Документ подписан простой электронной подписью
Информация о владельце:
ФИО: Задорожная Людмила Ивановна
Должность: Проректор по учебной работе
Дата подписания: 03.10.2023 10:19:13
Уникальный программный ключ:
faa404d1aeb2a023b5f4a331ee5ddc540496512d

МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное образовательное учреждение высшего образования

«Майкопский государственный технологический университет»

Факультет информационных систем в экономике и юриспруденции

Кафедра Информационной безопасности и прикладной информатики

УТВЕРЖДАЮ
Проректор по учебной работе
_____Л.И. Задорожная
«_____» _____ 20___г.

РАБОЧАЯ ПРОГРАММА

по дисциплине	**Б1.О.23 Организационное и правовое обеспечение информационной безопасности**
по направлению подготовки	10.03.01 Информационная безопасность
по профилю подготовки (специализации)	направленность (профиль) N 2 \"Организация и технология защиты информации\" (по отрасли или в сфере профессиональной деятельности)
квалификация (степень) выпускника	Бакалавр
форма обучения	Очная,
год начала подготовки	2022

Майкоп

Рабочая программа составлена на основе ФГОС ВО и учебного плана МГТУ по направлению подготовки (специальности) 10.03.01 Информационная безопасность

Составитель рабочей программы:

Доцент кафедры информационной безопасности и прикладной информатики,	Подписано простой ЭП 08.11.2022	Козлова Наталья Шумафовна
(должность, ученое звание, степень)	(подпись)	(Ф.И.О.)

Рабочая программа утверждена на заседании кафедры:

Информационной безопасности и прикладной информатики

(название кафедры)

Заведующий кафедрой:

18.01.2023	Подписано простой ЭП 18.01.2023	Чундышко Вячеслав Юрьевич
	(подпись)	(Ф.И.О.)

Согласовано:

Руководитель ОПОП
заведующий выпускающей кафедрой
по направлению подготовки (специальности)

18.01.2023	Подписано простой ЭП 18.01.2023	Чундышко Вячеслав Юрьевич
	(подпись)	(Ф.И.О.)

1. Цели и задачи учебной дисциплины (модуля)

Цель дисциплины «Организационное и правовое обеспечение информационной безопасности» приобретение студентами знаний по основам правового регулирования отношений в сфере информационной безопасности и организационным мероприятиям по защите информации, а также формирование практических навыков работы в реальных конкретных условиях.

Задачи дисциплины:

- знать основы организационной и правовой защиты информации, ее современные проблемы и терминологию, а также основные документы, регламентирующую организационную безопасность на объекте;

- изучить руководящие документы по обеспечению режима секретности и конфиденциальности на объекте;

- получить базовые представления о типовой структуре службы безопасности, ее основные задачи и функции должностных лиц;

– оценивать состояние организационной защиты информации на объекте;

– определять рациональные меры по обеспечению организационной и правовой защиты на объекте;

– организовать работу персонала с конфиденциальной информацией.

– иметь навыки выявления угроз информационной безопасности объекта и обеспечения режима секретности и конфиденциальности на объекте.

2. Место дисциплины (модуля) в структуре ОП по направлению подготовки (специальности)

Дисциплина входит в перечень курсов базовой части. Она имеет логические и содержательно-методические связи с дисциплинами по выбору базовой и вариативной частей профессионального цикла «Документоведение» «Защита и обработка конфиденциальных документов», «Защита интеллектуальной собственности и патентоведение», «Основы информационной безопасности» и др.

Дисциплина основана на знаниях научных основ и закономерностей развития общества.

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

Процесс изучения дисциплины направлен на формирование следующей(их) компетенции(й):

ОПК-2.3.1	Знает национальные, межгосударственные и международные стандарты в области защиты информации, нормативные правовые акты в области защиты информации, руководящие и методические документы уполномоченных федеральных органов исполнительной власти в области внедрения и эксплуатации средств защиты информации
ОПК-2.3.2	Умеет документировать процедуры и результаты контроля функционирования системы защиты информации; проводить испытания программно-технических средств защиты информации от НСД и специальных воздействий на соответствие требованиям по безопасности информации и техническим условиям
ОПК-2.3.3	Владеет навыками внесения изменений в эксплуатационную документацию и организационно-распорядительные документы по системе защиты информации; навыками разработки программ и методик испытаний опытного образца программно-технического средства защиты информации от НСД и специальных воздействий на соответствие техническим условиям
ОПК-2.4.1	Знает критерии оценки защищенности объекта информатизации, технические средства контроля эффективности мер защиты информации, методы измерений, контроля и технических расчетом характеристик программно-аппаратных средств защиты информации
ОПК-2.4.2	Умеет осуществлять контроль обеспечения уровня защищенности объектов информатизации
ОПК-2.4.3	Владеет навыками оценки защищенности объектов информатизации с помощью типовых программных средств
ОПК-5.1	Знает основы законодательства Российской Федерации, нормативные правовые акты, нормативные и методические документы в области информационной безопасности и защиты информации, правовые основы организации защиты государственной тайны и конфиденциальной информации, правовую характеристику преступлений в сфере компьютерной информации и меры ответственности за утрату, разглашение, модификацию и уничтожение защищаемой информации
ОПК-5.2	Умеет обосновывать решения, связанные с реализацией правовых норм по защите информации в пределах должностных обязанностей, предпринимать необходимые меры по восстановлению нарушенных прав
ОПК-5.3	Владеет навыками разрабатывать локальные правовые документы, регламентирующие работу по обеспечению информационной безопасности в организации
ОПК-6.1	Знает нормативные, руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации
ОПК-6.2	Умеет разрабатывать проекты локальных нормативных документов, регламентирующих защиту информации ограниченного доступа в организации
ОПК-6.3	Владеет навыками по разработке политики безопасности объекта информатизации
ОПК-9.1	Знает основные понятия и задачи криптографии, математические модели криптографических систем; способы и средства защиты информации от утечки по техническим каналам и контроля эффективности защиты информации
ОПК-9.2	Умеет применять математические модели для оценки стойкости СКЗИ и использовать в автоматизированных системах; пользоваться нормативными документами в области технической защиты информации

ПК-5.1	Знает нормативные правовые акты, методические документы, национальные стандарты в области защиты информации ограниченного доступа и аттестации объектов информатизации на соответствие требованиям по защите информации
ПК-5.2	Умеет разрабатывать программы и методики аттестационных испытаний выделенных (защищаемых) помещений на соответствие требованиям по защите информации, проводить аттестационные испытания, оформлять заключение по результатам аттестации выделенных (защищаемых) помещений на соответствие требованиям по защите информации
ПК-5.3	Владеет навыками подготовки аттестата соответствия выделенных (защищаемых) помещений требованиям по защите информации
ПК-7.1	Знает нормативные правовые акты, методические документы, национальные стандарты в области защиты информации ограниченного доступа, проектирования средств защиты информации, сертификации средств защиты информации на соответствие требованиям по безопасности информации и аттестации объектов информатизации на соответствие требованиям по защите информации, стандарты ЕСКД, ЕСТД и ЕСПД
ПК-7.2	Умеет оформлять рабочую и эксплуатационную документацию на средства и системы информатизации в защищенном исполнении
ПК-7.3	Владеет навыками разработки технического проекта средства и/или системы информатизации в защищенном исполнении
ПК-8.2	Умеет разрабатывать и реализовывать организационные меры, обеспечивающие эффективность системы защиты информации
УК-2.1	Формулирует в рамках поставленной цели совокупность взаимосвязанных задач, обеспечивающих ее достижение в соответствии с действующим законодательством
УК-2.2	Планирует реализацию задач в зоне своей ответственности с учетом имеющихся ресурсов и ограничений исходя из действующих правовых норм
УК-2.3	Решает конкретные задачи проекта заявленного качества и за установленное время.
УК-2.4	Публично представляет результаты решения конкретной задачи проекта.

4. Объем дисциплины (модуля) и виды учебной работы. Общая трудоемкость дисциплины

Объем дисциплины и виды учебной работы по очной форме обучения.

		Формы контроля (количество)	Виды занятий					Итого часов	з.е.
		Эк	Лек	Пр	КРАт	Контроль	СР		
Курс 3	Сем. 5	1	34	51	0.35	26.65	32	**144**	4

5. Структура и содержание учебной и воспитательной деятельности при реализации дисциплины

5.1. Структура дисциплины для очной формы обучения.

Сем	Раздел дисциплины	Неделя семестра	Виды учебной работы, включая самостоятельную работу и трудоемкость (в часах)								Формы текущего/промежуточной контроля успеваемости текущего (по неделям семестра), промежуточной аттестации (по семестрам)
			Лек	Лаб	ПР	СРП	КРАт	Контроль	СР	СЗ	
1	2	3	4	5	6	7	8	9	10	11	12
5	Введение. Назначение и структура правового обеспечения защиты информации. Задачи и функции правовой защиты информации. Правовые принципы защиты информации.	1	2		3				2		Обсуждение докладов. Реферат.
5	Российское законодательство в области информационной безопасности. Правовая ответственность за правонарушения в информационной сфере. Виды юридической ответственности за правонарушения в информационной сфере. Право на информацию, его охрана и защита. Интернет и право. Конституция РФ о праве на поиск, получение и передачу информации. Субъективные права.	2	2		3				2		Обсуждение докладов. Реферат.
5	Институт правовой защиты государственной тайны. Правовые основы защиты государственной тайны. Законодательные нормативно-правовые акты РФ, регулирующие защиту государственной тайны. Институт правовой защиты служебной тайны. Институт правовой защиты коммерческой тайны. Институт правовой защиты профессиональной тайны. Правовые основы защиты персональных данных .	3	2		3				2		Обсуждение докладов. Реферат.
5	Правовые вопросы защиты информации с использованием технических средств.	4	2		3				2		Обсуждение докладов. Реферат.
5	Институт правовой защиты интеллектуальной собственности. Понятие интеллектуальной собственности, ее виды и основные объекты образования. Интеллектуальный продукт как объект интеллектуальной собственности и предмет защиты.	5	2		3				2		Обсуждение докладов. Реферат.
5	Институт правовой защиты изобретений, полезных моделей, промышленных образцов. Патентное право. Лицензионный договор.	6	2		3				2		Обсуждение докладов. Реферат.
5	Институт правовой охраны: - средств индивидуализации участников гражданского	7	2		3				2		Обсуждение докладов. Реферат.

Сем	Раздел дисциплины	Неделя семестра	Виды учебной работы, включая самостоятельную работу и трудоемкость (в часах)								Формы текущего/промежуточной контроля успеваемости текущего (по неделям семестра), промежуточной аттестации (по семестрам)
			Лек	Лаб	ПР	СРП	КРАт	Контроль	СР	СЗ	
1	2	3	4	5	6	7	8	9	10	11	12
	оборота и производимой ими продукции. - программ для ЭВМ и баз данных. - программ для ЭВМ и баз данных. Порядок регистрации программ для ЭВМ и баз данных.										
5	Компьютерные преступления. Расследование преступлений в сфере компьютерной информации.	8	2		3				2		Обсуждение докладов. Реферат.
5	Организационные источники и каналы утечки. Силы, средства и условия «ОЗИ».	9	2		3				2		Обсуждение докладов. Реферат.
5	Подбор персонала на должности, связанные с работой с конфиденциальной информацией. Текущая работа с персоналом, обладающим конфиденциальной информацией.	10	2		3				2		Обсуждение докладов. Реферат.
5	Организация служебного расследования по фактам разглашения персоналом конфиденциальной информации.	11	2		3				2		Обсуждение докладов. Реферат.
5	Организация охраны территории, зданий, помещений и персонала.	12	2		3				2		Обсуждение докладов. Реферат.
5	Организация пропускного и внутри объектового режимов. Требования к помещениям и хранилищам, в которых ведутся закрытые работы и хранятся конфиденциальные документы и изделия Оборудование специальных хранилищ, сейфов и металлических шкафов, предназначенных для хранения конфиденциальных изделий и документов.	13	2		3				2		Обсуждение докладов. Реферат.
5	Организация подготовки и проведения совещаний и переговоров по конфиденциальным вопросам.	13	2		3				2		Обсуждение докладов. Реферат.
5	Аналитическая работа как основа управления системой организационной защиты информации.	14	2		3				2		Обсуждение докладов. Реферат.
5	Технология аналитической работы, ее основные этапы.	15	2		3				1		Обсуждение докладов. Реферат.
5	Планирование процессов организационной защиты информации.	16	2		3		0,35	26,65	1		Обсуждение докладов. Реферат.
	ИТОГО:		**34**		**51**		**0.35**	**26.65**	**32**		

5.4. Содержание разделов дисциплины (модуля) «Организационное и правовое обеспечение информационной безопасности», образовательные технологии

Лекционный курс

Сем	Наименование темы дисциплины	Трудоемкость (часы)			Содержание	Формируемые компетенции	Результаты освоения (знать, уметь, владеть)	Образовательные технологии
		ОФО	ЗФО	ОЗФО				
1	2	3	4	5	6	7	8	9
5	Введение. Назначение и структура правового обеспечения защиты информации. Задачи и функции правовой защиты информации. Правовые принципы защиты информации.	2			Предмет, задачи и содержание курса. Место курса среди других дисциплин. Анализ нормативных источников и литературы по дисциплине. Методы правовой защиты информации. Отрасли права, обеспечивающие правовое регулирование в сфере защиты информации. Роль права в регулировании комплекса отношений в сфере защиты информации. Основные системы ограничений на доступ к информации в российском праве. Правовые основы деятельности подразделений защиты информации.	ОПК-5.1; ОПК-5.3; ОПК-6.1; ПК-5.1; ПК-7.1;	Знать: современное состояние, особенности функционирования и возможности современных технологий, методов и средств защиты информации, их взаимосвязи с характеристиками внешних воздействий, вероятных угроз, решаемых задач и организационной структуры объекта защиты. Уметь: организовывать, управлять и поддерживать выполнение комплекса мер по информационной безопасности на основе учета принципов системности и плановости. Владеть: навыками применения подходов и методов организации систем информационной безопасности на основе определения характеристик внешних воздействий и вероятных угроз, выбора адекватных мер, технологий и средств защиты информации с учетом решаемых задач и особенностей конкретных организационно-технологических систем.	, Слайд-лекция

Сем	Наименование темы дисциплины	Трудоемкость (часы)			Содержание	Формируемые компетенции	Результаты освоения (знать, уметь, владеть)	Образовательные технологии
		ОФО	ЗФО	ОЗФО				
1	2	3	4	5	6	7	8	9
							Знать: профессиональную терминологию, законодательные акты, нормативно-методические документы по аттестации. Уметь: планировать, организовывать, координировать процессы, связанные с аттестацией объектов при разработке систем информационной безопасности. Владеть: навыками разработки орг анизационно-методического обеспечения процессов аттестации объектов на соответствие требованиям государственных или корпоративных документов	
5	Российское законодательство в области информационной безопасности. Правовая ответственность за правонарушения в информационной сфере. Виды юридической ответственности за правонарушения в информационной сфере. Право на информацию, его охрана и защита. Интернет и право. Конституция РФ о праве на поиск, получение и передачу информации. Субъективные права.	2			Основные законодательные акты, правовые нормы и положения. Понятие и виды информации, защищаемой законодательством Российской Федерации. Информация как объект права. Основы правового режима информационных ресурсов. Порядок пользования информационными ресурсами. Защита информации и прав субъектов в области информационных процессов. Правовые проблемы, связанные с защитой прав обладателей собственности на информацию и распоряжением	ОПК-5.1; ОПК-6.1; ПК-5.1; ПК-7.1;	Знать: современное состояние, особенности функционирования и возможности современных технологий, методов и средств защиты информации, их взаимосвязи с характеристиками внешних воздействий, вероятных угроз, решаемых задач и организационной структуры объекта защиты. Уметь: организовывать, управлять и поддерживать выполнение комплекса мер по информационной безопасности на основе учета принципов системности и плановости. Владеть: навыками применения	, Слайд-лекция

Сем	Наименование темы дисциплины	Трудоемкость (часы)			Содержание	Формируемые компетенции	Результаты освоения (знать, уметь, владеть)	Образовательные технологии
		ОФО	ЗФО	ОЗФО				
1	2	3	4	5	6	7	8	9
					информации. Система правовой ответственности за утечку информации и утрату носителей информации. Правовые гарантии поиска и получения информации. Право на поиск и получение документированной информации. Особенности реализации информационных правоотношений в Интернет.		подходов и методов организации систем информационной безопасности на основе определения характеристик внешних воздействий и вероятных угроз, выбора адекватных мер, технологий и средств защиты информации с учетом решаемых задач и особенностей конкретных организационно-технологических систем. Знать: профессиональную терминологию, законодательные акты, нормативно-методические документы по аттестации. Уметь: планировать, организовывать, координировать процессы, связанные с аттестацией объектов при разработке систем информационной безопасности. Владеть: навыками разработки орг анизационно-методического обеспечения процессов аттестации объектов на соответствие требованиям государственных или корпоративных документов.	
5	Институт правовой защиты государственной тайны. Правовые основы защиты государственной тайны. Законодательные нормативно-правовые акты РФ, регулирующие защиту государственной тайны. Институт правовой защиты служебной тайны. Институт правовой	2			Сведения, относимые к государственной тайне, и полномочия органов государственной власти и должностных лиц в области отнесения сведений к государственной тайне и их защиты. Грифы секретности носителей этих сведений. Порядок	ОПК-2.3.1; ОПК-5.1; ОПК-6.1; ПК-5.1; ПК-7.1;	Знать: современное состояние, особенности функционирования и возможности современных технологий, методов и средств защиты информации, их взаимосвязи с характеристиками внешних воздействий, вероятных угроз,	, Слайд-лекция

