, ОК 09, ОК 10, ОК 11, ПК 3.1, ПК 3.2, ПК 3.3, ПК 3.4	Л1.1, Л1.2, Л2.1, Л2.2, Э1, Э2, Э3		
2.3	Основные и вспомогательные технические средства и системы.	3/2	2	ОК 01, ОК 02, ОК 03, ОК 04, ОК 05, ОК 06, ОК 07, ОК 08, ОК 09, ОК 10, ОК 11, ПК 3.1, ПК 3.2, ПК 3.3, ПК 3.4	Л1.1, Л1.2, Л2.1, Л2.2, Э1, Э2, Э3		

2.4	Инженерные средства физической защиты	3/2	2	ОК 01, ОК 02, ОК 03, ОК 04, ОК 05, ОК 06, ОК 07, ОК 08, ОК 09, ОК 10, ОК 11, ПК 3.1, ПК 3.2, ПК 3.3, ПК 3.4	Л1.1, Л1.2, Л2.1, Л2.2, Э1, Э2, Э3		
2.5	Инженерные средства физической защиты	3/2	2	ОК 01, ОК 02, ОК 03, ОК 04, ОК 05, ОК 06, ОК 07, ОК 08, ОК 09, ОК 10, ОК 11, ПК 3.1, ПК 3.2, ПК 3.3, ПК 3.4	Л1.1, Л1.2, Л2.1, Л2.2, Э1, Э2, Э3		
2.6	Инженерные средства физической защиты	3/2	2	ОК 01, ОК 02, ОК 03, ОК 04, ОК 05, ОК 06, ОК 07, ОК 08, ОК 09, ОК 10, ОК 11, ПК 3.1, ПК 3.2, ПК 3.3, ПК 3.4	Л1.1, Л1.2, Л2.1, Л2.2, Э1, Э2, Э3		
2.7	Оптические, акустические, радиоэлектронные и материально-вещественные каналы утечки информации.	3/2	2	ОК 01, ОК 02, ОК 03, ОК 04, ОК 05, ОК 06, ОК 07, ОК 08, ОК 09, ОК 10, ОК 11, ПК 3.1, ПК 3.2, ПК 3.3, ПК 3.4	Л1.1, Л1.2, Л2.1, Л2.2, Э1, Э2, Э3		
2.8	Оптические, акустические, радиоэлектронные и материально-вещественные каналы утечки информации.	3/2	2	ОК 01, ОК 02, ОК 03, ОК 04, ОК 05, ОК 06, ОК 07, ОК 08, ОК 09, ОК 10, ОК 11, ПК 3.1, ПК 3.2, ПК 3.3, ПК 3.4	Л1.1, Л1.2, Л2.1, Л2.2, Э1, Э2, Э3		
2.9	Оптические, акустические, радиоэлектронные и материально-вещественные каналы утечки информации.	3/2	2	ОК 01, ОК 02, ОК 03, ОК 04, ОК 05, ОК 06, ОК 07, ОК 08, ОК 09, ОК 10, ОК 11, ПК 3.1, ПК 3.2, ПК 3.3, ПК 3.4	Л1.1, Л1.2, Л2.1, Л2.2, Э1, Э2, Э3		
2.10	Методы и средства технической разведки.	3/2	2	ОК 01, ОК 02, ОК 03, ОК 04, ОК 05, ОК 06, ОК 07, ОК 08, ОК 09, ОК 10, ОК 11, ПК 3.1, ПК 3.2, ПК 3.3, ПК 3.4	Л1.1, Л1.2, Л2.1, Л2.2, Э1, Э2, Э3		

2.11	Методы и средства технической разведки.	3/2	2	ОК 01, ОК 02, ОК 03, ОК 04, ОК 05, ОК 06, ОК 07, ОК 08, ОК 09, ОК 10, ОК 11, ПК 3.1, ПК 3.2, ПК 3.3, ПК 3.4	Л1.1, Л1.2, Л2.1, Л2.2, Э1, Э2, Э3		
2.12	Методы и средства технической разведки.	3/2	1	ОК 01, ОК 02, ОК 03, ОК 04, ОК 05, ОК 06, ОК 07, ОК 08, ОК 09, ОК 10, ОК 11, ПК 3.1, ПК 3.2, ПК 3.3, ПК 3.4	Л1.1, Л1.2, Л2.1, Л2.2, Э1, Э2, Э3		
2.13	Средства несанкционированного доступа к информации.	4/2	2	ОК 01, ОК 02, ОК 03, ОК 04, ОК 05, ОК 06, ОК 07, ОК 08, ОК 09, ОК 10, ОК 11, ПК 3.1, ПК 3.2, ПК 3.3, ПК 3.4	Л1.1, Л1.2, Л2.1, Л2.2, Э1, Э2, Э3		
2.14	Средства несанкционированного доступа к информации.	4/2	2	ОК 01, ОК 02, ОК 03, ОК 04, ОК 05, ОК 06, ОК 07, ОК 08, ОК 09, ОК 10, ОК 11, ПК 3.1, ПК 3.2, ПК 3.3, ПК 3.4	Л1.1, Л1.2, Л2.1, Л2.2, Э1, Э2, Э3		
2.15	Средства несанкционированного доступа к информации.	4/2	2	ОК 01, ОК 02, ОК 03, ОК 04, ОК 05, ОК 06, ОК 07, ОК 08, ОК 09, ОК 10, ОК 11, ПК 3.1, ПК 3.2, ПК 3.3, ПК 3.4	Л1.1, Л1.2, Л2.1, Л2.2, Э1, Э2, Э3		
2.16	Средства и возможности оптической разведки.	4/2	2	ОК 01, ОК 02, ОК 03, ОК 04, ОК 05, ОК 06, ОК 07, ОК 08, ОК 09, ОК 10, ОК 11, ПК 3.1, ПК 3.2, ПК 3.3, ПК 3.4	Л1.1, Л1.2, Л2.1, Л2.2, Э1, Э2, Э3		
2.17	Средства и возможности оптической разведки.	4/2	2	ОК 01, ОК 02, ОК 03, ОК 04, ОК 05, ОК 06, ОК 07, ОК 08, ОК 09, ОК 10, ОК 11, ПК 3.1, ПК 3.2, ПК 3.3, ПК 3.4	Л1.1, Л1.2, Л2.1, Л2.2, Э1, Э2, Э3		

2.18	Средства и возможности оптической разведки.	4/2	2	ОК 01, ОК 02, ОК 03, ОК 04, ОК 05, ОК 06, ОК 07, ОК 08, ОК 09, ОК 10, ОК 11, ПК 3.1, ПК 3.2, ПК 3.3, ПК 3.4	Л1.1, Л1.2, Л2.1, Л2.2, Э1, Э2, Э3		
2.19	Средства дистанционного съема информации.	4/2	2	ОК 01, ОК 02, ОК 03, ОК 04, ОК 05, ОК 06, ОК 07, ОК 08, ОК 09, ОК 10, ОК 11, ПК 3.1, ПК 3.2, ПК 3.3, ПК 3.4	Л1.1, Л1.2, Л2.1, Л2.2, Э1, Э2, Э3		
2.20	Средства дистанционного съема информации.	4/2	2	ОК 01, ОК 02, ОК 03, ОК 04, ОК 05, ОК 06, ОК 07, ОК 08, ОК 09, ОК 10, ОК 11, ПК 3.1, ПК 3.2, ПК 3.3, ПК 3.4	Л1.1, Л1.2, Л2.1, Л2.2, Э1, Э2, Э3		
2.21	Средства дистанционного съема информации.	4/2	2	ОК 01, ОК 02, ОК 03, ОК 04, ОК 05, ОК 06, ОК 07, ОК 08, ОК 09, ОК 10, ОК 11, ПК 3.1, ПК 3.2, ПК 3.3, ПК 3.4	Л1.1, Л1.2, Л2.1, Л2.2, Э1, Э2, Э3		
2.22	Измерение параметров физических полей	4/2	2	ОК 01, ОК 02, ОК 03, ОК 04, ОК 05, ОК 06, ОК 07, ОК 08, ОК 09, ОК 10, ОК 11, ПК 3.1, ПК 3.2, ПК 3.3, ПК 3.4	Л1.1, Л1.2, Л2.1, Л2.2, Э1, Э2, Э3		
2.23	Измерение параметров физических полей	4/2	2	ОК 01, ОК 02, ОК 03, ОК 04, ОК 05, ОК 06, ОК 07, ОК 08, ОК 09, ОК 10, ОК 11, ПК 3.1, ПК 3.2, ПК 3.3, ПК 3.4	Л1.1, Л1.2, Л2.1, Л2.2, Э1, Э2, Э3		
2.24	Измерение параметров физических полей	4/2	2	ОК 01, ОК 02, ОК 03, ОК 04, ОК 05, ОК 06, ОК 07, ОК 08, ОК 09, ОК 10, ОК 11, ПК 3.1, ПК 3.2, ПК 3.3, ПК 3.4	Л1.1, Л1.2, Л2.1, Л2.2, Э1, Э2, Э3		

2.25	Акустоэлектрические преобразования.	4/2	2	ОК 01, ОК 02, ОК 03, ОК 04, ОК 05, ОК 06, ОК 07, ОК 08, ОК 09, ОК 10, ОК 11, ПК 3.1, ПК 3.2, ПК 3.3, ПК 3.4	Л1.1, Л1.2, Л2.1, Л2.2, Э1, Э2, Э3		
2.26	Акустоэлектрические преобразования.	4/2	2	ОК 01, ОК 02, ОК 03, ОК 04, ОК 05, ОК 06, ОК 07, ОК 08, ОК 09, ОК 10, ОК 11, ПК 3.1, ПК 3.2, ПК 3.3, ПК 3.4	Л1.1, Л1.2, Л2.1, Л2.2, Э1, Э2, Э3		
2.27	Акустоэлектрические преобразования.	4/2	2	ОК 01, ОК 02, ОК 03, ОК 04, ОК 05, ОК 06, ОК 07, ОК 08, ОК 09, ОК 10, ОК 11, ПК 3.1, ПК 3.2, ПК 3.3, ПК 3.4	Л1.1, Л1.2, Л2.1, Л2.2, Э1, Э2, Э3		
2.28	Подавление опасных сигналов акустоэлектрических преобразований.	4/2	2	ОК 01, ОК 02, ОК 03, ОК 04, ОК 05, ОК 06, ОК 07, ОК 08, ОК 09, ОК 10, ОК 11, ПК 3.1, ПК 3.2, ПК 3.3, ПК 3.4	Л1.1, Л1.2, Л2.1, Л2.2, Э1, Э2, Э3		
2.29	Подавление опасных сигналов акустоэлектрических преобразований.	4/2	2	ОК 01, ОК 02, ОК 03, ОК 04, ОК 05, ОК 06, ОК 07, ОК 08, ОК 09, ОК 10, ОК 11, ПК 3.1, ПК 3.2, ПК 3.3, ПК 3.4	Л1.1, Л1.2, Л2.1, Л2.2, Э1, Э2, Э3		
2.30	Подавление опасных сигналов акустоэлектрических преобразований.	4/2	2	ОК 01, ОК 02, ОК 03, ОК 04, ОК 05, ОК 06, ОК 07, ОК 08, ОК 09, ОК 10, ОК 11, ПК 3.1, ПК 3.2, ПК 3.3, ПК 3.4	Л1.1, Л1.2, Л2.1, Л2.2, Э1, Э2, Э3		
2.31	Экранирование. Зашумление.	5/3	2	ОК 01, ОК 02, ОК 03, ОК 04, ОК 05, ОК 06, ОК 07, ОК 08, ОК 09, ОК 10, ОК 11, ПК 3.1, ПК 3.2, ПК 3.3, ПК 3.4	Л1.1, Л1.2, Л2.1, Л2.2, Э1, Э2, Э3		

2.32	Экранирование. Зашумление.	5/3	2	ОК 01, ОК 02, ОК 03, ОК 04, ОК 05, ОК 06, ОК 07, ОК 08, ОК 09, ОК 10, ОК 11, ПК 3.1, ПК 3.2, ПК 3.3, ПК 3.4	Л1.1, Л1.2, Л2.1, Л2.2, Э1, Э2, Э3		
2.33	Экранирование. Зашумление.	5/3	2	ОК 01, ОК 02, ОК 03, ОК 04, ОК 05, ОК 06, ОК 07, ОК 08, ОК 09, ОК 10, ОК 11, ПК 3.1, ПК 3.2, ПК 3.3, ПК 3.4	Л1.1, Л1.2, Л2.1, Л2.2, Э1, Э2, Э3		
2.34	Паразитная генерация радиоэлектронных средств.	5/3	2	ОК 01, ОК 02, ОК 03, ОК 04, ОК 05, ОК 06, ОК 07, ОК 08, ОК 09, ОК 10, ОК 11, ПК 3.1, ПК 3.2, ПК 3.3, ПК 3.4	Л1.1, Л1.2, Л2.1, Л2.2, Э1, Э2, Э3		
2.35	Паразитная генерация радиоэлектронных средств.	5/3	2	ОК 01, ОК 02, ОК 03, ОК 04, ОК 05, ОК 06, ОК 07, ОК 08, ОК 09, ОК 10, ОК 11, ПК 3.1, ПК 3.2, ПК 3.3, ПК 3.4	Л1.1, Л1.2, Л2.1, Л2.2, Э1, Э2, Э3		
2.36	Паразитная генерация радиоэлектронных средств.	5/3	2	ОК 01, ОК 02, ОК 03, ОК 04, ОК 05, ОК 06, ОК 07, ОК 08, ОК 09, ОК 10, ОК 11, ПК 3.1, ПК 3.2, ПК 3.3, ПК 3.4	Л1.1, Л1.2, Л2.1, Л2.2, Э1, Э2, Э3		
2.37	Утечка информации по цепям электропитания и заземления.	5/3	2	ОК 01, ОК 02, ОК 03, ОК 04, ОК 05, ОК 06, ОК 07, ОК 08, ОК 09, ОК 10, ОК 11, ПК 3.1, ПК 3.2, ПК 3.3, ПК 3.4	Л1.1, Л1.2, Л2.1, Л2.2, Э1, Э2, Э3		
2.38	Утечка информации по цепям электропитания и заземления.	5/3	2	ОК 01, ОК 02, ОК 03, ОК 04, ОК 05, ОК 06, ОК 07, ОК 08, ОК 09, ОК 10, ОК 11, ПК 3.1, ПК 3.2, ПК 3.3, ПК 3.4	Л1.1, Л1.2, Л2.1, Л2.2, Э1, Э2, Э3		

2.39	Утечка информации по цепям электропитания и заземления.	5/3	2	ОК 01, ОК 02, ОК 03, ОК 04, ОК 05, ОК 06, ОК 07, ОК 08, ОК 09, ОК 10, ОК 11, ПК 3.1, ПК 3.2, ПК 3.3, ПК 3.4	Л1.1, Л1.2, Л2.1, Л2.2, Э1, Э2, Э3		
2.40	Утечки по акустическому каналу	5/3	2	ОК 01, ОК 02, ОК 03, ОК 04, ОК 05, ОК 06, ОК 07, ОК 08, ОК 09, ОК 10, ОК 11, ПК 3.1, ПК 3.2, ПК 3.3, ПК 3.4	Л1.1, Л1.2, Л2.1, Л2.2, Э1, Э2, Э3		
2.41	Утечки по акустическому каналу	5/3	2	ОК 01, ОК 02, ОК 03, ОК 04, ОК 05, ОК 06, ОК 07, ОК 08, ОК 09, ОК 10, ОК 11, ПК 3.1, ПК 3.2, ПК 3.3, ПК 3.4	Л1.1, Л1.2, Л2.1, Л2.2, Э1, Э2, Э3		
2.42	Утечки по акустическому каналу	5/3	2	ОК 01, ОК 02, ОК 03, ОК 04, ОК 05, ОК 06, ОК 07, ОК 08, ОК 09, ОК 10, ОК 11, ПК 3.1, ПК 3.2, ПК 3.3, ПК 3.4	Л1.1, Л1.2, Л2.1, Л2.2, Э1, Э2, Э3		
2.43	Использование коммуникаций в качестве соединительных проводов.	5/3	2	ОК 01, ОК 02, ОК 03, ОК 04, ОК 05, ОК 06, ОК 07, ОК 08, ОК 09, ОК 10, ОК 11, ПК 3.1, ПК 3.2, ПК 3.3, ПК 3.4	Л1.1, Л1.2, Л2.1, Л2.2, Э1, Э2, Э3		
2.44	Использование коммуникаций в качестве соединительных проводов.	5/3	2	ОК 01, ОК 02, ОК 03, ОК 04, ОК 05, ОК 06, ОК 07, ОК 08, ОК 09, ОК 10, ОК 11, ПК 3.1, ПК 3.2, ПК 3.3, ПК 3.4	Л1.1, Л1.2, Л2.1, Л2.2, Э1, Э2, Э3		
2.45	Использование коммуникаций в качестве соединительных проводов.	5/3	2	ОК 01, ОК 02, ОК 03, ОК 04, ОК 05, ОК 06, ОК 07, ОК 08, ОК 09, ОК 10, ОК 11, ПК 3.1, ПК 3.2, ПК 3.3, ПК 3.4	Л1.1, Л1.2, Л2.1, Л2.2, Э1, Э2, Э3		

2.46	Негласная запись информации на диктофоны.	5/3	2	ОК 01, ОК 02, ОК 03, ОК 04, ОК 05, ОК 06, ОК 07, ОК 08, ОК 09, ОК 10, ОК 11, ПК 3.1, ПК 3.2, ПК 3.3, ПК 3.4	Л1.1, Л1.2, Л2.1, Л2.2, Э1, Э2, Э3		
2.47	Системы защиты от диктофонов.	5/3	2	ОК 01, ОК 02, ОК 03, ОК 04, ОК 05, ОК 06, ОК 07, ОК 08, ОК 09, ОК 10, ОК 11, ПК 3.1, ПК 3.2, ПК 3.3, ПК 3.4	Л1.1, Л1.2, Л2.1, Л2.2, Э1, Э2, Э3		
2.48	Системы защиты от диктофонов.	5/3	1	ОК 01, ОК 02, ОК 03, ОК 04, ОК 05, ОК 06, ОК 07, ОК 08, ОК 09, ОК 10, ОК 11, ПК 3.1, ПК 3.2, ПК 3.3, ПК 3.4	Л1.1, Л1.2, Л2.1, Л2.2, Э1, Э2, Э3		
	Раздел 3. Лабораторные занятия						
3.1	Содержательный анализ основных руководящих, нормативных и методических документов по защите информации и противодействию технической разведке.	3/2	2	ОК 01, ОК 02, ОК 03, ОК 04, ОК 05, ОК 06, ОК 07, ОК 08, ОК 09, ОК 10, ОК 11, ПК 3.1, ПК 3.2, ПК 3.3, ПК 3.4	Л1.1, Л1.2, Л2.1, Л2.2, Л3.1, Э1, Э2, Э3		
3.2	Содержательный анализ основных руководящих, нормативных и методических документов по защите информации и противодействию технической разведке.	3/2	2	ОК 01, ОК 02, ОК 03, ОК 04, ОК 05, ОК 06, ОК 07, ОК 08, ОК 09, ОК 10, ОК 11, ПК 3.1, ПК 3.2, ПК 3.3, ПК 3.4	Л1.1, Л1.2, Л2.1, Л2.2, Л3.1, Э1, Э2, Э3		
3.3	Защита от утечки по акустическому каналу	3/2	2	ОК 01, ОК 02, ОК 03, ОК 04, ОК 05, ОК 06, ОК 07, ОК 08, ОК 09, ОК 10, ОК 11, ПК 3.1, ПК 3.2, ПК 3.3, ПК 3.4	Л1.1, Л1.2, Л2.1, Л2.2, Л3.1, Э1, Э2, Э3		
	Раздел 4. Контроль						
4.1	Другие формы промежуточной аттестации	3/2		ОК 01, ОК 02, ОК 03, ОК 04, ОК 05, ОК 06, ОК 07, ОК 08, ОК 09, ОК 10, ОК 11, ПК 3.1, ПК 3.2, ПК 3.3, ПК 3.4	Л1.1, Л1.2, Л2.1, Л2.2, Л3.1, Э1, Э2, Э3		

4.2	Зачет	4/2		ОК 01, ОК 02, ОК 03, ОК 04, ОК 05, ОК 06, ОК 07, ОК 08, ОК 09, ОК 10, ОК 11, ПК 3.1, ПК 3.2, ПК 3.3, ПК 3.4	Л1.1, Л1.2, Л2.1, Л2.2, Л3.1, Э1, Э2, Э3		
4.3	Дифференцированный зачет	5/3		ОК 01, ОК 02, ОК 03, ОК 04, ОК 05, ОК 06, ОК 07, ОК 08, ОК 09, ОК 10, ОК 11, ПК 3.1, ПК 3.2, ПК 3.3, ПК 3.4	Л1.1, Л1.2, Л2.1, Л2.2, Л3.1, Э1, Э2, Э3		

5. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ ПРОВЕДЕНИЯ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

Размещен в приложении

6. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МДК, ПМ)

6.1. Рекомендуемая литература

6.1.1. Перечень основной литературы, необходимой для освоения дисциплины (МДК, ПМ)

	Авторы, составители	Заглавие	Издательство, год
Л1.1	Голиков, А.М.	Защита информации в инфокоммуникационных системах и сетях	Томск : Томский государственный университет систем управления и радиоэлектроники, 2015
Л1.2	Н.А. Свинарев, О.В. Ланкин, А.П. Данилкин и др	Инструментальный контроль и защита информации	Воронеж : Воронежский государственный университет инженерных технологий, 2013

6.1.2. Перечень дополнительной литературы, необходимой для освоения дисциплины (МДК, ПМ)

	Авторы, составители	Заглавие	Издательство, год
Л2.1	Титов, А.А	Технические средства защиты информации	Томск : Томский государственный университет систем управления и радиоэлектроники, 2010.
Л2.2	Креопалов, В.В.	Технические средства и методы защиты информации	Москва : Евразийский открытый институт, 2011

6.1.3. Перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине (МДК, ПМ)

	Авторы, составители	Заглавие	Издательство, год
Л3.1	Н.А. Руденков, А.В. Пролетарский, Е.В. Смирнова, А.М. Суровов	Технологии защиты информации в компьютерных сетях. Учебное пособие	Москва : Национальный Открытый Университет «ИНТУИТ», 2016.

