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.27 Основы управления информационной безопасностью**
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)

07.09.2023	Подписано простой ЭП 07.09.2023	И. Б. Берберьян
	(подпись)	(Ф.И.О.)

1. Цели и задачи учебной дисциплины (модуля)

Целью освоения дисциплины "Основы управления информационной безопасностью" являются получение необходимых знаний о принципах и методах, инструментальных средств, нормативных документах регуляторах, позволяющих успешно управлять информационной безопасность организации в условиях активного использования информационных технологий

Задачами изучения дисциплины являются:

- формирование навыков организации и методологии обеспечения информационной безопасности;

- создание представления о функциях, структурах и штатах подразделения информационной безопасности;

- изучение организационных основ, принципов, методов и технологий управления информационной безопасностью;

- развитие способностей по использованию существующей системы управления информационной безопасности.

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

Дисциплина входит в перечень курсов дисциплины, входящих в обязательный перечень базовой части. Она имеет логические и содержательно-методические связи с дисциплинами базовой и вариативной частей образовательного цикла «Организационное и правовое обеспечение информационной безопасности», «Документоведение и документооборот», «Информационное право» 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-10.1	Знает программно- аппаратные средства защиты информации в типовых операционных системах, системах управления базами данных, компьютерных сетях
ОПК-10.2	Умеет конфигурировать программно-аппаратные средства защиты информации в соответствии с заданными политиками безопасности
ОПК-10.3	Владеет принципами формирования политики информационной безопасности объекта информатизации
ОПК-2.3.1	Знает национальные, межгосударственные и международные стандарты в области защиты информации, нормативные правовые акты в области защиты информации, руководящие и методические документы уполномоченных федеральных органов исполнительной власти в области внедрения и эксплуатации средств защиты информации
ОПК-2.3.2	Умеет документировать процедуры и результаты контроля функционирования системы защиты информации; проводить испытания программно-технических средств защиты информации от НСД и специальных воздействий на соответствие требованиям по безопасности информации и техническим условиям
ОПК-2.3.3	Владеет навыками внесения изменений в эксплуатационную документацию и организационно-распорядительные документы по системе защиты информации; навыками разработки программ и методик испытаний опытного образца программно-технического средства защиты информации от НСД и специальных воздействий на соответствие техническим условиям
ОПК-2.4.1	Знает критерии оценки защищенности объекта информатизации, технические средства контроля эффективности мер защиты информации, методы измерений, контроля и технических расчетом характеристик программно-аппаратных средств защиты информации
ОПК-2.4.2	Умеет осуществлять контроль обеспечения уровня защищенности объектов информатизации
ОПК-2.4.3	Владеет навыками оценки защищенности объектов информатизации с помощью типовых программных средств
ОПК-5.1	Знает основы законодательства Российской Федерации, нормативные правовые акты, нормативные и методические документы в области информационной безопасности и защиты информации, правовые основы организации защиты государственной тайны и конфиденциальной информации, правовую характеристику преступлений в сфере компьютерной информации и меры ответственности за утрату, разглашение, модификацию и уничтожение защищаемой информации
ОПК-5.2	Умеет обосновывать решения, связанные с реализацией правовых норм по защите информации в пределах должностных обязанностей, предпринимать необходимые меры по восстановлению нарушенных прав
ОПК-5.3	Владеет навыками разрабатывать локальные правовые документы, регламентирующие работу по обеспечению информационной безопасности в организации
ОПК-6.1	Знает нормативные, руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации
ОПК-6.2	Умеет разрабатывать проекты локальных нормативных документов, регламентирующих защиту информации ограниченного доступа в организации
ОПК-6.3	Владеет навыками по разработке политики безопасности объекта информатизации



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-5.1	Знает нормативные правовые акты, методические документы, национальные стандарты в области защиты информации ограниченного доступа и аттестации объектов информатизации на соответствие требованиям по защите информации
ПК-5.2	Умеет разрабатывать программы и методики аттестационных испытаний выделенных (защищаемых) помещений на соответствие требованиям по защите информации, проводить аттестационные испытания, оформлять заключение по результатам аттестации выделенных (защищаемых) помещений на соответствие требованиям по защите информации
ПК-5.3	Владеет навыками подготовки аттестата соответствия выделенных (защищаемых) помещений требованиям по защите информации
ПК-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	Контроль	СР		
Курс 4	Сем. 7	1	17	34	0.35	26.65	30	**108**	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
7	Основные понятия информационной безопасности	1-2	1		2				3		Обсуждение докладов
7	Угрозы информационной безопасности в информационных системах	3-4	2		4				3		Реферат
7	Оценочные стандарты в информационной безопасности	5-6	2		4				3		Обсуждение докладов
7	Стандарты управления информационной безопасностью	7-8	2		4				3		Реферат
7	Создание СУИБ на предприятии	9-10	2		4				3		Обсуждение докладов
7	Правовые меры обеспечения информационной безопасности	11-12	2		4				3		Обсуждение докладов
7	Организационные меры обеспечения безопасности компьютерных информационных систем	13-14	2		4				4		Тестирорвание
7	Программно-технические меры обеспечения информационной безопасности. Идентификация, аутентификация, управление доступом	15	2		4				4		Реферат
7	Протоколирование и аудит, шифрование, контроль целостности.	16	2		4		0,35	26,65	4		Обсуждение докладов
	ИТОГО:		**17**		**34**		**0.35**	**26.65**	**30**		

5.4. Содержание разделов дисциплины (модуля) «Основы управления информационной безопасностью», 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
7	Основные понятия информационной безопасности	1			Понятие информационной безопасности. Основные составляющие информационной безопасности. Управление информационной без-опасностью. Важность и сложность проблемы информационной безопасности.	ОПК-2.3.1; ОПК-2.3.2; ОПК-2.3.3; ОПК-2.4.1; ОПК-5.1; ОПК-6.1; ОПК-5.3; ОПК-6.3; ОПК-6.2; ПК-4.1; ПК-5.1; ПК-5.3; ПК-8.3;	знать: основные стандарты, регламентирующие управление ИБ; принципы разработки процессов управления ИБ; подходы к интеграции СУИБ в общую систему управления предприятием. уметь: анализировать текущее состояние ИБ в организации с целью разработки требований к разрабатываемым процессам управления ИБ; определять цели и задачи, решаемые разрабатываемыми процессами управления ИБ; применять процессный под-ход к управлению ИБ в раз-личных сферах деятельности; используя современные методы и средства разрабатывать процессы управления ИБ, учитывающие особенности функционирования предприятия и решаемых им задач, и оценивать их эффективность; практически решать задачи формализации разрабатываемых процессов управления ИБ; разрабатывать и внедрять СУИБ и оценивать ее	, Слайд-лекция

