Аннотация к рабочей программе дисциплины «Гуманитарные аспекты информационной безопасности»

Цель преподавания дисциплины

Цель дисциплины – дать студентам основные сведения об этике новых отношений, учитывающих массовую компьютеризацию всех сторон жизни и деятельности личности, общества и государства, о социально-правовых проблемах информатизации и обеспечения информационной безопасности, о современных научных направлениях, связанных с решением этих проблем.

Задачи изучения дисциплины

Формирование требований и проектирование системы управления ИБ

Эффективное управление ИБ

Сформировать у студентов практические навыки анализа и оценки гуманитарных аспектов информации, ее политического, правового, экономического и социального содержания с позиции общенациональной безопасности нашей страны.

Компетенции, формируемые в результате освоения дисциплины

– УК-1: Способен осуществлять критический анализ проблемных ситуаций на основе системного подхода, вырабатывать стратегию действий;

– УК-6: Способен определять и реализовывать приоритеты собственной деятельности и способы ее совершенствования на основе самооценки и образования в течение всей жизни;

– ОПК-17: Способен анализировать основные этапы и закономерности исторического развития России, ее место и роль в контексте всеобщей истории, в том числе для формирования гражданской позиции и развития патриотизма.

Разделы дисциплины

1 Доктрина информационной безопасности Российской Федерации: аналитический обзор
2 Безопасность личности, общества и государства: дифференциация и взаимосвязь уровней информационной безопасности
3 Объективные и субъективные аспекты информационной безопасности в условиях социальной турбулентности
4 Экзистенциально-личностное измерение безопасности и информационная безопасность личности, духовная безопасность личности
5 Цивилизационные аспекты национально-информационной безопасности
6 Виртуальные девиантные сообщества и деструктивный контент социальных сетей

МИНОБРНАУКИ РОССИИ

Юго-Западный государственный университет

УТВЕРЖДАЮ:
И.о. декана факультета
фундаментальной и прикладной информатики
(наименование ф-та полностью)
_____М.О. Таныгин
(подпись, инициалы, фамилия)

«30» июня 2022г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Гуманитарные аспекты информационнойбезопасности
(наименование дисциплины)

ОПОП ВО 10.05.02 Информационная безопасность телекоммуникационных систем
шифр и наименование направления подготовки (специальности)

направленность (профиль, специализация) Управление безопасностью телекоммуникационных систем исетей
наименование направленности (профиля, специализации)

форма обучения очная
(очная, очно-заочная, заочная)

Курск – 2022

Рабочая программа дисциплины составлена в соответствии с ФГОС ВО – специалитет по специальности 10.05.02 Информационная безопасность телекоммуникационных систем на основании учебного плана ОПОП ВО 10.05.02 Информационная безопасность телекоммуникационных систем, профиль «Управление безопасностью телекоммуникационных систем и сетей», одобренного Ученым советом университета (протокол № 6 от 26.02.2021 г.).

Рабочая программа дисциплины обсуждена и рекомендована к реализации в образовательном процессе для обучения студентов по ОПОП ВО 10.05.02 Информационная безопасность телекоммуникационных систем, профиль «Управление безопасностью телекоммуникационных систем и сетей» на заседании кафедры информационной безопасности №11 «30» 06 20 22 г.

Зав. кафедрой _____ Таныгин М.О.

Разработчик программы

_____ Кулешова Е.А.

(ученая степень и ученое звание, Ф.И.О.)

Директор научной библиотеки _____ Макаровская В.Г.

Рабочая программа дисциплины пересмотрена, обсуждена и рекомендована к реализации в образовательном процессе на основании учебного плана ОПОП ВО 10.05.02 Информационная безопасность телекоммуникационных систем, профиль «Управление безопасностью телекоммуникационных систем и сетей», одобренного Ученым советом университета протокол № ___ « __ » _____ 20 ___ г., на заседании кафедры _____ .

(наименование кафедры, дата, номер протокола)

Зав. кафедрой _____

Рабочая программа дисциплины пересмотрена, обсуждена и рекомендована к реализации в образовательном процессе на основании учебного плана ОПОП ВО 10.05.02 Информационная безопасность телекоммуникационных систем, профиль «Управление безопасностью телекоммуникационных систем и сетей», одобренного Ученым советом университета протокол № ___ « __ » _____ 20 ___ г., на заседании кафедры _____ .

(наименование кафедры, дата, номер протокола)

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 преподавания дисциплины

Цель дисциплины – дать студентам основные сведения об этике новых отношений, учитывающих массовую компьютеризацию всех сторон жизни и деятельности личности, общества и государства, о социально-правовых проблемах информатизации и обеспечения информационной безопасности, о современных научных направлениях, связанных с решением этих проблем.

1.2. Задачи изучения дисциплины

Задачами дисциплины являются:
Формирование требований и проектирование системы управления ИБ.
Эффективное управление ИБ.
Сформировать у студентов практические навыки анализа и оценки гуманитарных аспектов информации, ее политического, правового, экономического и социального содержания с позиции общенациональной безопасности нашей страны.

