

Документ подписан простой электронной подписью

Информация о владельце:

ФИО: Таныгин Максим Олегович

Должность: и.о. декана факультета фундаментальной информатики и информационных технологий

Дата подписания: 10.10.2023 15:57:04

Уникальный программный ключ:

65ab2aa0d384efe8480e6a4c688eddbc475e411a

Аннотация к рабочей программе

дисциплины «Нормативно-правовое регулирование в сфере информационной безопасности»

Цель преподавания дисциплины

Цель дисциплины – формирование у студентов знаний в области нормативно-правового регулирования в сфере информационной безопасности для решения задач профессиональной деятельности организационно-управленческого типа.

Задачи изучения дисциплины

Задачами дисциплины являются:

1. Изучение руководящих и методических документов уполномоченных федеральных органов исполнительной власти по защите информации и обеспечения безопасности критической информационной инфраструктуры.

2. Изучение процесса организации получения организацией лицензий на лицензируемые виды деятельности по производству товаров и услуг в сфере обеспечения защиты.

3. Изучение процесса согласования с уполномоченными федеральными органами исполнительной власти условий поставки средств и систем защиты.

4. Обеспечить совместно с другими дисциплинами семестра теоретическую подготовку обучающихся к производственной практике по получению умений и навыков управленческой деятельности на предприятии-заказчике.

Индикаторы компетенций, формируемые в результате освоения дисциплины

ПК-4.1 Согласовывает с уполномоченными федеральными органами исполнительной власти условия поставки средств и систем защиты

ПК-4.2 Организует и проводит аттестацию средств и систем защиты

ПК-4.3 Формирует отчёты по изменению за выбранный период времени требований нормативных правовых актов, руководящих и методических документов, предъявляемых к системам защиты информации

ПК-5.1 Определяет перечень объектов информатизации и информации (сведений) ограниченного доступа, подлежащих защите

ПК-5.2 Выявляет степень участия персонала в обработке защищаемой информации

ПК-5.3 Разрабатывает отчетные документы и разделы технических заданий

Разделы дисциплины

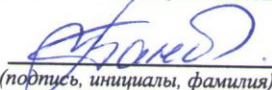
Информация, информационные системы как объект правового регулирования информационной безопасности. Правовая основа допуска и доступа персонала к защищаемым сведениям. Правовые основы защиты коммерческой тайны. Компьютерная информация – как объект информатизации. Лицензирование в области защиты информации. Сертификация в области защиты информации. Система правовой ответственности за утечку информации и утрату носителей информации. Правовые основы деятельности подразделений защиты информации. Правовые основы защиты персональных данных.

МИНОБРНАУКИ РОССИИ

Юго-Западный государственный университет

УТВЕРЖДАЮ:

Декан факультета ФиПИ

 Таныгин М.О.
(подпись, инициалы, фамилия)

« 30 » мая 20 23 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Нормативно-правовое регулирование в сфере информационной безопасности
(наименование дисциплины)

ОПОП ВО 10.04.01 Информационная безопасность,
(шифр и наименование направления подготовки)

направленность (профиль) «Защищенные информационные системы»
(наименование направленности (профиля))

форма обучения _____ очная

ОПОП ВО реализуется по модели дуального обучения

Курск – 2023

Рабочая программа дисциплины составлена:

– в соответствии с ФГОС ВО – магистратура по направлению подготовки 10.04.01 Информационная безопасность, утвержденным приказом Минобрнауки России от 26.11.2020 г. № 1455;

– на основании учебного плана ОПОП ВО 10.04.01 Информационная безопасность, направленность (профиль) «Защищенные информационные системы», одобренного Ученым советом университета (протокол № 12 от 29.05.2023).

– с учетом заказа-требования от 28.04.2023 на результаты освоения ОПОП ВО – программы магистратуры 10.04.01 Информационная безопасность, направленность (профиль) «Защищенные информационные системы», реализуемой по модели дуального обучения в ФГБОУ ВО «Юго-Западный государственный университет», от ООО ЦСБ «ЦИТ-ИНФОРМ»

(наименование предприятия (организации))

(приложение к общей характеристике ОПОП ВО).

Рабочая программа дисциплины обсуждена и рекомендована к реализации в образовательном процессе для дуального обучения студентов по ОПОП ВО 10.04.01 Информационная безопасность, направленность (профиль) «Защищенные информационные системы» на совместном заседании кафедры информационной безопасности

(наименование кафедры)

с представителями ООО ЦСБ «ЦИТ-ИНФОРМ»

(наименование предприятия (организации))

(протокол № 8 от 29. 05. 2023).

Зав. кафедрой

 А.Л. Марухленко

Разработчик программы
к.т.н.

 Е.А. Кулешова

/ Директор научной библиотеки

 В.Г. Макаровская

Рабочая программа дисциплины пересмотрена, обсуждена и рекомендована к реализации в образовательном процессе на основании учебного плана ОПОП ВО дуального обучения 10.04.01 Информационная безопасность, направленность (профиль) «Защищенные информационные системы», одобренного Ученым советом университета (протокол № __ от __. __. 20 __), на совместном заседании кафедры информационной безопасности

(наименование кафедры)

с представителями ООО ЦСБ «ЦИТ-ИНФОРМ»

(наименование предприятия (организации))

(протокол № __ от __. __. 20 __).

Зав. кафедрой _____

1 Цель и задачи дисциплины. Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения основной профессиональной образовательной программы

1.1 Цель дисциплины

Цель дисциплины – формирование у студентов знаний в области нормативно-правового регулирования в сфере информационной безопасности для решения задач профессиональной деятельности организационно-управленческого типа.

1.2 Задачи дисциплины

Задачами дисциплины являются:

1. Изучение руководящих и методических документов уполномоченных федеральных органов исполнительной власти по защите информации и обеспечения безопасности критической информационной инфраструктуры.

2. Изучение процесса организации получения организацией лицензий на лицензируемые виды деятельности по производству товаров и услуг в сфере обеспечения защиты.

3. Изучение процесса согласования с уполномоченными федеральными органами исполнительной власти условий поставки средств и систем защиты.

4. Обеспечить совместно с другими дисциплинами семестра теоретическую подготовку обучающихся к производственной практике по получению умений и навыков управленческой деятельности на предприятии-заказчике.

