МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное бюджетное образовательное учреждение
высшего образования «Кабардино-Балкарский государственный университет
им. Х.М. Бербекова» (КБГУ)

ИНСТИТУТ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА И ЦИФРОВЫХ ТЕХНОЛОГИЙ

КАФЕДРА КОМПЬЮТЕРНЫХ ТЕХНОЛОГИЙ И ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

СОГЛАСОВАНО

Руководитель образовательной программы
_____А.С. Ксенофонтов

«30» мая 2023 г.

УТВЕРЖДАЮ

Директор ИИИиЦТ
_____А.Х. Шапсигов

«30» мая 2023 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

«КОМПЛЕКСНАЯ СИСТЕМА ЗАЩИТЫ ИНФОРМАЦИИ НА ПРЕДПРИЯТИИ»

Направление подготовки (специальность)
10.03.01 – Информационная безопасность

Профиль подготовки:
«Организация и технология защиты информации»

Квалификация (степень) выпускника
Бакалавр

Форма обучения
очная

Нальчик 2023

Рабочая программа дисциплины «Комплексная система защиты информации на предприятии» / сост. доцент А.С. Ксенофонтов – Нальчик: ФГБОУ КБГУ, 2023. – 24 с.

Рабочая программа предназначена для преподавания дисциплины вариативной части студентам очной формы обучения по направлению подготовки 10.03.01 Информационная безопасность в 8 семестре.

Рабочая программа составлена с учетом Федерального государственного образовательного стандарта высшего образования по направлениям подготовки 10.03.01 Информационная безопасность, утвержденному приказом Министерства образования и науки Российской Федерации от 17 ноября 2020 г. N 1427, зарегистрированного в Минюсте России 18 февраля 2021 г. N 62548.

СОДЕРЖАНИЕ

Содержание

1. Цель и задачи освоения дисциплины (модуля)

Цель дисциплины: формирование компетентности в области разработки комплексной системы защиты информации предприятия, на основе оценки угроз безопасности информации, способов моделирования, технологии организации, кадрового, технологического и нормативно-методического обеспечения, методах оценки эффективности подобных систем.

Задачи дисциплины:

- изучение сущности, целей и задач комплексной системы защиты информации;
- изучение принципов и этапов разработки комплексной системы защиты информации;
- освоение технологии установления состава защищаемой информации и объектов защиты информации на предприятии;
- овладение методами оценки угроз безопасности информации;
- изучение параметров и структуры комплексной системы защиты информации;
- установление состава мероприятий по обеспечению функционирования комплексной системы защиты информации;
- изучение показателей и методик эффективности системы защиты информации.

2. Место дисциплины (модуля) в структуре ОПОП ВО

Дисциплина включена в базовую часть обязательных дисциплин учебного плана по направлению подготовки 10.03.01 Информационная безопасность профиль: Организация и технология защиты информации.

Изучение базируется на следующих дисциплинах: «Физика», «Матанализ», «Дискретная математика», « Инженерно-техническая защита информации».

Дисциплина «Комплексная система защиты информации на предприятии» является дисциплиной профессионального цикла и является опорой для подготовки выпускной квалификационной работы.

3. Требования к результатам освоения дисциплины (модуля)

Процесс изучения дисциплины направлен на формирование элементов следующих компетенций в соответствии с ФГОС ВО и ОПОП ВО по данному направлению подготовки:

общепрофессиональные компетенции (ОПК):

способен осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических документов в целях решения задач профессиональной деятельности *(ОПК-8):*

способен проводить подготовку исходных данных для проектирования подсистем, средств обеспечения защиты информации и для технико-экономического обоснования соответствующих проектных решений *(ОПК-12)*;

профессиональные компетенции (ПКС):

способен управлять полномочиями пользователей (ПКС-2.3):

способен выработать рекомендации для принятия решения о модернизации системы за-щиты информации (ПКС-4.3).

В результате освоения дисциплины студент должен:

знать:

- понятие, сущность, цели и задачи комплексной системы защиты информации;
- принципы организации и этапы разработки комплексной системы защиты информации;
- факторы, влияющие на организацию комплексной системы защиты информации;

- технологию определения состава защищаемой информации и объектов защиты;
- методы моделирования, анализа и оценки угроз защищаемой информации;
- виды моделей, описывающих процессы защиты информации;
- содержание технологического и организационного построения системы защиты информации на предприятии;
- состав мероприятий и условия, обеспечивающие функционирование системы защиты информации на предприятии;
- порядок кадрового, материально-технического и нормативно-методического обеспечения защиты информации на предприятии;
- порядок организации планирования и контроля комплексной системы защиты информации на предприятии;
- методику анализа эффективности системы защиты информации;
- порядок организации аттестации объектов информатизации по требованиям безопасности информации;

уметь:

- классифицировать защищаемую информацию по видам тайны и степеням конфиденциальности;
- классифицировать и оценивать угрозы информационной безопасности для объекта информатизации;
- формировать комплекс мер по защите информации на предприятии и оценивать их эффективность на основе заданных требований по безопасности информации;
- разрабатывать проекты нормативных и организационно-распорядительных документов, регламентирующих работу по защите информации на предприятии;

владеть:

- методиками проверки защищенности объектов информатизации на соответствие требованиям безопасности информации;
- технологией разработки организационно-функциональной структуры и комплекса нормативно-методического обеспечения комплексной защиты информации на предприятии.

4. Содержание и структура дисциплины (модуля)

В таблице 1 приводится описание содержания дисциплины, структурированное по разделам, с указанием по каждому разделу формы текущего контроля: защита лабораторной работы (ЛР), коллоквиум (К), рубежный контроль (РК), тестирование (Т).

Таблица 1

№	Наименование раздела	Содержание раздела	Код контролируемой компетенции (или ее части)	Форма текущего контроля
1	**Модуль 1. Концептуальные основы разработки комплексной системы защиты информации и определения объектов защиты Раздел 1. Концептуальные**	**Тема 1. Введение в дисциплину. Сущность комплексной системы защиты информации и принципы ее организации.** Цель, задачи дисциплины, значение ее для подготовки специалиста. Знания и умения студентов, которые должны быть получены в результате ее изучения. Понятие, сущность и назначение комплексной системы защиты информации, ее задачи для обеспечения деятельности предприятия. Принципы организации комплексной системы защиты	*ОПК-8*	(К), (РК), (Т), (ЛР)

	основы разработки комплексной системы защиты информации и определения объектов защиты	информации.		
		Тема 2. Методологические и концептуальные основы комплексной системы защиты информации. Методология защиты информации и ее основные задачи. Уровень обеспечения безопасности информации. Достаточность защиты информации. Варианты построения комплексной системы защиты. Основные факторы, влияющие на организацию комплексной системы защиты информации. Характер и степень влияния различных факторов на организацию системы защиты информации.	*ОПК-12*	(К), (РК), (Т), (ЛР)
		Тема 3. Определение и нормативное закрепление информации ограниченного доступа. Классификация информации по видам тайны и степеням конфиденциальности. Этапы работы по выявлению состава защищаемой информации. Нормативное закрепление состава защищаемой информации. Порядок организации нормативного закрепления информации ограниченного доступа.	*ОПК-12*	(К), (РК), (Т), (ЛР)
		Тема 4. Определение состава объектов защиты. Понятие объекта защиты. Последо-вательность определения объекта защиты. Значение носителей защищаемой информации как объектов защиты. Факторы, определяющие состав носителей информации. Сущность защищаемого объекта информатизации. Методика выявления состава носителей защищаемой информации. Основные и вспомогательные технические средства, и системы. Особенности помещений как объектов защиты.	ПКС-4.3	(К), (РК), (Т), (ЛР)
2	**Модуль 2. Моделирование угроз безопасности информации и процессов защиты информации на предприятии. Раздел 2. Моделирование угроз безопасности информации и процессов защиты информации на предприятии.**	**Тема 5. Источники, способы и результаты дестабилизирующего воздействия на информацию.** Определение источников дестабилизирующего воздействия на информацию. Модель формирования множества дестабилизирующих факторов. Понятие угрозы безопасности информации. Базовая модель угроз безопасности информации. Классификация угроз безопасности информации для объекта информатизации. Анализ и оценка угроз информационной безопасности объекта.	*ОПК-8* ПКС-2.3 ПКС-4.3	(К), (РК), (Т), (ЛР)
		Тема 6. Выявление каналов утечки н методов несанкционированного воздействия па информацию. Сущность утечки информации и несанкционированного воздействия на информацию. Структурная модель канала утечки информации. Технические каналы утечки информации и их классификация. Модель технических	ПКС-4.3	(К), (РК), (Т), (ЛР)