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

Таблица 1.3 – Результаты обучения по дисциплине

Планируемые результаты освоения основной профессиональной образовательной программы (компетенции, закрепленные за дисциплиной)		*Код и наименование индикатора достижения компетенции, закрепленного за дисциплиной*	*Планируемые результаты обучения по дисциплине, соотнесенные с индикаторами достижения компетенций*
код компетенции	*наименование компетенции*		
УК-1	Способен осуществлять критический анализ проблемных ситуаций на основе системного	УК-1.5 - Использует логико-методологический инструментарий для критической оценки современных концепций философского и	***Знать:*** - концепцию национальной безопасности РФ; - технологии повышения защищенности распределенных информационных систем; - административную, уголовную, гражданско-правовую

Планируемые результаты освоения основной профессиональной образовательной программы (компетенции, закрепленные за дисциплиной)		*Код и наименование индикатора достижения компетенции, закрепленного за дисциплиной*	*Планируемые результаты обучения по дисциплине, соотнесенные с индикаторами достижения компетенций*
код компетенции	*наименование компетенции*		
	подхода, вырабатывать стратегию действий	социального характера в своей предметной области	ответственность. ***Уметь:*** - выполнять определять характер угрозы и масштабы последствий; - минимизировать последствия ущерба за счет интеграции средств защиты. ***Владеть (****или* ***Иметь опыт деятельности):*** - навыками оценки угроз ИБ с точки зрения нормативно-правового обеспечения; - навыками ранжирования угроз с учетом масштаба возможных последствий.
УК-6	Способен определять и реализовывать приоритеты собственной деятельности и способы ее совершенствования на основе самооценки и образования в течение всей жизни	УК-6.2 - Определяет задачи саморазвития и профессионального роста, распределяет их на долго-, средне- и краткосрочные с обоснованием актуальности и определением необходимых ресурсов для их выполнения	***Знать***: роль информационной безопасности в социально-экономическом развитии общества; структуру университета, управления им, основы организации учебного процесса, виды занятий, обязанности и права студентов ***Уметь***: характеризовать назначение, взаимосвязи и основное содержание, включенных в учебный план разделов ОПОП, циклов дисциплин, модулей, практик, НИР, промежуточных и итоговых испытаний (аттестаций) обучающихся ***Владеть:*** навыками критического восприятия и изучения научно-технической информации.
		УК-6.3 - Использует основные возможности и инструменты	***Знать:*** уровни образования, типы и послевузовского образования и требования рынка труда, предъявляемые к

Планируемые результаты освоения основной профессиональной образовательной программы (компетенции, закрепленные за дисциплиной)		*Код и наименование индикатора достижения компетенции, закрепленного за дисциплиной*	*Планируемые результаты обучения по дисциплине, соотнесенные с индикаторами достижения компетенций*
код компетенции	*наименование компетенции*		
		непрерывного образования (образования в течение всей жизни) для реализации собственных потребностей с учетом личностных возможностей, временной перспективы развития деятельности и требований рынка труда	специалисту в области информационной безопасности. ***Уметь:*** выбирать образовательные траектории в зависимости от требований трудового законодательства и нормативных документов в области информационной безопасности . ***Владеть (****или* ***Иметь опыт деятельности):*** проектирования индивидуальной образовательной траектории.
ОПК-17	Способен анализировать основные этапы и закономерности исторического развития России, ее место и роль в контексте всеобщей истории, в том числе для формирования гражданской позиции и развития патриотизма.	ОПК-17.1 - Выявляет существенные черты исторических процессов, явлений и событий	***Знать:*** понятия, методы и технологии управления временим при решении задач информационной безопасности ***Уметь:*** организовывать по этапам и контролировать собственное выполнение задач информационной безопасности ***Владеть:*** навыками управления временем при решении профессиональных задач.
		ОПК-17.2 - Соотносит общие исторические процессы и отдельные факты	***Знать:*** формы информационной войны, стратегию и структуру современной информационной войны, составляющие информационного противоборства, технологии ведения информационной войны; типы и основные характеристики информационных кампаний, понятие и виды информационного оружия. ***Уметь:*** выделять специфику каждого из видов информационной войны. ***Владеть:*** навыками поиска и обработки информации в современных системах и сетях,

Планируемые результаты освоения основной профессиональной образовательной программы (компетенции, закрепленные за дисциплиной)		*Код и наименование индикатора достижения компетенции, закрепленного за дисциплиной*	*Планируемые результаты обучения по дисциплине, соотнесенные с индикаторами достижения компетенций*
код компетенции	*наименование компетенции*		
			организации вопросов создания и проведения мероприятий по обеспечению информационной безопасности объекта.
		ОПК-17.3 - Формулирует собственную позицию по различным проблемам истории	***Знать:*** особенности эволюции информационного противоборства, характеристику всех существующих в настоящее время видов информационной войны, основные особенности информационной среды, в которой происходит развитие источников распространения информационных войн, основные принципы введения информационных войн в историческом развитии. ***Уметь:***определять современные формы и средства информационного воздействия, принадлежность источников и каналы передачи информации, применять технологии противодействия угрозам информационным системам и сетям на объектах информатизации. ***Владеть:***навыками анализа информации, передаваемой в открытых источниках и телекоммуникационных сетях; противодействия средствам воздействия на функционирование информационных сетей и систем.

2. Указание места дисциплины в структуре основной профессиональной образовательной программы

Дисциплина «Гуманитарные аспекты информационной безопасности» входит в обязательную часть блока 1 «Дисциплины (модули)») основной профессиональной образовательной программы – программы специалитета 10.05.02 Информационная безопасность телекоммуникационных систем, профиль «Управление безопасностью телекоммуникационных систем и сетей». Дисциплина изучается на 4 курсе в 7 семестре.

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 трудоёмкость (объём) дисциплины составляет 3 зачётные единицы, 108 академических часов.

