Министерство науки и высшего образования РФ

Федеральное государственное бюджетное образовательное учреждение высшего образования

«Дагестанский государственный технический университет»

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

Дисциплина Управление информационной безопасностью
наименование дисциплины по ОПОП

для специальности 10.05.03 Информационная безопасность автоматизированных систем
код и полное наименование специальности

по специализации Безопасность открытых информационных систем

факультет Компьютерных технологий, вычислительной техники и энергетики
наименование факультета, где ведется дисциплина

кафедра Информационная безопасность
наименование кафедры, за которой закреплена дисциплина

Форма обучения очная курс 5 семестр (ы) А
очная, очно-заочная, заочная

г. Махачкала 2021

Программа составлена в соответствии с требованиями ФГОС ВО по специальности 10.05.03 Информационная безопасность автоматизированных систем с учетом рекомендаций и ОПОП ВО по специальности 10.05.03 Информационная безопасность автоматизированных систем и специализации Безопасность открытых информационных систем.

Разработчик _____ Качаева Г.И., к.э.н.
подпись (ФИО уч. степень, уч. звание)

«16» 09 2021г.

Зав. кафедрой, за которой закреплена дисциплина (модуль)_____
_____ Качаева Г.И.,к.э.н.
подпись (ФИО уч. степень, уч. звание)

«20» сентября 2021 г.

Программа одобрена на заседании выпускающей кафедры Информационная безопасность от 20 сентября 2021 года, протокол № 2 .

Зав. выпускающей кафедрой по данному направлению (специальности, профилю)
_____ Качаева Г.И., к.э.н.
подпись (ФИО уч. степень, уч. звание)

«20» сентября 2021 г.

Программа одобрена на заседании Методического совета факультета Компьютерных технологий, вычислительной техники и энергетики от «18» октября 2021 г., протокол № 2

Председатель Методического совета факультета КТВТиЭ
_____ Исабекова Т.И., к.ф-м.н., доцент
подпись (ФИО уч. степень, уч. звание)

от «18» октября 2021 г.

Декан факультета _____ Юсуфов Ш.А.
подпись ФИО

Начальник УО _____ Магомаева Э.В.
подпись ФИО

И.о проректора по УР _____ Баламирзоев Н.Л.
подпись ФИО

1. Цели и задачи освоения дисциплины.

Целями освоения дисциплины (модуля) «Управление информационной безопасностью» является формирование у обучающихся знаний и практических навыков планирования, идентификации и анализа рисков, моделирование рисков, проведение мониторинга.

Задачи дисциплины: владение: специализированным программным обеспечением, пониманием структуры и системы взаимосвязи процессов управления информационной безопасностью способность и готовность к построению систему управления информационной безопасность предприятия в условиях применения современных информационных технологий.

2.Место дисциплины в структуре ОПОП

Дисциплина «Управление информационной безопасностью» относится к обязательной части учебного плана.

Предшествующими дисциплинами, формирующими начальные знания, являются: Алгебра и геометрия, Дискретная математика, Информатика, Сети и системы передачи информации, Безопасность сетей ЭВМ.

Последующими дисциплинами являются: Основы управленческой деятельности, Защита программ и данных, Организация работы администратора автоматизированных систем, Защита информации от утечки по техническим каналам, Программно-аппаратные средства защиты информации, Виртуальные частные сети.

3. Компетенции обучающегося, формируемые в результате освоения дисциплины (модуля)

В результате освоения дисциплины «Управление информационной безопасностью» студент должен овладеть следующими компетенциями: УК-1; ОПК-5; ОПК-15.

Код компетенции	Наименование компетенции	Наименование показателя оценивания (показатели достижения заданного уровня освоения компетенций)
УК-1	Способен осуществлять критический анализ проблемных ситуаций на основе системного подхода, вырабатывать стратегию действий	УК-1.1.3 знает основные источники информации о проблемных ситуация в профессиональной деятельности и подходы к критическому анализу этой информации
ОПК-5	Способен применять нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации	ОПК-5.1.7 знает основные документы по стандартизации в сфере управления ИБ
		ОПК-5.1.8 знает принципы формирования политики информационной безопасности в автоматизированных системах
		ОПК-5.1.9 знает требования информационной безопасности при эксплуатации автоматизированной системы
		ОПК-5.2.6 умеет формировать политики информационной безопасности организации
		ОПК-5.2.7 умеет выполнять полный объем работ, связанных с реализацией частных политик информационной безопасности автоматизированной системы