Сем	Наименование темы дисциплины	Трудоемкость (часы)			Содержание	Формируемые компетенции	Результаты освоения (знать, уметь, владеть)	Образовательные технологии
		ОФО	ЗФО	ОЗФО				
1	2	3	4	5	6	7	8	9
	защиты коммерческой тайны. Институт правовой защиты профессиональной тайны. Правовые основы защиты персональных данных .				распоряжения сведениями, составляющими государственную тайну. Система защиты государственной тайны. Нормативно-правовые акты и положения Гражданского кодекса РФ, регулирующие правовую защиту служебной тайны. Источники права о профессиональной тайне. Объекты и субъекты права на профессиональную тайну. Основные положения Европейской конвенции о защите личности в связи с автоматической обработкой персональных данных. Основные положения Федерального закона «О персональных данных».		решаемых задач и организационной структуры объекта защиты. Уметь: организовывать, управлять и поддерживать выполнение комплекса мер по информационной безопасности на основе учета принципов системности и плановости. Владеть: навыками применения подходов и методов организации систем информационной безопасности на основе определения характеристик внешних воздействий и вероятных угроз, выбора адекватных мер, технологий и средств защиты информации с учетом решаемых задач и особенностей конкретных организационно-технологических систем. Знать: профессиональную терминологию, законодательные акты, нормативно-методические документы по аттестации. Уметь: планировать, организовывать, координировать процессы, связанные с аттестацией объектов при разработке систем информационной безопасности. Владеть: навыками разработки орг анизационно-методического обеспечения процессов аттестации объектов на соответствие требованиям	

Сем	Наименование темы дисциплины	Трудоемкость (часы)			Содержание	Формируемые компетенции	Результаты освоения (знать, уметь, владеть)	Образовательные технологии
		ОФО	ЗФО	ОЗФО				
1	2	3	4	5	6	7	8	9
							государственных или корпоративных документов	
5	Правовые вопросы защиты информации с использованием технических средств.	2			Электронная подпись. Электронный документ как доказательство. Процедура разрешения конфликтов. Лицензирование и сертификация в области обеспечения безопасности информации.	ОПК-2.3.1; ОПК-5.1; ОПК-6.1; ОПК-9.1; ПК-5.1;	Знать: современное состояние, особенности функционирования и возможности современных технологий, методов и средств защиты информации, их взаимосвязи с характеристиками внешних воздействий, вероятных угроз, решаемых задач и организационной структуры объекта защиты. Уметь: организовывать, управлять и поддерживать выполнение комплекса мер по информационной безопасности на основе учета принципов системности и плановости. Владеть: навыками применения подходов и методов организации систем информационной безопасности на основе определения характеристик внешних воздействий и вероятных угроз, выбора адекватных мер, технологий и средств защиты информации с учетом решаемых задач и особенностей конкретных организационно-технологических систем. Знать: профессиональную терминологию, законодательные акты, нормативно-методические документы по аттестации. Уметь: планировать,	, Слайд-лекция

Сем	Наименование темы дисциплины	Трудоемкость (часы)			Содержание	Формируемые компетенции	Результаты освоения (знать, уметь, владеть)	Образовательные технологии
		ОФО	ЗФО	ОЗФО				
1	2	3	4	5	6	7	8	9
							организовывать, координировать процессы, связанные с аттестацией объектов при разработке систем информационной безопасности. Владеть: навыками разработки организационно-методического обеспечения процессов аттестации объектов на соответствие требованиям государственных или корпоративных документов.	
5	Институт правовой защиты интеллектуальной собственности. Понятие интеллектуальной собственности, ее виды и основные объекты образования. Интеллектуальный продукт как объект интеллектуальной собственности и предмет защиты.	2			Общие положения Закона РФ «Об авторском праве и смежных правах». Объекты и субъекты авторского права и смежных прав. Личные неимущественные права и исключительные имущественные права авторов произведений литературы, науки и искусства. Возможность свободного использования произведений. Авторское право. Авторский договор. Порядок передачи автором своих имущественных прав по авторскому договору, условия и особенности договора. Содержание гражданско-правовых норм в области защиты интеллектуальной собственности. Уголовная ответственность за преступления в сфере интеллектуальной собственности. Участие России в международных	ОПК-2.3.1; ОПК-5.1; ОПК-5.2; ОПК-5.3; ОПК-6.1; ПК-5.1; ПК-7.1;	Знать: современное состояние, особенности функционирования и возможности современных технологий, методов и средств защиты информации, их взаимосвязи с характеристиками внешних воздействий, вероятных угроз, решаемых задач и организационной структуры объекта защиты. Уметь: организовывать, управлять и поддерживать выполнение комплекса мер по информационной безопасности на основе учета принципов системности и плановости. Владеть: навыками применения подходов и методов организации систем информационной безопасности на основе определения характеристик внешних	, Слайд-лекция

Сем	Наименование темы дисциплины	Трудоемкость (часы)			Содержание	Формируемые компетенции	Результаты освоения (знать, уметь, владеть)	Образовательные технологии
		ОФО	ЗФО	ОЗФО				
1	2	3	4	5	6	7	8	9
					соглашениях по защите авторских и смежных прав.		воздействий и вероятных угроз, выбора адекватных мер, технологий и средств защиты информации с учетом решаемых задач и особенностей конкретных организационно-технологических систем. Знать: профессиональную терминологию, законодательные акты, нормативно-методические документы по аттестации. Уметь: планировать, организовывать, координировать процессы, связанные с аттестацией объектов при разработке систем информационной безопасности. Владеть: навыками разработки орг анизационно-методического обеспечения процессов аттестации объектов на соответствие требованиям государственных или корпоративных документов.	
5	Институт правовой защиты изобретений, полезных моделей, промышленных образцов. Патентное право. Лицензионный договор.	2			История развития патентного права в России. Основные особенности патентного закона РФ. Краткая характеристика объектов патентного права. Оформление патентных прав. Патент как форма охраны объектов патентного права. Содержание патентных прав. Представление прав на использование объектов патентного права. Защита прав авторов	ОПК-2.3.1; ОПК-2.3.2; ОПК-2.3.3; ОПК-2.4.1; ОПК-2.4.2; ОПК-5.1; ОПК-5.2; ОПК-5.3; ОПК-6.1; ОПК-6.3; ОПК-9.1; ПК-5.1; ПК-5.3; ПК-7.1;	Знать: современное состояние, особенности функционирования и возможности современных технологий, методов и средств защиты информации, их взаимосвязи с характеристиками внешних воздействий, вероятных угроз, решаемых задач и организационной структуры объекта защиты. Уметь: организовывать, управлять и	, Слайд-лекция

Сем	Наименование темы дисциплины	Трудоемкость (часы)			Содержание	Формируемые компетенции	Результаты освоения (знать, уметь, владеть)	Образовательные технологии
		ОФО	ЗФО	ОЗФО				
1	2	3	4	5	6	7	8	9
					патентообладателей. Участие России в международных соглашениях по защите прав авторов и патентообладателей.		поддерживать выполнение комплекса мер по информационной безопасности на основе учета принципов системности и плановости. Владеть: навыками применения подходов и методов организации систем информационной безопасности на основе определения характеристик внешних воздействий и вероятных угроз, выбора адекватных мер, технологий и средств защиты информации с учетом решаемых задач и особенностей конкретных организационно-технологических систем. Знать: профессиональную терминологию, законодательные акты, нормативно-методические документы по аттестации. Уметь: планировать, организовывать, координировать процессы, связанные с аттестацией объектов при разработке систем информационной безопасности. Владеть: навыками разработки орг анизационно-методического обеспечения процессов аттестации объектов на соответствие требованиям государственных или корпоративных документов.	
5	Институт правовой охраны: - средств индивидуализации	2			История товарных знаков, их основные функции. Виды товарных знаков.	ОПК-2.3.1; ОПК-2.3.2; ОПК-2.4.1; ОПК-2.4.3; ОПК-2.4.2; ОПК-5.1;	Знать: современное состояние, особенности функционирования и	, Слайд-лекция

Сем	Наименование темы дисциплины	Трудоемкость (часы)			Содержание	Формируемые компетенции	Результаты освоения (знать, уметь, владеть)	Образовательные технологии
		ОФО	ЗФО	ОЗФО				
1	2	3	4	5	6	7	8	9
	участников гражданского оборота и производимой ими продукции. - программ для ЭВМ и баз данных. - программ для ЭВМ и баз данных. Порядок регистрации программ для ЭВМ и баз данных.				Порядок прекращения правовой охраны товарного знака. Нарушение прав на товарный знак. Порядок рассмотрения споров, связанных с использованием товарного знака. Защита прав их авторов. Порядок передачи прав на использование программ для ЭВМ и баз данных. Защита прав в судебном порядке. Авторский (лицензионный) договор, его содержание, существенные условия и порядок оформления.	ОПК-5.2; ОПК-5.3; ОПК-6.1; ОПК-6.2; ПК-5.3; ПК-7.1; ПК-8.2; УК-2.1; УК-2.2;	возможности современных технологий, методов и средств защиты информации, их взаимосвязи с характеристиками внешних воздействий, вероятных угроз, решаемых задач и организационной структуры объекта защиты. Уметь: организовывать, управлять и поддерживать выполнение комплекса мер по информационной безопасности на основе учета принципов системности и плановости. Владеть: навыками применения подходов и методов организации систем информационной безопасности на основе определения характеристик внешних воздействий и вероятных угроз, выбора адекватных мер, технологий и средств защиты информации с учетом решаемых задач и особенностей конкретных организационно-технологических систем. Знать: профессиональную терминологию, законодательные акты, нормативно-методические документы по аттестации. Уметь: планировать, организовывать, координировать процессы, связанные с аттестацией объектов при разработке систем информационной	

Сем	Наименование темы дисциплины	Трудоемкость (часы)			Содержание	Формируемые компетенции	Результаты освоения (знать, уметь, владеть)	Образовательные технологии
		ОФО	ЗФО	ОЗФО				
1	2	3	4	5	6	7	8	9
							безопасности. Владеть: навыками разработки организационно-методического обеспечения процессов аттестации объектов на соответствие требованиям государственных или корпоративных документов.	
5	Компьютерные преступления. Расследование преступлений в сфере компьютерной информации.	2			Понятие компьютерных преступлений и их классификация. Уголовно-правовая характеристика компьютерных преступлений. Криминалистическая характеристика компьютерных преступлений. Способы совершения преступлений в сфере компьютерной информации. Компьютерные вирусы. Тенденции развития компьютерной преступности в России.	ОПК-2.3.1; ОПК-2.3.2; ОПК-2.3.3; ОПК-2.4.1; ОПК-2.4.2; ОПК-2.4.3; ОПК-5.1; ОПК-5.2; ОПК-5.3; ОПК-6.2; ОПК-6.3; ОПК-9.1; ПК-5.3; ПК-7.2; ПК-8.2; УК-2.1; УК-2.2; УК-2.3;	Знать: современное состояние, особенности функционирования и возможности современных технологий, методов и средств защиты информации, их взаимосвязи с характеристиками внешних воздействий, вероятных угроз, решаемых задач и организационной структуры объекта защиты. Уметь: организовывать, управлять и поддерживать выполнение комплекса мер по информационной безопасности на основе учета принципов системности и плановости. Владеть: навыками применения подходов и методов организации систем информационной безопасности на основе определения характеристик внешних воздействий и вероятных угроз, выбора адекватных мер, технологий и средств защиты информации с учетом решаемых задач и особенностей конкретных	, Слайд-лекция

Сем	Наименование темы дисциплины	Трудоемкость (часы)			Содержание	Формируемые компетенции	Результаты освоения (знать, уметь, владеть)	Образовательные технологии
		ОФО	ЗФО	ОЗФО				
1	2	3	4	5	6	7	8	9
							организационно-технологических систем. Знать: профессиональную терминологию, законодательные акты, нормативно-методические документы по аттестации. Уметь: планировать, организовывать, координировать процессы, связанные с аттестацией объектов при разработке систем информационной безопасности. Владеть: навыками разработки организационно-методического обеспечения процессов аттестации объектов на соответствие требованиям государственных или корпоративных документов.	
5	Организационные источники и каналы утечки. Силы, средства и условия «ОЗИ».	2			Коммуникационный процесс и его базовые элементы: источник информации, отправитель, сообщение, канал, получатель. Источники конфиденциальной информации: люди, документы, изделия, технические носители и средства коммуникации. Организационные каналы передачи информации и каналы утечки информации и несанкционированного доступа к ней. Классификация организационных каналов утечки конфиденциальной информации.	ОПК-2.3.1; ОПК-2.3.2; ОПК-2.3.3; ОПК-2.4.1; ОПК-2.4.2; ОПК-5.1; ОПК-2.4.3; ОПК-5.2; ОПК-5.3; ОПК-6.1; ОПК-6.2; ОПК-6.3; ОПК-9.1; ОПК-9.2; ПК-5.1; ПК-5.3; ПК-7.3; ПК-7.2; ПК-8.2; УК-2.1;	Знать: современное состояние, особенности функционирования и возможности современных технологий, методов и средств защиты информации, их взаимосвязи с характеристиками внешних воздействий, вероятных угроз, решаемых задач и организационной структуры объекта защиты. Уметь: организовывать, управлять и поддерживать выполнение комплекса мер по информационной безопасности на основе учета принципов системности и	, Лекция-беседа

Сем	Наименование темы дисциплины	Трудоемкость (часы)			Содержание	Формируемые компетенции	Результаты освоения (знать, уметь, владеть)	Образовательные технологии
		ОФО	ЗФО	ОЗФО				
1	2	3	4	5	6	7	8	9
							плановости. Владеть: навыками применения подходов и методов организации систем информационной безопасности на основе определения характеристик внешних воздействий и вероятных угроз, выбора адекватных мер, технологий и средств защиты информации с учетом решаемых задач и особенностей конкретных организационно-технологических систем. Знать: профессиональную терминологию, законодательные акты, нормативно-методические документы по аттестации. Уметь: планировать, организовывать, координировать процессы, связанные с аттестацией объектов при разработке систем информационной безопасности. Владеть: навыками разработки организационно-методического обеспечения процессов аттестации объектов на соответствие требованиям государственных или корпоративных документов.	
5	Подбор персонала на должности, связанные с работой с конфиденциальной информацией. Текущая работа с персоналом, обладающим конфиденциальной информацией.	2			Персонал организации как источник конфиденциальной информации и один из основных каналов ее разглашения. Особенности подбора персонала на должности, связанные с работой с	ОПК-2.3.1; ОПК-2.4.2; ОПК-5.1; ОПК-5.2; ОПК-5.3; ОПК-6.1; ОПК-6.2; ОПК-6.3; ПК-5.1; ПК-7.1; ПК-8.2; УК-2.1;	Знать: современное состояние, особенности функционирования и возможности современных технологий, методов и средств защиты информации, их взаимосвязи с характеристиками	, Слайд-лекция

Сем	Наименование темы дисциплины	Трудоемкость (часы)			Содержание	Формируемые компетенции	Результаты освоения (знать, уметь, владеть)	Образовательные технологии
		ОФО	ЗФО	ОЗФО				
1	2	3	4	5	6	7	8	9
					конфиденциальной информацией. Оценка кандидатов на должности, связанные с доступом к конфиденциальной информации. Основные критерии оценки: уровень профессиональной подготовки, знаний, умений и наличие практического опыта работы; личностные характеристики. Методы проверки кандидатов на должности.		внешних воздействий, вероятных угроз, решаемых задач и организационной структуры объекта защиты. Уметь: организовывать, управлять и поддерживать выполнение комплекса мер по информационной безопасности на основе учета принципов системности и плановости. Владеть: навыками применения подходов и методов организации систем информационной безопасности на основе определения характеристик внешних воздействий и вероятных угроз, выбора адекватных мер, технологий и средств защиты информации с учетом решаемых задач и особенностей конкретных организационно-технологических систем. Знать: профессиональную терминологию, законодательные акты, нормативно-методические документы по аттестации. Уметь: планировать, организовывать, координировать процессы, связанные с аттестацией объектов при разработке систем информационной безопасности. Владеть: навыками разработки орг анизационно-методического обеспечения процессов аттестации объектов на	

Сем	Наименование темы дисциплины	Трудоемкость (часы)			Содержание	Формируемые компетенции	Результаты освоения (знать, уметь, владеть)	Образовательные технологии
		ОФО	ЗФО	ОЗФО				
1	2	3	4	5	6	7	8	9
							соответствие требованиям государственных или корпоративных документов.	
5	Организация служебного расследования по фактам разглашения персоналом конфиденциальной информации.	2			Понятие "служебное расследование по фактам разглашения информации". Цели и задачи служебного расследования. Основания для проведения служебного расследования. Процедура служебного расследования. Меры, принимаемые по результатам расследования. Документирование хода и результатов служебного расследования.	ОПК-2.3.1; ОПК-2.3.2; ОПК-2.3.3; ОПК-2.4.1; ОПК-5.1; ОПК-5.2; ОПК-5.3; ОПК-6.1; ОПК-6.2; ОПК-6.3; ПК-5.1; ПК-5.2; ПК-7.1; ПК-8.2; УК-2.1;	Знать: современное состояние, особенности функционирования и возможности современных технологий, методов и средств защиты информации, их взаимосвязи с характеристиками внешних воздействий, вероятных угроз, решаемых задач и организационной структуры объекта защиты. Уметь: организовывать, управлять и поддерживать выполнение комплекса мер по информационной безопасности на основе учета принципов системности и плановости. Владеть: навыками применения подходов и методов организации систем информационной безопасности на основе определения характеристик внешних воздействий и вероятных угроз, выбора адекватных мер, технологий и средств защиты информации с учетом решаемых задач и особенностей конкретных организационно-технологических систем. Знать: профессиональную терминологию, законодательные акты, нормативно-методические	, Слайд-лекция

