МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное учреждение высшего образования
«СЕВЕРО-КАВКАЗСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»
Институт сервиса, туризма и дизайна (филиал) СКФУ в г. Пятигорске

УТВЕРЖДАЮ
Зам. директора по учебной работе
Институт сервиса, туризма и дизайна
(филиал) СКФУ в г. Пятигорске
_____М.В. Мартыненко
"__" _____ 20____ г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Комплексная система защиты информации на предприятии

Направление подготовки	10.03.01 Информационная безопасность
Направленность (профиль)	Комплексная защита объектов информатизации
Квалификация выпускника	Бакалавр
Форма обучения	Очная
Год начала обучения	2020 г.
Изучается	в 8 семестре

СОГЛАСОВАНО:
Зав. выпускающей кафедры систем управления и информационных технологий
_____ И.М Першин
"__" _____ 20____ г.

Рассмотрено УМК
Протокол №__ от «__»_____20__г.
"__" _____ 20_____ г.
Председатель УМК института
_____ А.Б. Нарыжная

РАЗРАБОТАНО:
Зав. кафедрой систем управления и информационных технологий
_____ И.М Першин
"__" _____ 20____ г.

старший преподаватель кафедры систем управления и информационных технологий
_____ А.С. Ермаков
"__" _____ 20____ г.

Пятигорск, 2020

1. Цель и задачи освоения дисциплины

Целью освоения дисциплины «Комплексная система защиты информации на предприятии» является теоретическая и практическая подготовка студентов в области проектирования, создания и эксплуатации комплексных систем защиты информации на предприятии.

Задачи освоения дисциплины: сущность и задачи комплексной системы защиты информации (КСЗИ); принципы организации и этапы разработки КСЗИ; определение и нормативное закрепление объектов и субъектов защиты; анализ и оценка угроз безопасности информации; определение компонентов КСЗИ; построение моделей КСЗИ; принципы и методы планирования функционирования КСЗИ; состав методов и моделей оценки эффективности КСЗИ.

2. Место дисциплины в структуре образовательной программы

Дисциплина относится к вариативной части блока Б1.В.06. Ее освоение происходит в 8 семестре.

3. Связь с предшествующими дисциплинами

Для изучения данной дисциплины необходимы знания, навыки и компетенции, полученные при изучении дисциплин «Основы информационной безопасности», «Основы управленческой деятельности», «Метрология, стандартизация и сертификация».

4. Связь с последующими дисциплинами

Полученные в ходе изучения данной дисциплины профессиональные и общекультурные компетенции пригодятся при изучении таких дисциплин, как «Защищенные локальные вычислительные сети», «Технические средства защиты информации», «Защита персональных данных в информационных системах», «Организационное и правовое обеспечение информационной безопасности», «Управление проектами по защите информации и экономика защиты информации», «Безопасность баз данных», «Криптографические методы защиты информации», поможет в прохождении технологической практики, Эксплуатационной практики, преддипломной практики и защите выпускной квалификационной работы, включая подготовку к процедуре защиты и процедуру защиты.

5. Перечень планируемых результатов обучения по дисциплине (модулю), соотнесенных с планируемыми результатами освоения образовательной программы

5.1 Наименование компетенций

Код	Формулировка:
ОПК-7	способностью определять информационные ресурсы, подлежащие защите, угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты
ПК-1	способностью выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации
ПК-2	способностью применять программные средства системного, прикладного и специального назначения, инструментальные средства, языки и системы программирования для решения профессиональных задач
ПК-3	способностью администрировать подсистемы информационной безопасности объекта защиты
ПК-4	способность участвовать в работах по реализации политики информационной безопасности, применять комплексный подход к обеспечению информационной безопасности объекта защиты

ПК-7	способностью проводить анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности и участвовать в проведении технико-экономического обоснования соответствующих проектных решений
ПК-8	способностью оформлять рабочую техническую документацию с учетом действующих нормативных и методических документов
ПК-12	способность принимать участие в проведении экспериментальных исследований системы защиты информации
ПК-13	способность принимать участие в формировании, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации
ПК-15	способностью организовывать технологический процесс защиты информации ограниченного доступа в соответствии с нормативными правовыми актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю

5.2 Знания, умения и навыки и (или) опыт деятельности, характеризующие этапы формирования компетенций

Планируемые результаты обучения по дисциплине (модулю), характеризующие этапы формирования компетенций	Формируемые компетенции
Знать: ▪ информационные ресурсы, подлежащие защите ▪ угрозы безопасности информации и возможные пути их реализации. **Уметь**: ▪ определять информационные ресурсы, подлежащие защите, угрозы безопасности информации и возможные пути их реализации.	**ОПК-7**
Знать: ▪ программно-аппаратные и технические средства защиты информации. **Уметь:** ▪ выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных и технических средств защиты информации	**ПК-1**
Знать: ▪ программные средства системного, прикладного и специального назначения, инструментальные средства, языки и системы программирования для решения профессиональных задач; **Уметь:** ▪ применять программные средства системного, прикладного и специального назначения, инструментальные средства, языки и системы программирования для решения профессиональных задач; **Владеть:** ▪ способностью применять программные средства системного, прикладного и специального назначения, инструментальные средства, языки и системы программирования для решения профессиональных задач.	**ПК-2**
Знать:	**ПК-3**