1.3 Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения основной профессиональной образовательной программы

Таблица 1.3 – Результаты обучения по дисциплине

<i>Планируемые результаты освоения основной профессиональной образовательной программы (компетенции, закрепленные за дисциплиной)</i>		<i>Код и наименование индикатора достижения компетенции, закрепленного за дисциплиной</i>	<i>Планируемые результаты обучения по дисциплине, соотнесенные с индикаторами достижения компетенций</i>
<i>код компетенции</i>	<i>наименование компетенции</i>		
ПК-4	Способен управлять отношениями с регуляторами в сфере защиты информации	ПК-4.1 Согласовывает с уполномоченными федеральными органами исполнительной власти условия поставки средств и систем защиты	Знать: руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации и обеспечения безопасности критической информационной инфраструктуры

<i>Планируемые результаты освоения основной профессиональной образовательной программы (компетенции, закрепленные за дисциплиной)</i>		<i>Код и наименование индикатора достижения компетенции, закрепленного за дисциплиной</i>	<i>Планируемые результаты обучения по дисциплине, соотнесенные с индикаторами достижения компетенций</i>
<i>код компетенции</i>	<i>наименование компетенции</i>		
			<p>Уметь: организовывать получение организацией лицензий на лицензируемые виды деятельности по производству товаров и услуг в сфере обеспечения защиты</p> <p>Владеть (или Иметь опыт деятельности): согласование с уполномоченными федеральными органами исполнительной власти условий поставки средств и систем защиты</p>
		ПК-4.2 Организует и проводит аттестацию средств и систем защиты	<p>Знать: порядок аттестации ЗТКС на соответствие требованиям защиты информации</p> <p>Уметь: организовывать получение эксплуатирующей ЗТКС организацией разрешительных документов в соответствии с требованиями нормативных правовых актов</p> <p>Владеть (или Иметь опыт деятельности): организация и проведение аттестации ЗТКС в соответствии с требованиями нормативных правовых актов</p>
		ПК-4.3 Формирует отчёты по изменению за выбранный период времени требований нормативных правовых актов, руководящих и методических документов, предъявляемых к системам защиты информации	<p>Знать: нормативные правовые акты в области связи, информатизации и защиты информации</p> <p>Уметь: проводить мониторинг и анализ нормативных правовых актов, руководящих и методических документов уполномоченных федеральных органов исполнительной власти</p> <p>Владеть (или Иметь опыт деятельности):</p>

<i>Планируемые результаты освоения основной профессиональной образовательной программы (компетенции, закрепленные за дисциплиной)</i>		<i>Код и наименование индикатора достижения компетенции, закрепленного за дисциплиной</i>	<i>Планируемые результаты обучения по дисциплине, соотнесенные с индикаторами достижения компетенций</i>
<i>код компетенции</i>	<i>наименование компетенции</i>		
			мониторинг нормативных правовых актов, руководящих и методических документов уполномоченных федеральных органов исполнительной власти в сфере защиты СССЭ от НД и обеспечения безопасности критической информационной инфраструктуры
ПК-5	Способен обеспечить документальное сопровождение процесса обеспечения информационной безопасности	ПК-5.1 Определяет перечень объектов информатизации и информации (сведений) ограниченного доступа, подлежащих защите	<p>Знать: основные информационные технологии, используемые в автоматизированных системах, основные угрозы безопасности информации и модели нарушителя в автоматизированных системах</p> <p>Уметь: анализировать цели создания автоматизированных систем и задачи, решаемые автоматизированными системами</p> <p>Владеть (или Иметь опыт деятельности): анализ характера обрабатываемой информации и определение перечня информации, подлежащей защите</p>
		ПК-5.2 Выявляет степень участия персонала в обработке защищаемой информации	<p>Знать: принципы формирования политики информационной безопасности в автоматизированных системах, организационные меры по защите информации</p> <p>Уметь: определять класс защищенности автоматизированных систем и ее составных частей</p> <p>Владеть (или Иметь опыт деятельности): выявление степени участия</p>

<i>Планируемые результаты освоения основной профессиональной образовательной программы (компетенции, закрепленные за дисциплиной)</i>		<i>Код и наименование индикатора достижения компетенции, закрепленного за дисциплиной</i>	<i>Планируемые результаты обучения по дисциплине, соотнесенные с индикаторами достижения компетенций</i>
<i>код компетенции</i>	<i>наименование компетенции</i>		
			персонала в обработке защищаемой информации
		ПК-5.3 Разрабатывает отчетные документы и разделы технических заданий	<p>Знать: нормативные правовые акты в области защиты информации, методы защиты информации от несанкционированного доступа и утечки по техническим каналам, программно-аппаратные средства обеспечения защиты информации в программном обеспечении автоматизированных систем</p> <p>Уметь: организовывать работы по созданию, внедрению, проектированию, разработке и сопровождению защищенных автоматизированных систем</p> <p>Владеть (или Иметь опыт деятельности): разработка отчетных документов и разделов технических заданий</p>

2 Указание места дисциплины в структуре основной профессиональной образовательной программы

Дисциплина «Нормативно-правовое регулирование в сфере информационной безопасности» входит в часть, формируемую участниками образовательных отношений, блока 1 «Дисциплины (модули)» основной профессиональной образовательной программы – программы магистратуры 10.04.01 Информационная безопасность, направленность (профиль) «Защищенные информационные системы», реализуемой по модели дуального обучения.

Дисциплина изучается на 1 курсе в 1 семестре.

Дисциплина имеет практико-ориентированный характер и изучается до прохождения обучающимися производственной практики по получению умений и навыков управленческой деятельности, завершающей данный учебный год.

3 Объем дисциплины в зачетных единицах с указанием количества академических или астрономических часов, выделенных на контактную работу обучающихся с преподавателем (по видам учебных занятий) и на самостоятельную работу обучающихся

Общая трудоемкость (объем) дисциплины составляет 3 зачетные единицы (з.е.), 108 академических часов.

