

Документ подписан простой электронной подписью

Информация о владельце:

ФИО: Таныгин Максим Олегович

Должность: и.о. декана факультета фундаментальной информатики и информатизации

Дата подписания: 10.10.2023 15:57:04

Уникальный программный ключ

65ab2aa0d384efe8480e6a4c688eddbc475e411a

Аннотация к рабочей программе

дисциплины «Организация аудита информационной безопасности»

Цель преподавания дисциплины

Цель дисциплины – формирование у студентов знаний в области организации аудита 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. Анализ характера обрабатываемой информации и определение перечня информации, подлежащей защите.
3. Выявление степени участия персонала в обработке защищаемой информации.
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

Структура службы информационной безопасности. Функции основных групп службы безопасности. Цели и задачи службы информационной безопасности. Организационные основы и принципы деятельности службы информационной безопасности. Лицензирование видов деятельности службы безопасности. Управление службой защиты информации. Организация информационно-аналитической работы. Организация работы с персоналом предприятия.

МИНОБРНАУКИ РОССИИ

Юго-Западный государственный университет

УТВЕРЖДАЮ:

Декан факультета ФиПИ

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

« 30 » мая 20 23 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Организация аудита 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 «ЩИТ-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 «ЩИТ-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 «ЩИТ-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 организации аудита 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. Анализ характера обрабатываемой информации и определение перечня информации, подлежащей защите.

3. Выявление степени участия персонала в обработке защищаемой информации.

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 Уметь: организовывать получение

<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>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): мониторинг нормативных правовых актов, руководя-</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>		
			щих 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 персонала в обработке защищаемой информации</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>		
		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 «Организация аудита 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.	Структура службы информационной безопасности	Общая структурная схема службы защиты информации на примере ООО ЦСБ «ЩИТ-ИНФОРМ». Основные направления деятельности СУИБ
2.	Функции основных групп службы безопасности	Группа режима. Группа охраны и сопровождения. Техническая группа. Детективная группа. Должностные обязанности на примере ООО ЦСБ «ЩИТ-ИНФОРМ». Минимальный штатный состав СБ и обязанности сотрудников на примере ООО ЦСБ «ЩИТ-ИНФОРМ»

3.	Цели и задачи службы информационной безопасности	Цели обеспечения безопасности предприятия на примере ООО ЦСБ «ЩИТ-ИНФОРМ». Задачи службы Функции СИБ
4.	Организационные основы и принципы деятельности службы информационной безопасности	Организация деятельности службы безопасности на примере ООО ЦСБ «ЩИТ-ИНФОРМ». Правовое обеспечение службы. Принципы организации службы на примере ООО ЦСБ «ЩИТ-ИНФОРМ». Гарантии безопасности объектов защиты Пакет документов для СИБ
5.	Лицензирование видов деятельности службы безопасности.	Лицензирование видов деятельности службы безопасности предприятия на примере ООО ЦСБ «ЩИТ-ИНФОРМ»
6.	Управление службой защиты информации.	Методы управления СБП Функции процессов управления Функции процессов управления Методы управления Принципы управления СБП. Виды обеспечения деятельности СБП. Управление безопасностью предприятия в кризисных ситуациях на примере ООО ЦСБ «ЩИТ-ИНФОРМ»
7.	Организация информационно-аналитической работы.	Цели и задачи информационно-аналитической работы. Направления и методы аналитической работы Этапы выполнения информационно-аналитических исследований производственных ситуаций. Методы выполнения аналитических исследований на примере ООО ЦСБ «ЩИТ-ИНФОРМ»
8.	Организация работы с персоналом предприятия.	Подбор и подготовка кадров. Проверка персонала на благонадежность на примере ООО ЦСБ «ЩИТ-ИНФОРМ». Заключение контрактов и соглашений о секретности. Особенности увольнения сотрудников, владеющих конфиденциальной информацией на примере ООО ЦСБ «ЩИТ-ИНФОРМ»

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	Структура службы информационной безопасности	2	-	1	У-1-5 МУ- 1,2	УО, ПР, КЗ 1-3	ПК-4 ПК-5
2	Функции основных групп службы безопасности	2	-	-	У-1-5 МУ- 1,2	УО 4	ПК-4 ПК-5
3	Цели и задачи службы информационной безопасности	2	-	2	У-1-5 МУ- 1,2	УО, ПР, КЗ 5-6	ПК-4 ПК-5
4	Организационные основы и принципы деятельности службы информационной безопасности	2	-	-	У-1-5 МУ- 1,2	УО 7	ПК-4 ПК-5