Сем	Наименование темы дисциплины	Трудоемкость (часы)			Содержание	Формируемые компетенции	Результаты освоения (знать, уметь, владеть)	Образовательные технологии
		ОФО	ЗФО	ОЗФО				
1	2	3	4	5	6	7	8	9
							эффективность. владеть: терминологией и процессным подходом по-строения систем управления ИБ; навыками анализа активов организации, их угроз ИБ и уязвимостей в рамках области деятельности СУИБ; навыками построения как отдельных процессов управления ИБ, так и системы процессов в целом.	
7	Угрозы информационной безопасности в информационных системах	2			Основные определения и критерии классификации угроз. Основные угрозы доступности. Основные угрозы целостности. Основные угрозы конфиденциальности. Вредительские программы.	ОПК-10.2; ОПК-10.1; ОПК-10.3; ОПК-2.3.2; ОПК-2.3.1; ОПК-2.4.1; ОПК-5.1; ОПК-2.4.3; ОПК-5.2; ПК-4.1; ОПК-6.3; ПК-5.1; ПК-4.3; ПК-4.2; ПК-5.3; ПК-8.2; ПК-8.3;	знать: основные стандарты, регламентирующие управление ИБ; принципы разработки процессов управления ИБ; подходы к интеграции СУИБ в общую систему управления предприятием. уметь: анализировать текущее состояние ИБ в организации с целью разработки требований к разрабатываемым процессам управления ИБ; определять цели и задачи, решаемые разрабатываемыми процессами управления ИБ; применять процессный под-ход к управлению ИБ в раз-личных сферах деятельности; используя современные методы и средства разрабатывать процессы управления ИБ, учитывающие особенности функционирования предприятия и решаемых им задач, и оценивать их эффективность;	, Слайд-лекция

Сем	Наименование темы дисциплины	Трудоемкость (часы)			Содержание	Формируемые компетенции	Результаты освоения (знать, уметь, владеть)	Образовательные технологии
		ОФО	ЗФО	ОЗФО				
1	2	3	4	5	6	7	8	9
							практически решать задачи формализации разрабатываемых процессов управления ИБ; разрабатывать и внедрять СУИБ и оценивать ее эффективность. владеть: терминологией и процессным подходом по-строения систем управления ИБ; навыками анализа активов организации, их угроз ИБ и уязвимостей в рамках области деятельности СУИБ; навыками построения как отдельных процессов управления ИБ, так и системы процессов в целом.	
7	Оценочные стандарты в информационной безопасности	2			Роль стандартов ИБ. «Оранжевая книга» как оценочный стандарт. Международный стандарт ISO/IEC 15408. Критерии оценки безопасности информационных систем.	ОПК-2.3.2; ОПК-2.3.1; ОПК-5.1; ОПК-5.2; ОПК-6.1; ОПК-5.3; ОПК-6.2; ОПК-6.3; ПК-4.1; ПК-4.2; ПК-4.3; ПК-5.1; ПК-5.3; ПК-8.3;	знать: основные стандарты, регламентирующие управление ИБ; принципы разработки процессов управления ИБ; подходы к интеграции СУИБ в общую систему управления предприятием. уметь: анализировать текущее состояние ИБ в организации с целью разработки требований к разрабатываемым процессам управления ИБ; определять цели и задачи, решаемые разрабатываемыми процессами управления ИБ; применять процессный под-ход к управлению ИБ в раз-личных сферах деятельности; используя современные методы и средства разрабатывать процессы управления ИБ,	, Слайд-лекция

Сем	Наименование темы дисциплины	Трудоемкость (часы)			Содержание	Формируемые компетенции	Результаты освоения (знать, уметь, владеть)	Образовательные технологии
		ОФО	ЗФО	ОЗФО				
1	2	3	4	5	6	7	8	9
							учитывающие особенности функционирования предприятия и решаемых им задач, и оценивать их эффективность; практически решать задачи формализации разрабатываемых процессов управления ИБ; разрабатывать и внедрять СУИБ и оценивать ее эффективность. владеть: терминологией и процессным подходом по-строения систем управления ИБ; навыками анализа активов организации, их угроз ИБ и уязвимостей в рамках области деятельности СУИБ; навыками построения как отдельных процессов управления ИБ, так и системы процессов в целом.	
7	Стандарты управления информационной безопасностью	2			Стандарты управления информационной безопасностью BS 7799 и ISO/IEC 17799. Их основные положения. Международный стандарт ISO/IEC 27001:2005 "Системы управления информационной безопасности. Требования". Сертификация СУИБ на соответствие ISO 27001.	ОПК-10.1; ОПК-10.2; ОПК-2.3.3; ОПК-2.4.3; ОПК-2.4.2; ОПК-5.1; ОПК-5.2; ОПК-5.3; ОПК-6.1; ОПК-6.3; ПК-4.1; ОПК-6.2; ПК-5.2; ПК-5.1; ПК-8.2; ПК-5.3; ПК-8.3;	знать: основные стандарты, регламентирующие управление ИБ; принципы разработки процессов управления ИБ; подходы к интеграции СУИБ в общую систему управления предприятием. уметь: анализировать текущее состояние ИБ в организации с целью разработки требований к разрабатываемым процессам управления ИБ; определять цели и задачи, решаемые разрабатываемыми процессами управления ИБ; применять процессный под-ход к	, Слайд-лекция

Сем	Наименование темы дисциплины	Трудоемкость (часы)			Содержание	Формируемые компетенции	Результаты освоения (знать, уметь, владеть)	Образовательные технологии
		ОФО	ЗФО	ОЗФО				
1	2	3	4	5	6	7	8	9
							управлению ИБ в различных сферах деятельности; используя современные методы и средства разрабатывать процессы управления ИБ, учитывающие особенности функционирования предприятия и решаемых им задач, и оценивать их эффективность; практически решать задачи формализации разрабатываемых процессов управления ИБ; разрабатывать и внедрять СУИБ и оценивать ее эффективность. владеть: терминологией и процессным подходом построения систем управления ИБ; навыками анализа активов организации, их угроз ИБ и уязвимостей в рамках области деятельности СУИБ; навыками построения как отдельных процессов управления ИБ, так и системы процессов в целом.	
7	Создание СУИБ на предприятии	2			Этапы разработки и внедрения системы управления ИБ. Содержание этапов разработки и внедрения системы управления ИБ.	ОПК-10.1; ОПК-10.2; ОПК-10.3; ОПК-2.3.1; ОПК-2.4.1; ОПК-2.4.3; ОПК-2.4.2; ОПК-5.1; ОПК-6.2; ОПК-6.1; ОПК-6.3; ПК-4.1; ПК-4.2; ПК-5.1; ПК-4.3; ПК-5.2; ПК-5.3; ПК-8.3; ПК-8.2;	знать: основные стандарты, регламентирующие управление ИБ; принципы разработки процессов управления ИБ; подходы к интеграции СУИБ в общую систему управления предприятием. уметь: анализировать текущее состояние ИБ в организации с целью разработки требований к разрабатываемым процессам управления	, Слайд-лекция

