МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное учреждение высшего образования
«СЕВЕРО-КАВКАЗСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»
Пятигорский институт (филиал) СКФУ

УТВЕРЖДАЮ
Зам. директора по учебной работе
Пятигорского института (филиал)
СКФУ
_____ М.В. Мартыненко
«28» марта 2022 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ
«КОМПЛЕКСНАЯ СИСТЕМА ЗАЩИТЫ ИНФОРМАЦИИ НА ПРЕДПРИЯТИИ»

Направление подготовки/специальность **10.03.01 Информационная безопасность**
Направленность (профиль)/специализация **Безопасность компьютерных систем**
Форма обучения очная
Год начала обучения 2022
Реализуется в 7,8 семестре

Разработано
Доцент кафедры СУиИТ, кандидат техн. наук, доцент
Мартиросян К.В.

Пятигорск 2022 г.

1. Цель и задачи освоения дисциплины (модуля)

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 (модуля) в структуре образовательной программы

Дисциплина «Комплексная система защиты информации на предприятии» относится к дисциплинам обязательной части. Ее освоение происходит в 8 семестре.

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

Код, формулировка компетенции	Код, формулировка индикатора	Планируемые результаты обучения по дисциплине (модулю), характеризующие этапы формирования компетенций, индикаторов
ПК-9 Способность осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических материалов, составлять обзор по вопросам обеспечения информационной безопасности по профилю своей профессиональной деятельности	ИД-1 ПК-9 Знает методы поиска научно-технической информации. ИД-2 ПК-9 Способен выбирать необходимую информацию в области информационной безопасности; составлять обзор по вопросам обеспечения информационной безопасности. ИД-3 ПК-9 Владеет навыками изучения научно-технической литературы по вопросам обеспечения информационной безопасности по профилю своей профессиональной деятельности.	Умеет осуществлять поиск, критический анализ и синтез информации, применять системный подход для решения поставленных задач, осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических документов в целях решения задач профессиональной деятельности, осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических материалов, составлять обзор по вопросам обеспечения информационной безопасности по профилю своей профессиональной деятельности. Умеет при решении профессиональной задач организовывать защиту информации по
ОПК-12 Способен проводить подготовку исходных данных для проектирования подсистем, средств обеспечения защиты информации и для технико-экономического обоснования	ИД-1 ОПК-12 Понимает принципы работы средств обеспечения защиты информации; основные стандарты информационной безопасности; общие принципы организации информационных систем. ИД-2 ОПК-12 Способен готовить исходные данные для	

соответствующих проектных решений	проектирования информационных систем. ИД-3 ОПК-12 Владеет методами экономического обоснования проектных решений в области информационной безопасности; методами оценки рисков; методами предотвращения угроз конфиденциальности, целостности и доступности информации.	ограниченного доступа в соответствии с нормативными правовыми актами, нормативными и методическими документами Федеральной службы безопасности Российской Федерации, Федерации службы по техническому и экспортному контролю, проводить подготовку исходных данных для проектирования подсистем, средств обеспечения защиты информации и для технико-экономического обоснования соответствующих проектных решений, участвовать в работах по реализации политики информационной безопасности, применять комплексный подход к обеспечению информационной безопасности объекта защиты. Умеет принимать участие в организации и сопровождении аттестации объекта информатизации по требованиям безопасности информации, принимать участие в организации и проведении контрольных проверок работоспособности и эффективности применяемых программных, программно-аппаратных и технических средств защиты информации, оформлять рабочую техническую документацию с учетом действующих нормативных и методических документов, проводить эксперименты по заданной методике, обработку, оценку погрешности и достоверности их результатов, принимать участие в проведении экспериментальных исследований системы защиты информации. Умеет при решении профессиональной задач организовывать защиту информации по
ОПК-1.4 Способен оценивать уровень безопасности компьютерных систем и сетей, в том числе в соответствии с нормативными и корпоративными требованиями	ИД1 ОПК-1.4 Оценивает уровень безопасности компьютерных систем и сетей, в том числе в соответствии с нормативными и корпоративными требованиями	
ПК-4 Способность участвовать в работах по реализации политики информационной безопасности, применять комплексный подход к обеспечению информационной безопасности объекта защиты	ИД-1 ПК-4 Имеет знания виды комплексного подхода в организации политики информационной безопасности. ИД-2 ПК-4 Умеет формулировать, настраивать политики безопасности. ИД-3 ПК-4 Владеет навыками формулирования и контролирования соблюдения требований политики безопасности.	