		каналов утечки информатизации на типовом объекте информатизации. Каналы утечки из-за несанкционированного воздействия на информацию на системы, использующие информационно - коммуникационные технологии. Инсайдерские каналы утечки информации и «социальный инжиниринг» Методы «социального инжиниринга»		
		Тема 7. Моделирование процессов защиты информации. Понятие модели и объекта моделирования. Основные виды моделей и их характеристика. Задачи и этапы моделирования в процессе построения комплексной системы защиты информации. Понятие архитектуры системы защиты информации. Кибернетическая, функциональная, информационная и организационная модели комплексной системы защиты информации. Формальные модели безопасности. Теории и методы моделирования процессов защиты информации.	ПКС-4.3	(К), (РК), (Т), (ЛР)
	Модуль 2. Особенности построения комплексной системы защиты информации предприятия и оценка ее эффективности. Раздел 3. Особенности построения комплексной системы защиты информации предприятия и оценка ее эффективности	**Тема 8. Технологическое и организационное построение комплексной системы защиты информации.** Общее содержание работ по организации комплексной системы защиты информации. Характеристика технологического и организационного направлений создания комплексной системы защиты информации. Содержание стадий построения комплексной системы защиты информации. Предпроектное обследование. Назначение и структура технического задания, технико-экономического обоснования. Технический проект, рабочий проект. Апробация системы защиты информации и ввод ее в эксплуатацию.	*ОПК-8 ОПК-12*	
		Тема 9. Кадровое, материально-техническое и нормативно-методическое обеспечение защиты информации. Кадровое обеспечение функционирования комплексной системы защиты информации. Защита человеческих ресурсов. Распределение функций по защите информации. Материально-техническое обеспечение защиты информации. Нормативнометодическое обеспечение комплексной защиты информации на предприятии. Порядок разработки нормативных и организационно-распорядительных документов, регламентирующих работу по защите информации на предприятии.	*ОПК-8 ОПК-12*	
		Тема 10. Планирование и контроль комплексной системы защиты информации.	*ОПК-12*	

		Понятие, принципы и методы планирования комплексной системы защиты информации. Стадии планирования. Факторы, влияющие на выбор принципов и способов планирования. Структура и общее содержание планов предприятия и функционирования комплексной системы защиты информации. Организация выполнения планов. Сущность, цель, задачи и содержание контроля комплексной системы защиты информации. Виды и методы контроля системы защиты информации. Основные контрольные мероприятия по защите информации.		
		Тема 11. Оценка эффективности комплексной системы защиты информации. Понятие эффективности и эффективности защиты информации. Требование по защите информации. Показатель и норма эффективности защиты информации. Подходы к оценке эффективности систем защиты информации и их особенности. Состав методов и моделей оценки эффективности систем защиты информации. Области применения различных методов и моделей для решения задач оценки эффективности системы защиты информации на предприятии. Методики проверки защищенности объектов информатизации на соответствие требованиям нормативных документов.	ПКС-4.3	
		Тема 12. Аттестация объектов информатизации по требованиям безопасности информации. Состав и содержание нормативно - правовых актов по аттестации объектов информатизации. Система аттестации объектов информатизации по требованиям безопасности информации. Организация аттестационных испытаний. Типовое содержание аттестационных испытаний объектов информатизации. Аттестационные испытания автоматизированных систем на соответствие требованиям по защите информации от несанкционированного доступа Аттестационные испытания объектов вычислительной техники по требованиям безопасности информации от утечки по каналам побочных электромагнитных излучений и наводок. Аттестационные испытания выделенных помещений. Инструментальные средства для проведения аттестационных испытаний. Основы проведения поисковых мероприятий по выявлению закладочных устройств.	*ОПК-12* ПКС-2.3	

Структура дисциплины (модуля)

Общая трудоемкость дисциплины составляет 3 зачетные единицы (108 часов)

Таблица 2

Вид работы	**Трудоемкость, часы**	
	8 семестр	Всего
Общая трудоемкость (в зачетных единицах)	**108**	**108**
Контактная работа (в часах):	**60**	**60**
Лекции (Л)	30	30
Лабораторные работы (ЛР)		
Практические занятия (ПЗ)	30	30
Самостоятельная работа (в часах):	**21**	**21**
Курсовой проект (КП) Курсовая работа (КР)		
Самостоятельное изучение разделов	21	21
Подготовка и прохождение промежуточной аттестации	**27**	**27**
Вид промежуточной аттестации	**Экзамен**	**Экзамен**

Таблица 3. Лекционные занятия

№ п/п	**Тема**
1.	**Тема 1. Введение в дисциплину. Сущность комплексной системы защиты информации и принципы ее организации.** Цель, задачи дисциплины, значение ее для подготовки специалиста. Знания и умения студентов, которые должны быть получены в результате ее изучения. Понятие, сущность и назначение комплексной системы защиты информации, ее задачи для обеспечения деятельности предприятия. Принципы организации комплексной системы защиты информации.
2.	**Тема 2. Методологические и концептуальные основы комплексной системы защиты информации.** Методология защиты информации и ее основные задачи. Уровень обеспечения безопасности информации. Достаточность защиты информации. Варианты построения комплексной системы защиты. Основные факторы, влияющие на организацию комплексной системы защиты информации. Характер и степень влияния различных факторов на организацию системы защиты информации.
3.	**Тема 3. Определение и нормативное закрепление информации ограниченного доступа.** Классификация информации по видам тайны и степеням конфиденциальности. Этапы работы по выявлению состава защищаемой информации. Нормативное закрепление состава защищаемой информации. Порядок организации нормативного закрепления информации ограниченного доступа.
4.	**Тема 4. Определение состава объектов защиты.** Понятие объекта защиты. Последовательность определения объекта защиты. Значение носителей защищаемой информации как объектов защиты. Факторы, определяющие состав носителей информации. Сущность защищаемого объекта информатизации. Методика выявления состава носителей защищаемой информации. Основные и вспомогательные технические средства, и системы. Особенности помещений как объектов защиты.
5.	**Тема 5. Источники, способы и результаты дестабилизирующего воздействия на информацию.** Определение источников дестабилизирующего воздействия на информацию. Модель формирования множества дестабилизирующих факторов. Понятие угрозы безопасности информации. Базовая модель угроз безопасности информации. Классификация угроз безопасности информации для объекта информатизации. Анализ и оценка угроз информационной безопасности объекта.
6.	**Тема 6. Выявление каналов утечки н методов несанкционированного воздействия**

	па информацию. Сущность утечки информации и несанкционированного воздействия на информацию. Структурная модель канала утечки информации. Технические каналы утечки информации и их классификация. Модель технических каналов утечки информатизации на типовом объекте информатизации. Каналы утечки из-за несанкционированного воздействия на информацию на системы, использующие информационно - коммуникационные технологии. Инсайдерские каналы утечки информации и «социальный инжиниринг» Методы «социального инжиниринга»
7.	**Тема 7. Моделирование процессов защиты информации.** Понятие модели и объекта моделирования. Основные виды моделей и их характеристика. Задачи и этапы моделирования в процессе построения комплексной системы защиты информации. Понятие архитектуры системы защиты информации. Кибернетическая, функциональная, информационная и организационная модели комплексной системы защиты информации. Формальные модели безопасности. Теории и методы моделирования процессов защиты информации.
8.	**Тема 8. Технологическое и организационное построение комплексной системы защиты информации.** Общее содержание работ по организации комплексной системы защиты информации. Характеристика технологического и организационного направлений создания комплексной системы защиты информации. Содержание стадий построения комплексной системы защиты информации. Предпроектное обследование. Назначение и структура технического задания, технико-экономического обоснования. Технический проект, рабочий проект. Апробация системы защиты информации и ввод ее в эксплуатацию.
9.	**Тема 9. Кадровое, материально-техническое и нормативно-методическое обеспечение защиты информации.** Кадровое обеспечение функционирования комплексной системы защиты информации. Защита человеческих ресурсов. Распределение функций по защите информации. Материально-техническое обеспечение защиты информации. Нормативно-методическое обеспечение комплексной защиты информации на предприятии. Порядок разработки нормативных и организационно-распорядительных документов, регламентирующих работу по защите информации на предприятии.
10.	**Тема 10. Планирование и контроль комплексной системы защиты информации.** Понятие, принципы и методы планирования комплексной системы защиты информации. Стадии планирования. Факторы, влияющие на выбор принципов и способов планирования. Структура и общее содержание планов предприятия и функционирования комплексной системы защиты информации. Организация выполнения планов. Сущность, цель, задачи и содержание контроля комплексной системы защиты информации. Виды и методы контроля системы защиты информации. Основные контрольные мероприятия по защите информации.
11.	**Тема 11. Оценка эффективности комплексной системы защиты информации.** Понятие эффективности и эффективности защиты информации. Требование по защите информации. Показатель и норма эффективности защиты информации. Подходы к оценке эффективности систем защиты информации и их особенности. Состав методов и моделей оценки эффективности систем защиты информации. Области применения различных методов и моделей для решения задач оценки эффективности системы защиты информации на предприятии. Методики проверки защищенности объектов информатизации на соответствие требованиям нормативных документов.
12.	**Тема 12. Аттестация объектов информатизации по требованиям безопасности информации.** Состав и содержание нормативно - правовых актов по аттестации объектов информатизации. Система аттестации объектов информатизации по требованиям безопасности информации. Организация аттестационных испытаний. Типовое содержание аттестационных испытаний объектов информатизации. Аттестационные испытания автоматизированных систем на соответствие требованиям по защите информации от несанкционированного доступа Аттестационные испытания объектов вычислительной техники по требованиям безопасности информации от утечки по каналам побочных электромагнитных излучений и наводок. Аттестационные испытания выделенных помещений. Инструментальные средства для проведения аттестационных испытаний. Основы проведения поисковых мероприятий по выявлению закладочных устройств.