Таблица 3.1 – Объём дисциплины

Виды учебной работы	Всего, часов
Общая трудоемкость дисциплины	108
Контактная работа обучающихся с преподавателем по видам учебных занятий (всего)	72
в том числе:	
лекции	36
лабораторные занятия	
практические занятия	36
Самостоятельная работа обучающихся (всего)	35,9
Контроль (подготовка к экзамену)	
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
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.	Доктрина информационной безопасности Российской Федерации: аналитический обзор	объекты информатизации, информационные системы, сайты в сети Интернет, сети связи, информационные технологии, субъекты, деятельность которых связана с формированием и обработкой информации, развитием и использованием названных технологий, обеспечением информационной безопасности, основные социальные сферы, в которых предполагается обеспечение информационной безопасности
2.	Безопасность личности, общества и государства: дифференциация и взаимосвязь уровней информационной безопасности	личность (индивид), общество и государство, индивидуальный уровень (безопасность человека), социетальный, государственный и глобальный (международный или мировой), концепция сообщества безопасности
3.	Объективные и субъективные аспекты информационной безопасности в условиях социальной турбулентности	когнитивные аспекты восприятия, коллективная идентичность и безопасность, гражданское самосознание и способность самоорганизации сообщества, ценностные и культурные основания общественной системы
4.	Экзистенциально-личностное измерение безопасности и информационная безопасность личности, духовная безопасность личности	фундаментальными условиями трансформации человека как социокультурного и природного существа, разработка информационных технологий и социокультурных практик, социологический методологический контекст, гомеостатическое состояние, динамическая адаптации к меняющимся условиям, трансцендирование
5.	Цивилизационные аспекты национально-информационной безопасности	проблема экспликации параметров выстраивания стратегии безопасности, проблема онтологичности социального бытия
6.	Виртуальные девиантные сообщества и деструктивный контент социальных сетей	способы подачи медиа-материалов, информационная война

Таблица 4.1.2 – Содержание дисциплины и ее методическое обеспечение

№ п/п	Раздел (тема) 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.	Доктрина информационной безопасности Российской Федерации: аналитический обзор	6		1	У-1,2,3 МУ-1-2	УО, ЗПР 1-3	УК-1 УК-6 ОПК-17
2.	Безопасность личности, общества и государства: дифференциация и взаимосвязь уровней информационной безопасности	6		2,3,4	У-1,2,4 МУ-1-2	УО, ЗПР 4-6	УК-1 УК-6 ОПК-17
3.	Объективные и субъективные аспекты Информационной безопасности в условиях Социальной турбулентности	6		5	У-1,2,5 МУ-1-2	УО, ЗПР 7-9	УК-1 УК-6 ОПК-17
4.	Экзистенциально-личностное измерение безопасности и информационная безопасность личности, духовная безопасность личности	6		6	У-1,2,5-7 МУ-1-2	УО, ЗПР 10-12	УК-1 УК-6 ОПК-17
5.	Цивилизационные аспекты национально-информационной безопасности	6		7	У-1,2,5-7 МУ-1-2	УО, ЗПР 13-15	УК-1 УК-6 ОПК-17
6.	Виртуальные девиантные сообщества и деструктивный контент социальных сетей	6		8	У-1,2,5-7 МУ-1-2	УО, ЗПР 16-18	УК-1 УК-6 ОПК-17

УО – устный опрос, ЗПР – защита практической работы

4.2. Лабораторные работы и (или) практические работы

4.2.1 Практические работы

Таблица 4.2.1 – Практические работы

№	Наименование практической работы	Объем, час.
1.	Организационные и правовые основы обеспечения безопасности персональных данных	4
2.	Уголовная ответственность за правонарушения в сфере информационной безопасности	4
3.	Гражданская и дисциплинарная ответственность за правонарушения в сфере информационной безопасности	4
4.	Административная ответственность за правонарушения в сфере информационной безопасности	4
5.	Право собственности на информацию и интеллектуальная собственность	4
6.	Авторское право и лицензионные договоры	4
7.	Патентное право	4
8.	Правовой режим коммерческой тайны	4
Итого		36

4.3. Самостоятельнаяработастудентов (СРС)

Таблица 4.3 – Самостоятельная работа студентов

№	Наименование раздела учебной дисциплины	Срок выполнения	Время, затрачиваемое на выполнение СРС, час.
1	2	3	4
1.	Структура службы информационной безопасности Функции основных групп службы безопасности	1-3 неделя	5,9
2.	Цели и задачи службы информационной безопасности	4-6 неделя	6
3.	Организационные основы и принципы деятельности службы информационной безопасности	7-9 неделя	6
4.	Лицензирование видов деятельности службы безопасности.	10-12 неделя	6
5.	Управление службой защиты информации.	13-15 неделя	6

6.	Организация информационно-аналитической работы. Организация работы с персоналом предприятия.	16-18 недели	6
Итого			35,9

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

Студенты могут при самостоятельном изучении отдельных тем и вопросов дисциплин пользоваться учебно-наглядными пособиями, учебным оборудованием и методическими разработками кафедры в рабочее время, установленное Правилами внутреннего распорядка работников.

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

библиотекой университета:

− библиотечный фонд укомплектован учебной, методической, научной, периодической, справочной и художественной литературой в соответствии с 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 вопросов к зачету, методических указаний к выполнению практических работ.

типографией университета:

− путем помощи авторам в подготовке и издании научной, учебной, учебно-методической литературы;

− путем удовлетворения потребностей в тиражировании научной, учебной, учебно-методической литературы.

6. Образовательные технологии. Технологии использования воспитательного потенциала дисциплины

Реализация компетентностного подхода предусматривает широкое использование в образовательном процессе активных и интерактивных форм проведения занятий в сочетании с внеаудиторной работой с целью формирования общепрофессиональных компетенций обучающихся. В рамках дисциплины предусмотрены встречи с экспертами и специалистами Комитета цифрового

развития и связи Курской области.

