Приложение 5

Федеральное государственное бюджетное образовательное учреждение высшего образования «Тамбовский государственный университет имени Г.Р. Державина»
Институт математики, физики и информационных технологий
Кафедра математического моделирования и информационных технологий

УТВЕРЖДАЮ:
Директор института

И. Н. Якунина
«20» января 2021 г.

РАБОЧАЯ ПРОГРАММА

по дисциплине Б1.В.ОД.1 Аудит и аттестация объектов информатизации

Направление подготовки/специальность: 10.03.01 - Информационная безопасность

Профиль/направленность/специализация: Безопасность компьютерных систем

Уровень высшего образования: бакалавриат

Квалификация: Бакалавр

год набора: 2020

Тамбов, 2021

Автор программы:
Кандидат технических наук, доцент Зауголков Игорь Алексеевич

Рабочая программа составлена в соответствии с ФГОС ВО по направлению подготовки 10.03.01 - Информационная безопасность (уровень бакалавриата) (приказ Министерства образования и науки РФ от «01» декабря 2016 г. № 1515).

Рабочая программа принята на заседании Кафедры математического моделирования и информационных технологий «22» декабря 2020 г. Протокол № 4

Рассмотрена и одобрена на заседании Ученого совета Института математики, физики и информационных технологий, Протокол от «20» января 2021 г. № 1.

СОДЕРЖАНИЕ

1 Цели и задачи дисциплины…… 4

2 Место дисциплины в структуре ОП бакалавра…….. 6

3 Объем и содержание дисциплины…… 6

4 Контроль знаний обучающихся и типовые оценочные средства…… 10

5 Методические указания для обучающихся по освоению дисциплины (модуля)…….. 27

6 Учебно-методическое и информационное обеспечение дисциплины…… 28

7 Материально-техническое обеспечение дисциплины, программное обеспечение, профессиональны 29

1. Цели и задачи дисциплины

1.1 Цель дисциплины – формирование компетенций:

ПК-5 Способность принимать участие в организации и сопровождении аттестации объекта информатизации по требованиям безопасности информации

ПК-8 Способность оформлять рабочую техническую документацию с учетом действующих нормативных и методических документов

ПК-10 Способность проводить анализ информационной безопасности объектов и систем на соответствие требованиям стандартов в области информационной безопасности

1.2 Виды и задачи профессиональной деятельности по дисциплине:

- экспериментально-исследовательская
  - сбор, изучение научно-технической информации, отечественного и зарубежного опыта по тематике исследования
  - проведение экспериментов по заданной методике, обработка и анализ их результатов
  - проведение вычислительных экспериментов с использованием стандартных программных средств
- эксплуатационная
  - установка, настройка, эксплуатация и поддержание в работоспособном состоянии компонентов системы обеспечения информационной безопасности с учетом установленных требований
  - администрирование подсистем информационной безопасности объекта
  - участие в проведении аттестации объектов информатизации по требованиям безопасности информации и аудите информационной безопасности автоматизированных систем

1.3 В результате освоения дисциплины у обучающихся должны быть сформированы следующие компетенции:

Обобщенные трудовы	Код и наименование ко	Знания и умения, необходимые дл
	ПК-5 Способность принима	Знает и понимает:
		Знает: порядок проведения аттестационных испытаний
		Умеет (способен продемонстрировать):
		Умеет: подготавливать объекты информатизации к атте
		Владеет:
		Владеет: навыками оформления результатов аттестаци
	ПК-8 Способность оформл	Знает и понимает:
		Знает перечень технических средств защиты информац
		Умеет (способен продемонстрировать):
		Умеет (способен продемонстрировать): отыскивать нео
		Владеет:
		Владеет: навыками организации технологического про
	ПК-10 Способность провод	Знает и понимает:
		Знает требования стандартов в области информационно
		Умеет (способен продемонстрировать):
		Умеет проводить анализ информационной безопасност
		Владеет:
		Владеет подготовкой необходимых материалов для пол

1.4 Согласование междисциплинарных связей дисциплин, обеспечивающих освоение компетенций:

ПК-5 Способность принимать участие в организации и сопровождении аттестации объекта информатизации по требованиям безопасности информации

№	Наименование д	Форм

п/п		Очна (семе
		7
1	Эксплуатационная пр	+

ПК-8 Способность оформлять рабочую техническую документацию с учетом действующих нормативных и методических документов

№ п/п	Наименование д	Форма		
		Очная (семест		
		6	7	8
1	Практика по получени	+		
2	Преддипломная практ			+
3	Эксплуатационная пр		+	

ПК-10 Способность проводить анализ информационной безопасности объектов и систем на соответствие требованиям стандартов в области информационной безопасности

№ п/п	Наименование д	Форм	
		Очна (семе	
		5	8
1	Преддипломная практ		+
2	Теория систем и систе	+	
3	Экспертные системы	+	

2. Место дисциплины в структуре ОП бакалавриата:

Дисциплина «Аудит и аттестация объектов информатизации» относится к вариативной части учебного плана ОП по направлению подготовки 10.03.01 - Информационная безопасность.

Дисциплина «Аудит и аттестация объектов информатизации» изучается в 7, 8 семестрах.

3.Объем и содержание дисциплины

3.1.Объем дисциплины: 8 з.е.

Очная: 8 з.е.

Вид учебной работы	Очная (всего часов)
Общая трудоёмкость дисциплины	**288**
Контактная работа	126
Лекции (Лекции)	50
Лабораторные (Лаб. раб.)	76
Самостоятельная работа (СР)	126
Экзамен	36
Зачет	-

3.2.Содержание курса:

№ темы	Название раздела/темы	Вид учебной работы, час.	Формы текущего контроля

		Лекции	Лаб. раб.	СР	
		О	О	О	
7 семестр					
1	Введение.	4	12	14	Собеседование
2	Основы Законодательства РФ, руководящие и нормативные документы ФСТЭК (Гостехкомиссии) России, регламентирующие вопросы защиты информации.	4	14	20	Выполнение лабораторных работ ; Собеседование; Тестирование
3	Организация защиты автоматизированных систем и их компонентов от несанкционированного доступа.	6	14	20	Выполнение лабораторных работ ; Собеседование; Реферат
8 семестр					
4	Порядок подготовки и проведения аттестации объектов информатизации по требованиям ФСТЭК России.	12	11	18	Выполнение лабораторных работ ; Собеседование
5	Порядок проведения сертификационных испытаний средств защиты информации.	12	14	26	Выполнение лабораторных работ ; Собеседование
6	Порядок лицензирования деятельности по защите информации ФСТЭК России.	12	11	28	Выполнение лабораторных работ ; Собеседование

Тема 1. Введение. (ПК-10)

Лекция.