Сем	Наименование темы дисциплины	Трудоемкость (часы)			Содержание	Формируемые компетенции	Результаты освоения (знать, уметь, владеть)	Образовательные технологии
		ОФО	ЗФО	ОЗФО				
1	2	3	4	5	6	7	8	9
							документы по аттестации. Уметь: планировать, организовывать, координировать процессы, связанные с аттестацией объектов при разработке систем информационной безопасности. Владеть: навыками разработки организационно-методического обеспечения процессов аттестации объектов на соответствие требованиям государственных или корпоративных документов.	
5	Организация охраны территории, зданий, помещений и персонала.	2			Понятие "охрана". Цели и задачи охраны. Объекты охраны: территория, здания, помещения, персонал, информационные ресурсы и другие материальные и финансовые ценности. Особенности их охраны. Виды и способы охраны. Понятие о рубежах охраны. Много рубежная система охраны. Факторы выбора приемов и средств охраны.	ОПК-2.3.2; ОПК-2.3.3; ОПК-2.4.1; ОПК-2.4.2; ОПК-2.4.3; ОПК-5.1; ОПК-5.2; ОПК-5.3; ОПК-6.1; ОПК-6.2; ОПК-6.3; ОПК-9.1; ПК-5.1; ОПК-9.2; ПК-5.2; ПК-5.3; ПК-7.1; ПК-7.2; ПК-7.3; ПК-8.2; УК-2.1; УК-2.2; УК-2.3; УК-2.4;	Знать: современное состояние, особенности функционирования и возможности современных технологий, методов и средств защиты информации, их взаимосвязи с характеристиками внешних воздействий, вероятных угроз, решаемых задач и организационной структуры объекта защиты. Уметь: организовывать, управлять и поддерживать выполнение комплекса мер по информационной безопасности на основе учета принципов системности и плановости. Владеть: навыками применения подходов и методов организации систем информационной безопасности на основе	, Слайд-лекция

Сем	Наименование темы дисциплины	Трудоемкость (часы)			Содержание	Формируемые компетенции	Результаты освоения (знать, уметь, владеть)	Образовательные технологии
		ОФО	ЗФО	ОЗФО				
1	2	3	4	5	6	7	8	9
							определения характеристик внешних воздействий и вероятных угроз, выбора адекватных мер, технологий и средств защиты информации с учетом решаемых задач и особенностей конкретных организационно-технологических систем. Знать: профессиональную терминологию, законодательные акты, нормативно-методические документы по аттестации. Уметь: планировать, организовывать, координировать процессы, связанные с аттестацией объектов при разработке систем информационной безопасности. Владеть: навыками разработки организационно-методического обеспечения процессов аттестации объектов на соответствие требованиям государственных или корпоративных документов.	
5	Организация пропускного и внутри объектового режимов. Требования к помещениям и хранилищам, в которых ведутся закрытые работы и хранятся конфиденциальные документы и изделия Оборудование специальных хранилищ, сейфов и металлических шкафов, предназначенных для хранения	2			Понятие "пропускной режим". Цели и задачи пропускного режима. Организация пропускного режима. Понятие пропуска. Виды пропусков и отличительных шифров. Порядок оформления и выдачи пропусков. Контрольно-пропускные пункты, их оборудование и организация работы. Общие требования внутри объектового режима. Понятие режимных	ОПК-2.3.1; ОПК-2.3.2; ОПК-2.3.3; ОПК-2.4.1; ОПК-2.4.2; ОПК-2.4.3; ОПК-5.1; ОПК-5.2; ОПК-5.3; ОПК-6.1; ОПК-6.2; ОПК-6.3; ОПК-9.1; ОПК-9.2; ПК-5.2; ПК-5.3; ПК-7.1; ПК-7.3; ПК-7.2; ПК-8.2; УК-2.2; УК-2.3; УК-2.1;	Знать: современное состояние, особенности функционирования и возможности современных технологий, методов и средств защиты информации, их взаимосвязи с характеристиками внешних воздействий, вероятных угроз, решаемых задач и организационной структуры объекта защиты. Уметь:	, Слайд-лекция

Сем	Наименование темы дисциплины	Трудоемкость (часы)			Содержание	Формируемые компетенции	Результаты освоения (знать, уметь, владеть)	Образовательные технологии
		ОФО	ЗФО	ОЗФО				
1	2	3	4	5	6	7	8	9
	конфиденциальных изделий и документов.				помещений и требования, предъявляемые к ним. Особенности оборудования помещения, где ведутся конфиденциальные работы.		организовывать, управлять и поддерживать выполнение комплекса мер по информационной безопасности на основе учета принципов системности и плановости. Владеть: навыками применения подходов и методов организации систем информационной безопасности на основе определения характеристик внешних воздействий и вероятных угроз, выбора адекватных мер, технологий и средств защиты информации с учетом решаемых задач и особенностей конкретных организационно-технологических систем. Знать: профессиональную терминологию, законодательные акты, нормативно-методические документы по аттестации. Уметь: планировать, организовывать, координировать процессы, связанные с аттестацией объектов при разработке систем информационной безопасности. Владеть: навыками разработки орг анизационно-методического обеспечения процессов аттестации объектов на соответствие требованиям государственных или корпоративных документов.	
5	Организация подготовки	2			Основные требования,	ОПК-2.3.1; ОПК-2.3.2;	Знать: современное	, Слайд-лекция

Сем	Наименование темы дисциплины	Трудоемкость (часы)			Содержание	Формируемые компетенции	Результаты освоения (знать, уметь, владеть)	Образовательные технологии
		ОФО	ЗФО	ОЗФО				
1	2	3	4	5	6	7	8	9
	и проведения совещаний и переговоров по конфиденциальным вопросам.				предъявляемые к подготовке и проведению совещаний и переговоров по конфиденциальным вопросам.	ОПК-2.4.2; ОПК-2.4.3; ОПК-5.1; ОПК-5.3; ОПК-5.2; ОПК-6.2; ОПК-6.1; ПК-5.1; ПК-5.2; ПК-7.1; ПК-5.3; ПК-7.3; ПК-7.2; ПК-8.2; УК-2.2; УК-2.3; УК-2.4;	состояние, особенности функционирования и возможности современных технологий, методов и средств защиты информации, их взаимосвязи с характеристиками внешних воздействий, вероятных угроз, решаемых задач и организационной структуры объекта защиты. Уметь: организовывать, управлять и поддерживать выполнение комплекса мер по информационной безопасности на основе учета принципов системности и плановости. Владеть: навыками применения подходов и методов организации систем информационной безопасности на основе определения характеристик внешних воздействий и вероятных угроз, выбора адекватных мер, технологий и средств защиты информации с учетом решаемых задач и особенностей конкретных организационно-технологических систем. Знать: профессиональную терминологию, законодательные акты, нормативно-методические документы по аттестации. Уметь: планировать, организовывать, координировать процессы, связанные с аттестацией объектов при	

Сем	Наименование темы дисциплины	Трудоемкость (часы)			Содержание	Формируемые компетенции	Результаты освоения (знать, уметь, владеть)	Образовательные технологии
		ОФО	ЗФО	ОЗФО				
1	2	3	4	5	6	7	8	9
							разработке систем информационной безопасности. Владеть: навыками разработки организационно-методического обеспечения процессов аттестации объектов на соответствие требованиям государственных или корпоративных документов.	
5	Аналитическая работа как основа управления системой организационной защиты информации.	2			Понятие, цели и задачи аналитической работы по защите информации. Методики аналитической работы, обеспечивающие управляемость системы организационной защиты информации.	ОПК-2.3.1; ОПК-2.3.2; ОПК-2.3.3; ОПК-2.4.1; ОПК-2.4.2; ОПК-2.4.3; ОПК-5.1; ОПК-5.2; ОПК-5.3; ОПК-6.1; ОПК-6.3; ОПК-9.1; ОПК-9.2; ПК-5.1; ПК-5.2; ПК-5.3; ПК-7.2; ПК-7.3; ПК-8.2; УК-2.1; УК-2.2; УК-2.3; УК-2.4;	Знать: современное состояние, особенности функционирования и возможности современных технологий, методов и средств защиты информации, их взаимосвязи с характеристиками внешних воздействий, вероятных угроз, решаемых задач и организационной структуры объекта защиты. Уметь: организовывать, управлять и поддерживать выполнение комплекса мер по информационной безопасности на основе учета принципов системности и плановости. Владеть: навыками применения подходов и методов организации систем информационной безопасности на основе определения характеристик внешних воздействий и вероятных угроз, выбора адекватных мер, технологий и средств защиты информации с	, Слайд-лекция

Сем	Наименование темы дисциплины	Трудоемкость (часы)			Содержание	Формируемые компетенции	Результаты освоения (знать, уметь, владеть)	Образовательные технологии
		ОФО	ЗФО	ОЗФО				
1	2	3	4	5	6	7	8	9
							учетом решаемых задач и особенностей конкретных организационно-технологических систем. Знать: профессиональную терминологию, законодательные акты, нормативно-методические документы по аттестации. Уметь: планировать, организовывать, координировать процессы, связанные с аттестацией объектов при разработке систем информационной безопасности. Владеть: навыками разработки орг анизационно-методического обеспечения процессов аттестации объектов на соответствие требованиям государственных или корпоративных документов.	
5	Технология аналитической работы, ее основные этапы.	2			Первый этап. Определение проблемы, формулирование целей и предварительных гипотез (или версий). Разработка программы (проекта) исследования. Второй этап. Сбор информации. Отбор и анализ источников информации. Категории источников. Методы их оценки с точки зрения надежности. Внутренние и внешние источники. Третий этап. Анализ собранной информации - производство аналитического продукта, его распространение (использование).	ОПК-2.3.1; ОПК-2.3.2; ОПК-2.3.3; ОПК-2.4.1; ОПК-2.4.3; ОПК-2.4.2; ОПК-5.1; ОПК-5.2; ОПК-6.1; ОПК-6.2; ОПК-9.1; ОПК-6.3; ОПК-9.2; ПК-5.1; ПК-5.2; ПК-7.1; ПК-7.2; ПК-7.3; ПК-8.2; УК-2.1; УК-2.2; УК-2.3; УК-2.4;	Знать: современное состояние, особенности функционирования и возможности современных технологий, методов и средств защиты информации, их взаимосвязи с характеристиками внешних воздействий, вероятных угроз, решаемых задач и организационной структуры объекта защиты. Уметь: организовывать, управлять и поддерживать выполнение комплекса мер по информационной безопасности на основе	, Слайд-лекция

Сем	Наименование темы дисциплины	Трудоемкость (часы)			Содержание	Формируемые компетенции	Результаты освоения (знать, уметь, владеть)	Образовательные технологии
		ОФО	ЗФО	ОЗФО				
1	2	3	4	5	6	7	8	9
							учета принципов системности и плановости. Владеть: навыками применения подходов и методов организации систем информационной безопасности на основе определения характеристик внешних воздействий и вероятных угроз, выбора адекватных мер, технологий и средств защиты информации с учетом решаемых задач и особенностей конкретных организационно-технологических систем. Знать: профессиональную терминологию, законодательные акты, нормативно-методические документы по аттестации. Уметь: планировать, организовывать, координировать процессы, связанные с аттестацией объектов при разработке систем информационной безопасности. Владеть: навыками разработки организационно-методического обеспечения процессов аттестации объектов на соответствие требованиям государственных или корпоративных документов.	
5	Планирование процессов организационной защиты информации.	2			Сущность планирования как одной из основных функций управления системой организационной защиты информации. Цели планирования. Оценка и	ОПК-2.3.1; ОПК-2.3.2; ОПК-2.3.3; ОПК-2.4.1; ОПК-2.4.2; ОПК-2.4.3; ОПК-5.1; ОПК-5.2; ОПК-5.3; ОПК-6.1; ОПК-9.1; ОПК-6.3; ОПК-9.2; ПК-5.1; ПК-7.2; ПК-7.3; ПК-8.2; УК-2.2;	Знать: современное состояние, особенности функционирования и возможности современных технологий, методов и средств защиты информации, их	, Слайд-лекция

Сем	Наименование темы дисциплины	Трудоемкость (часы)			Содержание	Формируемые компетенции	Результаты освоения (знать, уметь, владеть)	Образовательные технологии
		ОФО	ЗФО	ОЗФО				
1	2	3	4	5	6	7	8	9
					анализ состояния системы ОЗИ как основа планирования. Стратегические и тактические планы. Соотношение планов ОЗИ с планами организации. Разновидности планов; их содержание и форма. Методы планирования. Особенности программно-целевого планирования.	УК-2.1; УК-2.3; УК-2.4;	взаимосвязи с характеристиками внешних воздействий, вероятных угроз, решаемых задач и организационной структуры объекта защиты. Уметь: организовывать, управлять и поддерживать выполнение комплекса мер по информационной безопасности на основе учета принципов системности и плановости. Владеть: навыками применения подходов и методов организации систем информационной безопасности на основе определения характеристик внешних воздействий и вероятных угроз, выбора адекватных мер, технологий и средств защиты информации с учетом решаемых задач и особенностей конкретных организационно-технологических систем. Знать: профессиональную терминологию, законодательные акты, нормативно-методические документы по аттестации. Уметь: планировать, организовывать, координировать процессы, связанные с аттестацией объектов при разработке систем информационной безопасности. Владеть: навыками разработки орг анизационно-методического	

Сем	Наименование темы дисциплины	Трудоемкость (часы)			Содержание	Формируемые компетенции	Результаты освоения (знать, уметь, владеть)	Образовательные технологии
		ОФО	ЗФО	ОЗФО				
1	2	3	4	5	6	7	8	9
							обеспечения процессов аттестации объектов на соответствие требованиям государственных или корпоративных документов.	
	ИТОГО:	**34**						

5.5. Практические занятия, их наименование, содержание и объем в часах

Сем	№ раздела дисциплины	Наименование практических занятий	Объем в часах		
			ОФО	ЗФО	ОЗФО
1	2	3	4	5	6
5	Введение. Назначение и структура правового обеспечения защиты информации. Задачи и функции правовой защиты информации. Правовые принципы защиты информации.	Предмет, задачи и содержание курса. Место курса среди других дисциплин. Анализ нормативных источников и литературы по дисциплине.Методы правовой защиты информации. Отрасли права, обеспечивающие правовое регулирование в сфере защиты информации. Роль права в регулировании комплекса отношений в сфере защиты информации. Основные системы ограничений на доступ к информации в российском праве. Правовые основы деятельности подразделений защиты информации.	3		
5	Российское законодательство в области информационной безопасности. Правовая ответственность за правонарушения в информационной сфере. Виды юридической ответственности за правонарушения в информационной сфере. Право на информацию, его охрана и защита. Интернет и право. Конституция РФ о праве на поиск, получение и передачу информации. Субъективные права.	Основные законодательные акты, правовые нормы и положения. Понятие и виды информации, защищаемой законодательством Российской Федерации.Информация как объект права. Основы правового режима информационных ресурсов. Порядок пользования информационными ресурсами. Защита информации и прав субъектов в области информационных процессов.Правовые проблемы, связанные с защитой прав обладателей собственности на информацию и распоряжением информации. Система правовой ответственности за утечку информации и утрату носителей информации. Правовые гарантии поиска и получения информации. Право на поиск и получение документированной информации. Особенности реализации информационных правоотношений в Интернет.	3		
5	Институт правовой защиты государственной тайны. Правовые основы защиты государственной тайны. Законодательные нормативно-правовые акты РФ, регулирующие защиту государственной тайны. Институт правовой защиты служебной тайны. Институт правовой защиты коммерческой тайны. Институт правовой защиты профессиональной тайны. Правовые основы защиты персональных данных .	Сведения, относимые к государственной тайне, и полномочия органов государственной власти и должностных лиц в области отнесения сведений к государственной тайне и их защиты. Грифы секретности носителей этих сведений. Порядок распоряжения сведениями, составляющими государственную тайну. Система защиты государственной тайны. Нормативно-правовые акты и положения Гражданского кодекса РФ, регулирующие правовую защиту служебной тайны. Источники права о профессиональной тайне. Объекты и субъекты права на профессиональную тайну. Основные положения Европейской конвенции о защите личности в связи с автоматической обработкой персональных данных.Основные положения Федерального закона «О персональных данных».	3		
5	Правовые вопросы защиты информации с использованием технических средств.	Электронная подпись. Электронный документ как доказательство. Процедура разрешения конфликтов. Лицензирование и сертификация в области обеспечения безопасности информации.	3		
5	Институт правовой защиты интеллектуальной собственности. Понятие интеллектуальной собственности, ее виды и основные объекты образования. Интеллектуальный продукт как объект интеллектуальной собственности и предмет защиты.	Общие положения Закона РФ «Об авторском праве и смежных правах». Объекты и субъекты авторского права и смежных прав. Личные неимущественные права и исключительные имущественные права авторов произведений литературы, науки и искусства. Возможность свободного использования произведений. Авторское право. Авторский договор. Порядок передачи автором своих имущественных прав по авторскому договору, условия и особенности договора.Содержание гражданско-правовых норм в области защиты интеллектуальной собственности. Уголовная ответственность за преступления в сфере интеллектуальной собственности. Участие России в международных соглашениях по защите авторских и смежных прав.	3		
5	Институт правовой защиты изобретений, полезных моделей, промышленных образцов. Патентное право. Лицензионный договор.	История развития патентного права в России. Основные особенности патентного закона РФ. Краткая характеристика объектов патентного права. Оформление патентных прав. Патент как форма охраны объектов патентного права. Содержание патентных прав. Представление прав на использование объектов патентного	3		