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

№	Наименование раздела	Используемые интерактивные образовательные технологии	Объём, час.
1.	Практическая работа №1	Разбор конкретных ситуаций	2
2.	Практическая работа №2	Разбор конкретных ситуаций	2
3.	Практическая работа №3	Разбор конкретных ситуаций	2
4.	Практическая работа №4	Разбор конкретных ситуаций	2
	Итого		8

Технологии использования воспитательного потенциала дисциплины

Содержание дисциплины обладает значительным воспитательным потенциалом, поскольку в нем аккумулирован научный опыт человечества. Реализация воспитательного потенциала дисциплины осуществляется в рамках единого образовательного и воспитательного процесса и способствует непрерывному развитию личности каждого обучающегося. Дисциплина вносит значимый вклад в формирование общей и профессиональной культуры обучающихся. Содержание дисциплины способствует правовому, экономическому, профессионально-трудовому, воспитанию обучающихся.

Реализация воспитательного потенциала дисциплины подразумевает:

– целенаправленный отбор преподавателем и включение в лекционный материал, материал для практических и (или) лабораторных занятий содержания, демонстрирующего обучающимся образцы настоящего научного подвижничества создателей и представителей данной отрасли науки (производства, экономики, культуры), высокого профессионализма ученых (представителей производства, деятелей культуры), их ответственности за результаты и последствия деятельности для человека и общества; примеры подлинной нравственности людей, причастных к развитию науки и производства;

– применение технологий, форм и методов преподавания дисциплины, имеющих высокий воспитательный эффект за счет создания условий для взаимодействия обучающихся с преподавателем, другими обучающимися, (командная работа, разбор конкретных ситуаций)*;*

– личный пример преподавателя, демонстрацию им в образовательной деятельности и общении с обучающимися за рамками образовательного процесса высокой общей и профессиональной культуры.

Реализация воспитательного потенциала дисциплины на учебных занятиях направлена на поддержание в университете единой развивающей образовательной и воспитательной среды. Реализация воспитательного потенциала дисциплины в ходе самостоятельной работы обучающихся способствует развитию в них

целеустремленности, инициативности, креативности, ответственности за результаты своей работы – качеств, необходимых для успешной социализации и профессионального становления.

7. Фонд оценочных средств для проведения промежуточной аттестации

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

Код и содержание компетенции	Этапы* формирования компетенций и дисциплины (модули), при изучении которых формируется данная компетенция		
	начальный	основной	завершающий
1	2	3	4
УК-1.5 Использует логико-методологический инструментарий для критической оценки современных концепций философского и социального характера в своей предметной области	Философия	Гуманитарные аспекты информационной безопасности	
УК-6.2 Определяет задачи саморазвития и профессионального роста, распределяет их на долго-, средне- и краткосрочные с обоснованием актуальности и определением необходимых ресурсов для их выполнения	Введение в специальность и планирование профессиональной карьеры	Гуманитарные аспекты информационной безопасности	
УК-6.3 Использует основные возможности и инструменты непрерывного образования (образования в течение всей жизни) для реализации собственных потребностей с учетом личностных возможностей, временной перспективы развития деятельности и требований рынка труда	Введение в специальность и планирование профессиональной карьеры	Гуманитарные аспекты информационной безопасности	
ОПК-17.1 Выявляет существенные черты исторических процессов, явлений и событий	История информационного противоборства История государства и права России Учебная ознакомительная практика		Гуманитарные аспекты информационной безопасности
ОПК-17.2 Соотносит общие исторические процессы и отдельные факты	История информационного противоборства История государства и права России Учебная ознакомительная практика		Гуманитарные аспекты информационной безопасности

ОПК-17.3 Формулирует собственную позицию по различным проблемам истории	История информационного противоборства История государства и права России Учебная ознакомительная практика	Гуманитарные аспекты информационной безопасности

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 *(указывается название этапа из п.7.1)*	Показатели оценивания компетенций *(индикаторы достижения компетенций, закрепленные за дисциплиной)*	Критерии и шкала оценивания компетенций		
		Пороговый уровень («удовлетворительно)	Продвинутый уровень (хорошо»)	Высокий уровень («отлично»)
УК-1/ завершающий	УК-1.5	***Знать:*** - концепцию национальной безопасности РФ; - административную, уголовную, гражданско-правовую ответственность. ***Уметь:*** - минимизировать последствия ущерба за счет интеграции средств защиты. ***Владеть (****или* ***Иметь опыт деятельности):*** - навыками ранжирования угроз с учетом масштаба возможных последствий;	***Знать:*** - технологии повышения защищенности распределенных информационных систем; ***Уметь:*** - выполнять определять характер угрозы и масштабы последствий; ***Владеть (****или* ***Иметь опыт деятельности):*** - навыками ранжирования угроз с учетом масштаба возможных последствий;	***Знать:*** - концепцию национальной безопасности РФ; - технологии повышения защищенности распределенных информационных систем; - административную, уголовную, гражданско-правовую ответственность. ***Уметь:*** - выполнять определять характер угрозы и масштабы последствий; - минимизировать последствия ущерба за счет интеграции средств защиты. ***Владеть (****или*