Предмет, цели, задачи и содержание курса «Аттестация объектов информатизации». Базовые знания, необходимые для изучения курса. Рекомендуемые учебные пособия.

Лабораторные работы.

Роль и место курса в подготовке специалистов по организации защиты информации в государственных и коммерческих структурах.

Задания для самостоятельной работы.

1.Проработка конспектов лекций и вопросов, вынесенных на самостоятельное изучение основной и дополнительной литературы.

2.Подготовка к тестированию.

Тема 2. Основы Законодательства РФ, руководящие и нормативные документы ФСТЭК (Гостехкомиссии) России, регламентирующие вопросы защиты информации. (ПК-10)

Лекция.

Федеральная служба по техническому и экспортному контролю (ФСТЭК России) — федеральный орган исполнительной власти России, осуществляющий реализацию государственной политики, организацию межведомственной координации и взаимодействия, специальные и контрольные функции в области государственной безопасности.

Приказ ФСТЭКРоссии от «14» марта 2014 г. n 31 "об утверждении требований к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами

Приказ ФСТЭК России № 21 от 18 февраля 2013 г. Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных

Лабораторные работы.

Специальные исследования ОТСС.

Задания для самостоятельной работы.

1. Проработка конспектов лекций и вопросов, вынесенных на самостоятельное изучение основной и дополнительной литературы.

2. Подготовка к тестированию.

Тема 3. Организация защиты автоматизированных систем и их компонентов от несанкционированного доступа. (ПК-10)

Лекция.

Внедрение современных информационных технологий (ИТ) на базе компьютерной техники и телекоммуникационных средств радикально изменили информационную среду.

Как следствие, усложнились процессы регулирования отношений между субъектами и информационными объектами. При решении задач защиты информации от НСД в АСОД предметом рассмотрения являются отношения доступа между субъектами и информационными объектами в среде программно-технического комплекса (ПТК) АСОД.

Рассматриваются отношения доступа между субъектами и элементами программно-технического комплекса, то есть программно-техническими ресурсами АСОД, и между элементами ПТК и информационными объектами, то есть информационными ресурсами АСОД. Естественно, предметом рассмотрения могут быть отношения доступа между элементами ПТК в определённых процессах, когда анализируются тракты доступа субъектов к информационным объектам.

Лабораторные работы.

Изучение средств измерений, применяемых при специальных исследованиях.

Задания для самостоятельной работы.

1. Проработка конспектов лекций и вопросов, вынесенных на самостоятельное изучение основной и дополнительной литературы.

2. Подготовка к тестированию, контрольной работе.

Тема 4. Порядок подготовки и проведения аттестации объектов информатизации по требованиям ФСТЭК России. (ПК-8)

Лекция.

Порядок проведения аттестации объектов информатизации по требованиям безопасности информации определяется следующими документами:

«Специальные требования и рекомендации по защите информации, составляющей государственную тайну, от утечки по техническим каналам», утверждены решением Гостехкомиссии России от 23 мая 1997 года № 55;

«Положение по аттестации объектов информатизации по требованиям безопасности информации», утверждено Председателем Гостехкомиссии России 25 ноября 1994 года;

«Методические рекомендации управлениям ФСТЭК России по федеральным округам об организации работ по аттестации объектов информатизации по требованиям безопасности информации, приказ Директора ФСТЭК России от 21 апреля 2006 года № 126.

Порядок проведения аттестации объектов информатизации по требованиям безопасности информации включает:1. Подача заявки на аттестацию объекта информатизации.Заявитель для получения аттестата соответствия направляет в управление ФСТЭК России по федеральному округу (далее - Управление) заявку на проведение аттестации объекта информатизации с необходимыми исходными данными по установленной форме (приложение № 1).2. Рассмотрение заявки на аттестацию, принятие решения на ее проведение, доведение решения до заявителя и органа по аттестации объектов информатизации.

Лабораторные работы.

Организация аттестации автоматизированных систем по требованиям безопасности информации в части защиты от НСД.

Задания для самостоятельной работы.

1. Проработка конспектов лекций и вопросов, вынесенных на самостоятельное изучение основной и дополнительной литературы.

2. Подготовка к тестированию.

Тема 5. Порядок проведения сертификационных испытаний средств защиты информации. (ПК-5)

Лекция.

Сертификация средств защиты информации производится в соответствии с "Положением о сертификации средств защиты информации", утвержденным постановлением Правительства Российской Федерации от 26 июня 1995 г.

Сертификация - форма осуществляемого органом по сертификации подтверждения соответствия объектов требованиям технических регламентов, положениям стандартов, сводов правил или условиям договоров.

Сертификат соответствия - документ, удостоверяющий соответствие объекта требованиям технических регламентов, положениям стандартов, сводов правил или условиям договоров.

Технические, криптографические, программные и другие средства, предназначенные для защиты сведений, составляющих государственную тайну, средства, в которых они реализованы, а также средства контроля эффективности защиты информации являются средствами защиты информации.

Указанные средства подлежат обязательной сертификации, которая проводится в рамках систем сертификации средств защиты информации

Лабораторные работы.

Проверка организационно-распорядительных документов.

Задания для самостоятельной работы.

1. Проработка конспектов лекций и вопросов, вынесенных на самостоятельное изучение основной и дополнительной литературы.

2. Подготовка к тестированию.

Тема 6. Порядок лицензирования деятельности по защите информации ФСТЭК России. (ПК-5)

Лекция.

Лицензирование деятельности по технической защите конфиденциальной информации-это вид деятельности направленный на выполнение работ и оказание услуг по ее защите от несанкционированного доступа, от ее утечки по техническим каналам, а также от специальных воздействий на такую информацию в целях ее уничтожения, искажения или блокирования доступа к ней.

В соответствии с Постановлением Правительства Российской Федерации от 3 февраля 2012 г. N 79 г. Москва "О лицензировании деятельности по технической защите конфиденциальной информации" лицензию по технической защите конфиденциальной информации обязаны получить организации, которые собираются осуществлять перечисленные ниже виды деятельности:

1) контроль защищенности конфиденциальной информации от утечки по техническим каналам;

2) контроль защищенности конфиденциальной информации от несанкционированного доступа и ее модификации в средствах и системах информатизации;

3) сертификационные испытания на соответствие требованиям по безопасности информации продукции, используемой в целях защиты конфиденциальной информации;

4) аттестационные испытания и аттестация на соответствие требованиям по защите информации;

5) установка, монтаж, испытания, ремонт средств защиты информации (технических средств защиты информации, защищенных технических средств обработки информации, технических средств контроля эффективности мер защиты информации, программных (программно-технических) средств защиты информации, защищенных программных (программно-технических) средств обработки информации, программных (программно-технических) средств контроля защищенности информации).

