Документ подписан простой электронной подписью
Информация о владельце:
ФИО: Таныгин Максим Олегович
Должность: и.о. декана факультета фундаментальной подготовки
Дата подписания: 06.10.2022 10:25:54
Уникальный программный ключ:
65ab2aa0d384efe8480e6a4c688eddbc475e411a

Аннотация к рабочей программе дисциплины «Система сертификации и лицензирования деятельности по защите информации»

Цель преподавания дисциплины

Целью преподавания дисциплины «Система сертификации и лицензирования деятельности по защите информации» является получение студентами знаний о основных подходах к разработке, реализации, эксплуатации, анализу, сопровождению и совершенствованию систем стандартизации и сертификации безопасности инфокоммуникационных сетей.

Задачи изучения дисциплины

– рассмотреть основы управления информационной безопасностью;

– рассмотреть оценочные стандарты в области информационной безопасности;

– рассмотреть создание системы управления информационной безопасности на предприятии;

– рассмотреть методики и технологии управления рисками;

– рассмотрение организационных меры обеспечения безопасности инфокоммуникационных систем.

Компетенции, формируемые в результате освоения дисциплины

Способен организовать работы по выполнению требований защиты информации ограниченного доступа в телекоммуникационных системах и сетях (ПК-8).

Разделы дисциплины

Оценочные стандарты в информационной безопасности. Стандарты управления информационной безопасностью. Международные стандарты информационной безопасности. Стандартизация в области облачных технологий. Управление рисками.

Основные понятия. Методика оценки рисков информационной безопасности компании Digital Security. Методики и технологии управления рисками. Разработка корпоративной методики анализа рисков. Лицензирование деятельности в области ТЗИ. Объект информатизации. Классификация объектов защиты. Общий порядок сертификации средств защиты информации. Порядок сертификации во ФСТЭК России. Аттестация объекта информатизации по требованиям безопасности информации. Требования и рекомендации по защите информации, обрабатываемой средствами вычислительной техники.

МИНОБРНАУКИ РОССИИ
Юго-Западный государственный университет

УТВЕРЖДАЮ:
Декан факультета
фундаментальной и прикладной
(наименование ф-та полностью)
информатики

М.О. Таныгин
(подпись, инициалы, фамилия)
«31» 05 20 21 г

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Система сертификации и лицензирования деятельности по защите информации
(наименование дисциплины)

ОПОП ВО 10.05.02 Информационная безопасность
шифр и наименование направление подготовки (специальности)

Управление безопасностью телекоммуникационных систем и сетей
наименование направленности (профиля, специализации)

форма обучения *очная*
очная, очно-заочная, заочная

Курск – 2021

Рабочая программа дисциплины «Система сертификации и лицензирования деятельности по защите информации» 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, специализация «Управление безопасностью телекоммуникационных систем и сетей», одобренного Ученым советом университета (протокол № __ «__» _____ 20___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 на основании учебного плана ОПОП ВО 10.05.02 Информационная безопасность телекоммуникационных систем, специализация «Управление безопасностью телекоммуникационных систем и сетей» на заседании кафедры информационной безопасности № «___» _____ 20____ г.

Зав. кафедрой _____ Таныгин М.О.

Разработчик программы
к.т.н., доцент _____ Ефремов М.А.
(ученая степень и ученое звание, Ф.И.О.)

Директор научной библиотеки _____ Макаровская В.Г.

Рабочая программа дисциплины «Система сертификации и лицензирования деятельности по защите информации» пересмотрена, обсуждена и рекомендована к реализации в образовательном процессе на основании учебного плана ОПОП ВО 10.05.02 Информационная безопасность телекоммуникационных систем, специализация «Управление безопасностью телекоммуникационных систем и сетей», одобренного Ученым советом университета протокол №6 «26» 02 2021 г., на заседании
кафедры ИБ, протокол №11 от 30.06.2022.
(наименование кафедры, дата, номер протокола)

Зав. кафедрой М.О. Таныгин

Рабочая программа дисциплины «Система сертификации и лицензирования деятельности по защите информации» пересмотрена, обсуждена и рекомендована к реализации в образовательном процессе на основании учебного плана ОПОП ВО 10.05.02 Информационная безопасность телекоммуникационных систем, специализация «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 дисциплины

Целью преподавания дисциплины «Система сертификации и лицензирования деятельности по защите информации» является получение студентами знаний о основных подходах к разработке, реализации, эксплуатации, анализу, сопровождению и совершенствованию систем стандартизации и сертификации безопасности инфокоммуникационных сетей

1.2 Задачи дисциплины

−рассмотреть основы управления информационной безопасностью;

−рассмотреть оценочные стандарты в области информационной безопасности;

− рассмотреть создание системы управления информационной безопасности на предприятии;

− рассмотреть методики и технологии управления рисками;

− рассмотрение организационных меры обеспечения безопасности инфокоммуникационных систем.