Сем	№ раздела дисциплины	Наименование практических занятий	Объем в часах		
			ОФО	ЗФО	ОЗФО
1	2	3	4	5	6
		права.Защита прав авторов патентообладателей. Участие России в международных соглашениях по защите прав авторов и патентообладателей.			
5	Институт правовой охраны: - средств индивидуализации участников гражданского оборота и производимой ими продукции. - программ для ЭВМ и баз данных. - программ для ЭВМ и баз данных. Порядок регистрации программ для ЭВМ и баз данных.	История товарных знаков, их основные функции. Виды товарных знаков. Порядок прекращения правовой охраны товарного знака. Нарушение прав на товарный знак. Порядок рассмотрения споров, связанных с использованием товарного знака. Защита прав их авторов. Порядок передачи прав на использование программ для ЭВМ и баз данных. Защита прав в судебном порядке. Авторский (лицензионный) договор, его содержание, существенные условия и порядок оформления.	3		
5	Компьютерные преступления. Расследование преступлений в сфере компьютерной информации.	Понятие компьютерных преступлений и их классификация. Уголовно-правовая характеристика компьютерных преступлений. Криминалистическая характеристика компьютерных преступлений. Способы совершения преступлений в сфере компьютерной информации. Компьютерные вирусы. Тенденции развития компьютерной преступности в России.	3		
5	Организационные источники и каналы утечки. Силы, средства и условия «ОЗИ».	Коммуникационный процесс и его базовые элементы: источник информации, отправитель, сообщение, канал, получатель. Источники конфиденциальной информации: люди, документы, изделия, технические носители и средства коммуникации. Организационные каналы передачи информации и каналы утечки информации и несанкционированного доступа к ней. Классификация организационных каналов утечки конфиденциальной информации.	3		
5	Подбор персонала на должности, связанные с работой с конфиденциальной информацией. Текущая работа с персоналом, обладающим конфиденциальной информацией.	Персонал организации как источник конфиденциальной информации и один из основных каналов ее разглашения.Особенности подбора персонала на должности, связанные с работой с конфиденциальной информацией. Оценка кандидатов на должности, связанные с доступом к конфиденциальной информации. Основные критерии оценки: уровень профессиональной подготовки, знаний, умений и наличие практического опыта работы; личностные характеристики. Методы проверки кандидатов на должности.	3		
5	Организация служебного расследования по фактам разглашения персоналом конфиденциальной информации.	Понятие "служебное расследование по фактам разглашения информации". Цели и задачи служебного расследования.Основания для проведения служебного расследования. Процедура служебного расследования. Меры, принимаемые по результатам расследования.Документирование хода и результатов служебного расследования.	3		
5	Организация охраны территории, зданий, помещений и персонала.	Понятие "охрана". Цели и задачи охраны. Объекты охраны: территория, здания, помещения, персонал, информационные ресурсы и другие материальные и финансовые ценности. Особенности их охраны.Виды и способы охраны. Понятие о рубежах охраны. Много рубежная система охраны.Факторы выбора приемов и средств охраны.	3		
5	Организация пропускного и внутри объектового режимов. Требования к помещениям и хранилищам, в которых ведутся закрытые работы и хранятся конфиденциальные документы и изделия Оборудование специальных хранилищ, сейфов и металлических шкафов, предназначенных для хранения конфиденциальных изделий и документов.	Понятие "пропускной режим". Цели и задачи пропускного режима.Организация пропускного режима. Понятие пропуска. Виды пропусков и отличительных шифров. Порядок оформления и выдачи пропусков.Контрольно-пропускные пункты, их оборудование и организация работы. Общие требования внутри объектового режима.	3		
5	Организация подготовки и проведения совещаний и переговоров по	Основные требования, предъявляемые к подготовке и проведению совещаний и переговоров по конфиденциальным вопросам.	3		

Сем	№ раздела дисциплины	Наименование практических занятий	Объем в часах		
			ОФО	ЗФО	ОЗФО
1	2	3	4	5	6
	конфиденциальным вопросам.				
5	Аналитическая работа как основа управления системой организационной защиты информации.	Понятие, цели и задачи аналитической работы по защите информации.Методики аналитической работы, обеспечивающие управляемость системы организационной защиты информации.	3		
5	Технология аналитической работы, ее основные этапы.	Первый этап. Определение проблемы, формулирование целей и предварительных гипотез (или версий). Разработка программы (проекта) исследования.Второй этап. Сбор информации. Отбор и анализ источников информации. Категории источников. Методы их оценки с точки зрения надежности. Внутренние и внешние источники.Третий этап. Анализ собранной информации - производство аналитического продукта, его распространение (использование).	3		
5	Планирование процессов организационной защиты информации.	Сущность планирования как одной из основных функций управления системой организационной защиты информации. Цели планирования. Оценка и анализ состояния системы ОЗИ как основа планирования.Стратегические и тактические планы. Соотношение планов ОЗИ с планами организации. Разновидности планов; их содержание и форма.Методы планирования. Особенности программно-целевого планирования.	3		
	ИТОГО:		**51**		

Симуляционные занятия, их наименование, содержание и объем в часах

Сем	№ раздела дисциплины	Наименование симуляционных занятий	Объем в часах		
			ОФО	ЗФО	ОЗФО
1	2	3	4	5	6
	ИТОГО:				

5.6. Лабораторные занятия, их наименование и объем в часах

Сем	№ раздела дисциплины	Наименование лабораторных работ	Объем в часах		
			ОФО	ЗФО	ОЗФО
1	2	3	4	5	6
	ИТОГО:				

5.7. Примерная тематика курсовых проектов (работ)

5.8. Самостоятельная работа студентов

Содержание и объем самостоятельной работы студентов

Сем	Разделы и темы рабочей программы самостоятельного изучения	Перечень домашних заданий и других вопросов для самостоятельного изучения	Сроки выполнения	Объем в часах		
				ОФО	ЗФО	ОЗФО
1	2	3	4	5	6	7
5	Введение. Назначение и структура правового обеспечения защиты информации. Задачи и функции правовой защиты информации. Правовые принципы защиты информации.	Составление плана-конспекта	1 неделя	2		
5	Российское законодательство в области информационной безопасности. Правовая ответственность за правонарушения в информационной сфере. Виды юридической ответственности за правонарушения в информационной сфере. Право на информацию, его охрана и защита. Интернет и право. Конституция РФ о праве на поиск, получение и передачу информации. Субъективные права.	Составление плана-конспекта	2 неделя	2		
5	Институт правовой защиты государственной тайны. Правовые основы защиты государственной тайны. Законодательные нормативно-правовые акты РФ, регулирующие защиту государственной тайны. Институт правовой защиты служебной тайны. Институт правовой защиты коммерческой тайны. Институт правовой защиты профессиональной тайны. Правовые основы защиты персональных данных .	Составление плана-конспекта	3 неделя	2		
5	Правовые вопросы защиты информации с использованием технических средств.	Составление плана-конспекта	4 неделя	2		
5	Институт правовой защиты интеллектуальной собственности. Понятие интеллектуальной собственности, ее виды и основные объекты образования. Интеллектуальный продукт как объект интеллектуальной собственности и предмет защиты.	Составление плана-конспекта	5 неделя	2		
5	Институт правовой защиты изобретений, полезных моделей, промышленных образцов. Патентное право. Лицензионный договор.	Составление плана-конспекта	6 неделя	2		
5	Институт правовой охраны: - средств	Составление плана-конспекта	7	2		

Сем	Разделы и темы рабочей программы самостоятельного изучения	Перечень домашних заданий и других вопросов для самостоятельного изучения	Сроки выполнения	Объем в часах		
				ОФО	ЗФО	ОЗФО
1	2	3	4	5	6	7
	индивидуализации участников гражданского оборота и производимой ими продукции. - программ для ЭВМ и баз данных. - программ для ЭВМ и баз данных. Порядок регистрации программ для ЭВМ и баз данных.		неделя			
5	Компьютерные преступления. Расследование преступлений в сфере компьютерной информации.	Составление плана-конспекта	8 неделя	2		
5	Организационные источники и каналы утечки. Силы, средства и условия «ОЗИ».	Составление плана-конспекта	9 неделя	2		
5	Подбор персонала на должности, связанные с работой с конфиденциальной информацией. Текущая работа с персоналом, обладающим конфиденциальной информацией.	Составление плана-конспекта	10 неделя	2		
5	Организация служебного расследования по фактам разглашения персоналом конфиденциальной информации.	Составление плана-конспекта	11 неделя	2		
5	Организация охраны территории, зданий, помещений и персонала.	Составление плана-конспекта	12 неделя	2		
5	Организация пропускного и внутри объектового режимов. Требования к помещениям и хранилищам, в которых ведутся закрытые работы и хранятся конфиденциальные документы и изделия Оборудование специальных хранилищ, сейфов и металлических шкафов, предназначенных для хранения конфиденциальных изделий и документов.	Составление плана-конспекта	13 неделя	2		
5	Организация подготовки и проведения совещаний и переговоров по конфиденциальным вопросам.	Составление плана-конспекта	14 неделя	2		
5	Аналитическая работа как основа управления системой организационной защиты информации.	Составление плана-конспекта	14 неделя	2		
5	Технология аналитической работы, ее основные этапы.	Составление плана-конспекта	15 неделя	1		
5	Планирование процессов организационной защиты информации.	Составление плана-конспекта	16 неделя	1		
	ИТОГО:			**32**		

5.9. Календарный график воспитательной работы по дисциплине

Модуль	Дата, место проведения	Название мероприятия	Форма проведения мероприятия	Ответственный	Достижения обучающихся

6. Перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине (модулю).

6.1. Методические указания (собственные разработки)

Название	Ссылка

6.2. Литература для самостоятельной работ

Название	Ссылка

Учебно-методические материалы для самостоятельной работы обучающихся из числа инвалидов и лиц с ограниченными возможностями здоровья (ОВЗ) предоставляются в формах, адаптированных к ограничениям их здоровья и восприятия информации:

Для лиц с нарушениями зрения:

- в печатной форме увеличенным шрифтом,
- в форме электронного документа,
- в форме аудиофайла,
- в печатной форме на языке Брайля.

Для лиц с нарушениями слуха:

- в печатной форме,
- в форме электронного документа.

Для лиц с нарушениями опорно-двигательного аппарата:

- в печатной форме,
- в форме электронного документа,
- в форме аудиофайла.

7. Фонд оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине (модулю)

7.1. Перечень компетенций с указанием этапов их формирования в процессе освоения образовательной программы

Этапы формирования компетенции (номер семестр согласного учебному плану)			Наименование учебных дисциплин, формирующие компетенции в процессе освоения образовательной программы
ОФО	**ЗФО**	**ОЗФО**	
ОПК-2.3.1 Знает национальные, межгосударственные и международные стандарты в области защиты информации, нормативные правовые акты в области защиты информации, руководящие и методические документы уполномоченных федеральных органов исполнительной власти в области внедрения и эксплуатации средств защиты информации			
5			Организационное и правовое обеспечение информационной безопасности
6			Защита информации от утечки по техническим каналам
67			Программно-аппаратные средства защиты информации
7			Основы управления информационной безопасностью
8			Комплексное обеспечение защиты информации объекта информатизации
5			Техническая защита информации
7			Нормативные акты и стандарты по информационной безопасности
8			Организация системы обеспечения информационной безопасности
3			Защита и обработка конфиденциальных документов
3			Защита информации в сети Интернет
ОПК-2.3.2 Умеет документировать процедуры и результаты контроля функционирования системы защиты информации; проводить испытания программно-технических средств защиты информации от НСД и специальных воздействий на соответствие требованиям по безопасности информации и техническим условиям			
5			Организационное и правовое обеспечение информационной безопасности
6			Защита информации от утечки по техническим каналам
67			Программно-аппаратные средства защиты информации
7			Основы управления информационной безопасностью
8			Комплексное обеспечение защиты информации объекта информатизации
5			Техническая защита информации
7			Нормативные акты и стандарты по информационной безопасности
8			Организация системы

Этапы формирования компетенции (номер семестр согласного учебному плану)			Наименование учебных дисциплин, формирующие компетенции в процессе освоения образовательной программы
ОФО	ЗФО	ОЗФО	
			обеспечения информационной безопасности
3			Защита и обработка конфиденциальных документов
3			Защита информации в сети Интернет
ОПК-2.3.3 Владеет навыками внесения изменений в эксплуатационную документацию и организационно-распорядительные документы по системе защиты информации; навыками разработки программ и методик испытаний опытного образца программно-технического средства защиты информации от НСД и специальных воздействий на соответствие техническим условиям			
5			Организационное и правовое обеспечение информационной безопасности
6			Защита информации от утечки по техническим каналам
67			Программно-аппаратные средства защиты информации
7			Основы управления информационной безопасностью
8			Комплексное обеспечение защиты информации объекта информатизации
5			Техническая защита информации
7			Нормативные акты и стандарты по информационной безопасности
8			Организация системы обеспечения информационной безопасности
3			Защита и обработка конфиденциальных документов
3			Защита информации в сети Интернет
ОПК-2.4.1 Знает критерии оценки защищенности объекта информатизации, технические средства контроля эффективности мер защиты информации, методы измерений, контроля и технических расчетом характеристик программно-аппаратных средств защиты информации			
5			Организационное и правовое обеспечение информационной безопасности
6			Защита информации от утечки по техническим каналам
67			Программно-аппаратные средства защиты информации
7			Основы управления информационной безопасностью
8			Комплексное обеспечение защиты информации объекта информатизации
5			Техническая защита информации
7			Нормативные акты и стандарты по информационной безопасности

Этапы формирования компетенции (номер семестр согласного учебному плану)			Наименование учебных дисциплин, формирующие компетенции в процессе освоения образовательной программы
ОФО	**ЗФО**	**ОЗФО**	
8			Организация системы обеспечения информационной безопасности
3			Защита и обработка конфиденциальных документов
3			Защита информации в сети Интернет
ОПК-2.4.2 Умеет осуществлять контроль обеспечения уровня защищенности объектов информатизации			
5			Организационное и правовое обеспечение информационной безопасности
6			Защита информации от утечки по техническим каналам
67			Программно-аппаратные средства защиты информации
7			Основы управления информационной безопасностью
8			Комплексное обеспечение защиты информации объекта информатизации
5			Техническая защита информации
7			Нормативные акты и стандарты по информационной безопасности
8			Организация системы обеспечения информационной безопасности
3			Защита и обработка конфиденциальных документов
3			Защита информации в сети Интернет
ОПК-2.4.3 Владеет навыками оценки защищенности объектов информатизации с помощью типовых программных средств			
5			Организационное и правовое обеспечение информационной безопасности
6			Защита информации от утечки по техническим каналам
67			Программно-аппаратные средства защиты информации
7			Основы управления информационной безопасностью
8			Комплексное обеспечение защиты информации объекта информатизации
5			Техническая защита информации
7			Нормативные акты и стандарты по информационной безопасности
8			Организация системы обеспечения информационной

Этапы формирования компетенции (номер семестр согласного учебному плану)			Наименование учебных дисциплин, формирующие компетенции в процессе освоения образовательной программы
ОФО	ЗФО	ОЗФО	
			безопасности
3			Защита и обработка конфиденциальных документов
3			Защита информации в сети Интернет

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

Планируемые результаты освоения компетенции	Критерии оценивания результатов обучения				Наименование оценочного средства
	неудовлетворительно	удовлетворительно	хорошо	отлично	
1	2	3	4	5	6
УК-2: Способен управлять проектом на всех этапах его жизненного цикла					
УК-2.2 Планирует реализацию задач в зоне своей ответственности с учетом имеющихся ресурсов и ограничений исходя из действующих правовых норм					
Знать:	Фрагментарные знания	Неполные знания	Сформированные, но содержащие отдельные пробелы знания	Сформированные систематические знания	контролирующие материалы по дисциплине, в числе которых могут быть: кейс-задания, задания для контрольной работы, тестовые задания, темы рефератов, докладов и другие.
Уметь:	Частичные умения	Неполные умения	Умения полные, допускаются небольшие ошибки	Сформированные умения	
Владеть:	Частичное владение навыками	Несистематическое применение навыков	В систематическом применении навыков допускаются пробелы	Успешное и систематическое применение навыков	
УК-2: Способен управлять проектом на всех этапах его жизненного цикла					
УК-2.3 Решает конкретные задачи проекта заявленного качества и за установленное время.					
Знать:	Фрагментарные знания	Неполные знания	Сформированные, но содержащие отдельные пробелы знания	Сформированные систематические знания	контролирующие материалы по дисциплине, в числе которых могут быть: кейс-задания, задания для контрольной работы, тестовые задания, темы рефератов, докладов и другие.
Уметь:	Частичные умения	Неполные умения	Умения полные, допускаются небольшие ошибки	Сформированные умения	
Владеть:	Частичное владение навыками	Несистематическое применение навыков	В систематическом применении навыков допускаются пробелы	Успешное и систематическое применение навыков	
УК-2: Способен управлять проектом на всех этапах его жизненного цикла					
УК-2.4 Публично представляет результаты решения конкретной задачи проекта.					
Знать:	Фрагментарные знания	Неполные знания	Сформированные, но содержащие отдельные пробелы знания	Сформированные систематические знания	контролирующие материалы по дисциплине, в числе которых могут быть: кейс-задания, задания для контрольной работы, тестовые задания, темы рефератов, докладов и другие.
Уметь:	Частичные умения	Неполные умения	Умения полные, допускаются небольшие ошибки	Сформированные умения	
Владеть:	Частичное владение навыками	Несистематическое применение навыков	В систематическом применении навыков допускаются пробелы	Успешное и систематическое применение навыков	
УК-2: Способен управлять проектом на всех этапах его жизненного цикла					
УК-2.1 Формулирует в рамках поставленной цели совокупность взаимосвязанных задач, обеспечивающих ее достижение в соответствии с действующим законодательством					
Знать:	Фрагментарные	Неполные знания	Сформированные,	Сформированные	контролирующие