ОПК-15	Способен осуществлять администрирование и контроль функционирования средств и систем защиты информации автоматизированных систем, инструментальный мониторинг защищенности автоматизированных систем	ОПК-15.1.3 знает программные средства, позволяющие вести автоматизированный аудит
		ОПК-15.2.6 умеет осуществлять выбор и обоснование критериев эффективности функционирования защищенных автоматизированных информационных систем
		ОПК-15.2.7 умеет разрабатывать предложения по совершенствованию системы управления информационной безопасностью автоматизированной системы

4. Объем и содержание дисциплины (модуля)

Форма обучения	**очная**	**очно-заочная**	**заочная**
Общая трудоемкость по дисциплине (ЗЕТ/ в часах)	4/144		
Семестр	А		
Лекции, час	51		
Практические занятия, час	-		
Лабораторные занятия, час	34		
Самостоятельная работа, час	23		
Курсовой проект (работа), РГР, семестр	А		
Зачет (при заочной форме **4 часа** отводится на контроль)	-		
Часы на экзамен (при очной, очно-заочной формах **1 ЗЕТ – 36 часов**, при заочной форме **9 часов** отводится на контроль)	**36**		

4.1.Содержание дисциплины (модуля) «Управление информационной безопасностью»

№ п/п	Раздел дисциплины, тема лекции и вопросы	Очная форма				Очно-заочная форма				Заочная форма			
		ЛК	ПЗ	ЛБ	СР	ЛК	ПЗ	ЛБ	СР	ЛК	ПЗ	ЛБ	СР
1	**Лекция №1 Тема: «Основы построения систем обеспечения информационной безопасности на предприятии»** Деятельность по обеспечению информационной безопасности. Предметная направленность деятельности по обеспечению информационной безопасности. Цель деятельности по обеспечению информационной безопасности. Принципы и форма деятельности по обеспечению информационной безопасности. Методы деятельности по обеспечению информационной безопасности. Средства обеспечения информационной безопасности. Субъекты обеспечения информационной безопасности.	2	-	1	1								
2	**Лекция №2 Тема: «Стандартизация систем и процессов управления информационной безопасностью»** Серия стандартов ISO/IEC. Стандарты на отдельные процессы управлении ИБ и оценку безопасности ИТ. Общие критерии и методология оценки безопасности информационных технологий. Рекомендации по аудиту систем менеджмента. Законы о Банке России. . Защита информации финансовых организаций. Методика оценки соответствия (оценка соответствия уровней защиты). Отраслевые стандарты в области управления ИБ - стандарты Банка России, рекомендации Банка России и положения Банка России по защите информации.	2		1	1								

3	**Лекция № 3 Тема: «Обеспечение информационной безопасности бизнеса»** Информационная сущность бизнеса. Роль руководства организации в обеспечении информационной безопасности. Определение информационной безопасности. Правовая среда бизнеса и ее свойства. Внутренняя нормативная база организации.	2	-	1									
4	**Лекция № 4 Тема: «Обеспечение информационной безопасности бизнеса»** . Модель информационной безопасности бизнеса. Обобщенная модель распределения ресурсов организации в условиях рисков. Ущерб и негативные последствия. Риск- ориентированный подход к обеспечению информационной безопасности бизнеса. Общая модель обеспечения ИБ бизнеса.	2	-	1	1								
5	**Лекция № 5 Тема: «Система управления информационной безопасностью бизнеса»** Модели непрерывного совершенствования и корпоративное управление. Модели непрерывного совершенствования и международные стандарты. Шаги реализации стандартной системы управления информационной безопасностью организации. Модели COSO, COBIT, ITIL. Контроль и аудит.	2	-	1	1								
6	**Лекция № 6 Тема: «Анализ объекта защиты»** Технология анализа объекта защиты. Типы информационных систем. Методы оценки ущерба от реализации угроз информационной безопасности. Комплекс стандартов в области информационной безопасности.	2	-	1	1								