Код компетенции/ этап *(указывается название этапа из п.7.1)*	Показатели оценивания компетенций *(индикаторы достижения компетенций, закрепленные за дисциплиной)*	Критерии и шкала оценивания компетенций		
		Пороговый уровень («удовлетворительно)	Продвинутый уровень (хорошо»)	Высокий уровень («отлично»)
				Иметь опыт деятельности): - навыками оценки угроз ИБ с точки зрения нормативно-правового обеспечения; - навыками ранжирования угроз с учетом масштаба возможных последствий;
УК-6/ завершающий	УК-6.2; Определяет задачи саморазвития и профессионального роста, распределяет их на долго-, средне- и краткосрочные с обоснованием актуальности и определением необходимых ресурсов для их выполнения	***Знать***: структуру университета, управления им, основы организации учебного процесса, виды занятий, обязанности и права студентов ***Уметь***: характеризовать основное содержание, включенных в учебный план разделов ОПОП, циклов дисциплин, модулей, практик, ***Владеть:***базовыми навыками критического восприятия и	***Знать***: роль информационной безопасности в социальноэкономическом развитии общества; структуру университета, управления им, основы организации учебного процесса, виды занятий, обязанности и права студентов ***Уметь***: характеризовать назначение, взаимосвязи и основное содержание, включенных в учебный план разделов ОПОП,	***Знать***: роль информационной безопасности в социальноэкономическом развитии общества; аспекты, влияющие на качество специалиста по информационной безопасности, основные профессиональные компетенции специалиста по информационной безопасности ***Уметь***: характеризовать назначение, взаимосвязи и основное содержание, включенных в учебный план

Код компетенции/ этап *(указывается название этапа из п.7.1)*	Показатели оценивания компетенций *(индикаторы достижения компетенций, закрепленные за дисциплиной)*	Критерии и шкала оценивания компетенций		
		Пороговый уровень («удовлетворительно)	Продвинутый уровень (хорошо»)	Высокий уровень («отлично»)
		изучения научно-технической информации.	циклов дисциплин, модулей, практик, НИР, промежуточных и итоговых испытаний (аттестаций) обучающихся ***Владеть:*** навыками критического восприятия и изучения научно-технической информации.	разделов ОПОП, циклов дисциплин, модулей, практик, НИР, промежуточных и итоговых испытаний (аттестаций) обучающихся и компетенций специалиста по информационной безопасности ***Владеть:***продвинутыми навыками критического восприятия и изучения научно-технической информации.
	УК-6.3 Использует основные возможности и инструменты непрерывного образования (образования в течение всей жизни) для реализации собственных потребностей с учетом личностных возможностей, временной перспективы	***Знать:*** уровни образования, типы и послевузовского образования и требования рынка труда, предъявляемые к специалисту в области информационной безопасности. ***Уметь:*** выбирать образовательные траектории в зависимости от требований трудового	***Знать:*** уровни образования, типы и послевузовского образования и требования рынка труда, предъявляемые к специалисту в области информационной безопасности. ***Уметь:*** выбирать образовательные траектории в зависимости от требований трудового	***Знать:*** уровни образования, типы и послевузовского образования и требования рынка труда, предъявляемые к специалисту в области информационной безопасности. ***Уметь:*** выбирать образовательные траектории в зависимости от требований трудового законодательства и

Код компетенции/ этап *(указывается название этапа из п.7.1)*	Показатели оценивания компетенций *(индикаторы достижения компетенций, закрепленные за дисциплиной)*	Критерии и шкала оценивания компетенций		
		Пороговый уровень («удовлетворительно)	Продвинутый уровень (хорошо»)	Высокий уровень («отлично»)
	развития деятельности и требований рынка труда	законодательства и нормативных документов в области информационной безопасности . ***Владеть (****или* ***Иметь опыт деятельности):*** проектирования индивидуальной образовательной траектории.	законодательства и нормативных документов в области информационной безопасности . ***Владеть (****или* ***Иметь опыт деятельности):*** проектирования индивидуальной образовательной траектории.	нормативных документов в области информационной безопасности . ***Владеть (****или* ***Иметь опыт деятельности):*** проектирования индивидуальной образовательной траектории.
ОПК-17/ завершающий	ОПК-17.1 Выявляет существенные черты исторических процессов, явлений и событий	***Знать***: понятия, управления временем ***Уметь***: контролировать собственное выполнение задач информационной безопасности ***Владеть:*** базовыми навыками управления временем при решении профессиональных задач.	***Знать***: понятия, методы и технологии управления временем при решении задач информационной безопасности ***Уметь***: организовывать по этапам и контролировать собственное выполнение задач информационной безопасности ***Владеть:*** навыками управления временем при решении профессиональных задач.	***Знать***: понятия, методы и технологии управления временем при решении сложных и нетиповых задач информационной безопасности ***Уметь***: организовывать, планировать, в т.ч. в автоматическом и полуавтоматическом режиме по этапам и контролировать собственное выполнение задач информационной безопасности ***Владеть:*** продвинутыми навыками управления временем при

Код компетенции/ этап *(указывается название этапа из п.7.1)*	Показатели оценивания компетенций *(индикаторы достижения компетенций, закрепленные за дисциплиной)*	Критерии и шкала оценивания компетенций		
		Пороговый уровень («удовлетворительно)	Продвинутый уровень (хорошо»)	Высокий уровень («отлично»)
				решении профессиональных задач.
	ОПК-17.2 Соотносит общие исторические процессы и отдельные факты	***Знать:*** основные направления информационной войны. ***Уметь:***определять особенности процесса введения информационных войн в условиях мировой политики. ***Владеть:***навыкам и использования имеющейся теоретической информации для решения практических задач в сфере осуществления информационных войн.	***Знать:*** особенности эволюции информационного противоборства;характеристику всех существующих в настоящее время видов информационной войны;основные особенности информационной среды, в которой происходит развитие источников распространения информационных войн. ***Уметь:*** выделять специфику каждого из видов информационной войны. ***Владеть:*** навыками использования имеющейся теоретической информации для решения практических	***Знать:*** основные принципы введения информационных войн в историческом развитии. ***Уметь:*** выделять специфику каждого из видов информационной войны. ***Владеть:*** навыками использования имеющейся теоретической информации для решения практических задач в сфере осуществления информационных войн.