Таблица 4. Практические и семинарские занятия

№ Темы	Темы семинарских занятий
1	Комплексная система защиты информации на предприятии и принципы ее организации (СЗ)
2	Оценка факторов, влияющих на организацию комплексной системы защиты информации (ПЗ)
3	Этапы работы по выявлению состава защищаемой информации на предприятии (ПЗ)
4	Определение состава объектов защиты на предприятии (ПЗ)
5	Анализ и оценка угроз информационной безопасности объекта информатизации (ПЗ)
6	Выявление каналов утечки информации на предприятии (ПЗ)
7	Задачи и этапы моделирования в процессе построения комплексной системы защиты информации (СЗ)
7	Моделирование процессов защиты информации (ПЗ)
8	Технологическое и организационное построение комплексной системы защиты информации (СЗ)
9	Разработка нормативных и организационно-распорядительных документов, регламентирующих работу по защите информации на предприятии (ПЗ)
10	Организация планирования и контроля комплексной системы защиты информации на предприятии (СЗ)
11	Применение методов и моделей оценки эффективности систем защиты информации (ПЗ)
12	Состав и содержание нормативно - правовых актов по аттестации объектов информатизации (СЗ)
12	Организация и проведение процедур аттестации объектов информатизации по требованиям безопасности информации (ПЗ)

Таблица 5. Самостоятельное изучение разделов дисциплины

№ раздела	**Вопросы, выносимые на самостоятельное изучение**
2	Характер и степень влияния различных факторов на организацию системы защиты информации
3	Порядок организации нормативного закрепления информации ограниченного доступа
4	Особенности помещений как объектов защиты
5	Базовые модели угроз безопасности различных видов информации ограниченного доступа
6	Методы «социального инжиниринга»
7	Формальные модели безопасности
8	Апробация системы защиты информации и ввод ее в эксплуатацию
9	Порядок разработки нормативных и организационно- распорядительных документов, регламентирующих работу по защите информации на предприятии
10	Основные контрольные мероприятия по защите информации
11	Области применения различных методов и моделей для решения задач оценки эффективности системы защиты информации на предприятии
12	Основы проведения поисковых мероприятий по выявлению закладочных устройств

5. Оценочные материалы для текущего и рубежного контроля успеваемости и промежуточной аттестации

Примерный перечень вопросов на коллоквиум по темам дисциплины (модуля)

1. Сущность комплексной системы защиты информации и принципы ее организации. Цель, задачи дисциплины, значение ее для подготовки специалиста.
2. Понятие, сущность и назначение комплексной системы защиты информации, ее задачи для обеспечения деятельности предприятия.
3. Методологические и концептуальные основы комплексной системы защиты информации.
4. Уровень обеспечения безопасности информации. Достаточность защиты информации.
5. Характер и степень влияния различных факторов на организацию системы защиты информации.
6. Этапы работы по выявлению состава защищаемой информации.
7. Определение состава объектов защиты. Понятие объекта защиты.
8. Факторы, определяющие состав носителей информации. Сущность защищаемого объекта информатизации.
9. Основные и вспомогательные технические средства, и системы. Особенности помещений как объектов защиты.
10. Определение источников дестабилизирующего воздействия на информацию.
11. Понятие угрозы безопасности информации. Базовая модель угроз безопасности информации.
12. Анализ и оценка угроз информационной безопасности объекта.
13. Технологическое и организационное построение комплексной системы защиты информации.
14. Характеристика технологического и организационного направлений создания комплексной системы защиты информации.
15. Защита человеческих ресурсов. Распределение функций по защите информации.
16. Нормативно-методическое обеспечение комплексной защиты информации на предприятии.
17. Планирование и контроль комплексной системы защиты информации.
18. Оценка эффективности комплексной системы защиты информации.

Образцы тестовых вопросов

1. Информация, зафиксированная на материальном носителе, с реквизитами, позволяющими ее идентифицировать, называется
    a) достоверной
    b) конфиденциальной
    c) документированной
    d) коммерческой тайной
2. По доступности информация классифицируется на
    a) открытую информацию и государственную тайну
    b) конфиденциальную информацию и информацию свободного доступа
    c) информацию с ограниченным доступом и общедоступную информацию
    d) виды информации, указанные в остальных пунктах
3. К конфиденциальной информации относятся документы, содержащие
    a) информацию о гражданах
    b) законодательные акты
    c) "ноу-хау"
    d) сведения о золотом запасе страны

4. Безопасность информации -
    a) процесс создания и использования в автоматизированных системах специальных механизмов, поддерживающих установленный статус ее защищенности
    b) поддержание на заданном уровне тех параметров находящейся в автоматизированной системе информации, которые характеризуют установленный статус ее хранения, обработки и использования
    c) события или действия, которые могут вызвать нарушение функционирования автоматизированной системы, связанное с уничтожением или несанкционированным использованием обрабатываемой в ней информации
    d) состояние защищенности информации хранимая и обрабатываемая в автоматизированной системе, от негативного воздействия на нее с точки зрения нарушения ее физической и логической целостности или несанкционированного доступа
5. Запрещено относить к информации ограниченного доступа
    a) информацию о чрезвычайных ситуациях
    b) информацию о деятельности органов государственной власти
    c) документы открытых архивов и библиотек
    d) все, перечисленное в остальных пунктах

Промежуточная аттестация

Примерный перечень вопросов к экзамену

1. Сущность комплексной системы защиты информации и принципы ее организации. Цель, задачи дисциплины, значение ее для подготовки специалиста.
2. Знания и умения студентов, которые должны быть получены в результате ее изучения.
3. Понятие, сущность и назначение комплексной системы защиты информации, ее задачи для обеспечения деятельности предприятия.
4. Принципы организации комплексной системы защиты информации.
5. Методологические и концептуальные основы комплексной системы защиты информации.
6. Методология защиты информации и ее основные задачи.
7. Уровень обеспечения безопасности информации. Достаточность защиты информации.
8. Варианты построения комплексной системы защиты. Основные факторы, влияющие на организацию комплексной системы защиты информации.
9. Характер и степень влияния различных факторов на организацию системы защиты информации.
10. Определение и нормативное закрепление информации ограниченного доступа. Классификация информации по видам тайны и степеням конфиденциальности.
11. Этапы работы по выявлению состава защищаемой информации.
12. Нормативное закрепление состава защищаемой информации. Порядок организации нормативного закрепления информации ограниченного доступа.
13. Определение состава объектов защиты. Понятие объекта защиты.
14. Последовательность определения объекта защиты. Значение носителей защищаемой информации как объектов защиты.
15. Факторы, определяющие состав носителей информации. Сущность защищаемого объекта информатизации.
16. Методика выявления состава носителей защищаемой информации.
17. Основные и вспомогательные технические средства, и системы. Особенности помещений как объектов защиты.