7	**Лекция № 7 Тема: «Анализ и оценка управленческих и экономических показателей системы управления информационной безопасностью бизнеса»** Способы оценки информационной безопасности. Основные элементы процесса оценки информационной безопасности. Способы измерения атрибутов объекта оценки информационной безопасности.	2	-	1									
8	**Лекция № 8 Тема: «Анализ и оценка управленческих и экономических показателей системы управления информационной безопасностью бизнеса»** Применение типовых моделей оценки на основе оценки процессов и уровней зрелости процессов для оценки информационной безопасности. Модель оценки информационной безопасности на основе оценки процессов. Риск-ориентированная оценка информационной безопасности.	2	-	1	1								
9	**Лекция № 9 Тема: «Модель угроз и модель нарушителя»** Подходы к формированию модели нарушителя и модели угроз. Требования регуляторов к формированию модели нарушителя и модели угроз.	2	-	2	1								
10	**Лекция № 10 Тема: «Социальные аспекты системы управления информационной безопасностью бизнеса»** Формализованное представление угроз ИБ от персонала. Общая характеристика угроз ИБ от персонала. Формализованное представление угроз ИБ от персонала.	2	-	1									
11	**Лекция № 11 Тема: «Социальные аспекты системы управления информационной безопасностью бизнеса»** Противодействие угрозам ИБ от персонала. Социальные аспекты угроз ИБ от персонала. Личность злоумышленника.	2	-	1	1								

12	**Лекция № 12 Тема: «Методы управления информационными рисками».** Рискообразующие факторы. Структура информационного риска. Понятие «Риск информационной безопасности». Методика анализа риска информационной безопасности. Обработка рисков информационной безопасности. Процесс «Управление рисками информационной безопасности».	2	-	1	1								
13	**Лекция № 13 Тема: «Анализ влияния информационного риска на деятельность организации»** Место управления рисками информационной безопасности в структуре управления операционными рисками организации. Место управления рисками информационной безопасности в структуре управления информационной безопасностью организации.	2	-	2	1								
14	**Лекция № 14 Тема: «Оценка рисков информационной безопасности»** Основные положения стандартов в области управления рисками информационной безопасности.	2	-	2	1								
15	**Лекция № 15 Тема: «Планирование деятельности по обработке рисков обеспечения информационной безопасности организации»** Обработка рисков информационной безопасности. Цели управления и средства обработки рисков информационной безопасности.	2	-	1	1								
16	**Лекция № 16 Тема: «Планирование деятельности по обработке рисков обеспечения информационной безопасности организации»** Модель обработки рисков информационной безопасности ISO/IEC 27001. Понятие «критерий принятия риска». Методы трансформации рисков информационной безопасности. Анализ эффективности результатов обработки рисков.	2	-	2	1								

17	**Лекция № 17 Тема: «Система управления информационной безопасностью»** Организация управления персоналом в контексте обеспечения информационной безопасности.	2	-	1	1								
18	**Лекция № 18 Тема: «Система управления информационной безопасностью»** Организация управления персоналом в контексте обеспечения информационной безопасности.	2	-	1	1								
19	**Лекции № 19 Тема: «Политика информационной безопасности»** Понятия политики обеспечения ИБ и политики ИБ организации. Причины выработки политики ИБ. Основные требования и принципы, учитываемые при разработке и внедрении политики ИБ. Содержание политики ИБ: содержание корпоративной политики ИБ, содержание частных политик ИБ, примеры частных политик ИБ. Жизненный цикл политики ИБ: разработка политики ИБ, внедрение политики ИБ, применение политики ИБ, аннулирование политики ИБ, ответственность за исполнение политики ИБ. Основные положения стандартов в области регламентации обеспечения информационной безопасности.	2	-	1	1								
20	**Лекция № 20 Тема: «Инфраструктура информационной безопасности»** Безопасность доступа сторонних организаций. Идентификация рисков, связанных с подключениями сторонних организаций. Условия безопасности в контрактах, заключённых со сторонними организациями. Классификация ресурсов и их контроль. Ответственность за ресурсы. Классификация информации. Безопасность персонала. Безопасность в должностных инструкциях и при выделении ресурсов. Обучение пользователей. Реагирование на события, таящие угрозу безопасности.	2	-	2	1								