▪ подсистемы информационной безопасности объекта защиты; **Уметь:** ▪ администрировать подсистемы информационной безопасности объекта защиты; **Владеть:** ▪ способностью администрировать подсистемы информационной безопасности объекта защиты	
Знать: ▪ работы по реализации политики информационной безопасности, применять комплексный подход к обеспечению информационной безопасности объекта защиты. **Уметь:** ▪ применять комплексный подход к обеспечению информационной безопасности объекта защиты. **Владеть:** ▪ навыками работы по реализации политики информационной безопасности.	**ПК-4**
Знать: ▪ анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности и участвовать в проведении технико-экономического обоснования соответствующих проектных решений. **Уметь:** ▪ проводить анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности и участвовать в проведении технико-экономического обоснования соответствующих проектных решений; **Владеть:** ▪ способностью проводить анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности и участвовать в проведении технико-экономического обоснования соответствующих проектных решений	**ПК-7**
Знать: ▪ рабочую техническую документацию с учетом действующих нормативных и методических документов. **Уметь:** ▪ оформлять рабочую техническую документацию с учетом действующих нормативных и методических документов; **Владеть:** ▪ способностью оформлять рабочую техническую документацию с учетом действующих нормативных и методических документов	**ПК-8**
Знать: ▪ экспериментальные исследования системы защиты информации. **Уметь:** ▪ принимать участие в проведении экспериментальных исследований системы защиты информации; **Владеть:** ▪ навыками участия в проведении экспериментальных исследований системы защиты информации.	**ПК-12**

Знать: ▪ формирование, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации. **Уметь:** ▪ принимать участие в формировании, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации; **Владеть:** ▪ навыками участия в формировании, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации.	**ПК-13**
Знать: ▪ технологический процесс защиты информации ограниченного доступа в соответствии с нормативными правовыми актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю. **Уметь:** ▪ организовывать технологический процесс защиты информации ограниченного доступа в соответствии с нормативными правовыми актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю; **Владеть:** ▪ способностью организовывать технологический процесс защиты информации ограниченного доступа в соответствии с нормативными правовыми актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю	**ПК-15**

6. Объем учебной дисциплины/модуля

	Астр. часов	Акад. часов	
Объем занятий: Итого	108 ч.	144 ч.	4 з.е.
В том числе аудиторных	54 ч.	72 ч.	
Из них:			
Лекций	13,5 ч.	18 ч.	
Лабораторных работ	27 ч.	36 ч.	
Практических занятий	13,5 ч.	18 ч.	
Самостоятельной работы	33,75 ч.	45 ч.	
Контроль	20,25 ч.	27 ч.	
Экзамен, курсовая работа			8 семестр

7. Содержание дисциплины, структурированное по темам (разделам) с указанием отведенного на них количества астрономических часов и видов занятий

7.1 Тематический план дисциплины

№	Раздел (тема) дисциплины	Реализуемые компетенции	Контактная работа обучающихся с преподавателем, часов				Самостоятельная работа, часов
			Лекции	Практические занятия	Лабораторные работы	Групповые консультации	
8 семестр							
1.	Тема 1. Сущность комплексной защиты информации на предприятии (в организации, учреждении).	ОПК-7, ПК-1, ПК-2, ПК-3, ПК-4, ПК-7, ПК-8, ПК-12, ПК-13, ПК-15	1,5	1,5	3		3,75
2.	Тема 2. Организация КСЗИ, этапы разработки и факторы, влияющие на организацию КСЗИ	ОПК-7, ПК-1, ПК-2, ПК-3, ПК-4, ПК-7, ПК-8, ПК-12, ПК-13, ПК-15	1,5	1,5	3		3,75
3.	Тема 3. Определение объектов защиты предприятия и утверждение перечней защищаемых сведений.	ОПК-7, ПК-1, ПК-2, ПК-3, ПК-4, ПК-7, ПК-8, ПК-12, ПК-13, ПК-15	1,5	1,5	3		3,75
4.	Тема 4. Организационное построение КСЗИ. Введение внутриобъектового режима на предприятии.	ОПК-7, ПК-1, ПК-2, ПК-3, ПК-4, ПК-7, ПК-8, ПК-12, ПК-13, ПК-15	1,5	1,5	3		3,75
5.	Тема 5. Определение угроз безопасности информации на предприятии.	ОПК-7, ПК-1, ПК-2, ПК-3, ПК-4, ПК-7, ПК-8, ПК-12, ПК-13, ПК-15	1,5	1,5	3		3,75
6.	Тема 6. Дестабилизирующие негативные воздействия на информацию и их нейтрализация.	ОПК-7, ПК-1, ПК-2, ПК-3, ПК-4, ПК-7, ПК-8, ПК-12, ПК-13, ПК-15	1,5	1,5	3		3,75
7.	Тема 7. Возможности несанкционированного доступа к защищаемой информации. Методы защиты объектов информатизации.	ОПК-7, ПК-1, ПК-2, ПК-3, ПК-4, ПК-7, ПК-8, ПК-12, ПК-13, ПК-15	1,5	1,5	3		3,75

8.	Тема 8. Методики оценки эффективности принятых мер по созданию КСЗИ	ОПК-7, ПК-1, ПК-2, ПК-3, ПК-4, ПК-7, ПК-8, ПК-12, ПК-13, ПК-15	1,5	1,5	3		3,75
9.	Тема 9. Система аттестации объектов информатизации.	ОПК-7, ПК-1, ПК-2, ПК-3, ПК-4, ПК-7, ПК-8, ПК-12, ПК-13, ПК-15	1,5	1,5	3		3,75
	Итого		**13,5**	**13,5**	**27**		**33,75**