Сем	Наименование темы дисциплины	Трудоемкость (часы)			Содержание	Формируемые компетенции	Результаты освоения (знать, уметь, владеть)	Образовательные технологии
		ОФО	ЗФО	ОЗФО				
1	2	3	4	5	6	7	8	9
							ИБ; определять цели и задачи, решаемые разрабатываемыми процессами управления ИБ; применять процессный под-ход к управлению ИБ в раз-личных сферах деятельности; используя современные методы и средства разрабатывать процессы управления ИБ, учитывающие особенности функционирования предприятия и решаемых им задач, и оценивать их эффективность; практически решать задачи формализации разрабатываемых процессов управления ИБ; разрабатывать и внедрять СУИБ и оценивать ее эффективность. владеть: терминологией и процессным подходом по-строения систем управления ИБ; навыками анализа активов организации, их угроз ИБ и уязвимостей в рамках области деятельности СУИБ; навыками построения как отдельных процессов управления ИБ, так и системы процессов в целом.	
7	Правовые меры обеспечения информационной безопасности	2			Основные направления обеспечения информационной безопасности. Законодательно-правовая база обеспечения информационной безопасности на предприятии.	ОПК-10.3; ОПК-2.3.1; ОПК-2.3.2; ОПК-2.3.3; ОПК-2.4.1; ОПК-5.1; ОПК-5.2; ОПК-5.3; ОПК-6.1; ОПК-6.2; ОПК-6.3; ПК-4.1; ПК-4.2; ПК-4.3; ПК-5.1; ПК-5.2; ПК-5.3; ПК-8.2; ПК-8.3;	знать: основные стандарты, регламентирующие управление ИБ; принципы разработки процессов управления ИБ; подходы к интеграции СУИБ в общую систему управления предприятием. уметь:	, Слайд-лекция

Сем	Наименование темы дисциплины	Трудоемкость (часы)			Содержание	Формируемые компетенции	Результаты освоения (знать, уметь, владеть)	Образовательные технологии
		ОФО	ЗФО	ОЗФО				
1	2	3	4	5	6	7	8	9
					Нормативные акты предприятия по информационной безопасности. Формы правовой защиты информации на предприятии. Другие документы предприятия, в которых отражаются вопросы обеспечения информационной безопасности.		анализировать текущее состояние ИБ в организации с целью разработки требований к разрабатываемым процессам управления ИБ; определять цели и задачи, решаемые разрабатываемыми процессами управления ИБ; применять процессный под-ход к управлению ИБ в раз-личных сферах деятельности; используя современные методы и средства разрабатывать процессы управления ИБ, учитывающие особенности функционирования предприятия и решаемых им задач, и оценивать их эффективность; практически решать задачи формализации разрабатываемых процессов управления ИБ; разрабатывать и внедрять СУИБ и оценивать ее эффективность. владеть: терминологией и процессным подходом по-строения систем управления ИБ; навыками анализа активов организации, их угроз ИБ и уязвимостей в рамках области деятельности СУИБ; навыками построения как отдельных процессов управления ИБ, так и системы процессов в целом.	
7	Организационные меры обеспечения безопасности	2			Общие положения организационной защиты. Особенности	ОПК-10.3; ОПК-2.3.1; ОПК-2.3.2; ОПК-2.3.3; ОПК-2.4.1; ОПК-5.1;	знать: основные стандарты, регламентирующие	, Лекция-беседа

Сем	Наименование темы дисциплины	Трудоемкость (часы)			Содержание	Формируемые компетенции	Результаты освоения (знать, уметь, владеть)	Образовательные технологии
		ОФО	ЗФО	ОЗФО				
1	2	3	4	5	6	7	8	9
	компьютерных информационных систем				организационной защиты компьютерных информационных систем и сетей. Служба безопасности предприятия.	ОПК-5.2; ОПК-5.3; ОПК-6.1; ПК-4.1; ОПК-6.3; ОПК-6.2; ПК-4.2; ПК-4.3; ПК-5.1; ПК-5.2; ПК-8.2; ПК-5.3; ПК-8.3;	управление ИБ; принципы разработки процессов управления ИБ; подходы к интеграции СУИБ в общую систему управления предприятием. уметь: анализировать текущее состояние ИБ в организации с целью разработки требований к разрабатываемым процессам управления ИБ; определять цели и задачи, решаемые разрабатываемыми процессами управления ИБ; применять процессный под-ход к управлению ИБ в раз-личных сферах деятельности; используя современные методы и средства разрабатывать процессы управления ИБ, учитывающие особенности функционирования предприятия и решаемых им задач, и оценивать их эффективность; практически решать задачи формализации разрабатываемых процессов управления ИБ; разрабатывать и внедрять СУИБ и оценивать ее эффективность. владеть: терминологией и процессным подходом по-строения систем управления ИБ; навыками анализа активов организации, их угроз ИБ и уязвимостей в рамках области деятельности СУИБ; навыками построения как отдельных процессов	

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
							управления ИБ, так и системы процессов в целом.	
7	Программно-технические меры обеспечения информационной безопасности. Идентификация, аутентификация, управление доступом	2			Основные программно-технические меры. Идентификация и аутентификация.	ОПК-10.1; ОПК-10.2; ОПК-2.3.3; ОПК-2.4.1; ОПК-2.4.2; ОПК-2.4.3; ОПК-6.2; ПК-5.2; ПК-5.3; ПК-8.2; ПК-8.3;	знать: основные стандарты, регламентирующие управление ИБ; принципы разработки процессов управления ИБ; подходы к интеграции СУИБ в общую систему управления предприятием. уметь: анализировать текущее состояние ИБ в организации с целью разработки требований к разрабатываемым процессам управления ИБ; определять цели и задачи, решаемые разрабатываемыми процессами управления ИБ; применять процессный под-ход к управлению ИБ в раз-личных сферах деятельности; используя современные методы и средства разрабатывать процессы управления ИБ, учитывающие особенности функционирования предприятия и решаемых им задач, и оценивать их эффективность; практически решать задачи формализации разрабатываемых процессов управления ИБ; разрабатывать и внедрять СУИБ и оценивать ее эффективность. владеть: терминологией и процессным подходом по-строения систем управления ИБ; навыками анализа активов	, Слайд-лекция