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

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*		
ПК – 8	Способен организовать работы по выполнению требований защиты информации ограниченного доступа в телекоммуникационных системах и сетях	ПК – 8.1 управляет работой специалистов по созданию и эксплуатации средств защиты информации в телекоммуникационных системах и сетях	***Знать:*** современные подходы к управлению информационной безопасностью ТКС; ***Уметь:*** анализировать текущее состояние ИБ на предприятии с целью разработки требований к разрабатываемым процессам управления ИБ; ***Владеть (****или* ***Иметь опыт деятельности):*** терминологией и процессным подходом построения систем управления ИБ;

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*		
		ПК – 8.2 формирует комплекс мер (принципов, правил, процедур, практических приемов, методов, средств) для защиты в телекоммуникационных системах и сетях информации ограниченного доступа	***Знать:*** принципы управления рисками при эксплуатации ТКС; ***Уметь:*** определять цели и задачи, решаемые разрабатываемыми процессами управления ИБ; ***Владеть (****или* ***Иметь опыт деятельности):*** навыками организации и сопровождения аттестации объекта на соответствие требованиям государственных или корпоративных нормативных документов;
		ПК – 8.3 управляет процессом разработки моделей угроз и моделей нарушителя безопасности компьютерных систем	***Знать:*** модели угроза и модели нарушителей безопасности в компьютерных системах ***Уметь:*** определять классы нарушителей и ряд угроз, реализуемых в определённых условиях состояния системы безопасности ***Владеть (****или* ***Иметь опыт деятельности):*** разработкой моделей угроз и нарушителей безопасности компьютерных систем
		ПК – 8.4 разрабатывает организационно-распорядительные документы, регламентирующие порядок эксплуатации телекоммуникационных систем и сетей	***Знать:*** основные стандарты, регламентирующие управление информационной безопасности; ***Уметь:*** актуализировать версии организационно-распорядительной документации для эксплуатации телекоммуникационных систем и сетей согласно изменениям, в системе безопасности ***Владеть (****или* ***Иметь опыт деятельности):*** разрабатывать документацию, регламентирующую порядок эксплуатации телекоммуникационных

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*		
			систем и сетей
		ПК – 8.5 определяет действия сотрудников при проведении мероприятий по информационной безопасности	***Знать:*** порядок действия сотрудников во время проведения мероприятий, направленных на поддержание информационной безопасности ***Уметь:*** используя современные методы и средства разрабатывать процессы проведения классификации и сертификации, учитывающие особенности телекоммуникационных систем, и оценивать их эффективность ***Владеть (****или* ***Иметь опыт деятельности):*** навыками составления порядка действия сотрудников для проведения мероприятий по информационной безопасности

2 Указание места дисциплины в структуре основной профессиональной образовательной программы

Дисциплина «Система сертификации и лицензирования деятельности по защите информации» входит в часть, формируемую участниками образовательных отношений, блока 1 «Дисциплины (модули)» основной профессиональной образовательной программы – программы специалитета 10.05.02 Информационная безопасность телекоммуникационных систем специализация «Управление безопасностью телекоммуникационных сетей и систем». Дисциплина изучается на 5 курсе в 10 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 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)	56.1
в том числе:	
лекции	28
лабораторные занятия	0
практические занятия	28
Самостоятельная работа обучающихся (всего)	51.9
Контроль (подготовка к экзамену)	0
Контактная работа по промежуточной аттестации (всегоАттКР)	0,1
в том числе:	
зачет	0,1
зачет с оценкой	не предусмотрен
курсовая работа (проект)	не предусмотрена
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	Оценочные стандарты в информационной безопасности	Роль стандартов ИБ, «Оранжевая книга» как оценочный стандарт, Международный стандарт ISO/IEC 15408, критерии оценки безопасности информационных систем.
2	Стандарты управления информационной безопасностью	Стандарты управления информационной безопасностью BS 7799 и ISO/IEC 17799. Их основные положения, международный стандарт ISO/IEC 27001:2005, сертификация СУИБ на соответствие ISO 27001.
3	Международные стандарты информационной безопасности	Стандарты комитета технической безопасности ETSI. Стандарт «надлежащей практики». Североамериканская корпорация по надежности электроснабжения (NERC). Рамки информационной безопасности NIST (NIST CSF). RFC 2196 ISA / IEC-62443. Программа оценки соответствия. Немецкий стандарт BSI