Таблица 3 – Объем дисциплины

Виды учебной работы	Всего, часов
Общая трудоемкость дисциплины	108
Контактная работа обучающихся с преподавателем по видам учебных занятий (всего)	54
в том числе:	
лекции	18
лабораторные занятия	не предусмотрены
практические занятия	36, из них практическая подготовка обучающихся – 4.
Самостоятельная работа обучающихся (всего)	53.9
Контроль (подготовка к экзамену)	не предусмотрен
Контактная работа по промежуточной аттестации (всего АттКР)	0,1
в том числе:	
зачет	0,1
зачет с оценкой	не предусмотрен
курсовая работа (проект)	не предусмотрен(-а)
экзамен (включая консультацию перед экзаменом)	не предусмотрен

4 Содержание дисциплины, структурированное по темам (разделам) с указанием отведенного на них количества академических часов и видов учебных занятий

4.1 Содержание дисциплины

Таблица 4.1.1 – Содержание дисциплины, структурированное по темам (разделам)

№ п/п	Раздел (тема) дисциплины	Содержание
1	2	3
1	Информация, информационные системы как объект правового регулирования информационной безопасности	Информация и информационные системы как объект правоотношений в сфере обеспечения информационной безопасности. Понятие и виды защищаемой информации по законодательству Российской Федерации. Анализ и оценка угроз информационной безопасности объекта. Оценка ущерба на примере ООО ЦСБ «ЩИТ-ИНФОРМ».
2	Правовая основа до-	Понятие о доступе к государственным информационным ре-

	пуска и доступа персонала к защищаемым сведениям	сурсам. Правовая защита информации и информационных ресурсов. Правовые режимы конфиденциальной информации. Правовая защита государственных информационных ресурсов. Система защиты государственной тайны на примере ООО ЦСБ «ЩИТ-ИНФОРМ».
3	Правовые основы защиты коммерческой тайны	Понятие коммерческой тайны как правовой категории. Определение сведений, составляющих коммерческую тайну. Объекты защиты коммерческой тайны. Правовое регулирование взаимоотношений администрации и персонала в области защиты информации на примере ООО ЦСБ «ЩИТ-ИНФОРМ»
4	Компьютерная информация – как объект информатизации	Понятие и классификация видов компьютерных правонарушений. Криминалистические характеристики компьютерных преступлений. Криминалистические аспекты проведения расследования преступлений в сфере компьютерной информации. Особенности проведения экспертизы в области компьютерной информации на примере ООО ЦСБ «ЩИТ-ИНФОРМ».
5	Лицензирование в области защиты информации	Основные понятия и организационная структура системы государственного лицензирования. Порядок лицензирования на примере ООО ЦСБ «ЩИТ-ИНФОРМ». Проведение специальной экспертизы предприятия на примере ООО ЦСБ «ЩИТ-ИНФОРМ». Порядок приостановления или аннулирования действия лицензии на примере ООО ЦСБ «ЩИТ-ИНФОРМ»
6	Сертификация в области защиты информации	Система сертификации средств защиты информации. Особенности сертификации средств защиты информации по требованиям безопасности на примере ООО ЦСБ «ЩИТ-ИНФОРМ»
7	Система правовой ответственности за утечку информации и утрату носителей информации	Понятие, виды норм и условия применения юридической ответственности за нарушение правовых норм в области защиты информации. Уголовная ответственность за нарушение правовых норм в сфере защищаемой информации. Административная ответственность за нарушения правовых норм в сфере защищаемой информации. Особенности юридической ответственности за нарушение норм информационной безопасности в области трудовых и гражданско-правовых отношений на примере ООО ЦСБ «ЩИТ-ИНФОРМ»
8	Правовые основы деятельности подразделений защиты информации	Правовая регламентация охранной деятельности. Служба безопасности объекта. Формы, средства и методы защиты объекта. Организация и обеспечение режима секретности на примере ООО ЦСБ «ЩИТ-ИНФОРМ». Организация пропускного и внутриобъектового режима на примере ООО ЦСБ «ЩИТ-ИНФОРМ»
9	Правовые основы за-	Понятие и виды персональных данных. Государственное ре-

щиты персональных данных	гулирование и правовой режим персональных данных ³ . Права и обязанности субъектов в области защиты персональных данных. Классификация информационных систем персональных данных на примере ООО ЦСБ «ЦИТ-ИНФОРМ». Принципы и особенности обработки персональных данных. Требования по обеспечению безопасности персональных данных на примере ООО ЦСБ «ЦИТ-ИНФОРМ». Ответственность за нарушение законодательства в области персональных данных
--------------------------	--

Таблица 4.1.2 – Содержание дисциплины и его методическое обеспечение

№ п/п	Раздел, темы дисциплины	Виды деятельности			Учебно-методические материалы	Формы текущего контроля успеваемости (по неделям семестра)	Компетенции
		№ лек., час	№ лаб.	№ пр.			
1	2	3	4	5	6	7	8
1	Информация, информационные системы как объект правового регулирования информационной безопасности	2	-	-	У-1-5 МУ- 1,2	УО, КЗ 1	ПК-4 ПК-5
2	Правовая основа допуска и доступа персонала к защищаемым сведениям	2	-	1	У-1-5 МУ- 1,2	УО, ПР 2-3	ПК-4 ПК-5
3	Правовые основы защиты коммерческой тайны	2	-	2	У-1-5 МУ- 1,2	УО, ПР 4-5	ПК-4 ПК-5
4	Компьютерная информация – как объект информатизации	2	-	-	У-1-5 МУ- 1,2	УО, КЗ, ПЗ 6	ПК-4 ПК-5
5	Лицензирование в области защиты информации	2	-	3	У-1-5 МУ- 1,2	УО, ПР, КЗ 7-8	ПК-4 ПК-5
6	Сертификация в области защиты информации	2	-	4	У-1-5 МУ- 1,2	УО, ПР 9-10	ПК-4 ПК-5
7	Система правовой ответственности за утечку информации и утрату носителей информации	2	-	5	У-1-5 МУ- 1,2	УО, ПР 10-11	ПК-4 ПК-5

8	Правовые основы деятельности подразделений защиты информации	2	-	-	У-1-5 МУ- 1,2	УО, КЗ 12	ПК-4 ПК-5
9	Правовые основы защиты персональных данных	2	-	6	У-1-5 МУ- 1,2	УО, ПР, КЗ 13-14	ПК-4 ПК-5
	Итого	18	-	-			

УО – устный опрос, ПР – защита практической работы, КЗ – кейс-задача, ПЗ - решение производственных задач.