Сем	Наименование темы дисциплины	Трудоемкость (часы)			Содержание	Формируемые компетенции	Результаты освоения (знать, уметь, владеть)	Образовательные технологии
		ОФО	ЗФО	ОЗФО				
1	2	3	4	5	6	7	8	9
							организации, их угроз ИБ и уязвимостей в рамках области деятельности СУИБ; навыками построения как отдельных процессов управления ИБ, так и системы процессов в целом.	
7	Протоколирование и аудит, шифрование, контроль целостности.	2			Протоколирование и аудит. Активный аудит. Шифрование. Контроль целостности. Цифровые сертификаты.	ОПК-10.1; ОПК-10.2; ОПК-10.3; ОПК-2.3.2; ОПК-2.3.3; ОПК-2.4.1; ОПК-2.4.2; ОПК-2.4.3; ОПК-6.2; ПК-5.2;	знать: основные стандарты, регламентирующие управление ИБ; принципы разработки процессов управления ИБ; подходы к интеграции СУИБ в общую систему управления предприятием. уметь: анализировать текущее состояние ИБ в организации с целью разработки требований к разрабатываемым процессам управления ИБ; определять цели и задачи, решаемые разрабатываемыми процессами управления ИБ; применять процессный под-ход к управлению ИБ в раз-личных сферах деятельности; используя современные методы и средства разрабатывать процессы управления ИБ, учитывающие особенности функционирования предприятия и решаемых им задач, и оценивать их эффективность; практически решать задачи формализации разрабатываемых процессов управления ИБ; разрабатывать и внедрять СУИБ и оценивать ее	, Слайд-лекция

Сем	Наименование темы дисциплины	Трудоемкость (часы)			Содержание	Формируемые компетенции	Результаты освоения (знать, уметь, владеть)	Образовательные технологии
		ОФО	ЗФО	ОЗФО				
1	2	3	4	5	6	7	8	9
							эффективность. владеть: терминологией и процессным подходом по-строения систем управления ИБ; навыками анализа активов организации, их угроз ИБ и уязвимостей в рамках области деятельности СУИБ; навыками построения как отдельных процессов управления ИБ, так и системы процессов в целом.	
	ИТОГО:	**17**						

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
7	Основные понятия информационной безопасности	Понятие информационной безопасности. Основные составляющие информационной безопасности. Управление информационной без-опасностью. Важность и сложность проблемы информационной безопасности.	2		
7	Угрозы информационной безопасности в информационных системах	Основные определения и критерии классификации угроз. Основные угрозы доступности. Основные угрозы целостности.Основные угрозы конфиденциальности.Вредительские программы.	4		
7	Оценочные стандарты в информационной безопасности	Роль стандартов ИБ.«Оранжевая книга» как оценочный стандарт.Международный стандарт ISO/IEC 15408. Критерии оценки безопасности информационных систем.	4		
7	Стандарты управления информационной безопасностью	Стандарты управления информационной безопасностью BS 7799 и ISO/IEC 17799. Их основные положения.Международный стандарт ISO/IEC 27001:2005 "Системы управления информационной безопасности. Требования".Сертификация СУИБ на соответствие ISO 27001.	4		
7	Создание СУИБ на предприятии	Этапы разработки и внедрения системы управления ИБ. Содержание этапов разработки и внедрения системы управления ИБ.	4		
7	Правовые меры обеспечения информационной безопасности	Основные направления обеспечения информационной безопасности.Законодательно-правовая база обеспечения информационной безопасности на предприятии. Нормативные акты предприятия по информационной безопасности.Формы правовой защиты информации на предприятии. Другие документы предприятия, в которых отражаются вопросы обеспечения информационной безопасности.	4		
7	Организационные меры обеспечения безопасности компьютерных информационных систем	Общие положения организационной защиты. Особенности организационной защиты компьютерных информационных систем и сетей. Служба безопасности предприятия.	4		
7	Программно-технические меры обеспечения информационной безопасности. Идентификация, аутентификация, управление доступом	Основные программно-технические меры.Идентификация и аутентификация.	4		
7	Протоколирование и аудит, шифрование, контроль целостности.	Протоколирование и аудит.Активный аудит. Шифрование. Контроль целостности. Цифровые сертификаты.	4		
	ИТОГО:		**34**		

Симуляционные занятия, их наименование, содержание и объем в часах

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

5.6. Лабораторные занятия, их наименование и объем в часах

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

5.7. Примерная тематика курсовых проектов (работ)

5.8. Самостоятельная работа студентов

Содержание и объем самостоятельной работы студентов

Сем	Разделы и темы рабочей программы самостоятельного изучения	Перечень домашних заданий и других вопросов для самостоятельного изучения	Сроки выполнения	Объем в часах		
				ОФО	ЗФО	ОЗФО
1	2	3	4	5	6	7
7	Основные понятия информационной безопасности	Составление плана-конспекта	1-2	3		
7	Угрозы информационной безопасности в информационных системах	Презентация с докладом	3-4	3		
7	Оценочные стандарты в информационной безопасности	Составление плана-конспекта	5-6	3		
7	Стандарты управления информационной безопасностью	Реферат	7-8	3		
7	Создание СУИБ на предприятии	Презентация с докладом	9-10	3		
7	Правовые меры обеспечения информационной безопасности	Составление плана-конспекта	11-12	3		
7	Организационные меры обеспечения безопасности компьютерных информационных систем	Презентация с докладом	12-13	4		
7	Программно-технические меры обеспечения информационной безопасности. Идентификация, аутентификация, управление доступом	Презентация с докладом	14-15	4		
7	Протоколирование и аудит, шифрование, контроль целостности.	Реферат	16	4		
	ИТОГО:			**30**		

5.9. Календарный график воспитательной работы по дисциплине

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

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

6.1. Методические указания (собственные разработки)

Название	Ссылка

6.2. Литература для самостоятельной работ

Название	Ссылка
Башлы, П.Н. Информационная безопасность и защита информации [Электронный ресурс]: учебник / П. Н. Башлы, А. В. Бабаш, Е. К. Баранова. - М.: РИОР, 2013. - 222 с. - ЭБС «Znanium.com»	http://znanium.com/catalog.php?bookinfo=405000
Баранова, Е.К. Информационная безопасность и защита информации [Электронный ресурс]: учебное пособие / Е.К. Баранова, А.В. Бабаш. - М.: РИОР: ИНФРА-М, 2019. - 322 с. - ЭБС «Znanium.com»	http://znanium.com/catalog/product/1009606
Жукова, М. Н. Управление информационной безопасностью. Ч. 2. Управление инцидентами информационной безопасности [Электронный ресурс]: учебное пособие / М. Н. Жукова, В. Г. Жуков, В. В. Золотарев. - Красноярск: Сиб. гос. аэрокосмич. ун-т, 2012. - 100 с. - ЭБС «Znanium.com»	http://znanium.com/catalog.php?bookinfo=463061
Золотарев, В. В. Управление информационной безопасностью. Ч. 1. Анализ информационных рисков [Электронный ресурс]: учебное пособие / В. В. Золотарев, Е. А. Данилова. - Красноярск:Сиб. гос. аэрокосмич. ун-т, 2010. - 144 с. - ЭБС «Znanium.com»	5. http://znanium.com/catalog.php?bookinfo=463037