4	Стандартизация в области облачных технологий	Стандарты, регулирующие безопасность облачных услуг. совместимость систем управления облаком между провайдером и заказчиком. Проекты международных стандартов по облачным вычислениям. Российская стандартизация облачных вычислений
5	Управление рисками. Основные понятия.	Выбор анализируемых объектов и уровня детализации их рассмотрения. Выбор методики оценки рисков.. Инвентаризация активов. Анализ угроз и их последствий, выявление уязвимых мест в защите. Оценка рисков.. Обработка рисков. Выбор защитных мер. Реализация и проверка выбранных мер.. Оценка остаточного риска
6	Методика оценки рисков информационной безопасности компании Digital Security	Описание архитектуры ИС. Расчет рисков по угрозе конфиденциальность Учет наличия доступа при помощи VPN. Расчет рисков по угрозе целостность
7	Методики и технологии управления рисками	Качественные методики управления рисками, количественные методики управления рисками, метод CRAMM.
8	Разработка корпоративной методики анализа рисков	Методы оценивания информационных рисков, табличные методы оценки рисков, методика анализа рисков Microsoft
9	Лицензирование деятельности в области ТЗИ.	Общий порядок лицензирования. Порядок получения лицензии следующий. Документы при лицензировании. Прекращение лицензии. Виды деятельности на осуществление которых требуется получение лицензии. Контроль за соблюдением лицензионных требований и условий.
10	Объект информатизации. Классификация объектов защиты.	Классификация информации. Классификация АС. Классификация СВТ. Политики разграничения доступа
11	Общий порядок сертификации средств защиты информации.	Понятие сертификации. Органы сертификации, их функции. Порядок проведения процедуры сертификации. Схемы проведения сертификации средств защиты информации.
12	Порядок сертификации во ФСТЭК России	Подача заявки на сертификацию во ФСТЭК России. Решение на проведение сертификационных испытаний. Заключение договора с испытательной лабораторией. Подготовка исходных данных. Сертификационные испытания.
13	Аттестация объекта информатизации по требованиям безопасности информации	Необходимость аттестации. Органы, проводящие аттестацию. Ответственность при проведении аттестации. Документальное сопровождение процедуры аттестации. Структура аттестата соответствия.
14	Требования и рекомендации по защите информации, обрабатываемой средствами вычислительной техники	Структура и содержание СТР-К. Обязательные требования. Желательные требования к объектам информатизации. Порядок обеспечения защиты информации в АС. Требования и рекомендации в зависимости от типа АС. Основные рекомендации по защите информации, составляющей коммерческую тайну.

Таблица 4.1.2 –Содержание дисциплины и его методическое обеспечение

№ п/п	Раздел учебной дисциплины	Виды учебной деятельности			Учебно-методические материалы	Формы текущего контроля успеваемости *(по неделям семестра)*	Компетенции
		лек.	№ лаб.	№ пр.			
1	Оценочные стандарты в информационной безопасности	2	-	1	У-1, МО-1	С	ПК – 8.1
2	Стандарты управления информационной безопасностью	2	-		У-1-3, 6	С	ПК – 8.3
3	Международные стандарты информационной безопасности	2	-	2	У-1,4-6, МО-2	С	ПК – 8.3
4	Стандартизация в области облачных технологий	2	-		У-2,8, МО-3	С	ПК – 8.4
5	Управление рисками. Основные понятия.	2	-		У-1	С	ПК – 8.1
6	Методика оценки рисков информационной безопасности компании Digital Security	2	-		У-1,4-6 МО-4	С	ПК – 8.2
7	Методики и технологии управления рисками	2	-		У-1,7	С	ПК – 8.1
8	Разработка корпоративной методики анализа рисков	2	-		У-1,4-6	С	ПК – 8.5
9	Лицензирование деятельности в области ТЗИ.	2	-	3	У-1,6,7	С, КО	ПК – 8.4
10	Объект информатизации. Классификация объектов защиты.	2	-		У-1,2	С, КО	ПК – 8.2
11	Общий порядок сертификации средств защиты информации.	2	-	4	У-4,5 МУ-3	С, КО	ПК – 8 .5
12	Порядок сертификации во ФСТЭК России	2	-		У-4,5	С, КО	ПК – 8.3
13	Аттестация объекта информатизации по требованиям безопасности информации	2	-		У-4,5 МУ-3	С, КО	ПК – 8.4
14	Требования и рекомендации по защите информации, обрабатываемой средствами вычислительной техники	2	-		У-4,5	С, КО	ПК – 8.5

С – собеседование, КО – контрольный опрос.