7.2 Наименование и содержание лекций

№ темы	Наименование тем дисциплины, их краткое содержание	Объем часов	Интерактивная форма проведения
	8 семестр		
1.	**Тема** Сущность комплексной защиты информации на предприятии (в организации, учреждении). *Задачи и функции комплексной системы защиты информации на предприятии.* *Цели создания КСЗИ на предприятии.* *Классификация формальных моделей безопасности.* *Модели обеспечения безопасности информации.*	1,5	Мультимедиа лекция
2.	**Тема** Организация КСЗИ, этапы разработки и факторы, влияющие на организацию КСЗИ *Принципы построения КСЗИ на предприятии. Общее содержание работ по организации КСЗИ.* *Методологические основы организации КСЗИ.* *Модели КСЗИ (принцип формализации требований безопасности и условий функционирования системы).* *Этапы разработки КСЗИ на предприятии.*	1,5	Мультимедиа лекция
3.	**Тема** Определение объектов защиты предприятия и утверждение перечней защищаемых сведений. *Классификация информации по видам тайн. Засекречивание и рассекречивание сведений и их носителей.* *Нормативно-правовые аспекты защиты коммерческой тайны. Порядок внедрения Перечня сведений, составляющих коммерческую тайну, внесение в него изменений и дополнений. Методика определения состава защищаемой информации на предприятии.*	1,5	Мультимедиа лекция
4.	**Тема** Организационное построение КСЗИ. Введение внутриобъектового режима на предприятии. *Правовая основа режима секретности на предприятии. Обязанности и запреты сотрудников, допущенных к конфиденциальной информации. Роль и место внутриобъектового и пропускного режимов в систе-*	1,5	Мультимедиа лекция

	ме защиты информации предприятия. *Основные подходы и принципы к организации внутриобъектового режима.*		
5.	**Тема** Определение угроз безопасности информации на предприятии. *Факторы и угрозы безопасности информации.* *Методика выявления нарушителей, тактики их действий и состава интересующей их информации.* *Модели нарушителей угроз безопасности предприятия.*	1,5	Мультимедиа лекция
6.	**Тема** Дестабилизирующие негативные воздействия на информацию и их нейтрализация. *Обеспечение безопасности информации в непредвиденных ситуациях.* *Реагирование на инциденты ИБ. Факторы, создающие угрозу информационной безопасности.* *Подготовка мероприятий на случай возникновения ЧС.*	1,5	Мультимедиа лекция
7.	**Тема** Возможности несанкционированного доступа к защищаемой информации. Методы защиты объектов информатизации. *Особенности помещений как объектов защиты для работы по защите информации. Защита от утечки информации по техническим каналам в автоматизированных системах. Защита от несанкционированного доступа к информации в автоматизированных системах. Особенности защиты речевой информации на предприятии.*	1,5	Мультимедиа лекция
8.	**Тема** Методики оценки эффективности принятых мер по созданию КСЗИ *Экономический подход к оценке эффективности комплексной системы защиты информации на предприятии. Организация управления, планирование функционирования и оценка эффективности КСЗИ.* *Цели проведения контрольных мероприятий в КСЗИ.*	1,5	Мультимедиа лекция
9.	**Тема** Система аттестации объектов информатизации. *Основные положения мероприятий по аттестации объектов информатизации.* *Методы проверок и испытаний объектов информатизации, используемые при аттестации.*	1,5	Мультимедиа лекция
	Итого	**13,5**	**13,5**

7.3 Наименование лабораторных работ

№ Темы	Наименование тем дисциплины, их краткое содержание	Объем часов	Интерактивная форма проведения
8 семестр			
1	Лабораторная работа №1. **Тема: «Определение перечня сведений конфиденциального характера на предприятии.».** *Изучение нормативно-правовой базы по закреплению перечней сведений конфиденциального характера на предприятии. Составление примерного перечня сведений, составляющих коммерческую тайну на предприятии.*	3	
2	Лабораторная работа №2 **Тема: «Определение перечня защищаемых ресурсов объекта информатизации»** *Выявление и документальное закрепление защищаемых информационных ресурсов автоматизированной системы, обрабатывающей сведения, составляющие коммерческую тайну.*	3	
3	Лабораторная работа №3 Тема: **«Разработка разрешительной системы доступа на объекте информатизации»** *Составление разрешительной системы доступа пользователей автоматизированной системы к определенным защищаемым информационным ресурсам, техническим средствам и программному обеспечению автоматизированной системы.*	3	
4	Лабораторная работа №4 Тема: **«Разработка модели нарушителя для объектов информатизации предприятия»** *Моделирование вероятного нарушителя в отношении абстрактной информационной системы предприятия на основе методических рекомендаций по обеспечению с помощью криптосредств безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств автоматизации, утвержденных 8 центром ФСБ 21 февраля 2008 года № 149/54-144.*	3	
5	Лабораторная работа № 5 **Тема: «Разработка модели**	3	

	угроз для объектов информатизации предприятия» *Составление одели угроз для абстрактного объекта информатизации предприятия на основе методики определения угроз безопасности информации в информационных системах, утвержденных ФСТЭК России, 2015 г.*		
6	Лабораторная работа №6 Тема: **«Проведение мероприятий по паспортизации объектов информатизации предприятия. Разработка технического паспорта»** *Составление технического паспорта на формальный объект информатизации по форме, утвержденной СТР-К.*	3	
7	Лабораторная работа № 7 **Тема: «Действия в чрезвычайных ситуациях на предприятии. Разработка инструкции по действиям в случае пожара, аварии, стихийного бедствия и при возникновении других чрезвычайных ситуаций на объекте».** *Моделирование действия по спасению конфиденциальных документов при чрезвычайной ситуации.*	3	
8	Лабораторная работа № 8 **Тема: «Составление политики безопасности предприятия»** *Разработка политики безопасности предприятия в рамках создания КСЗИ.*	3	
9	Лабораторная работа № 9. **Тема: «Подготовка объекта информатизации к аттестации по требованиям безопасности информации. Разработка пакета организационно-распорядительных документов»** *Разработка комплекта инструктивных материалов для абстрактного объекта информатизации перед проведением мероприятий по его аттестации.*	3	
	Итого	**27**	**7,5**