18. Источники, способы и результаты дестабилизирующего воздействия на информацию.
19. Определение источников дестабилизирующего воздействия на информацию.
20. Модель формирования множества дестабилизирующих факторов.
21. Понятие угрозы безопасности информации. Базовая модель угроз безопасности информации.
22. Классификация угроз безопасности информации для объекта информатизации.
23. Анализ и оценка угроз информационной безопасности объекта.
24. Выявление каналов утечки н методов несанкционированного воздействия па информацию.
25. Сущность утечки информации и несанкционированного воздействия на информацию.
26. Структурная модель канала утечки информации.
27. Технические каналы утечки информации и их классификация.
28. Модель технических каналов утечки информатизации на типовом объекте информатизации.
29. Каналы утечки из-за несанкционированного воздействия на информацию на системы, использующие информационно - коммуникационные технологии.
30. Инсайдерские каналы утечки информации и «социальный инжиниринг» Методы «социального инжиниринга»
31. Моделирование процессов защиты информации. Понятие модели и объекта моделирования. Основные виды моделей и их характеристика.
32. Задачи и этапы моделирования в процессе построения комплексной системы защиты информации.
33. Понятие архитектуры системы защиты информации.
34. Кибернетическая, функциональная, информационная и организационная модели комплексной системы защиты информации.
35. Формальные модели безопасности. Теории и методы моделирования процессов защиты информации.
36. Технологическое и организационное построение комплексной системы защиты информации.
37. Общее содержание работ по организации комплексной системы защиты информации.
38. Характеристика технологического и организационного направлений создания комплексной системы защиты информации.
39. Содержание стадий построения комплексной системы защиты информации. Предпроектное обследование.
40. Назначение и структура технического задания, технико-экономического обоснования. Технический проект, рабочий проект. Апробация системы защиты информации и ввод ее в эксплуатацию.
41. Кадровое, материально-техническое и нормативно-методическое обеспечение защиты информации. Кадровое обеспечение функционирования комплексной системы защиты информации.
42. Защита человеческих ресурсов. Распределение функций по защите информации.
43. Материально-техническое обеспечение защиты информации.
44. Нормативно-методическое обеспечение комплексной защиты информации на предприятии.
45. Порядок разработки нормативных и организационно-распорядительных документов, регламентирующих работу по защите информации на предприятии.
46. Планирование и контроль комплексной системы защиты информации.
47. Структура и общее содержание планов предприятия и функционирования комплексной системы защиты информации.
48. Организация выполнения планов. Сущность, цель, задачи и содержание контроля комплексной системы защиты информации.

49. Виды и методы контроля системы защиты информации. Основные контрольные мероприятия по защите информации.
50. Оценка эффективности комплексной системы защиты информации.
51. Понятие эффективности и эффективности защиты информации. Требование по защите информации. Показатель и норма эффективности защиты информации.
52. Подходы к оценке эффективности систем защиты информации и их особенности. Состав методов и моделей оценки эффективности систем защиты информации.
53. Области применения различных методов и моделей для решения задач оценки эффективности системы защиты информации на предприятии.
54. Методики проверки защищенности объектов информатизации на соответствие требованиям нормативных документов.
55. Аттестация объектов информатизации по требованиям безопасности информации.
56. Состав и содержание нормативно - правовых актов по аттестации объектов информатизации.
57. Система аттестации объектов информатизации по требованиям безопасности информации.
58. Организация аттестационных испытаний. Типовое содержание аттестационных испытаний объектов информатизации.
59. Аттестационные испытания автоматизированных систем на соответствие требованиям по защите информации от несанкционированного доступа
60. Аттестационные испытания объектов вычислительной техники по требованиям безопасности информации от утечки по каналам побочных электромагнитных излучений и наводок.
61. Аттестационные испытания выделенных помещений. Инструментальные средства для проведения аттестационных испытаний.
62. Основы проведения поисковых мероприятий по выявлению закладочных устройств.

Контроль курсовых работ

Курсовые работы не предусмотрены

6. Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и опыта деятельности

Максимальная сумма (100 баллов), набираемая студентом по дисциплине включает две составляющие:

– *первая составляющая* – оценка регулярности, своевременности и качества выполнения студентом учебной работы по изучению дисциплины в течение периода изучения дисциплины (семестра, или нескольких семестров) (сумма – не более 70 баллов). Баллы, характеризующие успеваемость студента по дисциплине, набираются им в течение всего периода обучения за изучение отдельных тем и выполнение отдельных видов работ.

– *вторая составляющая* – оценка знаний студента по результатам промежуточной аттестации (не более 30 –баллов).

Критерием оценки уровня сформированности компетенций в рамках учебной дисциплины является экзамен.

Общий балл текущего и рубежного контроля складывается из следующих составляющих приложение 2. В течение учебного процесса студент обязан отчитаться по теоретическому материалу и практическим занятиям: опросы, индивидуальные задания.

Целью промежуточных аттестаций по дисциплине является оценка качества освоения дисциплины обучающимися.

Критерии оценки качества освоения дисциплины

Оценка «отлично»– от 91 до 100 баллов – теоретическое содержание курса освоено полностью, без пробелов, необходимые практические навыки работы с освоенным материалом сформированы. Все предусмотренные программой обучения учебные задания выполнены, качество их выполнения оценено числом баллов, близким к максимальному. На экзамене студент демонстрирует глубокие знания предусмотренного программой материала, умеет четко, лаконично и логически последовательно отвечать на поставленные вопросы.

Оценка «хорошо» – от 81 до 90 баллов – теоретическое содержание курса освоено, необходимые практические навыки работы сформированы, выполненные учебные задания содержат незначительные ошибки. На экзамене студент демонстрирует твердое знания основного (программного) материала, умеет четко, грамотно, без существенных неточностей отвечать на поставленные вопросы.

Оценка «удовлетворительно» – от 61 до 80 баллов – теоретическое содержание курса освоено не полностью, необходимые практические навыки работы сформированы частично, выполненные учебные задания содержат грубые ошибки. На экзамене студент демонстрирует знание только основного материала, ответы содержат неточности, слабо аргументированы, нарушена последовательность изложения материала

Оценка «неудовлетворительно» – от 36 до 60 баллов – теоретическое содержание курса не освоено, необходимые практические навыки работы не сформированы, выполненные учебные задания содержат грубые ошибки, дополнительная самостоятельная работа над материалом курса не приведет к существенному повышению качества выполнения учебных заданий. На экзамене студент демонстрирует незнание значительной части программного материала, существенные ошибки в ответах на вопросы, неумение ориентироваться в материале, незнание основных понятий дисциплины.

Таблица 6. Результаты освоения учебной дисциплины, подлежащие проверке.

Результаты обучения (компетенции)	**Основные показатели оценки результатов обучения**	**Вид оценочного материала**
способен осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических документов в целях решения задач профессиональной деятельности *(ОПК-8):*	***Знать:*** - основные понятия и направления в защите компьютерной информации, - принципы классификации и примеры угроз безопасности базам данных и компьютерным системам, - современные подходы к защите баз данных и систем информационных технологий, - основные инструменты обеспечения многоуровневой безопасности в базах данных и информационных системах. ***Уметь:*** - конфигурировать встроенные средства безопасности в базах данных, - устанавливать и использовать одно из средств для шифрования информации и организации обмена данными с использованием электронной цифровой подписи; - устанавливать и настраивать программное обеспечение для защиты от вредоносного программного обеспечения; - настроить инструменты резервного копирования и восстановления информации ***Владеть:*** - методами аудита безопасности баз данных информационных систем, - методами анализа защищенности баз данных информационных систем	Типовые оценочные материалы для устного опроса *(раздел 5.1.1);* типовые тестовые задания *(раздел 5.2.2.);* примерные темы рефератов и эссе *(раздел 5.1.5);* типовые оценочные материалы к экзамену *(раздел 5.2.)* Оценочные материалы для самостоятельной работы (типовые задачи раздел 5.1.2.); примерные темы рефератов (раздел 5.1.3.); примерные темы докладов (раздел); типовые тестовые задания (раздел 5.2.2.) примерные темы рефераты (раздел 5.1.3).; примерные темы эссе (раздел 5.1.5);

