Документ подписан простой электронной подписью
Информация о владельце:
ФИО: Задорожная Людмила Ивановна
Должность: Проректор по учебной работе
Дата подписания: 03.10.2023 10:17:08
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.35 Организация системы обеспечения информационной безопасности**
по направлению подготовки	10.03.01 Информационная безопасность
по профилю подготовки (специализации)	Организация и технология защиты информации
квалификация (степень) выпускника	Бакалавр
форма обучения	Очная,
год начала подготовки	2023

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 06.09.2023	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:

12.09.2023	Подписано простой ЭП 12.09.2023	Чундышко Вячеслав Юрьевич
	(подпись)	(Ф.И.О.)

Согласовано:

Руководитель ОПОП
заведующий выпускающей кафедрой
по направлению подготовки (специальности)

12.09.2023	Подписано простой ЭП 12.09.2023	Чундышко Вячеслав Юрьевич
	(подпись)	(Ф.И.О.)

Согласовано:

НБ МГТУ

(название подразделения)

21.09.2023	Подписано простой ЭП 21.09.2023	И. Б. Берберьян
	(подпись)	(Ф.И.О.)

1. Цели и задачи учебной дисциплины (модуля)

Курс «Организация системы обеспечения информационной безопасности» ставит своей **целью** приобретение студентами знаний структуры, место и роль службы защиты информации в системе защиты информации; задачи и функции службы; структура и штаты службы; принципы, методы и технология управления службой; проектирование СЗИ.

Задача дисциплины:

определение места службы защиты информации в системе безопасности предприятия;

объяснение функций службы защиты информации;

обоснование оптимальной структуры и штатного состава службы защиты информации в зависимости от решаемых задач и выполняемых функций;

установление организационных основ и принципов деятельности службы защиты информации;

разрешение общих и специфических вопросов подбора, расстановки и обучения кадров, организации труда сотрудников службы защиты информации;

раскрытие принципов, методов и технологии управления службой защиты информации;

разрабатывать нормативные и методические документы по организации и функционированию службы защиты информации;

проектировать систему обеспечения ИБ.

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

Дисциплина входит в перечень курсов части дисциплин вариативной части. Она имеет логические и содержательно-методические связи с дисциплинами базовой и вариативной частей образовательного цикла «Организационное и правовое обеспечение информационной безопасности», «Техническая защита информации» и др.

Дисциплина основана на знаниях научных основ и закономерностей развития общества.

Промежуточная аттестация осуществляется в форме тестирования. Итоговая оценка успеваемости выставляется по результатам сдачи экзамена и учитывает оценки, получаемые обучающимися на промежуточных этапах аттестации.

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
ПК-4.1	Знает виды политик безопасности и их формирование, разработка профилей защиты и заданий по безопасности, решения о необходимости защиты информации, содержащейся в информационной системе
ПК-4.2	Умеет формировать политики безопасности, анализировать систему с целью определения необходимого уровня защищенности и доверия
ПК-4.3	Владеет навыками разработки руководящих документов по защите информации в организации
ПК-8.2	Умеет разрабатывать и реализовывать организационные меры, обеспечивающие эффективность системы защиты информации
ПК-8.3	Владеет навыками организации и сопровождения аттестации объектов вычислительной техники и выделенных (защищаемых) помещений на соответствие требованиям по защите информации



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	СР		
Курс 4	Сем. 8	1	20	20	0.35	41	**81.35**	3

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
8	Введение. Предмет, задачи и содержание курса. Значение и место курса в подготовке кадров.	1-2	2		2				4		Обсуждение докладов. Реферат.
8	Система обеспечения информационной безопасности.	3-4	2		2				4		Обсуждение докладов. Реферат.
8	Цели и задачи СБИ.	5-6	2		2				4		Обсуждение докладов. Реферат.
8	Функции службы защиты информации. Организация деятельности службы безопасности.	7-8	2		2				4		Обсуждение докладов. Реферат.
8	Организационные основы и принципы деятельности службы безопасности.	9-10	2		2				4		Обсуждение докладов. Реферат.
8	Пакет документов для службы безопасности.	11-12	2		2				4		Обсуждение докладов. Реферат.
8	Управление службой защиты информации. Методы управления.	13	2		2				4		Обсуждение докладов. Реферат.
8	Проектирование системы обеспечения информационной безопасности.	14	2		2				4		Обсуждение докладов. Реферат.
8	Создание комплексной системы (КСОИ).	15	2		2				4		Обсуждение докладов. Реферат.
8	Система информационной безопасности предприятия.	16	2		2		0.35		5		Обсуждение докладов. Реферат.
	ИТОГО:		**20**		**20**		**0.35**		**41**		

5.4. Содержание разделов дисциплины (модуля) «Организация системы обеспечения 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
8	Введение. Предмет, задачи и содержание курса. Значение и место курса в подготовке кадров.	2			Научная и учебная взаимосвязь курса и других дисциплин специальности. Структура курса. Распределение тем по видам аудиторных занятий. Формы проведения практических занятий. Формы проверки знаний. Анализ источников, научной и учебной литературы по курсу. Методика самостоятельной работы студентов. Знания и умения студентов, которые должны быть получены в результате изучения курса.	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; ПК-4.2; ПК-8.2; ПК-4.3; ПК-8.3;	Знать: особенности оформления рабочей технической документации, предъявляемые к ней требования. Уметь: оформлять рабочую техническую документацию с учетом действующих нормативных и методических документов в области информационной безопасности. Владеть: навыками работы с нормативными и методическими документами, регламентирующими процессы оформления технической документации в профессиональной сфере.	
8	Система обеспечения информационной безопасности.	2			Назначение службы защиты информации. Место службы защиты информации в системе безопасности предприятия. Служба защиты информации как составная часть системы защиты. Служба защиты информации как орган управления защитой информации. Служба защиты информации как координатор деятельности по	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; ПК-4.1; ПК-4.2; ПК-4.3; ПК-8.2; ПК-8.3;	Знать: особенности оформления рабочей технической документации, предъявляемые к ней требования. Уметь: оформлять рабочую техническую документацию с учетом действующих нормативных и методических документов в области информационной безопасности. Владеть:	