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	8
3	Составление обзорного документа по сертифицированным продуктам в заданной области информационной безопасности	8
4	Анализ заданного нормативно-правового акта Российской Федерации	6
Итого		28

4.3 Самостоятельная работа студентов (СРС)

Таблица 4.3 – Самостоятельнаяработа студентов

№ раздела (темы)	Наименование раздела (темы) дисциплины	Срок выполнения	Время, затрачиваемое на выполнение СРС, час
1	2	3	4
1.	Оценочные стандарты в информационной безопасности	2 неделя	2
2.	Стандарты управления информационной безопасностью	3 неделя	2
3.	Международные стандарты информационной безопасности	5 неделя	4
4.	Стандартизация в области облачных технологий	7 неделя	4
5.	Управление рисками. Основные понятия.	8 неделя	4
6.	Методика оценки рисков информационной безопасности компании Digital Security	10 неделя	4
7.	Методики и технологии управления рисками	11 неделя	4
8.	Разработка корпоративной методики анализа рисков	12 неделя	4
9.	Лицензирование деятельности в области ТЗИ.	13 неделя	4
10.	Объект информатизации. Классификация объектов защиты.	14 неделя	4
11.	Общий порядок сертификации средств защиты информации.	15 неделя	4
12.	Порядок сертификации во ФСТЭК России	16 неделя	4
13.	Аттестация объекта информатизации по требованиям безопасности информации	17 неделя	4
14.	Требования и рекомендации по защите информации, обрабатываемой средствами вычислительной техники	18 неделя	3,9
Итого			51,9

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 УП 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;

– тем рефератов;

– вопросов к зачету;

–методических указаний к выполнению лабораторных работ и т.д.

типографией университета:

– помощь авторам в подготовке и издании научной, учебной и методической литературы;

–удовлетворение потребности в тиражировании научной, учебной и 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 универсальных, общепрофессиональных и профессиональных компетенций обучающихся. В рамках дисциплины предусмотрено выполнение в ходе лабораторных практикоориентированных заданий.

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

№	Наименование раздела (темы лекции,	Используемые интерактивные	Объем,

	практического или лабораторного занятия)	образовательные технологии	час.
1	2	3	4
1	Выполнение практической №2 «Разработка структуры государственных и международных стандартов в Российской Федерации в области информационной безопасности и защиты информации»	Выполнение студентом интерактивных заданий по изучению системного подхода при создании структуры ГОСТ и ИСО.	6
2	Выполнение практической работы №3 «Составление обзорного документа по сертифицированным продуктам в заданной области информационной безопасности »	Выполнение студентом интерактивных заданий по анализу сертифицированных продуктов в заданной области информационной безопасности	6
Итого:			12

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 лабораторных занятий содержания, демонстрирующего обучающимся образцы настоящего научного подвижничества создателей и представителей данной отрасли науки, высокого профессионализма ученых, 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 обучающихся по дисциплине

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

Код и наименование компетенции	Этапы* формирования компетенций и дисциплины (модули)и практики, при изучении/ прохождении которых формируется данная компетенция		
	начальный	основной	завершающий
1	2	3	4
ПК – 8.1 управляет работой специалистов по созданию и эксплуатации средств защиты информации в телекоммуникационных системах и сетях	Порядок проведения аттестации объектов информатизации Организация и управление службой защиты информации Система сертификации и лицензирования деятельности по защите информации Производственная преддипломная практика Подготовка к процедуре защиты и защита выпускной квалификационной работы		
ПК – 8.2 формирует комплекс мер (принципов, правил, процедур, практических приемов, методов, средств) для защиты в телекоммуникационных системах и сетях информации ограниченного доступа			
ПК – 8.3 управляет процессом разработки моделей угроз и моделей нарушителя безопасности компьютерных систем			
ПК – 8.4 разрабатывает организационно-распорядительные документы, регламентирующие порядок эксплуатации телекоммуникационных систем и сетей			
ПК – 8.5 определяет действия сотрудников при проведении мероприятий по информационной безопасности			

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

Код компетенции/ этап	Показатели оценивания компетенций	Критерии и шкала оценивания компетенций		
		Пороговый уровень («удовлетворительно)	Продвинутый уровень (хорошо»)	Высокий уровень («отлично»)
1	2	3	4	5
ПК – 8 , начальный основной, завершающий	ПК – 8.1 управляет работой специалистов по созданию и эксплуатации средств защиты информации в телекоммуникационных системах и сетях	***Знать:*** - основы экономического обоснования проекта. ***Уметь:*** - анализировать исходные данные для обоснования целесообразности разработки проекта; - применять принципы выявления ключевых параметров работы ин-	***Знать:*** - основы формирования исходных данных для телекоммуникационных задач; ***Уметь:*** - анализировать исходные данные для обоснования целесообразности	***Знать:*** - основы формирования исходных данных для телекоммуникационных задач; - основы экономического обоснования проекта. ***Уметь:*** - анализировать исходные данные для обоснования целесообразно-