6.2. Перечень ресурсов информационно-телекоммуникационной сети "Интернет", необходимых для освоения дисциплины (МДК, ПМ)

Э1	Научная электронная библиотека eLIBRARY.RU	elibrary.ru
Э2	Электронно-библиотечная система «Книгафонд»	http://knigafund.ru/
Э3	Электронный каталог НТБ	catalog.lib.tpu.ru

6.3 Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине (МДК, ПМ), включая перечень программного обеспечения и информационных справочных систем (при необходимости)

6.3.1 Перечень программного обеспечения

-Win XP, 7

- DreamSpark Premium Electronic Software Delivery (3 years) Renewal 1203984220
- Kaspersky Endpoint Security 10 для Windows - 356¬160615-113525¬730¬94
- Права на ПО NetPolice School для Traffic Inspector Unlimited
- Права на ПО Traffic Inspector Anti-Virus powered by Kaspersky Special
-Traffic Inspector (Контракт 524 ДВГУПС от 15.07.2019)
Microsoft Windows Professional 10 Russian 1 License 5 шт,
базовый пакет для сертифицированной версии ОС Windows 8.1 Профессиональная/Pro для использования на 1 АРМ 5шт,
Microsoft Office Professional Plus 2019 Russian OLP 1 License 18 шт,
программа контроля сертифицированной версии ОС Windows 8.1 Профессиональная 5 шт,
Microsoft Windows Server CAL 2019 Russian OLP 1 License User CAL 22 шт,
Базовый пакет для сертифицированной версии ОС Microsoft Windows Server Datacenter 2012 R2 для использования на 2 процессора 1 шт,
ОС Astra Linux Special Edition (Box версия с установочным комплектом) 5 шт. - Контракт № 1272401815819000324/157 ДВГУПС от 15.03.2019 г.
RedCheck Professional на 1 IP-адрес на 1 год 10 шт, КриптоПро CSP версии 4.0 5 шт,
Dallas Lock 8.0-C с модулями «Межсетевой экран» и «Система обнаружения и предотвращения вторжений». 5 шт,
Secret Net Studio 8 в редакции «Постоянная защита» (бессрочная) с модулями защиты от НСД, контроля устройств (СКН) и межсетевого экранирования (МЭ) 6 шт,
Антивирус Kaspersky Endpoint Security бизнеса – Расширенный Russian Edition. 1500-2499 Node 1 year Educational Renewal License 20шт. - Контракт № 1272401815819000584/290 ДВГУПС от 08.05.2019 г.
Foxit Reader, свободно распространяемое ПО
6.3.2 Перечень информационных справочных систем
1. Профессиональная база данных, информационно-справочная система Гарант - http://www.garant.ru
2. Профессиональная база данных, информационно-справочная система КонсультантПлюс - http://www.consultant.ru

7. ОПИСАНИЕ МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЙ БАЗЫ, НЕОБХОДИМОЙ ДЛЯ ОСУЩЕСТВЛЕНИЯ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА ПО ДИСЦИПЛИНЕ (МОДУЛЮ)

Аудитория	Назначение	Оснащение
320	Учебная аудитория для проведения теоретических занятий (уроков). Лекционная аудитория.	Комплект мебели, проектор, персональный компьютер, комплект презентаций. - Win XP, 7 - DreamSpark Premium Electronic Software Delivery (3 years) Renewal 1203984220 - Kaspersky Endpoint Security 10 для Windows - 356¬160615-113525¬730¬94 - Права на ПО NetPolice School для Traffic Inspector Unlimited - Права на ПО Traffic Inspector Anti-Virus powered by Kaspersky Special -Traffic Inspector (Контракт 524 ДВГУПС от 15.07.2019)

324	Учебная аудитория для проведения теоретических занятий (уроков), практических занятий, лабораторных работ, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации. Лаборатория программных и программно-аппаратных средств защиты информации. Лаборатория "Защита информации от утечки за счет несанкционированного доступа в локальных вычислительных сетях".	Комплект учебной мебели, экран, автоматизированное рабочее место IZEC «Студент» в сборе 16 шт, Автоматизированное рабочее место IZEC «Преподаватель» в сборе 1 шт, автоматизированное рабочее место IZEC «Диспетчер АСУ ТП» в сборе 1 шт, сервер IZEC на платформе WOLF PASS 2U в сборе 1 шт, сервер IZEC на платформе SILVER PASS 1U в сборе 1 шт, Ноутбук HP 250 G6 15.6 1 шт, МФУ XEROX WC 6515DNI 1 шт, электронный идентификатор ruToken S 64 КБ 20 шт, электронный идентификатор JaCarta-2 PRO/ГОСТ 5 шт, средство доверенной загрузки Dallas Lock PCI-E Full Size 5 шт, средство доверенной загрузки "Соболь" версия 4 PCI-E 5 шт, рупор измерительный широкополосный П6-124 зав. № 150718305 в комплекте с диэлектрическим штативом, кабель КИ-18-5м-SMAM-SMAM, индуктор магнитный ИРМ-500М Зав. № 015, пробник напряжения Я6-122/1М Зав. № 024, токосъемник измерительный ТК-400М Зав. № 87, антенна измерительная дипольная активная АИ5-0 Зав. № 1742, мультимедийный проектор. Microsoft Windows Professional 10 Russian 1 License 5 шт, базовый пакет для сертифицированной версии ОС Windows 8.1 Профессиональная/Pro для использования на 1 АРМ 5шт, Microsoft Office Professional Plus 2019 Russian OLP 1 License 18 шт, программа контроля сертифицированной версии ОС Windows 8.1 Профессиональная 5 шт, Microsoft Windows Server CAL 2019 Russian OLP 1 License User CAL 22 шт, Базовый пакет для сертифицированной версии ОС Microsoft Windows Server Datacenter 2012 R2 для использования на 2 процессора 1 шт, ОС Astra Linux Special Edition (Box версия с установочным комплектом) 5 шт. - Контракт № 1272401815819000032 4/157 ДВГУПС от 15.03.2019 г. RedCheck Professional на 1 IP-адрес на 1 год 10 шт, КриптоПро CSP версии 4.0 5 шт, Dallas Lock 8.0-C с модулями «Межсетевой экран» и «Система обнаружения и предотвращения вторжений». 5 шт, Secret Net Studio 8 в редакции «Постоянная защита» (бессрочная) с модулями защиты от НСД, контроля устройств (СКН) и межсетевого экранирования (МЭ) 6 шт, Антивирус Kaspersky Endpoint Security бизнеса – Расширенный Russian Edition. 1500-2499 Node 1 year Educational Renewal License 20шт. - Контракт № 1272401815819000058 4/290 ДВГУПС от 08.05.2019 г.
331	Учебная аудитория для проведения лабораторных и практических занятий, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации. Лаборатория технических средств защиты информации. Лаборатория "Защита речевой информации".	Оснащенность: комплект учебной мебели, доска, системы виброакустического зашумления "Шорох-1", "Шорох-2", "Шорох-3", "Шорох-4", вибропреобразователи КВП-2, КВП-6, КВП-7, КВП-8,ПЭД-5, ПЭД-6, акустический излучатель, "OMS-2000", устройство дистанционного управления "ДУ-М", зашумляющая акустическая система "Хаос-4 ".
329	Учебная аудитория для проведения лабораторных и практических занятий, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации. "Лаборатория регистрации передачи информации по техническим каналам".	Комплект учебной мебели, доска, стационарный рентгеноскопический комплекс "Премьер-СТ", комплект индивидуальных дозиметров. Foxit Reader, свободно распространяемое ПО

8. МЕТОДИЧЕСКИЕ МАТЕРИАЛЫ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ (МДК, ПМ)

В процессе изучения дисциплины обучающиеся посещают лекции (уроки), практические и лабораторные занятия. На всех этапах обучения по МДК осуществляется контроль знаний.

Лекция (урок). Работа на лекции является очень важным видом деятельности обучающихся для изучения дисциплины , т.к. лектор ориентирует обучающихся в учебном материале. Краткие записи лекций (конспектирование) помогает усвоить материал. Написание конспекта лекций: кратко, схематично, последовательно фиксировать основные положения, выводы, формулировки, обобщения; помечать важные мысли, выделять ключевые слова, термины.

Практические и лабораторные занятия. Обучающиеся самостоятельно под руководством преподавателя выполняют задания по темам курса. Обучающиеся овладевают навыками, необходимыми для осуществления трудовой функции по профессии.

МДК.03.02 ***Инженерно-технические средства физической защиты объектов информатизации***

1. АННОТАЦИЯ ДИСЦИПЛИНЫ (МДК, ПМ)	
1.1	Цели и задачи физической защиты объектов информатизации. Общие сведения о комплексах инженерно-технических средств физической защиты. Система обнаружения комплекса инженерно-технических средств физической защиты. Система контроля и управления доступом. Система телевизионного наблюдения. Система сбора, обработки, отображения и документирования информации. Система воздействия. Применение инженерно-технических средств физической защиты. Эксплуатация инженерно-технических средств физической защиты.

2. МЕСТО ДИСЦИПЛИНЫ (МДК, ПМ) В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ	
Код дисциплины:	МДК.03.02
2.1	**Требования к предварительной подготовке обучающегося:**
2.1.1	ОП.07 Технические средства информатизации
2.1.2	МДК 03.01 Техническая защита информации
	МДК изучается в 2 семестре 3 курса и 1,2 семестрах 4 курса
2.2	**Дисциплины и практики, для которых освоение данной дисциплины (МДК, ПМ) необходимо как предшествующее:**
2.2.1	ПДП Преддипломная практика

3. ПЕРЕЧЕНЬ ПЛАНИРУЕМЫХ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ (МДК, ПМ), СООТНЕСЕННЫХ С ПЛАНИРУЕМЫМИ РЕЗУЛЬТАТАМИ ОСВОЕНИЯ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ
ОК 01: Выбирать способы решения задач профессиональной деятельности применительно к различным контекстам
Знать: актуальный профессиональный и социальный контекст, в котором приходится работать и жить; основные источники информации и ресурсы для решения задач и проблем в профессиональном и/или социальном контексте; алгоритмы выполнения работ в профессиональной и смежных областях; методы работы в профессиональной и смежных сферах; структуру плана для решения задач; порядок оценки результатов решения задач профессиональной деятельности
Уметь: распознавать задачу и/или проблему в профессиональном и/или социальном контексте; анализировать задачу и/или проблему и выделять её составные части; определять этапы решения задачи; выявлять и эффективно искать информацию, необходимую для решения задачи и/или проблемы; составить план действия; определить необходимые ресурсы; владеть актуальными методами работы в профессиональной и смежных сферах; реализовать составленный план; оценивать результат и последствия своих действий (самостоятельно или с помощью наставника)
ОК 02: Осуществлять поиск, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности
Знать: номенклатура информационных источников применяемых в профессиональной деятельности; приемы структурирования информации; формат оформления результатов поиска информации
Уметь: определять задачи для поиска информации; определять необходимые источники информации; планировать процесс поиска; структурировать получаемую информацию; выделять наиболее значимое в перечне информации; оценивать практическую значимость результатов поиска; оформлять результаты поиска
ОК 03: Планировать и реализовывать собственное профессиональное и личностное развитие
Знать: содержание актуальной нормативно-правовой документации; современная научная и профессиональная терминология; возможные траектории профессионального развития и самообразования
Уметь: определять актуальность нормативно-правовой документации в профессиональной деятельности; выстраивать траектории профессионального и личностного развития
ОК 04: Работать в коллективе и команде, эффективно взаимодействовать с коллегами, руководством, клиентами
Знать: психология коллектива; психология личности; основы проектной деятельности
Уметь: организовывать работу коллектива и команды; взаимодействовать с коллегами, руководством, клиентами
ОК 05: Осуществлять устную и письменную коммуникацию на государственном языке с учетом особенностей социального и культурного контекста
Знать: особенности социального и культурного контекста; правила оформления документов.
Уметь: излагать свои мысли на государственном языке; оформлять документы.
ОК 06: Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных общечеловеческих ценностей, применять стандарты антикоррупционного поведения
Знать: сущность гражданско-патриотической позиции; Общечеловеческие ценности; Правила поведения в ходе выполнения профессиональной деятельности
Уметь: описывать значимость своей профессии; Презентовать структуру профессиональной деятельности по специальности
ОК 07: Содействовать сохранению окружающей среды, ресурсосбережению, эффективно действовать в чрезвычайных ситуациях

Знать: правила экологической безопасности при ведении профессиональной деятельности; основные ресурсы, задействованные в профессиональной деятельности; пути обеспечения ресурсосбережения**.**
Уметь: соблюдать нормы экологической безопасности; определять направления ресурсосбережения в рамках профессиональной деятельности по специальности.
ОК 08: Использовать средства физической культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и поддержание необходимого уровня физической подготовленности
Знать: роль физической культуры в общекультурном, профессиональном и социальном развитии человека; основы здорового образа жизни; условия профессиональной деятельности и зоны риска физического здоровья для специальности; средства профилактики перенапряжения.
Уметь: использовать физкультурно-оздоровительную деятельность для укрепления здоровья, достижения жизненных и профессиональных целей; применять рациональные приемы двигательных функций в профессиональной деятельности; пользоваться средствами профилактики перенапряжения характерными для данной специальности
ОК 09: Использовать информационные технологии в профессиональной деятельности
Знать: современные средства и устройства информатизации; порядок их применения и программное обеспечение в профессиональной деятельности.
Уметь: применять средства информационных технологий для решения профессиональных задач; использовать современное программное обеспечение
ОК 10: Пользоваться профессиональной документацией на государственном и иностранном языках
Знать: правила построения простых и сложных предложений на профессиональные темы; основные общеупотребительные глаголы (бытовая и профессиональная лексика); лексический минимум, относящийся к описанию предметов, средств и процессов профессиональной деятельности; особенности произношения; правила чтения текстов профессиональной направленности
Уметь: понимать общий смысл четко произнесенных высказываний на известные темы (профессиональные и бытовые), понимать тексты на базовые профессиональные темы; участвовать в диалогах на знакомые общие и профессиональные темы; строить простые высказывания о себе и о своей профессиональной деятельности; кратко обосновывать и объяснить свои действия (текущие и планируемые); писать простые связные сообщения на знакомые или интересующие профессиональные темы
ОК 11: Использовать знания по финансовой грамотности, планировать предпринимательскую деятельность в профессиональной сфере
Знать: методы планирования предпринимательской деятельности в профессиональной сфере.
Уметь: использовать полученные знания и опыт в организации предпринимательской деятельности в профессиональной сфере.
ПК 3.5. Организовывать отдельные работы по физической защите объектов информатизации
Знать: основные принципы действия и характеристики технических средств физической защиты; основные способы физической защиты объектов информатизации; номенклатуру применяемых средств физической защиты объектов информатизации
Уметь: применять средства охранной сигнализации, охранного телевидения и систем контроля и управления доступом; применять инженерно-технические средства физической защиты объектов информатизации
Иметь практический опыт: установка, монтаж и настройка, техническое обслуживание, диагностика, устранение отказов и неисправностей, восстановление работоспособности инженерно-технических средств физической защиты

В результате освоения дисциплины (МДК, ПМ) обучающийся должен

3.1	**Знать:**
	актуальный профессиональный и социальный контекст, в котором приходится работать и жить; основные источники информации и ресурсы для решения задач и проблем в профессиональном и/или социальном контексте; алгоритмы выполнения работ в профессиональной и смежных областях; методы работы в профессиональной и смежных сферах; структуру плана для решения задач; порядок оценки результатов решения задач профессиональной деятельности; номенклатура информационных источников применяемых в профессиональной деятельности; приемы структурирования информации; формат оформления результатов поиска информации; содержание актуальной нормативно-правовой документации; современная научная и профессиональная терминология; возможные траектории профессионального развития и самообразования; психология коллектива; психология личности; основы проектной деятельности; особенности социального и культурного контекста; правила оформления документов; сущность гражданско-патриотической позиции; Общечеловеческие ценности; Правила поведения в ходе выполнения профессиональной деятельности; правила экологической безопасности при ведении профессиональной деятельности; основные ресурсы, задействованные в профессиональной деятельности; пути обеспечения ресурсосбережения; роль физической культуры в общекультурном, профессиональном и социальном развитии человека; основы здорового образа жизни; условия профессиональной деятельности и зоны риска физического здоровья для специальности; средства профилактики перенапряжения; современные средства и устройства информатизации; порядок их применения и программное обеспечение в профессиональной деятельности; правила построения простых и сложных предложений на профессиональные темы; основные общеупотребительные глаголы (бытовая и профессиональная лексика); лексический минимум, относящийся к описанию предметов, средств и процессов профессиональной

	деятельности; особенности произношения; правила чтения текстов профессиональной направленности; методы планирования предпринимательской деятельности в профессиональной сфере; основные принципы действия и характеристики технических средств физической защиты; основные способы физической защиты объектов информатизации; номенклатуру применяемых средств физической защиты объектов информатизации
3.2	**Уметь:**
	распознавать задачу и/или проблему в профессиональном и/или социальном контексте; анализировать задачу и/или проблему и выделять её составные части; определять этапы решения задачи; выявлять и эффективно искать информацию, необходимую для решения задачи и/или проблемы; составить план действия; определить необходимые ресурсы; владеть актуальными методами работы в профессиональной и смежных сферах; реализовать составленный план; оценивать результат и последствия своих действий (самостоятельно или с помощью наставника); определять задачи для поиска информации; определять необходимые источники информации; планировать процесс поиска; структурировать получаемую информацию; выделять наиболее значимое в перечне информации; оценивать практическую значимость результатов поиска; оформлять результаты поиска; определять актуальность нормативно-правовой документации в профессиональной деятельности; выстраивать траектории профессионального и личностного развития; организовывать работу коллектива и команды; взаимодействовать с коллегами, руководством, клиентами; излагать свои мысли на государственном языке; оформлять документы; описывать значимость своей профессии; Презентовать структуру профессиональной деятельности по специальности; соблюдать нормы экологической безопасности; определять направления ресурсосбережения в рамках профессиональной деятельности по специальности; использовать физкультурно-оздоровительную деятельность для укрепления здоровья, достижения жизненных и профессиональных целей; применять рациональные приемы двигательных функций в профессиональной деятельности; пользоваться средствами профилактики перенапряжения характерными для данной специальности; применять средства информационных технологий для решения профессиональных задач; использовать современное программное обеспечение; понимать общий смысл четко произнесенных высказываний на известные темы (профессиональные и бытовые), понимать тексты на базовые профессиональные темы; участвовать в диалогах на знакомые общие и профессиональные темы; строить простые высказывания о себе и о своей профессиональной деятельности; кратко обосновывать и объяснить свои действия (текущие и планируемые); писать простые связные сообщения на знакомые или интересующие профессиональные темы; использовать полученные знания и опыт в организации предпринимательской деятельности в профессиональной сфере; применять средства охранной сигнализации, охранного телевидения и систем контроля и управления доступом; применять инженерно-технические средства физической защиты объектов информатизации
3.3	**Иметь практический опыт:**
	установка, монтаж и настройка, техническое обслуживание, диагностика, устранение отказов и неисправностей, восстановление работоспособности инженерно-технических средств физической защиты

4. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (МДК, ПМ), СТРУКТУРИРОВАННОЕ ПО ТЕМАМ (РАЗДЕЛАМ) С УКАЗАНИЕМ ОТВЕДЕННОГО НА НИХ КОЛИЧЕСТВА АКАДЕМИЧЕСКИХ ЧАСОВ И ВИДОВ УЧЕБНЫХ ЗАНЯТИЙ

Код занятия	Наименование разделов и тем /вид занятия/	Семестр / Курс	Часов	Компетенции	Литература		Примечание
	Раздел 1. Лекционные занятия						
1.1	Цели и задачи физической защиты объектов информатизации.	6/3	2	ОК 01, ОК 02, ОК 03, ОК 04, ОК 05, ОК 06, ОК 07, ОК 08, ОК 09, ОК 10, ОК 11, ПК 3.5	Л1.1, Л1.2, Л2.1, Л2.2, Э1, Э2, Э3		
1.2	Цели и задачи физической защиты объектов информатизации.	6/3	2	ОК 01, ОК 02, ОК 03, ОК 04, ОК 05, ОК 06, ОК 07, ОК 08, ОК 09, ОК 10, ОК 11, ПК 3.5	Л1.1, Л1.2, Л2.1, Л2.2, Э1, Э2, Э3		
1.3	Цели и задачи физической защиты объектов информатизации.	6/3	2	ОК 01, ОК 02, ОК 03, ОК 04, ОК 05, ОК 06, ОК 07, ОК 08, ОК 09, ОК 10, ОК 11, ПК 3.5	Л1.1, Л1.2, Л2.1, Л2.2, Э1, Э2, Э3		

1.4	Цели и задачи физической защиты объектов информатизации.	6/3	2	ОК 01, ОК 02, ОК 03, ОК 04, ОК 05, ОК 06, ОК 07, ОК 08, ОК 09, ОК 10, ОК 11, ПК 3.5	Л1.1, Л1.2, Л2.1, Л2.2, Э1, Э2, Э3		
1.5	Цели и задачи физической защиты объектов информатизации.	6/3	2	ОК 01, ОК 02, ОК 03, ОК 04, ОК 05, ОК 06, ОК 07, ОК 08, ОК 09, ОК 10, ОК 11, ПК 3.5	Л1.1, Л1.2, Л2.1, Л2.2, Э1, Э2, Э3		
1.6	Общие сведения о комплексах инженерно-технических средств физической защиты.	6/3	2	ОК 01, ОК 02, ОК 03, ОК 04, ОК 05, ОК 06, ОК 07, ОК 08, ОК 09, ОК 10, ОК 11, ПК 3.5	Л1.1, Л1.2, Л2.1, Л2.2, Э1, Э2, Э3		
1.7	Общие сведения о комплексах инженерно-технических средств физической защиты.	6/3	2	ОК 01, ОК 02, ОК 03, ОК 04, ОК 05, ОК 06, ОК 07, ОК 08, ОК 09, ОК 10, ОК 11, ПК 3.5	Л1.1, Л1.2, Л2.1, Л2.2, Э1, Э2, Э3		
1.8	Общие сведения о комплексах инженерно-технических средств физической защиты.	6/3	2	ОК 01, ОК 02, ОК 03, ОК 04, ОК 05, ОК 06, ОК 07, ОК 08, ОК 09, ОК 10, ОК 11, ПК 3.5	Л1.1, Л1.2, Л2.1, Л2.2, Э1, Э2, Э3		
1.9	Общие сведения о комплексах инженерно-технических средств физической защиты.	6/3	2	ОК 01, ОК 02, ОК 03, ОК 04, ОК 05, ОК 06, ОК 07, ОК 08, ОК 09, ОК 10, ОК 11, ПК 3.5	Л1.1, Л1.2, Л2.1, Л2.2, Э1, Э2, Э3		
1.10	Общие сведения о комплексах инженерно-технических средств физической защиты.	6/3	2	ОК 01, ОК 02, ОК 03, ОК 04, ОК 05, ОК 06, ОК 07, ОК 08, ОК 09, ОК 10, ОК 11, ПК 3.5	Л1.1, Л1.2, Л2.1, Л2.2, Э1, Э2, Э3		
1.11	Система обнаружения комплекса инженерно-технических средств физической защиты.	6/3	2	ОК 01, ОК 02, ОК 03, ОК 04, ОК 05, ОК 06, ОК 07, ОК 08, ОК 09, ОК 10, ОК 11, ПК 3.5	Л1.1, Л1.2, Л2.1, Л2.2, Э1, Э2, Э3		
1.12	Система обнаружения комплекса инженерно-технических средств физической защиты.	6/3	2	ОК 01, ОК 02, ОК 03, ОК 04, ОК 05, ОК 06, ОК 07, ОК 08, ОК 09, ОК 10, ОК 11, ПК 3.5	Л1.1, Л1.2, Л2.1, Л2.2, Э1, Э2, Э3		
1.13	Система обнаружения комплекса инженерно-технических средств физической защиты.	6/3	2	ОК 01, ОК 02, ОК 03, ОК 04, ОК 05, ОК 06, ОК 07, ОК 08, ОК 09, ОК 10, ОК 11, ПК 3.5	Л1.1, Л1.2, Л2.1, Л2.2, Э1, Э2, Э3		