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
					обеспечению безопасности информации. Статус службы защиты информации в структуре предприятия.		навыками работы с нормативными и методическими документами, регламентирующими процессы оформления технической документации в профессиональной сфере.	
8	Цели и задачи СБИ.	2			Организационные задачи и функции службы защиты информации. Технологические задачи и функции службы защиты информации. Координационные задачи и функции службы защиты информации. Взаимосвязь и соотношение организационных, технологических и координационных задач и функций. Факторы, влияющие на определение задач и функций службы 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; ПК-4.1; ПК-4.2; ПК-4.3; ПК-8.2; ПК-8.3;	Знать: особенности оформления рабочей технической документации, предъявляемые к ней требования. Уметь: оформлять рабочую техническую документацию с учетом действующих нормативных и методических доку-ментов в области информационной безопасности. Владеть: навыками работы с нормативными и методическими документами, регламентирующими процессы оформления технической документации в профессиональной сфере.	
8	Функции службы защиты информации. Организация деятельности службы безопасности.	2			Общая структурная схема службы защиты информации. Подразделения службы защиты информации. Факторы, определяющие конкретную структуру службы защиты информации. Виды и типы организационных структур службы защиты информации. Централизованная и децентрализованная структуры службы	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; ПК-4.1; ПК-4.2; ПК-4.3; ПК-8.2; ПК-8.3;	Знать: особенности оформления рабочей технической документации, предъявляемые к ней требования. Уметь: оформлять рабочую техническую документацию с учетом действующих нормативных и методических доку-ментов в области информационной безопасности. Владеть:	

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 информации, условия, критерии, определяющие выбор структур. Должностной состав сотрудников службы защиты информации, его зависимость от характера выполняемых работ. Задачи, функции, права и ответственность заместителя (помощника) руководителя предприятия по безопасности в области защиты информации. Задачи, функции, права и ответственность руководителя службы защиты информации, его заместителей, руководителей подразделений службы защиты, функции сотрудников и уполномоченных службы защиты информации. Факторы, определяющие численность сотрудников службы защиты информации. Порядок создания службы защиты информации. Структура и содержание положения о службе защиты информации. Состав и содержание других нормативных документов, регламентирующих деятельность службы защиты информации.		навыками работы с нормативными и методическими документами, регламентирующими процессы оформления технической документации в профессиональной сфере.	
8	Организационные основы и принципы деятельности службы безопасности.	2			Общие и специфические требования, предъявляемые к сотрудникам службы защиты информации. Особенности подбора кадров. Методы	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-5.3; ПК-4.1; ПК-4.2; ПК-4.3; ПК-8.2; ПК-8.3;	Знать: особенности оформления рабочей технической документации, предъявляемые к ней требования. Уметь: оформлять рабочую	

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
					получения информации о кандидатурах на должности. Социально-психологические факторы, влияющие на расстановку кадров. Формы создания и способы поддержания необходимого микроклимата в коллективе. Формы повышения квалификации сотрудников. Подготовка кадрового резерва.		техническую документацию с учетом действующих нормативных и методических доку-ментов в области информационной безопасности. Владеть: навыками работы с нормативными и методическими документами, регламентирующими процессы оформления технической документации в профессиональной сфере.	
8	Пакет документов для службы безопасности.	2			Специфика деятельности сотрудников службы защиты информации. Распределение обязанностей между сотрудниками службы защиты информации. Обеспечение персональной ответственности за сохранность носителей информации. Структура и содержание должностных инструкций сотрудников службы защиты информации. Организация рабочих мест сотрудников службы защиты информации (рациональное размещение, оснащение оборудованием, техническими средствами). Обеспечение необходимых условий труда. Охрана труда. Культура труда. Карты организации трудового процесса.	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; ПК-4.1; ПК-4.2; ПК-4.3; ПК-8.2; ПК-8.3;	Знать: особенности оформления рабочей технической документации, предъявляемые к ней требования. Уметь: оформлять рабочую техническую документацию с учетом действующих нормативных и методических доку-ментов в области информационной безопасности. Владеть: навыками работы с нормативными и методическими документами, регламентирующими процессы оформления технической документации в профессиональной сфере.	
8	Управление службой защиты информации.	2			Основные принципы организации и	ОПК-2.3.2; ОПК-2.3.1; ОПК-2.3.3; ОПК-2.4.1;	Знать: особенности оформления рабочей	

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
	Методы управления.				деятельности службы защиты информации. Условия и факторы, влияющие на организацию работы службы защиты информации. Организация взаимодействия службы защиты информации и подразделений предприятия и соподчиненных внешних служб защиты информации.	ОПК-2.4.2; ОПК-2.4.3; ОПК-5.1; ОПК-5.2; ОПК-5.3; ПК-4.1; ПК-4.2; ПК-4.3; ПК-8.2; ПК-8.3;	технической документации, предъявляемые к ней требования. Уметь: оформлять рабочую техническую документацию с учетом действующих нормативных и методических доку-ментов в области информационной безопасности. Владеть: навыками работы с нормативными и методическими документами, регламентирующими процессы оформления технической документации в профессиональной сфере.	
8	Проектирование системы обеспечения информационной безопасности.	2			Принципы управления службой защиты информации. Понятие и сущность методов управления. Система методов управления. Адм инистративно-правовые методы управления. Экономические методы управления. Социально-психологические методы управления. Взаимосвязь методов управления. Необходимость комплексного и системного применения методов управления службой 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; ПК-4.1; ПК-4.2; ПК-4.3; ПК-8.2; ПК-8.3;	Знать: особенности оформления рабочей технической документации, предъявляемые к ней требования. Уметь: оформлять рабочую техническую документацию с учетом действующих нормативных и методических доку-ментов в области информационной безопасности. Владеть: навыками работы с нормативными и методическими документами, регламентирующими процессы оформления технической документации в профессиональной сфере.	
8	Создание комплексной системы (КСОИ).	2			Состав и содержание управленческих функций.	ОПК-2.3.1; ОПК-2.3.2; ОПК-2.3.3; ОПК-2.4.1;	Знать: особенности оформления рабочей	