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-10.1 Знает программно- аппаратные средства защиты информации в типовых операционных системах, системах управления базами данных, компьютерных сетях			
67			Программно-аппаратные средства защиты информации
7			Основы управления информационной безопасностью
ОПК-10.2 Умеет конфигурировать программно-аппаратные средства защиты информации в соответствии с заданными политиками безопасности			
67			Программно-аппаратные средства защиты информации
7			Основы управления информационной безопасностью
ОПК-10.3 Владеет принципами формирования политики информационной безопасности объекта информатизации			
67			Программно-аппаратные средства защиты информации
7			Основы управления информационной безопасностью
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			

Этапы формирования компетенции (номер семестр согласного учебному плану)			Наименование учебных дисциплин, формирующие компетенции в процессе освоения образовательной программы
ОФО	ЗФО	ОЗФО	
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-2.3.3 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			

Этапы формирования компетенции (номер семестр согласного учебному плану)			Наименование учебных дисциплин, формирующие компетенции в процессе освоения образовательной программы
ОФО	ЗФО	ОЗФО	
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
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

Этапы формирования компетенции (номер семестр согласного учебному плану)			Наименование учебных дисциплин, формирующие компетенции в процессе освоения образовательной программы
ОФО	ЗФО	ОЗФО	
			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-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

Этапы формирования компетенции (номер семестр согласного учебному плану)			Наименование учебных дисциплин, формирующие компетенции в процессе освоения образовательной программы
ОФО	ЗФО	ОЗФО	
			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 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
ОПК-6.1 Знает нормативные, руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации			
5			Организационное и правовое обеспечение информационной безопасности
67			Программно-аппаратные средства защиты информации

Этапы формирования компетенции (номер семестр согласного учебному плану)			Наименование учебных дисциплин, формирующие компетенции в процессе освоения образовательной программы
ОФО	ЗФО	ОЗФО	
7			Основы управления информационной безопасностью
5			Техническая защита информации
2			Учебно-лабораторная практика
4			Технологическая практика
6			Эксплуатационная практика
8			Преддипломная практика
ОПК-6.2 Умеет разрабатывать проекты локальных нормативных документов, регламентирующих защиту информации ограниченного доступа в организации			
5			Организационное и правовое обеспечение информационной безопасности
67			Программно-аппаратные средства защиты информации
7			Основы управления информационной безопасностью
5			Техническая защита информации
2			Учебно-лабораторная практика
4			Технологическая практика
6			Эксплуатационная практика
8			Преддипломная практика
ОПК-6.3 Владеет навыками по разработке политики безопасности объекта информатизации			
5			Организационное и правовое обеспечение информационной безопасности
67			Программно-аппаратные средства защиты информации
7			Основы управления информационной безопасностью
5			Техническая защита информации
4			Технологическая практика
6			Эксплуатационная практика
8			Преддипломная практика
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

Этапы формирования компетенции (номер семестр согласного учебному плану)			Наименование учебных дисциплин, формирующие компетенции в процессе освоения образовательной программы
ОФО	ЗФО	ОЗФО	
			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 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-5.1 Знает нормативные правовые акты, методические документы, национальные стандарты в области защиты информации ограниченного доступа и аттестации объектов информатизации на соответствие требованиям по защите информации			
2			Основы информационной безопасности
5			Организационное и правовое обеспечение информационной безопасности
7			Основы управления информационной

Этапы формирования компетенции (номер семестр согласного учебному плану)			Наименование учебных дисциплин, формирующие компетенции в процессе освоения образовательной программы
ОФО	ЗФО	ОЗФО	
			безопасностью
8			Комплексное обеспечение защиты информации объекта информатизации
7			Нормативные акты и стандарты по информационной безопасности
ПК-5.2 Умеет разрабатывать программы и методики аттестационных испытаний выделенных (защищаемых) помещений на соответствие требованиям по защите информации, проводить аттестационные испытания, оформлять заключение по результатам аттестации выделенных (защищаемых) помещений на соответствие требованиям по защите информации			
2			Основы информационной безопасности
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
ПК-5.3 Владеет навыками подготовки аттестата соответствия выделенных (защищаемых) помещений требованиям по защите информации			
2			Основы информационной безопасности
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
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

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
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
ОПК-6: Способен осуществлять исследования объектов и процессов в области строительства и жилищно-коммунального хозяйства					
ОПК-6.2 Умеет разрабатывать проекты локальных нормативных документов, регламентирующих защиту информации ограниченного доступа 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-4.2 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	Несистематическое применение	В систематическом	Успешное и систематическое	

Планируемые результаты освоения компетенции	Критерии оценивания результатов обучения				Наименование оценочного средства
	неудовлетворительно	удовлетворительно	хорошо	отлично	
1	2	3	4	5	6
	навыками	навыков	применении навыков допускаются пробелы	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 навыков допускаются пробелы	Успешное и систематическое применение навыков	
ПК-5: Способен принимать участие в организации и сопровождении аттестации объекта информатизации по требованиям безопасности информации					
ПК-5.1 Знает нормативные правовые акты, методические документы, национальные стандарты в области защиты информации ограниченного доступа и аттестации объектов информатизации на соответствие требованиям по защите информации					
Знать:	Фрагментарные знания	Неполные знания	Сформированные, но содержащие отдельные пробелы знания	Сформированные систематические знания	
Уметь:	Частичные умения	Неполные умения	Умения полные, допускаются небольшие ошибки	Сформированные умения	
Владеть:	Частичное владение навыками	Несистематическое применение навыков	В систематическом применении навыков допускаются пробелы	Успешное и систематическое применение навыков	
ПК-5: Способен принимать участие в организации и сопровождении аттестации объекта информатизации по требованиям безопасности информации					
ПК-5.2 Умеет разрабатывать программы и методики аттестационных испытаний выделенных (защищаемых) помещений на соответствие требованиям по защите информации, проводить аттестационные испытания, оформлять заключение по результатам аттестации выделенных (защищаемых) помещений на соответствие требованиям по защите информации					
Знать:	Фрагментарные знания	Неполные знания	Сформированные, но содержащие отдельные пробелы знания	Сформированные систематические знания	
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-2.3.1 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	Сформированные систематические знания	