Планируемые результаты освоения компетенции	Критерии оценивания результатов обучения				Наименование оценочного средства
	неудовлетворительно	удовлетворительно	хорошо	отлично	
1	2	3	4	5	6
	знания		но содержащие отдельные пробелы знания	систематические знания	материалы по дисциплине, в числе которых могут быть: кейс-задания, задания для контрольной работы, тестовые задания, темы рефератов, докладов и другие.
Уметь:	Частичные умения	Неполные умения	Умения полные, допускаются небольшие ошибки	Сформированные умения	
Владеть:	Частичное владение навыками	Несистематическое применение навыков	В систематическом применении навыков допускаются пробелы	Успешное и систематическое применение навыков	
ОПК-9: Способен применять средства криптографической и технической защиты информации для решения задач профессиональной деятельности;					
ОПК-9.1 Знает основные понятия и задачи криптографии, математические модели криптографических систем; способы и средства защиты информации от утечки по техническим каналам и контроля эффективности защиты информации					
Знать:	Фрагментарные знания	Неполные знания	Сформированные, но содержащие отдельные пробелы знания	Сформированные систематические знания	контролирующие материалы по дисциплине, в числе которых могут быть: кейс-задания, задания для контрольной работы, тестовые задания, темы рефератов, докладов и другие.
Уметь:	Частичные умения	Неполные умения	Умения полные, допускаются небольшие ошибки	Сформированные умения	
Владеть:	Частичное владение навыками	Несистематическое применение навыков	В систематическом применении навыков допускаются пробелы	Успешное и систематическое применение навыков	
ОПК-9: Способен применять средства криптографической и технической защиты информации для решения задач профессиональной деятельности;					
ОПК-9.2 Умеет применять математические модели для оценки стойкости СКЗИ и использовать в автоматизированных системах; пользоваться нормативными документами в области технической защиты информации					
Знать:	Фрагментарные знания	Неполные знания	Сформированные, но содержащие отдельные пробелы знания	Сформированные систематические знания	контролирующие материалы по дисциплине, в числе которых могут быть: кейс-задания, задания для контрольной работы, тестовые задания, темы рефератов, докладов и другие.
Уметь:	Частичные умения	Неполные умения	Умения полные, допускаются небольшие ошибки	Сформированные умения	
Владеть:	Частичное владение навыками	Несистематическое применение навыков	В систематическом применении навыков допускаются пробелы	Успешное и систематическое применение навыков	
ПК-5: Способен принимать участие в организации и сопровождении аттестации объекта информатизации по требованиям безопасности информации					
ПК-5.1 Знает нормативные правовые акты, методические документы, национальные стандарты в области защиты информации ограниченного доступа и аттестации объектов информатизации на соответствие требованиям по защите информации					
Знать:	Фрагментарные знания	Неполные знания	Сформированные, но содержащие отдельные пробелы знания	Сформированные систематические знания	контролирующие материалы по дисциплине, в числе которых могут быть: кейс-задания, задания для контрольной работы, тестовые задания, темы рефератов, докладов и другие.
Уметь:	Частичные умения	Неполные умения	Умения полные, допускаются небольшие ошибки	Сформированные умения	
Владеть:	Частичное владение навыками	Несистематическое применение навыков	В систематическом применении навыков допускаются пробелы	Успешное и систематическое применение навыков	



Планируемые результаты освоения компетенции	Критерии оценивания результатов обучения				Наименование оценочного средства
	неудовлетворительно	удовлетворительно	хорошо	отлично	
1	2	3	4	5	6
ОПК-5: Способен вести и организовывать проектно-изыскательские работы в области строительства и жилищно-коммунального хозяйства, осуществлять техническую экспертизу проектов и авторский надзор за их соблюдением					
ОПК-5.1 Знает основы законодательства Российской Федерации, нормативные правовые акты, нормативные и методические документы в области информационной безопасности и защиты информации, правовые основы организации защиты государственной тайны и конфиденциальной информации, правовую характеристику преступлений в сфере компьютерной информации и меры ответственности за утрату, разглашение, модификацию и уничтожение защищаемой информации					
Знать:	Фрагментарные знания	Неполные знания	Сформированные, но содержащие отдельные пробелы знания	Сформированные систематические знания	контролирующие материалы по дисциплине, в числе которых могут быть: кейс-задания, задания для контрольной работы, тестовые задания, темы рефератов, докладов и другие.
Уметь:	Частичные умения	Неполные умения	Умения полные, допускаются небольшие ошибки	Сформированные умения	
Владеть:	Частичное владение навыками	Несистематическое применение навыков	В систематическом применении навыков допускаются пробелы	Успешное и систематическое применение навыков	
ОПК-5: Способен вести и организовывать проектно-изыскательские работы в области строительства и жилищно-коммунального хозяйства, осуществлять техническую экспертизу проектов и авторский надзор за их соблюдением					
ОПК-5.2 Умеет обосновывать решения, связанные с реализацией правовых норм по защите информации в пределах должностных обязанностей, предпринимать необходимые меры по восстановлению нарушенных прав					
Знать:	Фрагментарные знания	Неполные знания	Сформированные, но содержащие отдельные пробелы знания	Сформированные систематические знания	контролирующие материалы по дисциплине, в числе которых могут быть: кейс-задания, задания для контрольной работы, тестовые задания, темы рефератов, докладов и другие.
Уметь:	Частичные умения	Неполные умения	Умения полные, допускаются небольшие ошибки	Сформированные умения	
Владеть:	Частичное владение навыками	Несистематическое применение навыков	В систематическом применении навыков допускаются пробелы	Успешное и систематическое применение навыков	
ПК-5: Способен принимать участие в организации и сопровождении аттестации объекта информатизации по требованиям безопасности информации					
ПК-5.2 Умеет разрабатывать программы и методики аттестационных испытаний выделенных (защищаемых) помещений на соответствие требованиям по защите информации, проводить аттестационные испытания, оформлять заключение по результатам аттестации выделенных (защищаемых) помещений на соответствие требованиям по защите информации					
Знать:	Фрагментарные знания	Неполные знания	Сформированные, но содержащие отдельные пробелы знания	Сформированные систематические знания	контролирующие материалы по дисциплине, в числе которых могут быть: кейс-задания, задания для контрольной работы, тестовые задания, темы рефератов, докладов и другие.
Уметь:	Частичные умения	Неполные умения	Умения полные, допускаются небольшие ошибки	Сформированные умения	
Владеть:	Частичное владение навыками	Несистематическое применение навыков	В систематическом применении навыков допускаются пробелы	Успешное и систематическое применение навыков	
ПК-5: Способен принимать участие в организации и сопровождении аттестации объекта информатизации по требованиям безопасности информации					
ПК-5.3 Владеет навыками подготовки аттестата соответствия выделенных (защищаемых) помещений требованиям по защите информации					
Знать:	Фрагментарные знания	Неполные знания	Сформированные, но содержащие отдельные пробелы знания	Сформированные систематические знания	контролирующие материалы по дисциплине, в числе которых могут быть: кейс-задания, задания для контрольной

Планируемые результаты освоения компетенции	Критерии оценивания результатов обучения				Наименование оценочного средства
	неудовлетворительно	удовлетворительно	хорошо	отлично	
1	2	3	4	5	6
Уметь:	Частичные умения	Неполные умения	Умения полные, допускаются небольшие ошибки	Сформированные умения	работы, тестовые задания, темы рефератов, докладов и другие.
Владеть:	Частичное владение навыками	Несистематическое применение навыков	В систематическом применении навыков допускаются пробелы	Успешное и систематическое применение навыков	
ОПК-5: Способен вести и организовывать проектно-изыскательские работы в области строительства и жилищно-коммунального хозяйства, осуществлять техническую экспертизу проектов и авторский надзор за их соблюдением					
ОПК-5.3 Владеет навыками разрабатывать локальные правовые документы, регламентирующие работу по обеспечению информационной безопасности в организации					
Знать:	Фрагментарные знания	Неполные знания	Сформированные, но содержащие отдельные пробелы знания	Сформированные систематические знания	контролирующие материалы по дисциплине, в числе которых могут быть: кейс-задания, задания для контрольной работы, тестовые задания, темы рефератов, докладов и другие.
Уметь:	Частичные умения	Неполные умения	Умения полные, допускаются небольшие ошибки	Сформированные умения	
Владеть:	Частичное владение навыками	Несистематическое применение навыков	В систематическом применении навыков допускаются пробелы	Успешное и систематическое применение навыков	
ПК-7: Способен оформлять рабочую техническую документацию с учетом действующих нормативных и методических документов					
ПК-7.1 Знает нормативные правовые акты, методические документы, национальные стандарты в области защиты информации ограниченного доступа, проектирования средств защиты информации, сертификации средств защиты информации на соответствие требованиям по безопасности информации и аттестации объектов информатизации на соответствие требованиям по защите информации, стандарты ЕСКД, ЕСТД и ЕСПД					
Знать:	Фрагментарные знания	Неполные знания	Сформированные, но содержащие отдельные пробелы знания	Сформированные систематические знания	контролирующие материалы по дисциплине, в числе которых могут быть: кейс-задания, задания для контрольной работы, тестовые задания, темы рефератов, докладов и другие.
Уметь:	Частичные умения	Неполные умения	Умения полные, допускаются небольшие ошибки	Сформированные умения	
Владеть:	Частичное владение навыками	Несистематическое применение навыков	В систематическом применении навыков допускаются пробелы	Успешное и систематическое применение навыков	
ОПК-7: Способен управлять организацией, осуществляющей деятельность в строительной отрасли и сфере жилищно-коммунального хозяйства, организовывать и оптимизировать ее производственную деятельность					
ОПК-7.1 Знает основные принципы построения компьютера, формы и способы представления данных; области и особенности применения языков программирования высокого уровня					
Знать:	Фрагментарные знания	Неполные знания	Сформированные, но содержащие отдельные пробелы знания	Сформированные систематические знания	контролирующие материалы по дисциплине, в числе которых могут быть: кейс-задания, задания для контрольной работы, тестовые задания, темы рефератов, докладов и другие.
Уметь:	Частичные умения	Неполные умения	Умения полные, допускаются небольшие ошибки	Сформированные умения	
Владеть:	Частичное владение навыками	Несистематическое применение навыков	В систематическом применении навыков допускаются пробелы	Успешное и систематическое применение навыков	
ПК-7: Способен оформлять рабочую техническую документацию с учетом действующих нормативных и методических документов					
ПК-7.2 Умеет оформлять рабочую и эксплуатационную документацию на средства и системы информатизации в защищенном исполнении					

Планируемые результаты освоения компетенции	Критерии оценивания результатов обучения				Наименование оценочного средства
	неудовлетворительно	удовлетворительно	хорошо	отлично	
1	2	3	4	5	6
Знать:	Фрагментарные знания	Неполные знания	Сформированные, но содержащие отдельные пробелы знания	Сформированные систематические знания	контролирующие материалы по дисциплине, в числе которых могут быть: кейс-задания, задания для контрольной работы, тестовые задания, темы рефератов, докладов и другие.
Уметь:	Частичные умения	Неполные умения	Умения полные, допускаются небольшие ошибки	Сформированные умения	
Владеть:	Частичное владение навыками	Несистематическое применение навыков	В систематическом применении навыков допускаются пробелы	Успешное и систематическое применение навыков	
ОПК-7: Способен управлять организацией, осуществляющей деятельность в строительной отрасли и сфере жилищно-коммунального хозяйства, организовывать и оптимизировать ее производственную деятельность					
ОПК-7.2 Умеет работать с интегрированной средой разработки программного обеспечения; разрабатывать и реализовывать на языке высокого уровня алгоритмы решения типовых профессиональных задач					
Знать:	Фрагментарные знания	Неполные знания	Сформированные, но содержащие отдельные пробелы знания	Сформированные систематические знания	контролирующие материалы по дисциплине, в числе которых могут быть: кейс-задания, задания для контрольной работы, тестовые задания, темы рефератов, докладов и другие.
Уметь:	Частичные умения	Неполные умения	Умения полные, допускаются небольшие ошибки	Сформированные умения	
Владеть:	Частичное владение навыками	Несистематическое применение навыков	В систематическом применении навыков допускаются пробелы	Успешное и систематическое применение навыков	
ПК-7: Способен оформлять рабочую техническую документацию с учетом действующих нормативных и методических документов					
ПК-7.3 Владеет навыками разработки технического проекта средства и/или системы информатизации в защищенном исполнении					
Знать:	Фрагментарные знания	Неполные знания	Сформированные, но содержащие отдельные пробелы знания	Сформированные систематические знания	контролирующие материалы по дисциплине, в числе которых могут быть: кейс-задания, задания для контрольной работы, тестовые задания, темы рефератов, докладов и другие.
Уметь:	Частичные умения	Неполные умения	Умения полные, допускаются небольшие ошибки	Сформированные умения	
Владеть:	Частичное владение навыками	Несистематическое применение навыков	В систематическом применении навыков допускаются пробелы	Успешное и систематическое применение навыков	
ОПК-7: Способен управлять организацией, осуществляющей деятельность в строительной отрасли и сфере жилищно-коммунального хозяйства, организовывать и оптимизировать ее производственную деятельность					
ОПК-7.3 Владеть навыками разработки, документирования, тестирования и отладки программ; разработки алгоритмов решения типовых профессиональных задач					
Знать:	Фрагментарные знания	Неполные знания	Сформированные, но содержащие отдельные пробелы знания	Сформированные систематические знания	контролирующие материалы по дисциплине, в числе которых могут быть: кейс-задания, задания для контрольной работы, тестовые задания, темы рефератов, докладов и другие.
Уметь:	Частичные умения	Неполные умения	Умения полные, допускаются небольшие ошибки	Сформированные умения	
Владеть:	Частичное владение навыками	Несистематическое применение навыков	В систематическом применении навыков допускаются пробелы	Успешное и систематическое применение навыков	
ОПК-2: Способен анализировать, критически осмысливать и представлять информацию, осуществлять поиск научно-технической информации, приобретать новые знания, в том числе с помощью информационных технологий					

Планируемые результаты освоения компетенции	Критерии оценивания результатов обучения				Наименование оценочного средства
	неудовлетворительно	удовлетворительно	хорошо	отлично	
1	2	3	4	5	6
ОПК-2.3.1 Знает национальные, межгосударственные и международные стандарты в области защиты информации, нормативные правовые акты в области защиты информации, руководящие и методические документы уполномоченных федеральных органов исполнительной власти в области внедрения и эксплуатации средств защиты информации					
Знать:	Фрагментарные знания	Неполные знания	Сформированные, но содержащие отдельные пробелы знания	Сформированные систематические знания	контролирующие материалы по дисциплине, в числе которых могут быть: кейс-задания, задания для контрольной работы, тестовые задания, темы рефератов, докладов и другие.
Уметь:	Частичные умения	Неполные умения	Умения полные, допускаются небольшие ошибки	Сформированные умения	
Владеть:	Частичное владение навыками	Несистематическое применение навыков	В систематическом применении навыков допускаются пробелы	Успешное и систематическое применение навыков	
ОПК-2: Способен анализировать, критически осмысливать и представлять информацию, осуществлять поиск научно-технической информации, приобретать новые знания, в том числе с помощью информационных технологий					
ОПК-2.3.2 Умеет документировать процедуры и результаты контроля функционирования системы защиты информации; проводить испытания программно-технических средств защиты информации от НСД и специальных воздействий на соответствие требованиям по безопасности информации и техническим условиям					
Знать:	Фрагментарные знания	Неполные знания	Сформированные, но содержащие отдельные пробелы знания	Сформированные систематические знания	контролирующие материалы по дисциплине, в числе которых могут быть: кейс-задания, задания для контрольной работы, тестовые задания, темы рефератов, докладов и другие.
Уметь:	Частичные умения	Неполные умения	Умения полные, допускаются небольшие ошибки	Сформированные умения	
Владеть:	Частичное владение навыками	Несистематическое применение навыков	В систематическом применении навыков допускаются пробелы	Успешное и систематическое применение навыков	
ОПК-2: Способен анализировать, критически осмысливать и представлять информацию, осуществлять поиск научно-технической информации, приобретать новые знания, в том числе с помощью информационных технологий					
ОПК-2.3.3 Владеет навыками внесения изменений в эксплуатационную документацию и организационно-распорядительные документы по системе защиты информации; навыками разработки программ и методик испытаний опытного образца программно-технического средства защиты информации от НСД и специальных воздействий на соответствие техническим условиям					
Знать:	Фрагментарные знания	Неполные знания	Сформированные, но содержащие отдельные пробелы знания	Сформированные систематические знания	контролирующие материалы по дисциплине, в числе которых могут быть: кейс-задания, задания для контрольной работы, тестовые задания, темы рефератов, докладов и другие.
Уметь:	Частичные умения	Неполные умения	Умения полные, допускаются небольшие ошибки	Сформированные умения	
Владеть:	Частичное владение навыками	Несистематическое применение навыков	В систематическом применении навыков допускаются пробелы	Успешное и систематическое применение навыков	
ОПК-2: Способен анализировать, критически осмысливать и представлять информацию, осуществлять поиск научно-технической информации, приобретать новые знания, в том числе с помощью информационных технологий					
ОПК-2.4.1 Знает критерии оценки защищенности объекта информатизации, технические средства контроля эффективности мер защиты информации, методы измерений, контроля и технических расчетом характеристик программно-аппаратных средств защиты информации					
Знать:	Фрагментарные знания	Неполные знания	Сформированные, но содержащие отдельные пробелы знания	Сформированные систематические знания	контролирующие материалы по дисциплине, в числе которых могут быть: кейс-задания, задания для контрольной работы, тестовые