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
					Технология управления службой защиты информации. Значение управленческих решений. Цели планирования. Виды планирования, их назначение. Содержание и структура планов. Технология планирования. Методы и формы контроля выполнения планов. Критерии эффективности службы защиты информации. Методы оценки качества службы защиты информации. Пути и способы повышения эффективности управления службой защиты информации. Задачи КСОИ Принципы создания КСОИ Этапы создания КСОИ	ОПК-2.4.2; ОПК-2.4.3; ОПК-5.1; ОПК-5.2; ОПК-5.3; ПК-4.1; ПК-4.2; ПК-4.3; ПК-8.2; ПК-8.3;	технической документации, предъявляемые к ней требования. Уметь: оформлять рабочую техническую документацию с учетом действующих нормативных и методических доку-ментов в области информационной безопасности. Владеть: навыками работы с нормативными и методическими документами, регламентирующими процессы оформления технической документации в профессиональной сфере.	
8	Система информационной безопасности предприятия.	2			Модель построения системы информационной безопасности. Определение границ исследования. Построение модели информационной технологии. Выбор контрмер. Оценка достигаемой защищенности. Методология анализа рисков. Построение профиля защиты. Формирование организационной политики безопасности. Формулирование целей безопасности объекта. Определение функциональных требований безопасности. Требования гарантии	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; ПК-4.1; ПК-4.2; ПК-4.3; ПК-8.2; ПК-8.3;	Знать: особенности оформления рабочей технической документации, предъявляемые к ней требования. Уметь: оформлять рабочую техническую документацию с учетом действующих нормативных и методических доку-ментов в области информационной безопасности. Владеть: навыками работы с нормативными и методическими документами, регламентирующими процессы оформления технической документации в	

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
					достигаемой защищенности. Формирование перечня требований. Оценка достигаемой защищенности.		профессиональной сфере.	
	ИТОГО:	**20**						

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
8	Введение. Предмет, задачи и содержание курса. Значение и место курса в подготовке кадров.	Научная и учебная взаимосвязь курса и других дисциплин специальности. Структура курса. Распределение тем по видам аудиторных занятий. Формы проведения практических занятий. Формы проверки знаний. Анализ источников, научной и учебной литературы по курсу. Методика самостоятельной работы студентов. Знания и умения студентов, которые должны быть получены в результате изучения курса.	2		
8	Система обеспечения информационной безопасности.	Назначение службы защиты информации. Место службы защиты информации в системе безопасности предприятия. Служба защиты информации как составная часть системы защиты. Служба защиты информации как орган управления защитой информации. Служба защиты информации как координатор деятельности по обеспечению безопасности информации. Статус службы защиты информации в структуре предприятия.	2		
8	Цели и задачи СБИ.	Организационные задачи и функции службы защиты информации. Технологические задачи и функции службы защиты информации. Координационные задачи и функции службы защиты информации. Взаимосвязь и соотношение организационных, технологических и координационных задач и функций. Факторы, влияющие на определение задач и функций службы защиты информации.	2		
8	Функции службы защиты информации. Организация деятельности службы безопасности.	Общая структурная схема службы защиты информации. Подразделения службы защиты информации. Факторы, определяющие конкретную структуру службы защиты информации. Виды и типы организационных структур службы защиты информации. Централизованная и децентрализованная структуры службы защиты информации, условия, критерии, определяющие выбор структур. Должностной состав сотрудников службы защиты информации, его зависимость от характера выполняемых работ. Задачи, функции, права и ответственность заместителя (помощника) руководителя предприятия по безопасности в области защиты информации. Задачи, функции, права и ответственность руководителя службы защиты информации, его заместителей, руководителей подразделений службы защиты, функции сотрудников и уполномоченных службы защиты информации. Факторы, определяющие численность сотрудников службы защиты информации. Порядок создания службы защиты информации. Структура и содержание положения о службе защиты информации. Состав и содержание других нормативных документов, регламентирующих деятельность службы защиты информации.	2		
8	Организационные основы и принципы деятельности службы безопасности.	Основные принципы организации и деятельности службы защиты информации. Условия и факторы, влияющие на организацию работы службы защиты информации. Организация взаимодействия службы защиты информации и подразделений предприятия и соподчиненных внешних служб защиты информации.	2		
8	Пакет документов для службы безопасности.	Общие и специфические требования, предъявляемые к сотрудникам службы защиты информации. Особенности подбора кадров. Методы получения информации о кандидатурах на должности. Социально-психологические факторы, влияющие на расстановку кадров. Формы создания и способы поддержания необходимого микроклимата в коллективе. Формы повышения квалификации сотрудников. Подготовка кадрового резерва.	2		
8	Управление службой защиты информации. Методы управления.	Специфика деятельности сотрудников службы защиты информации. Распределение обязанностей между сотрудниками службы защиты информации. Обеспечение персональной ответственности за сохранность носителей информации. Структура и	2		