21	**Лекции № 21 Тема: «Управление инцидентами информационной безопасности»** Основные положения стандартов в области управления инцидентами информационной безопасности. Регламентация действий сотрудников при возникновении нештатных ситуаций.	2	-	1	1								
22	**Лекции № 22 Тема: «Управление инцидентами ИБ и обеспечение непрерывности бизнеса»** Нормативная база управления инцидентами ИБ и обеспечение непрерывности бизнеса. Стандарт ISO 27035 Идентификация, протоколирование, реагирование на инциденты ИБ. Влияние инцидентов ИБ на бизнес-процессы. Средства управления событиями ИБ. SOC-центры ИБ, SIEM-системы управления информацией о безопасности и событиями информационной безопасности, IRP-системы автоматизации реагирования на инциденты информационной безопасности Управление непрерывностью бизнеса организации.	2	-	1	1								
23	**Лекция № 23 Тема: «Аудит методов и средств обеспечения информационной безопасности организации»** Аудит информационной безопасности. Стандарты и практики аудита информационной безопасности. Международный стандарт ISO 19011. Методы организации, подготовки и проведения аудита информационной безопасности. Обработка результатов аудита. Место аудита информационной безопасности в структуре управления информационной безопасностью организации.	2	-	2	1								
24	**Лекция № 24 Тема: «Физическая безопасность и безопасность окружающей среды»** Защищѐнные области. Защита оборудования. Администрирование компьютерных систем и вычислительный сетей. Операционные процедуры и обязанности. Планирование систем и их приѐмка. Защита от вредоносного программного обеспечения. Обслуживание систем. Оперирование с носителями информации и их защита. Обмен данными и программами.	2	-	2	1								

25	**Лекция № 25 Тема: «Управление доступом к системам»** Производственные требования к управлению доступом к системам. Управление доступом пользователей. Обязанности пользователей. Слежение за доступом к системам и их использованием. Разработка и сопровождение информационных систем. Требования к безопасности систем. Безопасность в прикладных системах. Защита файлов прикладных систем. Безопасность в среде разработки и рабочей среде. Вопросы бесперебойной работы организации. Выполнение правовых требований. Проверка безопасности информационных систем.	2	-	1	1								
26	**Лекция № 27 Тема: «Процессы проверки системы управления ИБ и оценка деятельности по управлению ИБ»** Нормативное обеспечение проверки и оценки деятельности по управлению информационной безопасностью. Аудит СУИБ. Процесс аудита. Внутренний и внешний аудит. Аудит первой, второй и третьей сторонами. Подготовка к выполнению аудита. Подготовка и представление отчетов в устной и письменной форме о результатах аудита. Принятие решений о необходимости соответствующих последующих аудиторских проверок. Оценка деятельности по управлению информационной безопасностью.	1	-	1	1								
Форма текущего контроля успеваемости (по срокам текущих аттестаций в семестре)		Входная конт.работа 1 аттестация 1-5 тема 2 аттестация 6-10 тема 3 аттестация 11-15 тема								Входная конт.работа; Контрольная работа			
Форма промежуточной аттестации (по семестрам)		Экзамен				Зачет/ зачет с оценкой/ экзамен				Зачет/ зачет с оценкой/ экзамен			
Итого		51	-	34	23								

К видам учебной работы в вузе отнесены: лекции, консультации, семинары, практические занятия, лабораторные работы, контрольные работы, коллоквиумы, самостоятельные работы, научно- исследовательская работа, практики, курсовое проектирование (курсовая работа). Вуз может устанавливать другие виды учебных занятий.

** - Разделы, тематику и вопросы по дисциплине следует разделить на три текущие аттестации в соответствии со сроками проведения текущих аттестаций. По материалу программы, пройденному студентом после завершения 3-ей аттестации до конца семестра (2-3 недели), контроль успеваемости осуществляется при сдаче зачета или экзамена.*

4.2. Содержание лабораторных (практических) занятий

№ п/п	№ лекции из рабочей программы	Наименование лабораторного (практического, семинарского) занятия	Количество часов			Рекомендуемая литература и методические разработки (№ источника из списка литературы)
			Очно	Очно-заочно	Заочно	
1	2	3	4	5	6	7
1	№1	Основы построения систем обеспечения информационной безопасности на предприятии	1			№№ 1-7
2	№2	Стандартизация систем и процессов управления информационной безопасностью	1			№№ 1-7
3	№3	Обеспечение информационной безопасности бизнеса	2			№№ 1-7
4	№ 4	Система управления информационной безопасностью бизнеса	1			№№ 1-7
5	№5	Анализ объекта защиты	1			№№ 1-7
6	№6	Анализ и оценка управленческих и экономических показателей системы управления информационной безопасностью бизнеса	2			№№ 1-7
7	№7	Модель угроз и модель нарушителя	2			№№ 1-7
8	№8	Социальные аспекты системы управления информационной безопасностью бизнеса	2			№№ 1-7
9	№9	Методы управления информационными рисками	1			№№ 1-7
10	№10	Анализ влияния информационного риска на деятельность организации	2			№№ 1-7
11	№ 11	Оценка рисков информационной безопасности	2			№№ 1-7
12	№ 12	Планирование деятельности по обработке рисков обеспечения информационной безопасности организации	2			№№ 1-7
13	№ 13	Система управления информационной безопасностью	2			№№ 1-7
14	№ 14	Политика информационной безопасности	2			№№ 1-7
15	№ 15	Инфраструктура информационной безопасности	2			№№ 1-7

