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.Б.21 Комплексная система защиты информации 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

1.1 Цель дисциплины – формирование компетенций:

ОК-2 Способность использовать основы экономических знаний при оценке эффективности результатов деятельности в различных сферах

ПК-4 Способность участвовать в работах по реализации политики информационной безопасности, применять комплексный подход к обеспечению информационной безопасности объекта защиты

ПК-7 Способность проводить анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности и участвовать и проведении технико-экономического обоснования соответствующих проектных решений

ПК-13 Способность принимать участие в формировании, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации

1.2 Виды и задачи профессиональной деятельности по дисциплине:

- организационно-управленческая
  - осуществление организационно-правового обеспечения информационной безопасности объекта защиты
  - организация работы малых коллективов исполнителей
  - участие в совершенствовании системы управления информационной безопасностью
  - изучение и обобщение опыта работы других учреждений, организаций и предприятий в области защиты информации, в том числе информации ограниченного доступа
  - контроль эффективности реализации политики информационной безопасности объекта защиты
- 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
	ОК-2 Способность использ	Знает и понимает: основ комплексной системы защиты информации
		Умеет (способен продемонстрировать): выносить аргументированные суждения по комплексно
		Владеет: Владеет навыками расчета экономической эффективно
	ПК-4 Способность участво	Знает и понимает: основных тенденций создания комплекса мер по обеспе
		Умеет (способен продемонстрировать): самостоятельно анализировать меры по обеспечению б
		Владеет: формальной постановки и решения задач защиты инфо
	ПК-7 Способность проводи обоснования соответствую	Знает и понимает: основных целей, задач, методов по контролю за обеспе
		Умеет (способен продемонстрировать): администрировать подсистемы ИБ определять рациона
		Владеет: эксплуатации подсистем ИБ, разработки практических

	ПК-13 Способность принимать участие в формировании, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации	Знает и понимает: каким образом можно построить исчерпывающую моде
		Умеет (способен продемонстрировать): составлять модель нарушителя; наладить систему упра
		Владеет: Владеет: навыками оценки рисков ИБ на предприятии;

1.4 Согласование междисциплинарных связей дисциплин, обеспечивающих освоение компетенций:

ОК-2 Способность использовать основы экономических знаний при оценке эффективности результатов деятельности в различных сферах

№ п/п	Наименование д	Форма		
		Очная (семест		
		1	2	6
1	Введение в проектную		+	
2	Инновационная эконо			+
3	Экономика	+		

ПК-4 Способность участвовать в работах по реализации политики информационной безопасности, применять комплексный подход к обеспечению информационной безопасности объекта защиты

№ п/п	Наименование д	Форм
		Очна (семе
		7
1	Эксплуатационная пр	+

ПК-7 Способность проводить анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности и участвовать и проведении технико-экономического обоснования соответствующих проектных решений

№ п/п	Наименование д	Форм
		Очна (семе
		8
1	Преддипломная практ	+

ПК-13 Способность принимать участие в формировании, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации

№ п/п	Наименование д	Форм	
		Очна (семе	
		7	8
1	Основы управления и	+	
2	Преддипломная практ		+

2. Место дисциплины в структуре ОП бакалавриата:

Дисциплина «Комплексная система защиты информации объектов информатизации» относится к базовой части учебного плана ОП по направлению подготовки 10.03.01 - Информационная безопасность.

Дисциплина «Комплексная система защиты информации объектов информатизации» изучается в 5 семестре.

3.Объем и содержание дисциплины

3.1.Объем дисциплины: 3 з.е.

Очная: 3 з.е.

Вид учебной работы	Очная (всего часов)
Общая трудоёмкость дисциплины	**108**
Контактная работа	52
Лекции (Лекции)	18
Лабораторные (Лаб. раб.)	34
Самостоятельная работа (СР)	56
Экзамен	-

3.2.Содержание курса:

№ темы	Название раздела/темы	Вид учебной работы, час.			Формы текущего контроля
		Лекции	Лаб. раб.	СР	
		О	О	О	
5 семестр					
1	Законодательно-правовые и организационные основы обеспечения информационной безопасности предприятия	2	4	8	Защита лабораторных работ ; Собеседование
2	Принципы организации и этапы разработки КСЗИ	2	4	8	Защита лабораторных работ
3	Моделирование КСЗИ	4	Пп 4	8	Защита лабораторных работ ; Тестирование; Практическое задание для практической подготовки