Планируемые результаты освоения компетенции	Критерии оценивания результатов обучения				Наименование оценочного средства
	неудовлетворительно	удовлетворительно	хорошо	отлично	
1	2	3	4	5	6
Уметь:	Частичные умения	Неполные умения	Умения полные, допускаются небольшие ошибки	Сформированные умения	задания, темы рефератов, докладов и другие.
Владеть:	Частичное владение навыками	Несистематическое применение навыков	В систематическом применении навыков допускаются пробелы	Успешное и систематическое применение навыков	
ОПК-2: Способен анализировать, критически осмысливать и представлять информацию, осуществлять поиск научно-технической информации, приобретать новые знания, в том числе с помощью информационных технологий					
ОПК-2.4.2 Умеет осуществлять контроль обеспечения уровня защищенности объектов информатизации					
Знать:	Фрагментарные знания	Неполные знания	Сформированные, но содержащие отдельные пробелы знания	Сформированные систематические знания	контролирующие материалы по дисциплине, в числе которых могут быть: кейс-задания, задания для контрольной работы, тестовые задания, темы рефератов, докладов и другие.
Уметь:	Частичные умения	Неполные умения	Умения полные, допускаются небольшие ошибки	Сформированные умения	
Владеть:	Частичное владение навыками	Несистематическое применение навыков	В систематическом применении навыков допускаются пробелы	Успешное и систематическое применение навыков	
ОПК-2: Способен анализировать, критически осмысливать и представлять информацию, осуществлять поиск научно-технической информации, приобретать новые знания, в том числе с помощью информационных технологий					
ОПК-2.4.3 Владеет навыками оценки защищенности объектов информатизации с помощью типовых программных средств					
Знать:	Фрагментарные знания	Неполные знания	Сформированные, но содержащие отдельные пробелы знания	Сформированные систематические знания	контролирующие материалы по дисциплине, в числе которых могут быть: кейс-задания, задания для контрольной работы, тестовые задания, темы рефератов, докладов и другие.
Уметь:	Частичные умения	Неполные умения	Умения полные, допускаются небольшие ошибки	Сформированные умения	
Владеть:	Частичное владение навыками	Несистематическое применение навыков	В систематическом применении навыков допускаются пробелы	Успешное и систематическое применение навыков	
ПК-8: Способен принимать участие в формировании, организации и поддержания выполнения комплекса мер по обеспечению информационной безопасности, управлении процессом их реализации					
ПК-8.2 Умеет разрабатывать и реализовывать организационные меры, обеспечивающие эффективность системы защиты информации					
Знать:	Фрагментарные знания	Неполные знания	Сформированные, но содержащие отдельные пробелы знания	Сформированные систематические знания	контролирующие материалы по дисциплине, в числе которых могут быть: кейс-задания, задания для контрольной работы, тестовые задания, темы рефератов, докладов и другие.
Уметь:	Частичные умения	Неполные умения	Умения полные, допускаются небольшие ошибки	Сформированные умения	
Владеть:	Частичное владение навыками	Несистематическое применение навыков	В систематическом применении навыков допускаются пробелы	Успешное и систематическое применение навыков	
ОПК-8: Способен осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических документов в целях решения задач профессиональной деятельности;					
ОПК-8.2 Умеет обобщать, анализировать и систематизировать научную информацию в области информационной безопасности; пользоваться информационно- справочными системами					
Знать:	Фрагментарные знания	Неполные знания	Сформированные, но содержащие отдельные	Сформированные систематические знания	контролирующие материалы по дисциплине, в

Планируемые результаты освоения компетенции	Критерии оценивания результатов обучения				Наименование оценочного средства
	неудовлетворительно	удовлетворительно	хорошо	отлично	
1	2	3	4	5	6
			пробелы знания		числе которых могут быть: кейс-задания, задания для контрольной работы, тестовые задания, темы рефератов, докладов и другие.
Уметь:	Частичные умения	Неполные умения	Умения полные, допускаются небольшие ошибки	Сформированные умения	
Владеть:	Частичное владение навыками	Несистематическое применение навыков	В систематическом применении навыков допускаются пробелы	Успешное и систематическое применение навыков	

7.3. Типовые контрольные задания и иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций в процессе освоения образовательной программы

Темы рефератов

1.Правовое регулирование коммерческой тайны.

2.Правовой механизм и способы защиты коммерческой тайны в РФ.

3.Правовые основы защиты государственной тайны.

4.Право граждан на информацию в системе защиты государственной тайны.

5.Правовые аспекты защиты банковской тайны в РФ.

6.Правовая защита прав авторов программ для ЭВМ и баз данных.

7.Организационно-правовые меры предупреждения преступлений в сфере компьютерной информации.

8.Анализ российского законодательства в сфере безопасности информационных систем.

9.Уголовно-правовые формы защиты компьютерной информации.

10.Порядок разрешения гражданско-правовых споров при нарушении прав владельцев интеллектуальной собственности.

11.Основные направления совершенствования правового обеспечения информационной безопасности РФ с учетом зарубежного опыта.

12.Анализ мер юридической ответственности за разглашение защищаемой информации.

13.Международное сотрудничество в области охраны интеллектуальной собственности.

14.Правовые основы интеллектуальной собственности.

15.Расследование преступлений в сфере компьютерной информации.

16.Уголовно-правовая характеристика компьютерных преступлений.

17.Тенденции развития компьютерной преступности в России.

18.Правовые режимы защиты информации.

19.Правовые вопросы защиты информации с использованием технических средств.

20.Интеллектуальная собственность в сети Интернет.

21.Оценка и анализ особенностей системы организационной защиты информации (объект прохождения практики).

22.Рекомендации по внедрению системы видеонаблюдения на социальном объекте (объект прохождения практики)

23.Исследование технологий работы персонала, связанного с конфиденциальной информацией (объект прохождения практики).

24.Анализ и совершенствование организации охраны территорий, зданий, помещений и персонала (объект прохождения практики).

25.Совершенствование организации пропускного и внутриобъектового режимов (объект прохождения практики).

26.Подбор в организации персонала, связанного с конфиденциальной информацией (объект прохождения практики).

27.Организация защиты информации при приеме в организации посетителей (объект прохождения практики).

28.Организация защиты информации при осуществлении рекламной и публикаторской деятельности (объект прохождения практики).

29.Аналитическая работа как основа управления системой организационной защиты информации (объект прохождения практики).

30.Организационная защита информации при приеме в организации командированных лиц (объект прохождения практики).

Темы докладов

1.Анализ организации защиты информации при приеме в организации иностранных представителей (объект прохождения практики).

2.Анализ организации защиты информации в кадровой службе (объект прохождения практики).

3.Исследование защиты информации при работе с посетителями (объект прохождения практики).

4.Анализ целей и задач информационно-аналитической работы (объект прохождения практики).

5.Исследование методов и направлений информационно-аналитической работы (объект прохождения практики).

6.Анализов информационно-аналитической работы (объект прохождения практики).

7.Анализ организационной структуры службы безопасности (объект прохождения практики).

8.Исследование организационного обеспечения безопасности информации ограниченного доступа и (объект прохождения практики).



9.Анализ организации режима секретности, его особенностей и содержания на ... (объект прохождения практики).

10.Порядок действий во внештатной ситуации на ... (объект прохождения практики).

11.Описание основных факторов и угроз информационной безопасности (объект прохождения практики).

12.Оценки рисков информационной безопасности (объект прохождения практики).

13.Методы противодействия возможным угрозам информационной безопасности (объект прохождения практики).

14.Построение модели противника и организационные методы противодействия угрозам (объект прохождения практики).

15.Разработка политик безопасности (объект прохождения практики).

16.Рекомендации для построения и контроля информационной среды на основе стандарта CobiT (объект прохождения практики).

17.Оценки безопасности ИТ на основе ГОСТ Р ИСО/МЭК 15408-2002 ИТ (объект прохождения практики).

18.Обоснование затрат на информационную безопасность (объект прохождения практики).

19.Организация электронного документооборота (объект прохождения практики).

20.Обоснование необходимости создания подразделения по защите информации и его штатной численности (объект прохождения практики).

21.Разработка структуры и порядка межведомственного взаимодействия по вопросам обеспечения информационной безопасности (объект прохождения практики).

22.Методы оценки лояльности персонала (сотрудников) (объект прохождения практики).

23.Рекомендации по организации резервного копирования, архивирования и восстановления информационных ресурсов (объект прохождения практики).

24.Рекомендации по организации работы с информацией, составляющей коммерческую тайну (объект прохождения практики).

25.Совершенствование организации и обеспечения защиты коммерческой тайны на ... (объект прохождения практики).

Контрольные тесты и задания

Выберите верный вариант. «К информации открытого типа всегда относятся:

А) сведения о человеке, его семье и личной жизни;

Б) технология изготовления продуктов и услуг фирмы;

В) информация о фактах нарушения прав и свобод человека;

Г) стратегия действий фирмы на рынке.

К секретной информации относится:



А) государственная тайна;

Б) коммерческая тайна;

В) профессиональная тайна;

Г) конфиденциальная информация.

Напишите определение понятия «государственная тайна»:

_____
_____

Сферу коммерческой тайны регулирует:

А) Федеральный закон «О коммерческой тайне в коммерческих организациях»;

Б) Федеральный закон «О коммерческих организациях»;

В) Федеральный конституционный закон «О коммерческой тайне»

Г) Федеральный закон «О коммерческой тайне».

Ценность конфиденциальной информации означает:

А) размер прибыли при использовании такой информации фирмой;

Б) размер убытков при утрате такой информации;

В) моральный ущерб при утрате такой информации или ее использовании в неправомерных целях;

Г) размер прибыли при использовании такой информации фирмой и размер убытков при ее утрате.

К объектам авторского права НЕ относятся (выберите несколько вариантов):

А) произведения науки;

Б) фонограмма;

В) программы для ЭВМ;

Г) литературное произведение;

Д) официальные документы (например, судебные решения);

Е) сообщения новостного характера.

Промышленный образец – это…

А) художественно-конструкторское решение изделия, которое определяет его внешний вид;

Б) художественно-конструкторское решение изделия, которое определяет его внешний вид и должно быть новым, промышленно применимым и оригинальным;

В) техническое решение изделия;

Г) техническое решение изделия, которое обладает мировой новизной, неочевидностью и осуществимо промышленным путем.



Права на полезную модель защищаются:

А) авторским свидетельством;

Б) патентом;

Г) патентом или авторским свидетельством;

Д) справкой о регистрации модели.

9. Незаинтересованное лицо с точки зрения угроз конфиденциальной информации – это…

А) третье лицо, которое всегда помогает злоумышленнику;

Б) постороннее лицо, не представляющее угрозы для конфиденциальной информации;

В) постороннее лицо, получившее конфиденциальную информацию во владение в силу обстоятельств или безответственности персонала;

Г) третье лицо, преднамеренно получившее конфиденциальную информацию во владение.

10. Разглашение или огласка информации связана с:

А) утратой информации по вине персонала, в результате чего со сведениями ознакомились лица, не допущенные к ним;

Б) противоправное, преднамеренное действие, в результате чего лицо овладело конфиденциальной информацией, не имея на то права доступа;

В) бесконтрольный выход конфиденциальных данных за пределы организации или круга лиц, которым она была доверена

Тестовые задания

1. Информационная безопасность

а) – это деятельность, направленная на предотвращение утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию;

б) - мероприятия и действия, которые должны осуществлять должностные лица в процессе работы с информацией для обеспечения заданного уровня её безопасности;

в) - это комплекс направлений и методов управленческого, ограничительного и технологического характера, определяющих основы и содержание системы защиты, побуждающих персонал соблюдать правила защиты конфиденциальной информации.

2. К способам НСД относятся*:

а) инициативное сотрудничество, подслушивание;

б) перехват, сбор и аналитическая обработка;

в) создание механизма и условий оперативного реагирования на угрозы безопасности и проявления негативных тенденций в функционировании предприятия;

г) эффективное пресечение посягательств на ресурсы и персонал.

3. Аналитическое исследование источников конфиденциальной информации предусматривает:*

а) выявление и классификация максимально возможных источников конфиденциальной информации;

б) выявление и классификация максимального состава источников угроз конфиденциальной информации;

в) изучение данных учета осведомленности сотрудников о тайне;

г) ведение и анализ полноты перечня существующей информации

4. Сколько стадий проходят теоретические экспертные системы в своем развитии:

а) 2;

б) 3.;

в) 5.

5. При выполнении информационно-аналитической работы необходимо решить следующие задачи*:

а) обеспечить безопасность собственных информационных ресурсов;

б) контроль за оформлением открытого делопроизводства и секретной документации;

в) обеспечить эффективность и исключить дублирование при сборе и распространении информации

г) вопросы допуска сотрудников к закрытым работам и документам.

6. Защищаемые государством сведения в области его военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб безопасности государства - это…

а) Государственная тайна;

б) Коммерческая тайна;

в) Служебная тайна.

7. В основу работы подразделений по защите государственной тайны положены следующие документы*:

а) "Инструкция по обеспечению режима секретности в министерствах, ведомствах, на предприятиях и в организациях";

б) "Перечень сведений, составляющих государственную тайну";

в) "Производственная документация по ведению секретного делопроизводства";

г) "Положение о порядке установления степени секретности сведений, содержащихся в работах, документах и изделиях".

8.**Защитные действия это**

а) – комплекс мероприятий, ориентированных на пресечение разглашения, защиту информации от утечки и противодействия несанкционированному доступу;

б) - выявление возможных каналов утечки информации, присущих для данного предприятия;

в) - разработка и реализация мероприятий по своевременному закрытию выявленных каналов утечки закрытой информации;

г) - планирование всей работы по вопросам режима секретности, защиты от технических разведок на предприятии;

д) - организация и ведение общей профилактической работы по защите закрытой информации от технических разведок.

9.**Способы НСД:**

а) инициативное сотрудничество, склонение к сотрудничеству, выведывание и выпытывание;

б) законное подслушивание и захват заложников;

в) сбор и анализ открытой информации с целью получения достоверных и объемлющих сведений по интересующему злоумышленника аспекту деятельности объекта его интересов.

10.**Какие из перечисленных задач обеспечения безопасности информации решаются на организационном уровне?*:**

а) организация работ по разработке системы защиты информации;

б) шифрование файлов с данными;

в) защита каналов связи;

г) распространение конфиденциальной информации;

д) разработка нормативно-правовой документации.

Примерный перечень вопросов к зачету по дисциплине

«Организационное и правовое обеспечение информационной безопасности»

1.Основы законодательства Российской Федерации в области информационной безопасности и защиты информации.

2.Понятие и виды информации, защищаемой законодательством Российской Федерации.

3.Государственная тайна как особый вид защищаемой информации.

4.Система защиты государственной тайны.

5.Засекречивание информации.

6.Организационные и технические способы защиты государственной тайны.

7.Коммерческая тайна.

8.Служебная тайна

9.Профессиональные тайны.

10.Процессуальные тайны.

11.Персональные данные.

12.Правовой режим защиты государственной тайны.

13.Правовой режим банковской тайны.

14.Правовой режим персональных данных.

15.Электронная цифровая подпись.

16.Электронный документ как доказательство.

17.Лицензирование и сертификация в области обеспечения безопасности информации.

18.Понятие и структура интеллектуальной собственности.

19.Регулирование информационных отношений институтом авторского права при производстве, передаче и распространении информации.

20.Регулирование информационных отношений институтом авторского права при производстве, передаче и распространении программ для ЭВМ, при создании и эксплуатации баз данных.

21.Регулирование информационных отношений институтом патентного права.

22.Развитие международной системы охраны авторских прав.

23.Субъекты авторского права.

24.Права обладателей авторских прав.

25.Защита авторских и смежных прав в законодательстве РФ.

26.Интеллектуальная собственность в сети Интернет.

27.Правовые формы организации деятельности СМИ.

28.Правовое регулирование в области производства и распространения рекламы как разновидности массовой информации.

29.Законодательство в области библиотечного дела.

30.Правовое регулирование архивного дела.

31.Правовая ответственность за правонарушения в информационной сфере.

32.Виды юридической ответственности за правонарушения в информационной сфере.

33.Понятие компьютерных преступлений.

34.Классификация компьютерных преступлений.

35.Уголовно-правовая характеристика компьютерных преступлений.

36.Неправомерный доступ к компьютерной информации (ст.272).

37.Создание, использование и распространение вредоносных программ для ЭВМ (ст.273).

38.Нарушение правил эксплуатации ЭВМ, системы ЭВМ или сети (ст.274).

39.Криминалистическая характеристика компьютерных преступлений.

40.Характеристика преступлений, совершаемых в сфере компьютерной информации.

41.Основные виды преступлений в сфере программного обеспечения.

42.Изготовление контрафактных экземпляров программ конечным пользователем.