способен проводить подготовку исходных данных для проектирования подсистем, средств обеспечения защиты информации и для технико-экономического обоснования соответствующих проектных решений *(ОПК-12)*;	*Знать:* цели, задачи, принципы и основные направления обеспечения информационной безопасности предприятия, угрозы предприятия на основе анализа структуры и содержания информационных процессов его, угрозы информационной безопасности государства, содержание информационной войны, методы и средства ее ведения, понимать угрозы безопасности информации, методы анализа структуры и особенности функционирования объекта защиты, принципы организации информационных систем в соответствии с требованиями по защите информации. *Уметь:* применять современные подходы к построению систем защиты информации, выбирать и анализировать показатели качества и критерии оценки систем информационного нападения и систем защиты информации, определять информационные ресурсы, подлежащие защите, проводить классификацию объектов и субъектов информационных систем. *Владеть*: навыками формальной постановки и решения задачи обеспечения информационной безопасности, навыками определения возможных путей нейтрализации угроз, принципами распределения прав и ответственности при организации доступа к объектам.	Типовые оценочные материалы для устного опроса *(раздел 5.1.1);* типовые тестовые задания *(раздел 5.2.2.);* примерные темы рефератов и эссе *(раздел 5.1.5);* типовые оценочные материалы к экзамену *(раздел 5.2.)* Оценочные материалы для самостоятельной работы (типовые задачи раздел 5.1.2.); примерные темы рефератов (раздел 5.1.3.); примерные темы докладов (раздел); типовые тестовые задания (раздел 5.2.2.) примерные темы рефераты (раздел 5.1.3).; примерные темы эссе (раздел 5.1.5);
способен управлять полномочиями пользователей (ПКС-2.3):	*Знать:* общую структуру комплексных систем защиты информации; угрозы информационной безопасности. *Уметь:* выявлять угрозы информационной безопасности. *Владеть*: методикой защиты от угроз информационной безопасности.	Коллоквиум Выполнение и защита лабораторных работ Тестирование
способен выработать рекомендации для принятия решения о модернизации системы за-щиты информации (ПКС-4.3).	*Знать:* нормативно-методическое обеспечение защиты информации, требования к формированию политики информационной безопасности на предприятии, - основные физические процессы, характерные для системы приборов технических средств охраны; - основные технические характеристики широко применяемых в настоящее время систем и приборов технических средств охраны, комплекс мер по обеспечению информационной безопасности, а также способы управления процессом их реализации, особенности формирования, организации и поддержания работоспособности комплекса мер по обеспечению информационной безопасности предприятия в рамках службы защиты информации. *Уметь:* производить обеспечение комплексной защиты информации, - принимать участие в формировании; - организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности; - управлять процессом их реализации, применять полученные знания для обеспечения информационной безопасности средствами службы защиты информации, формулировать и выстраивать основные положения политики	Типовые оценочные материалы для устного опроса *(раздел 5.1.1);* типовые тестовые задания *(раздел 5.2.2.);* примерные темы рефератов и эссе *(раздел 5.1.5);* типовые оценочные материалы к экзамену *(раздел 5.2.)* Оценочные материалы для самостоятельной работы (типовые задачи раздел 5.1.2.); примерные темы рефератов (раздел 5.1.3.); примерные темы докладов (раздел); типовые тестовые задания (раздел 5.2.2.) примерные темы рефераты (раздел 5.1.3).; примерные темы эссе (раздел 5.1.5);

	безопасности, - определять характеристики защищаемого объекта, включающие физические условия, рабочие процессы на объекте, правила, регламентирующие работу, принятые на объекте, требования органов государственного регулирования, вопросы аварийной безопасности, юридические вопросы; - составлять «модель» нарушителя, возможные пути и способы его проникновения на охраняемый объект. *Владеть*: методикой обеспечения комплексной защиты информации, навыками управления процессом реализации комплекса мер по обеспечению информационной безопасности предприятия в рамках службы защиты информации, методами формирования требований по защите информации, методами проектирования комплексов технических средств охраны для заданного объекта, навыками управления процессом реализации комплекса мер по обеспечению информационной безопасности.	

7. Учебно-методическое обеспечение дисциплины (модуля)

7.1. *Основная литература*

1. Основы информационной безопасности [Электронный ресурс]: учебник для студентов вузов, обучающихся по направлению подготовки «Правовое обеспечение национальной безопасности»/ В.Ю. Рогозин [и др.].— Электрон. текстовые данные.— М.: ЮНИТИ-ДАНА, 2017.— 287 c.— Режим доступа: http://www.iprbookshop.ru/72444.html.— ЭБС «IPRbooks»
2. Кармановский Н.С. Организационно-правовое и методическое обеспечение информационной безопасности [Электронный ресурс]: учебное пособие/ Кармановский Н.С., Михайличенко О.В., Прохожев Н.Н.— Электрон. текстовые данные.— СПб.: Университет ИТМО, 2016.— 169 c.— Режим доступа: http://www.iprbookshop.ru/67452.html.— ЭБС «IPRbooks»
3. Никифоров С.Н. Защита информации. Защищенные сети [Электронный ресурс]: учебное пособие/ Никифоров С.Н.— Электрон. текстовые данные.— СПб.: Санкт-Петербургский государственный архитектурно-строительный университет, ЭБС АСВ, 2017.— 80 c.— Режим доступа: http://www.iprbookshop.ru/74382.html.— ЭБС «IPRbooks»
4. Сагдеев К.М. Физические основы защиты информации [Электронный ресурс]: учебное пособие/ Сагдеев К.М., Петренко В.И., Чипига А.Ф.— Электрон. текстовые данные.— Ставрополь: Северо-Кавказский федеральный университет, 2015.— 394 c.— Режим доступа: http://www.iprbookshop.ru/63152.html.— ЭБС «IPRbooks»
5. Комплексное обеспечение информационной безопасности автоматизированных систем [Электронный ресурс]: лабораторный практикум/ М.А. Лапина [и др.].— Электрон. текстовые данные.— Ставрополь: Северо-Кавказский федеральный университет, 2016.— 242 c.— Режим доступа: http://www.iprbookshop.ru/62945.html.— ЭБС «IPRbooks»

7.2. *Дополнительная литература*

1. Бурькова Е.В. Физическая защита объектов информатизации [Электронный ресурс]: учебное пособие/ Бурькова Е.В.— Электрон. текстовые данные.— Оренбург: Оренбургский государственный университет, ЭБС АСВ, 2017.— 158 с.— Режим доступа: http://www.iprbookshop.ru/71349.html.— ЭБС «IPRbooks»
2. Голиков А.М. Защита информации от утечки по техническим каналам [Электронный ресурс]: учебное пособие/ Голиков А.М.— Электрон. текстовые данные.— Томск: Томский государственный университет систем управления и радиоэлектроники, 2015.— 256 с.— Режим доступа: http://www.iprbookshop.ru/72090.html.— ЭБС «IPRbooks»
3. Скрипник Д.А. Общие вопросы технической защиты информации [Электронный ресурс]/ Скрипник Д.А.— Электрон. текстовые данные.— М.: Интернет-Университет Информационных Технологий (ИНТУИТ), 2016.— 424 с.— Режим доступа: http://www.iprbookshop.ru/52161.html.— ЭБС «IPRbooks»
4. Джонс К.Д. Инструментальные средства обеспечения безопасности [Электронный ресурс]/ Джонс К.Д., Шема М., Джонсон Б.С.— Электрон. текстовые данные.— М.: Интернет-Университет Информационных Технологий (ИНТУИТ), 2016.— 914 с.— Режим доступа: http://www.iprbookshop.ru/73679.html.— ЭБС «IPRbooks»
5. Никифоров С.Н. Защита информации. Защита от внешних вторжений [Электронный ресурс]: учебное пособие/ Никифоров С.Н.— Электрон. текстовые данные.— СПб.: Санкт-Петербургский государственный архитектурно-строительный университет, ЭБС АСВ, 2017.— 84 с.— Режим доступа: http://www.iprbookshop.ru/74381.html.— ЭБС «IPRbooks»

7.3. *Периодические издания*

Перечень периодических изданий, получаемых библиотекой КБГУ:

- Вестник МГУ. Вычислительная математика и кибернетика
- Вестник российского общества информатики и вычислительной техники
- Информатика и образование
- Информационные технологии
- Мир ПК
- Персональный компьютер сегодня
- Программирование
- Информационная безопасность

7.4. *Интернет-ресурсы*

1. http://fstec.ru/ Федеральная служба по техническому и экспортному контролю
2. http://www.fsb.ru/ Федеральная служба безопасности
3. http://clsz.fsb.ru/ Центр по лицензированию, сертификации и защите государственной тайны ФСБ России
4. http://pravo.gov.ru/ Официальный интернет-портал правовой информации

7.5. *Методические указания по проведению различных учебных занятий, к курсовому проектированию и другим видам самостоятельной работы*

Методические рекомендации при работе над конспектом во время проведения лекции

В процессе лекционных занятий целесообразно конспектировать учебный материал. Для этого используются общие и утвердившиеся в практике правила, и приемы конспектирования лекций:

Конспектирование лекций ведется в специально отведенной для этого тетради, каждый лист которой должен иметь поля, на которых делаются пометки из рекомендованной литературы, дополняющие материал прослушанной лекции, а также подчеркивающие особую важность тех или иных теоретических положений.