Сем	№ раздела дисциплины	Наименование практических занятий	Объем в часах		
			ОФО	ЗФО	ОЗФО
1	2	3	4	5	6
		содержание должностных инструкций сотрудников службы защиты информации. Организация рабочих мест сотрудников службы защиты информации (рациональное размещение, оснащение оборудованием, техническими средствами). Обеспечение необходимых условий труда. Охрана труда. Культура труда. Карты организации трудового процесса.			
8	Проектирование системы обеспечения информационной безопасности.	Принципы управления службой защиты информации. Понятие и сущность методов управления. Система методов управления. Административно-правовые методы управления. Экономические методы управления. Социально-психологические методы управления. Взаимосвязь методов управления. Необходимость комплексного и системного применения методов управления службой защиты информации.	2		
8	Создание комплексной системы (КСОИ).	остав и содержание управленческих функций. Технология управления службой защиты информации. Значение управленческих решений. Цели планирования. Виды планирования, их назначение. Содержание и структура планов. Технология планирования. Методы и формы контроля выполнения планов. Критерии эффективности службы защиты информации. Методы оценки качества службы защиты информации. Пути и способы повышения эффективности управления службой защиты информации.Задачи КСОИ.Принципы создания КСОИ.Этапы создания КСОИ.	2		
8	Система информационной безопасности предприятия.	Модель построения системы информационной безопасности.Определение границ исследования.Построение модели информационной технологии.Выбор контрмер.Оценка достигаемой защищенности.Методология анализа рисков.Построение профиля защиты.Формирование организационной политики безопасности.Формулирование целей безопасности объекта.Определение функциональных требований безопасности.Требования гарантии достигаемой защищенности.Формирование перечня требований.Оценка достигаемой защищенности.	2		
	ИТОГО:		**20**		

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)

нет

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
8	Введение. Предмет, задачи и содержание курса. Значение и место курса в подготовке кадров.	Составление плана-конспекта. Написание реферата.	1-2	4		
8	Система обеспечения информационной безопасности.	Составление плана-конспекта. Написание реферата.	3-4	4		
8	Цели и задачи СБИ.	Составление плана-конспекта. Написание реферата.	5-6	4		
8	Функции службы защиты информации. Организация деятельности службы безопасности.	Составление плана-конспекта. Написание реферата.	7-8	4		
8	Организационные основы и принципы деятельности службы безопасности.	Составление плана-конспекта. Написание реферата.	9-10	4		
8	Пакет документов для службы безопасности.	Составление плана-конспекта. Написание реферата.	11-12	4		
8	Управление службой защиты информации. Методы управления.	Составление плана-конспекта. Написание реферата.	13	4		
8	Проектирование системы обеспечения информационной безопасности.	Составление плана-конспекта. Написание реферата.	14	4		
8	Создание комплексной системы (КСОИ).	Составление плана-конспекта. Написание реферата.	15	4		
8	Система информационной безопасности предприятия.	Составление плана-конспекта. Написание реферата.	16	5		
	ИТОГО:			**41**		

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
Довгаль, В.А. (Майкопский государственный технологический университет). Системы защиты информации в ведущих зарубежных странах : учеб. пособие / В.А. Довгаль ; М-во образования и науки РФ, ГОУ ВПО Майкоп. гос. технол. ун-т. - Майкоп : МГТУ, 2010. - 112 с.	http://lib.mkgtu.ru:8002/libdata.php?id=2000014830&DOK=021165&BASE=000530

6.2. Литература для самостоятельной работ

Название	Ссылка
Филиппов, Б.И. Информационная безопасность. Основы надежности средств связи [Электронный ресурс]: учебник / Б.И. Филиппов, О.Г. Шерстнева. - Сара-тов: Ай Пи Эр Медиа, 2019. - 227 с. - ЭБС «IPRbooks»	http://www.iprbookshop.ru/80290.html
Баранова, Е.К. Информационная безопасность и защита информации [Электронный ресурс]: учебное пособие / Баранова Е.К., Бабаш А.В. - М.: РИОР, ИНФРА-М, 2019. - 322 с. - ЭБС «Znanium.com»	http://znanium.com/catalog/product/1009606
Сычев, Ю.Н. Стандарты информационной безопасности. Защита и обработка конфиденциальных документов [Электронный ресурс]: учебное пособие / Ю.Н. Сычев. - Саратов: Вузовское образование, 2018. - 195 с. - ЭБС «IPRbooks»	http://www.iprbookshop.ru/72345.html
Глотина, И.М. Средства безопасности операционной системы Windows Server 2008 [Электронный ресурс]: учебно-методическое пособие / И.М. Глотина. - Са-ратов: Вузовское образование, 2018. - 141 с. - ЭБС «IPRbooks»	http://www.iprbookshop.ru/72538.html
Фороузан, Б. А. Криптография и безопасность сетей [Электронный ресурс]: учебное пособие / Б.А. Фороузан. - Москва, Саратов: Интернет-Университет Информационных Технологий (ИНТУИТ), Вузовское образование, 2017. - 782 с. - ЭБС «IPRbooks»	http://www.iprbookshop.ru/72337.html

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
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			
3			Документоведение и документооборот
6			Основы управленческой деятельности
5			Организационное и правовое обеспечение информационной безопасности
7			Основы управления информационной безопасностью
8			Комплексное обеспечение защиты информации объекта информатизации
7			Нормативные акты и стандарты по информационной безопасности
8			Организация системы обеспечения информационной безопасности
67			Научно-исследовательская работа по организации и технологии защиты информации
1			Введение в специальность
8			Защита интеллектуальной собственности и патентоведение
8			Авторское право
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			
3			Документоведение и документооборот
6			Основы управленческой деятельности
5			Организационное и правовое обеспечение информационной безопасности
7			Основы управления информационной безопасностью
8			Комплексное обеспечение защиты информации объекта информатизации
7			Нормативные акты и стандарты по информационной безопасности
8			Организация системы обеспечения информационной безопасности
1			Введение в специальность
8			Защита интеллектуальной