7.4 Наименование практических занятий

№ Темы	**Наименование тем дисциплины, их краткое содержание**	**Объем часов**	**Интерактивная форма проведения**
	8 семестр		
1	Практическое занятие №1. **Тема: «Формальное построение модели защиты автоматизированной системы».** *НА примере абстрактной сети предприятия необходимо сделать формальное описание объекта защиты.*	1,5	
2	Практическое занятие №2 **Тема: «Обзор этапов со-**	1,5	

	здания и составляющих КСЗИ. Составление неформального перечня действий по созданию КСЗИ на абстрактном предприятии» *Закрепление лекционного материала по этапам создания КСЗИ.*		
3	Практическое занятие №3 Тема: **«Определение порядка действий для создания перечня сведений, составляющих коммерческую тайн.»** *Составление неформального перечня сведений, утвержденного на заседании комиссии предприятия*	1,5	
4	Практическое занятие №4 Тема: «Пропускной и внутриобъектовый режим на предприятии» *Закрепление лекционного материала. Составление инструкции по пропускному и внутриобъектовому режиму на предприятии.*	1,5	
5	Практическое занятие № 5 **Тема: «Разработка технологического процесса автоматизированной обработки и хранения информации на предприятии»** *Составление описания технологического процесса обработки информации на объекте информатизации.*	1,5	
6	Практическое занятие №6 **«Подготовка мероприятий на случай возникновения ЧС»** *Разработка инструкции должностных лиц при ЧС на предприятии*	1,5	
7	Лабораторная работа № 7 **«Защита от несанкционированного доступа к информации в автоматизированных системах. Классификация АС.».** *Научиться определять требования к классам защищенности АС в соответствие с руководящими документами ФСТЭК России.*	1,5	
8	Практическое занятие № 8 **Тема: «Организационно-технический контроль мероприятий по защите объектов информатизации.»** *Научиться проводить внутренний объектовый контроль защищенности за состоянием защиты объектов информатизации.*	1,5	
9	Практическое занятие № 9. **Тема: «Программа и методики аттестационных испытаний»** *приобрести практические навыки по составлению программ проведения мероприятий по аттестации объекта информатизации.*	1,5	

	Итого	**13,5**	

7.5 Технологическая карта самостоятельной работы обучающегося

Технологическая карта

Коды реализуемых компетенций	Вид деятельности студентов	Итоговый продукт самостоятельной работы	Средства и технологии оценки	Объем часов, в том числе		
				СРС	Контактная работа с преподавателем	Всего
ОПК-7, ПК-1, ПК-2, ПК-3, ПК-4, ПК-7, ПК-8, ПК-12, ПК-13, ПК-15	Изучение литературы по темам 1-9	Конспект	собеседование	4,36	0,49	4,85
ОПК-7, ПК-1, ПК-2, ПК-3, ПК-4, ПК-7, ПК-8, ПК-12, ПК-13, ПК-15	Подготовка к лекциям	Конспект	собеседование	1,21	0,14	1,35
ОПК-7, ПК-1, ПК-2, ПК-3, ПК-4, ПК-7, ПК-8, ПК-12, ПК-13, ПК-15	подготовка к лабораторным работам	Отчет	отчет письменный	7,29	0,81	8,1
ОПК-7, ПК-1, ПК-2, ПК-3, ПК-4, ПК-7, ПК-8, ПК-12, ПК-13, ПК-15	подготовка к практическим занятиям	Отчет	отчет письменный	6,07	0,68	6,75
ОПК-7, ПК-1, ПК-2, ПК-3, ПК-4, ПК-7, ПК-8, ПК-12, ПК-13, ПК-15	Выполнение курсовой работы	Курсовая работа	Курсовая работа	11,43	1,27	12,7
			Итого	30,37	3,38	33.75

8. Фонд оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине

8.1 Перечень компетенций с указанием этапов их формирования в процессе освоения ОП ВО. Паспорт фонда оценочных средств

Фонд оценочных средств, позволяющий оценить уровень сформированности компетенций, размещен в УМК дисциплины «Техническая защита информации» на кафедре системы управления, информационные технологии и представлен следующими компонентами:

Код оцениваемой компетенции	Этап формирования компетенции (№ темы)	Средства и технологии оценки	Тип контроля (текущий/промежуточный)	Вид контроля (текущий/промежуточный)	Наименование оценочного средства
ОПК-7, ПК-1, ПК-2, ПК-3, ПК-4, ПК-7, ПК-8, ПК-12, ПК-13, ПК-15	1-9	Отчёт письменный	текущий	письменный	Темы индивидуальных заданий для лабораторных занятий
ОПК-7, ПК-1, ПК-2, ПК-3, ПК-4, ПК-7, ПК-8, ПК-12, ПК-13, ПК-15	1-9	Отчёт письменный	текущий	письменный	Темы индивидуальных заданий для практических занятий
ОПК-7, ПК-1, ПК-2, ПК-3, ПК-4, ПК-7, ПК-8, ПК-12, ПК-13, ПК-15	1-9	собеседование	текущий	устный	Вопросы для собеседования
ОПК-7, ПК-1, ПК-2, ПК-3, ПК-4, ПК-7, ПК-8, ПК-12, ПК-13, ПК-15	1-9	Курсовая работа	промежуточный	письменный	Оценочные средства для курсового проекта
		Собеседование	промежуточный	устный	Вопросы к экзамену
					Вопросы для проверки уровня знаний
					Вопросы (задания) для проверки умений и навыков

8.2 Описание показателей и критериев оценивания компетенций на различных этапах их формирования, описание шкалы оценивания

Уровни сформированности	Индикаторы	Дескрипторы			
		2 балла	3 балла	4 балла	5 баллов