Целесообразно записывать тему и план лекций, рекомендуемую литературу к теме. Записи разделов лекции должны иметь заголовки, подзаголовки, красные строки. Для выделения разделов, выводов, определений, основных идей можно использовать цветные карандаши и фломастеры.

Названные в лекции ссылки на первоисточники надо пометить на полях, чтобы при самостоятельной работе найти и вписать их. В конспекте дословно записываются определения понятий, категорий и законов. Остальное должно быть записано своими словами.

Каждому студенту необходимо выработать и использовать допустимые сокращения наиболее распространенных терминов и понятий.

Методические рекомендации при подготовке к коллоквиуму

- проработать конспекты лекций по вопросам коллоквиума;
- прочитать основную и дополнительную литературу, рекомендованную по изучаемым вопросам;
- ответить на вопросы коллоквиума;
- при затруднениях, проконсультироваться с преподавателем.

Критерии оценивания

Оценка			
неудовлетворительно 2 балла	**удовлетворительно 4 балла**	**хорошо 6 баллов**	**отлично 8 баллов**
Студент не знает значительной части вопросов, допускает существенные ошибки в ответах на вопросы.	Студент поверхностно знает вопросы коллоквиума, допускает неточности в ответе на вопрос	Студент хорошо знает материал, грамотно и по существу излагает его, допуская некоторые неточности в ответе на вопрос.	Студент в полном объеме знает материал, грамотно и по существу излагает его, не допуская существенных неточностей в ответе на вопрос.

Методические рекомендации по организации самостоятельной работы

Самостоятельная работа (по В.И. Далю «самостоятельный – человек, имеющий свои твердые убеждения») осуществляется при всех формах обучения: очной и заочной.

Самостоятельная работа обучающихся - способ активного, целенаправленного приобретения студентом новых для него знаний и умений без непосредственного участия в этом процесса преподавателей. Повышение роли самостоятельной работы обучающихся при проведении различных видов учебных занятий предполагает:

– оптимизацию методов обучения, внедрение в учебный процесс новых технологий обучения, повышающих производительность труда преподавателя, активное использование

информационных технологий, позволяющих обучающемуся в удобное для него время осваивать учебный материал;

– широкое внедрение компьютеризированного тестирования;

– совершенствование методики проведения практик и научно-исследовательской работы обучающихся, поскольку именно эти виды учебной работы в первую очередь готовят обучающихся к самостоятельному выполнению профессиональных задач;

– модернизацию системы курсового и дипломного проектирования, которая должна повышать роль студента в подборе материала, поиске путей решения задач.

Самостоятельная работа приводит студента к получению нового знания, упорядочению и углублению имеющихся знаний, формированию у него профессиональных навыков и умений. Самостоятельная работа выполняет ряд функций:

– развивающую;
– информационно-обучающую;
– ориентирующую и стимулирующую;
– воспитывающую;
– исследовательскую.

В рамках курса выполняются следующие виды самостоятельной работы:

1. Проработка учебного материала (по конспектам, учебной и научной литературе);
2. Выполнение разно уровневых задач и заданий;
3. Работа с тестами и вопросами для самопроверки;
4. Выполнение итоговой контрольной работы.

Студентам рекомендуется с самого начала освоения курса работать с литературой и предлагаемыми заданиями в форме подготовки к очередному аудиторному занятию. При этом актуализируются имеющиеся знания, а также создается база для усвоения нового материала, возникают вопросы, ответы на которые студент получает в аудитории.

Необходимо отметить, что некоторые задания для самостоятельной работы по курсу имеют определенную специфику. При освоении курса студент может пользоваться библиотекой вуза, которая в полной мере обеспечена соответствующей литературой. Значительную помощь в подготовке к очередному занятию может оказать имеющийся в учебно-методическом комплексе краткий конспект лекций. Он же может использоваться и для закрепления полученного в аудитории материала. Самостоятельная работа студентов предусмотрена учебным планом и выполняется в обязательном порядке. Задания предложены по каждой изучаемой теме и могут готовиться индивидуально или в группе. По необходимости студент может обращаться за консультацией к преподавателю. Выполнение заданий контролируется и оценивается преподавателем.

Для успешного самостоятельного изучения материала сегодня используются различные средства обучения, среди которых особое место занимают информационные технологии разного уровня и направленности: электронные учебники и курсы лекций, базы тестовых заданий и задач. Электронный учебник представляет собой программное средство, позволяющее представить для изучения теоретический материал, организовать апробирование, тренаж и самостоятельную творческую работу, помогающее студентам и преподавателю оценить уровень знаний в определенной тематике, а также содержащее необходимую справочную информацию. Электронный учебник может интегрировать в себе возможности различных педагогических программных средств: обучающих программ, справочников, учебных баз данных, тренажеров, контролирующих программ.

Для успешной организации самостоятельной работы все активнее применяются разнообразные образовательные ресурсы в сети Интернет: системы тестирования по различным областям, виртуальные лекции, лаборатории, при этом пользователю достаточно иметь компьютер и подключение к Интернету для того, чтобы связаться с преподавателем, решать вычислительные задачи и получать знания. Использование сетей усиливает роль самостоятельной работы студента и позволяет кардинальным образом изменить методику преподавания.

Студент может получать все задания и методические указания через сервер, что дает ему возможность привести в соответствие личные возможности с необходимыми для выполнения работ трудозатратами. Студент имеет возможность выполнять работу дома или в аудитории. Большое воспитательное и образовательное значение в самостоятельном учебном труде студента имеет самоконтроль. Самоконтроль возбуждает и поддерживает внимание и интерес, повышает активность памяти и мышления, позволяет студенту своевременно обнаружить и устранить допущенные ошибки и недостатки, объективно определить уровень своих знаний, практических умений. Самое доступное и простое средство самоконтроля с применением информационно-коммуникационных технологий - это ряд тестов «on-line», которые позволяют в режиме реального времени определить свой уровень владения предметным материалом, выявить свои ошибки и получить рекомендации по самосовершенствованию.

Методические рекомендации по работе с литературой

Всю литературу можно разделить на учебники и учебные пособия, оригинальные научные монографические источники, научные публикации в периодической печати. Из них можно выделить литературу основную (рекомендуемую), дополнительную и литературу для углубленного изучения дисциплины.

Изучение дисциплины следует начинать с учебника, поскольку учебник – это книга, в которой изложены основы научных знаний по определенному предмету в соответствии с целями и задачами обучения, установленными программой.

При работе с литературой необходимо учитывать, что имеются различные виды чтения, и каждый из них используется на определенных этапах освоения материала.

Предварительное чтение направлено на выявление в тексте незнакомых терминов и поиск их значения в справочной литературе. В частности, при чтении указанной литературы необходимо подробнейшим образом анализировать понятия.

Сквозное чтение предполагает прочтение материала от начала до конца. Сквозное чтение литературы из приведенного списка дает возможность студенту сформировать свод основных понятий из изучаемой области и свободно владеть ими.

Выборочное – наоборот, имеет целью поиск и отбор материала. В рамках данного курса выборочное чтение, как способ освоения содержания курса, должно использоваться при подготовке к практическим занятиям по соответствующим разделам.

Аналитическое чтение – это критический разбор текста с последующим его конспектированием. Освоение указанных понятий будет наиболее эффективным в том случае, если при чтении текстов студент будет задавать к этим текстам вопросы. Часть из этих вопросов сформулирована в ФОС в перечне вопросов для собеседования. Перечень этих вопросов ограничен, поэтому важно не только содержание вопросов, но сам принцип освоения литературы с помощью вопросов к текстам.

Целью *изучающего* чтения является глубокое и всестороннее понимание учебной информации. Есть несколько приемов изучающего чтения:

1. Чтение по алгоритму предполагает разбиение информации на блоки: название; автор; источник; основная идея текста; фактический материал; анализ текста путем сопоставления имеющихся точек зрения по рассматриваемым вопросам; новизна.

2. Прием постановки вопросов к тексту имеет следующий алгоритм:
   - медленно прочитать текст, стараясь понять смысл изложенного;
   - выделить ключевые слова в тексте;
   - постараться понять основные идеи, подтекст и общий замысел автора.

3. Прием тезирования заключается в формулировании тезисов в виде положений, утверждений, выводов.

К этому можно добавить и иные приемы: прием реферирования, прием комментирования.