Планируемые результаты освоения компетенции	Критерии оценивания результатов обучения				Наименование оценочного средства
	неудовлетворительно	удовлетворительно	хорошо	отлично	
1	2	3	4	5	6
			пробелы 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-5: Способен принимать участие в организации и сопровождении аттестации объекта информатизации по требованиям безопасности информации					
ПК-5.3 Владеет навыками подготовки аттестата соответствия выделенных (защищаемых) помещений требованиям по защите информации					
Знать:	Фрагментарные знания	Неполные знания	Сформированные, но содержащие отдельные пробелы знания	Сформированные систематические знания	
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-6: Способен осуществлять исследования объектов и процессов в области строительства и жилищно-коммунального хозяйства					
ОПК-6.3 Владеет навыками по разработке политики безопасности объекта 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	
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	Сформированные систематические	

Планируемые результаты освоения компетенции	Критерии оценивания результатов обучения				Наименование оценочного средства
	неудовлетворительно	удовлетворительно	хорошо	отлично	
1	2	3	4	5	6
			отдельные пробелы знания	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 ошибки	Сформированные умения	
Владеть:	Частичное владение навыками	Несистематическое применение навыков	В систематическом применении навыков допускаются пробелы	Успешное и систематическое применение навыков	
ОПК-6: Способен осуществлять исследования объектов и процессов в области строительства и жилищно-коммунального хозяйства					
ОПК-6.1 Знает нормативные, руководящие и методические документы уполномоченных федеральных органов исполнительной власти 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-5.1 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-					

Планируемые результаты освоения компетенции	Критерии оценивания результатов обучения				Наименование оценочного средства
	неудовлетворительно	удовлетворительно	хорошо	отлично	
1	2	3	4	5	6
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 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-2.4.2 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	Успешное и систематическое применение навыков	

Планируемые результаты освоения компетенции	Критерии оценивания результатов обучения				Наименование оценочного средства
	неудовлетворительно	удовлетворительно	хорошо	отлично	
1	2	3	4	5	6
			пробелы		
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	
ОПК-10: Способен в качестве технического специалиста принимать участие в формировании политики информационной безопасности, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации на объекте защиты;					
ОПК-10.1 Знает программно- аппаратные средства защиты информации в типовых операционных системах, системах управления базами данных, компьютерных сетях					
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-10: Способен в качестве технического специалиста принимать участие в формировании политики информационной безопасности, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации на объекте защиты;					
ОПК-10.2 Умеет конфигурировать программно-аппаратные средства защиты информации в соответствии с заданными политиками безопасности					
Знать:	Фрагментарные знания	Неполные знания	Сформированные, но содержащие отдельные пробелы знания	Сформированные систематические знания	
Уметь:	Частичные умения	Неполные умения	Умения полные, допускаются	Сформированные умения	

Планируемые результаты освоения компетенции	Критерии оценивания результатов обучения				Наименование оценочного средства
	неудовлетворительно	удовлетворительно	хорошо	отлично	
1	2	3	4	5	6
			небольшие ошибки		
Владеть:	Частичное владение навыками	Несистематическое применение навыков	В систематическом применении навыков допускаются пробелы	Успешное и систематическое применение навыков	
ОПК-10: Способен в качестве технического специалиста принимать участие в формировании политики информационной безопасности, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации на объекте защиты;					
ОПК-10.3 Владеет принципами формирования политики информационной безопасности объекта 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	

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.Стандартизация систем и процессов управления информационной безопасностью

2.Стандарты на отдельные процессы управления ИБ и оценку безопасности ИТ

3.Отраслевые стандарты в области управления ИБ - стандарты банковской системы Российской Федерации

4.Политика информационной безопасности

5.Система управления ИБ организации

6.Процессный подход в рамках управления ИБ

7.Совершенствование СУИБ

8.Работа с процессами СУИБ организации

9.Стратегии построения и внедрения СУИБ

10.Построение и внедрение СУИБ в целом

11.Построение и внедрение процессов СУИБ по отдельности

Темы докладов

1.Основные понятия информационной безопасности

2.Угрозы информационной безопасности в информационных системах

3.Оценочные стандарты в информационной безопасности

4.Стандарты управления информационной безопасностью

5.Создание СУИБ на предприятии

6.Правовые меры обеспечения информационной безопасности

7.Основные направления обеспечения информационной безопасности.8.Законодательно-правовая база обеспечения информационной безопасности на предприятии. 9.Нормативные акты предприятия по информационной безопасности.

10.Организационные меры обеспечения безопасности компьютерных информационных систем.

11.Программно-технические меры обеспечения информационной безопасности. Идентификация, аутентификация, управление доступом.

12.Протоколирование и аудит, шифрование, контроль целостности.

Тестовые задания для определения остаточных знаний

Тест по дисциплине

«Основы управления информационной безопасностью»

*** - несколько вариантов ответов**

1. Кто является основным ответственным за определение уровня классификации информации?

1) руководитель среднего звена;
2) высшее руководство;
3) владелец;
4) пользователь.

2. Какая категория является наиболее рискованной для компании с точки зрения вероятного мошенничества и нарушения безопасности?

1) сотрудники;
2) хакеры;
3) атакующие;
4) контрагенты (лица, работающие по договору).

3. Когда целесообразно не предпринимать никаких действий в отношении выявленных рисков?

1) никогда. Для обеспечения хорошей безопасности нужно учитывать и снижать все риски;

2) когда риски не могут быть приняты во внимание по политическим соображениям;

3) когда необходимые защитные меры слишком сложны;

4) когда стоимость контрмер превышает ценность актива и потенциальные потери.



4. Программа Melissa — это:

1) бомба;

2) почтовый вирус;

3) червь.

5. Среди ниже перечисленных отметьте две троянские программы *:

1) I LOVE YOU;

2) Back Orifice;

3) Netbus.

6. Уголовный кодекс РФ не предусматривает наказания за:

1) создание, использование и распространение вредоносных программ;

2) ведение личной корреспонденции на производственной технической базе;

3) нарушение правил эксплуатации информационных систем.

7. Уровень безопасности «В» согласно «Оранжевой книге» характеризуется:

1) произвольным управлением доступом ;

2) принудительным управлением доступом;

3) верифицируемой безопасностью.

8. Согласно рекомендациям X.800 выделяются следующие сервисы безопасности:

1) управление квотами;

2) управление доступом;

3) экранирование.

9. Риск является функцией:

1) размера возможного ущерба;

2) числа пользователей информационной системы;

3) уставного капитала организации.

***10.** В число этапов управления рисками входят:

1) идентификация активов;

2) ликвидация пассивов;

3) выбор объектов оценки.

11. Первый шаг в анализе угроз — это:

1) идентификация угроз;

2) аутентификация угроз;

3) ликвидация угроз.

Контрольные тесты и задания для проведения промежуточной аттестации

Тест по дисциплине

«Основы управления информационной безопасностью»

1. Метод, при котором символы шифруемого текста последовательно складываются с символами некоторой специальной последовательности, называется методом:

1)гаммирования;

2)подстановки;

3)кодирования;

4)перестановки;

5)аналитических преобразований.