Код компетенции/ этап	Показатели оценивания компетенций	Критерии и шкала оценивания компетенций		
		Пороговый уровень («удовлетворительно)	Продвинутый уровень (хорошо»)	Высокий уровень («отлично»)
1	2	3	4	5
		формационной системы; ***Владеть (****или* ***Иметь опыт деятельности):*** - приемами анализа полноты и корректности ключевых параметров эксплуатации;	разработки проекта; - применять принципы выявления ключевых параметров работы информационной системы; ***Владеть (****или* ***Иметь опыт деятельности):*** - приемами анализа полноты и корректности ключевых параметров эксплуатации	сти разработки проекта; - анализировать предметную область и создавать декларативное описание задачи; - применять принципы выявления ключевых параметров работы информационной системы; ***Владеть (****или* ***Иметь опыт деятельности):*** - приемами анализа полноты и корректности ключевых параметров эксплуатации;
	ПК – 8.2 формирует комплекс мер (принципов, правил, процедур, практических приемов, методов, средств) для защиты в телекоммуникационных системах и сетях информации ограниченного доступа	***Знать:*** - технологии повышения защищенности распределенных информационных систем; ***Уметь:*** - проектировать регламент защищенного взаимодействия компонентов ТЛК системы; ***Владеть (****или* ***Иметь опыт деятельности):*** - навыками обеспечения совместимого взаимодействия отдельных модулей;	***Знать:*** - технологии повышения защищенности распределенных информационных систем; ***Уметь:*** - выполнять определять характер угрозы и масштабы последствий; - минимизировать последствия ущерба за счет интеграции средств защиты. ***Владеть (****или* ***Иметь опыт деятельности):*** - навыками разработки компонентов ТЛК систем; - навыками обеспечения совместимого взаимодействия отдельных модулей	***Знать:*** - технологии повышения защищенности распределенных информационных систем; ***Уметь:*** - выполнять определять характер угрозы и масштабы последствий; - проектировать регламент защищенного взаимодействия компонентов ТЛК системы; - минимизировать последствия ущерба за счет интеграции средств защиты. ***Владеть (****или* ***Иметь опыт деятельности):*** - навыками разработки компонентов ТЛК систем; - навыками обеспечения совместимого взаимодействия отдельных модулей;

Код компетенции/ этап	Показатели оценивания компетенций	Критерии и шкала оценивания компетенций		
		Пороговый уровень («удовлетворительно)	Продвинутый уровень (хорошо»)	Высокий уровень («отлично»)
1	2	3	4	5
	ПК – 8.3 управляет процессом разработки моделей угроз и моделей нарушителя безопасности компьютерных систем	***Знать:*** - основы использования управляющих директив. ***Уметь:*** - минимизировать количество потенциальных нештатных ситуаций работы программы. ***Владеть (****или* ***Иметь опыт деятельности):*** - технологией ведения протокола работы системы с выводом промежуточных результатов обработки данных.	***Знать:*** - особенности вывода промежуточных значений в ходе работы модулей; ***Уметь:*** - минимизировать количество потенциальных нештатных ситуаций работы программы. ***Владеть (****или* ***Иметь опыт деятельности):*** - установки директив, определяющих работу программных модулей	***Знать:*** - особенности вывода промежуточных значений в ходе работы модулей; - основы использования управляющих директив. ***Уметь:*** - выполнять отладку приложения в пошаговом режиме и с контрольными точками; - минимизировать количество потенциальных нештатных ситуаций работы программы. ***Владеть (****или* ***Иметь опыт деятельности):*** - установки директив, определяющих работу программных модулей; - технологией ведения протокола работы системы с выводом промежуточных результатов обработки данных.
	ПК – 8.4 разрабатывает организационно-распорядительные документы, регламентирующие порядок эксплуатации телекоммуникационных систем и сетей	***Знать:*** - основы работы в режиме пошаговой отладки передачи конфиденциальных данных в информационной системе; - основы шифрования потоков данных; ***Уметь:*** - выводить сообщения в случае возникновения нештатных ситуаций работы информационной системы; - интегрировать средства защиты на программном уровне. ***Владеть (****или* ***Иметь опыт деятельности):*** - навыками оценки защищенности информационной системы с уче-	***Знать:*** - основы шифрования потоков данных; - основы использования средств защиты информации. ***Уметь:*** - организовать безопасную работу в масштабе вычислительной сети; - выводить сообщения в случае возникновения нештатных ситуаций работы информационной системы; - интегрировать	***Знать:*** - основы работы в режиме пошаговой отладки передачи конфиденциальных данных в информационной системе; - основы шифрования потоков данных; - основы использования средств защиты информации. ***Уметь:*** - организовать безопасную работу в масштабе вычислительной сети; - выводить сообщения в случае возникновения нештатных ситуаций работы информационной системы; - интегрировать средства защиты на про-