Лабораторные работы.

Контроль механизмов идентификации и аутентификации пользователей.

Задания для самостоятельной работы.

1. Проработка конспектов лекций и вопросов, вынесенных на самостоятельное изучение основной и дополнительной литературы.

2. Подготовка к тестированию, контрольной работе.

4. Контроль знаний обучающихся и типовые оценочные средства

4.1. Распределение баллов:

7 семестр

- посещаемость – 10 баллов
- текущий контроль – 70 баллов
- контрольные срезы – 2 среза по 10 баллов каждый
- премиальные баллы – 20 баллов

Распределение баллов по заданиям:

№ т мы	Название т	Формы	Max. ко	Методика проведения занятия и оце

1.	Введение.	**Собеседование(контрольный срез)**	10	Собеседование предполагает организацию беседы преподавателя с Устный опрос может применяться в различных формах: фронталь - правильность ответа по содержанию; - полнота и глубина ответа; - сознательность ответа; - логика изложения материала; - рациональность использованных приемов и способов решения п - своевременность и эффективность использования наглядных пос - использование дополнительного материала; - рациональность использования времени, отведенного на задание 10 баллов – студент умеет сопоставить полученную при подготовк 7 баллов - студент умеет применять полученную при подготовке к 5 балла – студент владеет теоретическим материалом по теме прак Если студент не владеет проблематикой практического занятия, не
2.	Основы Законод регламентир	Выполне	20	Лабораторные работы выполняются по текущему разделу или тем 20 баллов – лабораторная работа выполнена в полном объёме, студ 13 балла – лабораторная работа выполнена, но имеет некоторые не 6 баллов - лабораторная работа в целом выполнена, однако в проц
		Собесе	10	Собеседование предполагает организацию беседы преподавателя с Устный опрос может применяться в различных формах: фронталь - правильность ответа по содержанию; - полнота и глубина ответа; - сознательность ответа; - логика изложения материала; - рациональность использованных приемов и способов решения п - своевременность и эффективность использования наглядных пос - использование дополнительного материала; - рациональность использования времени, отведенного на задание 10 баллов – студент умеет сопоставить полученную при подготовк 7 баллов - студент умеет применять полученную при подготовке к 5 балла – студент владеет теоретическим материалом по теме прак Если студент не владеет проблематикой практического занятия, не
		Тестир	10	Оценка теста по текущему разделу или теме дисциплины
3.	Организация за	Выполне	20	Лабораторные работы выполняются по текущему разделу или тем 20 баллов – лабораторная работа выполнена в полном объёме, студ 13 балла – лабораторная работа выполнена, но имеет некоторые не 6 баллов - лабораторная работа в целом выполнена, однако в проц
		Собеседование(контрольный срез)	10	Собеседование предполагает организацию беседы преподавателя с Устный опрос может применяться в различных формах: фронталь - правильность ответа по содержанию; - полнота и глубина ответа; - сознательность ответа; - логика изложения материала; - рациональность использованных приемов и способов решения п - своевременность и эффективность использования наглядных пос - использование дополнительного материала; - рациональность использования времени, отведенного на задание 10 баллов – студент умеет сопоставить полученную при подготовк 7 баллов - студент умеет применять полученную при подготовке к 5 балла – студент владеет теоретическим материалом по теме прак Если студент не владеет проблематикой практического занятия, не
		Рефер	10	8-10 баллов – реферат выполнен обучающимся самостоятельно, в соответствии с правилами ГОСТа 6-7 баллов – во введение четко сформулированы основные позици 3-5 балла – во введение основные позиции реферата сформулиров 1-2 балла – текст реферата представляет несамостоятельное (комп

4.	Посещаемость	10	10 баллов – стопроцентное посещение занятий студентом 7-9 баллов – посещаемость студента составляет не менее 80 % зан 4-6 баллов – посещаемость студента составляет не менее 50 % зан 1-3 балла – посещаемость студента составляет не менее 25 % заня
5.	Премиальные б	20	Дополнительные премиальные баллы могут быть начислены: - за проект, выполненный по заказу работодателя и реализованный - постоянная активность во время практических занятий – 10 балл - полностью подготовленная к публикации статья по тематике в ра - участие с докладом во всероссийской олимпиаде по тематике изу - участие в выставке по тематике изучаемой дисциплины – 20 бал - публикация статьи по тематике изучаемой дисциплины в сборни
6.	Итого за семес	100	

8 семестр

- посещаемость – 10 баллов
- текущий контроль – 40 баллов
- контрольные срезы – 2 среза по 10 баллов каждый
- премиальные баллы – 20 баллов
- ответ на экзамене: не более 30 баллов

Распределение баллов по заданиям:

№ т мы	Название т	Формы	Max. ко	Методика проведения занятия и оце
1.	Порядок подгот	Выполне	10	Лабораторные работы выполняются по текущему разделу или тем 10 баллов – лабораторная работа выполнена в полном объёме, студ 5 баллов – лабораторная работа выполнена, но имеет некоторые не 3 балла - лабораторная работа в целом выполнена, однако в проце
		Собеседо вание(ко нтрольн ый срез)	10	Собеседование предполагает организацию беседы преподавателя с Устный опрос может применяться в различных формах: фронталы - правильность ответа по содержанию; - полнота и глубина ответа; - сознательность ответа; - логика изложения материала; - рациональность использованных приемов и способов решения п - своевременность и эффективность использования наглядных пос - использование дополнительного материала; - рациональность использования времени, отведенного на задание 10 баллов – студент умеет сопоставить полученную при подготовк 7 баллов - студент умеет применять полученную при подготовке к 5 балла – студент владеет теоретическим материалом по теме прак Если студент не владеет проблематикой практического занятия, не
2.	Порядок пров	Выполне	10	Лабораторные работы выполняются по текущему разделу или тем 10 баллов – лабораторная работа выполнена в полном объёме, студ 5 баллов – лабораторная работа выполнена, но имеет некоторые не 3 балла - лабораторная работа в целом выполнена, однако в проце