		ограниченного доступа в соответствии с нормативными правовыми актами, нормативными и методическими документами Федеральной службы безопасности Российской Федерации, Федерации службы по техническому и экспортному контролю, проводить подготовку исходных данных для проектирования подсистем, средств обеспечения защиты информации и для технико-экономического обоснования соответствующих проектных решений, участвовать в работах по реализации политики информационной безопасности, применять комплексный подход к обеспечению информационной безопасности объекта защиты.

4. Объем учебной дисциплины (модуля) и формы контроля

Объем занятий:	З.е.	Астр. ч.	Из них в форме практической подготовки
Всего:	6	162	
Из них аудиторных:		85,5	
Лекций		36	
Лабораторных работ		36	
Практических занятий		13,5	
Самостоятельной работы		22,5	
Формы контроля:			
Экзамен	8 семестр		

5. Содержание дисциплины (модуля), структурированное по темам (разделам) с указанием количества часов и видов занятий

5.1.Тематический план дисциплины (модуля)

№	Раздел (тема) дисциплины	Реализуемые компетенции, индикаторы	Контактная работа обучающихся с преподавателем, часов	Самостоятельная

			Лекции	Практические занятия	Лабораторные работы	Групповые консультации	
7 семестр							
1	Базовые понятия дисциплины	ИД-1 ПК-9, ИД-2 ПК-9, ИД-3 ПК-9, ИД-1 ОПК-12, ИД-2 ОПК-12, ИД-3 ОПК-12,	4,5	3	4,5		3
2	Сущность и задачи комплексной системы защиты информации	ИД1 ОПК-1.4, ИД-1 ПК-4, ИД-2 ПК-4, ИД-3 ПК-4	4,5	3	4,5		3
3	Принципы организации и этапы разработки комплексной системы защиты информации	ИД-1 ПК-9, ИД-2 ПК-9, ИД-3 ПК-9, ИД-1 ОПК-12, ИД-2 ОПК-12, ИД-3 ОПК-12,	4,5	3	4,5		3
4	Определение объектов защиты	ИД1 ОПК-1.4, ИД-1 ПК-4, ИД-2 ПК-4, ИД-3 ПК-4	4,5	3	4,5		3
5	Разработка модели комплексной системы защиты информации	ИД-1 ПК-9, ИД-2 ПК-9, ИД-3 ПК-9, ИД-1 ОПК-12, ИД-2 ОПК-12, ИД-3 ОПК-12,	4,5	0,75	4,5		0,75
6	Определение и нормативное закрепление состава защищаемой информации	ИД1 ОПК-1.4, ИД-1 ПК-4, ИД-2 ПК-4, ИД-3 ПК-4	4,5	0,75	4,5		0,75
	Итого за 7семестр		**27**	**13,5**	**27**		**13,5**
8 семестр							
7	Тема 1. Сущность комплексной защиты информации на предприятии (в организации, учреждении).	ИД-1 ПК-9, ИД-2 ПК-9, ИД-3 ПК-9, ИД-1 ОПК-12, ИД-2 ОПК-12, ИД-3 ОПК-12, ИД1 ОПК-1.4, ИД-1 ПК-4, ИД-2 ПК-4, ИД-3 ПК-4	1,5				
8	Тема 2. Организация КСЗИ, этапы разработки и факторы, влияющие на организацию КСЗИ	ИД-1 ПК-9, ИД-2 ПК-9, ИД-3 ПК-9, ИД-1 ОПК-12, ИД-2 ОПК-12, ИД-3 ОПК-12, ИД1 ОПК-1.4, ИД-1 ПК-4, ИД-2 ПК-4, ИД-3 ПК-4	1,5		1,5		1,5
9	Тема 3. Определение объектов защиты предприятия и утверждение перечней защищаемой	ИД-1 ПК-9, ИД-2 ПК-9, ИД-3 ПК-9, ИД-1 ОПК-12, ИД-2 ОПК-12, ИД-3 ОПК-12, ИД1 ОПК-1.4, ИД-1 ПК-4, ИД-2 ПК-4, ИД-3 ПК-4	1,5		1,5		1,5
10	Тема 4. Организационное	ИД-1 ПК-9, ИД-2 ПК-	1,5				