43.Способы совершения преступлений в сфере компьютерной информации.

44.Компьютерные вирусы: общие сведения.

45.Классификация вирусов.

46.Классификация антивирусных средств.

47.Методы защиты от компьютерных вирусов.

48.Тенденции развития компьютерной преступности в России.

49.Криминалистические аспекты проведения расследования компьютерных преступлений.

50.Тактика обнаружения, изъятия и фиксации компьютерной информации при производстве следственных действий.

51.Экспертиза преступлений в сфере компьютерной информации.

52.Назовите основные виды угроз безопасности предприятия.

53.Перечислите цель и задачи системы безопасности предприятия.

54.Какие средства используются для обеспечения безопасности предприятия?

55.Дайте определение трем видам правомерного овладения конфиденциальной информацией.

56.Определите в процентах степень опасности внутренних и внешних угроз неправомерному овладению информацией.

57.Какие компоненты входят в состав концептуальной модели безопасности информации?

58.Назовите основные принципы построения системы безопасности предприятия?

59.Какими инструкциями руководствуются при организации работы службы безопасности предприятия?

60.Назвать основные виды безопасности на предприятии.

61.Что необходимо включать в коллективный договор для правового обеспечения защиты информации?

62.Перечислить основные нормативные документы,

регламентирующие деятельность в области защиты информации.

63.В чем состоит суть лицензирования деятельности предприятий в области защиты информации?

64.Какие виды деятельности предприятия в области защиты информации необходимо лицензировать?

65.Назвать разделы устава службы безопасности предприятия и дать им характеристику.

66.Какие подразделения входят в состав СБП?



67.Назовите основные функции СБП.

68.Каким законом регламентируются функции СБП?

69.По каким направлениям производится расследование факта разглашения коммерческой тайны?

70.Чем определяется состав СБП?

7.4. Методические материалы, определяющие процедуры оценивания знаний, умений и навыков, и опыта деятельности, характеризующих этапы формирования компетенций

Требования к написанию реферата

Продукт самостоятельной работы студента, представляющий собой краткое изложение в письменном виде полученных результатов (учебно-исследовательской) темы, где автор раскрывает суть исследуемой проблемы, приводит различные точки зрения, а также собственные взгляды на нее.

Реферат должен быть структурирован (по главам, разделам, параграфам) и включать разделы: введение, основная часть, заключение, список использованных источников. В зависимости от тематики реферата к нему могут быть оформлены приложения, содержащие документы, иллюстрации, таблицы, схемы и т.д. Объем реферата – 15-20 страниц печатного текста, включая титульный лист, введение, заключение и список литературы.

Его задачами являются:

1. Формирование умений самостоятельной работы с источниками литературы, их систематизация;

2. Развитие навыков логического мышления;

3. Углубление теоретических знаний по проблеме исследования.

При оценке реферата используются следующие критерии:

- новизна текста;

- обоснованность выбора источника;

- степень раскрытия сущности вопроса;

- соблюдения требований к оформлению.

Критерии оценивания реферата:	
«отлично»	Выполнены все требования к написанию и защите реферата: обозначена проблема и обоснована её актуальность, сделан краткий анализ различных точек зрения на рассматриваемую проблему и логично изложена собственная позиция, сформулированы выводы, тема раскрыта полностью, выдержан объём, соблюдены требования к внешнему оформлению, даны правильные ответы на дополнительные вопросы.
«хорошо»	Основные требования к реферату и его защите выполнены, но при этом допущены недочёты. В частности, имеются неточности в изложении материала; отсутствует логическая последовательность в суждениях; невыдержан объём реферата; имеются упущения в оформлении; на дополнительные вопросы при защите даны неполные ответы.
«удовлетвори-тельно»	Имеются существенные отступления от требований к реферированию. В частности: тема освещена лишь частично; допущены фактические ошибки в содержании реферата или при ответе на дополнительные вопросы; во время защиты отсутствует вывод.

«неудовлетво-рительно»	Тема реферата не раскрыта, обнаруживается существенное не понимание проблемы.

Тематика рефератов выдается преподавателем в конце семинарского занятия.

Требования к написанию доклада

Доклад – продукт самостоятельной работы обучающегося, представляющий собой публичное выступление по представлению полученных результатов решения определенной учебно-практической, учебно-исследовательской или научной темы.

Критерии оценивания доклада:

Отметка
«отлично» выполнены все требования к написанию и защите доклада: обозначена проблема и обоснована её актуальность, сделан краткий анализ различных точек зрения на рассматриваемую проблему и логично изложена собственная позиция, сформулированы выводы, тема раскрыта полностью, выдержан объём, соблюдены требования к внешнему офо рмлению, даны правильные ответы на дополнительные вопросы.

Отметка «хорошо» - основные требования к докладу и его защите выполнены, но при этом до пущены недочёты. В частности, имеются неточности в изложении материала, отсутствует лог ическая последовательность в суждениях, не выдержан объём реферата, имеются упущения в оформлении, не допускает существенных неточностей в ответе на дополнительный вопрос.

Отметка «удовлетворительно» - имеются существенные отступления от требований к докладу. В частности, тема освещена лишь частично, допущены фактические ошибки в содер жании доклада или при ответе на дополнительные вопросы, во время защиты отсутствует вывод.

Отметка «неудовлетворительно» - тема доклада не раскрыта, обнаруживается существенное непонимание проблемы.

Требования к выполнению тестового задания

Тестирование является одним из основных средств формального контроля качества обучения. Это метод, основанный на стандартизированных заданиях, которые позволяют измерить психофизиологические и личностные характеристики, а также знания, умения и навыки испытуемого.

Основные принципы тестирования, следующие:

− связь с целями обучения - цели тестирования должны отвечать критериям социальной полезности и значимости, научной корректности и общественной поддержки;

− объективность - использование в педагогических измерениях этого принципа призвано не допустить субъективизма и предвзятости в процессе этих измерений;

− справедливость и гласность - одинаково доброжелательное отношение ко всем обучающимся, открытость всех этапов процесса измерений, своевременность ознакомления обучающихся с результатами измерений;

− систематичность – систематичность тестирований и самопроверок каждого учебного модуля, раздела и каждой темы; важным аспектом данного принципа является требование репрезентативного представления содержания учебного курса в содержании теста;

- гуманность и этичность - тестовые задания и процедура тестирования должны исключать нанесение какого-либо вреда обучающимся, не допускать ущемления их по национальному, этническому, материальному, расовому, территориальному, культурному и другим

признакам;

Важнейшим является принцип, в соответствии с которым тесты должны быть построены по методике, обеспечивающей выполнение требований соответствующего федерального государственного образовательного стандарта.

В тестовых заданиях используются четыре типа вопросов:

− закрытая форма - является наиболее распространенной и предлагает несколько альтернативных ответов на поставленный вопрос. Например, обучающемуся задается вопрос, требующий альтернативного ответа «да» или «нет», «является» или «не является», «относится» или «не относится» и т.п. Тестовое задание, содержащее вопрос в закрытой форме, включает в себя один или несколько правильных ответов и иногда называется выборочным заданием. Закрытая форма вопросов используется также в тестах-задачах с выборочными ответами. В тестовом задании в этом случае сформулированы условие задачи и все необходимые исходные данные, а в ответах представлены несколько вариантов результата решения в числовом или буквенном виде. Обучающийся должен решить задачу и показать, какой из представленных ответов он получил.

− открытая форма - вопрос в открытой форме представляет собой утверждение, которое необходимо дополнить. Данная форма может быть представлена в тестовом задании, например, в виде словесного текста, формулы (уравнения), графика, в которых пропущены существенные составляющие - части слова или буквы, условные обозначения, линии или изображения элементов схемы и графика. Обучающийся должен по памяти вставить соответствующие элементы в указанные места («пропуски»).

− установление соответствия - в данном случае обучающемуся предлагают два списка, между элементами которых следует установить соответствие;

− установление последовательности - предполагает необходимость установить правильную последовательность предлагаемого списка слов или фраз.

Критерии оценки знаний при проведении тестирования

Отметка «отлично» выставляется при условии правильного ответа не менее чем 85% тестовых заданий;

Отметка «хорошо» выставляется при условии правильного ответа не менее чем 70 % тестовых заданий;

Отметка «удовлетворительно» выставляется при условии правильного ответа не менее 50 %;

Отметка «неудовлетворительно» выставляется при условии правильного ответа менее чем на 50 % тестовых заданий.

Результаты текущего контроля используются при проведении промежуточной аттестации.

Критерии оценки знаний на экзамене

Экзамен может проводиться вформе устного опроса побилетам (вопросам) или без билетов, с предварительной подготовкой илибез подготовки, поусмотрению преподавателя. Экзаменатор вправе задавать вопросы сверх билета, а также, помимо теоретических вопросов, давать задачи попрограмме данного курса.

Экзаменационные билеты (вопросы) утверждаются назаседании кафедры иподписываются заведующим кафедрой. Вбилете должно содержаться неболее трех вопросов. Комплект экзаменационных билетов подисциплине должен содержать15—20 билетов.

Экзаменатор может проставить экзамен без опросаили собеседования тем студентам, которые активно участвовали всеминарских занятиях.



Отметка «отлично» - студент глубоко и прочно усвоил весь программный материал, исчерпывающе, последовательно, грамотно и логически стройно его излагает, тесно увязывает теорию с практикой. Студент не затрудняется с ответом при видоизменении задания, свободно справляется с задачами, заданиями и другими видами применения знаний, показывает знания законодательного и нормативно-технического материалов, правильно обосновывает принятые решения, владеет разносторонними навыками и приемами выполнения практических работ, обнаруживает умение самостоятельно обобщать и излагать материал, не допуская ошибок.

Отметка «хорошо» - студент твердо знает программный материал, грамотно и по существу излагает его, не допускает существенных неточностей в ответе на вопрос, может правильно применять теоретические положения и владеет необходимыми навыками при выполнении практических заданий.

Отметка «удовлетворительно» - студент усвоил только основной материал, но не знает отдельных деталей, допускает неточности, недостаточно правильные формулировки, нарушает последовательность в изложении программного материала и испытывает затруднения в выполнении практических заданий.

Отметка «неудовлетворительно» **-** студент не знает значительной части программного материала, допускает существенные ошибки, с большими затруднениями выполняет практические работы.

8. Учебно-методическое и информационное обеспечение дисциплины (модуля)

8.1. Основная литература

Название	Ссылка

8.2. Дополнительная литература

Название	Ссылка

8.3. Информационно-телекоммуникационные ресурсы сети «Интернет»

1.ФСТЭК России. Федеральная служба по техническому и экспортному контролю: официальный сайт. – Москва. – URL: https://fstec.ru// – Текст: электронный. 2.Информика: [сайт] / Федеральное государственное автономное учреждение «Государственный научно-исследовательский институт информационных технологий и телекоммуникаций». – Москва.– URL: https://informika.ru/. – Текст: электронный. 3.Всероссийский научно-исследовательский институт автоматизации управления в непромышленной сфере имени В. В. Соломатина (ВНИИНС им. В.В. Соломатина): официальный сайт. – Москва. – URL: http://www.vniins.ru/index.php?lang=%D0%A0%D1%83%D1%81. – Текст: электронный. 4.Parallel.ru. Лаборатория Параллельных информационных технологий: [сайт] / Научно-исследовательский вычислительный центр Московского государственного университета имени М.В.Ломоносова. – Москва.– URL: https://parallel.ru/about. – Текст: электронный. 5.RSDN: [сайт]. – [Москва]. – URL: http://rsdn.org/. – Текст: электронный. 6.Лаборатория Касперского: официальный сайт. – Москва. – URL: https://www.kaspersky.ru/. – Текст: электронный. 7.InformationSecurity. Информационная безопасность: [сайт]. – Москва. – URL: http://www.itsec.ru/news. – Текст: электронный. Znanium.com. Базовая коллекция : электронно-библиотечная система : сайт / ООО "Научно-издательский центр Инфра-М". – Москва, 2011 - – URL: http://znanium.com/catalog (дата обновления: 06.06.2019). - Режим доступа: для зарегистрир. пользователей. – Текст: электронный. Фонд ЭБС формируется с учетом всех изменений образовательных стандартов и включает учебники, учебные пособия, УМК, монографии, авторефераты, диссертации, энциклопедии, словари и справочники, законодательно-нормативные документы, специальные периодические издания и издания, выпускаемые издательствами вузов. http://znanium.com/catalog/ Национальная электронная библиотека (НЭБ) : федеральная государственная информационная система : сайт / Министерство культуры Российской Федерации, Российская государственная библиотека. – Москва, 2004 - – URL: https://нэб.рф/. - Режим доступа: для зарегистрир. пользователей. – Текст: электронный. НЭБ - проект Российской государственной библиотеки. Начиная с 2004 г. Проект Национальная электронная библиотека (НЭБ) разрабатывается ведущими российскими библиотеками при поддержке Министерства культуры Российской Федерации. Основная цель НЭБ - обеспечить свободный доступ гражданам Российской Федерации ко всем изданным, издаваемым и хранящимся в фондах российских библиотек изданиям и научным работам, – от книжных памятников истории и культуры, до новейших авторских произведений. В настоящее время проект НЭБ включает более 1.660.000 электронных книг, более 33.000.000 записей каталогов.РОССИЙСКАЯ НАЦИОНАЛЬНАЯ БИБЛИОТЕКА (РНБ) : сайт / Российская национальная библиотека. - Москва : РНБ, 1998. - URL: http://nlr.ru/. – Режим доступа: для зарегистрир. пользователей. – Текст: электронный. "... одна из крупнейших в мире и вторая по величине фондов в Российской Федерации – служит российской культуре и науке, хранит национальную память, способствует просвещению населяющих Россию народов и распространению идей гуманизма. ... В фондах Библиотеки хранится более 38,6 млн экз. произведений печати и иных информационных ресурсов, в том числе и на электронных носителях, доступных широкому кругу пользователей. Ежегодно РНБ посещает около 850 тыс. читателей, которым выдается до 5 млн изданий, к ее электронным ресурсам обращаются за год свыше 10 млн удаленных пользователей. ... Сохраняя культурную и историческую



преемственность, верность библиотечным традициям, заложенным еще в Императорской Публичной библиотеке, РНБ сегодня — современное информационное учреждение, оснащенное новейшим оборудованием и своевременно отвечающее на насущные вызовы времени." (цитата с сайта РНБ: http://nlr.ru/nlr_visit/RA1162/rnb-today) https://нэб.рф/ ФСТЭК России. Федеральная служба по техническому и экспортному контролю : официальный сайт. – Москва. – URL: https://fstec.ru// - Текст: электронный.Является федеральным органом исполнительной власти, осуществляющим межотраслевую координацию и функциональное регулирование деятельности по обеспечению защиты информации. https://fstec.ru/ Всероссийский научно-исследовательский институт автоматизации управления в непромышленной сфере имени В. В. Соломатина (ВНИИНС им. В.В. Соломатина) : официальный сайт. – Москва. – URL: http://www.vniins.ru/index.php?lang=%D0%A0%D1%83%D1%81. – Текст: электронный.ВНИИНС - это современное высокотехнологичное научно-производственное предприятие, занимающее ключевую позицию в развитии отечественной IT индустрии. Приоритетной задачей которого является создание отечественных информационных технологий, внедрение которых обеспечит технологическую независимость России от зарубежных производителей программного обеспечения. http://www.vniins.ru/index.php?lang=%D0%A0%D1%83%D1%81 InformationSecurity. Информационная безопасность : [сайт]. – Москва, 2019. – URL: http://www.itsec.ru/news. - Текст: электронный.Портал об информационной безопасности: новости, форум, программные новинки, архив изданий по информационной безопасности. http://www.itsec.ru/news Лаборатория Касперского : официальный сайт. – Москва, 2019. - . – URL: https://www.kaspersky.ru/. – Текст: электронный.Самый популярный в России и крупнейший в Европе производитель систем защиты от вирусов, спама и хакерских атак. Компания входит в четвёрку ведущих мировых производителей программных решений для обеспечения информационной безопасности. https://www.kaspersky.ru/

9. Методические указания для обучающихся по освоению дисциплины (модуля)

Вид работ	Методические рекомендации
лекции	В ходе лекционных занятий вести конспектирование учебного материала. Обращать внимание на категории, формулировки, раскрывающие суть тех или иных явлений и процессов, научные выводы и практические рекомендации, положительный опыт в ораторском искусстве. Желательно оставить в рабочих конспектах поля для пометок.
практические занятия	Работа на практических занятиях предполагает активное участие в дискуссиях. Важной формой самостоятельной работы обучающегося является систематическая и планомерная подготовка к практическому занятию. После лекции следует познакомиться с планом практических занятий и списком обязательной и дополнительной литературы, которую необходимо прочитать, изучить и законспектировать. Разъяснение по вопросам новой темы даются преподавателем в конце предыдущего практического занятия.
самостоятельная работа	САМОСТОЯТЕЛЬНАЯ РАБОТА требует, прежде всего, чтения рекомендуемых источников и монографических работ, их реферирования, подготовки докладов и сообщений. Важным этапом в самостоятельной работе является повторение материала по конспекту лекции. Одна из главных составляющих внеаудиторной подготовки - работа с книгой. Она предполагает: внимательное прочтение, критическое осмысление содержания, обоснование собственной позиции по дискуссионным моментам, постановки интересующих вопросов, которые могут стать предметом обсуждения на семинаре. При работе с терминами необходимо обращаться к словарям, в том числе доступным в Интернете.
Экзамен	При подготовке к ЭКЗАМЕНУ необходимо опираться, прежде всего, на лекции, а также на источники, которые разбирались на семинарах в течение семестра. В каждом билете на зачете содержится два вопроса. Ответ на экзамене предполагает полное и последовательное изложение изученного материала, а также демонстрацию способности и готовности применить полученные теоретические знания к предлагаемым практическим заданиям.