Код компетенции/ этап	Показатели оценивания компетенций	Критерии и шкала оценивания компетенций		
		Пороговый уровень («удовлетворительно)	Продвинутый уровень (хорошо»)	Высокий уровень («отлично»)
1	2	3	4	5
		том возможных угроз.	средства защиты на программном уровне. ***Владеть (****или* ***Иметь опыт деятельности):*** - навыками установки программных средств защиты	граммном уровне. ***Владеть (****или* ***Иметь опыт деятельности):*** - навыками установки программных средств защиты; - навыками оценки защищенности информационной системы с учетом возможных угроз.
	ПК – 8.5 определяет действия сотрудников при проведении мероприятий по информационной безопасности	***Знать:*** - модели жизненного цикла программного обеспечения; ***Уметь:*** - разрабатывать базовые компоненты ТЛК систем; ***Владеть (****или* ***Иметь опыт деятельности):*** - навыками интеграции отдельных компонентов в состав единой распределенной системы.	***Знать:*** - этапы разработки программного обеспечения; - модели жизненного цикла программного обеспечения; ***Уметь:*** - принимать обоснованные решения по выбору технологий разработки; ***Владеть (****или* ***Иметь опыт деятельности):*** - навыками разработки компонентов ТЛК систем на программном уровне; - навыками интеграции отдельных компонентов в состав единой распределенной системы.	***Знать:*** - этапы разработки программного обеспечения; - модели жизненного цикла программного обеспечения; ***Уметь:*** - разрабатывать базовые компоненты ТЛК систем; - принимать обоснованные решения по выбору технологий разработки; ***Владеть (****или* ***Иметь опыт деятельности):*** - навыками разработки компонентов ТЛК систем на программном уровне; - навыками интеграции отдельных компонентов в состав единой распределенной системы.

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	Оценочные стандарты в информационной безопасности	ПК – 8.1	Лекция, практическая работа, СРС	Собеседование	1-5	Согласно табл. 7.2
				Контрольные вопросы к ПР №1	1-7	
2	Стандарты управления информационной безопасностью	ПК – 8.3	Лекция, СРС	Собеседование	6-10	Согласно табл. 7.2
3	Международные стандарты информационной безопасности	ПК – 8.3	Лекция, СРС, практическая работа	Собеседование	11-15	Согласно табл. 7.2
				Контрольные вопросы к ПР №2	1-9	
4	Стандартизация в области облачных технологий	ПК – 8.4	Лекция, СРС, практическая работа	Собеседование	16-20	Согласно табл. 7.2
5	Управление рисками. Основные понятия	ПК – 8.1	Лекция, СРС	Собеседование	21-25	Согласно табл. 7.2
6	Методика оценки рисков информационной безопасности компании Digital Security	ПК – 8.2	Лекция, СРС, практическая работа	Собеседование	25-30	Согласно табл. 7.2
7	Методики и технологии управления рисками	ПК – 8.1	Лекция, СРС	Собеседование	31-35	Согласно табл. 7.2
8	Разработка корпоративной методики анализа рисков	ПК – 8.5	Лекция, СРС	Собеседование	36-40	Согласно табл. 7.2
9	Лицензирова-	ПК – 8.4	Лекция, СРС	Собеседование	1-10	Согласно табл. 7.2

	ние деятельности в области ТЗИ.			Контрольные вопросы к ПР№3	1-8	
10	Объект информатизации. Классификация объектов защиты.	ПК – 8.2	Лекция, СРС	Собеседование	1-9	Согласно табл. 7.2
11	Общий порядок сертификации средств защиты информации.	ПК – 8.5	Лекция, СРС	Собеседование	1-8	Согласно табл. 7.2
				Контрольные вопросы к ПР№3	1-11	
12	Порядок сертификации во ФСТЭК России	ПК – 8.3	Лекция, СРС	Собеседование	1-8	Согласно табл. 7.2
13	Аттестация объекта информатизации по требованиям безопасности информации	ПК – 8.4	Лекция, СРС	Собеседование	1-7	Согласно табл. 7.2
14	Требования и рекомендации по защите информации, обрабатываемой средствами вычислительной техники	ПК – 8.5	Лекция, СРС	Собеседование	1-7	Согласно табл. 7.2

Примеры типовых контрольных заданий для проведения текущего контроля успеваемости

Вопросы для собеседования по разделу (теме) Тема 8. Разработка корпоративной методики анализа рисков.

1. Цели и задачи работ по анализу рисков в системе
2. Этапы проведения работ по анализу рисков
3. Как формируется стратегия управления рисками и на основании каких критериев
4. Опишите основные методы анализа рисков
5. Приведите пример оценки риска.
6. Назначение и задачи планирования управления рисками

Контрольные вопросы к практической работе 1 «Определение класса государственной информационной системы (ГИС)

1. Какие функции выполняет СЗИ предприятия для решения задач защиты информации?
2. Как строится структура полномасштабной системы обеспечения безопасности и защиты информации предприятия?
3. Какова специфика организации и выполнения охранных функций?
4. Каковы суть и содержание нормативной основы организации ЗСИ?
5. Какие факторы влияют на формирование организационно-правового обеспечения защиты информации?
6. Какова структура организационно-правовой основы защиты информации?
7. Опишите организационно-правовые мероприятия по защите конфиденциальной информации.