	построение КСЗИ. Введение внутриобъектового режима на предприятии.	9, ИД-3 ПК-9, ИД-1 ОПК-12, ИД-2 ОПК-12, ИД-3 ОПК-12, ИД1 ОПК-1.4, ИД-1 ПК-4, ИД-2 ПК-4, ИД-3 ПК-4					
11	Тема 5. Определение угроз безопасности информации на предприятии.	ИД-1 ПК-9, ИД-2 ПК-9, ИД-3 ПК-9, ИД-1 ОПК-12, ИД-2 ОПК-12, ИД-3 ОПК-12, ИД1 ОПК-1.4, ИД-1 ПК-4, ИД-2 ПК-4, ИД-3 ПК-4	1,5		1,5		1,5
12	Тема 6. Дестабилизирующие негативные воздействия на информацию и их нейтрализация.	ИД-1 ПК-9, ИД-2 ПК-9, ИД-3 ПК-9, ИД-1 ОПК-12, ИД-2 ОПК-12, ИД-3 ОПК-12, ИД1 ОПК-1.4, ИД-1 ПК-4, ИД-2 ПК-4, ИД-3 ПК-4	0,75		0,75		0,75
13	Тема 7. Возможности несанкционированного доступа к защищаемой информации. Методы защиты объектов информатизации.	ИД-1 ПК-9, ИД-2 ПК-9, ИД-3 ПК-9, ИД-1 ОПК-12, ИД-2 ОПК-12, ИД-3 ОПК-12, ИД1 ОПК-1.4, ИД-1 ПК-4, ИД-2 ПК-4, ИД-3 ПК-4	0,75		0,75		0,75
14	Тема 8. Методики оценки эффективности принятых мер по созданию КСЗИ	ИД-1 ПК-9, ИД-2 ПК-9, ИД-3 ПК-9, ИД-1 ОПК-12, ИД-2 ОПК-12, ИД-3 ОПК-12, ИД1 ОПК-1.4, ИД-1 ПК-4, ИД-2 ПК-4, ИД-3 ПК-4			1,5		1,5
15	Тема 9. Система аттестации объектов информатизации.	ИД-1 ПК-9, ИД-2 ПК-9, ИД-3 ПК-9, ИД-1 ОПК-12, ИД-2 ОПК-12, ИД-3 ОПК-12, ИД1 ОПК-1.4, ИД-1 ПК-4, ИД-2 ПК-4, ИД-3 ПК-4			1,5		1,5
	Итого за 8 семестр		**9**		**9**		**9**
	ИТОГО		**36**	**13,5**	**36**		**22,5**

5.2 Наименование и содержание лекций

№ Темы дисциплины	Наименование тем дисциплины, их краткое содержание	Объем часов	Из них практическая подготовка, часов
7 семестр			
1	Базовые понятия дисциплины 1. Предмет и задачи курса. Взаимосвязь [illegible] темы курса, [illegible]м и видам научно-	4,5	

	исследовательской работы студентов по проблемам курса. Формы контроля знаний		
2	Сущность и задачи комплексной системы защиты информации 1. Понятие и сущность КСЗИ 2. Назначение КСЗИ	4,5	
3	Принципы организации и этапы разработки комплекснойсистемы защиты информации 1. Методологические основы организации КСЗИ 2. КСЗИ как сложная человеко-машинная система	4,5	
4	Определение объектов защиты 1. Значение носителей защищаемой информации как объектов защиты 2. Факторы, определяющие состав носителей информации 3. Методика выявления состава носителей защищаемой информации	4,5	
5	Разработка модели комплексной системы защиты информации 1. Понятие модели объекта, основные виды моделей и их характеристика 2. Модель как инструмент количественного и качественного анализа комплексной системы защиты информации 3. Значение моделирования процессов комплексной системы защиты информации	4,5	
6	Определение и нормативное закрепление состава защищаемой информации 1. Методика определения состава защищаемой информации 2. Этапы работы по выявлению состава защищаемой информации	4,5	
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	
2	**Тема** Организация КСЗИ, этапы разработки и факторы, влияющие на *Принципы построения КСЗИ на предприятии. Общее содержание работ по организации КСЗИ.*	1,5	