Код компетенции/ этап *(указывается название этапа из п.7.1)*	Показатели оценивания компетенций *(индикаторы достижения компетенций, закрепленные за дисциплиной)*	Критерии и шкала оценивания компетенций		
		Пороговый уровень («удовлетворительно)	Продвинутый уровень (хорошо»)	Высокий уровень («отлично»)
			задач в сфере осуществления информационных войн.	
	ОПК-17.3 Формулирует собственную позицию по различным проблемам истории	***Знать:*** влияние информационного противоборства на возможность обеспечения технологического процесса защиты информации. ***Уметь:*** описывать уязвимые для информационного влияния процессы обеспечения ИБ. ***Владеть:*** навыками поддержания технологического процесса обеспечения ИБ в условиях информационного противодействия.	***Знать:*** основные аспекты влияния информационного противоборства на возможность обеспечения технологического процесса защиты информации. ***Уметь:*** выделять уязвимые для информационного влияния процессы обеспечения ИБ. ***Владеть:*** навыками обеспечения технологического процесса обеспечения ИБ в условиях информационного противодействия.	***Знать:*** методы и средства информационного воздействия. ***Уметь:*** выделять уязвимые для информационного влияния процессы обеспечения ИБ и нивелировать выделенные угрозы. ***Владеть:*** навыками планирования и обеспечения технологического процесса обеспечения ИБ в условиях информационного противодействия.

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 образовательной программы

Таблица 7.3 – Паспорт комплекта оценочных средств для текущего контроля

№ п/п	Раздел (тема) дисциплины	Код контролируемой компетенции (или её части)	Технология формирования	Оценочные средства		Описание шкал оценивания
				наименование	№№ заданий	
1	2	3	4	5	6	7
1	Доктрина информационной безопасности Российской Федерации: аналитический обзор	УК-1 УК-6 ОПК-17	Лекция, СРС, практическое занятие, доклад	Вопросы для УО КВЗПР №1	1-5 1-8	Согласно таблице 7.2
2	Безопасность личности, общества и государства: дифференциация и взаимосвязь уровней информационной безопасности	УК-1 УК-6 ОПК-17	Лекция, СРС, практическое занятие, доклад	Вопросы для УО КВЗПР №2,3,4	1-5 1-9	Согласно таблице 7.2
3	Объективные и субъективные аспекты Информационной безопасности в условиях Социальной турбулентности	УК-1 УК-6 ОПК-17	Лекция, СРС, практическое занятие	Вопросы для УО КВЗПР №5	1-5 1-10	Согласно таблице 7.2
4	Экзистенциально-личностное измерение безопасности и информационная безопасность личности,	УК-1 УК-6 ОПК-17	Лекция, СРС	Вопросы для УО КВЗПР №6	1-5 1-10	Согласно таблице 7.2

	духовная безопасность личности					
5	Цивилизационные аспекты национально-информационной безопасности	УК-1 УК-6 ОПК-17	Лекция, СРС, практическое занятие	Вопросы для УО КВЗПР №7	1-5 1-10	Согласно таблице 7.2
6	Виртуальные девиантные сообщества и деструктивный контент социальных сетей	УК-1 УК-6 ОПК-17	Лекция, СРС	Вопросы для УО КВЗПР №8	1-5 1-7	Согласно таблице 7.2

СРС – самостоятельная работа студента,

КВЗПР – контрольные вопросы для защиты практических работ.

Примеры типовых контрольных заданий для текущего контроля

Вопросы для устного опроса по разделу (теме) 1. «Доктрина информационной безопасности Российской Федерации: аналитический обзор»

1. Как называется состояние информации, при котором доступ к ней осуществляют только субъекты, имеющие на него право?
2. Как называется состояние информации, при котором отсутствует любое ее изменение, либо изменение осуществляется только преднамеренно субъектами, имеющими на него право?
3. Как называется состояние информации, при котором субъекты, имеющие право доступа, могут реализовывать его беспрепятственно?
4. Перечислите основные социальные сферы, в которых предполагается обеспечение информационной безопасности.
5. Перечислите объекты информатизации, деятельность которых связана с формированием и обработкой информации, развитием и использованием названных технологий.

Вопросы для защиты практической работы «Разработка структуры государственных и международных стандартов в Российской Федерации в области информационной безопасности и защиты информации»

1. Дать полное определение ГОСТ
2. Дать полное определение ИСО

3. Как проводится сертификация средств защиты информации?
4. Что показывают характеристики данного средства защиты?
5. Какая основная информация содержится в сертификате?

Полностью оценочные средства представлены в учебно-методическом комплексе дисциплины.

Типовые задания для промежуточной аттестации

Промежуточная аттестация по дисциплине проводится в форме зачета. Зачет проводится в форме тестирования (бланкового).

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.

Умения, навыки (или опыт деятельности) и компетенции проверяются с помощью компетентностно-ориентированных задач (ситуационных, производственных или кейсового характера) и различного вида конструкторов.

Примеры типовых заданий для проведения
промежуточной аттестации обучающихся

Задание в закрытой форме:

Что из перечисленного относится к числу основных аспектов информационной безопасности:

(1) подотчетность - полнота регистрационной информации о действиях субъектов

(2) приватность - сокрытие информации о личности пользователя

(3) конфиденциальность - защита от несанкционированного ознакомления

Задание в открытой форме:

Нормы поведения, которые традиционно сложились по мере распространения сетевых и информационных технологий. Это … меры защиты информации.