4.2 Лабораторные работы и (или) практические занятия

4.2.1 Практические работы

Таблица 4.2.1 – Практические работы

№	Наименование практической работы	Объем, час.
1	2	3
1	Организационно-правовые механизмы обеспечения информационной безопасности	6
2	Технические средства защиты информации	6
3	Защита персональных данных	6
4	Разработка организационно-распорядительной документации для объекта информатизации	6, из них практическая подготовка обучающихся – 4
5	Анализ эффективности применения средств защиты информации на объекте информатизации	6
6	Разработка модели угроз информационной безопасности	6
Итого		36, из них практическая подготовка обучающихся – 4

4.3 Самостоятельная работа студентов (СРС)

Таблица 4.3 – Самостоятельная работа студентов

№ раздела (темы)	Наименование раздела (темы) дисциплины	Срок выполнения	Время, затрачиваемое на выполнение СРС, час
1	2	3	4
1.	Информация, информационные системы как объект правового регулирования информационной безопасности	1-2 неделя	6
2.	Правовая основа допуска и доступа персонала к защищаемым сведениям	3-4 неделя	6
3.	Правовые основы защиты коммерческой тайны	5-6 неделя	6
4.	Компьютерная информация – как объект информатизации	7-8 неделя	6
5.	Лицензирование в области защиты информации	9-10 неделя	6
6.	Сертификация в области защиты информации	11 неделя	6
7.	Система правовой ответственности за утечку информации и утрату носителей информации	12 неделя	6
8.	Правовые основы деятельности подразделений защиты информации	13 неделя	6
9.	Правовые основы защиты персональных данных	14 неделя	5,9
Итого			53,9

5 Перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине

При самостоятельном изучении отдельных тем и вопросов дисциплины студенты могут пользоваться учебно-наглядными пособиями, учебным оборудованием и методическими разработками кафедры *информационной безопасности* в рабочее время, установленное Правилами внутреннего распорядка работников университета.

Учебно-методическое обеспечение самостоятельной работы обучающихся по данной дисциплине организуется:

библиотекой университета:

- библиотечный фонд укомплектован учебной, методической, научной, периодической, справочной и художественной литературой в соответствии с учебным планом и данной РПД;

- имеется доступ к основным информационным образовательным ресурсам, информационной базе данных, в том числе библиографической, возможность выхода в Интернет.

кафедрой:

- путем обеспечения доступности всего необходимого учебно-методического и справочного материала;
- путем предоставления сведений о наличии учебно-методической литературы, современных программных средств.

- путем разработки:
 - методических рекомендаций, пособий по организации самостоятельной работы студентов;
 - методических указаний к выполнению практических работ и т.д.

типографией университета:

- посредством оказания помощи авторам в подготовке и издании научной, учебной и методической литературы;
- посредством удовлетворения потребности в тиражировании научной, учебной и методической литературы.

6 Образовательные технологии. Практическая подготовка обучающихся

Реализация программы магистратуры по модели дуального обучения и компетентностного подхода предусматривают широкое использование в образовательном процессе активных и интерактивных форм проведения занятий в сочетании с внеаудиторной работой с целью формирования профессиональных компетенций обучающихся.

Таблица 6.1 – Интерактивные образовательные технологии, используемые при проведении аудиторных занятий

№	Наименование раздела (темы лекции, практического или лабораторного занятия)	Используемые интерактивные образовательные технологии	Объем, час.
1	2	3	4
1	Организационно-правовые механизмы обеспечения информационной безопасности	<i>кейс-технология</i>	4
2	Разработка организационно-распорядительной документации для объекта информатизации	<i>кейс-технология</i>	4
3	Анализ эффективности применения средств защиты информации на объекте информатизации	<i>кейс-технология</i>	4
4	Разработка модели угроз информационной безопасности	<i>кейс-технология</i>	6
Итого:			18

Практическая подготовка обучающихся при реализации дисциплины осуществляется путем проведения практических занятий, предусматривающих участие обучающихся в выполнении отдельных элементов работ, связанных с будущей профессиональной деятельностью и направленных на формирование, закрепление, развитие практических навыков и компетенций по направленности (профилю) программы магистратуры.

Практическая подготовка обучающихся при реализации дисциплины организуется в модельных условиях (оборудованных в подразделениях университета на кафедре информационной безопасности).

Практическая подготовка обучающихся проводится в соответствии с положением П 02.181.

7 Фонд оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине

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

Таблица 7.1 – Этапы формирования компетенций

Код и наименование компетенции	Этапы ¹ формирования компетенций и дисциплины (модули), практики, при изучении которых формируется данная компетенция		
	начальный	основной	завершающий
1	2	3	4
ПК-4 Способен управлять отношениями с регуляторами в сфере защиты информации	Организация аудита информационной безопасности Нормативно-правовое регулирование в сфере информационной безопасности	Производственная практика по получению умений и навыков управленческой деятельности	Методы и средства защиты информации в системах электронного документооборота Управление разработкой систем безопасности Производственная преддипломная практика
ПК-5 Способен обеспечивать документальное сопровождение процесса обеспечения информационной безопасности	Организация работ по обеспечению безопасности в информационных системах Организация аудита информационной безопасности Нормативно-правовое регулирование в сфере информационной безопасности	Производственная практика по получению умений и навыков управленческой деятельности	Производственная преддипломная практика

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

Таблица 7.2 – Показатели и критерии оценивания компетенций, шкала оценивания

Код компетенции/ этап (наименование этапа по таблице 6.1)	Показатели оценивания компетенций (индикаторы достижения компетенций, закреплённые за практикой)	Критерии и шкала оценивания компетенций			
		Недостаточный уровень («неудовл.»)	Пороговый уровень («удовл.»)	Продвинутый уровень («хорошо»)	Высокий уровень («отлично»)
1	2	3	4	5	6
ПК-4/ основной	<p>ПК-4.1 Согласовывает с уполномоченными федеральными органами исполнительной власти условия поставки средств и систем защиты</p> <p>ПК-4.2 Организует и проводит аттестацию средств и систем защиты</p> <p>ПК-4.3 Формирует отчёты по изменению за выбран-</p>	<p>Знать: демонстрирует менее 60% знаний, указанных в таблице 1.3 для ПК-4. Обучающийся нуждается в постоянных подсказках; допускает грубые ошибки, которые не может исправить самостоятельно.</p>	<p>Знать: демонстрирует 60-74% знаний, указанных в таблице 1.3 для ПК-4. Знания обучающегося имеют поверхностный характер, имеют место неточности и ошибки.</p>	<p>Знать: демонстрирует 75-89% знаний, указанных в таблице 1.3 для ПК-4. Обучающийся имеет хорошие, но не исчерпывающие знания; допускает неточности.</p>	<p>Знать: демонстрирует 90-100% знаний, указанных в таблице 1.3 для ПК-4. Знания обучающегося являются прочными и глубокими, имеют системный характер. Обучающийся свободно оперирует знаниями.</p>
		<p>Уметь: демонстрирует менее 60% умений, установленных в таблице 1.3 для ПК-4.</p>	<p>Уметь: в целом сформированные, но вызывающие затруднения при самостоятельном применении умения, указанные в таблице 1.3 для ПК-4.</p>	<p>Уметь: сформированные и самостоятельно применяемые умения, указанные в таблице 1.3 для ПК-4.</p>	<p>Уметь: хорошо развитые, уверенно и успешно применяемые умения, указанные в таблице 1.3 для ПК-4.</p>