	Методологические основы организации КСЗИ. *Модели КСЗИ (принцип формализации требований безопасности и условий функционирования системы).* *Этапы разработки КСЗИ на предприятии.*		
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	
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 системе защиты информации предприятия.* *Основные подходы и принципы к организации внутриобъектового режима.*	1,5	
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	
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.* *Планирование мероприятий на случай возникновения ЧС.*	0,75	
7	**Тема** Возможности несанкционированного	0,75	

	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.*		
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.*		
9	**Тема** Система аттестации объектов информатизации. *Основные положения мероприятий по аттестации объектов информатизации. Методы проверок и испытаний объектов информатизации, используемые при аттестации.*		
	Итого за 8 семестр	**9**	
	ИТОГО	**36**	

5.3 Наименование лабораторных работ

№ Темы дисциплины	Наименование тем дисциплины, их краткое содержание	Объем часов	Из них практическая подготовка, часов
7 семестр			
1	Сущность и общее содержание комплексной системы защиты информации	4,5	
2	Определение и нормативное закрепление состава защищаемой информации	4,5	
3	Разработка моделей объектов защиты	4,5	
4	Моделирование комплексной системы защиты информации	4,5	
5	Подбор технических средств для защиты информации	4,5	
6	Система контроля и управления доступом	4,5	
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.*		
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.*	1,5	
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.*	1,5	
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.*		
5	Лабораторная работа № 5 **Тема: «Разработка модели 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.*	1,5	
6	Лабораторная работа №6 Тема:	0,75	

	«Проведение мероприятий по паспортизации объектов информатизации предприятия. Разработка технического паспорта» *Составление технического паспорта на формальный объект информатизации по форме, утвержденной СТР-К.*		
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.*	0,75	
8	Лабораторная работа № 8 **Тема: «Составление политики безопасности предприятия»** *Разработка политики безопасности предприятия в рамках создания КСЗИ.*	1,5	
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.*	1,5	
	Итого за 8 семестр	**9**	
	Итого	**36**	

5.4 Наименование практических занятий

№ Темы дисциплины	Наименование тем дисциплины, их краткое содержание	Объем часов	Из них практическая подготовка, часов
7 семестр			
1	Понятийный аппарат дисциплины	3	
2	Задачи комплексной системы защиты информации	3	
3	Принципы организации комплексной системы защиты информации	3	
4	Определение объектов защиты	3	
5	Этапы создания комплексной системы защиты информации	0,75	
6	Потенциальные каналы и методы несанкционированного доступа к	0,75	

	информации		
	Итого за 7 семестр	**13,5**	
	Итого	**13,5**	

5.5 Технологическая карта самостоятельной работы обучающегося

Коды реализуемых компетенций, индикатора(ов)	Вид деятельности студентов	Средства и технологии оценки	Объем часов, в том числе		
			СРС	Контактная работа с преподавателем	Всего
8 семестр					
ИД-1 ПК-9, ИД-2 ПК-9, ИД-3 ПК-9, ИД-1 ОПК-12, ИД-2 ОПК-12, ИД-3 ОПК-12, ИД1 ОПК-1.4, ИД-1 ПК-4, ИД-2 ПК-4, ИД-3 ПК-4,	Самостоятельное изучение литературы	Собеседование	5,67	0,63	6,3
ИД-1 ПК-9, ИД-2 ПК-9, ИД-3 ПК-9, ИД-1 ОПК-12, ИД-2 ОПК-12, ИД-3 ОПК-12, ИД1 ОПК-1.4, ИД-1 ПК-4, ИД-2 ПК-4, ИД-3 ПК-4	Подготовка к лабораторным занятиям	Собеседование	2,43	0,27	2,7
Итого за 8 семестр			8,1	0,9	9
Итого			8,1	0,9	9

6. Фонд оценочных средств для проведения текущего контроля успеваемости и промежуточной аттестации обучающихся по дисциплине (модулю)

Фонд оценочных средств (ФОС) для проведения текущего контроля успеваемости и промежуточной аттестации обучающихся по дисциплине «Комплексная система защиты информации на предприятии» базируется на перечне осваиваемых компетенций с указанием этапов их формирования в процессе освоения дисциплины (модуля). ФОС обеспечивает объективный контроль достижения запланированных результатов обучения. ФОС включает в себя:

- описание показателей и критериев оценивания компетенций на различных этапах их формирования, описание шкал оценивания;
- методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций;
- типовые контрольные задания и иные материалы, необходимые для оценки знаний, умений и уровня овладения формируемыми компетенциями в процессе освоения дисциплины (модуля).