4	Функционирование КСЗИ	4	Пп 6	8	Защита лабораторных работ ; Реферат; Практическое задание для практической подготовки
5	Способы обеспечения информационной безопасности информационных систем	2	6	8	Защита лабораторных работ ; Собеседование
6	Обеспечение безопасности персональных данных, обрабатываемых в информационных системах	2	4	8	Защита лабораторных работ
7	Обеспечение безопасности информации в ключевых системах информационной инфраструктуры	2	6	8	Собеседование

Тема 1. Законодательно-правовые и организационные основы обеспечения информационной безопасности предприятия (ОК-2)

Лекция.

Законодательно-правовые и организационные основы обеспечения информационной безопасности предприятия. Сущность и задачи комплексной системы защиты информации (КСЗИ) на предприятии.

Лабораторные работы.

Оценка состояния защищенности предприятия

Оценка состояния защищенности по направлениям обеспечения безопасности:

- Состав и структура службы безопасности.
- Правовое обеспечение безопасности.
- Организационные меры защиты.
- Инженерно-техническое обеспечение безопасности.
- Управление безопасностью.

Задания для самостоятельной работы.

1. Проработка конспектов лекций и вопросов, вынесенных на самостоятельное изучение основной и дополнительной литературы.
2. Подготовка к тестированию.

Тема 2. Принципы организации и этапы разработки КСЗИ (ОК-2)

Лекция.

Факторы, влияющие на организацию КСЗИ. Определение и нормативное закрепление состава защищаемой информации, определение объектов защиты, анализ и оценка угроз безопасности информации.

Выявление и оценка источников, способов и результатов дестабилизирующего воздействия на информацию. Выбор методов и способов предотвращения угроз безопасности информации.

Этапы разработки КСЗИ.

Лабораторные работы.

Определение защищенности информации при несанкционированном доступе.

1. Подсчитать вероятности событий 1-8 при T=500 часов.
2. Найти вероятности сложных событий:

$$P\{Д(1) + E\}=P\{Д(1)\} + P\{E\} - P\{Д(1)\}\times P\{E\},$$

$$P\{Д(2) + E\}=P\{Д(2)\} + P\{E\} - P\{Д(2)\}\times P\{E\},$$

$$P\{СВ(1)\ А(1)\}=P\{C\}\times P\{B(1)\}\times P\{A(1)\},$$

$$P\{СВ(2)\ А(2)\}=P\{C\}\times P\{B(2)\}\times P\{A(2)\},$$

$$P\{СВ(1)\ А(1) + СВ(2)\ А(2)\}=1 - (1 - P\{СВ(1)\ А(1)\})(1 - P\{СВ(2)\ А(2)\}),$$

$$P\{E + СВ(1)\ А(1) + СВ(2)\ А(2)\}=1 - (1 - P\{E\})(1 - P\{СВ(1)\ А(1)\})(1 -$$

$$-P\{СВ(2)\ А(2)\}).$$

Задания для самостоятельной работы.

1. Проработка конспектов лекций и вопросов, вынесенных на самостоятельное изучение основной и дополнительной литературы.
2. Подготовка к тестированию.

Тема 3. Моделирование КСЗИ (ПК-4)

Лекция.

Определение условий функционирования КСЗИ. Разработка модели КСЗИ. Определение компонентов КСЗИ, технологическое и организационное построение КСЗИ.

Кадровое, материально-техническое и нормативно-методическое обеспечение функционирования КСЗИ.

Лабораторные работы.

Составить перечень персональных данных, обрабатываемых в выбранном объекте (организация, фирма, предприятие и т.д.).

Задания для самостоятельной работы.

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

Подготовка к тестированию.

Тема 4. Функционирование КСЗИ (ПК-4)

Лекция.

Назначение, структура и содержание управления КСЗИ, принципы и методы планирования функционирования КСЗИ.

Сущность и содержание контроля функционирования КСЗИ. Управление КСЗИ в условиях чрезвычайных ситуаций. Методы оценки эффективности КСЗИ.

Лабораторные работы.

Определение уровня исходной защищенности ИСДн.

Контрольные задания. Определить уровень исходной защищенности ИСПДн выбранного объекта (организация, фирма, предприятие и т.д.).