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

Типовые задания для проведения промежуточной аттестации обучающихся

Промежуточная аттестация по дисциплине проводится в форме зачета. Зачет проводится в виде компьютерного тестирования.

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. 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 сложно-

сти. Такой формат КИМ позволяет объективно определить качество освоения обучающимися основных элементов содержания дисциплины и уровень сформированности компетенций.

Примеры типовых заданий для проведения промежуточной аттестации обучающихся

Задание в закрытой форме:
Используя браузер выполняется запрос методом ___.

Задание в открытой форме:
Вредоносные вставки при обращении к базе данных называются:
- инъекциями
- синхронизацией
-транзакциями

Задание на установление правильной последовательности,
Пользователь зарегистрирован, авторизован, аутентифицирован.

Задание на установление соответствия:
1 Наиболее эффективный в системах обработки конфиденциальных данных алгоритм
2 Наиболее эффективный в системах реального времени алгоритм диспетчеризации
3 Наиболее просто реализуемый алгоритм
4 Алгоритм, позволяющий реализовывать динамические приоритеты
5 Алгоритм, при котором процесс может оставаться неограниченно долго в режиме ожидания
А "самый короткий - следующий"
Б алгоритм планирования согласно приоритетам
В "самый длинный - следующий"
Г выбор случайного процесса

Компетентностно-ориентированная задача:
В качестве входной информации берется текстовый файл, состоящий из ФИО студента, названия кафедры и специальности. Исходный поток данных соответствует последовательности бит, расположение которых определяется формулой, учитывающей порядковый номер студента по списку.

$$ci = (7i+n) \bmod 13 + 13i$$

Ключ скремблера соответствует номеру зачетки студента «слева направо», генератор псевдослучайных чисел - аналогично «справа налево».

Порядок выполнения работы:
1. Сформировать блок исходных данных (не более 48 бит)

2. Рассчитать состояния скремблера для обработки входного блока
3. Рассчитать период зацикливания и период наибольшей длины скремблера.
4. Произвести скремблирование исходных данных.
5. Подобрать скремблер минимальной разрядности, который не зациклится при обработке всего исходного файла.

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 02.016–2018 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
Определение класса государственной информационной системы (ГИС)	4	Выполнил, но «не защитил»	6	Выполнил и «защитил»
Разработка структуры государственных и международных стандартов в Российской Федерации в области информационной безопасности и защиты информации	4	Выполнил, но «не защитил»	6	Выполнил и «защитил»
Составление обзорного документа по сертифицированным продуктам в заданной области информационной безопасности	4	Выполнил, но «не защитил»	6	Выполнил и «защитил»
Анализ заданного нормативно-правового акта Российской Федерации	4	Выполнил, но «не защитил»	6	Выполнил и «защитил»
СРС	8		24	
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 : [16+] / А. Л. Марухленко, Л. О. Марухленко, М. А. Ефремов и др. – Москва ; Берлин : Директ-Медиа, 2021. – 210 с. : ил., схем., табл. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=598988 (дата обращения: 07.09.2021). – Библиогр.: с. 196-205. – ISBN 978-5-4499-1671-6. – DOI 10.23681/598988. – Текст : электронный.

2 Крылова, Г. Д. Основы стандартизации, сертификации, метрологии : учебник / Г. Д. Крылова. - 3-е изд., перераб. и доп. - Москва : Юнити-Дана, 2015. - 671 с. - URL: http://biblioclub.ru/index.php?page=book&id=114433 (дата обращения: 09.09.2019) . - режим доступа: по подписке. - Текст : электронный.

3 Камардин, Н. Б. Метрология, стандартизация, подтверждение соответствия : учебное пособие / Н. Б. Камардин, И. Ю. Суркова. - Казань : Издательство КНИТУ, 2013. - 240 с. - URL: http://biblioclub.ru/index.php?page=book&id=258829 (дата обращения: 09.09.2019) . - режим доступа: по подписке. - Текст : электронный.

8.2 Дополнительная учебная литература

1. 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. : ил., табл. - ISBN 978-5-7681-08 57-1. – Текст: непосредственный.

2. Организационно-правовое обеспечение информационной безопасности [Текст] : учебное пособие / под ред. А. А. Стрельцова. - М. : Академия, 2008. - 256 с.

3. Романов, О. А. Организационное обеспечение информационной безопасности [Текст] : учебник / О. А. Романов, С. А. Бабин, С. Г. Жданов. - М. : Академия, 2008. - 192 с.