		Собесе	10	Собеседование предполагает организацию беседы преподавателя с Устный опрос может применяться в различных формах: фронталь - правильность ответа по содержанию; - полнота и глубина ответа; - сознательность ответа; - логика изложения материала; - рациональность использованных приемов и способов решения п - своевременность и эффективность использования наглядных пос - использование дополнительного материала; - рациональность использования времени, отведенного на задание 10 баллов – студент умеет сопоставить полученную при подготовк 7 баллов - студент умеет применять полученную при подготовке к 5 балла – студент владеет теоретическим материалом по теме прак Если студент не владеет проблематикой практического занятия, не
3.	Порядок лице	Выполне	10	Лабораторные работы выполняются по текущему разделу или тем 10 баллов – лабораторная работа выполнена в полном объёме, студ 6 балла – лабораторная работа выполнена, но имеет некоторые нет 3 балла - лабораторная работа в целом выполнена, однако в проце
		Собеседование(контрольный срез)	10	Собеседование предполагает организацию беседы преподавателя с Устный опрос может применяться в различных формах: фронталь - правильность ответа по содержанию; - полнота и глубина ответа; - сознательность ответа; - логика изложения материала; - рациональность использованных приемов и способов решения п - своевременность и эффективность использования наглядных пос - использование дополнительного материала; - рациональность использования времени, отведенного на задание 10 баллов – студент умеет сопоставить полученную при подготовк 7 баллов - студент умеет применять полученную при подготовке к 5 балла – студент владеет теоретическим материалом по теме прак Если студент не владеет проблематикой практического занятия, не
4.	Посещаемость		10	10 баллов – стопроцентное посещение занятий студентом 7-9 баллов – посещаемость студента составляет не менее 80 % зан 4-6 баллов – посещаемость студента составляет не менее 50 % зан 1-3 балла – посещаемость студента составляет не менее 25 % заня
5.	Премиальные б		20	Дополнительные премиальные баллы могут быть начислены: - за проект, выполненный по заказу работодателя и реализованный - постоянная активность во время практических занятий – 10 балл - полностью подготовленная к публикации статья по тематике в ра - участие с докладом во всероссийской олимпиаде по тематике изу - участие в выставке по тематике изучаемой дисциплины – 20 бал - публикация статьи по тематике изучаемой дисциплины в сборни
6.	Ответ на экзам		30	Оценка «удовлетворительно»- студент имеет достаточный минима Оценка «хорошо» – ▪достаточно полные и систематизированные з научных и профессиональных задач; усвоение основной и дополн - Оценка «отлично» – систематизированные и гл и полные знани дисциплины, а также по основным вопросам, выходящим за преде глубокое усвоение основной и дополнительной литературы, реком
7.	Итого за семес		100	

Итоговая оценка по экзамену выставляется в 100-балльной шкале и в традиционной четырехбалльной шкале. Перевод 100-балльной рейтинговой оценки по дисциплине в традиционную четырехбалльную осуществляется следующим образом:

100-балльная система	Традиционная система

85 - 100 баллов	Отлично
70 - 84 баллов	Хорошо
50 - 69 баллов	Удовлетворительно
Менее 50	Неудовлетворительно

4.2 Типовые оценочные средства текущего контроля

Выполнение лабораторных работ

Тема 2. Основы Законодательства РФ, руководящие и нормативные документы ФСТЭК (Гостехкомиссии) России, регламентирующие вопросы защиты информации.

Установление необходимости обработки (обсуждения) информации ограниченного доступа на объекте информатизации.

Цель работы Проанализировать перечень сведений конфиденциального характера, обрабатываемых в организации, и состав мероприятий по защите информации

Исполнение При проведении работ по защите государственных информационных ресурсов перечень сведений конфиденциального характера, обрабатываемых в организации, и состав мероприятий по защите информации устанавливают в соответствии с требованиями нормативных и методических документов по защите информации

Защита ЛР. Разработка перечня сведений конфиденциального характера, обрабатываемых в организации

Тема 3. Организация защиты автоматизированных систем и их компонентов от несанкционированного доступа.

Проверка документов на полноту и достаточность их содержания, а также проверка соответствия их содержания требованиям к безопасности информации.

Цель работы Проверка содержания документов на достаточность указанных в них сведений в соответствии с требованиями нормативных и методических документов по безопасности информации

Исполнение составление наименования и характеристики объекта информатизации;

• перечня технических и программных средств объекта информатизации;

определение класса защищенности объекта информатизации;

Защита ЛР. Разработка документов заявителя для проведения аттестации

Тема 4. Порядок подготовки и проведения аттестации объектов информатизации по требованиям ФСТЭК России.

Изучение технологического процесса автоматизированной обработки информации ограниченного доступа

Цель работы Изучается схема информационных потоков в автоматизированной системе. Определяются возможности доступа к хранимой, обрабатываемой и передаваемой информации

Исполнение В описании технологического процесса обработки информации должны быть указаны:

• перечень субъектов доступа (сотрудников организации);

• перечень объектов доступа;

• режим обработки информации (однопользовательский и мно- гопользовательский);

особенности обработки, хранения, удаления, передачи и ко- пирования информации, а также доступа к ней

Тема 5. Порядок проведения сертификационных испытаний средств защиты информации.

Проверка соответствия состава и структуры программно-технических средств автоматизированной системы представленной документации

Цель работы Выявляются программно-технические средства, потенциально опасные с точки зрения обеспечения безопасности обработки, хра- нения и передачи информации ограниченного доступа

Исполнение При наличии установленных в автоматизированной системе средств разработки и отладки программного обеспечения проверяются условия эксплуатации этих программных средств на соответствие требованиям нормативных и методических документов по защите информации

Тема 6. Порядок лицензирования деятельности по защите информации ФСТЭК России.

Разграничение доступа пользователей на объекте информатизации

Цель работы Определение уровней полномочий пользователей по доступу к информации ограниченного доступа, обрабатываемой и (или) обсуждаемой на объекте информатизации

Исполнение Проверяется соответствие разрешительной системы доступа требованиям нормативных и методических документов по безо- пасности информаци

Реферат

Тема 3. Организация защиты автоматизированных систем и их компонентов от несанкционированного доступа.

1 Законодательство о персональных данных.

3.Защита авторских прав.

4.Назначение, функции и типы систем видеозащиты.

5.Как подписывать с помощью ЭЦП электронные документы различных форматов.

6.Обзор угроз и технологий защиты Wi-Fi-сетей.

7.Проблемы внедрения дискового шифрования.