компетенций					
(для каждой компетенции)	**ОПК-4**				
	Знать: ▪ значение информации в развитии современного общества, применять информационные технологии для поиска и обработки информации	Не знает: ▪ зна чение информации в развитии современного общества, применять информационные технологии для поиска и обработки информации	Не достаточно хорошо умеет: ▪ Частичные знания в значении-информации в развитии современного общества, применять информационные технологии для поиска и обработки информации	Знает: ▪ значение информации в развитии современного общества, применять информационные технологии для поиска и обработки информации	
	Уметь: ▪ понимает значение информации в развитии современного общества, применять информационные технологии для поиска и обработки информации	Не умеет: ▪ понять значения информации в развитии современного общества, применять информационные технологии для поиска и обработки информации	Частично умеет: ▪ в понимании значения информации в развитии современного общества, применять информационные технологии для поиска и обработки информации	Умеет: ▪ работать в понимании значения информации в развитии современного общества, применять информационные технологии для поиска и обработки информации	
	Владеть: ▪ готовностью к пониманию значения информации в развитии современного общества, применять ин-	Не владеет ▪ готовностью к пониманию значения информации в развитии современного общества,	Частично владеет ▪ готовностью к пониманию значения информации в развитии современно-	Владеет ▪ готовностью к пониманию значения информации в развитии современного общества, применять ин-	

	формационные технологии для поиска и обработки информации	применять информационные технологии для поиска и обработки информации	го общества, применять информационные технологии для поиска и обработки информации	формационные технологии для поиска и обработки информации	
ПК-1					
Базовый	**Уметь:** ▪ работы по установке, настройке и обслуживанию ТСЗИ; ▪ оценивать эффективность применяемых ТСЗИ; ▪ проводить анализ исходных данных для проектирования подсистемы противодействия утечки информации по техническим каналам утечки на объекте информатизации; ▪ вырабатывать обоснованные проектные решения по обеспечению защиты информации	Не умеет: ▪ работы по установке, настройке и обслуживанию ТСЗИ; ▪ оценивать эффективность применяемых ТСЗИ; ▪ проводить анализ исходных данных для проектирования подсистемы противодействия утечки информации по техническим каналам утечки на объекте информатизации; ▪ вырабатывать обоснованные проектные решения по обеспечению защиты информации	Не достаточно хорошо умеет: ▪ работы по установке, настройке и обслуживанию ТСЗИ; ▪ оценивать эффективность применяемых ТСЗИ; ▪ проводить анализ исходных данных для проектирования подсистемы противодействия утечки информации по техническим каналам утечки на объекте информатизации; ▪ вырабатывать обоснованные проектные решения по обеспечению защиты информации	Умеет: ▪ работы по установке, настройке и обслуживанию ТСЗИ; ▪ оценивать эффективность применяемых ТСЗИ; ▪ проводить анализ исходных данных для проектирования подсистемы противодействия утечки информации по техническим каналам утечки на объекте информатизации; ▪ вырабатывать обоснованные проектные решения по обеспечению защиты информации	
	ПК-4				
	Знать: ▪ клас-	Не знает: ▪ клас	Не достаточно хоро-	Знает ▪ клас-	

	сификацию, характеристики технических каналов утечки информации, возможности технических разведок; ▪ методы, способы и средства защиты информации от утечки по техническим каналам, методы и средства контроля эффективности технической защиты информации.	сификацию, характеристики технических каналов утечки информации, возможности технических разведок; ▪ методы, способы и средства защиты информации от утечки по техническим каналам, методы и средства контроля эффективности технической защиты информации.	шо знает классификацию, характеристики технических каналов утечки информации, возможности технических разведок; ▪ методы, способы и средства защиты информации от утечки по техническим каналам, методы и средства контроля эффективности технической защиты информации.	сификацию, характеристики технических каналов утечки информации, возможности технических разведок; ▪ методы, способы и средства защиты информации от утечки по техническим каналам, методы и средства контроля эффективности технической защиты информации.	
	ПК-5				
	Знать порядок организации и проведения аттестации объектов информатизации на соответствие требованиям по защите информации	Не знает порядок организации и проведения аттестации объектов информатизации на соответствие требованиям по защите информации	Не достаточно знает порядок организации и проведения аттестации объектов информатизации на соответствие требованиям по защите информации	Знает на достаточно хорошем уровне порядок организации и проведения аттестации объектов информатизации на соответствие требованиям по защите инфор-мации	
	ПК-12				
	Уметь: ▪ осуществлять технические мероприятия по обеспечению защиты информации от ее утечки по техническим каналам с учетом организа-	▪ Не умеет осуществлять технические мероприятия по обеспечению защиты информации от ее утечки по техническим кана-	▪ Не достаточно хорошо осуществляет технические мероприятия по обеспечению защиты информации от ее утечки по техниче-	▪ Достаточно хорошо умеет осуществлять технические мероприятия по обеспечению защиты информации от ее утечки по техническим каналам с уче-	

	ционной структуры объекта защиты и вероятных угроз; ▪ проводить специальные исследования технических средств и систем для аттестации объектов на соответствие требованиям нормативных документов; ▪ выполнять мероприятия по эксплуатации технических средств защиты информации от ее утечки по техническим каналам	лам с учетом организационной структуры объекта защиты и вероятных угроз; ▪ проводить специальные исследования технических средств и систем для аттестации объектов на соответствие требованиям нормативных документов; выполнять мероприятия по эксплуатации технических средств защиты информации от ее утечки по техническим каналам	ским каналам с учетом организационной структуры объекта защиты и вероятных угроз; ▪ проводить специальные исследования технических средств и систем для аттестации объектов на соответствие требованиям нормативных документов; ▪ выполнять мероприятия по эксплуатации технических средств защиты информации от ее утечки по техническим каналам	том организационной структуры объекта защиты и вероятных угроз; ▪ проводить специальные исследования технических средств и систем для аттестации объектов на соответствие требованиям нормативных документов; ▪ выполнять мероприятия по эксплуатации технических средств защиты информации от ее утечки по техническим каналам	
	ПК-13				
	Уметь проводить экспериментальные исследования технических средств и систем с учетом требований по обеспечению информационной безопасности по методикам норматив-	**Не умеет** проводить экспериментальные исследования технических средств и систем с учетом требований по обеспечению информационной	Не достаточно хорошо проводит экспериментальные исследования технических средств и систем с учетом требований по обеспече-	Достаточно хорошо умеет проводить экспериментальные исследования технических средств и систем с учетом требований по обеспечению информационной безопасности	