1.14	Система обнаружения комплекса инженерно-технических средств физической защиты.	6/3	2	ОК 01, ОК 02, ОК 03, ОК 04, ОК 05, ОК 06, ОК 07, ОК 08, ОК 09, ОК 10, ОК 11, ПК 3.5	Л1.1, Л1.2, Л2.1, Л2.2, Э1, Э2, Э3		
1.15	Система обнаружения комплекса инженерно-технических средств физической защиты.	6/3	1	ОК 01, ОК 02, ОК 03, ОК 04, ОК 05, ОК 06, ОК 07, ОК 08, ОК 09, ОК 10, ОК 11, ПК 3.5	Л1.1, Л1.2, Л2.1, Л2.2, Э1, Э2, Э3		
1.16	Система контроля и управления доступом.	7/4	2	ОК 01, ОК 02, ОК 03, ОК 04, ОК 05, ОК 06, ОК 07, ОК 08, ОК 09, ОК 10, ОК 11, ПК 3.5	Л1.1, Л1.2, Л2.1, Л2.2, Э1, Э2, Э3		
1.17	Система контроля и управления доступом.	7/4	2	ОК 01, ОК 02, ОК 03, ОК 04, ОК 05, ОК 06, ОК 07, ОК 08, ОК 09, ОК 10, ОК 11, ПК 3.5	Л1.1, Л1.2, Л2.1, Л2.2, Э1, Э2, Э3		
1.18	Система контроля и управления доступом.	7/4	2	ОК 01, ОК 02, ОК 03, ОК 04, ОК 05, ОК 06, ОК 07, ОК 08, ОК 09, ОК 10, ОК 11, ПК 3.5	Л1.1, Л1.2, Л2.1, Л2.2, Э1, Э2, Э3		
1.19	Система контроля и управления доступом.	7/4	2	ОК 01, ОК 02, ОК 03, ОК 04, ОК 05, ОК 06, ОК 07, ОК 08, ОК 09, ОК 10, ОК 11, ПК 3.5	Л1.1, Л1.2, Л2.1, Л2.2, Э1, Э2, Э3		
1.20	Система контроля и управления доступом.	7/4	2	ОК 01, ОК 02, ОК 03, ОК 04, ОК 05, ОК 06, ОК 07, ОК 08, ОК 09, ОК 10, ОК 11, ПК 3.5	Л1.1, Л1.2, Л2.1, Л2.2, Э1, Э2, Э3		
1.21	Система телевизионного наблюдения.	7/4	2	ОК 01, ОК 02, ОК 03, ОК 04, ОК 05, ОК 06, ОК 07, ОК 08, ОК 09, ОК 10, ОК 11, ПК 3.5	Л1.1, Л1.2, Л2.1, Л2.2, Э1, Э2, Э3		
1.22	Система телевизионного наблюдения.	7/4	2	ОК 01, ОК 02, ОК 03, ОК 04, ОК 05, ОК 06, ОК 07, ОК 08, ОК 09, ОК 10, ОК 11, ПК 3.5	Л1.1, Л1.2, Л2.1, Л2.2, Э1, Э2, Э3		
1.23	Система телевизионного наблюдения.	7/4	2	ОК 01, ОК 02, ОК 03, ОК 04, ОК 05, ОК 06, ОК 07, ОК 08, ОК 09, ОК 10, ОК 11, ПК 3.5	Л1.1, Л1.2, Л2.1, Л2.2, Э1, Э2, Э3		

1.24	Система телевизионного наблюдения.	7/4	2	ОК 01, ОК 02, ОК 03, ОК 04, ОК 05, ОК 06, ОК 07, ОК 08, ОК 09, ОК 10, ОК 11, ПК 3.5	Л1.1, Л1.2, Л2.1, Л2.2, Э1, Э2, Э3		
1.25	Система сбора, обработки, отображения и документирования информации.	8/4	2	ОК 01, ОК 02, ОК 03, ОК 04, ОК 05, ОК 06, ОК 07, ОК 08, ОК 09, ОК 10, ОК 11, ПК 3.5	Л1.1, Л1.2, Л2.1, Л2.2, Э1, Э2, Э3		
1.26	Система сбора, обработки, отображения и документирования информации.	8/4	2	ОК 01, ОК 02, ОК 03, ОК 04, ОК 05, ОК 06, ОК 07, ОК 08, ОК 09, ОК 10, ОК 11, ПК 3.5	Л1.1, Л1.2, Л2.1, Л2.2, Э1, Э2, Э3		
1.27	Система сбора, обработки, отображения и документирования информации.	8/4	2	ОК 01, ОК 02, ОК 03, ОК 04, ОК 05, ОК 06, ОК 07, ОК 08, ОК 09, ОК 10, ОК 11, ПК 3.5	Л1.1, Л1.2, Л2.1, Л2.2, Э1, Э2, Э3		
1.28	Система сбора, обработки, отображения и документирования информации.	8/4	2	ОК 01, ОК 02, ОК 03, ОК 04, ОК 05, ОК 06, ОК 07, ОК 08, ОК 09, ОК 10, ОК 11, ПК 3.5	Л1.1, Л1.2, Л2.1, Л2.2, Э1, Э2, Э3		
1.29	Система сбора, обработки, отображения и документирования информации.	8/4	2	ОК 01, ОК 02, ОК 03, ОК 04, ОК 05, ОК 06, ОК 07, ОК 08, ОК 09, ОК 10, ОК 11, ПК 3.5	Л1.1, Л1.2, Л2.1, Л2.2, Э1, Э2, Э3		
1.30	Система сбора, обработки, отображения и документирования информации.	8/4	2	ОК 01, ОК 02, ОК 03, ОК 04, ОК 05, ОК 06, ОК 07, ОК 08, ОК 09, ОК 10, ОК 11, ПК 3.5	Л1.1, Л1.2, Л2.1, Л2.2, Э1, Э2, Э3		
1.31	Система воздействия.	8/4	2	ОК 01, ОК 02, ОК 03, ОК 04, ОК 05, ОК 06, ОК 07, ОК 08, ОК 09, ОК 10, ОК 11, ПК 3.5	Л1.1, Л1.2, Л2.1, Л2.2, Э1, Э2, Э3		
1.32	Система воздействия.	8/4	2	ОК 01, ОК 02, ОК 03, ОК 04, ОК 05, ОК 06, ОК 07, ОК 08, ОК 09, ОК 10, ОК 11, ПК 3.5	Л1.1, Л1.2, Л2.1, Л2.2, Э1, Э2, Э3		
1.33	Система воздействия.	8/4	2	ОК 01, ОК 02, ОК 03, ОК 04, ОК 05, ОК 06, ОК 07, ОК 08, ОК 09, ОК 10, ОК 11, ПК 3.5	Л1.1, Л1.2, Л2.1, Л2.2, Э1, Э2, Э3		

1.34	Система воздействия.	8/4	2	ОК 01, ОК 02, ОК 03, ОК 04, ОК 05, ОК 06, ОК 07, ОК 08, ОК 09, ОК 10, ОК 11, ПК 3.5	Л1.1, Л1.2, Л2.1, Л2.2, Э1, Э2, Э3		
1.35	Система воздействия.	8/4	2	ОК 01, ОК 02, ОК 03, ОК 04, ОК 05, ОК 06, ОК 07, ОК 08, ОК 09, ОК 10, ОК 11, ПК 3.5	Л1.1, Л1.2, Л2.1, Л2.2, Э1, Э2, Э3		
1.36	Система воздействия.	8/4	2	ОК 01, ОК 02, ОК 03, ОК 04, ОК 05, ОК 06, ОК 07, ОК 08, ОК 09, ОК 10, ОК 11, ПК 3.5	Л1.1, Л1.2, Л2.1, Л2.2, Э1, Э2, Э3		
1.37	Применение инженерно-технических средств физической защиты.	8/4	2	ОК 01, ОК 02, ОК 03, ОК 04, ОК 05, ОК 06, ОК 07, ОК 08, ОК 09, ОК 10, ОК 11, ПК 3.5	Л1.1, Л1.2, Л2.1, Л2.2, Э1, Э2, Э3		
1.38	Применение инженерно-технических средств физической защиты.	8/4	2	ОК 01, ОК 02, ОК 03, ОК 04, ОК 05, ОК 06, ОК 07, ОК 08, ОК 09, ОК 10, ОК 11, ПК 3.5	Л1.1, Л1.2, Л2.1, Л2.2, Э1, Э2, Э3		
1.39	Применение инженерно-технических средств физической защиты.	8/4	2	ОК 01, ОК 02, ОК 03, ОК 04, ОК 05, ОК 06, ОК 07, ОК 08, ОК 09, ОК 10, ОК 11, ПК 3.5	Л1.1, Л1.2, Л2.1, Л2.2, Э1, Э2, Э3		
1.40	Применение инженерно-технических средств физической защиты.	8/4	2	ОК 01, ОК 02, ОК 03, ОК 04, ОК 05, ОК 06, ОК 07, ОК 08, ОК 09, ОК 10, ОК 11, ПК 3.5	Л1.1, Л1.2, Л2.1, Л2.2, Э1, Э2, Э3		
1.41	Применение инженерно-технических средств физической защиты.	8/4	2	ОК 01, ОК 02, ОК 03, ОК 04, ОК 05, ОК 06, ОК 07, ОК 08, ОК 09, ОК 10, ОК 11, ПК 3.5	Л1.1, Л1.2, Л2.1, Л2.2, Э1, Э2, Э3		
1.42	Применение инженерно-технических средств физической защиты.	8/4	2	ОК 01, ОК 02, ОК 03, ОК 04, ОК 05, ОК 06, ОК 07, ОК 08, ОК 09, ОК 10, ОК 11, ПК 3.5	Л1.1, Л1.2, Л2.1, Л2.2, Э1, Э2, Э3		
1.43	Эксплуатация инженерно-технических средств физической защиты.	8/4	2	ОК 01, ОК 02, ОК 03, ОК 04, ОК 05, ОК 06, ОК 07, ОК 08, ОК 09, ОК 10, ОК 11, ПК 3.5	Л1.1, Л1.2, Л2.1, Л2.2, Э1, Э2, Э3		

1.44	Эксплуатация инженерно-технических средств физической защиты.	8/4	2	ОК 01, ОК 02, ОК 03, ОК 04, ОК 05, ОК 06, ОК 07, ОК 08, ОК 09, ОК 10, ОК 11, ПК 3.5	Л1.1, Л1.2, Л2.1, Л2.2, Э1, Э2, Э3		
1.45	Эксплуатация инженерно-технических средств физической защиты.	8/4	2	ОК 01, ОК 02, ОК 03, ОК 04, ОК 05, ОК 06, ОК 07, ОК 08, ОК 09, ОК 10, ОК 11, ПК 3.5	Л1.1, Л1.2, Л2.1, Л2.2, Э1, Э2, Э3		
1.46	Эксплуатация инженерно-технических средств физической защиты.	8/4	2	ОК 01, ОК 02, ОК 03, ОК 04, ОК 05, ОК 06, ОК 07, ОК 08, ОК 09, ОК 10, ОК 11, ПК 3.5	Л1.1, Л1.2, Л2.1, Л2.2, Э1, Э2, Э3		
1.47	Эксплуатация инженерно-технических средств физической защиты.	8/4	2	ОК 01, ОК 02, ОК 03, ОК 04, ОК 05, ОК 06, ОК 07, ОК 08, ОК 09, ОК 10, ОК 11, ПК 3.5	Л1.1, Л1.2, Л2.1, Л2.2, Э1, Э2, Э3		
	Раздел 2. Практические занятия						
2.1	Модель нарушителя и возможные пути и способы его проникновения на охраняемый объект.	6/3	2	ОК 01, ОК 02, ОК 03, ОК 04, ОК 05, ОК 06, ОК 07, ОК 08, ОК 09, ОК 10, ОК 11, ПК 3.5	Л1.1, Л1.2, Л2.1, Л2.2, Э1, Э2, Э3		
2.2	Модель нарушителя и возможные пути и способы его проникновения на охраняемый объект	6/3	2	ОК 01, ОК 02, ОК 03, ОК 04, ОК 05, ОК 06, ОК 07, ОК 08, ОК 09, ОК 10, ОК 11, ПК 3.5	Л1.1, Л1.2, Л2.1, Л2.2, Э1, Э2, Э3		
2.3	Построение интегрированных систем охраны.	6/3	2	ОК 01, ОК 02, ОК 03, ОК 04, ОК 05, ОК 06, ОК 07, ОК 08, ОК 09, ОК 10, ОК 11, ПК 3.5	Л1.1, Л1.2, Л2.1, Л2.2, Э1, Э2, Э3		
2.4	Построение интегрированных систем охраны.	6/3	2	ОК 01, ОК 02, ОК 03, ОК 04, ОК 05, ОК 06, ОК 07, ОК 08, ОК 09, ОК 10, ОК 11, ПК 3.5	Л1.1, Л1.2, Л2.1, Л2.2, Э1, Э2, Э3		
2.5	Построение интегрированных систем охраны.	6/3	2	ОК 01, ОК 02, ОК 03, ОК 04, ОК 05, ОК 06, ОК 07, ОК 08, ОК 09, ОК 10, ОК 11, ПК 3.5	Л1.1, Л1.2, Л2.1, Л2.2, Э1, Э2, Э3		

2.6	Построение систем обеспечения безопасности объекта.	7/4	2	ОК 01, ОК 02, ОК 03, ОК 04, ОК 05, ОК 06, ОК 07, ОК 08, ОК 09, ОК 10, ОК 11, ПК 3.5	Л1.1, Л1.2, Л2.1, Л2.2, Э1, Э2, Э3		
2.7	Построение систем обеспечения безопасности объекта.	7/4	2	ОК 01, ОК 02, ОК 03, ОК 04, ОК 05, ОК 06, ОК 07, ОК 08, ОК 09, ОК 10, ОК 11, ПК 3.5	Л1.1, Л1.2, Л2.1, Л2.2, Э1, Э2, Э3		
2.8	Построение системы охранной сигнализации.	8/4	2	ОК 01, ОК 02, ОК 03, ОК 04, ОК 05, ОК 06, ОК 07, ОК 08, ОК 09, ОК 10, ОК 11, ПК 3.5	Л1.1, Л1.2, Л2.1, Л2.2, Э1, Э2, Э3		
2.9	Построение системы охранной сигнализации.	8/4	2	ОК 01, ОК 02, ОК 03, ОК 04, ОК 05, ОК 06, ОК 07, ОК 08, ОК 09, ОК 10, ОК 11, ПК 3.5	Л1.1, Л1.2, Л2.1, Л2.2, Э1, Э2, Э3		
2.10	Построение системы охранной сигнализации.	8/4	2	ОК 01, ОК 02, ОК 03, ОК 04, ОК 05, ОК 06, ОК 07, ОК 08, ОК 09, ОК 10, ОК 11, ПК 3.5	Л1.1, Л1.2, Л2.1, Л2.2, Э1, Э2, Э3		
2.11	Устройство, работа и применение аппаратных средств аутентификации пользователя	8/4	2	ОК 01, ОК 02, ОК 03, ОК 04, ОК 05, ОК 06, ОК 07, ОК 08, ОК 09, ОК 10, ОК 11, ПК 3.5	Л1.1, Л1.2, Л2.1, Л2.2, Э1, Э2, Э3		
2.12	Устройство, работа и применение аппаратных средств аутентификации пользователя	8/4	2	ОК 01, ОК 02, ОК 03, ОК 04, ОК 05, ОК 06, ОК 07, ОК 08, ОК 09, ОК 10, ОК 11, ПК 3.5	Л1.1, Л1.2, Л2.1, Л2.2, Э1, Э2, Э3		
2.13	Устройство, работы и применение средств контроля доступа	8/4	2	ОК 01, ОК 02, ОК 03, ОК 04, ОК 05, ОК 06, ОК 07, ОК 08, ОК 09, ОК 10, ОК 11, ПК 3.5	Л1.1, Л1.2, Л2.1, Л2.2, Э1, Э2, Э3		
2.14	Устройство, работы и применение средств контроля доступа	8/4	2	ОК 01, ОК 02, ОК 03, ОК 04, ОК 05, ОК 06, ОК 07, ОК 08, ОК 09, ОК 10, ОК 11, ПК 3.5	Л1.1, Л1.2, Л2.1, Л2.2, Э1, Э2, Э3		
2.15	Устройство, работы и применение средств контроля доступа	8/4	2	ОК 01, ОК 02, ОК 03, ОК 04, ОК 05, ОК 06, ОК 07, ОК 08, ОК 09, ОК 10, ОК 11, ПК 3.5	Л1.1, Л1.2, Л2.1, Л2.2, Э1, Э2, Э3		

2.16	Устройство, работа и применение средств видеонаблюдения.	8/4	2	ОК 01, ОК 02, ОК 03, ОК 04, ОК 05, ОК 06, ОК 07, ОК 08, ОК 09, ОК 10, ОК 11, ПК 3.5	Л1.1, Л1.2, Л2.1, Л2.2, Э1, Э2, Э3		
2.17	Устройство, работа и применение средств видеонаблюдения.	8/4	2	ОК 01, ОК 02, ОК 03, ОК 04, ОК 05, ОК 06, ОК 07, ОК 08, ОК 09, ОК 10, ОК 11, ПК 3.5	Л1.1, Л1.2, Л2.1, Л2.2, Э1, Э2, Э3		
2.18	Устройство, работа и применение средств видеонаблюдения.	8/4	2	ОК 01, ОК 02, ОК 03, ОК 04, ОК 05, ОК 06, ОК 07, ОК 08, ОК 09, ОК 10, ОК 11, ПК 3.5	Л1.1, Л1.2, Л2.1, Л2.2, Э1, Э2, Э3		
	Раздел 3. Лабораторные занятия						
3.1	Монтаж датчиков пожарной и охранной сигнализации	6/3	2	ОК 01, ОК 02, ОК 03, ОК 04, ОК 05, ОК 06, ОК 07, ОК 08, ОК 09, ОК 10, ОК 11, ПК 3.5	Л1.1, Л1.2, Л2.1, Л2.2, Л3.1, Э1, Э2, Э3		
3.2	Монтаж датчиков пожарной и охранной сигнализации	6/3	2	ОК 01, ОК 02, ОК 03, ОК 04, ОК 05, ОК 06, ОК 07, ОК 08, ОК 09, ОК 10, ОК 11, ПК 3.5	Л1.1, Л1.2, Л2.1, Л2.2, Л3.1, Э1, Э2, Э3		
3.3	Монтаж датчиков пожарной и охранной сигнализации	6/3	2	ОК 01, ОК 02, ОК 03, ОК 04, ОК 05, ОК 06, ОК 07, ОК 08, ОК 09, ОК 10, ОК 11, ПК 3.5	Л1.1, Л1.2, Л2.1, Л2.2, Л3.1, Э1, Э2, Э3		
3.4	Объектовые и периметровые средства обнаружения.	7/4	2	ОК 01, ОК 02, ОК 03, ОК 04, ОК 05, ОК 06, ОК 07, ОК 08, ОК 09, ОК 10, ОК 11, ПК 3.5	Л1.1, Л1.2, Л2.1, Л2.2, Л3.1, Э1, Э2, Э3		
3.5	Объектовые и периметровые средства обнаружения.	7/4	2	ОК 01, ОК 02, ОК 03, ОК 04, ОК 05, ОК 06, ОК 07, ОК 08, ОК 09, ОК 10, ОК 11, ПК 3.5	Л1.1, Л1.2, Л2.1, Л2.2, Л3.1, Э1, Э2, Э3		
3.6	Объектовые и периметровые средства обнаружения.	7/4	2	ОК 01, ОК 02, ОК 03, ОК 04, ОК 05, ОК 06, ОК 07, ОК 08, ОК 09, ОК 10, ОК 11, ПК 3.5	Л1.1, Л1.2, Л2.1, Л2.2, Л3.1, Э1, Э2, Э3		