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

10.1. Перечень необходимого программного обеспечения

Название
Cisco Packet Tracer Свободная лицензия
Microsoft .NET Framework 4.7 Свободная лицензия
Microsoft Office Word 2010 Номер продукта 14.0.6024.1000 SP1 MSO 02260-018-0000106-48095
Антивирус kaspersky endpoint security Лицензионный договор от 17.02.2021 № 203-20122401
Операционная система Windows Договор от 26.05.2020 № 32009117096 Договор от 17.01.2019 № 31908696765

10.2. Перечень необходимых информационных справочных систем:

Каждый обучающийся в течение всего периода обучения обеспечен индивидуальным неограниченным доступом к электронно-библиотечным системам:

Название
Znanium.com. Базовая коллекция : электронно-библиотечная система : сайт / ООО 'Научно-издательский центр Инфра-М'. – Москва, 2011 - – URL: http://znanium.com/catalog (дата обновления: 06.06.2019). - Режим доступа: для зарегистрир. пользователей. – Текст: электронный. Фонд ЭБС формируется с учетом всех изменений образовательных стандартов и включает учебники, учебные пособия, УМК, монографии, авторефераты, диссертации, энциклопедии, словари и справочники, законодательно-нормативные документы, специальные периодические издания и издания, выпускаемые издательствами вузов. http://znanium.com/catalog/
IPRBooks. Базовая коллекция : электронно-библиотечная система : сайт / Общество с ограниченной ответственностью Компания 'Ай Пи Ар Медиа'. – Саратов, 2010 - . – URL: http://www.iprbookshop.ru/586.html - Режим доступа: для зарегистрир. пользователей. – Текст электронный. Является распространенным образовательным электронным ресурсом для высших и средних специальных учебных заведений, научно-исследовательских институтов, публичных библиотек, приобретающих корпоративный доступ для своих обучающихся, преподавателей и т.д. ЭБС включает учебную и научную литературу по направлениям подготовки высшего и среднего профессионального образования.ЭБС «Консультант студента». Коллекция Информационная безопасность : студенческая электронная библиотека : сайт / ООО «Политехресурс». Электронная библиотека технического вуза. – Москва, 2012. - . – URL: https://www.studentlibrary.ru/ru/catalogue/switch_kit/x2016-034.html - Режим доступа: для зарегистрир. пользователей. – Текст электронный.Является электронной библиотечной системой (ЭБС), предоставляющей доступ через сеть Интернет к учебной литературе и дополнительным материалам, приобретенным на основании прямых договоров с правообладателями. Полностью соответствует требованиям федеральных государственных образовательных стандартов третьего поколения (ФГОС ВО 3+) к комплектованию библиотек, в том числе электронных, в части формирования фондов основной и дополнительной литературы, для СПО, ВО и аспирантуры. http://www.iprbookshop.ru/586.html
Национальная электронная библиотека (НЭБ) : федеральная государственная информационная система : сайт / Министерство культуры Российской Федерации, Российская государственная библиотека. – Москва, 2004 - – URL: https://нэб.рф/. - Режим доступа: для зарегистрир. пользователей. – Текст: электронный. НЭБ - проект Российской государственной библиотеки. Начиная с 2004 г. Проект Национальная электронная библиотека (НЭБ) разрабатывается ведущими российскими библиотеками при поддержке Министерства культуры Российской Федерации. Основная цель НЭБ - обеспечить свободный доступ гражданам Российской Федерации ко всем изданным, издаваемым и хранящимся в фондах российских библиотек изданиям и научным работам, – от книжных памятников истории и культуры, до новейших авторских произведений. В настоящее время проект НЭБ включает более 1.660.000 электронных книг, более 33.000.000 записей каталогов.РОССИЙСКАЯ НАЦИОНАЛЬНАЯ БИБЛИОТЕКА (РНБ) : сайт / Российская национальная библиотека. - Москва : РНБ, 1998. - URL: http://nlr.ru/. – Режим доступа: для зарегистрир. пользователей. – Текст: электронный. '... одна из крупнейших в мире и вторая по величине фондов в Российской Федерации – служит российской культуре и науке, хранит национальную память, способствует просвещению населяющих Россию народов и распространению идей гуманизма. ... В фондах Библиотеки хранится более 38,6 млн экз. произведений печати и иных информационных ресурсов, в том числе и на электронных носителях, доступных широкому кругу пользователей. Ежегодно РНБ посещает около 850 тыс. читателей, которым выдается до 5 млн изданий, к ее электронным ресурсам обращаются за год свыше 10 млн удаленных пользователей. ... Сохраняя культурную и историческую преемственность, верность библиотечным традициям, заложенным еще в Императорской Публичной библиотеке, РНБ сегодня — современное информационное учреждение, оснащенное новейшим оборудованием и своевременно отвечающее на насущные вызовы времени.' (цитата с сайта РНБ: http://nlr.ru/nlr_visit/RA1162/rnb-today) https://нэб.рф/
Периодические издания доступные обучающимся и сотрудникам ФГБОУ ВО МГТУ по подписке и на основании контрактов и лицензионных соглашений. /index.php/resursy/37-periodicheskie-izdaniya
ФСТЭК России. Федеральная служба по техническому и экспортному контролю : официальный сайт. – Москва. – URL: https://fstec.ru// - Текст: электронный.Является федеральным органом исполнительной власти, осуществляющим межотраслевую координацию и функциональное регулирование деятельности по обеспечению защиты информации. https://fstec.ru/
Всероссийский научно-исследовательский институт автоматизации управления в непромышленной сфере имени В.

Название
В. Соломатина (ВНИИНС им. В.В. Соломатина) : официальный сайт. – Москва. – URL: http://www.vniins.ru/index.php?lang=%D0%A0%D1%83%D1%81. – Текст: электронный.ВНИИНС - это современное высокотехнологичное научно-производственное предприятие, занимающее ключевую позицию в развитии отечественной IT индустрии. Приоритетной задачей которого является создание отечественных информационных технологий, внедрение которых обеспечит технологическую независимость России от зарубежных производителей программного обеспечения. http://www.vniins.ru/index.php?lang=%D0%A0%D1%83%D1%81
Лаборатория Касперского : официальный сайт. – Москва, 2019. - . – URL: https://www.kaspersky.ru/. – Текст: электронный.Самый популярный в России и крупнейший в Европе производитель систем защиты от вирусов, спама и хакерских атак. Компания входит в четвёрку ведущих мировых производителей программных решений для обеспечения информационной безопасности. https://www.kaspersky.ru/
CYBERLENINKA : научная электронная библиотека : сайт. – Москва, 2014. - . – URL: https://cyberleninka.ru// - Режим доступа: для зарегистрир. пользователей. – Текст: электронный. КиберЛенинка - это научная электронная библиотека, построенная на парадигме открытой науки (Open Science), основными задачами которой является популяризация науки и научной деятельности, общественный контроль качества научных публикаций, развитие междисциплинарных исследований, современного института научной рецензии, повышение цитируемости российской науки и построение инфраструктуры знаний. https://cyberleninka.ru/
eLIBRARY.RU. : научная электронная библиотека : сайт. – Москва, 2000. - . – URL: https://elibrary.ru/defaultx.asp. - Режим доступа: для зарегистрир. пользователей. – Текст: электронный. Платформа eLIBRARY.RU была создана в 1999 году по инициативе Российского фонда фундаментальных исследований для обеспечения российским ученым электронного доступа к ведущим иностранным научным изданиям. С 2005 года eLIBRARY.RU начала работу с русскоязычными публикациями и ныне является ведущей электронной библиотекой научной периодики на русском языке в мире. https://elibrary.ru/defaultx.asp

Для обучающихся обеспечен доступ (удаленный доступ) к следующим современным профессиональным базам данных, информационным справочным и поисковым системам:

Название
Znanium.com. Базовая коллекция : электронно-библиотечная система : сайт / ООО 'Научно-издательский центр Инфра-М'. – Москва, 2011 - – URL: http://znanium.com/catalog (дата обновления: 06.06.2019). - Режим доступа: для зарегистрир. пользователей. – Текст: электронный. Фонд ЭБС формируется с учетом всех изменений образовательных стандартов и включает учебники, учебные пособия, УМК, монографии, авторефераты, диссертации, энциклопедии, словари и справочники, законодательно-нормативные документы, специальные периодические издания и издания, выпускаемые издательствами вузов. http://znanium.com/catalog/
IPRBooks. Базовая коллекция : электронно-библиотечная система : сайт / Общество с ограниченной ответственностью Компания 'Ай Пи Ар Медиа'. – Саратов, 2010 - . – URL: http://www.iprbookshop.ru/586.html - Режим доступа: для зарегистрир. пользователей. – Текст электронный. Является распространенным образовательным электронным ресурсом для высших и средних специальных учебных заведений, научно-исследовательских институтов, публичных библиотек, приобретающих корпоративный доступ для своих обучающихся, преподавателей и т.д. ЭБС включает учебную и научную литературу по направлениям подготовки высшего и среднего профессионального образования.ЭБС «Консультант студента». Коллекция Информационная безопасность : студенческая электронная библиотека : сайт / ООО «Политехресурс». Электронная библиотека технического вуза. – Москва, 2012. - . – URL: https://www.studentlibrary.ru/ru/catalogue/switch_kit/x2016-034.html - Режим доступа: для зарегистрир. пользователей. – Текст электронный.Является электронной библиотечной системой (ЭБС), предоставляющей доступ через сеть Интернет к учебной литературе и дополнительным материалам, приобретенным на основании прямых договоров с правообладателями. Полностью соответствует требованиям федеральных государственных образовательных стандартов третьего поколения (ФГОС ВО 3+) к комплектованию библиотек, в том числе электронных, в части формирования фондов основной и дополнительной литературы, для СПО, ВО и аспирантуры. http://www.iprbookshop.ru/586.html
Национальная электронная библиотека (НЭБ) : федеральная государственная информационная система : сайт / Министерство культуры Российской Федерации, Российская государственная библиотека. – Москва, 2004 - – URL: https://нэб.рф/. - Режим доступа: для зарегистрир. пользователей. – Текст: электронный. НЭБ - проект Российской государственной библиотеки. Начиная с 2004 г. Проект Национальная электронная библиотека (НЭБ) разрабатывается ведущими российскими библиотеками при поддержке Министерства культуры Российской Федерации. Основная цель НЭБ - обеспечить свободный доступ гражданам Российской Федерации ко всем изданным, издаваемым и хранящимся в фондах российских библиотек изданиям и научным работам, – от книжных памятников истории и культуры, до новейших авторских произведений. В настоящее время проект НЭБ включает более 1.660.000 электронных книг, более 33.000.000 записей каталогов.РОССИЙСКАЯ НАЦИОНАЛЬНАЯ БИБЛИОТЕКА (РНБ) : сайт / Российская национальная библиотека. - Москва : РНБ, 1998. - URL: http://nlr.ru/. – Режим доступа: для зарегистрир. пользователей. – Текст: электронный. '... одна из крупнейших в мире и вторая по величине фондов в Российской Федерации – служит российской культуре и науке, хранит национальную память, способствует просвещению населяющих Россию народов и распространению идей гуманизма. ... В фондах Библиотеки хранится более 38,6 млн экз. произведений печати и иных информационных ресурсов, в том числе и на электронных носителях, доступных широкому кругу пользователей. Ежегодно РНБ посещает около 850 тыс. читателей, которым выдается до 5 млн изданий, к ее электронным ресурсам обращаются за год свыше 10 млн удаленных пользователей. ... Сохраняя культурную и историческую преемственность, верность библиотечным традициям, заложенным еще в Императорской Публичной библиотеке, РНБ сегодня — современное информационное учреждение, оснащенное новейшим оборудованием и своевременно отвечающее на насущные вызовы времени.' (цитата с сайта РНБ: http://nlr.ru/nlr_visit/RA1162/rnb-today) https://нэб.рф/
eLIBRARY.RU. : научная электронная библиотека : сайт. – Москва, 2000. - . – URL: https://elibrary.ru/defaultx.asp. -

Название
Режим доступа: для зарегистрир. пользователей. – Текст: электронный. Платформа eLIBRARY.RU была создана в 1999 году по инициативе Российского фонда фундаментальных исследований для обеспечения российским ученым электронного доступа к ведущим иностранным научным изданиям. С 2005 года eLIBRARY.RU начала работу с русскоязычными публикациями и ныне является ведущей электронной библиотекой научной периодики на русском языке в мире. https://elibrary.ru/defaultx.asp
CYBERLENINKA : научная электронная библиотека : сайт. – Москва, 2014. - . – URL: https://cyberleninka.ru// - Режим доступа: для зарегистрир. пользователей. – Текст: электронный. КиберЛенинка - это научная электронная библиотека, построенная на парадигме открытой науки (Open Science), основными задачами которой является популяризация науки и научной деятельности, общественный контроль качества научных публикаций, развитие междисциплинарных исследований, современного института научной рецензии, повышение цитируемости российской науки и построение инфраструктуры знаний. https://cyberleninka.ru/
Периодические издания доступные обучающимся и сотрудникам ФГБОУ ВО МГТУ по подписке и на основании контрактов и лицензионных соглашений. /index.php/resursy/37-periodicheskie-izdaniya
ФСТЭК России. Федеральная служба по техническому и экспортному контролю : официальный сайт. – Москва. – URL: https://fstec.ru// - Текст: электронный.Является федеральным органом исполнительной власти, осуществляющим межотраслевую координацию и функциональное регулирование деятельности по обеспечению защиты информации. https://fstec.ru/
Всероссийский научно-исследовательский институт автоматизации управления в непромышленной сфере имени В. В. Соломатина (ВНИИНС им. В.В. Соломатина) : официальный сайт. – Москва. – URL: http://www.vniins.ru/index.php?lang=%D0%A0%D1%83%D1%81. – Текст: электронный.ВНИИНС - это современное высокотехнологичное научно-производственное предприятие, занимающее ключевую позицию в развитии отечественной IT индустрии. Приоритетной задачей которого является создание отечественных информационных технологий, внедрение которых обеспечит технологическую независимость России от зарубежных производителей программного обеспечения. http://www.vniins.ru/index.php?lang=%D0%A0%D1%83%D1%81
Лаборатория Касперского : официальный сайт. – Москва, 2019. - . – URL: https://www.kaspersky.ru/. – Текст: электронный.Самый популярный в России и крупнейший в Европе производитель систем защиты от вирусов, спама и хакерских атак. Компания входит в четвёрку ведущих мировых производителей программных решений для обеспечения информационной безопасности. https://www.kaspersky.ru/
InformationSecurity. Информационная безопасность : [сайт]. – Москва, 2019. – URL: http://www.itsec.ru/news. - Текст: электронный.Портал об информационной безопасности: новости, форум, программные новинки, архив изданий по информационной безопасности. http://www.itsec.ru/news



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

Наименования специальных помещений и помещений для самостоятельной работы	Оснащенность специальных помещений и помещений для самостоятельной работы	Перечень лицензионного программного обеспечения. Реквизиты подтверждающего документа
Лаборатория проектирования информационных систем (3-3-2) 385000, Республика Адыгея, г. Майкоп, ул. Пушкина, дом № 177, Учебный корпус № 3	Компьютерное рабочее место (системный блок, монитор, клавиатура, мышь) – 13 шт.; маршрутизатор; IP камеры – 2 шт.	
Лаборатория компьютерных технологий и методов программирования; Лаборатория программного обеспечения и сопровождения компьютерных систем; Лаборатория вычислительной техники, архитектуры персонального компьютера и периферийных устройств; Лаборатория программирования и баз данных (3-3-10) 385000, Республика Адыгея, г. Майкоп, ул. Пушкина, дом № 177, Учебный корпус № 3	Компьютерное рабочее место (системный блок, монитор, клавиатура, мышь) – 16 шт.; маршрутизатор; IP камеры – 3 шт.; мультимедийное оборудование (проектор, экран)/14 комплектов компьютерных комплектующих для произведения сборки, разборки и сервисного обслуживания ПК и оргтехники; специализированная мебель для сервисного обслуживания ПК с заземлением и защитой от статического напряжения, программное обеспечение общего и профессионального назначения/программное обеспечение: Windows 10 Pro 64-bit (Лицензия : код продукта 00331-20070-64990-AA980); Windows 10 Pro 64-bit (Лицензия : код продукта 00331-20070-64990-AA980); 7-Zip – бесплатная; Microsoft Office-лицензионная; Kaspersky Lab-26FE-000451-5729CF81; K-Lite Codec Pack-бесплатная; Microsoft Analysis Services- бесплатная; Mozilla Firefox-бесплатная; Google Chrome-бесплатная; AdobeAcrobat 11.0 – бесплатная/автоматизированное рабочее место преподавателя; сервер в лаборатории (8-х ядерный процессор с частотой 3 ГГц, оперативная память объемом 16 Гб, жесткие диски общим объемом 1 Тб, программное обеспечение: WindowsServer 2012); проектор и экран; маркерная доска; программное обеспечение общего и профессионального назначения, в том числе включающее в себя следующее ПО: EclipseIDEforJavaEEDevelopers, .NETFrameworkJDK 8, Microsoft SQLServerExpressEdition, MicrosoftVisioProfessional, MicrosoftVisualStudio, MySQLInstallerforWindows, NetBeans, SQLServerManagementStudio, MicrosoftSQLServerJavaConnector, AndroidStudio, IntelliJIDEA.	