	ных документов ФСТЭК.	безопасности по методикам нормативных документов ФСТЭК.	нию информационной безопасности по методикам нормативных документов	по методикам нормативных документов ФСТЭК.	
Повышенный	ПК-1				
	Уметь вырабатывать обоснованные проектные решения по обеспечению защиты информации;				Умеет вырабатывать обоснованные проектные решения по обеспечению защиты информации;
	ПК -4				
	▪ Знать методы, способы и средства защиты информации от утечки по техническим каналам, методы и средства контроля эффектив-ности технической защиты информации				▪ Знает методы, способы и средства защиты информации от утечки по техническим каналам, методы и средства контроля эффектив-ности технической защиты информации
	ПК-5				
	▪ Уметь: выполнять мероприятия по эксплуатации технических средств защиты информации от ее утечки по техническим каналам				Умеет выполнять мероприятия по эксплуатации технических средств защиты информации от ее утечки по техническим каналам

В рамках рейтинговой системы успеваемость студентов по дисциплине оцениваются знания, умения навыки в ходе текущего контроля и промежуточной аттестации.

Текущий контроль
Рейтинговая оценка знаний студента

№ п/п	Вид деятельности студентов	Сроки выполнения	Количество баллов
	8 семестр		
1.	Выполнение лабораторных работ 1-3	6 неделя	25
2.	Выполнение лабораторных работ 4-9	14 неделя	30
	Итого за 8 семестр		**55**

Максимально возможный балл за весь текущий контроль устанавливается равным **55.** Текущее контрольное мероприятие считается сданным, если студент получил за него не менее 60% от установленного для этого контроля максимального балла. Рейтинговый балл, выставляемый студенту за текущее контрольное мероприятие, сданное студентом в установленные графиком контрольных мероприятий сроки, определяется следующим образом:

Уровень выполнения контрольного задания	Рейтинговый балл (в % от максимального балла за контрольное задание)
Отличный	**100**
Хороший	**80**
Удовлетворительный	**60**
Неудовлетворительный	**0**

Промежуточная аттестация в форме **экзамена** предусматривает проведение обязательной экзаменационной процедуры и оценивается 40 баллами из 100. В случае если рейтинговый балл студента по дисциплине по итогам семестра равен 60, то программой автоматически добавляется 32 премиальных балла и выставляется оценка «отлично». Положительный ответ студента на экзамене оценивается рейтинговыми баллами в диапазоне от **20** до **40** (**20**$\leq S_{экз} \leq$**40**), оценка **меньше 20** баллов считается неудовлетворительной.

Шкала соответствия рейтингового балла экзамена 5-балльной системе

Рейтинговый балл по дисциплине	**Оценка по 5-балльной системе**
35 – 40	Отлично
28 – 34	Хорошо
20 – 27	Удовлетворительно

Итоговая оценка по дисциплине, изучаемой в семестре, определяется по сумме баллов, набранных за работу в течение семестра, и баллов, полученных при сдаче экзамена:

Шкала пересчета рейтингового балла по дисциплине в оценку по 5-балльной системе

Рейтинговый балл по дисциплине	***Оценка по 5-балльной системе***
88 – 100	*Отлично*
72 – 87	*Хорошо*
53 – 71	*Удовлетворительно*
<53	*Неудовлетворительно*

Промежуточная аттестация в форме **курсовой работы.** Максимальная сумма балов по **курсовой работе** устанавливается в **100** балов и переводится в оценку по 5-бальной системе в соответствии со шкалой:

Шкала соответствия рейтингового балла 5-бальной системе

Рейтинговый балл	**Оценка по 5-балльной системе**

88 – 100	Отлично
72 – 87	Хорошо
53 – 71	Удовлетворительно
<53	*Неудовлетворительно*

8.3 Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих этап формирования компетенций

Вопросы к экзамену (8 семестр)
Вопросы для проверки уровня обученности:

Знать:

1. Модели нарушителей угроз безопасности предприятия.
2. Защита от утечки информации по техническим каналам в автоматизированных системах.
3. Защита от несанкционированного доступа к информации в автоматизированных системах.
4. Организационно-распорядительные документы организации для подготовки к работе на автоматизированных системах.
5. Особенности защиты речевой информации на предприятии.
6. Условия функционирования КСЗИ на предприятии.
7. Влияние формы собственности на особенности защиты информации ограниченного доступа.
8. Влияние организационно-правовой формы предприятия на особенности защиты информации ограниченного доступа.
9. Факторы, определяющие необходимость защиты периметра здания предприятия.
10. Особенности помещений как объектов защиты для работы по защите информации.
11. Роль и место внутриобъектового и пропускного режимов в системе защиты информации предприятия.
12. Силы и средства, используемые при организации внутриобъектового режима.
13. Модели КСЗИ (принцип формализации требований безопасности и условий функционирования системы).
14. Основные подходы к проектированию КСЗИ на предприятии.
15. Кадровый аспект обеспечения безопасности информации.
16. Основные положения мероприятий по аттестации объектов информатизации.
17. Программа аттестационных испытаний автоматизированной системы.
18. Экспертно-документальный метод проведения аттестационных испытаний.
19. Сертификация средств защиты информации, использующихся при построении КСЗИ предприятия.
20. Виды контроля функционирования КСЗИ.
21. Цели проведения контрольных мероприятий в КСЗИ.