Важной составляющей любого солидного научного издания является список литературы, на которую ссылается автор. При возникновении интереса к какой-то

обсуждаемой в тексте проблеме всегда есть возможность обратиться к списку относящейся к ней литературы. В этом случае вся проблема как бы разбивается на составляющие части, каждая из которых может изучаться отдельно от других. При этом важно не терять из вида общий контекст и не погружаться чрезмерно в детали, потому что таким образом можно не увидеть главного.

Подготовка к экзамену должна проводиться на основе лекционного материала, материала практических занятий с обязательным обращением к основным учебникам по курсу. Это позволит исключить ошибки в понимании материала, облегчит его осмысление, прокомментирует материал многочисленными примерами.

Методические рекомендации по написанию рефератов

Реферат представляет собой сокращенный пересказ содержания первичного документа (или его части) с основными фактическими сведениями и выводами. Написание реферата используется в учебном процессе вуза в целях приобретения студентом необходимой профессиональной подготовки, развития умения и навыков самостоятельного научного поиска: изучения литературы по выбранной теме, анализа различных источников и точек зрения, обобщения материала, выделения главного, формулирования выводов и т. п. С помощью рефератов студент глубже постигает наиболее сложные проблемы курса, учится лаконично излагать свои мысли, правильно оформлять работу, докладывать результаты своего труда. Процесс написания реферата включает: выбор темы; подбор нормативных актов, специальной литературы и иных источников, их изучение; составление плана; написание текста работы и ее оформление; устное изложение реферата.

Рефераты пишутся по наиболее актуальным темам. В них на основе тщательного анализа и обобщения научного материала сопоставляются различные взгляды авторов и определяется собственная позиция студента с изложением соответствующих аргументов. Темы рефератов должны охватывать и дискуссионные вопросы курса. Они призваны отражать передовые научные идеи, обобщать тенденции практической деятельности, учитывая при этом изменения в текущем законодательстве. Рекомендованная ниже тематика рефератов примерная. Студент при желании может сам предложить ту или иную тему, предварительно согласовав ее с научным руководителем.

Реферат, как правило, состоит из введения, в котором кратко обосновывается актуальность, научная и практическая значимость избранной темы, основного материала, содержащего суть проблемы и пути ее решения, и заключения, где формируются выводы, оценки, предложения. Общий объем реферата 20 листов.

Технические требования к оформлению реферата следующие. Реферат оформляется на листах формата А4, с обязательной нумерацией страниц, причем номер страницы на первом, титульном, листе не ставится. Поля: верхнее, нижнее, правое, левое – 20 мм. Абзацный отступ – 1,25; Рисунки должны создаваться в циклических редакторах или как рисунок Microsoft Word (сгруппированный). Таблицы выполнять табличными ячейками Microsoft Word. Сканирование рисунков и таблиц не допускается. Выравнивание текста (по ширине страницы) необходимо выполнять только стандартными способами, а не с помощью пробелов. Размер текста в рисунках и таблицах – 12 кегль. На титульном листе реферата нужно указать: название учебного заведения, факультета, номер группы и фамилию, имя и отчество автора, тему, место и год его написания. Рекомендуемый объем работы складывается из следующих составляющих: титульный лист (1 страница), содержание (1 страница), введение (1 – 2 страницы), основная часть, которую можно разделить на главы или разделы (10 – 15 страниц), заключение (1 – 3 страницы), список литературы (1 страница), приложение (не обязательно). Если реферат содержит таблицу, то ее номер и название располагаются сверху таблицы, если рисунок, то внизу рисунка.

Содержательные части реферата – это введение, основная часть и заключение. Введение должно содержать рассуждение по поводу того, что рассматриваемая тема актуальна (то есть современна и к ней есть большой интерес в настоящее время), а также постановку цели исследования, которая непосредственно связана с названием работы. Также

во введении могут быть поставлены задачи (но не обязательно, так как работа невелика по объему), которые детализируют цель. В заключении пишутся конкретные, содержательные выводы.

Содержание реферата студент докладывает на семинаре, кружке, научной конференции. Предварительно подготовив тезисы доклада, студент в течение 7 - 10 минут должен кратко изложить основные положения своей работы. После доклада автор отвечает на вопросы, затем выступают оппоненты, которые заранее познакомились с текстом реферата, и отмечают его сильные и слабые стороны. На основе обсуждения обучающемуся выставляется соответствующая оценка.

Методические рекомендации для подготовки к экзамену:

Экзамен в 7 семестре является формой итогового контроля знаний и умений, обучающихся по данной дисциплине, полученных на лекциях, практических занятиях и в процессе самостоятельной работы. Основой для определения оценки служит уровень усвоения обучающимися материала, предусмотренного данной рабочей программой К экзамену допускаются студенты, набравшие 36 и более баллов по итогам текущего и промежуточного контроля. На экзамене студент может набрать от 15 до 30 баллов.

В период подготовки к экзамену обучающиеся вновь обращаются к учебно-методическому материалу и закрепляют промежуточные знания.

Подготовка обучающегося к экзамен включает три этапа:

- самостоятельная работа в течение семестра;
- непосредственная подготовка в дни, предшествующие экзамену по темам курса;
- подготовка к ответу на экзаменационные вопросы.

При подготовке к экзамену обучающимся целесообразно использовать материалы лекций, учебно-методические комплексы, нормативные документы, основную и дополнительную литературу.

На экзамен выносится материал в объеме, предусмотренном рабочей программой учебной дисциплины за семестр. Экзамен проводится в письменной / устной форме.

При проведении экзамена в письменной (устной) форме, ведущий преподаватель составляет экзаменационные билеты, которые включают в себя: тестовые задания; теоретические задания; задачи или ситуации. Формулировка теоретических задания совпадает с формулировкой перечня экзаменационных вопросов, доведенных до сведения обучающихся накануне экзаменационной сессии. Содержание вопросов одного билета относится к различным разделам программы с тем, чтобы более полно охватить материал учебной дисциплины.

В аудитории, где проводится устный экзамен, должно одновременно находиться не более шести студентов на одного преподавателя, принимающего экзамен. На подготовку ответа на билет на экзамене отводится 40 минут.

При проведении письменного экзамена на работу отводиться 60 минут.

Результат устного (письменного) экзамена выражается оценками:

Оценка «отлично»– от 91 до 100 баллов – теоретическое содержание курса освоено полностью, без пробелов, необходимые практические навыки работы с освоенным материалом сформированы. Все предусмотренные программой обучения учебные задания выполнены, качество их выполнения оценено числом баллов, близким к максимальному. На экзамене студент демонстрирует глубокие знания предусмотренного программой материала, умеет четко, лаконично и логически последовательно отвечать на поставленные вопросы.

Оценка «хорошо» – от 81 до 90 баллов – теоретическое содержание курса освоено, необходимые практические навыки работы сформированы, выполненные учебные задания содержат незначительные ошибки. На экзамене студент демонстрирует твердое знания основного (программного) материала, умеет четко, грамотно, без существенных неточностей отвечать на поставленные вопросы.

Оценка «удовлетворительно» – от 61 до 80 баллов – теоретическое содержание курса освоено не полностью, необходимые практические навыки работы сформированы частично, выполненные учебные задания содержат грубые ошибки. На экзамене студент

демонстрирует знание только основного материала, ответы содержат неточности, слабо аргументированы, нарушена последовательность изложения материала

Оценка «неудовлетворительно» – от 36 до 60 баллов – теоретическое содержание курса не освоено, необходимые практические навыки работы не сформированы, выполненные учебные задания содержат грубые ошибки, дополнительная самостоятельная работа над материалом курса не приведет к существенному повышению качества выполнения учебных заданий. На экзамене студент демонстрирует незнание значительной части программного материала, существенные ошибки в ответах на вопросы, неумение ориентироваться в материале, незнание основных понятий дисциплины

Методические рекомендации по выполнению лабораторных работ

Выполнение каждой лабораторной работы складывается из следующих этапов.

1. Самостоятельная подготовка студентов к работе. Перед началом работы студенты должны четко представлять себе цель работы, изучить теоретические сведения к лабораторной работе

2. Выполнение работы. Этот этап осуществляется в соответствии с методическими указаниями, которые содержатся в описании к каждой работе. Сформулировать выводы по проделанной работе.

3. Составление отчета о проделанной работе. К отчету о выполненной работе предъявляются следующие требования:

Отчет должен содержать исчерпывающие данные, как о цели работы, так и о результатах в следующей последовательности:

- Титульный лист
- цель работы
- задание на лабораторную работу для своего варианта
- ответы на контрольные вопросы
- результаты выполнения работы
- выводы по работе.

4. Защита лабораторной работы с представлением отчета. Защита лабораторной работы проходит в форме свободной беседы по теме лабораторной работы.