ФОС является приложением к данной программе дисциплины (модуля).

7. Методические указания для обучающихся по освоению дисциплины

Приступая к работе, каждый студент должен принимать во внимание следующие положения:

Дисциплина построена по тематическому принципу, каждая тема представляет собой логически завершенный раздел.

Лекционный материал посвящен рассмотрению ключевых, базовых положений курсов и разъяснению учебных заданий, выносимых на самостоятельную работу студентов.

Практические работы направлены на приобретение опыта практической работы в соответствующей предметной области.

Самостоятельная работа студентов направлена на самостоятельное изучение дополнительного материала, подготовку к практическим занятиям, а также выполнения всех видов самостоятельной работы.

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

8. Учебно-методическое и информационное обеспечение дисциплины

8.1. Перечень основной и дополнительной литературы, необходимой для освоения дисциплины (модуля)

8.1.1. 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 Исследовательский 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.

8.1.2. 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.

8.2 Перечень учебно-методического обеспечения самостоятельной работы обучающихся по дисциплине (модулю)

1. Методические указания по выполнению лабораторных работ по дисциплине «Комплексная система защиты информации на предприятии».
2. Методические рекомендации для студентов по организации самостоятельной работы по дисциплине «Комплексная система защиты информации на предприятии».

8.3. Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины (модуля)

1. www.intuit.ru – национальный открытый университет «ИНТУИТ»;
2. www.window.edu.ru –единое окно доступа к образовательным ресурсам;
3. www.citforum.ru – сервер информационных технологий.
4. http://biblioclub.ru
5. http://elibrary.ru/
6.

9. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине (модулю), включая перечень программного обеспечения и информационных справочных систем

При освоении знаний используется компьютерная техника, демонстрации презентационных мультимедийных материалов. На семинарских и практических занятиях

студенты представляют презентации, подготовленные ими в часы самостоятельной работы.

Информационно-справочные и информационно-правовые системы, используемые при изучении дисциплины:

1	КонсультантПлюс - http://www.consultant.ru/

Программное обеспечение:

1	Операционная система: Microsoft Windows 8: 2013-02(3000). Бессрочная лицензия. Договор № 01-эа/13 от 25.02.2013. Окончание бесплатной поддержки – 2023-01 ИЛИ Операционная система: Microsoft Windows 10: 2016-08(20), 2017-10(67), 2018-01(18), 2018-04(6), 2018-05(6), 2019-02(7). Бессрочная лицензия. Договоры № 27-эа/16 от 02.08.2016. и № 0321100021117000009_229123 от 10.10.2017. На текущий момент окончания поддержки не анонсировано.
2	Базовый пакет программ Microsoft Office (Word, Excel, PowerPoint). MicrosoftOfficeStandard 2013: договор № 01-эа/13 от 25.02.2013г., Лицензирование Microsoft Office https://support.microsoft.com/ru-ru/lifecycle/search/16674 Дата начала жизненного цикла 09.01.2013г.; набор обновлений Office 2013 Service Pack1 Дата начала жизненного цикла 25.02.2014г., Дата окончания основной фазы поддержки 10.04.2018; Дополнительная дата окончания поддержки 11.04.2023г.

10. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине (модулю)

Лекционные занятия	Учебная аудитория для проведения учебных занятий, оснащена мультимедиа оборудованием и техническими средствами обучения. Мультимедийное оборудование: проектор, компьютер, экран настенный. Комплект учебной мебели.
Лабораторные занятия	Лаборатория информационных систем, оснащенное персональными компьютерами, мультимедийным оборудованием: проектор, компьютер, экран настенный и комплектом учебной мебели.
Самостоятельная работа	Помещения для самостоятельной работы обучающихся, оснащенное компьютерной техникой с возможностью подключения к сети «Интернет» и обеспечением доступа к электронной информационно-образовательной среде.

Учебные аудитории для проведения учебных занятий, оснащены оборудованием и техническими средствами обучения.

Помещения для самостоятельной работы обучающихся, оснащенные компьютерной техникой с возможностью подключения к сети "Интернет" и обеспечением доступа к электронной информационно-образовательной среде.

11. 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 также 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.