8.Борьба со спамом: основные подходы, классификация, примеры, прогнозы на будущее.

9.Особенности процессов аутентификации в корпоративной среде.

10.Квантовая криптография.

11.Утечки информации: как избежать. Безопасность смартфонов.

12.Безопасность применения пластиковых карт - законодательство и практика.

13.Защита CD- и DVD-дисковот копирования.

14.Современные угрозы и защита электронной почты.

15.Программные средства анализа локальных сетей на предмет уязвимостей.

16.Безопасность применения платежных систем - законодательство и практика.

17.Аудит программного кода по требованиям безопасности.

18.Антишпионское ПО (antispyware).

19.Обеспечение безопасности Web-сервисов.

20.Защита от внутренних угроз.

21.Технологии RFID.

22.Уничтожение информации на магнитных носителях.

23.Ботнеты - плацдарм современных кибератак.

24.Цифровые водяные знаки в изображениях.

25.Электронный документооборот. Модели нарушителя.

26.Идентификация по голосу. Скрытые возможности.

27.Безопасность океанских портов.

28.Безопасность связи.

29.Безопасность розничной торговли.

30.Банковская безопасность.

31.Информатизация управления транспортной безопасностью.

32.Биопаспорт.

33.Обзор современных платформ архивации данных.

34.Что такое консалтинг в области ИБ.

35.Бухгалтерская отчетность как источник рассекречивания информации.

36.Управление рисками: обзор употребительных подходов.

37.Категорирование информации и информационных систем. Обеспечение базового уровня информационной безопасности.

38.Распределенные атаки на распределенные системы.

39.Оценка безопасности автоматизированных систем.

40.Windows и Linux: что безопаснее?

41.Функциональная безопасность программных средств.

42.Технологические процессы и стандарты обеспечения функциональной безопасности в жизненном цикле программных средств.

43.Информационная безопасность: экономические аспекты.

Собеседование

Тема 1. Введение.

1. Понятие аттестации ОИ. Объекты информатизации, аттестуемые по требованиям безопасности информации. ОИ, подлежащие аттестации.

2. Назначение проведения аттестации.

3. Перечень проводимых работ при проведении аттестации.

Тема 2. Основы Законодательства РФ, руководящие и нормативные документы ФСТЭК (Гостехкомиссии) России, регламентирующие вопросы защиты информации.

1. Федеральная служба по техническому и экспортному контролю (ФСТЭК России)

2. Приказ ФСТЭК России от «14» марта 2014 г. n 31 "об утверждении требований к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами

3. Приказ ФСТЭК России № 21 от 18 февраля 2013 г. Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных

Тема 3. Организация защиты автоматизированных систем и их компонентов от несанкционированного доступа.

1. Внедрение современных ИТ на базе компьютерной техники и телекоммуникационных средств

2. Задачи защиты информации от НСД в АСОД

3. Тракты доступа субъектов к информационным объектам

Тема 4. Порядок подготовки и проведения аттестации объектов информатизации по требованиям ФСТЭК России.

1. Документы, определяющие порядок проведения аттестации объектов информатизации по требованиям безопасности информации

2. Порядок проведения аттестации объектов информатизации по требованиям безопасности информации

3. Рассмотрение заявки на аттестацию, принятие решения на ее проведение, доведение решения до заявителя и органа по аттестации объектов информатизации.

Тема 5. Порядок проведения сертификационных испытаний средств защиты информации.

1. "Положение о сертификации средств защиты информации"

2. Понятие сертификации

3. Понятие сертификата соответствия
4. Технические, криптографические, программные и другие средства, предназначенные для защиты сведений, составляющих государственную тайну
5.Технические средства, подлежащие обязательной сертификации

Тема 6. Порядок лицензирования деятельности по защите информации ФСТЭК России.

1. Лицензирование деятельности по технической защите конфиденциальной информации
2. Контроль защищенности конфиденциальной информации от утечки по техническим каналам
3. Контроль защищенности конфиденциальной информации от несанкционированного доступа и ее модификации в средствах и системах информатизации
4. Сертификационные испытания на соответствие требованиям по безопасности информации продукции, используемой в целях защиты конфиденциальной информации
5. Установка, монтаж, испытания, ремонт средств защиты информации

Тестирование

Тема 2. Основы Законодательства РФ, руководящие и нормативные документы ФСТЭК (Гостехкомиссии) России, регламентирующие вопросы защиты информации.

1. Основной проблемой реализации систем защиты явля-ется:

a) исключение случай-ного и преднамеренного получения информации посто-ронними лицами;

b) разграничение доступа к устройствам и ресурсам системы всех пользователей, администрации и обслуживающего персонала;

c) системы защиты не должны со-здавать заметных неудобств пользователям в ходе их рабо-ты с ресурсами системы.

d) все вышеперечисленное.

2. Комплексный (системный) подход к построению любой системы включает в себя:

a) изучение объ-екта внедряемой системы; оценку угроз безопасности объ-екта; анализ средств, которыми будем оперировать при построении системы; оценку экономической целесооб-разности; изучение самой системы, ее свойств, принципов работы и возможность увеличения ее эффективности; со-отношение всех внутренних и внешних факторов; возмож-ность дополнительных изменений в процессе построения системы и полную организацию всего процесса от начала до конца; +

b) совокупности науч-ных, научно-технических и организационных мероприятий и применения специальных средств и методов, а создания целостной системы организационно-технологических ме-роприятий и применения комплекса специальных средств и методов;

c) разработку единой концепции как полной совокупности научно обос-нованных взглядов, положений и решений, необходимых и достаточных для оптимальной организации и обеспечения надежности защиты информации.

3. Какими бывают стратегии защиты информации?

a) оборонительная, наступательная, упреждающая;

b) наступательная, инженерная, сигнализационная, адаптивная;

c) инженерно-техническая, программно-аппаратная, программная, организационная.