16	№ 16	Управление инцидентами информационной безопасности	2			№№ 1-7
17	№ 17	Управление инцидентами ИБ и обеспечение непрерывности бизнеса	2			№№ 1-7
18	№ 18	Аудит методов и средств обеспечения информационной безопасности организации	2			№№ 1-7
19	№19	Физическая безопасность и безопасность окружающей среды	1			№№ 1-7
20	№20	Управление доступом к системам	1			№№ 1-7
21	№21	Процессы проверки системы управления ИБ и оценка деятельности по управлению ИБ	1			№№ 1-7
ИТОГО			34			

4.3. Тематика для самостоятельной работы студента

№ п/п	Тематика по содержанию дисциплины, выделенная для самостоятельного изучения	Количество часов из содержания дисциплины			Рекомендуемая литература и источники информации	Формы контроля СРС
		Очно	Очно-заочно	Заочно		
1	2	3	4	5	6	7
1	Основы построения систем обеспечения информационной безопасности на предприятии	1			№№ 1-7	Опрос, реферат
2	Обеспечение информационной безопасности бизнеса	1			№№ 1-7	Опрос, реферат
3	Система управления информационной безопасностью бизнеса	1			№№ 1-7	Опрос, реферат
4	Анализ объекта защиты	1			№№ 1-7	Опрос, реферат
5	Анализ и оценка управленческих и экономических показателей системы управления информационной безопасностью бизнеса	1			№№ 1-7	Опрос, реферат
6	Модель угроз и модель нарушителя	1			№№ 1-7	Опрос, реферат
7	Социальные аспекты системы управления информационной безопасностью бизнеса	1			№№ 1-7	Опрос, реферат
8	Методы управления информационными рисками. Анализ влияния информационного риска на деятельность организации	1			№№ 1-7	Опрос, реферат
9	Оценка рисков информационной безопасности»	1			№№ 1-7	Опрос,

						реферат
10	Планирование деятельности по обработке рисков обеспечения информационной безопасности организации	1			№№ 1-7	Опрос, реферат
11	Система управления информационной безопасностью	1			№№ 1-7	Опрос, реферат
12	Политика информационной безопасности	2			№№ 1-7	Опрос, реферат
13	Управление инцидентами информационной безопасности	2			№№ 1-7	Опрос, реферат
14	Инфраструктура информационной безопасности	2			№№ 1-7	Опрос, реферат
15	Аудит методов и средств обеспечения информационной безопасности организации	2			№№ 1-7	Опрос, реферат
16	Физическая безопасность и безопасность окружающей среды	2			№№ 1-7	Опрос, реферат
17	Управление доступом к системам	2			№№ 1-7	Опрос, реферат
ИТОГО		**23**				

5. Образовательные технологии

В соответствии с требованиями ФГОС ВО по специальности подготовки реализация компетентностного подхода предусматривается широкое использование в учебном процессе активных и интерактивных форм проведения занятий.

Аудиторная работа включает: лекции, практические занятия, мастер-классы, консультации.

В курсе лекций использованы наглядные, иллюстрированные материалы, обширная информация в табличной и графической формах, а также электронные ресурсы сети Интернет. Разработаны продвинутые лекции (с визуализацией) в формате презентаций, с использованием пакета прикладных программ MS Power Point.

Внеаудиторная работа призвана для формирования и развития профессиональных навыков обучающихся. Самостоятельная работа включает: выполнение домашних заданий, подготовка рефератов, участие в дискуссиях, работа в информационно-образовательной среде. В конце обучения проводится экзамен.