	ный период времени требований нормативных правовых актов, руководящих и методических документов, предъявляемых к системам защиты информации	Владеть (или Иметь опыт деятельности): навыки, указанные в таблице 1.3 для ПК-4, не развиты.	Владеть (или Иметь опыт деятельности): навыки, указанные в таблице 1.3 для ПК-4, развиты на элементарном уровне.	Владеть (или Иметь опыт деятельности): навыки, указанные в таблице 1.3 для ПК-4, хорошо развиты.	Владеть (или Иметь опыт деятельности): навыки, указанные в таблице 1.3 для ПК-4, доведены до автоматизма.
ПК-5/ основной	ПК-5.1 Определяет перечень объектов информатизации и информации (сведений) ограниченного доступа, подлежащих защите ПК-5.2 Выявляет степень участия персонала в обработке защищаемой информации ПК-5.3 Разрабатывает отчетные документы и разделы техниче-	Знать: демонстрирует менее 60% знаний, указанных в таблице 1.3 для ПК-5. Обучающийся нуждается в постоянных подсказках; допускает грубые ошибки, которые не может исправить самостоятельно.	Знать: демонстрирует 60-74% знаний, указанных в таблице 1.3 для ПК-5. Знания обучающегося имеют поверхностный характер, имеют место неточности и ошибки.	Знать: демонстрирует 75-89% знаний, указанных в таблице 1.3 для ПК-5. Обучающийся имеет хорошие, но не исчерпывающие знания; допускает неточности.	Знать: демонстрирует 90-100% знаний, указанных в таблице 1.3 для ПК-5. Знания обучающегося являются прочными и глубокими, имеют системный характер. Обучающийся свободно оперирует знаниями.
		Уметь: демонстрирует менее 60% умений, установленных в таблице 1.3 для ПК-5.	Уметь: в целом сформированные, но вызывающие затруднения при самостоятельном применении умения, указанные в таблице 1.3 для ПК-5.	Уметь: сформированные и самостоятельно применяемые умения, указанные в таблице 1.3 для ПК-5.	Уметь: хорошо развитые, уверенно и успешно применяемые умения, указанные в таблице 1.3 для ПК-5.

	ских заданий	Владеть (или Иметь опыт деятельности): навыки, указанные в таблице 1.3 для ПК-5, не развиты.	Владеть (или Иметь опыт деятельности): навыки, указанные в таблице 1.3 для ПК-5, развиты на элементарном уровне.	Владеть (или Иметь опыт деятельности): навыки, указанные в таблице 1.3 для ПК-5, хорошо развиты.	Владеть (или Иметь опыт деятельности): навыки, указанные в таблице 1.3 для ПК-5, доведены до автоматизма.
--	--------------	--	--	--	---

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

Таблица 7.3 - Паспорт комплекта оценочных средств для текущего контроля успеваемости

№ п/п	Раздел (тема) дисциплины	Код контролируемой компетенции (или ее части)	Технология формирования	Оценочные средства		Описание шкал оценивания
				наименование	№№ заданий	
1	2	3	4	5	6	7
1	Информация, информационные системы как объект правового регулирования информационной безопасности	ПК-4 ПК-5	лекция, СРС	Вопросы для УО Кейс-задача	1-10 1	Согласно табл.7.2
2	Правовая основа допуска и доступа персонала к защищаемым сведениям	ПК-4 ПК-5	лекция, практическое занятие, СРС	Вопросы для УО КВЗПР	1-10 1-10	Согласно табл.7.2
3	Правовые основы защиты коммерческой тайны	ПК-4 ПК-5	лекция, практическое занятие, СРС	Вопросы для УО КВЗПР	1-10 1-10	Согласно табл.7.2
4	Компьютерная	ПК-4	лекция, СРС	Вопросы для УО	1-10	Согласно

№ п/п	Раздел (тема) дисциплины	Код контролируемой компетенции (или ее части)	Технология формирования	Оценочные средства		Описание шкал оценивания
				наименование	№№ заданий	
1	2	3	4	5	6	7
	информация – как объект информатизации	ПК-5		Кейс-задача Производственная задача	2 1-10	табл.7.2
5	Лицензирование в области защиты информации	ПК-4 ПК-5	лекция, практическое занятие, СРС	Вопросы для УО КВЗПР Кейс-задача	1-10 1-10 3	Согласно табл.7.2
6	Сертификация в области защиты информации	ПК-4 ПК-5	лекция, практическое занятие, СРС	Вопросы для УО КВЗПР	1-10 1-10	Согласно табл.7.2
7	Система правовой ответственности за утечку информации и утрату носителей информации	ПК-4 ПК-5	лекция, практическое занятие, СРС	Вопросы для УО КВЗПР	1-10 1-10	Согласно табл.7.2
8	Правовые основы деятельности подразделений защиты информации	ПК-4 ПК-5	лекция, СРС	Вопросы для УО Кейс-задача	1-10 4	Согласно табл.7.2
9	Правовые основы защиты персональных данных	ПК-4 ПК-5	лекция, практическое занятие, СРС	Вопросы для УО КВЗПР Кейс-задача	1-10 1-10 5	Согласно табл.7.2

КВЗПР – контрольные вопросы для защиты практической работы

7.3.1 Примеры типовых контрольных заданий для проведения текущего контроля успеваемости

а) Вопросы для устного опроса по разделу (теме) № 2 «Правовая основа допуска и доступа персонала к защищаемым сведениям»

1. Понятие государственных информационных ресурсов.
2. История и причины возникновения проблемы законодательного обеспечения защиты государственной тайны.
3. Основные направления разработка проблемы правового обеспечения защиты информации?
4. В чем сущность комплексной защиты информации?

5. Основные задачи и функции Государственной технической комиссии при Президенте РФ?

б) Производственная задача

В вашей компании был обнаружен случай утечки конфиденциальной информации. Какие нормативно-правовые требования необходимо выполнить для уведомления компетентных органов и пострадавших лиц о случившемся?

в) Контрольные вопросы для защиты практической работы №6 «Разработка модели угроз информационной безопасности».

1. Что вы понимаете под моделью угроз информационной безопасности?
2. Назовите шаги построения модели угроз информационной безопасности.
3. В модели должны учитываться все актуальные угрозы на всех стадиях их жизненного цикла? Если нет, то какие?
4. Содержание модели угроз?»?

г) Кейс задача

Вы являетесь ответственным за информационную безопасность в крупной компании, которая занимается разработкой программного обеспечения.