1 **4. Что должна включать в себя система защиты от утечки?**

a) защита от наблюдения, прослушивания, перехвата, контроль вещественных носителей (комплексы мероприятий по контролю звукопроницаемости помещений, предотвращение утечки информации путем шифрования, контроль за уничтожением носителей и т.д.)

b) звукоизоляция, глушение, экранирование);

c) защита от перехвата (шифрование, экранирование, зашумление, фильтрация);+

комплекс защиты от перехвата (шифрование, экранирование, зашумление, фильтрация)

комплекс предотвр. утечки вещ.носителей (учет и скрытие отходов, уничтожение отходов)

d) определение полномочий пользователя (учет и анализ потока информации, распределение полномочий пользователей, ведения журнала учета);

e) установки пропускного режима (КПП на входе в здание, контроль доступа в помещения для совещаний и хранилищ конфиденциальных данных);

5. Какие элементы входят в состав информационных правоотношений ?

a) должностные инструкции, обращение, фиксирование, хранение;

b) права, ограничение прав, обязанности, ответственность;

c)права, обязанности, фиксирование, хранение

d) права, ограничение прав, должностные инструкции, ответственность

4.3 Промежуточная аттестация по дисциплине проводится в форме зачета, экзамена

Типовые вопросы зачета (ПК-5, ПК-8, ПК-10)

1. Понятие аттестации ОИ. Объекты информатизации, аттестуемые по требованиям безопасности информации. ОИ, подлежащие аттестации.
2. Назначение проведения аттестации.
3. Перечень проводимых работ при проведении аттестации.
4. Основные руководящие документы ФСТЭК России по аттестации объектовинформатизации
5. Организационная структура системы аттестации объектов информатизации потребованиям безопасности информации
6. Функции заявителя.
7. Перечень документов заявителя для аттестации защищаемого помещения.
8. Перечень документов заявителя для аттестации АС.
9. Порядок проведения аттестации объектов информатизации
10. Содержание заявки на проведения аттестации объектов информатизации
11. Исходные данные по аттестуемому ОИ
12. Перечень СЗИ, подлежащих сертификации по требованиям безопасности информации

Типовые задания для зачета (ПК-5, ПК-8, ПК-10)

Не предусмотрены

Типовые вопросы экзамена (ПК-5, ПК-8, ПК-10)

1. Содержание программы аттестационных испытаний
2. Цели и виды аттестационных испытаний
3. Условия и порядок проведения аттестационных испытаний
4. Этапы программы аттестационных испытаний
5. Методика аттестационных испытаний
6. Анализ процесса обработки информации

7. Испытание подсистемы управления доступом
8. Испытание подсистемы регистрации и учета
9. Испытание подсистемы обеспечения целостности
10. Состав аттестационной комиссии
11. Документы, оформляемые по результатам спецпроверки и аттестации.
12. Содержание заключения по результатам аттестации
13. Оформление, регистрация и выдача аттестатов соответствия
14. Содержание аттестата соответствия

Типовые задания для экзамена (ПК-5, ПК-8, ПК-10)

1. Основной проблемой реализации систем защиты явля-ется:

1. исключение случай-ного и преднамеренного получения информации посто-ронними лицами;
2. разграничение доступа к устройствам и ресурсам системы всех пользователей, администрации и обслуживающего персонала;
3. системы защиты не должны со-здавать заметных неудобств пользователям в ходе их рабо-ты с ресурсами системы.
4. все вышеперечисленное.(+)

5. Комплексный (системный) подход к построению любой системы включает в себя:

1. изучение объ-екта внедряемой системы; оценку угроз безопасности объ-екта; анализ средств, которыми будем оперировать при построении системы; оценку экономической целесооб-разности; изучение самой системы, ее свойств, принципов работы и возможность увеличения ее эффективности; со-отношение всех внутренних и внешних факторов; возмож-ность дополнительных изменений в процессе построения системы и полную организацию всего процесса от начала до конца; (+)
2. совокупности науч-ных, научно-технических и организационных мероприятий и применения специальных средств и методов, а создания целостной системы организационно-технологических ме-роприятий и применения комплекса специальных средств и методов;
3. разработку единой концепции как полной совокупности научно обос-нованных взглядов, положений и решений, необходимых и достаточных для оптимальной организации и обеспечения надежности защиты информации.

4. Какими бывают стратегии защиты информации?

1. оборонительная, наступательная, упреждающая; (+)
2. наступательная, инженерная, сигнализационная, адаптивная;
3. инженерно-техническая, программно-аппаратная, программная, организационная.

4. Что должна включать в себя система защиты от утечки?

1. защита от наблюдения, прослушивания, перехвата, контроль вещественных носителей (комплексы мероприятий по контролю звукопроницаемости помещений, предотвращение утечки информации путем шифрования, контроль за уничтожением носителей и т.д.)
2. звукоизоляция, глушение, экранирование);(+)
3. защита от перехвата (шифрование, экранирование, зашумление, фильтрация);(+)

комплекс защиты от перехвата (шифрование, экранирование, зашумление, фильтрация)

комплекс предотвр. утечки вещ.носителей (учет и скрытие отходов, уничтожение отходов)

4. определение полномочий пользователя (учет и анализ потока информации, распределение полномочий пользователей, ведения журнала учета);
5. установки пропускного режима (КПП на входе в здание, контроль доступа в помещения для совещаний и хранилищ конфиденциальных данных);

6. Какие элементы входят в состав информационных правоотношений ?

1. должностные инструкции, обращение, фиксирование, хранение;
2. права, ограничение прав, обязанности, ответственность;(+)
3. права, обязанности, фиксирование, хранение;

4. права, ограничение прав, должностные инструкции, ответственность.

4.4. Шкала оценивания промежуточной аттестации

Зачет

Оценка	Компете	Дескрипторы (уровни) – основные признак
«зачтено» (50 - 100 балл	ПК-5	Демонстрирует высокий уровень знаний теории Анализирует значимые проблемы, дает оценку основным тенденциям развития. Ответ построен логично, материал излагается четко, ясно, хорошим языком, аргументировано.
	ПК-8	Демонстрирует достаточный уровень знаний аудита и аттестации объектов информатизации. Эффективно использует нормативные правовые акты в профессиональной деятельности. Достаточно свободно ориентируется в необходимых нормативных правовых актах и информационно-правовых нормах в системе действующего законодательства. Демонстрирует достаточные навыки организации технологического процесса защиты информации в соответствии с правовыми нормативными актами и нормативными методическими документами.
	ПК-10	Свободно ориентируется в основных целях, задачах, методах контроля за обеспечением защиты информации, На вопросы отвечает кратко, аргументировано, уверенно, по существу
«не зачтено» (0 - 49 баллов	ПК-5	Демонстрирует слабый уровень знаний. Не может определить проблемы, дать оценку основным тенденциям развития. Неуверенно и логически непоследовательно излагает материал.
	ПК-8	Не демонстрирует знаниеаудита и аттестации объектов информатизации. Не анализирует существующие методики определений требования к защите информации. Демонстрирует не достаточное знание принципов обеспечения защиты информации и источников угроз ИБ. Не способен продемонстрировать современные подходы к технологиям и методам обеспечения ИБ.
	ПК-10	Не ориентируется в основных целях, задачах, методах контроля за обеспечением защиты информацииНе ориентируется в информационном и иллюстративном материале Неправильно отвечает на поставленные вопросы или затрудняется с ответом

Экзамен

Оценка	Компете	Дескрипторы (уровни) – основные признак
	ПК-5	Демонстрирует высокий уровень знаний теории Анализирует значимые проблемы, дает оценку основным тенденциям развития. Ответ построен логично, материал излагается четко, ясно, хорошим языком, аргументировано.