3.7	Управление системой телевизионного наблюдения с автоматизированного рабочего места.	8/4	2	ОК 01, ОК 02, ОК 03, ОК 04, ОК 05, ОК 06, ОК 07, ОК 08, ОК 09, ОК 10, ОК 11, ПК 3.5	Л1.1, Л1.2, Л2.1, Л2.2, Л3.1, Э1, Э2, Э3		
3.8	Управление системой телевизионного наблюдения с автоматизированного рабочего места.	8/4	2	ОК 01, ОК 02, ОК 03, ОК 04, ОК 05, ОК 06, ОК 07, ОК 08, ОК 09, ОК 10, ОК 11, ПК 3.5	Л1.1, Л1.2, Л2.1, Л2.2, Л3.1, Э1, Э2, Э3		
3.9	Установка и настройка периметровых и объектовых технических средств обнаружения, периферийного оборудования системы телевизионного наблюдения.	8/4	2	ОК 01, ОК 02, ОК 03, ОК 04, ОК 05, ОК 06, ОК 07, ОК 08, ОК 09, ОК 10, ОК 11, ПК 3.5	Л1.1, Л1.2, Л2.1, Л2.2, Л3.1, Э1, Э2, Э3		
3.10	Установка и настройка периметровых и объектовых технических средств обнаружения, периферийного оборудования системы телевизионного наблюдения.	8/4	2	ОК 01, ОК 02, ОК 03, ОК 04, ОК 05, ОК 06, ОК 07, ОК 08, ОК 09, ОК 10, ОК 11, ПК 3.5	Л1.1, Л1.2, Л2.1, Л2.2, Л3.1, Э1, Э2, Э3		
3.11	Установка и настройка периметровых и объектовых технических средств обнаружения, периферийного оборудования системы телевизионного наблюдения.	8/4	2	ОК 01, ОК 02, ОК 03, ОК 04, ОК 05, ОК 06, ОК 07, ОК 08, ОК 09, ОК 10, ОК 11, ПК 3.5	Л1.1, Л1.2, Л2.1, Л2.2, Л3.1, Э1, Э2, Э3		
3.12	Диагностика, устранение отказов и восстановление работоспособности технических средств физической защиты.	8/4	2	ОК 01, ОК 02, ОК 03, ОК 04, ОК 05, ОК 06, ОК 07, ОК 08, ОК 09, ОК 10, ОК 11, ПК 3.5	Л1.1, Л1.2, Л2.1, Л2.2, Л3.1, Э1, Э2, Э3		
3.13	Диагностика, устранение отказов и восстановление работоспособности технических средств физической защиты.	8/4	2	ОК 01, ОК 02, ОК 03, ОК 04, ОК 05, ОК 06, ОК 07, ОК 08, ОК 09, ОК 10, ОК 11, ПК 3.5	Л1.1, Л1.2, Л2.1, Л2.2, Л3.1, Э1, Э2, Э3		
3.14	Диагностика, устранение отказов и восстановление работоспособности технических средств физической защиты.	8/4	2	ОК 01, ОК 02, ОК 03, ОК 04, ОК 05, ОК 06, ОК 07, ОК 08, ОК 09, ОК 10, ОК 11, ПК 3.5	Л1.1, Л1.2, Л2.1, Л2.2, Л3.1, Э1, Э2, Э3		
3.15	Организация ремонта технических средств физической защиты.	8/4	2	ОК 01, ОК 02, ОК 03, ОК 04, ОК 05, ОК 06, ОК 07, ОК 08, ОК 09, ОК 10, ОК 11, ПК 3.5	Л1.1, Л1.2, Л2.1, Л2.2, Л3.1, Э1, Э2, Э3		
	Организация ремонта технических средств физической защиты.	8/4	2	ОК 01, ОК 02, ОК 03, ОК 04, ОК 05, ОК 06, ОК 07, ОК 08, ОК 09, ОК 10, ОК 11, ПК 3.5	Л1.1, Л1.2, Л2.1, Л2.2, Л3.1, Э1, Э2, Э3		

	Организация ремонта технических средств физической защиты.	8/4	2	ОК 01, ОК 02, ОК 03, ОК 04, ОК 05, ОК 06, ОК 07, ОК 08, ОК 09, ОК 10, ОК 11, ПК 3.5	Л1.1, Л1.2, Л2.1, Л2.2, Л3.1, Э1, Э2, Э3		
	Раздел 4. Курсовое проектирование.						
4.1	Выполнение курсового проекта по заданной теме.	8/4	30	ОК 01, ОК 02, ОК 03, ОК 04, ОК 05, ОК 06, ОК 07, ОК 08, ОК 09, ОК 10, ОК 11, ПК 3.5	Л1.1, Л1.2, Л2.1, Л2.2, Л3.1, Э1, Э2, Э3		
	Раздел 5. Контроль						
5.1	Другие формы промежуточной аттестации	6/3		ОК 01, ОК 02, ОК 03, ОК 04, ОК 05, ОК 06, ОК 07, ОК 08, ОК 09, ОК 10, ОК 11, ПК 3.5	Л1.1, Л1.2, Л2.1, Л2.2, Л3.1, Э1, Э2, Э3		
5.2	Другие формы промежуточной аттестации	7/4		ОК 01, ОК 02, ОК 03, ОК 04, ОК 05, ОК 06, ОК 07, ОК 08, ОК 09, ОК 10, ОК 11, ПК 3.5	Л1.1, Л1.2, Л2.1, Л2.2, Л3.1, Э1, Э2, Э3		
5.3	Курсовой проект	8/4		ОК 01, ОК 02, ОК 03, ОК 04, ОК 05, ОК 06, ОК 07, ОК 08, ОК 09, ОК 10, ОК 11, ПК 3.5	Л1.1, Л1.2, Л2.1, Л2.2, Л3.1, Э1, Э2, Э3		
5.4	Экзамен	8/4	8	ОК 01, ОК 02, ОК 03, ОК 04, ОК 05, ОК 06, ОК 07, ОК 08, ОК 09, ОК 10, ОК 11, ПК 3.5	Л1.1, Л1.2, Л2.1, Л2.2, Л3.1, Э1, Э2, Э3		

5. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ ПРОВЕДЕНИЯ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

Размещен в приложении

6. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МДК, ПМ)

6.1. Рекомендуемая литература

6.1.1. Перечень основной литературы, необходимой для освоения дисциплины (МДК, ПМ)

	Авторы, составители	Заглавие	Издательство, год
Л1.1	Сердюк, В.А	. Организация и технологии защиты информации: обнаружение и предотвращение информационных атак в автоматизированных системах предприятий	Москва : Издательский дом Высшей школы экономики, 2015.
Л1.2	Сагдеев, К.М.	Физические основы защиты информации	Ставрополь : СКФУ, 2015

6.1.2. Перечень дополнительной литературы, необходимой для освоения дисциплины (МДК, ПМ)

	Авторы, составители	Заглавие	Издательство, год
Л2.1	Гуляев, В.П.	Анализ демаскирующих признаков объектов информатизации и технических каналов утечки информации	Екатеринбург : Издательство Уральского университета, 2014

Л2.2	Семенихина, Д.В.	Теоретические основы радиоэлектронной борьбы. Радиоэлектронная разведка и радиоэлектронное противодействие.	Ростов-на-Дону : Издательство Южного федерального университета, 2015.

6.1.3. Перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине (МДК, ПМ)

	Авторы, составители	Заглавие	Издательство, год
Л3.1	Петров, В.В.	Комплексные системы безопасности современного города. Учебное пособие	Таганрог : Издательство Южного федерального университета, 2017

6.2. Перечень ресурсов информационно-телекоммуникационной сети "Интернет", необходимых для освоения дисциплины (МДК, ПМ)

Э1	Научная электронная библиотека eLIBRARY.RU	elibrary.ru
Э2	Электронно-библиотечная система «Книгафонд»	http://knigafund.ru/
Э3	Электронный каталог НТБ	catalog.lib.tpu.ru

6.3 Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине (МДК, ПМ), включая перечень программного обеспечения и информационных справочных систем (при необходимости)

6.3.1 Перечень программного обеспечения

Win XP, 7

- DreamSpark Premium Electronic Software Delivery (3 years) Renewal 1203984220

- Kaspersky Endpoint Security 10 для Windows - 356¬160615-113525¬730¬94

- Права на ПО NetPolice School для Traffic Inspector Unlimited

- Права на ПО Traffic Inspector Anti-Virus powered by Kaspersky Special

-Traffic Inspector (Контракт 524 ДВГУПС от 15.07.2019)

Microsoft Windows Professional 10 Russian 1 License 5 шт,

базовый пакет для сертифицированной версии ОС Windows 8.1 Профессиональная/Pro для использования на 1 АРМ

Microsoft Office Professional Plus 2019 Russian OLP 1 License 18 шт,

программа контроля сертифицированной версии ОС Windows 8.1 Профессиональная 5 шт,

Microsoft Windows Server CAL 2019 Russian OLP 1 License User CAL 22 шт,

Базовый пакет для сертифицированной версии ОС Microsoft Windows Server Datacenter 2012 R2 для использования на 2 процессора 1 шт,

ОС Astra Linux Special Edition (Box версия с установочным комплектом) 5 шт. - Контракт № 1272401815819000032 4/157 ДВГУПС от 15.03.2019 г.

RedCheck Professional на 1 IP-адрес на 1 год 10 шт, КриптоПро CSP версии 4.0 5 шт,

Dallas Lock 8.0-C с модулями «Межсетевой экран» и «Система обнаружения и предотвращения вторжений». 5 шт,

Secret Net Studio 8 в редакции «Постоянная защита» (бессрочная) с модулями защиты от НСД, контроля устройств (СКН) и межсетевого экранирования (МЭ) 6 шт,

Антивирус Kaspersky Endpoint Security бизнеса – Расширенный Russian Edition. 1500-2499 Node 1 year Educational Renewal License 20шт. - Контракт № 1272401815819000058 4/290 ДВГУПС от 08.05.2019 г.

6.3.2 Перечень информационных справочных систем

1. Профессиональная база данных, информационно-справочная система Гарант - http://www.garant.ru

2. Профессиональная база данных, информационно-справочная система КонсультантПлюс - http://www.consultant.ru

7. ОПИСАНИЕ МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЙ БАЗЫ, НЕОБХОДИМОЙ ДЛЯ ОСУЩЕСТВЛЕНИЯ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА ПО ДИСЦИПЛИНЕ (МОДУЛЮ)

Аудитория	Назначение	Оснащение
320	Учебная аудитория для проведения теоретических занятий (уроков). Лекционная аудитория.	Комплект мебели, проектор, персональный компьютер, комплект презентаций. - Win XP, 7 - DreamSpark Premium Electronic Software Delivery (3 years) Renewal 1203984220 - Kaspersky Endpoint Security 10 для Windows - 356¬160615-113525¬730¬94 - Права на ПО NetPolice School для Traffic Inspector Unlimited - Права на ПО Traffic Inspector Anti-Virus powered by Kaspersky Special -Traffic Inspector (Контракт 524 ДВГУПС от 15.07.2019)

324	Учебная аудитория для проведения теоретических занятий (уроков), практических занятий, лабораторных работ, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации. Лаборатория программных и программно-аппаратных средств защиты информации. Лаборатория "Защита информации от утечки за счет несанкционированного доступа в локальных вычислительных сетях".	Комплект учебной мебели, экран, автоматизированное рабочее место IZEC «Студент» в сборе 16 шт, Автоматизированное рабочее место IZEC «Преподаватель» в сборе 1 шт, автоматизированное рабочее место IZEC «Диспетчер АСУ ТП» в сборе 1 шт, сервер IZEC на платформе WOLF PASS 2U в сборе 1 шт, сервер IZEC на платформе SILVER PASS 1U в сборе 1 шт, Ноутбук HP 250 G6 15.6 1 шт, МФУ XEROX WC 6515DNI 1 шт, электронный идентификатор ruToken S 64 КБ 20 шт, электронный идентификатор JaCarta-2 PRO/ГОСТ 5 шт, средство доверенной загрузки Dallas Lock PCI-E Full Size 5 шт, средство доверенной загрузки "Соболь" версия 4 PCI-E 5 шт, рупор измерительный широкополосный П6-124 зав. № 150718305 в комплекте с диэлектрическим штативом, кабель КИ-18-5м-SMAM-SMAM, индуктор магнитный ИРМ-500М Зав. № 015, пробник напряжения Я6-122/1М Зав. № 024, токосъемник измерительный ТК-400М Зав. № 87, антенна измерительная дипольная активная АИ5-0 Зав. № 1742, мультимедийный проектор. Microsoft Windows Professional 10 Russian 1 License 5 шт, базовый пакет для сертифицированной версии ОС Windows 8.1 Профессиональная/Pro для использования на 1 АРМ 5шт, Microsoft Office Professional Plus 2019 Russian OLP 1 License 18 шт, программа контроля сертифицированной версии ОС Windows 8.1 Профессиональная 5 шт, Microsoft Windows Server CAL 2019 Russian OLP 1 License User CAL 22 шт, Базовый пакет для сертифицированной версии ОС Microsoft Windows Server Datacenter 2012 R2 для использования на 2 процессора 1 шт, ОС Astra Linux Special Edition (Box версия с установочным комплектом) 5 шт. - Контракт № 1272401815819000324/157 ДВГУПС от 15.03.2019 г. RedCheck Professional на 1 IP-адрес на 1 год 10 шт, КриптоПро CSP версии 4.0 5 шт, Dallas Lock 8.0-C с модулями «Межсетевой экран» и «Система обнаружения и предотвращения вторжений». 5 шт, Secret Net Studio 8 в редакции «Постоянная защита» (бессрочная) с модулями защиты от НСД, контроля устройств (СКН) и межсетевого экранирования (МЭ) 6 шт, Антивирус Kaspersky Endpoint Security бизнеса – Расширенный Russian Edition. 1500-2499 Node 1 year Educational Renewal License 20шт. - Контракт № 1272401815819000584/290 ДВГУПС от 08.05.2019 г.

8. МЕТОДИЧЕСКИЕ МАТЕРИАЛЫ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ (МДК, ПМ)

В процессе изучения дисциплины обучающиеся посещают лекции (уроки), практические и лабораторные занятия. На всех этапах обучения по МДК осуществляется контроль знаний.

Подготовка к лекциям (урокам), практическим и лабораторным занятиям включает изучение конспекта лекций, учебных пособий, основной и дополнительной литературы, законодательных и нормативных источников.

Лекция (урок). Работа на лекции является очень важным видом деятельности обучающихся для изучения дисциплины , т.к. лектор ориентирует обучающихся в учебном материале. Краткие записи лекций (конспектирование) помогает усвоить материал. Написание конспекта лекций: кратко, схематично, последовательно фиксировать основные положения, выводы, формулировки, обобщения; помечать важные мысли, выделять ключевые слова, термины.

Практические и лабораторные занятия. Обучающиеся самостоятельно под руководством преподавателя выполняют задания по темам курса. Обучающиеся овладевают навыками, необходимыми для осуществления трудовой функции по профессии.

Курсовой проект. Цель курсового проекта – закрепление знаний и практических навыков, которые получены обучающимся при изучении дисциплины.. Обучающиеся выполняют курсовой проект под руководством преподавателя, выполненный проект сдается для проверки. Проект допускается к защите, и задача студента – защитить ее положительно. Неудовлетворительно выполненная работа подлежит переработке в соответствии с замечаниями преподавателя, содержащимися в рецензии. Защита курсового проекта - это специально организованная беседа преподавателя с обучающимся по разделам и рассчитанное на выяснение объема знаний обучающихся по определенному вопросу, теме, проблеме и т.п. Темы курсовых проектов приведены в приложении 1.

ОСНОВНЫЕ ПРАВИЛА ОФОРМЛЕНИЯ КУРСОВОГО ПРОЕКТА

Схемы, графики также нумеруются арабскими цифрами в пределах раздела и обозначаются термином «Рисунок», являющимся первым словом в подрисуночной подписи, которая приводится ниже иллюстрации шрифтом на 2 пт меньше основного.

Приводимые в тексте цитаты должны соответствовать оригиналу и иметь на него ссылку, которую оформляют в квадратных скобках номером источника, согласно списку использованной литературы. Затем ставится запятая и номер страницы (например, [5, с. 124]. Также оформляется ссылка на реферируемый источник, только без указания страниц.

Список используемых источников приводится в следующей последовательности: Законы РФ, Указы Президента, Постановления Правительства, Положения, другие нормативные акты, далее размещаются все остальные источники в алфавитном порядке. Текст отчета оформляется на листах стандартного формата (297×210), заполненных с одной стороны, размер полей: левое – 30 мм, правое – 10 мм, верхнее и нижнее – 20 мм; шрифт Times New Roman 14, обычный; выравнивание по ширине; абзацный отступ 15 мм; межстрочный интервал 1,5; автоматический перенос слов. Первым листом текста является титульный лист (номер не ставится), вторым – содержание с указанием номеров страниц частей работы. Страницы нумеруются арабскими цифрами, которые располагаются в центре страницы.

Разделы и подразделы должны иметь нумерацию и обозначаются арабскими цифрами. Номера подразделов устанавливаются в рамках раздела и имеют двухзначный номер, цифры которого разделяются точкой (например, первый подраздел второго раздела будет иметь номер 2.1).

Структурные части проекта (содержание, введение, заключение, список использованных источников) не нумеруются, а их название размещается по центру страницы. Приложения к отчету, упоминание о них с указанием наименования отражается в содержании после списка использованных источников, они обозначаются заглавными буквами (А, Б и т.д., кроме букв Е, З, Й, О, Ч, Ь Ы, Ъ). Например: «Приложение А. Системы охраны участка».

Каждый раздел проекта необходимо оформлять с новой страницы, перед текстом с абзацного отступа пишется название раздела, затем первого подраздела обычным шрифтом. Эти названия не подчеркиваются, полужирный шрифт и курсив не используются. Размещение подразделов следует друг за другом.

Таблицы, рисунки приводятся по тексту, после первого упоминания о них, таблицы нумеруются арабскими цифрами в пределах раздела и располагаются с абзаца (слева), затем в одну строку после слова «Таблица» и знака «-» пишется ее заголовок. Размер текста таблицы – 12 кегль.

Допускается перенос таблицы на следующую страницу, но при этом ее «шапка» без текста при переносе не должна оставаться на предыдущей странице. На новой странице над продолжающейся таблицей пишется нумерационный заголовок «Продолжение таблицы 3.1», если она не закончена, или «Окончание таблицы 3.1», если закончена, с выравниванием по левому краю. Название таблицы не повторяется, но повторяется шапка таблицы (заголовки и подзаголовки столбцов).

Схемы, графики также нумеруются арабскими цифрами в пределах раздела и обозначаются термином «Рисунок», являющимся первым словом в подрисуночной подписи, которая приводится ниже иллюстрации шрифтом на 2 пт меньше основного.

Приводимые в тексте цитаты должны соответствовать оригиналу и иметь на него ссылку, которую оформляют в квадратных скобках номером источника, согласно списку использованной литературы. Затем ставится запятая и номер страницы (например, [5, с. 124]. Также оформляется ссылка на реферируемый источник, только без указания страниц.

Список используемых источников приводится в следующей последовательности: Законы РФ, Указы Президента, Постановления Правительства, другие нормативные акты, далее размещаются все остальные источники в алфавитном порядке

Приложение 1

Оценочные материалы при формировании рабочей программы
ПМ.03 Защита информации техническими средствами

МДК.03.01 Техническая защита информации

1. Описание показателей, критериев и шкал оценивания компетенций.

1.1. Показатели и критерии оценивания компетенций ОК 01, ОК 02, ОК 03, ОК 04, ОК 05, ОК 06, ОК 07, ОК 08, ОК 09, ОК10, ОК11, ПК 3.1, ПК 3.2, ПК 3.3, ПК 3.4

Объект оценки	Уровни сформированности компетенций	Критерий оценивания результатов обучения
Обучающийся	Низкий уровень Пороговый уровень Повышенный уровень Высокий уровень	Уровень результатов обучения **не ниже порогового**

1.2. Шкалы оценивания компетенций ОК 01, ОК 02, ОК 03, ОК 04, ОК 05, ОК 06, ОК 07, ОК 08, ОК 09, ОК10, ОК11, ПК 3.1, ПК 3.2, ПК 3.3, ПК 3.4, при сдаче других форм промежуточной аттестации (устного опроса) и дифференцированного зачета

Достигнутый уровень результата обучения	Характеристика уровня сформированности компетенций	Шкала оценивания
		Устный опрос (дифференцированный зачет)
Низкий уровень	Обучающийся: -обнаружил пробелы в знаниях основного учебно-программного материала; -допустил принципиальные ошибки в выполнении заданий, предусмотренных программой; -не может продолжить обучение или приступить к профессиональной деятельности по окончании программы без дополнительных занятий по соответствующей дисциплине.	Неудовлетворительно
Пороговый уровень	Обучающийся: -обнаружил знание основного учебно-программного материала в объёме, необходимом для дальнейшей учебной и предстоящей профессиональной деятельности; -справляется с выполнением заданий, предусмотренных программой; -знаком с основной литературой, рекомендованной рабочей программой дисциплины; -допустил неточности в ответе на вопросы и при выполнении заданий по учебно-программному материалу, но обладает необходимыми знаниями для их устранения под руководством преподавателя.	Удовлетворительно
Повышенный уровень	Обучающийся: - обнаружил полное знание учебно-программного материала; -успешно выполнил задания, предусмотренные программой; -усвоил основную литературу, рекомендованную рабочей программой дисциплины; -показал систематический характер знаний учебно-программного материала; -способен к самостоятельному пополнению знаний по учебно-программному материалу и обновлению в ходе дальнейшей учебной работы и профессиональной деятельности.	Хорошо
Высокий уровень	Обучающийся: -обнаружил всесторонние, систематические и глубокие знания учебно-программного материала; -умеет свободно выполнять задания, предусмотренные программой; -ознакомился с дополнительной литературой; -усвоил взаимосвязь основных понятий дисциплин и их значение для приобретения профессии; -проявил творческие способности в понимании учебно-программного материала.	Отлично

1.3. Шкалы оценивания компетенций ОК 01, ОК 02, ОК 03, ОК 04, ОК 05, ОК 06, ОК 07, ОК 08, ОК 09, ОК10, ОК11, ПК 3.1, ПК 3.2, ПК 3.3, ПК 3.4 при сдаче зачета.

Достигнутый уровень результата обучения	Характеристика уровня сформированности компетенций	Шкала оценивания
Пороговый уровень	Обучающийся: - обнаружил на зачете всесторонние, систематические и глубокие знания учебно-программного материала; - допустил небольшие упущения в ответах на вопросы, существенным образом не снижающие их качество; - допустил существенное упущение в ответе на один из вопросов, которое за тем было устранено студентом с помощью уточняющих вопросов; - допустил существенное упущение в ответах на вопросы, часть из которых была устранена студентом с помощью уточняющих вопросов	Зачтено
Низкий уровень	Обучающийся: - допустил существенные упущения при ответах на все вопросы преподавателя; - обнаружил пробелы более чем 50% в знаниях основного учебно-программного материала	Не зачтено

1.4. Описание шкал оценивания

Компетенции обучающегося оценивается следующим образом:

Планируемый уровень результатов освоения	Содержание шкалы оценивания достигнутого уровня результата обучения			
	Неудовлетворительно (Не зачтено)	Удовлетворительно (Зачтено)	Хорошо (Зачтено)	Отлично (Зачтено)
Знать	Неспособность обучающегося самостоятельно продемонстрировать наличие знаний при решении заданий, которые были представлены преподавателем вместе с образцом их решения.	Обучающийся способен самостоятельно продемонстрировать наличие знаний при решении заданий, которые были представлены преподавателем вместе с образцом их решения.	Обучающийся демонстрирует способность к самостоятельному применению знаний при решении заданий, аналогичных тем, которые представлял преподаватель, и при его консультативной поддержке в части современных проблем.	Обучающийся демонстрирует способность к самостоятельному применению знаний в выборе способа решения неизвестных или нестандартных заданий и при консультативной поддержке в части междисциплинарных связей.
Уметь	Отсутствие у обучающегося самостоятельности в применении умений по использованию методов освоения учебной дисциплины.	Обучающийся демонстрирует самостоятельность в применении умений решения учебных заданий в полном соответствии с образцом, данным преподавателем.	Обучающийся продемонстрирует самостоятельное применение умений решения заданий, аналогичных тем, которые представлял преподаватель, и при его консультативной поддержке в части современных проблем.	Обучающийся демонстрирует самостоятельное применение умений решения неизвестных или нестандартных заданий и при консультативной поддержке преподавателя в части междисциплинарных связей.
Иметь практический опыт	Неспособность самостоятельно проявить навык решения поставленной задачи по стандартному образцу повторно.	Обучающийся демонстрирует самостоятельность в применении навыка по заданиям, решение которых было показано преподавателем.	Обучающийся демонстрирует самостоятельное применение навыка решения заданий, аналогичных тем, которые представлял преподаватель, и при его консультативной поддержке в части современных проблем.	Обучающийся демонстрирует самостоятельное применение навыка решения неизвестных или нестандартных заданий и при консультативной поддержке преподавателя в части междисциплинарных связей.