2. Согласно «Оранжевой книге» дискреционную защиту имеет группа критериев:

1)D;

2)A;

3)B;

4)C.

3. Степень защищенности информации от негативного воздействия на неё с точки зрения нарушения её физической и логической целостности или несанкционированного использования — это

1)уязвимость информации;

2)надежность информации;

3)защищенность информации;

4)безопасность информации.

4. Проверка подлинности субъекта по предъявленному им идентификатору для принятия решения о предоставлении ему доступа к ресурсам системы — это

1)аудит;

2)аутентификация;

3)авторизация;

4)идентификация.

5. Согласно «Оранжевой книге» уникальные идентификаторы должны иметь:

1)наиболее важные субъекты;

2)наиболее важные объекты;

3)все субъекты;

4)все объекты.

6. Организационные требования к системе защиты это-

1)управленческие и идентификационные;

2)административные и аппаратурные;

3)административные и процедурные;

4)аппаратурные и физические.

7. При избирательной политике безопасности в матрице доступа субъекту системы соответствует:

1)ячейка;

2)строка;

3)прямоугольная область;

4)столбец.

8. Наукой, изучающей математические методы защиты информации путем ее преобразования, является:

1)криптоанализ;

2)криптология;

3)стеганография;

4)криптография.

9. Первым этапом разработки системы защиты ИС является:

1)анализ потенциально возможных угроз информации;

2)изучение информационных потоков;

3)стандартизация программного обеспечения;

4)оценка возможных потерь.

10. Обеспечением скрытности информации в информационных массивах занимается:

1)криптография;

2)криптоанализ;

3)криптология;

4)Стеганография.

Примерный перечень вопросов к экзамену по дисциплине



1. Понятие информационной безопасности.

2. Основные составляющие информационной безопасности.

3. Управление информационной безопасностью.

4. Важность и сложность проблемы информационной безопасности

5. Основные определения и критерии классификации угроз.

6. Основные угрозы доступности.

7. Основные угрозы целостности.

8. Основные угрозы конфиденциальности.

9. Вредительские программы

10. Роль стандартов ИБ.

11. "Оранжевая книга" как оценочный стандарт.

12. Международный стандарт ISO/IEC 15408. Критерии оценки безопасности информационных систем.

13. Стандарты управления информационной безопасностью BS 7799 и ISO/IEC 17799. Их основные положения.

14. Международный стандарт ISO/IEC 27001:2005 "Системы управления информационной безопасности. Требования".

15. Сертификация СУИБ на соответствие ISO 27001.

16. Метод оценки рисков на основе модели угроз и уязвимостей

17. Расчет рисков по угрозе информационной безопасности

18. Задание контрмер

19. Качественные методики управления рисками.

20. Количественные методики управления рисками. Метод CRAMM.

21. Обоснование необходимости инвестиций в информационную безопасность компании.

22. Методика FRAP (фреп).

23. Методика OCTAVE (октэйв)

24. Методика Risk Watch (риск вэтч).

25. Основные направления обеспечения информационной безопасности.

26. Законодательно-правовая база обеспечения информационной безопасности на предприятии.

27. Нормативные акты предприятия по информационной безопасности.

28. Формы правовой защиты информации на предприятии.

29. Другие документы предприятия, в которых отражаются вопросы обеспечения информационной безопасности.

30. Общие положения организационной защиты.

31. Особенности организационной защиты компьютерных информационных систем и сетей.

32. Служба безопасности предприятия.

33. Основные программно-технические меры.

34. Идентификация и аутентификация.

35. Управление доступом

36. Протоколирование и аудит

37. Активный аудит.

38. Шифрование.

39. Контроль целостности.

40. Цифровые сертификаты.

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

Требования к написанию реферата

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

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

Его задачами являются:

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

2. Развитие навыков логического мышления;

3. Углубление теоретических знаний по проблеме исследования.

При оценке реферата используются следующие критерии:

- новизна текста;

- обоснованность выбора источника;

- степень раскрытия сущности вопроса;

- соблюдения требований к оформлению.

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

Тематика рефератов выдается преподавателем в конце семинарского занятия.

Требования к написанию доклада

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

Критерии оценивания доклада:

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

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

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

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

Требования к выполнению тестового задания

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

Основные принципы тестирования, следующие:

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

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

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

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

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

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

В тестовых заданиях используются четыре типа вопросов:

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

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

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

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

Критерии оценки знаний при проведении тестирования

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

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

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

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

Результаты текущего контроля используются при проведении промежуточной аттестации.



Критерии оценки знаний на экзамене

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

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

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

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

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

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

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

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

8.1. Основная литература

Название	Ссылка
Башлы, П.Н. Информационная безопасность и защита информации [Электронный ресурс]: учебник / П. Н. Башлы, А. В. Бабаш, Е. К. Баранова. - М.: РИОР, 2013. - 222 с. - ЭБС «Znanium.com»	http://znanium.com/catalog.php?bookinfo=405000

8.2. Дополнительная литература

Название	Ссылка
Баранова, Е.К. Информационная безопасность и защита информации [Электронный ресурс]: учебное пособие / Е.К. Баранова, А.В. Бабаш. - М.: РИОР: ИНФРА-М, 2019. - 322 с. - ЭБС «Znanium.com»	http://znanium.com/catalog/product/1009606
Жукова, М. Н. Управление информационной безопасностью. Ч. 2. Управление инцидентами информационной безопасности [Электронный ресурс]: учебное пособие / М. Н. Жукова, В. Г. Жуков, В. В. Золотарев. - Красноярск: Сиб. гос. аэрокосмич. ун-т, 2012. - 100 с. - ЭБС «Znanium.com»	http://znanium.com/catalog.php?bookinfo=463061
Золотарев, В. В. Управление информационной безопасностью. Ч. 1. Анализ информационных рисков [Электронный ресурс]: учебное пособие / В. В. Золотарев, Е. А. Данилова. - Красноярск:Сиб. гос. аэрокосмич. ун-т, 2010. - 144 с. - ЭБС «Znanium.com»	http://znanium.com/catalog.php?bookinfo=463037

8.3. Информационно-телекоммуникационные ресурсы сети «Интернет»

Ресурсы Интернет открытого доступа (Open Access) 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.