Задание на установление правильной последовательности,

Расположите по порядку основные формы информационного противоборства
1.информационное доминирование
2.информационная асимметрия
3.информационное сдерживание
4.информационная агрессия
5.контроль и управление информацией

Задание на установление соответствия:
Установить соответствие

1) Принцип разумной достаточности	a) защита не должна обеспечиваться только за счет секретности структурной безопасности и алгоритмов функционирования ее подсистемы.
2) Принцип разумной избыточности	b) Должны быть реализованы принципы гибкости управления, обеспечивающие возможность настройки механизмов в процессе функционирования системы.
3) Принцип гибкости управления и применения	c) на этапе разработки системы защиты в нее должна закладываться некий потенциал, который позволил бы увеличить срок ее жизнеспособности.
4) Открытость алгоритмов и механизмов защиты	d) Необходимо правильно выбрать тот уровень защиты, при котором затраты, риск взлома и размер возможного ущерба были бы приемлемыми.

Компетентностно-ориентированная задача:

1. Приведите перечень средств информационно-психологического воздействия и манипулирования мнением и их описание (ложные авторитеты, сокрытие фактов, использование ярко выраженной эмоциональной окраски и пр.).

2. Отберите два информационных сообщения, размещенных в СМИ и/или СМК разными сторонами противоборства, на тему выбранного события.

3.Проведите фактологический анализ данных сообщений.

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

7.4Методические 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»;

– 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	1,5	Выполнил, доля правильных ответов от 50% до 90%	3	Выполнил, доля правильных ответов более 90%
Практическая работа №2	1,5	Выполнил, доля правильных ответов от 50% до 90%	3	Выполнил, доля правильных ответов более 90%
Практическая работа №3	1,5	Выполнил, доля правильных ответов от 50% до 90%	3	Выполнил, доля правильных ответов более 90%
Практическая работа №4	1,5	Выполнил, доля правильных ответов от 50% до 90%	3	Выполнил, доля правильных ответов более 90%
Практическая работа №5	1,5	Выполнил, доля правильных ответов от 50% до 90%	3	Выполнил, доля правильных ответов более 90%
Практическая работа №6	1,5	Выполнил, доля правильных ответов от 50% до 90%	3	Выполнил, доля правильных ответов более 90%
Практическая работа №7	1,5	Выполнил, доля правильных ответов от 50% до	3	Выполнил, доля правильных ответов более 90%

		90%		
Практическая работа №8	1,5	Выполнил, доля правильных ответов от 50% до 90%	3	Выполнил, доля правильных ответов более 90%
Устный опрос по теме 1	2	Доля правильных ответов от 50% до 90%	4	Доля правильных ответов более 90%
Устный опрос по теме 2	2	Доля правильных ответов от 50% до 90%	4	Доля правильных ответов более 90%
Устный опрос по теме 3	2	Доля правильных ответов от 50% до 90%	4	Доля правильных ответов более 90%
Устный опрос по теме 4	2	Доля правильных ответов от 50% до 90%	4	Доля правильных ответов более 90%
Устный опрос по теме 5	2	Доля правильных ответов от 50% до 90%	4	Доля правильных ответов более 90%
Устный опрос по теме 6	2	Доля правильных ответов от 50% до 90%	4	Доля правильных ответов более 90%
Итого	24		48	
Посещаемость	0		16	
Зачет	0		36	
Итого	24		100	

Для промежуточной аттестации обучающихся, проводимой в виде тестирования, используется следующая методика оценивания знаний, умений, навыков и (или) опыта деятельности. В каждом варианте КИМ –16 заданий (15 вопросов и одна 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 за тестирование –36 баллов.

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

8.1 Основная учебная литература

1. Технологии обеспечения безопасности информационных систем : учебное пособие / А. Л. Марухленко, Л. О. Марухленко, М. А. Ефремов и др. –

Москва ; Берлин : Директ-Медиа, 2021. – 210 с. – URL: https://biblioclub.ru/index.php?page=book&id=598988 (дата обращения: 02.09.2022). – Режим доступа: по подписке. – Текст : электронный.

2. Корнилова, А. А. Защита персональных данных : учебное пособие / А. А. Корнилова, Д. С. Юнусова, А. С. Исмагилова ; Башкирский государственный университет. – Уфа : Башкирский государственный университет, 2020. – 119 с. – URL: https://biblioclub.ru/index.php?page=book&id=611314 (дата обращения: 02.09.2022). – Режим доступа: по подписке. – Текст : электронный.

8.2 Дополнительная учебная литература

3.Философские проблемы информационного противоборства: учебное пособие для бакалавров, студентов, магистрантов и аспирантов : учебное пособие / В. С. Поликарпов, В. Е. Шибанов, Е. В. Поликарпова, К. Е. Румянцев. – Ростов-на-Дону ; Таганрог : Южный федеральный университет, 2018. – 211 с. – URL: https://biblioclub.ru/index.php?page=book&id=499981 (дата обращения: 23.08.2022). – Режим доступа : по подписке. – Текст : электронный.

4.Спеваков, А. Г. Основы правового обеспечения информационной безопасности : учебное пособие / А. Г. Спеваков, А. П. Фисун ; Юго-Зап. гос. ун-т. - Курск : ЮЗГУ, 2013. - Ч. 1. - 150 с. - Текст : электронный.

5.Жаров, М. Хроники информационной войны: монография / М. Жаров, Т. Шевяков. - Москва: Европа, 2009. - 48 с. - URL: http://biblioclub.ru/index.php?page=book&id=44917 (дата обращения: 09.08.2022) . - Режим доступа : по подписке. - Текст : электронный.

6.Киселёв, А. Г. Теория и практика массовой информации: общество - СМИ - власть : учебник / А. Г. Киселёв. - Москва : Юнити, 2017. - 431 с. - URL: https://biblioclub.ru/index.php?page=book_red&id=691915 (дата обращения 09.03.2022) . - Режим доступа : по подписке. - Текст : электронный.