4. Титов, В. С. Метрология, стандартизация и сертификация : учебное пособие / В. С. Титов, В. Е. Эрастов ; Министерство образования и науки Российской Федерации, Курский государственный технический университет. - Курск : КГТУ, 2005. - 184 с. - ISBN 5-7681-0240-X : 85.00 р. - Текст : непосредственный.

5. Кретова, Валерия Михайловна. Метрология, стандартизация и сертификация : конспект лекций / В. М. Кретова ; МИНОБРНАУКИ РОССИИ, Юго-Западный государственный университет. - Курск : ЮЗГУ, 2011. - 168 с. - Имеется электрон.аналог. - 170 р. - Текст : непосредственный.

1.3 Перечень методических указаний

1) Определение класса государственной информационной системы (ГИС) [Электронный ресурс] : методические указания по выполнению практической работы : [для студентов укрупненной группы специальностей 10.00.00 дневной формы обучения] / Юго-Зап. гос. ун-т ; сост.: Е. С. Волокитина, М. О. Таныгин. - Курск : ЮЗГУ, 2017. - 12 с.

2) Разработка структуры государственных и международных стандартов в Российской Федерации в области информационной безопасности и защиты информации [Электронный ресурс] : методические указания по выполнению практической работы : [для студентов укрупненной группы специальностей 10.00.00 дневной формы обучения] / Юго-Зап. гос. ун-т ; сост.: Е. С. Волокитина, М. О. Таныгин. - Курск : ЮЗГУ, 2017. - 7 с.

3) Составление обзорного документа по сертифицированным продуктам в заданной области информационной безопасности [Электронный ресурс] : методические указания по выполнению практической работы : [для студентов укрупненной группы специальностей 10.00.00 дневной формы обучения] / Юго-Зап. гос. ун-т ; сост.: Е. С. Волокитина, М. О. Таныгин. - Курск : ЮЗГУ, 2017. - 7 с.

4) Анализ заданного нормативно-правового акта Российской Федерации [Электронный ресурс] : методические указания по выполнению практической работы : [для студентов укрупненной группы специальностей 10.00.00 дневной формы обучения] / Юго-Зап. гос. ун-т ; сост.: Е. С. Волокитина, М. О. Таныгин. - Курск : ЮЗГУ, 2017. - 7 с.

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

1. http://biblioclub.ru - Электронно-библиотечная система «Университетская библиотека онлайн».
2. www.elibrary.ru/defaultx.asp - научная электронная библиотека.
3. www.edu.ru - федеральный портал «Российское образование».
4. www.consultant.ru - Официальный сайт компании «Консультант Плюс».
5. Федеральная служба безопасности [официальный сайт]. Режим доступа: http://www.fsb.ru/.

6. Научно-информационный портал ВИНИТИ РАН [официальный сайт]. Режим доступа: http://www.consultant.ru/

10 Методические указания для обучающихся по освоению дисциплины

Основными видами аудиторной работы студента при изучении дисциплины «Система сертификации и лицензирования деятельности по защите информации» являются лекции 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 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.

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 готовят рефераты по отдельным темам дисциплины, выступают 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 работам, а также по результатам докладов.

Преподаватель уже на первых занятиях объясняет студентам, какие формы обучения следует использовать при самостоятельном изучении дисциплины «Система сертификации и лицензирования деятельности по защите информации»: 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, отработку студентами пропущенных лекций, 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 закрепления 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 освоению учебного материала. В случае необходимости студенты обращаются за консультацией к преподавателю по вопросам дисциплины «Система сертификации и лицензирования деятельности по защите информации» с целью освоения и закрепления компетенций.

Основная цель самостоятельной работы студента при изучении дисциплины «Система сертификации и лицензирования деятельности по защите информации» - 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)

Microsoft Office 2016.Лицензионный договор №S0000000722 от 21.12.2015 г. с ООО «АйТи46», лицензионный договор №K0000000117 от 21.12.2015 г. с ООО «СМСКанал», Kaspersky Endpoint Security Russian Edition, лицензия 156A-140624-192234,Windows 7, договор IT000012385

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

Учебная аудитория для проведения занятий лекционного и практического типа или лаборатории кафедры информационная безопасность, оснащенные мебелью: столы, стулья для обучающихся; стол, стул для преподавателя; доска, проектор для демонстрации презентаций. Помещение для самостоятельной работы Компьютер PDC2160/iC33/2*512Mb/HDD 160Gb/DVD-ROM/FDD/ATX350W/ K/m/ OFF/l 7"TFT E700 (6 шт)

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 такжесурдопереводчиков и тифлосурдопереводчиков. Текущий контроль успеваемости осуществляется в письменной форме: обучающийся письменноотвечает 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
	измененных	замененных	аннулированных	новых			