2. Перечень вопросов к другим формам промежуточной аттестации (устному опросу), зачету, дифференцированному зачету

2.1 Примерный перечень вопросов к другим формам промежуточной аттестации (устному опросу).
Компетенции ОК 01, ОК 02, ОК 06, ОК 07, ОК 08, ПК 3.1, ПК 3.2, ПК 3.3

1. Предмет и задачи технической защиты информации. Основные параметры системы защиты информации.
2. Характеристика инженерно-технической защиты информации как области информационной безопасности. Системный подход при решении задач инженерно-технической защиты информации.
3. Задачи и требования к способам и средствам защиты информации техническими средствами.
4. Принципы системного анализа проблем инженерно-технической защиты информации. Классификация способов и средств защиты информации.
5. Особенности информации как предмета защиты.
6. Свойства информации.
7. Виды, источники и носители защищаемой информации.

Компетенции ОК 01, ОК 02, ОК 03, ОК 04, ОК 05, ПК 3.3, ПК 3.4

8. Демаскирующие признаки объектов наблюдения, сигналов и веществ.
9. Понятие об опасном сигнале. Источники опасных сигналов.
10. Основные и вспомогательные технические средства и системы.
11. Основные руководящие, нормативные и методические документы по защите информации и противодействию технической разведке.
12. Понятие и особенности утечки информации.
13. Структура канала утечки информации. Характеристика каналов утечки информации.
14. Классификация существующих физических полей и технических каналов утечки информации.
15. Радиоэлектронный каналы утечки информации, характеристика.
16. Оптический канал утечки информации, характеристика.

Компетенции ОК 01, ОК 02, ОК 03, ОК 04, ОК 05, ОК 09, ОК10, ОК11, ПК 3.1, ПК 3.2, ПК 3.3

17. Акустический каналы утечки информации, характеристика.
18. Материально-вещественный канал утечки информации, характеристика.
19. Основные виды угроз информации
20. Физические основы побочных электромагнитных излучений и наводок.
21. Акустоэлектрические преобразования. Паразитная генерация радиоэлектронных средств.
22. Виды паразитных связей и наводок. Физические явления, вызывающие утечку информации по цепям электропитания и заземления.
23. Подавление опасных сигналов акустоэлектрических преобразований. Экранирование. Зашумление.
24. Технические средства акустической разведки.
25. Технические средства для уничтожения информации и носителей информации, порядок применения.
26. Этапы эксплуатации технических средств защиты информации. Установка и настройка технических средств защиты информации.
27. Классификация демаскирующих признаков
28. Телевизионные системы наблюдения. Приборы ночного видения.

2.2 Примерный перечень вопросов к зачету.
Компетенции ОК 01, ОК 02, ОК 06, ОК 07, ОК 08, ПК 3.1, ПК 3.2, ПК 3.3

1. Скрытие речевой информации в каналах связи.
2. Непосредственное подслушивание звуковой информации.
3. Система защиты от утечки по акустическому каналу (Энергетическое скрытие акустических сигналов).
4. Принцип работы микрофона и телефона. Использование коммуникаций в качестве соединительных проводов.
5. Прослушивание информации направленными микрофонами.
6. Электронные стетоскопы.
7. Лазерные системы подслушивания.
8. Гидроакустические преобразователи.
9. Системы защиты информации от утечки по вибрационному каналу.

Компетенции ОК 01, ОК 02, ОК 03, ОК 04, ОК 05, ПК 3.3, ПК 3.4

10. Негласная запись информации на диктофоны.
11. Системы защиты от диктофонов.
12. Системы защиты информации от утечки по вибрационному каналу .
13. Прослушивание информации от радиотелефонов.
14. Прослушивание информации от работающей аппаратуры.
15. Прослушивание информации от радиозакладок.
16. Прослушивание информации от пассивных закладок.

17. Системы защиты от утечки по электромагнитному каналу.
18. Системы защиты от утечки от радиозакладок.
19. Контактный и бесконтактный методы съема информации за счет непосредственного подключения к телефонной линии.
20. Использование микрофона телефонного аппарата при положенной телефонной трубке.

Компетенции ОК 01, ОК 02, ОК 03, ОК 04, ОК 05, ОК 09, ОК10, ОК11, ПК 3.1, ПК 3.2, ПК 3.3
21. Утечка информации по сотовым цепям связи.
22. Низкочастотное устройство съема информации.
23. Высокочастотное устройство съема информации.
24. Защита информации от несанкционированной утечки по электросетевому каналу.
25. Защита информации от несанкционированной утечки по проводному каналу.
26. Виды, содержание и порядок проведения технического обслуживания средств защиты информации.
27. Организация ремонта технических средств защиты информации.
28. Диагностика, устранение отказов и восстановление работоспособности технических средств защиты информации.
29. Система защиты информации по оптическому каналу.

2.3 Примерный перечень вопросов к дифференцированному зачету.
Компетенции ОК 01, ОК 02, ОК 6, ОК 7, ОК 8, ПК 3.1, ПК 3.2, ПК 3.3
1. Принципы системного анализа проблем инженерно-технической защиты информации.
2. Классификация способов и средств защиты информации.
3. Особенности информации как предмета защиты.
4. Свойства информации.
5. Виды, источники и носители защищаемой информации.
6. Прослушивание информации направленными микрофонами.
7. Электронные стетоскопы.
8. Лазерные системы подслушивания.
9. Гидроакустические преобразователи.
10. Системы защиты информации от утечки по вибрационному каналу.

Компетенции ОК 01, ОК 02, ОК 03, ОК 04, ОК 05, ПК 3.3, ПК 3.4
11. Структура канала утечки информации. Характеристика каналов утечки информации.
12. Классификация существующих физических полей и технических каналов утечки информации.
13. Радиоэлектронный каналы утечки информации, характеристика.
14. Оптический канал утечки информации, характеристика.
15. Прослушивание информации от радиотелефонов.
16. Прослушивание информации от работающей аппаратуры.
17. Прослушивание информации от радиозакладок.
18. Прослушивание информации о пассивных закладок.
19. Системы защиты от утечки по электромагнитному каналу.

Компетенции ОК 01, ОК 02, ОК 03, ОК 04, ОК 05, ОК 09, ОК10, ОК11, ПК 3.1, ПК 3.2, ПК 3.3
20. Технические средства акустической разведки.
21. Технические средства для уничтожения информации и носителей информации, порядок применения.
22. Этапы эксплуатации технических средств защиты информации.
23. Установка и настройка технических средств защиты информации.
24. Классификация демаскирующих признаков
25. Телевизионные системы наблюдения. Приборы ночного видения.
26. Защита информации от несанкционированной утечки по электросетевому каналу.
27. Защита информации от несанкционированной утечки по проводному каналу.

3. Тестовые задания. Оценка по результатам тестирования.

3.1. Примерные задания теста по МДК 03.01 к другим формам промежуточной аттестации.
Компетенции ОК 01, ОК 02, ОК 6, ОК 7, ОК 8, ПК 3.1, ПК 3.2, ПК 3.3
1. К видам каналов утечки информации относятся …
- субъективные
- объективные
- технические
- материально-вещественные

2. Концепция системы защиты от информационного оружия должна включать …
- средства нанесения контратаки с помощью информационного оружия
- процедуры нанесения атак с помощью информационного оружия
- механизмы защиты пользователей от различных типов и уровней угроз для национальной информационной инфраструктуры

- признаки, сигнализирующие о возможном нападении
- процедуры оценки уровня и особенностей атаки против национальной инфраструктуры в целом и отдельных пользователей

3. Формой защиты информации является …
- аналитическая
- организационно-техническая
- страховая
- правовая

4. Симптомами заражения является …
- изменение длины файлов и даты создания
- уменьшение объёма системной памяти и свободного места на диске без видимых причин периодическое мерцание экрана
- замедление работы программ, зависание и перезагрузка

5. Инженерно-техническая защита решает задачи по предотвращению или уменьшению угроз, вызванных …
- стихийными носителями угроз
- попытками злоумышленников проникнуть к местам хранения источников информации
- организованной или случайной утечкой информации с использованием различных технических средств

6. Контролируемая зона – это …
- территория объекта
- территория объекта, на которой возможно пребывание посторонних лиц
- территория объекта, на которой исключено неконтролируемое пребывание лиц

7. Показателем безопасности информации является …
- время, необходимое на взлом защиты информации
- вероятность предотвращения угрозы
- время, в течение которого обеспечивается определённый уровень безопасности
- вероятность возникновения угрозы информационной безопасности

Компетенции ОК 01, ОК 02, ОК 03, ОК 04, ОК 05, ПК 3.3, ПК 3.4
8. Базовая схема системы передачи информации представляет собой:
- передатчик – эфир - приемник
- источник информации – канал связи – получатель информации
- человек – компьютер - человек

9. В необходимый минимум средств защиты от вирусов входит …
- выходной контроль
- профилактика
- входной контроль
- архивирование

10. Электромагнитный канал утечки информации возникает за счет …
- побочных электромагнитных излучений технических средств передачи информации
- побочных излучений технических средств передачи информации
- высокочастотного облучения технических средств передачи информации

11. К наиболее важным методам защиты информации от нелегального доступа относится …
- архивирование (создание резервных копий)
- использование специальных «электронных ключей»
- установление паролей на доступ к информации
- использование антивирусных программ
- шифрование

12. К методам выявления технических каналов утечки информации относится …
- инструментальный контроль
- физический поиск

- тестирование

13. Видовая информация – это …

- информация о внутреннем виде объекта разведки или документа, получаемая при помощи технических средств разведки в виде их изображений
- информация о внешнем виде объекта разведки или документа, получаемая при помощи технических средств разведки в виде их изображений
- информация о внешнем виде объекта разведки или документа, получаемая при помощи программных средств разведки в виде их изображений

14. Техническая защита информации – это защита информации …

- с помощью программно-аппаратных средств
- некриптографическими методами
- криптографическими методами

15. Наиболее важными методами защиты информации от ошибочных действий пользователя является …

- установление специальных атрибутов файлов
- автоматический запрос на подтверждение выполнения команды или операции
- шифрование файлов
- предоставление возможности отмены последнего действия
- дублирование носителей информации

Компетенции ОК 01, ОК 02, ОК 03, ОК 04, ОК 05, ОК 09, ОК10, ОК11, ПК 3.1, ПК 3.2, ПК 3.3

16. Вспомогательные технические средства и системы, это средства …

- и системы непосредственно участвующие в обработке информации ограниченного доступа
- и системы непосредственно не участвующие в обработке информации ограниченного доступа
- телефонной связи, компьютеры

17. Незаконный сбор, присвоение и передача сведений составляющих коммерческую тайну, наносящий ее владельцу ущерб, - это ...

- добросовестная конкуренция
- конфиденциальная информация
- политическая разведка
- промышленный шпионаж

18. Организационно-технические мероприятия – это мероприятия, которые вводят ограничения на … функционирования объекта защиты

- результаты
- параметры
- условия

19. К демаскирующим признакам по времени проявления признаков относятся …

- эпизодические
- периодические
- долгосрочные
- краткосрочные
- постоянные

20. Акустическая информация – это …

- распространение акустических волн различной формы и длительности, распространяющиеся от источника в окружающее пространство
- звуковые волны
- возмущения упругой среды различной формы и длительности, распространяющиеся от источника в окружающее пространство

3.2. Примерные задания теста по МДК 03.01 к зачету.

Компетенции ОК 01, ОК 02, ОК 6, ОК 07, ОК 08, ПК 3.1, ПК 3.2, ПК 3.3

1. Признаки вещества:

- цвет, ширина спектра
- мощность, частота, амплитуда

- физический и химический состав, структура и свойства

2. Средства инженерно-технической защиты подразделяются на:
- физические, аппаратные, программные, криптографические, комбинированные
- физические, программные, криптографические, комбинированные
- физические, аппаратные, программные, комбинированные

3. Технические средства передачи информации – это технические средства …
- непосредственно обрабатывающие информацию ограниченного доступа
- непосредственно обрабатывающие информацию
- не обрабатывающие информацию ограниченного доступа

4. Особенностью речевых сообщений является …
- виртуальность
- документальность
- конфиденциальность
- целостность

5. К демаскирующим признакам по информативности признаков относятся …
- прямые (дополнительные признаки объекта) [информативность в пределах от 0 до 1]
- именные (однозначно определяющие объект) [информативность =1]
- информационно-психологические
- косвенные (признаки, непосредственно не принадлежащие объекту)
- технические
- физические

6. Основные типы систем обнаружения атак …
- локальные
- сетевые
- программные
- аппаратные

7. К демаскирующим признакам по состоянию объекта относятся …
- опознавательные признаки
- признаки физические
- признаки программные
- признаки деятельности

Компетенции ОК 01, ОК 02, ОК 03, ОК 04, ОК 05, ПК 3.3, ПК 3.4
8. Задачи, поставленные в рамках концепции национальной безопасности приоритетное развитие отечественных современных информационных и телекоммуникационных технологий и …
- ускорение развития новых информационных технологий и их широкое распространение
- установление необходимого баланса между потребностью в свободном обмене информацией и допустимыми ограничениями её распространения
- совершенствование информационной структуры

9. Объектом защиты может являться …
- информационные процессы
- носители информации
- субъект

10. Физические системы защиты подразделяются на:
- системы ограждения и физической изоляции, системы контроля доступа, запирающие устройства и хранилища
- системы ограждения и физической изоляции, запирающие устройства и хранилища
- системы охлаждения, системы этз, запирающие устройства и хранилища

11. Источником информации при утечке по техническим каналам может являться …
- информация, обрабатываемая техническими средствами передачи информации
- видовая информация

- информация, передаваемая по каналам связи
- человек

12. Признаки сигналов описывают параметры полей и генерирующих сигналов:
- высоту, ширину, длину
- форму, размеры, детали, тон, цвет, структуру и фактуру
- мощность, частота, природа, вид (аналог, импульс), ширина спектра;

13. Видовые признаки включают:
- запах, палитру, оттенки
- высоту, ширину, длину
- форму, размеры, детали, тон, цвет, структуру и фактуру
- частоту, амплитуду, ширину спектра

14. Классифицировать компьютерные вирусы можно по …
- степени опасности
- способу заражения среды обитания
- степени полезности
- объёму программы
- среде обитания

15. FireWall – это …
- почтовая программа
- графический редактор
- тоже самое что и интернет браузер
- тоже самое что и брэндмауэр

Компетенции ОК 01, ОК 02, ОК 03, ОК 04, ОК 05, ОК 09, ОК10, ОК11, ПК 3.1, ПК 3.2, ПК 3.3
16. Периодичность аттестационных проверок для помещений первой и второй группы:
- не реже 3 раз в год
- не реже 2 раз в год
- не реже 1 раза в год

17. К методам защиты по вибрационному каналу относится …
- обследование стетоскопами
- изучение архитектурно-строительной документации
- маскирование

18. Параметрический канал утечки информации возникает за счет …
- высокочастотного облучения информационных сигналов
- побочных электромагнитных излучений информационных сигналов
- низкочастотного облучения информационных сигналов

19. Аттестация выделенных помещений – это проверка выделенных помещений и находящихся в них …
- технических средств на соответствие требованиям защиты
- технических средств на несоответствие требованиям защиты
- программных средств на соответствие требованиям защиты

20. К демаскирующим признакам по характеристикам объекта относятся …
- искусственные
- видовые (форма, размеры, детали, фактура)
- признаки сигнала (мощность, частота, вид, спектр)
- архитектурные (фасад, высота)
- признаки вещества (физ/хим состав, структура, свойства)

21. Утечка информации по техническим каналам реализуется в результате …
- подслушивания конфиденциальных разговоров и акустических сигналов
- перехвата различного рода полей и сигналов
- наблюдения за источниками информации

- недостаточной организацией защиты информации

22. Информативность – мера … признака

- объемности
- открытости
- индивидуальности
- показательности

23. При экранировании помещения применяется …

- фтористая сетка
- алюминиевая фольга
- листовая сталь
- медная сетка

3.3. Примерные задания теста по МДК 03.01 к дифференцированному зачету.
Компетенции ОК 01, ОК 02, ОК 06, ОК 07, ОК 08, ПК 3.1, ПК 3.2, ПК 3.3

1. Особенностью речевых сообщений является …

- виртуальность
- документальность
- конфиденциальность
- целостность

2. К демаскирующим признакам по информативности признаков относятся …

- прямые (дополнительные признаки объекта) [информативность в пределах от 0 до 1]
- именные (однозначно определяющие объект) [информативность =1]
- информационно-психологические
- косвенные (признаки, непосредственно не принадлежащие объекту)
- технические
- физические

3. Основные типы систем обнаружения атак …

- локальные
- сетевые
- программные
- аппаратные

4. К демаскирующим признакам по состоянию объекта относятся …

- опознавательные признаки
- признаки физические
- признаки программные
- признаки деятельности

5. Инженерно-техническая защита решает задачи по предотвращению или уменьшению угроз, вызванных …

- стихийными носителями угроз
- попытками злоумышленников проникнуть к местам хранения источников информации
- организованной или случайной утечкой информации с использованием различных технических средств

6. Контролируемая зона – это …

- территория объекта
- территория объекта, на которой возможно пребывание посторонних лиц
- территория объекта, на которой исключено неконтролируемое пребывание лиц

7. Показателем безопасности информации является …

- время, необходимое на взлом защиты информации
- вероятность предотвращения угрозы
- время, в течение которого обеспечивается определённый уровень безопасности
- вероятность возникновения угрозы информационной безопасности

Компетенции ОК 01, ОК 02, ОК 03, ОК 04, ОК 05, ПК 3.3, ПК 3.4

8. Задачи, поставленные в рамках концепции национальной безопасности приоритетное развитие отечественных современных информационных и телекоммуникационных технологий и …

- ускорение развития новых информационных технологий и их широкое распространение
- установление необходимого баланса между потребностью в свободном обмене информацией и допустимыми ограничениями её распространения
- совершенствование информационной структуры

9. Объектом защиты может являться …

- информационные процессы
- носители информации
- субъект

10. Физические системы защиты подразделяются на:

- системы ограждения и физической изоляции, системы контроля доступа, запирающие устройства и хранилища
- системы ограждения и физической изоляции, запирающие устройства и хранилища
- системы охлаждения, системы этз, запирающие устройства и хранилища

11. Источником информации при утечке по техническим каналам может являться …

- информация, обрабатываемая техническими средствами передачи информации
- видовая информация
- информация, передаваемая по каналам связи
- человек

12. К наиболее важным методам защиты информации от нелегального доступа относится …

- архивирование (создание резервных копий)
- использование специальных «электронных ключей»
- установление паролей на доступ к информации
- использование антивирусных программ
- шифрование

13. К методам выявления технических каналов утечки информации относится …

- инструментальный контроль
- физический поиск
- тестирование

14. Видовая информация – это …

- информация о внутреннем виде объекта разведки или документа, получаемая при помощи технических средств разведки в виде их изображений
- информация о внешнем виде объекта разведки или документа, получаемая при помощи технических средств разведки в виде их изображений
- информация о внешнем виде объекта разведки или документа, получаемая при помощи программных средств разведки в виде их изображений

Компетенции ОК 01, ОК 02, ОК 03, ОК 04, ОК 05, ОК 09, ОК10, ОК11, ПК 3.1, ПК 3.2, ПК 3.3

15. Утечка информации по техническим каналам реализуется в результате …

- подслушивания конфиденциальных разговоров и акустических сигналов
- перехвата различного рода полей и сигналов
- наблюдения за источниками информации
- недостаточной организацией защиты информации

16. Информативность – мера … признака

- объемности
- открытости
- индивидуальности
- показательности

17. При экранировании помещения применяется …

- фтористая сетка
- алюминиевая фольга

- листовая сталь
- медная сетка

18. К демаскирующим признакам по времени проявления признаков относятся …

- эпизодические
- периодические
- долгосрочные
- краткосрочные
- постоянные

19. Акустическая информация – это …

- распространение акустических волн различной формы и длительности, распространяющиеся от источника в окружающее пространство
- звуковые волны
- возмущения упругой среды различной формы и длительности, распространяющиеся от источника в окружающее пространство

3.4. Соответствие между бальной системой и системой оценивания по результатам тестирования устанавливается посредством следующей таблицы:

Объект оценки	Показатели оценивания результатов обучения	Оценка	Уровень результатов обучения
Обучающийся	60 баллов и менее	«Неудовлетворительно» (Не зачтено)	Низкий уровень
	74 – 61 баллов	«Удовлетворительно» (Зачтено)	Пороговый уровень
	84 – 75 баллов	«Хорошо» (Зачтено)	Повышенный уровень
	100 – 85 баллов	«Отлично» (Зачтено)	Высокий уровень

4. Оценка ответа обучающегося на вопросы.

4.1. Оценка ответа обучающегося на вопросы к другим формам промежуточной аттестации (устному опросу), зачету, дифференцированному зачету.

Элементы оценивания	Содержание шкалы оценивания			
	Неудовлетворительно (Не зачтено)	Удовлетворительно (Зачтено)	Хорошо (Зачтено)	Отлично (Зачтено)
Соответствие ответов формулировкам вопросов (заданий)	Полное несоответствие по всем вопросам	Значительные погрешности	Незначительные погрешности	Полное соответствие
Структура, последовательность и логика ответа. Умение четко, понятно, грамотно и свободно излагать свои мысли	Полное несоответствие критерию.	Значительное несоответствие критерию	Незначительное несоответствие критерию	Соответствие критерию при ответе на все вопросы.
Знание нормативных, правовых документов и специальной литературы	Полное незнание нормативной и правовой базы и специальной литературы	Имеют место существенные упущения (незнание большей части из документов и специальной литературы по названию, содержанию и т.д.).	Имеют место несущественные упущения и незнание отдельных (единичных) работ из числа обязательной литературы.	Полное соответствие данному критерию ответов на все вопросы.
Умение увязывать теорию с практикой, в том числе в области профессиональной работы	Умение связать теорию с практикой работы не проявляется.	Умение связать вопросы теории и практики проявляется редко.	Умение связать вопросы теории и практики в основном проявляется.	Полное соответствие данному критерию. Способность интегрировать знания и привлекать сведения из различных научных сфер
Качество ответов на	На все дополнительные	Ответы на большую	1. Даны неполные	Даны верные

дополнительные вопросы	вопросы преподавателя даны неверные ответы.	часть дополнительных вопросов преподавателя даны неверно.	ответы на дополнительные вопросы преподавателя. 2. Дан один неверный ответ на дополнительные вопросы преподавателя.	ответы на все дополнительные вопросы преподавателя.