Однажды вы узнали, что один из ваших сотрудников, не имеющий необходимых полномочий, имел доступ к базе данных клиентов, содержащей конфиденциальную информацию.

Вы обратились к руководству компании и сообщили о нарушении нормативно-правового регулирования в сфере информационной безопасности. Однако, руководство компании проигнорировало ваше сообщение и не предприняло никаких мер для устранения нарушения. Как вы будете действовать в данной ситуации?

Задачи:

Составьте план действий для устранения нарушения нормативно-правового регулирования в сфере информационной безопасности в компании.

Определите, какие нормативные документы были нарушены, и какие меры должны быть предприняты для исправления нарушений.

Подготовьте отчет для руководства компании, в котором обоснуйте необходимость устранения нарушений, перечислите все риски, связанные с невыполнением нормативных требований, и предложите конкретные меры по исправлению ситуации.

Рассмотрите возможность обратиться к правоохранительным органам для привлечения ответственных лиц к ответственности за нарушение нормативно-правового регулирования в сфере информационной безопасности.

Полностью оценочные материалы и оценочные средства для проведения текущего контроля успеваемости представлены в УММ по дисциплине.

7.3.2 Типовые задания для проведения промежуточной аттестации обучающихся

Промежуточная аттестация по дисциплине проводится в форме зачета. На промежуточной аттестации по дисциплине применяется механизм квалификационного экзамена. Зачет имеет структуру квалификационного экзамена и состоит из 2 частей:

- теоретической (бланковое тестирование);
- практической (решение компетентностно-ориентированной задачи).

На теоретической части зачета (тестировании) проверяются знания и частично – умения и навыки обучающихся. Для тестирования используются контрольно-измерительные материалы (КИМ) – вопросы и задания в тестовой форме, составляющие банк тестовых заданий (БТЗ) по дисциплине, утвержденный в установленном в университете порядке.

Проверяемыми на промежуточной аттестации элементами содержания являются темы дисциплины, указанные в разделе 4 настоящей программы. Все темы дисциплины отражены в КИМ в равных долях (%). БТЗ включает в себя не менее 100 заданий и постоянно пополняется. БТЗ хранится на бумажном носителе в составе УММ и электронном виде в ЭИОС университета.

Для проверки *знаний* используются вопросы и задания в различных формах:

- закрытой (с выбором одного или нескольких правильных ответов),
- открытой (необходимо вписать правильный ответ),
- на установление правильной последовательности,
- на установление соответствия.

На практической части зачета проверяются результаты практической подготовки: *компетенции, включая умения, навыки (или опыт деятельности)*). Результаты практической подготовки (*компетенции, включая умения, навыки (или опыт деятельности)*) проверяются с помощью компетентностно-ориентированных задач (ситуационных, производственных, кейс-задач или кейсов) и различного вида конструкторов».

Все задачи являются многоходовыми. Некоторые задачи, проверяющие уровень сформированности компетенций, являются многовариантными. Часть умений, навыков и компетенций прямо не отражена в формулировках задач, но они могут быть проявлены обучающимися при их решении.

В каждый вариант КИМ включаются задания по каждому проверяемому элементу содержания во всех перечисленных выше формах и разного уровня сложности. Такой формат КИМ позволяет объективно определить качество освоения обучающимися основных элементов содержания дисциплины и уровень сформированности компетенций.

а) Примеры типовых заданий для теоретической части зачета (тестирования)

Задание в закрытой форме:

Что включают в себя системы управления ИБ?

А. Политика, планирование, должностные обязанности, процедуры, процессы и ресурсы.

В. Организационную структуру, политики, планирование, должностные обязанности, практики,

С. Организационную структуру, политики, планирование, должностные обязанности, практики.

Д. Организационную структуру, политики, планирование, должностные обязанности, практики, процедуры, процессы и ресурсы.

Е. Организационную структуру, политики, должностные обязанности, практики, процессы и ресурсы.

Задание в открытой форме:

1. Основными принципами политики безопасности являются...

2. Политика безопасности верхнего уровня включает...

3. Удаленный доступ к сервису организован...

4. Системный подход к защите информации базируется на принципах...

Задание на установление правильной последовательности.

Установить действия этапа анализа рисков:

1. Оценка вероятности того, что угроза будет реализована на практике

2. Оценка рисков технологических и информационных активов

3. Идентификация и оценка стоимости технологических и информационных активов

4. Анализ угроз, для которых технологические и информационные активы являются целевым объектом

Задание на установление соответствия: между средствами и функциями

1	Человек, информация, технические средства	А	Информационное оружие
2	Целенаправленное производство и распространение специальной информации, оказывающей непосредственное влияние на функционирование и развитие психологической среды общества, психику и поведение населения, руководства страны, военнослужащих	Б	Информационное воздействие
3	Комплекс технических средств и технологий, предназначенных для получения контроля над информационными ресурсами потенциального противника в целях выведения их из строя, получения или модификации содержащихся в них данных, целенаправленного продвижения выгодной	В	Элементы информационного пространства

	информации (или дезинформации)		
		Г	Психологическое воздействие

б) Примеры типовых заданий для практической части зачета (или зачета с оценкой, или экзамена)

Компетентностно-ориентированная задача:

Ваша компания работает с персональными данными клиентов. Какие требования к защите таких данных установлены в нормативно-правовых актах вашей страны? Какие меры безопасности должна предпринять компания для соблюдения этих требований?

Полностью оценочные материалы и оценочные средства для проведения промежуточной аттестации обучающихся представлены в УММ по дисциплине.

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

Процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций, регулируются следующими нормативными актами университета:

– положение П 02.016 «О балльно-рейтинговой системе оценивания результатов обучения по дисциплинам (модулям) и практикам при освоении обучающимися образовательных программ»;

– положение П 02.207 «Проектирование и реализация основных профессиональных программ высшего образования – программ магистратуры по модели дуального обучения»;

– методические указания, используемые в образовательном процессе, указанные в списке литературы.

Для *текущего контроля успеваемости* по дисциплине в рамках действующей в университете балльно-рейтинговой системы применяется следующий порядок начисления баллов:

Таблица 7.4 – Порядок начисления баллов в рамках БРС

Форма контроля	Минимальный балл		Максимальный балл	
	балл	примечание	балл	примечание
1	2	3	4	5
Практическая работа № 1-6	8	Выполнил, но не ответил или неполно ответил на какой-либо вопрос	16	Выполнил, правильно и полно ответил на все вопросы
Устный опрос по темам 1-9	8	Не ответил или неполно ответил на какой-либо вопрос	16	Правильно и полно ответил на все вопросы
Кейс	4	Выполнил, но не ответил или неполно ответил на какой-либо вопрос	8	Выполнил, правильно и полно ответил на все вопросы
Производственная задача	4	Выполнил, но не ответил или неполно ответил на какой-либо вопрос	8	Выполнил, правильно и полно ответил на все вопросы
Итого	24		48	
Посещаемость	0		16	
Зачет	0		36	
Итого	24		100	

Для проведения промежуточной аттестации обучающихся (теоретической части и практической части) используется следующая методика оценивания знаний, умений, навыков и (или) опыта деятельности. В каждом варианте КИМ –16 заданий (15 вопросов для тестирования и одна компетентностно-ориентированная задача).