«отлично» (85 - 100 балл	ПК-8	Демонстрирует достаточный уровень знаний аудита и аттестации объектов информатизации. Эффективно использует нормативные правовые акты в профессиональной деятельности. Достаточно свободно ориентируется в необходимых нормативных правовых актах и информационно-правовых нормах в системе действующего законодательства. Демонстрирует достаточные навыки организации технологического процесса защиты информации в соответствии с правовыми нормативными актами и нормативными методическими документами.
	ПК-10	Свободно ориентируется в основных целях, задачах, методах контроля за обеспечением защиты информации, На вопросы отвечает кратко, аргументировано, уверенно, по существу
«хорошо» (70 - 84 балло	ПК-5	Демонстрирует достаточный уровень знаний теории. Неуверенно определяет проблемы, дает оценку основным тенденциям развития Ответ не всегда логично выстроен, материал излагается без применения научной терминологии.
	ПК-8	Демонстрирует достаточный уровень знаний аудита и аттестации объектов информатизации. Анализирует существующие методики определений требования к защите информации Демонстрирует достаточное знание принципов обеспечения защиты информации и источников угроз ИБ Способен продемонстрировать современные подходы к технологиям и методам обеспечения ИБ.
	ПК-10	Достаточно ориентируется в основных целях, задачах, методах контроля за обеспечением защиты информации, в том числе сведений, составляющих государственную тайну. Достаточно ориентируется в информационном и иллюстративном материале.Вопросы, задаваемые преподавателем, вызывают затруднения.
«удовлетворите (50 - 69 балло	ПК-5	Демонстрирует низкий уровень знаний теории Неуверенно определяет проблемы, дает оценку основным тенденциям развития Ответ не всегда логично выстроен, материал излагается без применения научной терминологии.
	ПК-8	Демонстрирует не достаточный уровень знаний аудита и аттестации объектов информатизации. Не анализирует существующие методики определений требования к защите информации. Демонстрирует недостаточное знание принципов обеспечения защиты информации и источников угроз ИБ Способен в некоторой степени продемонстрировать современные подходы к технологиям и методам обеспечения ИБ.
	ПК-10	Слабо ориентируется в основных целях, задачах, методах контроля за обеспечением защиты информации, Вопросы, задаваемые преподавателем, вызывают затруднения. Слабо ориентируется в информационном и иллюстративном материале (примеры из практики, таблицы, графики и т.д.).
	ПК-5	Демонстрирует слабый уровень знаний. Не может определить проблемы, дать оценку основным тенденциям развития. Неуверенно и логически непоследовательно излагает материал.

«неудовлетвори (менее 50 бал	ПК-8	Не демонстрирует знаниеаудита и аттестации объектов информатизации. Не анализирует существующие методики определений требования к защите информации. Демонстрирует не достаточное знание принципов обеспечения защиты информации и источников угроз ИБ. Не способен продемонстрировать современные подходы к технологиям и методам обеспечения ИБ.
	ПК-10	Не ориентируется в основных целях, задачах, методах контроля за обеспечением защиты информацииНе ориентируется в информационном и иллюстративном материале Неправильно отвечает на поставленные вопросы или затрудняется с ответом

5. Методические указания для обучающихся по освоению дисциплины (модуля)

5.1 Методические указания по организации самостоятельной работы обучающихся:

Приступая к изучению дисциплины, в первую очередь обучающимся необходимо ознакомиться содержанием рабочей программы дисциплины (РПД), которая определяет содержание, объем, а также порядок изучения и преподавания учебной дисциплины, ее раздела, части.

Для самостоятельной работы важное значение имеют разделы «Объем и содержание дисциплины», «Учебно-методическое и информационное обеспечение дисциплины» и «Материально-техническое обеспечение дисциплины, программное обеспечение, профессиональные базы данных и информационные справочные системы».

В разделе «Объем и содержание дисциплины» указываются все разделы и темы изучаемой дисциплины, а также виды занятий и планируемый объем в академических часах.

В разделе «Учебно-методическое и информационное обеспечение дисциплины» указана рекомендуемая основная и дополнительная литература.

В разделе «Материально-техническое обеспечение дисциплины, программное обеспечение, профессиональные базы данных и информационные справочные системы» содержится перечень профессиональных баз данных и информационных справочных систем, необходимых для освоения дисциплины.

5.2 Рекомендации обучающимся по работе с теоретическими материалами по дисциплине

При изучении и проработке теоретического материала необходимо:

- просмотреть еще раз презентацию лекции в системе MOODLe, повторить законспектированный на лекционном занятии материал и дополнить его с учетом рекомендованной дополнительной литературы;

- при самостоятельном изучении теоретической темы сделать конспект, используя рекомендованные в РПД источники, профессиональные базы данных и информационные справочные системы:

- ответить на вопросы для самостоятельной работы, по теме представленные в пункте 3.2 РПД.

- при подготовке к текущему контролю использовать материалы фонда оценочных средств (ФОС).

5.3 Рекомендации по работе с научной и учебной литературой

Работа с основной и дополнительной литературой является главной формой самостоятельной работы и необходима при подготовке к устному опросу на семинарских занятиях, к дебатам, тестированию, экзамену. Она включает проработку лекционного материала и рекомендованных источников и литературы по тематике лекций.

Конспект лекции должен содержать реферативную запись основных вопросов лекции, в том числе с опорой на размещенные в системе MOODLe презентаци, основных источников и литературы по темам, выводы по каждому вопросу. Конспект может быть выполнен в рамках распечатки выдачи презентаций лекций или в отдельной тетради по предмету. Он должен быть аккуратным, хорошо читаемым, не содержать не относящуюся к теме информацию или рисунки.

Конспекты научной литературы при самостоятельной подготовке к занятиям должны содержать ответы на каждый поставленный в теме вопрос, иметь ссылку на источник информации с обязательным указанием автора, названия и года издания используемой научной литературы. Конспект может быть опорным (содержать лишь основные ключевые позиции), но при этом позволяющим дать полный ответ по вопросу, может быть подробным. Объем конспекта определяется самим студентом.