7. Балдин, К. В. Управление рисками : учебное пособие / К. В. Балдин, С. Н. Воробьев. – Москва :Юнити-Дана, 2017. – 511 с. – URL: https://biblioclub.ru/index.php?page=book&id=615795 (дата обращения: 23.08.2021). – Режим доступа : по подписке. – Текст : электронный.

8.3 Перечень методических указаний

1. Гуманитарные аспекты информационной безопасности: методические указания по выполнению практических работ / Юго-Зап. гос. ун-т; сост.: Е.А. Кулешова. – Курск, 2023. – 26 с.: Библиогр.: с. 26.

2. Гуманитарные аспекты информационной безопасности: методические указания для самостоятельной работы / Юго-Зап. гос. ун-т; сост.: Е.А. Кулешова. – Курск, 2023. – 57 с.: Библиогр.: с. 57.

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

1. http://e.lanbook.com - Электронно-библиотечная система «Лань».
2. http://www.iqlib.ru - Электронно-библиотечная система IQLib.
3. http://window.edu.ru -Электронная библиотека «Единое окно доступа к образовательным ресурсам».
4. http://biblioclub.ru – Электронно-библиотечная система «Университетская библиотека онлайн».
5. http://www.fsb.ru - Федеральная служба безопасности [официальный сайт].
6. http://fstec.ru - Федеральная служба по техническому и экспортному контролю [официальный сайт].
7. http://microsoft.com - Корпорация Microsoft[официальный сайт].
8. http://www.consultant.ruКомпания«Консультант Плюс» [официальный сайт].

10 Методические указания для обучающихся по освоению дисциплины

Основными видами аудиторной работы студента при изучении дисциплины «Гуманитарные аспекты информационной безопасности» являются лекции, лабораторные и практические занятия. Студент не имеет права пропускать занятия без уважительных причин.

На лекциях излагаются и разъясняются основные понятия темы, связанные с ней теоретические и практические проблемы, даются рекомендации для самостоятельной работы. В ходе лекции студент должен внимательно слушать и конспектировать материал.

Изучение наиболее важных тем или разделов дисциплины завершают лабораторные и практические занятия, 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.

Лабораторному и 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.

По согласованию с преподавателем или по его заданию студенты готовить рефераты по отдельным темам дисциплины, выступать на занятиях с докладами. Основу докладов составляет, как правило, содержание подготовленных студентами рефератов.

Качество учебной работы студентов преподаватель оценивает по результатам тестирования, собеседования, защиты отчетов по лабораторным и практическим работам, а также по результатам докладов.

Преподаватель уже на первых занятиях объясняет студентам, какие формы обучения следует использовать при самостоятельном изучении дисциплины «Гуманитарные аспекты информационной безопасности»: конспектирование учебной литературы и лекции, составление словарей понятий и терминов и т. п.

В процессе обучения преподаватели используют активные формы работы со студентами: чтение лекций, привлечение студентов к творческому процессу на лекциях, промежуточный контроль путем отработки студентами пропущенных лекции, участие в групповых и индивидуальных консультациях (собеседовании). Эти формы способствуют выработке у студентов умения работать с учебником и литературой. Изучение литературы составляет значительную часть самостоятельной работы студента. Это большой труд, требующий усилий и желания студента. В самом начале работы над книгой важно определить цель и направление этой работы. Прочитанное следует закрепить в памяти. Одним из приемов закрепление освоенного материала является конспектирование, без которого немыслима серьезная работа над литературой. Систематическое конспектирование помогает научиться правильно, кратко и четко излагать своими словами прочитанный материал.

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 усвоению учебного материала. В случае необходимости студенты обращаются за консультацией к преподавателю по вопросам дисциплины «Гуманитарные аспекты информационной безопасности» с целью усвоения и закрепления компетенций.

Основная цель самостоятельной работы студента при изучении дисциплины «Гуманитарные аспекты информационной безопасности» - закрепить теоретические знания, полученные в процессе лекционных занятий, а также сформировать практические навыки самостоятельного анализа особенностей дисциплины.

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

MicrosoftOffice 2016.Лицензионный договор №S0000000722 от 21.12.2015 г. с ООО «АйТи46», лицензионный договор №К0000000117 от 21.12.2015 г. с ООО «СМСКанал»,

Kaspersky Endpoint Security Russian Edition, лицензия 156A-140624-192234,

Windows 7, договор IT000012385

Oracle Virtualbox (Бесплатная, GNU General Public License),

Microsoft Visual Studio 2010 Professional Договор IT000012385

MS SQL Server Developer Edition (Бесплатная, GNU General Public License)

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

Учебная аудитория для проведения занятий лекционного типа и лаборатории кафедры информационной безопасности, оснащенные учебной мебелью: столы, стулья для обучающихся; стол, стул для преподавателя; доска. Компьютеры (10шт) CPU AMD-Phenom, ОЗУ 16 GB, HDD 2 Tb, монитор Aok 21”. Проекционный экран на штативе; Мультимедиацентр: ноутбукASUSX50VLPMD-T2330/14"/1024Mb/ 160Gb/сумка/проектор inFocusIN24+

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. Доклад (реферат) также может быть представлен в письменной форме, при этом требования к содержанию остаются теми же, а требования к качеству изложения материала (понятность, качество речи, взаимодействие с аудиторией и т. д.) заменяются на соответствующие требования, предъявляемые к письменным работам (качество оформления текста и списка литературы, грамотность, наличие иллюстрационных материалов и т.д.). 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, 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
	изме-ненных	замененных	аннулированных	новых			