Каждый верный ответ оценивается следующим образом:

- задание в закрытой форме – 2 балла,
- задание в открытой форме – 2 балла,
- задание на установление правильной последовательности – 2 балла,
- задание на установление соответствия – 2 балла,
- решение компетентностно-ориентированной задачи – 6 баллов.

Максимальное количество баллов по промежуточной аттестации – 36.

8 Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины

8.1 Основная учебная литература

1. Гулак, М. Л. Аудит информационной безопасности. Прикладная статистика : учебное пособие / М. Л. Гулак, М. Ю. Рытов, О. М. Голембиовская. — Москва : Ай Пи Ар Медиа, 2020. — 121 с. — ISBN 978-5-4497-0713-0. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: <https://www.iprbookshop.ru/97630.html> (дата обращения: 09.10.2023). — Режим доступа: для авторизир. пользователей

2. Арзуманян, А. Б. Международные стандарты правовой защиты информации и информационных технологий : учебное пособие / А. Б. Арзуманян. — Ростов-на-Дону, Таганрог : Издательство Южного федерального университета, 2020. — 140 с. — ISBN 978-5-9275-3546-0. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: <https://www.iprbookshop.ru/107955.html> (дата обращения: 09.10.2023). — Режим доступа: для авторизир. пользователей

8.2 Дополнительная учебная литература

3. Аверченков, В. И. Служба защиты информации. Организация и управление : учебное пособие для вузов / В. И. Аверченков, М. Ю. Рытов. — Брянск : Брянский государственный технический университет, 2012. — 186 с. — ISBN 5-89838-138-4. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: <https://www.iprbookshop.ru/7008.html> (дата обращения: 09.10.2023). — Режим доступа: для авторизир. пользователей

4. Аверченков, В. И. Аудит информационной безопасности : учебное пособие для вузов / В. И. Аверченков. — Брянск : Брянский государственный технический университет, 2012. — 268 с. — ISBN 978-89838-487-6. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: <https://www.iprbookshop.ru/6991.html> (дата обращения: 09.10.2023). — Режим доступа: для авторизир. пользователей

5. Аудит информационной безопасности органов исполнительной власти : учебное пособие / В. И. Аверченков, М. Ю. Рытов, А. В. Кувыклин, М. В. Рудановский. — Брянск : Брянский государственный технический университет, 2012. — 100 с. — ISBN 978-89838-491-3. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: <https://www.iprbookshop.ru/6992.html> (дата обращения: 09.10.2023). — Режим доступа: для авторизир. пользователей

8.3 Перечень методических указаний

1. Нормативно-правовое регулирование в сфере информационной безопасности: методические указания по выполнению практических работ / Юго-Зап. гос. ун-т; сост.: Е.А. Кулешова. – Курск, 2023. – 31 с.: Библиогр.: с. 30. – Текст: электронный.

2. Нормативно-правовое регулирование в сфере информационной безопасности: методические указания для самостоятельной работы / Юго-Зап. гос. ун-т; сост.: Е.А. Кулешова. – Курск, 2023. – 27 с.: Библиогр.: с. 27. – Текст: электронный.

9 Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины

1. Федеральная служба безопасности [официальный сайт]. Режим доступа: <http://www.fsb.ru/>
2. Федеральная служба по техническому и экспортному контролю [официальный сайт]. Режим доступа: <http://fstec.ru/>
3. Электронно-библиотечная система «Лань» - <http://e.lanbook.com/>
4. Электронно-библиотечная система IQLib – <http://www.iqlib.ru>
5. Электронная библиотека «Единое окно доступа к образовательным ресурсам» - <http://window.edu.ru/>

10 Методические указания для обучающихся по освоению дисциплины

Основными видами аудиторной работы студента при изучении дисциплины являются лекции и практические занятия.

На лекциях излагаются и разъясняются основные понятия и положения каждой новой темы; важные положения аргументируются и иллюстрируются примерами из практики; объясняется практическая значимость изучаемой темы; делаются выводы; даются рекомендации для самостоятельной работы по данной теме. На лекциях необходимо задавать преподавателю уточняющие вопросы с целью уяснения теоретических положений, разрешения спорных вопросов. В ходе лекции студент должен конспектировать учебный материал. Конспектирование лекций – сложный вид работы, предполагающий интенсивную умственную деятельность студента. Конспект является полезным тогда, когда записано самое существенное и сделано это лично студентом в режиме реального времени в течение лекции. Не следует стремиться записать лекцию дословно. Целесообразно вначале понять основную мысль, излагаемую лектором, а затем кратко записать ее. Желательно заранее оставлять в тетради пробелы, куда позднее, при самостоятельной работе с конспектом, можно внести дополнительные записи. Конспект лекции лучше подразделять на пункты, соблюдая красную строку. Этому в большой степе-

ни будут способствовать вопросы плана лекции, который преподаватель дает в начале лекционного занятия. Следует обращать внимание на акценты, выводы, которые делает лектор, отмечая наиболее важные моменты в лекционном материале.

Необходимым является глубокое освоение содержания лекции и свободное владение им, в том числе использованной в ней терминологией. Работу с конспектом лекции целесообразно проводить непосредственно после ее прослушивания, что способствует лучшему усвоению материала, позволяет своевременно выявить и устранить «пробелы» в знаниях. Работа с конспектом лекции предполагает перечитывание конспекта, внесение в него, по необходимости, уточнений, дополнений, разъяснений и изменений. Некоторые вопросы выносятся за рамки лекций. Изучение вопросов, выносимых за рамки лекционных занятий, предполагает самостоятельное изучение студентами дополнительной литературы, указанной в п.8.2.

Изучение наиболее важных тем или разделов дисциплины продолжается на практических занятиях, которые обеспечивают контроль подготовленности студента; закрепление учебного материала; приобретение опыта устных публичных выступлений, ведения дискуссии, в том числе аргументации и защиты выдвигаемых положений и тезисов.