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

Раздел / Тема с указанием основных учебных элементов	Методы обучения	Способы (формы) обучения	Средства обучения	Формируемые компетенции
Основные понятия информационной безопасности Понятиеинформационной безопасности. Основные составляющие информационной безопасности. Управление информационной безопасностью. Важность и сложность проблемы информационной безопасности	**по источнику знаний:** лекция, чтение, конспектирование **по назначению:** приобретение знаний, анализ, закрепление, проверка знаний **по типу познавательной деятельности**: объяснительно-иллюстративный, репродуктивный	Домашние задания	Учебники, учебные пособия, первоисточники	ОПК-7: Способность определять информационные ресурсы, подлежащие защите, угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты.
Угрозы информационной безопасности в информационных системах Основные определения и критерии классификации угроз. Основные угрозы доступности. Основные угрозы целостности. Основные угрозы конфиденциальности. Вредительские программы	**по источнику знаний:** лекция, чтение, конспектирование **по назначению:** приобретение знаний, анализ, закрепление, проверка знаний **по типу познавательной деятельности**: объяснительно-иллюстративный, репродуктивный	Самостоятельная работа обучающегося, домашние задания	Учебники, учебные пособия	ПК-4 способность участвовать в работах по реализации политики информационной безопасности, применять комплексный подход к обеспечению информационной безопасности объекта защиты.

Оценочные стандарты в информационной безопасности Роль стандартов ИБ. «Оранжевая книга» как оценочный стандарт. Международный стандарт ISO/IEC 15408. Критерии оценки безопасности информационных систем.				
Стандарты управления информационной безопасностью Стандарты управления информационной безопасностью BS 7799 и ISO/IEC 17799. Их основные положения. Международный стандарт ISO/IEC 27001:2005 "Системы управления информационной безопасности. Требования". Сертификация СУИБ на соответствие ISO 27001.	**по источнику знаний:** лекция, чтение, конспектирование **по назначению:** приобретение знаний, анализ, закрепление, проверка знаний **по типу познавательной деятельности**: объяснительно-иллюстративный, репродуктивный	Домашние задания	Учебники, учебные пособия, первоисточники	ПК-13 способность принимать участие в формировании, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации.
Создание СУИБ на предприятии Этапы разработки и внедрения системы управления ИБ. Содержание этапов разработки и внедрения системы управления ИБ.	**по источнику знаний:** лекция, чтение, конспектирование **по назначению:** приобретение знаний, анализ, закрепление, проверка знаний **по типу познавательной деятельности**: объяснительно-иллюстративный,	Самостоятельная работа обучающегося, домашние задания	Учебники, учебные пособия, раздаточный материал	ОПК-7: Способность определять информационные ресурсы, подлежащие защите, угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты.

	репродуктивный			
Правовые меры обеспечения информационной безопасности Основные направления обеспечения информационной безопасности. Законодательно-правовая база обеспечения информационной безопасности на предприятии.	**по источнику знаний:** лекция, чтение, конспектирование **по назначению:** приобретение знаний, анализ, закрепление, проверка знаний **по типу познавательной деятельности**: объяснительно-иллюстративный, репродуктивный	Самостоятельная работа обучающегося, домашние задания	Учебники, учебные пособия, , раздаточный материал	ПК-4 способность участвовать в работах по реализации политики информационной безопасности, применять комплексный подход к обеспечению информационной безопасности объекта защиты.
Нормативные акты предприятия по информационной безопасности. Формы правовой защиты информации на предприятии. Другие документы предприятия, в которых отражаются вопросы обеспечения информационной безопасности	**по источнику знаний:** лекция, чтение, конспектирование **по назначению:** приобретение знаний, анализ, закрепление, проверка знаний **по типу познавательной деятельности**: объяснительно-иллюстративный, репродуктивный	Самостоятельная работа обучающегося, домашние задания	Учебники, учебные пособия	ПК-13 способность принимать участие в формировании, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации.
Организационные меры обеспечения безопасности компьютерных информационных систем. Общие положения организационной защиты. Особенности организационной защиты компьютерных	**по источнику знаний:** лекция, чтение, конспектирование **по назначению:** приобретение знаний, анализ, закрепление, проверка знаний **по типу познавательной**	Домашние задания	Учебники, учебные пособия, первоисточники	ОПК-7: Способность определять информационные ресурсы, подлежащие защите, угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей

информационных систем и сетей. Служба безопасности предприятия.	**деятельности**: объяснительно-иллюстративный, репродуктивный			функционирования объекта защиты.
Программно-технические меры обеспечения информационной безопасности. Идентификация, аутентификация, управление доступом. Основные программно-технические меры. Идентификация и аутентификация.	**по источнику знаний:** лекция, чтение, конспектирование **по назначению:** приобретение знаний, анализ, закрепление, проверка знаний **по типу познавательной деятельности**: объяснительно-иллюстративный, репродуктивный	Самостоятельная работа обучающегося, домашние задания	Учебники, учебные пособия, раздаточный материал	ПК-4 способность участвовать в работах по реализации политики информационной безопасности, применять комплексный подход к обеспечению информационной безопасности объекта защиты.
Протоколирование и аудит, шифрование, контроль целостности. Протоколирование и аудит. Активный аудит. Шифрование. Контроль целостности. Цифровые сертификаты	**по источнику знаний:** лекция, чтение, конспектирование **по назначению:** приобретение знаний, анализ, закрепление, проверка знаний **по типу познавательной деятельности**: объяснительно-иллюстративный, репродуктивный	Самостоятельная работа обучающегося, домашние задания	Учебники, учебные пособия, , раздаточный материал	ПК-13 способность принимать участие в формировании, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации.

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
Microsoft Office Word 2010 Номер продукта 14.0.6024.1000 SP1 MSO 02260-018-0000106-48095
Операционная система Windows Договор от 26.05.2020 № 32009117096 Договор от 17.01.2019 № 31908696765
Офисный пакет Microsoft office 2016 Договор от 26.05.2020 № 32009117096 Договор от 17.01.2019 № 31908696765

10.2. Перечень необходимых информационных справочных систем:

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

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

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

Название
(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
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/
Лаборатория Касперского : официальный сайт. – Москва, 2019. - . – URL: https://www.kaspersky.ru/. – Текст: электронный.Самый популярный в России и крупнейший в Европе производитель систем защиты от вирусов, спама и хакерских атак. Компания входит в четвёрку ведущих мировых производителей программных решений для обеспечения информационной безопасности. https://www.kaspersky.ru/
InformationSecurity. Информационная безопасность : [сайт]. – Москва, 2019. – URL: http://www.itsec.ru/news. - Текст: электронный.Портал об информационной безопасности: новости, форум, программные новинки, архив изданий по информационной безопасности. http://www.itsec.ru/news

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

Наименования специальных помещений и помещений для самостоятельной работы	Оснащенность специальных помещений и помещений для самостоятельной работы	Перечень лицензионного программного обеспечения. Реквизиты подтверждающего документа
Лаборатория 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, MicrosoftSQLServerExpressEdition, MicrosoftVisioProfessional, MicrosoftVisualStudio, MySQLInstallerforWindows, NetBeans, SQLServerManagementStudio, MicrosoftSQLServerJavaConnector, AndroidStudio, IntelliJIDEA.	