Методические рекомендации по подготовке к тестированию

Тесты – это вопросы или задания, предусматривающие конкретный, краткий, четкий ответ на имеющиеся эталоны ответов. При самостоятельной подготовке к тестированию студенту необходимо:

а) готовясь к тестированию, проработать информационный материал по дисциплине. Проконсультироваться с преподавателем по вопросу выбора учебной литературы;

б) четко выясните все условия тестирования заранее. Знать, сколько тестов Вам будет предложено, сколько времени отводится на тестирование, какова система оценки результатов и т.д.

в) приступая к работе с тестами, внимательно и до конца прочтите вопрос и предлагаемые варианты ответов. Выберите правильные (их может быть несколько). На отдельном листке ответов выпишите цифру вопроса и буквы, соответствующие правильным ответам;

г) в процессе решения желательно применять несколько подходов в решении задания. Это позволяет максимально гибко оперировать методами решения, находя каждый раз оптимальный вариант.

д) если Вы встретили чрезвычайно трудный для Вас вопрос, не тратьте много времени на него. Переходите к другим тестам. Вернитесь к трудному вопросу в конце.

е) обязательно оставьте время для проверки ответов, чтобы избежать механических ошибок.

Критерии оценивания

Оценка			
неудовлетворительно 0 баллов	**удовлетворительно 3 балла**	**хорошо 4 балла**	**отлично 5 баллов**
Менее 50 % правильно выполненных заданий.	50-70% правильно выполненных заданий.	71-85% правильно выполненных заданий.	86-100% правильно выполненных заданий.

8. Материально-техническое обеспечение дисциплины

8.1. Требования к материально-техническому обеспечению

Специализированная аудитория, используемая при проведении занятий лекционного типа №42, №43, №44, №48, №48а, №56, №58 оснащена мультимедийным проектором и комплектом аппаратуры, позволяющей демонстрировать текстовые и графические материалы.

Лаборатории оснащены необходимым оборудованием: Аппаратно-программный комплекс Sound Cleaner II, ЛГШ 701, АПК «Колибри», АПК «ST 131 Пиранья II», Microsoft Office, 7-zip, Adobe Acrobat Reader DC и др. Междисциплинарная научно-исследовательская лаборатория специальных психофизиологических исследований.

- Продукты MICROCOFT (WINEDUperDVC ALNG UpgrdSAPk MVL A Faculty EES (Корпоративная подписка на продукты Windows операционная система и офис)) ДОГОВОР №10/ЭА-223.
- Kaspersky Endpoint Security для бизнеса – Стандартный Russian Edition. 1500-2499 Node 1 year Educational Renewal License, ДОГОВОР № 15/ЭА-223.
- Mathlab/Simulink ДОГОВОР №80/ЕЛ-223.
- Adobe Creative Cloud for Teams – All Apps. Лицензии Education Device license для образовательных организаций ДОГОВОР № 15/ЭА-223.
- ABBYY FineReader ДОГОВОР № 15/ЭА-223.
- Антиплагиат ВУЗ ДОГОВОР № 15/ЭА-223.
- файловый менеджер Far Manager.
- 7zip-архиватор.
- Adobe Reader (свободное распространение)

Студенты имеют доступ через Интернет доступ к единому образовательному порталу, где в открытом доступе имеются ресурсы учебно-методической литературы, являющиеся разработками ведущих ВУЗов России.

8.2. Особенности реализации дисциплины для инвалидов и лиц с ограниченными возможностями здоровья

Для студентов с ограниченными возможностями здоровья созданы специальные условия для получения образования. В целях доступности получения высшего образования по образовательным программам инвалидами и лицами с ограниченными возможностями здоровья университетом обеспечивается:

1. Альтернативная версия официального сайта в сети «Интернет» для слабовидящих;
2. Для инвалидов с нарушениями зрения (слабовидящие, слепые):

– присутствие ассистента, оказывающего обучающемуся необходимую помощь, дублирование вслух справочной информации о расписании учебных занятий; наличие средств для усиления остаточного зрения, брайлевской компьютерной техники, видеоувеличителей, программ невизуального доступа к информации, программ-синтезаторов речи и других технических средств приема-передачи учебной информации в доступных формах для студентов с нарушениями зрения;

– задания для выполнения на экзамене зачитываются ассистентом;

– письменные задания выполняются на бумаге, надиктовываются ассистенту обучающимся;

3.Для инвалидов и лиц с ограниченными возможностями здоровья по слуху (слабослышащие, глухие):

– на зачете/экзамене присутствует ассистент, оказывающий студенту необходимую техническую помощь с учетом индивидуальных особенностей (он помогает занять рабочее место, передвигаться, прочитать и оформить задание, в том числе записывая под диктовку);

– зачет/экзамен проводится в письменной форме;

4. Для инвалидов и лиц с ограниченными возможностями здоровья, имеющих нарушения опорно-двигательного аппарата, созданы материально-технические условия, обеспечивающие возможность беспрепятственного доступа обучающихся в учебные помещения, объекту питания, туалетные и другие помещения университета, а также пребывания в указанных помещениях (наличие расширенных дверных проемов, поручней и других приспособлений).

– письменные задания выполняются на компьютере со специализированным программным обеспечением или надиктовываются ассистенту;

– по желанию студента экзамен проводится в устной форме.

Обучающиеся из числа лиц с ограниченными возможностями здоровья обеспечены электронными образовательными ресурсами в формах, адаптированных к ограничениям их здоровья.

.

9. ЛИСТ ПЕРЕУТВЕРЖДЕНИЯ РАБОЧЕЙ ПРОГРАММЫ ДИСЦИПЛИНЫ

Рабочая программа:

одобрена на 2023/2024 учебный год. Протокол № _____ заседания кафедры от «___»_____20__ г.

В рабочую программу внесены следующие изменения:

_____
_____
_____
_____
_____

Разработчик программы _____
Зав. кафедрой _____

ПРИЛОЖЕНИЕ

Распределение баллов текущего и рубежного контроля

№п/п	Вид контроля	Сумма баллов			
		Общая сумма	1-я точка	2-я точка	3-я точка
1	Посещение занятий	до 10 баллов	до 3 б.	до 3б.	до 4б.
2	Текущий контроль:	до 30 баллов	до 10 б.	до 10 б.	до 10 б.
3	Рубежный контроль (тестирование и коллоквиум)	до 30 баллов	до 10 б.	до 10 б.	до 10 б.
4	Итого сумма текущего и рубежного контроля	до 70 баллов	до 23б	до 23 б	до 24 б

Приложение 2

Распределение баллов текущего и рубежного контроля

№п/п	*Вид контроля*	*Сумма баллов*			
		Общая сумма	*1-я точка*	*2-я точка*	*3-я точка*
1-	***Посещение занятий***	***до 10 баллов***	***до 3 б.***	***до 3б.***	***до 4б.***
2-	***Текущий контроль:***	***до 30 баллов***	***до 10 б.***	***до 10 б.***	***до 10 б.***
	Ответ на 5 вопросов	*от 0 до15 б.*	*от 0 до 5 б.*	*от0 до 5 б.*	*от0 до 5 б.*
	Полный правильный ответ	до 15 баллов	5 б.	5 б.	5 б.
	Неполный правильный ответ	от 3 до15 б.	от1 до 5 б.	от 1 до 5 б.	от 1 до 5 б.
	Ответ, содержащий неточности, ошибки	0б.	0б.	0б.	0б.
	Выполнение самостоятельных заданий (решение задач, написание рефератов, доклад, эссе)	*от 0 до15 б.*	*от 0 до 5 б.*	*от 0 до 5 б*	*от 0 до 5 б*
1.	***Рубежный контроль***	***до 30 баллов***	***до 10 б.***	***до 10 б.***	***до 10 б.***
	тестирование	от 0- до 12б.	от 0- до 4б.	от 0- до 4б.	от 0- до 4б.
	коллоквиум	от 0 до 18б.	от 0 до 6 б.	от 0 до 6 б.	от 0 до 6 б.
	Итого сумма текущего и рубежного контроля	***до 70баллов***	***до 23б.***	***до 23б***	***до 24б***
	Первый этап (базовый)уровень) – оценка «удовлетворительно»	не менее 36 б**.**	не менее 12 б.	не менее 12 б	не менее 12 б
	Второй этап (продвинутый)уровень) – оценка «хорошо»	менее 70 б. (51-69 б.)	менее 23 б	менее 23 б	менее 24б

	Третий этап (высокий уровень) - оценка «отлично»	не менее 70 б.	не менее 23 б.	не менее 23 б	не менее 24б