5	Лицензирование видов деятельности службы безопасности.	2	-	3	У-1-5 МУ- 1,2	УО, ПР, КЗ, ПЗ 8-10	ПК-4 ПК-5
6	Управление службой защиты информации.	2	-	-	У-1-5 МУ- 1,2	УО 11	ПК-4 ПК-5
7	Организация информационно-аналитической работы.	2	-	4	У-1-5 МУ- 1,2	УО, ПР, КЗ 12-13	ПК-4 ПК-5
8	Организация работы с персоналом предприятия.	4	-	-	У-1-5 МУ- 1,2	УО, КЗ 14	ПК-4 ПК-5
	Итого	18	-	-			

УО – устный опрос, ПР – защита практической работы, КЗ – решение кейса, ПЗ – решение производственной задачи.

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	Определение класса государственной информационной системы (ГИС)	6
2	Разработка структуры государственных и международных стандартов в Российской Федерации в области информационной безопасности и защиты информации	6
3	Техническое задание на создание информационной системы и системы защиты информации	12, из них практическая подготовка обучающихся – 4
4	Основные методы управления информационной безопасностью в ГИС	12
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.	Структура службы информационной безопасности	1-2 неделя	6
2.	Функции основных групп службы безопасности	3-4 неделя	6
3.	Цели и задачи службы информационной безопасности	5-6 неделя	8
4.	Организационные основы и принципы деятельности службы информационной безопасности	7-8 неделя	8
5.	Лицензирование видов деятельности службы безопасности.	9-10 неделя	8
6.	Управление службой защиты информации.	11 неделя	6
7.	Организация информационно-аналитической работы.	12 неделя	6
8.	Организация работы с персоналом предприятия.	13-14 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	Определение класса государственной информационной системы (ГИС)	<i>кейс-технология</i>	4
2	Разработка структуры государственных и международных стандартов в Российской Федерации в области информационной безопасности и защиты информации	<i>кейс-технология</i>	4
3	Техническое задание на создание информационной системы и системы защиты информации	<i>кейс-технология</i>	6
4	Основные методы управления информационной безопасностью в ГИС	<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	Структура службы информационной безопасности	ПК-4 ПК-5	лекция, практическое занятие, СРС	Вопросы для УО КВЗПР Решение кейса	1-10 1-10 1	Согласно табл.7.2
2	Функции основных групп службы безопасности	ПК-4 ПК-5	лекция, практическое занятие, СРС	Вопросы для УО	1-10	Согласно табл.7.2
3	Цели и задачи службы информационной безопасности	ПК-4 ПК-5	лекция, практическое занятие, СРС	Вопросы для УО КВЗПР Решение кейса	1-10 1-10 2	Согласно табл.7.2
4	Организационные основы и принципы деятельности службы информационной безопасности	ПК-4 ПК-5	лекция, практическое занятие, СРС	Вопросы для УО	1-10	Согласно табл.7.2
5	Лицензирование видов деятельности службы безопасности.	ПК-4 ПК-5	лекция, практическое занятие, СРС	Вопросы для УО КВЗПР Кейс	1-10 1-10 3	Согласно табл.7.2

№ 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
				Производственная задача	1-10	
6	Управление службой защиты информации.	ПК-4 ПК-5	лекция, практическое занятие, СРС	Вопросы для УО	1-10	Согласно табл.7.2
7	Организация информационно-аналитической работы.	ПК-4 ПК-5	лекция, практическое занятие, СРС	Вопросы для УО КВЗПР Решение кейса	1-10 1-10 4	Согласно табл.7.2
8	Организация работы с персоналом предприятия.	ПК-4 ПК-5	лекция, СРС	Вопросы для УО Решение кейса	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) № 6 «Управление службой защиты информации.»

1. Назовите варианты реализации организационной структуры службы информационной безопасности и условия выбора того или иного варианта.

2. Назовите вопросы, решение которых предворяет создание службы информационной безопасности

3. Назовите и охарактеризуйте методы управления службой информационной безопасности

4. Назовите и охарактеризуйте основные функции процессов управления

5. Назовите набор признаков, свидетельствующих о возможных условиях для реализации преступного замысла в отношении охраняемого объекта

б) Производственная задача

В компании была обнаружена утечка конфиденциальной информации. Необходимо провести аудит информационной безопасности, чтобы выявить причины утечки и разработать меры для предотвращения подобных инцидентов в будущем. Какие методы аудита нужно использовать для достижения этих целей?