Удельный вес занятий, проводимых в интерактивных формах, определяется главной целью программы, особенностью контингента обучающихся и содержанием дисциплины, и в целом в учебном процессе они составляют не менее 30% аудиторных занятий.

6. Оценочные средства для текущего контроля успеваемости, промежуточной аттестации по итогам освоения дисциплины и учебно-методическое обеспечение самостоятельной работы студентов

Оценочные средства приведены в ФОС (Приложение А)

7. Учебно-методическое и информационное обеспечение дисциплины

Рекомендуемая литература и источники информации (основная и дополнительная)

Зав. библиотекой _____ **Алиева Ж.А.**

п/п	Виды занятий	Необходимая учебная, учебно-методическая (основная и дополнительная) литература, программное обеспечение и Интернет-ресурсы	Количество изданий	
			В библиотеке	На кафедре
Основная				
1.		Шилов, А. К. Управление информационной безопасностью : учебное пособие / А. К. Шилов. — Ростов-на-Дону, Таганрог : Издательство Южного федерального университета, 2018. — 120 с. — ISBN 978-5-9275-2742-7. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. —	URL: https://www.iprbookshop.ru/87643.html	
2.		Абденов, А. Ж. Современные системы управления информационной безопасностью : учебное пособие / А. Ж. Абденов, Г. А. Дронова, В. А. Трушин. — Новосибирск : Новосибирский государственный технический университет, 2017. — 48 с. — ISBN 978-5-7782-3236-5. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. —	URL: https://www.iprbookshop.ru/91427.html	
3.	лк, пз, срс	Газизов, А. Р. Управление информационной безопасностью : учебное пособие / А. Р. Газизов, С. Б. Петренкова, Д. В. Фатхи. — Ростов-на-Дону : Донской государственный технический университет, 2019. — 115 с. — ISBN 978-5-7890-1775-3. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. —	URL: https://www.iprbookshop.ru/117771.html	
Дополнительная				
4.	лк, пз, срс	Милославская, Н. Г. Управление информационной безопасностью.	URL: https://www.iprbooks	

		Конспект лекций : учебное пособие / Н. Г. Милославская, А. И. Толстой. — Москва : Национальный исследовательский ядерный университет «МИФИ», 2020. — 534 с. — ISBN 978-5-7262-2694-1. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. —	hop.ru/125513.html
5.	лк, пз, срс	Пакин, А. И. Информационная безопасность информационных систем управления предприятием : учебное пособие по части курса / А. И. Пакин. — Москва : Московская государственная академия водного транспорта, 2009. — 41 с. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. —	URL: https://www.iprbookshop.ru/46462.html
6.	лк, пз, срс	Пелешенко, В. С. Менеджмент инцидентов информационной безопасности защищенных автоматизированных систем управления : учебное пособие / В. С. Пелешенко, С. В. Говорова, М. А. Лапина. — Ставрополь : Северо-Кавказский федеральный университет, 2017. — 86 с. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. —	URL: https://www.iprbookshop.ru/69405.html
7.	лк, пз, срс	Добровольский, В. С. Управление интеллектуальной безопасностью: организационные и правовые основы информационной безопасности : учебное пособие / В. С. Добровольский. — Москва : Издательский Дом МИСиС, 2014. — 224 с. — ISBN 978-5-87623-789-7. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. —	URL: https://www.iprbookshop.ru/97872.html

8. Материально-техническое обеспечение дисциплины (модуля) «Управление информационной безопасностью»

Материально-техническое обеспечение дисциплины включает:

- библиотечный фонд (учебная, учебно-методическая, справочная экономическая литература, экономическая научная и деловая периодика);
- компьютеризированные рабочие места для обучаемых с доступом в сеть Интернет (лаборатории по автоматизированным информационным системам, оснащенные современной электронно-вычислительной техникой с соответствующим программным обеспечением);
- аудитории, оборудованные проекционной техникой.

Для проведения практических занятий используются компьютерные классы кафедры ИБ, оборудованные современными персональными компьютерами, характеристики которых не ниже:

Pentium 4, DDR 1 Gb, HDD – 150 GB, Video Card – 126 MB, CD/DVD, USB -2.

Все персональные компьютеры подключены к сети университета и имеют выход в глобальную сеть Интернет.

На компьютере предустанавливается ОС Windows XP/Vista/7 и программное обеспечение MS Office 2010, Borland C++ , Borland C++ Builder 6 и др. Приложение командной строки dumpasn1 Питера Гутмана (Peter Gutmann) для просмотра файлов формата ASN.1 BER/DER: dumpasn1.rar (Windows, x86).