Примечание: итоговая оценка формируется как средняя арифметическая результатов элементов оценивания.

МДК.03.02 Инженерно-технические средства физической защиты объектов информатизации

1. Описание показателей, критериев и шкал оценивания компетенций.

1.1. Показатели и критерии оценивания компетенций ОК 01, ОК 02, ОК 03, ОК 04, ОК 5, ОК 06, ОК 07, ОК 08, ОК 09, ОК10, ОК11, ПК 3.5

Объект оценки	Уровни сформированности компетенций	Критерий оценивания результатов обучения
Обучающийся	Низкий уровень Пороговый уровень Повышенный уровень Высокий уровень	Уровень результатов обучения **не ниже порогового**

1.2. Шкалы оценивания компетенций ОК 01, ОК 02, ОК 03, ОК 04, ОК 5, ОК 06, ОК 07, ОК 08, ОК 09, ОК10, ОК11, ПК 3.5 при сдаче других форм промежуточной аттестации (устного опроса) и экзамена

Достигнутый уровень результата обучения	Характеристика уровня сформированности компетенций	Шкала оценивания
		Дифференцированный зачет (Экзамен)
Низкий уровень	Обучающийся: -обнаружил пробелы в знаниях основного учебно-программного материала; -допустил принципиальные ошибки в выполнении заданий, предусмотренных программой; -не может продолжить обучение или приступить к профессиональной деятельности по окончании программы без дополнительных занятий по соответствующей дисциплине.	Неудовлетворительно
Пороговый уровень	Обучающийся: -обнаружил знание основного учебно-программного материала в объёме, необходимом для дальнейшей учебной и предстоящей профессиональной деятельности; -справляется с выполнением заданий, предусмотренных программой; -знаком с основной литературой, рекомендованной рабочей программой дисциплины; -допустил неточности в ответе на вопросы и при выполнении заданий по учебно-программному материалу, но обладает необходимыми знаниями для их устранения под руководством преподавателя.	Удовлетворительно
Повышенный уровень	Обучающийся: - обнаружил полное знание учебно-программного материала; -успешно выполнил задания, предусмотренные программой; -усвоил основную литературу, рекомендованную рабочей программой дисциплины; -показал систематический характер знаний учебно-программного материала; -способен к самостоятельному пополнению знаний по учебно-программному материалу и обновлению в ходе дальнейшей учебной работы и профессиональной деятельности.	Хорошо
Высокий уровень	Обучающийся: -обнаружил всесторонние, систематические и глубокие знания учебно-программного материала; -умеет свободно выполнять задания, предусмотренные программой; -ознакомился с дополнительной литературой; -усвоил взаимосвязь основных понятий дисциплин и их значение для приобретения профессии; -проявил творческие способности в понимании учебно-программного материала.	Отлично

1.3. Шкалы оценивания компетенций ОК 01, ОК 02, ОК 03, ОК 04, ОК 05, ОК 06, ОК 07, ОК 08, ОК 09, ОК10, ОК11, ПК 3.5 при защите курсового проекта

Достигнутый уровень результата обучения	Характеристика уровня сформированности компетенций	Шкала оценивания
Низкий уровень	Содержание работы не удовлетворяет требованиям, предъявляемым к КП; на защите КП обучающийся не смог обосновать результаты проведенных расчетов (исследований); цель КП не достигнута; структура работы нарушает требования нормативных документов; выводы отсутствуют или не отражают теоретические положения, обсуждаемые в работе; в работе много орфографических ошибок, опечаток и других технических недостатков; язык	Неудовлетворительно

	не соответствует нормам научного стиля речи.	
Пороговый уровень	Содержание работы удовлетворяет требованиям, предъявляемым к КП; на защите КП обучающийся не смог обосновать все результаты проведенных расчетов (исследований); задачи КП решены не в полном объеме, цель не достигнута; структура работы отвечает требованиям нормативных документов; выводы присутствуют, но не полностью отражают теоретические положения, обсуждаемые в работе; в работе присутствуют орфографические ошибки, опечатки; язык соответствует нормам научного стиля речи; при защите КП обучающийся излагает материал неполно и допускает неточности в определении понятий или формулировке правил; затрудняется или отвечает не правильно на поставленный вопрос	Удовлетворительно
Повышенный уровень	Содержание работы удовлетворяет требованиям, предъявляемым к КП; на защите КП обучающийся смог обосновать все результаты проведенных расчетов (исследований); задачи КП решены в полном объеме, цель достигнута; структура работы отвечает требованиям нормативных документов; выводы присутствуют, но не полностью отражают теоретические положения, обсуждаемые в работе; в работе практически отсутствуют орфографические ошибки, опечатки; язык соответствует нормам научного стиля речи; при защите КП полно обучающийся излагает материал, дает правильное определение основных понятий; затрудняется или отвечает не правильно на некоторые вопросы	Хорошо
Высокий	Содержание работы удовлетворяет требованиям, предъявляемым к КП; на защите КП обучающийся смог обосновать все результаты проведенных расчетов (исследований); задачи КП решены в полном объеме, цель достигнута; структура работы отвечает требованиям нормативных документов; выводы присутствуют и полностью отражают теоретические положения, обсуждаемые в работе; в работе отсутствуют орфографические ошибки, опечатки; язык соответствует нормам научного стиля речи; при защите КП обучающийся полно излагает материал, дает правильное определение основных понятий; четко и грамотно отвечает на вопросы	Отлично

1.4. Описание шкал оценивания

Компетенции обучающегося оценивается следующим образом:

Планируемый уровень результатов освоения	Содержание шкалы оценивания достигнутого уровня результата обучения			
	Неудовлетворительно	Удовлетворительно	Хорошо	Отлично
Знать	Неспособность обучающегося самостоятельно продемонстрировать наличие знаний при решении заданий, которые были представлены преподавателем вместе с образцом их решения.	Обучающийся способен самостоятельно продемонстрировать наличие знаний при решении заданий, которые были представлены преподавателем вместе с образцом их решения.	Обучающийся демонстрирует способность к самостоятельному применению знаний при решении заданий, аналогичных тем, которые представлял преподаватель, и при его консультативной поддержке в части современных проблем.	Обучающийся демонстрирует способность к самостоятельному применению знаний в выборе способа решения неизвестных или нестандартных заданий и при консультативной поддержке в части междисциплинарных связей.
Уметь	Отсутствие у обучающегося самостоятельности в применении умений по использованию методов освоения учебной дисциплины.	Обучающийся демонстрирует самостоятельность в применении умений решения учебных заданий в полном соответствии с образцом, данным преподавателем.	Обучающийся продемонстрирует самостоятельное применение умений решения заданий, аналогичных тем, которые представлял преподаватель, и при его консультативной поддержке в части современных проблем.	Обучающийся демонстрирует самостоятельное применение умений решения неизвестных или нестандартных заданий и при консультативной поддержке преподавателя в части междисциплинарных связей.
Иметь практический	Неспособность самостоятельно	Обучающийся демонстрирует	Обучающийся демонстрирует	Обучающийся демонстрирует

опыт	проявить навык решения поставленной задачи по стандартному образцу повторно.	самостоятельность в применении навыка по заданиям, решение которых было показано преподавателем.	самостоятельное применение навыка решения заданий, аналогичных тем, которые представлял преподаватель, и при его консультативной поддержке в части современных проблем.	самостоятельное применение навыка решения неизвестных или нестандартных заданий и при консультативной поддержке преподавателя в части междисциплинарных связей.

2. Перечень вопросов к другим формам промежуточной аттестации (устному опросу) и экзамену.

2.1 Примерный перечень вопросов к другим формам промежуточной аттестации (устному опросу). (6 семестр)
Компетенции ОК 01, ОК 02, ОК 03, ОК 04, ОК 08, ОК 09, ОК10, ОК11, ПК 3.5

1. Виды информации, защищаемой техническими средствами.
2. Свойства информации, как предмета защиты.
3. Определение и классификация демаскирующих признаков объектов.
4. Видовые демаскирующие признаки объекта, признаки веществ.
5. Понятие об информационных сигналах и их источники.
6. Основные и вспомогательные технические средства и системы.
7. Классификация и принципы действия акустических преобразователей.

Компетенции ОК 01, ОК 05, ОК 06, ОК 07, ОК 08, ОК 09, ОК10, ОК11, ПК 3.5

8. Средства противодействия утечки информации по оптическим каналам.
9. Структура и виды радиоэлектронных каналов утечки информации.
10. Классификация и особенности распространения радиоволн.
11. Распространение информативных сигналов в радиоэлектронных каналах утечки информации.
12. Классификация помех.
13. Характер распространения звука в различных средах. Реверберация.
14. Структура акустического канала утечки информации.
15. Виды акустических каналов утечки информации.

Компетенции ОК 01, ОК 02, ОК 03, ОК 04, ОК 05, ОК 06, ПК 3.5

16. Средства контроля и управления средствами охраны.
17. Состав и структура системы видеоконтроля.
18. Назначение и характеристики составных частей системы видеоконтроля.
19. Принцип работы детектора движения.
20. Структурное скрытие речевой информации в телефонных каналах связи.
21. Энергетическое скрытие акустического сигнала.
22. Характеристики и классификация закладных устройств.

2.2 Темы курсового проекта. Примерный перечень вопросов к защите курсового проекта.

2.2.1 Темы курсового проекта
Компетенции ОК 01, ОК 02, ОК 03, ОК 04, ОК 05, ОК 06, ОК 07, ОК 08, ОК 09, ОК10, ОК11, ПК 3.5

1. Оптимизация защиты персональных данных работников предприятия
2. Изучение и оптимизация защиты коммерческой тайны.
3. Интеграция охранно-пожарной сигнализации, СКУД и системы видеонаблюдения в комплексную систему безопасности.
4. Разработка политики информационной безопасности для организации
5. Организация безопасного удаленного доступа к ЛВС.
6. Проектирование и модернизация комплексной системы защиты информации (КСЗИ).
7. Обоснование и модернизация мер организационной защиты. конфиденциальной информации при взаимодействии сотрудников предприятия со сторонними организациями.
8. Проектирование и модернизация методов и форм работы с персоналом предприятия, допущенным к конфиденциальной информации.
9. Проектирование систем видеонаблюдения и СКУД для обеспечения защиты информации.
10. Проектирование и модернизация системы защиты информации конфиденциального характера от утечки по техническим каналам.
11. Проектирование и модернизация комплексной системы защиты информации в кабинете руководителя предприятия.
12. Защита акустической информации в организации.

13. Проектирование и модернизация систем видеонаблюдения и контроля ОПС к объектам информатизации.
14. Обеспечение безопасной работы в выделенном помещении при обмене данными со сторонними организациями.

2.2.2 Примерный перечень вопросов к защите курсового проекта.
Компетенции ОК 01, ОК 02, ОК 03, ОК 04, ОК 07, ОК 08, ОК 09, ОК10, ОК11, ПК 3.5

1. Классификация технических каналов утечки информации.
2. Характеристики и комплексное использование технических каналов утечки информации.
3. Возможности и классификация оптических каналов утечки информации.
4. Структура оптического канала утечки информации.
5. Назначение, принципы работы, характеристики средств наблюдения (оптические приборы, фото и киноаппараты, приборы ночного видения).
6. Системы обнаружения оптических устройств.

Компетенции ОК 01, ОК 02, ОК 03, ОК 04, ОК 05, ОК 06, ПК 3.5

1. Средства поиска излучающих закладных устройств.
2. Средства поиска неизлучающих закладных устройств.
3. Средства и способы подавления закладных устройств.
4. Акустические преемники их структура и характеристики.
5. Характеристики и классификация микрофонов.
6. Конструкция и работа микрофонов по принципу действия.

2.3 Примерный перечень вопросов к другим формам промежуточной аттестации (устному опросу). (7 семестр)
Компетенции ОК 01, ОК 02, ОК 03, ОК 04, ОК 08, ОК 09, ОК10, ОК11, ПК 3.5

1. Основные задачи инженерно-технической защиты информации.
2. Факторы, влияющие на эффективность инженерно-технической защиты информации.
3. Базовые принципы инженерно-технической защиты информации (общие, специальные, дополнительные).
4. Объект информатизации (определение).
5. Основные технические средства и системы (ОТСС).
6. Вспомогательные технические средства и системы (ВТСС).
7. Технический канал утечки информации (определение).
8. Схема технического канала утечки информации
9. Показатели эффективности инженерно-технической защиты информации.

Компетенции ОК 01, ОК 05, ОК 06, ОК 07, ОК 08, ОК 09, ОК10, ОК11, ПК 3.5

10. Основные направления инженерно-технической защиты информации.
11. Демаскирующие признаки объекта (общая классификация, классификация по характеристикам объекта – видовые, сигнальные, вещество).
12. Демаскирующие признаки объекта (общая классификация, классификация по информативности и по времени проявления).
13. Источники и носители информации. Принципы записи и съема информации.
14. Источники сигналов (общая классификация, классификация основных и вспомогательных источников информации).
15. Источники сигналов (классификация по физической природе, акустоэлектронные преобразователи).
16. Источники сигналов (классификация по физической природе, излучатели низкочастотных и высокочастотных сигналов).
17. Источники сигналов (классификация по физической природе, паразитные связи и наводки).

Компетенции ОК 01, ОК 02, ОК 03, ОК 04, ОК 05, ОК 06, ПК 3.5

18. Побочные электромагнитные излучения и наводки; структура, классификация и основные характеристики технических каналов утечки информации.
19. Схема технического канала утечки информации, возникающего за счет побочных электромагнитных излучений
20. Классификация технической разведки (по физической природе носителя), основные этапы и процедуры добывания информации технической разведкой; возможности видов технической разведки.
21. Способы и средства добывания информации без физического проникновения в контролируемую зону.
22. Способы и средства наблюдения в оптическом диапазоне.
23. Способы и средства наблюдения в радиодиапазоне.
24. Скрытие речевой информации в каналах связи.
25. Энергетическое скрытие акустических информативных сигналов
26. Обнаружение и локализация закладных устройств, подавление их сигналов.
27. Подавление опасных сигналов акустоэлектрических преобразователей.
28. Экранирование и компенсация информативных полей;
29. Подавление информативных сигналов в цепях заземления и электропитания.

2.4 Примерный перечень вопросов к экзамену. Образец экзаменационного билета.

2.4.1 Примерный перечень вопросов к экзамену.

Компетенции ОК 01, ОК 02, ОК 03, ОК 04, ОК 08, ОК 09, ОК10, ОК11, ПК 3.5

1. Виды информации, защищаемой техническими средствами.
2. Свойства информации, как предмета защиты.
3. Определение и классификация демаскирующих признаков объектов.
4. Видовые демаскирующие признаки объекта, признаки веществ.
5. Понятие об информационных сигналах и их источники.
6. Основные и вспомогательные технические средства и системы.
7. Классификация и принципы действия акустических преобразователей.
8. Побочные высокочастотные и низкочастотные излучения технических средств.
9. Утечка информации по цепям электропитания и заземления
10. Виды угроз безопасности информации.
11. Основные задачи и типовая структура разведки.
12. Классификация органов технической разведки.
13. Утечка информации. Типовая структура технического канала утечки информации.
14. Классификация технических каналов утечки информации.
15. Характеристики и комплексное использование технических каналов утечки информации.
16. Возможности и классификация оптических каналов утечки информации.
17. Структура оптического канала утечки информации.
18. Назначение, принципы работы, характеристики средств наблюдения (оптические приборы, фото и киноаппараты, приборы ночного видения).
19. Системы обнаружения оптических устройств.

Компетенции ОК 01, ОК 05, ОК 06, ОК 07, ОК 08, ОК 09, ОК10, ОК11, ПК 3.5

20. Средства противодействия утечки информации по оптическим каналам.
21. Структура и виды радиоэлектронных каналов утечки информации.
22. Классификация и особенности распространения радиоволн.
23. Распространение информативных сигналов в радиоэлектронных каналах утечки информации.
24. Классификация помех.
25. Характер распространения звука в различных средах. Реверберация.
26. Структура акустического канала утечки информации.
27. Виды акустических каналов утечки информации.
28. Структура вещественных каналов утечки информации.
29. Демаскирующие признаки веществ.
30. Методы добывания информации о вещественных признаках.
31. Задачи и принципы инженерно-технической защиты информации.
32. Классификация методов инженерно-технической защиты информации.
33. Характеристика методов физической защиты информации.
34. Структура системы инженерной защиты и охраны объектов.
35. Средства инженерной защиты объектов.
36. Структура комплексов управления и доступом людей и транспорта.
37. Способы идентификации людей.
38. Классификация извещателей.

Компетенции ОК 01, ОК 02, ОК 03, ОК 04, ОК 05, ОК 06, ПК 3.5

39. Средства контроля и управления средствами охраны.
40. Состав и структура системы видеоконтроля.
41. Назначение и характеристики составных частей системы видеоконтроля.
42. Принцип работы детектора движения.
43. Структурное скрытие речевой информации в телефонных каналах связи.
44. Энергетическое скрытие акустического сигнала.
45. Характеристики и классификация закладных устройств.
46. Демаскирующие признаки закладных устройств. Способы маскировки закладных устройств.
47. Средства поиска излучающих закладных устройств.
48. Средства поиска неизлучающих закладных устройств.
49. Средства и способы подавления закладных устройств.
50. Акустические преемники их структура и характеристики.
51. Характеристики и классификация микрофонов.
52. Конструкция и работа микрофонов по принципу действия.

53. Характеристики направленности микрофонов.
54. Конструкция и работа остронаправленных микрофонов.
55. Диктофоны, средства лазерного подслушивания.
56. Добывание информации путем высокочастотного навязывания.
57. Экранирование электромагнитных полей.
58. Экранирование электрических проводов.
59. Компенсация полей.
60. Средства экранирования электромагнитных полей

2.4.2. Образец экзаменационного билета по МДК 03.02

<table>
<tr><td colspan="3">Дальневосточный государственный университет путей сообщения</td></tr>
<tr><td>ПЦК
«Информационная безопасность автоматизированных систем»
название
_____
семестр, учебный год</td><td>Экзаменационный билет №
по дисциплине
МДК 03.02
название
для направления подготовки/ специальности
10.02.05 Обеспечение информационной безопасности автоматизированных систем
код, название
технический
профиль/специализация</td><td>«Утверждаю»
Председатель ПЦК
_____
ФИО
«___» _____ 20 __ г.</td></tr>
<tr><td colspan="3">1. Определение и классификация демаскирующих признаков объектов. (ОК 01, ОК 02, ОК 03, ОК 04, ОК 08, ОК 09, ОК10, ОК11, ПК 3.5)</td></tr>
<tr><td colspan="3">2. Классификация и особенности распространения радиоволн. (ОК 01, ОК 5, ОК 06, ОК 07, ОК 08, ОК 09, ОК10, ОК11, ПК 3.5)</td></tr>
<tr><td colspan="3">3. Экранирование электромагнитных полей. (ОК 01, ОК 02, ОК 03, ОК 04, ОК 5, ОК 06, ПК 3.5)</td></tr>
</table>

3. Тестовые задания. Оценка по результатам тестирования.

3.1. Примерные задания теста по МДК 03.02 к другим формам промежуточной аттестации. (6 семестр)

Компетенции ОК 01, ОК 02, ОК 03, ОК 04, ОК 08, ОК 09, ОК10, ОК11, ПК 3.5

1. **Из перечисленного: 1) администраторы; 2) пользователи; 3) задания; 4) терминалы; 5) программы; 6) файлы — модель политики безопасности Адепт-50 рассматривает следующие группы безопасности**:
   - 2, 3, 4, 6
   - 1, 2, 5, 6
   - 3, 4, 5, 6
   - 1, 2, 3, 4

2. **Абстрактное описание системы, без связи с ее реализацией, дает модель политики безопасности**
   - Белла-ЛаПадула
   - на основе анализа угроз
   - с полным перекрытием
   - Лендвера

3. **В модели политики безопасности Лендвера многоуровневая информационная структура называется**
   - контейнером
   - массивом
   - множеством
   - объектом

4. **В модели политики безопасности Лендвера ссылка на сущность, если это идентификатор сущности, называется**
   - прямой
   - простой
   - циклической
   - косвенной

5. **Выделения пользователем и администраторам только тех прав доступа, которые им необходимы это**
- принцип минимизации привилегий
- принцип простоты и управляемости ИС
- принцип многоуровневой защиты
- принцип максимизации привилегий

Компетенции ОК 01, ОК 05, ОК 06, ОК 07, ОК 08, ОК 09, ОК10, ОК11, ПК 3.5

6. **Главным параметром криптосистемы является показатель**
- Криптостойкости
- скорости шифрования
- безошибочности шифрования
- надежности функционирования

7. **Два ключа используются в криптосистемах**
- с открытым ключом
- двойного шифрования
- симметричных
- с закрытым ключом

8. **Длина исходного ключа в ГОСТ 28147-89 (бит)**
- 256
- 56
- 128
- 64

9. **Для решения проблемы правильности выбора и надежности функционирования средств защиты в «Европейских критериях» вводится понятие**
- адекватности средств защиты
- унификации средств защиты
- надежности защиты информации
- оптимизации средств защиты

10. **Достоинствами аппаратной реализации криптографического закрытия данных являются**
- высокая производительность и простота
- целостность и безопасность
- доступность и конфиденциальность
- практичность и гибкость

Компетенции ОК 01, ОК 02, ОК 03, ОК 04, ОК 05, ОК 06, ПК 3.5

11. **Достоинством дискретных моделей политики безопасности является**
- простой механизм реализации
- числовая вероятностная оценка надежности
- высокая степень надежности
- динамичность

12. **Достоинством модели политики безопасности на основе анализа угроз системе является**
- числовая вероятностная оценка надежности
- высокая степень надежности
- динамичность
- простой механизм реализации

13. **Если средства защиты могут быть преодолены только государственной спецслужбой, то согласно «Европейским критериям» безопасность считается**
- высокой
- сверхвысокой
- стандартной
- базовой

14. **Если средство защиты способно противостоять отдельным атакам, то согласно «Европейским критериям» безопасность считается**

- базовой
- стандартной
- низкой
- средней

15. **Защита с применением меток безопасности согласно «Оранжевой книге» используется в системах класса**
- B1
- C2
- B2
- C1

3.2. Примерные задания теста по МДК 03.02 к другим формам промежуточной аттестации. (7 семестр)

Компетенции ОК 01, ОК 02, ОК 03, ОК 04, ОК 08, ОК 09, ОК10, ОК11, ПК 3.5

1. Количество уровней адекватности, которое определяют «Европейские критерии»
   - 7
   - 3
   - 5
   - 10