Практическому занятию предшествует самостоятельная работа студента, связанная с освоением материала, полученного на лекциях, и материалов, изложенных в учебниках и учебных пособиях, а также литературе, рекомендованной преподавателем. Самостоятельная работа с учебниками, учебными пособиями, научной, справочной литературой, материалами периодических изданий и Интернета является наиболее эффективным методом получения дополнительных знаний, позволяет значительно активизировать процесс овладения информацией, способствует более глубокому усвоению изучаемого материала. При работе с источниками и литературой необходимо:

- сопоставлять, сравнивать, классифицировать, группировать, систематизировать информацию в соответствии с определенной учебной задачей;
- обобщать полученную информацию, оценивать прочитанное;
- фиксировать основное содержание прочитанного текста; формулировать устно и письменно основную идею текста; составлять план, формулировать тезисы.

Самостоятельную работу следует начинать с первых занятий. От занятия к занятию нужно регулярно прочитывать конспект лекций, знакомиться с соответствующими разделами учебника, читать и конспектировать литературу по каждой теме дисциплины. Самостоятельная работа дает студентам возможность равномерно распределить нагрузку, способствует более глубокому и качественному освоению учебного материала. В случае необходимости студенты обращаются за консультацией к преподавателю. Обязательным элементом самостоятельной работы по дисциплине является самоконтроль. Одной из важных задач обучения студентов способам и приемам самообразования является формирование у них умения самостоятельно контролиро-

вать и адекватно оценивать результаты своей учебной деятельности и на этой основе управлять процессом овладения знаниями. Овладение умениями самоконтроля приучает студентов к планированию учебного труда, способствует углублению их внимания, памяти и выступает как важный фактор развития познавательных способностей. Самоконтроль включает:

- оперативный анализ глубины и прочности собственных знаний и умений;
- критическую оценку результатов своей познавательной деятельности.

Самоконтроль учит ценить свое время, позволяет вовремя заметить и исправить свои ошибки. Формы самоконтроля могут быть следующими:

- устный пересказ текста лекции и сравнение его с содержанием конспекта лекции;
- составление плана, тезисов, формулировок ключевых положений текста по памяти;
- пересказ с опорой на иллюстрации, чертежи, схемы, таблицы, опорные положения.

Самоконтроль учебной деятельности позволяет студенту оценивать эффективность и рациональность применяемых методов и форм умственного труда, находить допусаемые недочеты и на этой основе проводить необходимую коррекцию своей познавательной деятельности.

При подготовке к промежуточной аттестации по дисциплине необходимо повторить основные теоретические положения каждой изученной темы и основные термины, самостоятельно решить несколько типовых компетентностно-ориентированных задач.

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

Информационные технологии:

1. Средства для просмотра презентаций;
2. Средства для проведения онлайн-конференций.
3. Электронно-образовательная среда ЮЗГУ

Программное обеспечение:

1. OpenOffice: режим доступа: свободный.
2. Яндекс.Телемост: режим доступа: свободный.

Информационные справочные системы:

1. Научно-информационный портал ВИНТИ РАН. Режим доступа: свободный.
2. База данных "Патенты России". Режим доступа: свободный.

3. Электронно-библиотечная система «Университетская библиотека онлайн» Режим доступа: по подписке.
4. Электронная библиотека диссертаций и авторефератов РГБ. Режим доступа: свободный.
5. Электронный каталог Научной библиотеки ЮЗГУ. Режим доступа: свободный.

12 Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине

Аудиторные занятия по дисциплине проводятся в учебной аудитории для проведения занятий лекционного типа и лаборатории кафедры информационной безопасности, оснащенных стандартной учебной мебелью (столы и стулья для обучающихся; стол и стул для преподавателя; доска).

Для организации образовательного процесса применяются технические средства обучения: Проекционный экран на штативе; Мультимедиа центр: ноутбук ASUS X50VL PMD-T2330/1471024Mb/160Gb/ сумка/ проектор inFocus IN24.

Для осуществления практической подготовки обучающихся при реализации дисциплины используются оборудование и технические средства обучения кафедры информационной безопасности :

1. Класс ПЭВМ - Asus-P7P55LX-/DDR34096Mb/Coree i3-540/SATA-11 500 Gb Hitachi/PCI-E 512Mb, Монитор TFT Wide 23.
2. Мультимедиацентр: ноутбук ASUS X50VL PMD - T2330/14"/1024Mb/ 160Gb/ сумка/проектор inFocus IN24+ .
3. Экран мобильный Draper Diplomat 60x60.

13 Особенности реализации дисциплины для инвалидов и лиц с ограниченными возможностями здоровья

При обучении лиц с ограниченными возможностями здоровья учитываются их индивидуальные психофизические особенности. Обучение инвалидов осуществляется также в соответствии с индивидуальной программой реабилитации инвалида (при наличии).

Для лиц с нарушением слуха возможно предоставление учебной информации в визуальной форме (краткий конспект лекций; тексты заданий, напечатанные увеличенным шрифтом), на аудиторных занятиях допускается присутствие ассистента, а также сурдопереводчиков и тифлосурдопереводчиков. Текущий контроль успеваемости осуществляется в письменной форме: обучающийся письменно отвечает на вопросы, письменно выполняет практические задания. Промежуточная аттестация для лиц с нарушениями слуха проводится в письменной форме, при этом используются общие критерии оценивания. При необходимости время подготовки к ответу может быть увеличено.

Для лиц с нарушением зрения допускается аудиальное предоставление информации, а также использование на аудиторных занятиях звукозаписывающих устройств (диктофонов и т.д.). Допускается присутствие на занятиях ассистента (помощника), оказывающего обучающимся необходимую техническую помощь. Текущий контроль успеваемости осуществляется в устной форме. При проведении промежуточной аттестации для лиц с нарушением зрения тестирование может быть заменено на устное собеседование по вопросам.

Для лиц с ограниченными возможностями здоровья, имеющих нарушения опорно-двигательного аппарата, на аудиторных занятиях, а также при проведении процедур текущего контроля успеваемости и промежуточной аттестации могут быть предоставлены необходимые технические средства (персональный компьютер, ноутбук или другой гаджет); допускается присутствие ассистента (ассистентов), оказывающего обучающимся необходимую техническую помощь (занять рабочее место, передвигаться по аудитории, прочитывать задание, оформить ответ, общаться с преподавателем).

14 Лист дополнений и изменений, внесенных в рабочую программу дисциплины

Номер изменения	Номера страниц				Всего страниц	Дата	Основание для изменения и подпись лица, проводившего изменения
	измененных	замененных	аннулированных	новых			