Этапы формирования компетенции (номер семестр согласного учебному плану)			Наименование учебных дисциплин, формирующие компетенции в процессе освоения образовательной программы
ОФО	ЗФО	ОЗФО	
			собственности и патентоведение
8			Авторское право
ОПК-5.3 Владеет навыками разрабатывать локальные правовые документы, регламентирующие работу по обеспечению информационной безопасности в организации			
3			Документоведение и документооборот
6			Основы управленческой деятельности
5			Организационное и правовое обеспечение информационной безопасности
7			Основы управления информационной безопасностью
8			Комплексное обеспечение защиты информации объекта информатизации
7			Нормативные акты и стандарты по информационной безопасности
8			Организация системы обеспечения информационной безопасности
67			Научно-исследовательская работа по организации и технологии защиты информации
1			Введение в специальность
8			Защита интеллектуальной собственности и патентоведение
8			Авторское право
ПК-4.1 Знает виды политик безопасности и их формирование, разработка профилей защиты и заданий по безопасности, решения о необходимости защиты информации, содержащейся в информационной системе			
7			Основы управления информационной безопасностью
8			Комплексное обеспечение защиты информации объекта информатизации
8			Организация системы обеспечения информационной безопасности
34			Модуль получения квалификации "Администратор информационной безопасности вычислительной сети"
4			Администрирование безопасности в операционных системах
3			Защита и обработка конфиденциальных документов
3			Защита информации в сети Интернет
ПК-4.2 Умеет формировать политики безопасности, анализировать систему с целью определения необходимого уровня защищенности и доверия			
7			Основы управления информационной безопасностью
8			Комплексное обеспечение

Этапы формирования компетенции (номер семестр согласного учебному плану)			Наименование учебных дисциплин, формирующие компетенции в процессе освоения образовательной программы
ОФО	ЗФО	ОЗФО	
			защиты информации объекта информатизации
8			Организация системы обеспечения информационной безопасности
34			Модуль получения квалификации "Администратор информационной безопасности вычислительной сети"
4			Администрирование безопасности в операционных системах
3			Защита и обработка конфиденциальных документов
3			Защита информации в сети Интернет
ПК-4.3 Владеет навыками разработки руководящих документов по защите информации в организации			
7			Основы управления информационной безопасностью
8			Комплексное обеспечение защиты информации объекта информатизации
8			Организация системы обеспечения информационной безопасности
34			Модуль получения квалификации "Администратор информационной безопасности вычислительной сети"
4			Администрирование безопасности в операционных системах
3			Защита и обработка конфиденциальных документов
3			Защита информации в сети Интернет
ПК-8.2 Умеет разрабатывать и реализовывать организационные меры, обеспечивающие эффективность системы защиты информации			
5			Организационное и правовое обеспечение информационной безопасности
7			Основы управления информационной безопасностью
8			Комплексное обеспечение защиты информации объекта информатизации
8			Организация системы обеспечения информационной безопасности
ПК-8.3 Владеет навыками организации и сопровождения аттестации объектов вычислительной техники и выделенных (защищаемых) помещений на соответствие требованиям по защите информации			
7			Основы управления информационной безопасностью
8			Комплексное обеспечение защиты информации

Этапы формирования компетенции (номер семестр согласного учебному плану)			Наименование учебных дисциплин, формирующие компетенции в процессе освоения образовательной программы
ОФО	ЗФО	ОЗФО	
			объекта информатизации
7			Нормативные акты и стандарты по информационной безопасности
8			Организация системы обеспечения информационной безопасности

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
ПК-4: Способен участвовать в работах по реализации политики информационной безопасности, применять комплексный подход к обеспечению информационной безопасности объекта защиты					
ПК-4.2 Умеет формировать политики безопасности, анализировать систему с целью определения необходимого уровня защищенности и доверия					
Знать:	Фрагментарные знания	Неполные знания	Сформированные, но содержащие отдельные пробелы знания	Сформированные систематические знания	
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-4: Способен участвовать в работах по реализации политики информационной безопасности, применять комплексный подход к обеспечению информационной безопасности объекта защиты					
ПК-4.3 Владеет навыками разработки руководящих документов по защите информации в организации					
Знать:	Фрагментарные знания	Неполные знания	Сформированные, но содержащие отдельные пробелы знания	Сформированные систематические знания	
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-4: Способен участвовать в работах по реализации политики информационной безопасности, применять комплексный подход к обеспечению информационной безопасности объекта защиты					
ПК-4.1 Знает виды политик безопасности и их формирование, разработка профилей защиты и заданий по безопасности, решения о необходимости защиты информации, содержащейся в информационной системе					
Знать:	Фрагментарные знания	Неполные знания	Сформированные, но содержащие отдельные пробелы знания	Сформированные систематические знания	
Уметь:	Частичные умения	Неполные умения	Умения полные, допускаются небольшие ошибки	Сформированные умения	
Владеть:	Частичное владение навыками	Несистематическое применение навыков	В систематическом применении	Успешное и систематическое применение	

Планируемые результаты освоения компетенции	Критерии оценивания результатов обучения				Наименование оценочного средства
	неудовлетворительно	удовлетворительно	хорошо	отлично	
1	2	3	4	5	6
			навыков допускаются пробелы	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-2.3.1 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	
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	
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-8.3 Владеет навыками организации и сопровождения аттестации объектов вычислительной техники и выделенных (защищаемых) помещений на соответствие требованиям по защите информации					
Знать:	Фрагментарные знания	Неполные знания	Сформированные, но содержащие отдельные пробелы знания	Сформированные систематические знания	
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-5.3 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	
Уметь:	Частичные умения	Неполные умения	Умения полные, допускаются небольшие	Сформированные умения	

Планируемые результаты освоения компетенции	Критерии оценивания результатов обучения				Наименование оценочного средства
	неудовлетворительно	удовлетворительно	хорошо	отлично	
1	2	3	4	5	6
			ошибки		
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-5.1 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	
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	
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	
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	Неполные знания	Сформированные,	Сформированные	

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	
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-2.4.2 Умеет осуществлять контроль обеспечения уровня защищенности объектов информатизации					
Знать:	Фрагментарные знания	Неполные знания	Сформированные, но содержащие отдельные пробелы знания	Сформированные систематические знания	
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	
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	
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.Место и роль службы защиты информации в системе защиты информации.