2. Конечное множество используемых для кодирования информации знаков называется
   - алфавитом
   - кодом
   - ключом
   - шифром

3. Математические методы нарушения конфиденциальности и аутентичности информации без знания ключей объединяет
   - криптоанализ
   - криптография
   - стеганография
   - криптология

4. Модели политики безопасности на основе анализа угроз системе исследуют вероятность преодоления системы защиты за определенное время
   - фиксированными затратами
   - ограниченной компетенцией злоумышленника
   - фиксированным ресурсом

5. Надежность СЗИ определяется
   - самым слабым звеном
   - количеством отраженных атак
   - усредненным показателем
   - самым сильным звеном

6. Наименее затратный криптоанализ для криптоалгоритма RSA
   - разложение числа на простые множители
   - перебор по всему ключевому пространству
   - перебор по выборочному ключевому пространству
   - разложение числа на сложные множители

7. Недостатком дискретных моделей политики безопасности является
   - статичность
   - необходимость дополнительного обучения персонала
   - изначальное допущение вскрываемости системы
   - сложный механизм реализации

8. Недостатком модели политики безопасности на основе анализа угроз системе является
   - изначальное допущение вскрываемости системы
   - необходимость дополнительного обучения персонала
   - сложный механизм реализации
   - статичность

9. Нормативный документ, регламентирующий все аспекты безопасности продукта информационных технологий, называется
   - профилем защиты
   - профилем безопасности
   - стандартом безопасности
   - системой защиты

10. Обеспечением скрытности информации в информационных массивах занимается
    - стеганография
    - криптоанализ
    - криптология
    - криптография

Компетенции ОК 01, ОК 05, ОК 06, ОК 07, ОК 08, ОК 09, ОК10, ОК11, ПК 3.5

11. Основным положением модели системы безопасности с полным перекрытием является наличие на каждом пути проникновения в систему
    - хотя бы одного средства безопасности
    - аудита
    - пароля
    - всех средств безопасности

12. Первым этапом разработки системы защиты ИС является
    - анализ потенциально возможных угроз информации
    - оценка возможных потерь
    - стандартизация программного обеспечения
    - изучение информационных потоков

13. По документам ГТК количество классов защищенности СВТ от НСД к информации
    - 6
    - 9
    - 8
    - 7

14. По документам ГТК самый низкий класс защищенности СВТ от НСД к информации
    - 6
    - 9
    - 0
    - 1

15. Политика информационной безопасности — это
    - совокупность законов, правил, определяющих управленческие и проектные решения в области защиты информации
    - стандарт безопасности
    - профиль защиты
    - итоговый документ анализа рисков

16. При избирательной политике безопасности в матрице доступа объекту системы соответствует
    - строка
    - прямоугольная область
    - ячейка
    - столбец

17. Конкретизацией модели Белла-ЛаПадула является модель политики безопасности
    - LWM
    - На основе анализа угроз
    - С полным перекрытием
    - Лендвера

18. Метод управления доступом, при котором каждому объекту системы присваивается метка критичности, определяющая ценность информации, называется
    - мандатным
    - привилегированным
    - идентифицируемым
    - избирательным

19. На многопользовательские системы с информацией одного уровня конфиденциальности согласно «Оранжевой книге» рассчитан класс
    - C1
    - B2
    - C2
    - B1

20. Наименее затратный криптоанализ для криптоалгоритма DES
    - перебор по всему ключевому пространству
    - разложение числа на сложные множители
    - разложение числа на простые множители
    - перебор по выборочному ключевому пространству

Компетенции ОК 01, ОК 02, ОК 03, ОК 04, ОК 05, ОК 06, ПК 3.5

21. Наукой, изучающей математические методы защиты информации путем ее преобразования, является
- криптология
- криптоанализ
- стеганография
- криптография

22. Недостатком модели конечных состояний политики безопасности является
- сложность реализации
- изменение линий связи
- статичность
- низкая степень надежности

23. Недостаток систем шифрования с открытым ключом
- относительно низкая производительность
- необходимость распространения секретных ключей
- при использовании простой замены легко произвести подмену одного шифрованного текста другим
- на одном и том же ключе одинаковые 64-битные блоки открытого текста перейдут в одинаковые блоки шифрованного текста

24. Обеспечение целостности информации в условиях случайного воздействия изучается
- теорией помехоустойчивого кодирования
- криптологией
- стеганографией
- криптоанализом

25. Организационные требования к системе защиты
- административные и процедурные
- управленческие и идентификационные
- административные и аппаратурные
- аппаратурные и физические

26. Основу политики безопасности составляет
- способ управления доступом
- программное обеспечение
- управление риском
- выбор каналов связи

27. По документам ГТК количество классов защищенности АС от НСД
- 9
- 6
- 8
- 7

28. По документам ГТК самый высокий класс защищенности СВТ от НСД к информации
- 1
- 9
- 7
- 6

29. Позволяет получать доступ к информации, перехваченной другими программными закладками, модель воздействия программных закладок типа
- компрометация
- уборка мусора
- наблюдение
- перехват

30. При избирательной политике безопасности в матрице доступа на пересечении столбца и строки указывается
- тип разрешенного доступа
- объект системы
- субъект системы
- факт доступа

3.3. Примерные задания теста по МДК 03.02 к экзамену

Компетенции ОК 01, ОК 02, ОК 03, ОК 04, ОК 08, ОК 09, ОК10, ОК11, ПК 3.5

1. Из перечисленного: 1) анализ потенциального злоумышленника; 2) оценка возможных затрат; 3) оценка возможных потерь; 4) анализ потенциальных угроз — процесс анализа рисков при разработке системы защиты ИС включает

o 3, 4
o 2, 4
o 1, 3
o 1, 2

2. Из перечисленного: 1) занижение уровня секретности; 2) завышение уровня секретности; 3) запись вслепую; 4) лишняя запись; 5) удаленная запись; 6) привилегированные субъекты — проблемами модели Белла-ЛаПадула являются
- 2, 3, 5, 6
- 2, 3, 4
- 4, 5, 6
- 1, 2, 3, 4

3. Из перечисленного: 1) объект; 2) множество; 3) операция; 4) контейнер — в модели политики безопасности Лендвера сущностью могут являться
- 1, 4
- 3, 4
- 1, 2
- 2, 3

4. Из перечисленного: 1) оповещение о попытках нарушения защиты; 2) идентификация; 3) аутентификация; 4) учет носителей информации; 5) управление потоками информации — подсистема управления доступом системы защиты информации должна обеспечивать
- 2, 3, 5
- 1, 2, 5
- 3, 4, 5
- 1, 2, 3

5. Из перечисленного: 1) привилегированная; 2) избирательная; 3) полномочная; 4) оптимальная; 5) минимальная; 6) максимальная — видами политики безопасности являются
- 2, 3
- 2, 3, 4
- 4, 5, 6
- 1, 2, 3

6. Из перечисленного: 1) протоколирование; 2) тестирование программ; 3) аутентификация; 4) обработка угроз; 5) резервное копирование — группами требований к документированию системы защиты информации являются
- 1, 2, 4
- 2, 3, 4
- 3, 4, 5
- 1, 2, 3

7. Из перечисленного: 1) случайная; 2) преднамеренная; 3) стихийная; 4) детерминированная; 5) объективная; 6) субъективная — угрозы безопасности по природе происхождения классифицируются как
- 1, 2
- 1, 2, 3, 4
- 5, 6
- 3, 4

8. Из перечисленного: 1) технические; 2) общие; 3) организационные; 4) конкретные; 5) программные — группами требований к системам защиты информации являются
- 2, 3, 4
- 1, 2, 4
- 3, 4, 5
- 1, 2, 3

9. Из перечисленных категорий требований безопасности: 1) политика безопасности; 2) аудит; 3) идентификация ; 4) корректность; 5) аутентификация — в «Оранжевой книге» предложены
- 1, 2, 4
- 1, 2, 5
- 3, 4, 5
- 1, 2, 3

10. Из перечисленных множеств: 1) установленные полномочия; 2) пользователи; 3) терминалы; 4) операции; 5) программы; 6) ресурсы — модель безопасности Хартстона описывается множествами
- o 1, 2, 4, 6
- o 2, 4, 6
- o 4, 5, 6
- o 1, 2, 3, 4

11. Из перечисленных моделей: 1) Адепт-50; 2) игровая; 3) Хартстона; 4) с полным перекрытием; 5) Белла-ЛаПадула; 6) LWM — моделями политики безопасности на основе дискретных компонент являются
- o 1, 3
- o 1, 3, 5
- o 4, 5, 6
- o 1, 2, 3

Компетенции ОК 01, ОК 05, ОК 06, ОК 07, ОК 08, ОК 09, ОК10, ОК11, ПК 3.5

12. Из перечисленных предположений о: 1) категориях лиц; 2) мотивах; 3) квалификации; 4) возможных потерях; 5)возможных путях реализации угроз — при разработке модели нарушителя ИС определяются
- o 1, 2, 3
- o 1, 2, 4
- o 1, 3, 5
- o 3, 4, 5

13. Из перечисленных разделов: 1) симметричные криптосистемы; 2) криптосистемы с открытым ключом; 3) асимметричные криптосистемы; 4) системы электронной подписи; 5) стеганография; 6) управление ключами — криптография включает
- o 1, 2, 4, 6
- o 2, 4, 6
- o 4, 5, 6
- o 1, 2, 3

14. Из перечисленных типов: 1) перехватчики; 2) имитаторы; 3) наблюдатели; 4) фильтры; 5) заместители — все клавиатурные шпионы делятся на
- o 2, 4, 5
- o 1, 3, 4
- o 2, 3, 4
- o 1, 2, 3, 5

15. Из перечисленных уровней безопасности: 1) базовый; 2) низкий; 3) средний; 4) стандартный; 5) высокий — в «Европейских критериях» определены
- o 1, 3, 5
- o 2, 3, 5
- o 2, 3, 4
- o 1, 2, 5

16. Класс F-DC согласно «Европейским критериям» характеризуется повышенными требованиями к
- o Конфиденциальности
- o обеспечению работоспособности
- o унификации
- o адекватности

17. Из перечисленного: 1) идентификация и аутентификация; 2) регистрация и учет; 3) непрерывность защиты; 4) политика безопасности — согласно «Оранжевой книге» требованиями в области аудита являются
- o 1, 2
- o 2, 4
- o 1, 3
- o 3, 4

18. Из перечисленного: 1) оповещение о попытках нарушения защиты; 2) идентификация; 3) аутентификация; 4) учет носителей информации; 5) управление потоками информации — подсистема регистрации и учета системы защиты информации должна обеспечивать

- o 1, 4
- o 3, 4
- o 1, 2
- o 2, 3

19. Из перечисленного: 1) перехват; 2) искажение; 3) внедрение; 4) захват ресурсов; 5) уборка мусора; 6) наблюдение и компрометация — различают модели воздействия программных закладок на компьютеры
- o 1, 2, 5, 6
- o 1, 2, 3
- o 4, 5, 6
- o 1, 2, 3, 6

Компетенции ОК 01, ОК 02, ОК 03, ОК 04, ОК 05, ОК 06, ПК 3.5

20. Из перечисленного: 1) простая замена с обратной связью; 2) простая замена; 3) гаммирование; 4) гаммирование с обратной связью; 5) выработка имитовставки; 6) электронная кодированная книга — ГОСТ 28147-89 используется в режимах
- o 2, 3, 4, 5
- o 1, 3, 5, 6
- o 1, 2, 3, 4
- o 1, 4, 5, 6

21. Из перечисленного: 1) случайная; 2) преднамеренная; 3) объективная; 4) субъективная; 5) стихийная; 6) детерминированная — угрозы безопасности по предпосылкам появления классифицируются как
- o 3, 4
- o 1, 2, 3, 4
- o 5, 6
- o 1, 2

22. Из перечисленного: 1) степень прогнозируемости; 2) природа происхождения; 3) предпосылки появления; 4) источники угроз; 5) размер ущерба — параметрами классификации угроз безопасности информации являются
- o 2, 3, 4
- o 1, 5
- o 3, 4, 5
- o 1, 2, 3

23. Из перечисленного: 1) эффективность; 2) корректность; 3) унификация; 4) конфиденциальность — аспектами адекватности средств защиты являются
- o 1, 2
- o 2, 4
- o 1, 3
- o 3, 4

24. Из перечисленных классов: 1) обнаруживаемые операционной системой при загрузке; 2) качественные и визуальные; 3) аппаратные; 4) обнаруживаемые средствами тестирования и диагностики — признаки присутствия программной закладки в компьютере можно разделить на
- o 2, 4
- o 1, 3
- o 2, 3
- o 1, 4

25. Из перечисленных моделей: 1) Адепт-50; 2) игровая; 3) Хартстона; 4) с полным перекрытием; 5) Белла-ЛаПадула; 6) LWM — моделями политики безопасности на основе анализа угроз системе являются
- o 2, 4
- o 2, 4, 6
- o 4, 5, 6
- o 1, 2, 3

26. Из перечисленных моделей: 1) Лендвера; 2) игровая; 3) Хартстона; 4) с полным перекрытием; 5) Белла-ЛаПадула; 6) LWM — моделями политики безопасности на основе конечных состояний являются
- o 1, 5, 6

- o 1, 2, 6
- o 4, 5, 6
- o 1, 2, 3

27. Из перечисленных программных закладок: 1) вирусные; 2) троянские; 3) программно-аппаратные; 4) загрузочные; 5) драйверные; 6) прикладные — по методу внедрения в компьютерную систему различают

- o 3, 4, 5, 6
- o 1, 2, 3, 6
- o 2, 3, 4, 5
- o 1, 2, 4, 6

28. Из перечисленных свойств: 1) конфиденциальность; 2) восстанавливаемость; 3) доступность; 4) целостность; 5) детерминированность — безопасная система обладает

- o 1, 3, 4
- o 1, 3, 5
- o 2, 4, 5
- o 1, 2, 3

29. Из перечисленных требований: 1) резервное копирование; 2) аутентификация; 3) необходимость записи всех движений защищаемых данных; 4) накопление статистики — при разработке протоколирования в системе защиты учитываются

- o 3, 4
- o 1, 4
- o 2, 3
- o 1, 2

3.4. Соответствие между бальной системой и системой оценивания по результатам тестирования устанавливается посредством следующей таблицы:

Объект оценки	Показатели оценивания результатов обучения	Оценка	Уровень результатов обучения
Обучающийся	60 баллов и менее	«Не удовлетворительно»	Низкий уровень
	74 – 61 баллов	«Удовлетворительно»	Пороговый уровень
	84 – 75 баллов	«Хорошо»	Повышенный уровень
	100 – 85 баллов	«Отлично»	Высокий уровень

4. Оценка ответа обучающегося на вопросы.

4.1 Оценка ответа обучающегося на вопросы при защите курсового проекта

Элементы оценивания	Содержание шкалы оценивания			
	Неудовлетворительно	Удовлетворительно	Хорошо	Отлично
Соответствие содержания КП методике расчета (исследования)	Полное несоответствие содержания КП поставленным целям или их отсутствие	Значительные погрешности	Незначительные погрешности	Полное соответствие
Качество обзора литературы	Недостаточный анализ	Отечественная литература	Современная отечественная литература	Новая отечественная и зарубежная литература
Творческий характер КП, степень самостоятельности в разработке	Работа в значительной степени не является самостоятельной	В значительной степени в работе использованы выводы, выдержки из других авторов без ссылок на них	В ряде случае отсутствуют ссылки на источник информации	Полное соответствие критерию
Использование современных информационных технологий	Современные информационные технологии, вычислительная техника не были использованы	Современные информационные технологии, вычислительная техника использованы слабо. Допущены	Имеют место небольшие погрешности в использовании современных информационных технологий,	Полное соответствие критерию

		серьезные ошибки в расчетах	вычислительной техники	
Качество графического материала в КП	Не раскрывают смысл работы, небрежно оформлено, с большими отклонениями от требований ГОСТ, ЕСКД и др.	Не полностью раскрывают смысл, есть существенные погрешности в оформлении	Не полностью раскрывают смысл, есть погрешность в оформлении	Полностью раскрывают смысл и отвечают ГОСТ, ЕСКД и др.
Грамотность изложения текста КП	Много стилистических и грамматических ошибок	Есть отдельные грамматические и стилистические ошибки	Есть отдельные грамматические ошибки	Текст КП читается легко, ошибки отсутствуют
Соответствие требованиям, предъявляемым к оформлению КП	Полное не выполнение требований, предъявляемых к оформлению	Требования, предъявляемые к оформлению КП, нарушены	Допущены незначительные погрешности в оформлении КП	КП соответствует всем предъявленным требованиям
Качество доклада	В докладе не раскрыта тема КП, нарушен регламент	Не соблюден регламент, недостаточно раскрыта тема КП	Есть ошибки в регламенте и использовании чертежей	Соблюдение времени, полное раскрытие темы КП
Качество ответов на вопросы	Не может ответить на дополнительные вопросы	Знание основного материала	Высокая эрудиция, нет существенных ошибок	Ответы точные, высокий уровень эрудиции

4.2. Оценка ответа обучающегося на вопросы к другим формам промежуточной аттестации и экзамену.

Элементы оценивания	Содержание шкалы оценивания			
	Не удовлетворительно	Удовлетворительно	Хорошо	Отлично
Соответствие ответов формулировкам вопросов (заданий)	Полное несоответствие по всем вопросам	Значительные погрешности	Незначительные погрешности	Полное соответствие
Структура, последовательность и логика ответа. Умение четко, понятно, грамотно и свободно излагать свои мысли	Полное несоответствие критерию.	Значительное несоответствие критерию	Незначительное несоответствие критерию	Соответствие критерию при ответе на все вопросы.
Знание нормативных, правовых документов и специальной литературы	Полное незнание нормативной и правовой базы и специальной литературы	Имеют место существенные упущения (незнание большей части из документов и специальной литературы по названию, содержанию и т.д.).	Имеют место несущественные упущения и незнание отдельных (единичных) работ из числа обязательной литературы.	Полное соответствие данному критерию ответов на все вопросы.
Умение увязывать теорию с практикой, в том числе в области профессиональной работы	Умение связать теорию с практикой работы не проявляется.	Умение связать вопросы теории и практики проявляется редко.	Умение связать вопросы теории и практики в основном проявляется.	Полное соответствие данному критерию. Способность интегрировать знания и привлекать сведения из различных научных сфер
Качество ответов на дополнительные вопросы	На все дополнительные вопросы преподавателя даны неверные ответы.	Ответы на большую часть дополнительных вопросов преподавателя даны неверно.	1. Даны неполные ответы на дополнительные вопросы преподавателя. 2. Дан один неверный ответ на дополнительные вопросы преподавателя.	Даны верные ответы на все дополнительные вопросы преподавателя.

Примечание: итоговая оценка формируется как средняя арифметическая результатов элементов оценивания.

ПМ.03 Защита информации техническими средствами

1. Описание показателей, критериев и шкал оценивания компетенций.

1.1. Показатели и критерии оценивания компетенций ОК 01, ОК 02, ОК 03, ОК 04, ОК 05, ОК 06, ОК 07, ОК 08, ОК 09, ОК10, ОК11, ПК 3.1, ПК 3.2, ПК 3.3, ПК 3.4, ПК 3.5

Объект оценки	Уровни сформированности компетенций	Критерий оценивания результатов обучения
Обучающийся	Низкий уровень Пороговый уровень Повышенный уровень Высокий уровень	Уровень результатов обучения **не ниже порогового**

1.2. Шкалы оценивания компетенций ОК 01, ОК 02, ОК 03, ОК 04, ОК 05, ОК 06, ОК 07, ОК 08, ОК 09, ОК10, ОК11, ПК 3.1, ПК 3.2, ПК 3.3, ПК 3.4, ПК 3.5 при сдаче квалификационного экзамена

Достигнутый уровень результата обучения	Характеристика уровня сформированности компетенций	Шкала оценивания
		Экзамен
Низкий уровень	Обучающийся: -обнаружил пробелы в знаниях основного учебно-программного материала; -допустил принципиальные ошибки в выполнении заданий, предусмотренных программой; -не может продолжить обучение или приступить к профессиональной деятельности по окончании программы без дополнительных занятий по соответствующей дисциплине.	Неудовлетворительно
Пороговый уровень	Обучающийся: -обнаружил знание основного учебно-программного материала в объёме, необходимом для дальнейшей учебной и предстоящей профессиональной деятельности; -справляется с выполнением заданий, предусмотренных программой; -знаком с основной литературой, рекомендованной рабочей программой дисциплины; -допустил неточности в ответе на вопросы и при выполнении заданий по учебно-программному материалу, но обладает необходимыми знаниями для их устранения под руководством преподавателя.	Удовлетворительно
Повышенный уровень	Обучающийся: - обнаружил полное знание учебно-программного материала; -успешно выполнил задания, предусмотренные программой; -усвоил основную литературу, рекомендованную рабочей программой дисциплины; -показал систематический характер знаний учебно-программного материала; -способен к самостоятельному пополнению знаний по учебно-программному материалу и обновлению в ходе дальнейшей учебной работы и профессиональной деятельности.	Хорошо
Высокий уровень	Обучающийся: -обнаружил всесторонние, систематические и глубокие знания учебно-программного материала; -умеет свободно выполнять задания, предусмотренные программой; -ознакомился с дополнительной литературой; -усвоил взаимосвязь основных понятий дисциплин и их значение для приобретения профессии; -проявил творческие способности в понимании учебно-программного материала.	Отлично

1.3. Описание шкал оценивания

Компетенции обучающегося оценивается следующим образом:

Планируемый уровень результатов освоения	Содержание шкалы оценивания достигнутого уровня результата обучения			
	Неудовлетворительно	Удовлетворительно	Хорошо	Отлично
Знать	Неспособность обучающегося самостоятельно продемонстрировать наличие знаний при решении заданий, которые были представлены преподавателем вместе с образцом их решения.	Обучающийся способен самостоятельно продемонстрировать наличие знаний при решении заданий, которые были представлены преподавателем вместе с образцом их решения.	Обучающийся демонстрирует способность к самостоятельному применению знаний при решении заданий, аналогичных тем, которые представлял преподаватель, и при его консультативной поддержке в части современных проблем.	Обучающийся демонстрирует способность к самостоятельному применению знаний в выборе способа решения неизвестных или нестандартных заданий и при консультативной поддержке в части междисциплинарных связей.
Уметь	Отсутствие у обучающегося самостоятельности в применении умений по использованию методов освоения учебной дисциплины.	Обучающийся демонстрирует самостоятельность в применении умений решения учебных заданий в полном соответствии с образцом, данным преподавателем.	Обучающийся продемонстрирует самостоятельное применение умений решения заданий, аналогичных тем, которые представлял преподаватель, и при его консультативной поддержке в части современных проблем.	Обучающийся демонстрирует самостоятельное применение умений решения неизвестных или нестандартных заданий и при консультативной поддержке преподавателя в части междисциплинарных связей.
Иметь практический опыт	Неспособность самостоятельно проявить навык решения поставленной задачи по стандартному образцу повторно.	Обучающийся демонстрирует самостоятельность в применении навыка по заданиям, решение которых было показано преподавателем.	Обучающийся демонстрирует самостоятельное применение навыка решения заданий, аналогичных тем, которые представлял преподаватель, и при его консультативной поддержке в части современных проблем.	Обучающийся демонстрирует самостоятельное применение навыка решения неизвестных или нестандартных заданий и при консультативной поддержке преподавателя в части междисциплинарных связей.