8.4. Материально-техническая база, необходимая для осуществления образовательного процесса по дисциплине

При проведения лекционных и практических (семинарских) занятий предусматривается использование систем мультимедиа, программного обеспечения и информационных справочных систем:

Microsoft Office (Word, Excel, PowerPoint, Access)

ЭБС http://library.mirea.ru/.

Специальные условия инвалидам и лицам с ограниченными возможностями здоровья (ОВЗ)

Специальные условия обучения и направления работы с инвалидами и лицами с ОВЗ определены на основании:

- Федерального закона от 29.12.2012 №273-ФЗ «Об образовании в Российской Федерации»;
- Федерального закона от 24.11.1995 № 181-ФЗ «О социальной защите инвалидов в Российской Федерации»;
- приказа Минобрнауки России от 05.04.2017 № 301 «Об утверждении Порядка организации и осуществления образовательной деятельности по образовательным программам высшего образования – программам бакалавриата, программам специалитета, программам магистратуры»;
- методических рекомендаций по организации образовательного процесса для обучения инвалидов и лиц с ограниченными возможностями здоровья в образовательных организациях высшего образования, в том числе оснащенности образовательного процесса, утвержденных Минобрнауки России 08.04.2014 № АК-44/05вн).

Под специальными условиями для получения образования обучающихся с ОВЗ понимаются условия обучения, воспитания и развития, включающие в себя использование при необходимости адаптированных образовательных программ и методов обучения и воспитания, специальных учебников, учебных пособий и дидактических материалов, специальных технических средств обучения коллективного и индивидуального пользования, предоставление услуг ассистента (помощника), оказывающего необходимую помощь, проведение групповых и индивидуальных коррекционных занятий, обеспечение доступа в

здания ДГТУ и другие условия, без которых невозможно или затруднено освоение ОПОП обучающихся с ОВЗ.

Обучение в рамках учебной дисциплины обучающихся с ОВЗ осуществляется ДГТУ с учетом особенностей психофизического развития, индивидуальных возможностей и состояния здоровья таких обучающихся.

Обучение по учебной дисциплине обучающихся с ОВЗ может быть организовано как совместно с другими обучающимися, так и в отдельных группах.

В целях доступности обучения по дисциплине обеспечивается:

1) для лиц с ограниченными возможностями здоровья по зрению:

- наличие альтернативной версии официального сайта ДГТУ в сети «Интернет» для слабовидящих;

- весь необходимый для изучения материал, согласно учебному плану (в том числе, для обучающихся по индивидуальным учебным планам) предоставляется в электронном виде на диске.

- индивидуальное равномерное освещение не менее 300 люкс;

- присутствие ассистента, оказывающего обучающемуся необходимую помощь;

- обеспечение возможности выпуска альтернативных форматов печатных материалов (крупный шрифт или аудиофайлы);

- обеспечение доступа обучающегося, являющегося слепым и использующего собаку-проводника, к зданию ДГТУ.

2) для лиц с ОВЗ по слуху:

- наличие микрофонов и звукоусиливающей аппаратуры коллективного пользования (аудиоколонки);

3) для лиц с ОВЗ, имеющих нарушения опорно-двигательного аппарата, материально-технические условия должны обеспечивать возможность беспрепятственного доступа обучающихся в учебные помещения, столовые, туалетные и другие помещения организации, а также пребывания в указанных помещениях (наличие пандусов, поручней, расширенных дверных проемов и других приспособлений).

Перед началом обучения могут проводиться консультативные занятия, позволяющие студентам с ОВЗ адаптироваться к учебному процессу.

В процессе ведения учебной дисциплины научно-педагогическим работникам рекомендуется использование социально-активных и рефлексивных методов обучения, технологий социокультурной реабилитации с целью оказания помощи обучающимся с ОВЗ в установлении полноценных межличностных отношений с другими обучающимися, создании комфортного психологического климата в учебной группе.

Особенности проведения текущей и промежуточной аттестации по дисциплине для обучающихся с ОВЗ устанавливаются с учетом индивидуальных психофизических особенностей (устно, письменно на бумаге, письменно на компьютере, в форме тестирования и др.). При необходимости предоставляется дополнительное время для подготовки ответа на зачете или экзамене