2.Задачи и функции службы защиты информации.

3.Структура и штаты службы защиты информации.

4.Организационные основы и принципы деятельности службы защиты информации.

5.Подбор, расстановка и обучение сотрудников службы защиты информации.

6.Организация труда сотрудников службы защиты информации.

7.Принципы и методы управления службой защиты информации.

8.Технология управления службой защиты информации.

Темы докладов

1.Виды угроз информационным ресурсам – по возрастанию степени их опасности

2.Задача обеспечения информационной безопасности

3.Безопасность при выборе персонала и работе с ним

4.Подготовка и переподготовка пользователей и специалистов по защите информации.

5.Реагирование на нарушения информационной безопасности.

6.Набор и отбор персонала в службу ЗИ, методы

7.Отбор, критерии отбора

8.Требования к специалистам по защите информации

9.Обучение работников службы ЗИ, цели

10.Принципы управления службой ЗИ

11.Основные цели деятельности службы ЗИ

12.Линейная структура организации

13.Линейно-штабная структура организации

14.Методы управления службой ЗИ

15.Структура процесса управления в самом общем виде

16.Функции процессов управления, 4 типовых функции:

17.Виды обеспечения деятельности службы ЗИ

18.Положение о службе ЗИ (основные положения, их содержание)

19.Документы для объекта информатизации

20.Общие документы для объекта органа управления

21.Структура и содержание должностной инструкции сотрудника СЗИ

22.Порядок обеспечения персональной ответственности за сохранность носителей информации

Тестовые задания для определения остаточных знаний

1. Под системой безопасности предприятия в настоящее время понимается -

1. организованная совокупность специальных органов, служб, средств, методов и мероприятий, обеспечивающих защиту жизненно важных интересов личности, предприятия и государства от внутренних и внешних угроз

2.организованная совокупность специальных органов, обеспечивающих защиту жизненно важных интересов личности, предприятия и государства от внутренних и внешних угроз

3.охранно-пожарная сигнализация

4.любая система, гарантирующая безопасность персонала

2. Целями системы безопасности являются:

1.защита прав предприятия, его структурных подразделений и сотрудников

2.сохранение и эффективное использование финансовых, материальных и информационных ресурсов

3.повышение имиджа и роста прибылей за счет обеспечения качества услуг и безопасности клиентов

4.пугать прохожих

3. Кому подчиняется подразделение ЗИ?

1. Руководителю организации

2.Главному бухгалтеру

3.Никому

4.Всем

4. Для достижения целей и задач системы безопасности, используются различные средства обеспечения безопасности предприятия, среди которых можно выделить следующие:

1.Технические средства

2.Организационные средства

3.Информационные средства

4.Забавные средства

5. Какие бывают виды проверки?

1.Плановая

2.Интенсивная

3.Внезапная

4.Нежданная

6. Какие основные принципы, которые следует учитывать при построении систем безопасности:

1.Комплексность

2.Своевременность

3.Непрерывность

4.Неторопливость

7. Какие основные принципы, которые следует учитывать при построении систем безопасности:

1.Активность

2.Законность

3.Резвость

4.Прозрачность

8. Могут ли быть включены в должностные инструкции действия, не относящиеся к компетенции отдела?

1.нет

2.да

3.иногда

4.с разрешения руководителя

9. Какие основные принципы, которые следует учитывать при построении систем безопасности:

1.Совершенствование

2.Централизация управления

3.Безобразность поведения

4.Сверхсовершенствование

10. Система управления СБП может быть рассмотрена с позиции общего подхода к построению социальных организационных систем. В этом случае выделяется три вида управленческой деятельности:

1.Стратегическое управление

2.Текущее (календарное) управление

3.Оперативное регулирование (руководство)

4.Внешнее управление (антикризисное руководство)

Контрольные тесты для проведения промежуточной аттестации

1. С какого момента начинается процесс управления рисками:

Оценки рисков

Мониторинга

Анализа угроз

Обработки рисков

2 .Основные задачи СЗИ:

Изучение аналитических материалов

Контроль проводимых аукционов

Обеспечение шифровальной связью

Обеспечение бесперебойной работы автоматизированных систем

Разработка организационно-распорядительных документов

3. Структура СЗИ формируется по следующим направлениям:

Администрирование безопасности ЛВС

Администрирование безопасности БД

Прослушивание сотрудников организации

Установление слежения за сотрудниками организации

Эксплуатация абонентского пункта специальной связи

Комплексная защита информации

4. Какой документ определяет, сколько сотрудников организации должны иметь допуск к секретной информации:

Должностной регламент

Специальный приказ руководителя организации

Номенклатура должностей

5. К какой категории мер противодействия угрозам ИБ относится использование систем видеонаблюдения:

Физической

Технологической

Технической

Организационной

6.Какие из нижеперечисленных сведений нуждаются в защите:

Аналитические материалы

Домашние адреса сотрудников

Контактные телефоны организации

История достижений

Планы модернизации

7.Какое из ниже перечисленных направлений не относятся к структуре СЗИ:

Комплексная защита информации

Мониторинг телефонных разговоров с санкции ФСБ

Эксплуатация абонентского пункта специальной связи

Администрирование ЛВС

Администрирование безопасности БД

8.Виды угроз безопасности:

Комплексный

Внешний

Уголовный

Административный

Внутренний

9.Какой тип угроз представляет наибольшую опасность с точки зрения ИБ:

Умышленные искусственные угрозы

Умышленные естественные угрозы

Неумышленные естественные угрозы

Администрирование безопасности БД

10. Какой канал утечки конфиденциальной информации представляет наибольшую опасность:

Внешние носители информации

Системы мгновенных сообщений

Документы, отправляемые на печать

Чтение информации с экрана

11.Какие из перечисленных ниже событий являются инцидентами информационной безопасности:

Удаление документа

Плановая перезагрузка компьютера

Проведение финансовой транзакции через Интернет

Получение сообщения от неизвестного отправителя

Сообщение об ошибке в программе

12.К какому типу Интернет - угроз относятся массовые рассылки сообщений с целью получения конфиденциальной информации:

Спам

Фишинг

Вирусы

Программы-шпионы

13. Основные угрозы доступности информации:

непреднамеренные ошибки пользователей

злонамеренное изменение данных

хакерская атака

отказ программного и аппаратного обеспечения

разрушение или повреждение помещений

перехват данных

14. К формам защиты информации не относятся:

аналитическая

правовая

организационно-техническая

страховая

15. Информация, составляющая государственную тайну, не может иметь гриф…:

«для служебного пользования»

«секретно»

«совершенно секретно»

«особой важности»

16. Утечка информации – это…:

Несанкционированный процесс переноса информации от источника к злоумышленнику

Процесс раскрытия секретной информации

Процесс уничтожения информации

Непреднамеренная утрата носителя информации

17. Вид угрозы действия, направленного на несанкционированное использование информационных ресурсов, не оказывающего при этом влияния на её функционирование - угроза:

активная

пассивная

18. Разглашение информации – это…:

умышленное действие с конфиденциальными сведениями приведшее к ознакомлению с ними лиц не допущенных к ним

бесконтрольный выход конфиденциальной информации за пределы организации или круга лиц, которым она была доверена

противоправное преднамеренное овладение конфиденциальной информацией

Непреднамеренная утрата носителя информации

20. Какую опасность могут представлять файлы «cookie»:

Заражение вредоносным кодом

Отказ в обслуживании

Отслеживание посещений сайтов

Перегрузка каналов связи

21. Форматирование носителя гарантирует полное удаление записанной на него информации:

Да

Нет

22. Что называют источником конфиденциальной информации:

объект, обладающий определенными охраняемыми сведениями, представляющими интерес для злоумышленников

сведения о предметах, объектах, явлениях и процессах, отображаемые на каком-либо носителе

доступ к информации, нарушающий правила разграничения доступа с использованием штатных средств, предоставляемых средствами вычислительной техники

это защищаемые предприятием сведения в области производства и коммерческой деятельности

способ, позволяющий нарушителю получить доступ к обрабатываемой или хранящейся в ПЭВМ информации

Примерный перечень вопросов к экзамену по дисциплине

1. Определение и виды опасностей

2. Определение и виды угроз

3. Цели системы безопасности

4. Основные задачи системы безопасности предприятия

5. Средства обеспечения безопасности предприятия

6. Определение информационной безопасности

7. Компоненты (источники, объекты, действия) учитываемые при построении модели информационной безопасности предприятия.

8. Наиболее важные компоненты (источники, объекты, действия) модели информационной безопасности предприятия

9. Что является объектом угроз информационной безопасности

10. Что выступает в качестве источников угроз ИБ

11. Разглашение

12. Утечка

13. Несанкционированный доступ

14. Классификация угроз по признакам:

15. Основные принципы, которые следует учитывать при построении систем безопасности

16. Три вида управленческой деятельности

17. Понятие организационного проектированием

18. Три основные задачи организационного проектирование

19. Виды связей управления в организациях

20. За что отвечает служба защиты информации

21. Дополнительные обязанности, возлагаемые при необходимости на службу защиты информации

22. Основные требования, учитываемые при создании СЗИ на предприятии

23. Кто может входить в структуру службы ЗИ

24. Сотрудник группы безопасности, его обязанности

25. Администратор безопасности системы, его обязанности

26. Администратор безопасности данных, его обязанности

27. Руководитель группы, его обязанности

28. Перечень основных организационно-технических мероприятий, выполняемых СЗИ:



29. Мероприятия, осуществляемые начальником отдела защиты информации

30. Перечислите виды деятельности, выполняемые службой ЗИ

31. Кто должен входить в состав службы ЗИ?

32. Назовите перечень основных организационных технических мероприятий, выполняемых сотрудниками службы ЗИ.

33. Назовите основные обязанности начальника службы ЗИ.

34. Что должен выполнять сотрудник службы ЗИ?

35. На примере должностной инструкции инженера по защите информации опишите четыре обязательных раздела подобных документов.

36. Что должен знать инженер по защите информации

37. виды конфиденциальной информации

38. Что относится к мерам по обеспечению надежности персонала

39. Виды угроз информационным ресурсам – по возрастанию степени их опасности

40. Задача обеспечения информационной безопасности

41. Безопасность при выборе персонала и работе с ним

42. Подготовка и переподготовка пользователей и специалистов по защите информации.

43. Реагирование на нарушения информационной безопасности.