Примерный перечень вопросов к квалификационному экзамену по ПМ.03.

Компетенции ОК 01, ОК 02, ОК 6, ОК 7, ОК 8, ПК 3.1, ПК 3.2, ПК 3.3

1. Принципы системного анализа проблем инженерно-технической защиты информации.
2. Классификация способов и средств защиты информации.
3. Особенности информации как предмета защиты.
4. Свойства информации.
5. Виды, источники и носители защищаемой информации.
6. Прослушивание информации направленными микрофонами.
7. Электронные стетоскопы.
8. Лазерные системы подслушивания.
9. Гидроакустические преобразователи.
10. Системы защиты информации от утечки по вибрационному каналу.

Компетенции ОК 01, ОК 02, ОК 03, ОК 04, ОК 05, ПК 3.3, ПК 3.4

11. Структура канала утечки информации. Характеристика каналов утечки информации.
12. Классификация существующих физических полей и технических каналов утечки информации.
13. Радиоэлектронные каналы утечки информации, характеристика.
14. Оптический канал утечки информации, характеристика.
15. Прослушивание информации от радиотелефонов.
16. Прослушивание информации от работающей аппаратуры.
17. Прослушивание информации от радиозакладок.

18. Прослушивание информации от пассивных закладок.
19. Системы защиты от утечки по электромагнитному каналу.

Компетенции ОК 01, ОК 02, ОК 03, ОК 04, ОК 05, ОК 09, ОК10, ОК11, ПК 3.1, ПК 3.2, ПК 3.3

20. Технические средства акустической разведки.
21. Технические средства для уничтожения информации и носителей информации, порядок применения.
22. Этапы эксплуатации технических средств защиты информации.
23. Установка и настройка технических средств защиты информации.
24. Классификация демаскирующих признаков
25. Телевизионные системы наблюдения. Приборы ночного видения.
26. Защита информации от несанкционированной утечки по электросетевому каналу.
27. Защита информации от несанкционированной утечки по проводному каналу.

Компетенции ОК 01, ОК 02, ОК 03, ОК 04, ОК 08, ОК 09, ОК10, ОК11, ПК 3.5

28. Виды информации, защищаемой техническими средствами.
29. Свойства информации, как предмета защиты.
30. Определение и классификация демаскирующих признаков объектов.
31. Видовые демаскирующие признаки объекта, признаки веществ.
32. Понятие об информационных сигналах и их источники.
33. Основные и вспомогательные технические средства и системы.
34. Классификация и принципы действия акустических преобразователей.
35. Побочные высокочастотные и низкочастотные излучения технических средств.
36. Утечка информации по цепям электропитания и заземления
37. Виды угроз безопасности информации.
38. Основные задачи и типовая структура разведки.
39. Классификация органов технической разведки.
40. Утечка информации. Типовая структура технического канала утечки информации.
41. Классификация технических каналов утечки информации.
42. Характеристики и комплексное использование технических каналов утечки информации.
43. Возможности и классификация оптических каналов утечки информации.
44. Структура оптического канала утечки информации.
45. Назначение, принципы работы, характеристики средств наблюдения (оптические приборы, фото и киноаппараты, приборы ночного видения).
46. Системы обнаружения оптических устройств.

Компетенции ОК 01, ОК 05, ОК 06, ОК 07, ОК 08, ОК 09, ОК10, ОК11, ПК 3.4, ПК 3.5

47. Средства противодействия утечки информации по оптическим каналам.
48. Структура и виды радиоэлектронных каналов утечки информации.
49. Классификация и особенности распространения радиоволн.
50. Распространение информативных сигналов в радиоэлектронных каналах утечки информации.
51. Классификация помех.
52. Характер распространения звука в различных средах. Реверберация.
53. Структура акустического канала утечки информации.
54. Виды акустических каналов утечки информации.
55. Структура вещественных каналов утечки информации.
56. Демаскирующие признаки веществ.
57. Методы добывания информации о вещественных признаках.
58. Задачи и принципы инженерно-технической защиты информации.
59. Классификация методов инженерно-технической защиты информации.
60. Характеристика методов физической защиты информации.
61. Структура системы инженерной защиты и охраны объектов.
62. Средства инженерной защиты объектов.
63. Структура комплексов управления и доступом людей и транспорта.
64. Способы идентификации людей.
65. Классификация извещателей.

Компетенции ОК 01, ОК 02, ОК 03, ОК 04, ОК 05, ОК 06, ПК 3.5

66. Средства контроля и управления средствами охраны.
67. Состав и структура системы видеоконтроля.
68. Назначение и характеристики составных частей системы видеоконтроля.
69. Принцип работы детектора движения.

70. Структурное скрытие речевой информации в телефонных каналах связи.
71. Энергетическое скрытие акустического сигнала.
72. Характеристики и классификация закладных устройств.
73. Демаскирующие признаки закладных устройств. Способы маскировки закладных устройств.
74. Средства поиска излучающих закладных устройств.
75. Средства поиска неизлучающих закладных устройств.
76. Средства и способы подавления закладных устройств.
77. Акустические преемники их структура и характеристики.
78. Характеристики и классификация микрофонов.
79. Конструкция и работа микрофонов по принципу действия.
80. Характеристики направленности микрофонов.
81. Конструкция и работа остронаправленных микрофонов.
82. Диктофоны, средства лазерного подслушивания.
83. Добывание информации путем высокочастотного навязывания.
84. Экранирование электромагнитных полей.
85. Экранирование электрических проводов.
86. Компенсация полей.
87. Средства экранирования электромагнитных полей

Образец экзаменационного билета по ПМ.03

<table>
<tr><td colspan="3">Дальневосточный государственный университет путей сообщения</td></tr>
<tr><td>ПЦК
Информационная безопасность автоматизированных систем
название
_____
семестр, учебный год</td><td>Экзаменационный билет №
по ПМ.03 Защита информации техничсекими средствами
название
для направления подготовки/специальности
10.02.05 Обеспечение информационной безопасности автоматизированных систем
код, название
технический
профиль/специализация</td><td>«Утверждаю»
Председатель ПЦК
_____
ФИО
«___» _____ 20 __ г.</td></tr>
<tr><td colspan="3">1. Радиоэлектронные каналы утечки информации, характеристика. (ОК 01, ОК 02, ОК 03, ОК 04, ОК 05, ПК 3.3, ПК 3.4)</td></tr>
<tr><td colspan="3">2. Технические средства акустической разведки. ОК 01, ОК 02, ОК 03, ОК 04, ОК 05, ОК 09, ОК10, ОК11, ПК 3.1, ПК 3.2, ПК 3.3</td></tr>
<tr><td colspan="3">3. Классификация извещателей. (ОК 01, ОК 05, ОК 06, ОК 07, ОК 08, ОК 09, ОК10, ОК11, ПК 3.5)</td></tr>
</table>

3. Тестовые задания. Оценка по результатам тестирования.

3.1. Примерные задания теста по ПМ 03.
Компетенции ОК 01, ОК 02, ОК 6, ОК 7, ОК 8, ПК 3.1, ПК 3.2, ПК 3.3

1. Особенностью речевых сообщений является …

- виртуальность
- документальность
- конфиденциальность
- целостность

2. К демаскирующим признакам по информативности признаков относятся …

- прямые (дополнительные признаки объекта) [информативность в пределах от 0 до 1]
- именные (однозначно определяющие объект) [информативность =1]
- информационно-психологические
- косвенные (признаки, непосредственно не принадлежащие объекту)
- технические
- физические

3. Основные типы систем обнаружения атак …

- локальные
- сетевые
- программные
- аппаратные

4. К демаскирующим признакам по состоянию объекта относятся …

- опознавательные признаки
- признаки физические
- признаки программные
- признаки деятельности

5. Инженерно-техническая защита решает задачи по предотвращению или уменьшению угроз, вызванных …
- стихийными носителями угроз
- попытками злоумышленников проникнуть к местам хранения источников информации
- организованной или случайной утечкой информации с использованием различных технических средств

6. Контролируемая зона – это …
- территория объекта
- территория объекта, на которой возможно пребывание посторонних лиц
- территория объекта, на которой исключено неконтролируемое пребывание лиц

7. Показателем безопасности информации является …
- время, необходимое на взлом защиты информации
- вероятность предотвращения угрозы
- время, в течение которого обеспечивается определённый уровень безопасности
- вероятность возникновения угрозы информационной безопасности

Компетенции ОК 01, ОК 02, ОК 03, ОК 04, ОК 05, ПК 3.3, ПК 3.4
8. Задачи, поставленные в рамках концепции национальной безопасности приоритетное развитие отечественных современных информационных и телекоммуникационных технологий и …
- ускорение развития новых информационных технологий и их широкое распространение
- установление необходимого баланса между потребностью в свободном обмене информацией и допустимыми ограничениями её распространения
- совершенствование информационной структуры

9. Объектом защиты может являться …
- информационные процессы
- носители информации
- субъект

10. Физические системы защиты подразделяются на:
- системы ограждения и физической изоляции, системы контроля доступа, запирающие устройства и хранилища
- системы ограждения и физической изоляции, запирающие устройства и хранилища
- системы охлаждения, системы этз, запирающие устройства и хранилища

11. Источником информации при утечке по техническим каналам может являться …
- информация, обрабатываемая техническими средствами передачи информации
- видовая информация
- информация, передаваемая по каналам связи
- человек

12. К наиболее важным методам защиты информации от нелегального доступа относится …
- архивирование (создание резервных копий)
- использование специальных «электронных ключей»
- установление паролей на доступ к информации
- использование антивирусных программ
- шифрование

13. К методам выявления технических каналов утечки информации относится …
- инструментальный контроль
- физический поиск
- тестирование

14. Видовая информация – это …
- информация о внутреннем виде объекта разведки или документа, получаемая при помощи технических средств разведки в виде их изображений

- информация о внешнем виде объекта разведки или документа, получаемая при помощи технических средств разведки в виде их изображений
- информация о внешнем виде объекта разведки или документа, получаемая при помощи программных средств разведки в виде их изображений

Компетенции ОК 01, ОК 02, ОК 03, ОК 04, ОК 05, ОК 09, ОК10, ОК11, ПК 3.1, ПК 3.2, ПК 3.3

15. Утечка информации по техническим каналам реализуется в результате …

- подслушивания конфиденциальных разговоров и акустических сигналов
- перехвата различного рода полей и сигналов
- наблюдения за источниками информации
- недостаточной организацией защиты информации

16. Информативность – мера … признака

- объемности
- открытости
- индивидуальности
- показательности

17. При экранировании помещения применяется …

- фтористая сетка
- алюминиевая фольга
- листовая сталь
- медная сетка

18. К демаскирующим признакам по времени проявления признаков относятся …

- эпизодические
- периодические
- долгосрочные
- краткосрочные
- постоянные

19. Акустическая информация – это …

- распространение акустических волн различной формы и длительности, распространяющиеся от источника в окружающее пространство
- звуковые волны
- возмущения упругой среды различной формы и длительности, распространяющиеся от источника в окружающее пространство

Компетенции ОК 01, ОК 02, ОК 03, ОК 04, ОК 08, ОК 09, ОК10, ОК11, ПК 3.5

1. Из перечисленного: 1) анализ потенциального злоумышленника; 2) оценка возможных затрат; 3) оценка возможных потерь; 4) анализ потенциальных угроз — процесс анализа рисков при разработке системы защиты ИС включает

o 3, 4
o 2, 4
o 1, 3
o 1, 2

2. Из перечисленного: 1) занижение уровня секретности; 2) завышение уровня секретности; 3) запись вслепую; 4) лишняя запись; 5) удаленная запись; 6) привилегированные субъекты — проблемами модели Белла-ЛаПадула являются

o 2, 3, 5, 6
o 2, 3, 4
o 4, 5, 6
o 1, 2, 3, 4

3. Из перечисленного: 1) объект ; 2) множество; 3) операция; 4) контейнер — в модели политики безопасности Лендвера сущностью могут являться

o 1, 4
o 3, 4
o 1, 2
o 2, 3

4. Из перечисленного: 1) оповещение о попытках нарушения защиты; 2) идентификация; 3) аутентификация; 4) учет носителей информации; 5) управление потоками информации — подсистема управления доступом системы защиты информации должна обеспечивать
- o 2, 3, 5
- o 1, 2, 5
- o 3, 4, 5
- o 1, 2, 3

5. Из перечисленного: 1) привилегированная; 2) избирательная; 3) полномочная; 4) оптимальная; 5) минимальная; 6) максимальная — видами политики безопасности являются
- o 2, 3
- o 2, 3, 4
- o 4, 5, 6
- o 1, 2, 3

6. Из перечисленного: 1) протоколирование; 2) тестирование программ; 3) аутентификация; 4) обработка угроз; 5) резервное копирование — группами требований к документированию системы защиты информации являются
- o 1, 2, 4
- o 2, 3, 4
- o 3, 4, 5
- o 1, 2, 3

7. Из перечисленного: 1) случайная; 2) преднамеренная; 3) стихийная; 4) детерминированная; 5) объективная; 6) субъективная — угрозы безопасности по природе происхождения классифицируются как
- o 1, 2
- o 1, 2, 3, 4
- o 5, 6
- o 3, 4

8. Из перечисленного: 1) технические; 2) общие; 3) организационные; 4) конкретные; 5) программные — группами требований к системам защиты информации являются
- o 2, 3, 4
- o 1, 2, 4
- o 3, 4, 5
- o 1, 2, 3

9. Из перечисленных категорий требований безопасности: 1) политика безопасности; 2) аудит; 3) идентификация ; 4) корректность; 5) аутентификация — в «Оранжевой книге» предложены
- o 1, 2, 4
- o 1, 2, 5
- o 3, 4, 5
- o 1, 2, 3

10. Из перечисленных множеств: 1) установленные полномочия; 2) пользователи; 3) терминалы; 4) операции; 5) программы; 6) ресурсы — модель безопасности Хартстона описывается множествами
- o 1, 2, 4, 6
- o 2, 4, 6
- o 4, 5, 6
- o 1, 2, 3, 4

11. Из перечисленных моделей: 1) Адепт-50; 2) игровая; 3) Хартстона; 4) с полным перекрытием; 5) Белла-ЛаПадула; 6) LWM — моделями политики безопасности на основе дискретных компонент являются
- o 1, 3
- o 1, 3, 5
- o 4, 5, 6
- o 1, 2, 3

Компетенции ОК 01, ОК 05, ОК 06, ОК 07, ОК 08, ОК 09, ОК10, ОК11, ПК 3.5

12. Из перечисленных предположений о: 1) категориях лиц; 2) мотивах; 3) квалификации; 4) возможных потерях; 5)возможных путях реализации угроз — при разработке модели нарушителя ИС определяются
- 1, 2, 3
- 1, 2, 4
- 1, 3, 5
- 3, 4, 5

13. Из перечисленных разделов: 1) симметричные криптосистемы; 2) криптосистемы с открытым ключом; 3) асимметричные криптосистемы; 4) системы электронной подписи; 5) стеганография; 6) управление ключами — криптография включает
- 1, 2, 4, 6
- 2, 4, 6
- 4, 5, 6
- 1, 2, 3

14. Из перечисленных типов: 1) перехватчики; 2) имитаторы; 3) наблюдатели; 4) фильтры; 5) заместители — все клавиатурные шпионы делятся на
- 2, 4, 5
- 1, 3, 4
- 2, 3, 4
- 1, 2, 3, 5

15. Из перечисленных уровней безопасности: 1) базовый; 2) низкий; 3) средний; 4) стандартный; 5) высокий — в «Европейских критериях» определены
- 1, 3, 5
- 2, 3, 5
- 2, 3, 4
- 1, 2, 5

16. Класс F-DC согласно «Европейским критериям» характеризуется повышенными требованиями к
- Конфиденциальности
- обеспечению работоспособности
- унификации
- адекватности

17. Из перечисленного: 1) идентификация и аутентификация; 2) регистрация и учет; 3) непрерывность защиты; 4) политика безопасности — согласно «Оранжевой книге» требованиями в области аудита являются
- 1, 2
- 2, 4
- 1, 3
- 3, 4

18. Из перечисленного: 1) оповещение о попытках нарушения защиты; 2) идентификация; 3) аутентификация; 4) учет носителей информации; 5) управление потоками информации — подсистема регистрации и учета системы защиты информации должна обеспечивать
- 1, 4
- 3, 4
- 1, 2
- 2, 3

19. Из перечисленного: 1) перехват; 2) искажение; 3) внедрение; 4) захват ресурсов; 5) уборка мусора; 6) наблюдение и компрометация — различают модели воздействия программных закладок на компьютеры
- 1, 2, 5, 6
- 1, 2, 3
- 4, 5, 6
- 1, 2, 3, 6

Компетенции ОК 01, ОК 02, ОК 03, ОК 04, ОК 05, ОК 06, ПК 3.5

20. Из перечисленного: 1) простая замена с обратной связью; 2) простая замена; 3) гаммирование; 4) гаммирование с обратной связью; 5) выработка имитовставки; 6) электронная кодированная книга — ГОСТ 28147-89 используется в режимах
- o 2, 3, 4, 5
- o 1, 3, 5, 6
- o 1, 2, 3, 4
- o 1, 4, 5, 6

21. Из перечисленного: 1) случайная; 2) преднамеренная; 3) объективная; 4) субъективная; 5) стихийная; 6) детерминированная — угрозы безопасности по предпосылкам появления классифицируются как
- o 3, 4
- o 1, 2, 3, 4
- o 5, 6
- o 1, 2

22. Из перечисленного: 1) степень прогнозируемости; 2) природа происхождения; 3) предпосылки появления; 4) источники угроз; 5) размер ущерба — параметрами классификации угроз безопасности информации являются
- o 2, 3, 4
- o 1, 5
- o 3, 4, 5
- o 1, 2, 3

23. Из перечисленного: 1) эффективность; 2) корректность; 3) унификация; 4) конфиденциальность — аспектами адекватности средств защиты являются
- o 1, 2
- o 2, 4
- o 1, 3
- o 3, 4

24. Из перечисленных классов: 1) обнаруживаемые операционной системой при загрузке; 2) качественные и визуальные; 3) аппаратные; 4) обнаруживаемые средствами тестирования и диагностики — признаки присутствия программной закладки в компьютере можно разделить на
- o 2, 4
- o 1, 3
- o 2, 3
- o 1, 4

25. Из перечисленных моделей: 1) Адепт-50; 2) игровая; 3) Хартстона; 4) с полным перекрытием; 5) Белла-ЛаПадула; 6) LWM — моделями политики безопасности на основе анализа угроз системе являются
- o 2, 4
- o 2, 4, 6
- o 4, 5, 6
- o 1, 2, 3

26. Из перечисленных моделей: 1) Лендвера; 2) игровая; 3) Хартстона; 4) с полным перекрытием; 5) Белла-ЛаПадула; 6) LWM — моделями политики безопасности на основе конечных состояний являются
- o 1, 5, 6
- o 1, 2, 6
- o 4, 5, 6
- o 1, 2, 3

27. Из перечисленных программных закладок: 1) вирусные; 2) троянские; 3) программно-аппаратные; 4) загрузочные; 5) драйверные; 6) прикладные — по методу внедрения в компьютерную систему различают
- o 3, 4, 5, 6
- o 1, 2, 3, 6
- o 2, 3, 4, 5
- o 1, 2, 4, 6

28. Из перечисленных свойств: 1) конфиденциальность; 2) восстанавливаемость; 3) доступность; 4) целостность; 5) детерминированность — безопасная система обладает

- o 1, 3, 4
- o 1, 3, 5
- o 2, 4, 5
- o 1, 2, 3

29. Из перечисленных требований: 1) резервное копирование; 2) аутентификация; 3) необходимость записи всех движений защищаемых данных; 4) накопление статистики — при разработке протоколирования в системе защиты учитываются

- o 3, 4
- o 1, 4
- o 2, 3
- o 1, 2

3.2. Соответствие между бальной системой и системой оценивания по результатам тестирования устанавливается посредством следующей таблицы:

Объект оценки	Показатели оценивания результатов обучения	Оценка	Уровень результатов обучения
Обучающийся	60 баллов и менее	«Неудовлетворительно»	Низкий уровень
	74 – 61 баллов	«Удовлетворительно»	Пороговый уровень
	84 – 75 баллов	«Хорошо»	Повышенный уровень
	100 – 85 баллов	«Отлично»	Высокий уровень

4. Оценка ответа обучающегося на вопросы экзаменационного билета.

4.1. Оценка ответа обучающегося на вопросы экзаменационного билета.

Элементы оценивания	Содержание шкалы оценивания			
	Неудовлетворительно	Удовлетворительно	Хорошо	Отлично
Соответствие ответов формулировкам вопросов (заданий)	Полное несоответствие по всем вопросам	Значительные погрешности	Незначительные погрешности	Полное соответствие
Структура, последовательность и логика ответа. Умение четко, понятно, грамотно и свободно излагать свои мысли	Полное несоответствие критерию.	Значительное несоответствие критерию	Незначительное несоответствие критерию	Соответствие критерию при ответе на все вопросы.
Знание нормативных, правовых документов и специальной литературы	Полное незнание нормативной и правовой базы и специальной литературы	Имеют место существенные упущения (незнание большей части из документов и специальной литературы по названию, содержанию и т.д.).	Имеют место несущественные упущения и незнание отдельных (единичных) работ из числа обязательной литературы.	Полное соответствие данному критерию ответов на все вопросы.
Умение увязывать теорию с практикой, в том числе в области профессиональной работы	Умение связать теорию с практикой работы не проявляется.	Умение связать вопросы теории и практики проявляется редко.	Умение связать вопросы теории и практики в основном проявляется.	Полное соответствие данному критерию. Способность интегрировать знания и привлекать сведения из различных научных сфер
Качество ответов на дополнительные вопросы	На все дополнительные вопросы преподавателя даны неверные ответы.	Ответы на большую часть дополнительных вопросов преподавателя даны неверно.	1. Даны неполные ответы на дополнительные вопросы преподавателя. 2. Дан один неверный ответ на дополнительные вопросы преподавателя.	Даны верные ответы на все дополнительные вопросы преподавателя.

Примечание: итоговая оценка формируется как средняя арифметическая результатов элементов оценивания.