в) Контрольные вопросы для защиты практической работы №3 «Техническое задание на создание информационной системы и системы защиты информации».

1. Где необходима электронная подпись документов?
2. Какие могут быть альтернативные наборы вариантов решения?
3. Как определялась схема рассадки людей?
4. Какой перечень документов по которым готовился?
5. Какой регулятор контролирует данную область информационной безопасности?

Г) Кейс задача

Вы назначены ответственным за информационную безопасность в небольшой компании, которая занимается продажей товаров в Интернете.

Компания находится в стадии быстрого развития, и вы обеспокоены возможными уязвимостями в системах безопасности компании.

Компания использует несколько серверов для обработки заказов, хранения данных клиентов и выполнения других задач. В компании также есть несколько рабочих станций для работы с данными и электронной почтой, а также Wi-Fi сеть для доступа к Интернету.

Ваша задача - провести аудит информационной безопасности компании, чтобы идентифицировать уязвимости в системах безопасности, а также разработать план мероприятий по их устранению.

Какие этапы аудита информационной безопасности вы проведете?

Какие инструменты и технологии вы будете использовать для проведения аудита?

Как вы оцените уровень уязвимостей в системах безопасности компании?

Какие меры безопасности вы предложите для устранения уязвимостей?

Как вы оцените эффективность мероприятий, предпринятых после аудита?

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.

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

E. 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

1. Задание на установление соответствия: Установить соответствие оценки рисков в зависимости от факторов:

1) Высокий риск	a) Предполагается, что без снижения таких рисков обращение к информационной системе предприятия может оказать отрицательное влияние на бизнес;
2) Существенный риск	b) Здесь требуется эффективная стратегия управления рисками, которая позволит уменьшить или полностью исключить отрицательные последствия нападения;
3) Умеренный риск	c) Усилия по управлению рисками в данном случае не будут играть важной роли.
	d) В отношении рисков, попавших в эту область, достаточно применить основные процедуры управления рисками;

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

Компетентностно-ориентированная задача:

Ваша компания хочет убедиться, что ее персонал полностью соответствует политике информационной безопасности. Как вы определите, какие требования политики безопасности могут быть нарушены? Как вы будете проверять соответствие персонала этим требованиям?.

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	2	Выполнил, но не ответил или неполно ответил на какой-либо вопрос	4	Выполнил, правильно и полно ответил на все вопросы
Практическая работа № 2	2	Выполнил, но не ответил или неполно ответил на какой-либо вопрос	4	Выполнил, правильно и полно ответил на все вопросы
Практическая работа № 3	2	Выполнил, но не ответил или неполно ответил на какой-либо вопрос	4	Выполнил, правильно и полно ответил на все вопросы
Практическая работа № 4	2	Выполнил, но не ответил или неполно ответил на какой-либо вопрос	4	Выполнил, правильно и полно ответил на все вопросы
Кейс	6	Выполнил, но не ответил или неполно ответил на	12	Выполнил, правильно и полно ответил на все вопро-

Форма контроля	Минимальный балл		Максимальный балл	
	балл	примечание	балл	примечание
1	2	3	4	5
		какой-либо вопрос		сы
Устный опрос по темам 1-8	6	Выполнил, но не ответил или неполно ответил на какой-либо вопрос	12	Выполнил, правильно и 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. Организация аудита информационной безопасности: методические указания по выполнению практических работ / Юго-Зап. гос. ун-т; сост.: Е.А. Кулешова. – Курск, 2023. – 29 с.: Библиогр.: с. 29. - Текст : электронный.
2. Организация аудита информационной безопасности: методические указания для самостоятельной работы / Юго-Зап. гос. ун-т; сост.: Е.А. Кулешова. – Курск, 2023. – 61 с.: Библиогр.: с. 59. - 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 степени будут способствовать вопросы плана лекции, который преподаватель дает в начале лекционного занятия. Следует обращать внимание на акценты, вы-

воды, 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 контролировать и адекватно оценивать результаты своей учебной деятельности и на этой основе управлять процессом овладения знаниями. Овладение умениями са-

моконтроля 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 допускаемые 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 звукозаписи-

вающих 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, прочитать 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			