44. Набор и отбор персонала в службу ЗИ, методы

45. Отбор, критерии отбора

46. Требования к специалистам по защите информации

47. Обучение работников службы ЗИ, цели

48. Принципы управления службой ЗИ

49. Основные цели деятельности службы ЗИ

50 Линейная структура организации

51. Линейно-штабная структура организации

52. Методы управления службой ЗИ

53. Структура процесса управления в самом общем виде

54. Функции процессов управления, 4 типовых функции:

55. Виды обеспечения деятельности службы ЗИ

56. Положение о службе ЗИ(основные положения, их содержание)

57. Документы для объекта информатизации

58. Общие документы для объекта органа управления

59. Структура и содержание должностной инструкции сотрудника СЗИ

60. Порядок обеспечения персональной ответственности за сохранность носителей информации

61. Задачи КСОИ

62. Принципы создания КСОИ

63. Этапы создания КСОИ

64. Модель построения системы информационной безопасности.

65. Определение границ исследования.

66. Построение модели информационной технологии.

67. Выбор контрмер.

68. Оценка достигаемой защищенности.

69. Методология анализа рисков.

70. Построение профиля защиты.

71. Формирование организационной политики безопасности.

72. Формулирование целей безопасности объекта.

73. Определение функциональных требований безопасности.

74. Требования гарантии достигаемой защищенности.

75. Формирование перечня требований.

76. Оценка достигаемой защищенности.

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

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

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 «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 «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.

Экзаменатор может проставить экзамен без опроса или собеседования тем студентам, которые активно участвовали в семинарских занятиях.

Экзаменационные билеты (вопросы) утверждаются на заседании кафедры и подписываются заведующим кафедрой. В билете должно содержаться не более трех вопросов. Комплект экзаменационных билетов по дисциплине должен содержать15—20 билетов.

Экзамен может проводиться в форме устного опроса по билетам (вопросам) или без билетов, с предварительной подготовкой ил и без подготовки, по усмотрению преподавателя. Экзаменатор вправе задавать вопросы сверх билета, а также, помимо теоретических вопросов, давать задачи по программе данного курса.





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

8.1. Основная литература

Название	Ссылка
Филиппов, Б.И. Информационная безопасность. Основы надежности средств связи [Электронный ресурс]: учебник / Б.И. Филиппов, О.Г. Шерстнева. - Сара-тов: Ай Пи Эр Медиа, 2019. - 227 с. - ЭБС «IPRbooks»	http://www.iprbookshop.ru/80290.html
Баранова, Е.К. Информационная безопасность и защита информации [Электронный ресурс]: учебное пособие / Баранова Е.К., Бабаш А.В. - М.: РИОР, ИНФРА-М, 2019. - 322 с. - ЭБС «Znanium.com»	http://znanium.com/catalog/product/1009606

8.2. Дополнительная литература

Название	Ссылка
Сычев, Ю.Н. Стандарты информационной безопасности. Защита и обработка конфиденциальных документов [Электронный ресурс]: учебное пособие / Ю.Н. Сычев. - Саратов: Вузовское образование, 2018. - 195 с. - ЭБС «IPRbooks»	http://www.iprbookshop.ru/72345.html
Глотина, И.М. Средства безопасности операционной системы Windows Server 2008 [Электронный ресурс]: учебно-методическое пособие / И.М. Глотина. - Са-ратов: Вузовское образование, 2018. - 141 с. - ЭБС «IPRbooks»	http://www.iprbookshop.ru/72538.html
Фороузан, Б. А. Криптография и безопасность сетей [Электронный ресурс]: учебное пособие / Б.А. Фороузан. - Москва, Саратов: Интернет-Университет Информационных Технологий (ИНТУИТ), Вузовское образование, 2017. - 782 с. - ЭБС «IPRbooks»	http://www.iprbookshop.ru/72337.html
Лапонина, О.Р. Основы сетевой безопасности. Криптографические алгоритмы и протоколы взаимодействия [Электронный ресурс]: учебное пособие / О.Р. Лапонина. - М.: Интернет-Университет Информационных Технологий (ИНТУИТ), 2016. - 242 с. - ЭБС «IPRbooks»	http://www.iprbookshop.ru/52217.html
Мэйволд, Э. Безопасность сетей [Электронный ресурс]: учебное пособие / Э. Мэйволд. - М.: Интернет-Университет Информационных Технологий (ИНТУИТ), 2016. - 571 с. - ЭБС «IPRbooks»	http://www.iprbookshop.ru/73727.html

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/ 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

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
Microsoft .NET Framework 4.7 Свободная лицензия
Офисный пакет Microsoft office 2016 Договор от 26.05.2020 № 32009117096 Договор от 17.01.2019 № 31908696765
Антивирус kaspersky endpoint security Лицензионный договор от 17.02.2021 № 203-20122401
Microsoft Office Word 2010 Номер продукта 14.0.6024.1000 SP1 MSO 02260-018-0000106-48095

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/
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
CYBERLENINKA : научная электронная библиотека : сайт. – Москва, 2014. - . – URL: https://cyberleninka.ru// - Режим доступа: для зарегистрир. пользователей. – Текст: электронный. КиберЛенинка - это научная электронная

Название
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

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.'

Название
(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. - 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
Parallel.ru. Лаборатория Параллельных информационных технологий : [сайт] / Научно-исследовательский вычислительный центр Московского государственного университета имени М.В.Ломоносова. – Москва, [20??]. - – URL: https://parallel.ru/about. - Текст: электронный.На страницах сервера собрана и систематизирована информация, которая так или иначе связана с параллельными вычислениями - бурно развивающейся областью современной науки, активно проникающей во все новые и новые стороны жизни. Проектирование автомобилей и самолетов, нефтедобыча и фармакология, прогноз климатических изменений, синтез новых материалов и многие другие направления деятельности человека просто немыслимы без использования параллельных информационных технологий. https://parallel.ru/about
RSDN : [сайт]. – [Москва], 2001. - . - URL: http://rsdn.org/. - Текст: электронный.Русскоязычный сайт, посвящённый программированию под Windows. http://rsdn.org/

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.	