Уметь, владеть:

1. Резервирование информации и отказоустойчивость.
2. Разработка технологического процесса автоматизированной обработки и хранения информации на предприятии.
3. Определение возможностей несанкционированного доступа к речевой информа ции, обрабатываемой во время проведения закрытых совещаний на предприятии.
4. Основные подходы и принципы к организации внутриобъектового режима.
5. Этапы разработки КСЗИ на предприятии.
6. Экономический подход к оценке эффективности комплексной системы защиты информации на предприятии.
7. Организация управления, планирование функционирования и оценка эффективности КСЗИ.
8. Методы проверок и испытаний объектов информатизации, используемые при аттестации.
9. Методики аттестационных испытаний автоматизированной системы.

Тематика курсовых работ

1. Оптимальное построение системы защиты информации для автоматизированной системы на предприятии.
2. Оптимальное построение системы защиты информации для защищаемого помещения на предприятии.
3. Определение возможностей несанкционированного доступа к информации, обрабатываемой средствами вычислительной техники на предприятии.
4. Определение возможностей несанкционированного доступа к речевой информации, обрабатываемой во время проведения закрытых совещаний на предприятии.
5. Актуальные технические каналы утечек конфиденциальной информации на предприятии и меры по их выявлению и защите.
6. Модель нарушителя информационной безопасности предприятия.
7. Особенности помещений как объектов защиты для работы по защите информации.
8. Факторы и методика защиты периметра и здания предприятия от угроз информационной безопасности.
9. Кадровое обеспечение функционирования комплексной системы зашиты информации на предприятии.
10. Экономический подход к оценке эффективности комплексной системы защиты информации на предприятии.
11. Периодический контроль защищенности систем защиты информации на предприятии.

12. Методы обеспечения безопасности информации на предприятии в непредвиденных и чрезвычайных ситуациях.
13. Методики резервирования защищаемой информации и повышения отказоустойчивости систем обработки и хранения информации на предприятии.
14. Критерии и показатели оценки безопасности информации на предприятии.
15. Анализ и оценка информационных рисков, угроз и уязвимостей комплексной системы защиты информации на предприятии.
16. Роль и место технических средств охраны, видеонаблюдения и систем контроля управления доступом в комплексной системе защиты информации на предприятии.
17. Методы и средства превентивной защиты информации на предприятии.
18. Методы и средства аудита комплексной системы защиты информации на предприятии.
19. Анализ факторов, создающих угрозу информационной безопасности предприятия.
20. Меры по предотвращению последствий инцидентов информационной безопасности на предприятии.

8.4 Методические материалы, определяющие процедуры оценивания знаний, умений, навыков, характеризующих этапы формирования компетенций

Процедура проведения экзамена осуществляется в соответствии с Положением о проведении текущего контроля успеваемости и промежуточной аттестации обучающихся по образовательным программам высшего образования в СКФУ. В экзаменационный билет включаются 2 теоретических вопроса. Для подготовки по билету отводится 30 минут.

При подготовке к ответу студенту предоставляется право пользования справочными материалами.

При проверке задания, оцениваются последовательность, рациональность выполнения, точность расчетов, правильность выполнения чертежей и рисунков.

Для выполнения курсовой работы по дисциплине необходимо получить индивидуальное задание, ознакомиться с исходными данными, изучить основную литературу. При проверке задания оцениваются понимание студента темы и содержание работы.

При защите курсовой работы оцениваются: практическая и научная значимость работы, оценка работы рецензентом и ответы на вопросы, а также учитывается качество оформления проекта (пояснительная записка и приложения, если они есть).

Текущая аттестация студентов проводится преподавателями, ведущими лабораторные по дисциплине, в следующих формах: отчет письменный, собеседование, курсовая работа.

Допуск к защите отчетов по лабораторным работам происходит при наличии у студентов печатного варианта отчета. Защита отчета проходит в форме доклада студента по выполненной работе и ответов на вопросы преподавателя. Максимальное количество баллов студент получает, если оформление отчета соответсвует установленным требованиям, а отчет полностью раскрывает суть работы. Основанием для снижением оценки являются:

- частично не соовествует установленным требованиям;

- в отчете непольностью раскрывается суть работы.

Отчет может быть отправлен на доработку в следующих случаях:

- полностью не соовествует установленным требованиям;
- не раскрыта суть работы.

Процедура проведения собеседования проводится в следующей форме: студенту выдается вопрос для собеседования, он готовит ответ (в письменной или устной форме) и отчитывается преподавателю по заданному вопросу. При подготовке к ответу студенту предоставляется право пользования справочными материалами. При проверке задания, оцениваются:

- последовательность и рациональность выполнения;
- точность вычислений;
- знание технологий, использованных при выполнении задания.

Критерии оценивания ответов на вопросы собеседования, отчёта, курсовой работы приведены в Фонде оценочных средств по дисциплине «Комплексная система защиты информации на предприятии».

9 Методические указания для обучающихся по освоению дисциплины

На первом этапе необходимо ознакомиться с рабочей программой дисциплины, в которой рассмотрено содержание тем дисциплины лекционного курса, взаимосвязь тем лекций с практическими занятиями, темы и виды самостоятельной работы. По каждому виду самостоятельной работы предусмотрены определённые формы отчетности.