В процессе работы с основной и дополнительной литературой студент может:

- делать записи по ходу чтения в виде простого или развернутого плана (создавать перечень основных вопросов, рассмотренных в источнике);
- составлять тезисы (цитирование наиболее важных мест статьи или монографии, короткое изложение основных мыслей автора);
- готовить аннотации (краткое обобщение основных вопросов работы);
- создавать конспекты (развернутые тезисы).

5.4. Рекомендации по подготовке к отдельным заданиям текущего контроля

Собеседование предполагает организацию беседы преподавателя со студентами по вопросам практического занятия с целью более обстоятельного выявления их знаний по определенному разделу, теме, проблеме и т.п. Все члены группы могут участвовать в обсуждении, добавлять информацию, дискутировать, задавать вопросы и т.д.

Устный опрос может применяться в различных формах: фронтальный, индивидуальный, комбинированный. Основные качества устного ответа подлежащего оценке:

- правильность ответа по содержанию;
- полнота и глубина ответа;
- сознательность ответа;
- логика изложения материала;
- рациональность использованных приемов и способов решения поставленной учебной задачи;
- своевременность и эффективность использования наглядных пособий и технических средств при ответе;
- использование дополнительного материала;
- рациональность использования времени, отведенного на задание.

Устный опрос может сопровождаться презентацией, которая подготавливается по одному из вопросов практического занятия. При выступлении с презентацией необходимо обращать внимание на такие моменты как:

- содержание презентации: актуальность темы, полнота ее раскрытия, смысловое содержание, соответствие заявленной темы содержанию, соответствие методическим требованиям (цели. ссылки на ресурсы. соответствие содержания и литературы), практическая направленность, соответствие содержания заявленной форме, адекватность использования технических средств учебным задачам, последовательность и логичность презентуемого материала;
- оформление презентации: объем (оптимальное количество), дизайн (читаемость, наличие и соответствие графики и анимации, звуковое оформление, структурирование информации, соответствие заявленным требованиям), оригинальность оформления, эстетика, использование возможности программной среды, соответствие стандартам оформления;
- личностные качества: ораторские способности. соблюдение регламента, эмоциональность, умение ответить на вопросы, систематизированные, глубокие и полные знания по всем разделам программы:
- содержание выступления: логичность изложения материала, раскрытие темы, доступность изложения, эффективность применения средств ИКТ, способы и условия достижения результативности и эффективности для выполнения задач своей профессиональной или учебной деятельности, доказательность принимаемых решений, умение аргументировать свои заключения, выводы.

6. Учебно-методическое и информационное обеспечение дисциплины

6.1 Основная литература:

1. Кияев В., Граничин О. Информатизация предприятия. - Москва: Национальный Открытый Университет «ИНТУИТ», 2016. - 235 с. - Текст : электронный // ЭБС «Университетская библиотека онлайн» [сайт]. - URL: http://biblioclub.ru/index.php?page=book&id=429037

2. Жихарев А. П. Автоматизированные информационные системы и ресурсы города Москвы : научное издание. - Москва: Юнити-Дана : Закон и право, 2014. - 255 с. - Текст : электронный // ЭБС «Университетская библиотека онлайн» [сайт]. - URL: http://biblioclub.ru/index.php?page=book&id=447946

6.2 Дополнительная литература:

1. Лопатин Д.В. Защита компьютерных систем от деструктивных программ : Учеб.-метод. пособие. - Тамбов: Изд-во ТГУ, 2005. - 158 с.

2. Лопатин Д.В., Калинина Ю.В. Безопасные информационные технологии : электрон. учеб. пособие. - Тамбов: [Б.и.], 2014. - 1 электрон. опт. диск (CD-ROM)

3. Программно-аппаратная защита информации : учеб.-метод. комплекс, Блок 1: Теоретические и практические аспекты защиты программного обеспечения на основе уникальных характеристик рабочей среды конечного пользователя. - [Тамбов]: Изд-во ТГУ, [200. - 1 электрон. опт. диск (CD-ROM).

6.3 Иные источники:

1. Федеральный портал «Российское образование» - http://www.edu.ru/

7. Материально-техническое обеспечение дисциплины, программное обеспечение, профессиональные базы данных и информационные справочные системы

Для проведения занятий по дисциплине необходимо следующее материально-техническое обеспечение: учебные аудитории для проведения занятий лекционного и семинарского типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации, помещения для самостоятельной работы.

Учебные аудитории и помещения для самостоятельной работы укомплектованы специализированной мебелью и техническими средствами обучения, служащими для представления учебной информации большой аудитории.

Помещения для самостоятельной работы укомплектованы компьютерной техникой с возможностью подключения к сети "Интернет" и обеспечением доступа в электронную информационно-образовательную среду Университета.

Для проведения занятий лекционного типа используются наборы демонстрационного оборудования, обеспечивающие тематические иллюстрации (проектор, ноутбук, экран/ интерактивная доска).

Лицензионное программное обеспечение:

LibreOffice

Microsoft Office Профессиональный плюс 2007

Microsoft Windows 10

Профессиональные базы данных и информационные справочные системы:

1. Научная электронная библиотека eLIBRARY.ru. – URL: https://elibrary.ru

2. Российская национальная библиотека. – URL: http://nlr.ru

3. Российская государственная библиотека. – URL: https://www.rsl.ru

4. Электронная библиотека РФФИ. – URL: https://www.rfbr.ru/rffi/ru/library

5. Университетская библиотека онлайн: электронно-библиотечная система. – URL: https://biblioclub.ru

6. Консультант студента. Гуманитарные науки: электронно-библиотечная система. – URL: https://www.studentlibrary.ru

7. Электронный каталог Фундаментальной библиотеки ТГУ. – URL: http://biblio.tsutmb.ru/elektronnyij-katalog

8. Научная электронная библиотека Российской академии естествознания. – URL: https://www.monographies.ru

9. Президентская библиотека имени Б.Н. Ельцина. – URL: https://www.prlib.ru

Электронная информационно-образовательная среда

https://auth.tsutmb.ru/authorize?response_type=code&client_id=moodle&state=xyz

Взаимодействие преподавателя и студента в процессе обучения осуществляется посредством мультимедийных, гипертекстовых, сетевых, телекоммуникационных технологий, используемых в электронной информационно-образовательной среде университета.