Для успешного освоения дисциплины, необходимо выполнить следующие виды самостоятельной работы, используя рекомендуемые источники информации

№ п/п	Виды самостоятельной работы	Рекомендуемые источники информации (№ источника)			
		Основная	Дополнительная	Методическая литература	Интернет-ресурсы
1.	изучение литературы по темам 1-9	1,2	1,2	1-3	1-2
2.	проработка лекционного материала	1,2	1,2	1-3	1-2
3.	подготовка к лабораторным работам	1,2	1,2	1-3	1-2
4.	подготовка к практическим занятиям	1,2	1,2	1-3	1-2
5.	Выполнение курсовой работы	1,2	1,2	1-4	1-2

10. Учебно-методическое и информационное обеспечение дисциплины

10.1. Перечень основной и дополнительной литературы, необходимой для освоения дисциплины.

10.1.1. Перечень основной литературы:

1. Астахова А.В. Информационные системы в экономике и защита информации на предприятиях — участниках ВЭД [Электронный ресурс]: учебное пособие/ Астахова А.В.— Электрон. текстовые данные.— СПб.: Троицкий мост, 2014.— 216 с.— Режим доступа: http://www.iprbookshop.ru/40860.— ЭБС «IPRbooks», по паролю

2. Сердюк, В.А. Организация и технологии защиты информации: обнаружение и предотвращение информационных атак в автоматизированных системах предприятий : учебное пособие / В.А. Сердюк ; Высшая Школа Экономики Национальный Исследова-

тельский Университет. - М. : Издательский дом Высшей школы экономики, 2015. - 574 с. : ил. - Библ. в кн. - ISBN 978-5-7598-0698-1 ; То же [Электронный ресурс]. - URL: //biblioclub.ru/index.php?page=book&id=440285.

10.1.2. Перечень дополнительной литературы:

1. Разработка системы технической защиты информации: учебное пособие [Электронный ресурс]/ В.И. Аверченков, М.Ю. Рытов, А.В. Кувыклин, Т.Р. Гайнулин. – 2-е изд., стер. – М.: Флинта, 2014. – URL:http://biblioclub.ru/index.php?page=book&id=93349
2. Чипига, А.Ф. Информационная безопасность автоматизированных систем: учеб. пособие/ А. Ф. Чипига- М.: Гелиос АРВ, 2013.

10.2. Перечень учебно-методического обеспечения самостоятельной работы обучающихся по дисциплине:

1. Методические рекомендации для студентов по организации и проведению самостоятельной работы по дисциплине Комплексная система защиты информации на предприятии.
2. Методические указания по выполнению лабораторных работ по дисциплине Комплексная система защиты информации на предприятии.
3. Методические указания по выполнению практических занятий по дисциплине Комплексная система защиты информации на предприятии.
4. Методические указания по выполнению курсовой работы по дисциплине Комплексная система защиты информации на предприятии.

10.3. Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины:

1. http://biblioclub.ru
2. http://elibrary.ru/

11.1.5. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине, включая перечень программного обеспечения и информационных справочных систем

***Информационные технологии*:**

- Персональные компьютеры, объединенные в локальную сеть и имеющие выход в Интернет;
- Мультимедиа лекции

***Информационные справочные системы*:**

- www.consultant.ru
- www.garant.ru

***Перечень программного обеспечения и информационно-справочных систем*:**

Стандартные приложения Windows

12. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине обеспечение дисциплины

1. Лекционная аудитория, оснащенная мультимедийным проектором;

2. Компьютерная лаборатория, оснащенная персональными компьютерами в количестве 10 шт., объединенными в локальную сеть, имеющими в списке установленого ПО пакет офисных приложений и имеющими выход в Интернет.

13. Особенности освоения дисциплины (модуля) лицами с ограниченными возможностями здоровья

Обучающимся с ограниченными возможностями здоровья предоставляются специальные учебники, учебные пособия и дидактические материалы, специальные технические средства обучения коллективного и индивидуального пользования, услуги ассистента (помощника), оказывающего обучающимся необходимую техническую помощь, а также услуги сурдопереводчиков и тифлосурдопереводчиков.

Освоение дисциплины (модуля) обучающимися с ограниченными возможностями здоровья может быть организовано совместно с другими обучающимися, а так же в отдельных группах.

Освоение дисциплины (модуля) обучающимися с ограниченными возможностями здоровья осуществляется с учетом особенностей психофизического развития, индивидуальных возможностей и состояния здоровья.

В целях доступности получения высшего образования по образовательной программе лицами с ограниченными возможностями здоровья при освоении дисциплины (модуля) обеспечивается:

1) для лиц с ограниченными возможностями здоровья по зрению:

- присутствие ассистента, оказывающий студенту необходимую техническую помощь с учетом индивидуальных особенностей (помогает занять рабочее место, передвигаться, прочитать и оформить задание, в том числе, записывая под диктовку),
- письменные задания, а также инструкции о порядке их выполнения оформляются увеличенным шрифтом,
- специальные учебники, учебные пособия и дидактические материалы (имеющие крупный шрифт или аудиофайлы),
- индивидуальное равномерное освещение не менее 300 люкс,
- при необходимости студенту для выполнения задания предоставляется увеличивающее устройство;

2) для лиц с ограниченными возможностями здоровья по слуху:

- присутствие ассистента, оказывающий студенту необходимую техническую помощь с учетом индивидуальных особенностей (помогает занять рабочее место, передвигаться, прочитать и оформить задание, в том числе, записывая под диктовку),
- обеспечивается наличие звукоусиливающей аппаратуры коллективного пользования, при необходимости обучающемуся предоставляется звукоусиливающая аппаратура индивидуального пользования;
- обеспечивается надлежащими звуковыми средствами воспроизведения информации;

3) для лиц с ограниченными возможностями здоровья, имеющих нарушения опорно-двигательного аппарата (в том числе с тяжелыми нарушениями двигательных функций верхних конечностей или отсутствием верхних конечностей)

- письменные задания выполняются на компьютере со специализированным программным обеспечением или надиктовываются ассистенту;
- по желанию студента задания могут выполняться в устной форме.