Задания для самостоятельной работы.

1. Проработка конспектов лекций и вопросов, вынесенных на самостоятельное изучение основной и дополнительной литературы.
2. Подготовка к тестированию.

Тема 5. Способы обеспечения информационной безопасности информационных систем (ПК-7)

Лекция.

Понятие и классификации информационных систем предприятия. Специфика построения корпоративных ИС. Угрозы информации в корпоративных ИС. Противодействия угрозам в корпоративных ИС.

Лабораторные работы.

Определение актуальности угроз безопасности персональных данных в ИСПДН. Контрольные задания.

Составить перечень возможныхУБПДн

Определить вероятности реализации угроз нарушителем в ИСПДн

Определение возможности реализации угрозы в ИСПДн АС

Составить перечень актуальных угроз безопасности ПДн в ИСПДн АС

Задания для самостоятельной работы.

1. Проработка конспектов лекций и вопросов, вынесенных на самостоятельное изучение основной и дополнительной литературы.
2. Подготовка к тестированию.

Тема 6. Обеспечение безопасности персональных данных, обрабатываемых в информационных системах (ПК-13)

Лекция.

Нормативно-правовое регулирование обеспечения безопасности персональных данных, обрабатываемых в информационных системах.

Лабораторные работы.

Расчет рисков информационной системы на основе модели угроз и уязвимостей. Расчет рисков по угрозе информационной безопасности

На первом этапе рассчитываем уровень угрозы по уязвимости Th на основе критичности и вероятности реализации угрозы через данную уязвимость. Уровень угрозы показывает, насколько критичным является воздействие данной угрозы на ресурс с учетом вероятности ее реализации.

Задания для самостоятельной работы.

1. Законодательно-правовые обеспечения информационной безопасности предприятия.
2. Организационные основы обеспечения информационной безопасности предприятия.
3. Задачи комплексной системы защиты информации (КСЗИ) на предприятии.
4. Определение объектов защиты, состава защищаемой информации предприятия.
5. Нормативное закрепление состава защищаемой информации предприятия.
6. Определение функций КСЗИ по защите информации предприятия.

Тема 7. Обеспечение безопасности информации в ключевых системах информационной инфраструктуры (ПК-13)

Лекция.

Информационная структура предприятия. Обеспечение безопасности информации в ключевых системах информационной инфраструктуры.

Лабораторные работы.

Технология оценки угроз и уязвимостей.

Для оценки угроз и уязвимостей применяются различные методы, в основе которых могут лежать:

- экспертные оценки;
- статистические данные;
- учет факторов, влияющих на уровни угроз и уязвимостей.

Задания для самостоятельной работы.

1 Современные технические средства несанкционированного доступа к информации.
2 Анализ и оценка угроз безопасности информации.
3 Выявление и оценка источников, способов и результатов дестабилизирующего воздействия на информацию.
4 Современные технические средства охраны и защиты информации.
5 Выбор методов и способов предотвращения угроз безопасности информации.
6 Определение условий функционирования КСЗИ.
7 Определение компонентов КСЗИ
8 Технологическое и организационное построение КСЗИ.
9 Кадровое, материально-техническое обеспечение функционирования КСЗИ.

4. Контроль знаний обучающихся и типовые оценочные средства

4.1. Распределение баллов:

5 семестр

- посещаемость – 10 баллов
- текущий контроль – 52 балла
- контрольные срезы – 2 среза: 6 баллов, 2 балла
- 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.	Законодательно	Защита	4	Лабораторные работы выполняются по тематике практических за 4 баллов – лабораторная работа выполнена в полном объёме, студе 2 балла – лабораторная работа выполнена, но имеет некоторые нет 1 балла - лабораторная работа в целом выполнена, однако в проце
		Собеседо вание(ко нтрольн ый срез)	6	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 6 баллов – студент умеет сопоставить полученную при подготовке 3 баллов - студент умеет применять полученную при подготовке к 2 балла – студент владеет теоретическим материалом по теме прак Если студент не владеет проблематикой практического занятия, не
2.	Принципы	Защита	6	Лабораторные работы выполняются по тематике практических за 6 баллов – лабораторная работа выполнена в полном объёме, студе 4 балла – лабораторная работа выполнена, но имеет некоторые нет 2 балла - лабораторная работа в целом выполнена, однако в проце

3.	Моделиро	Защита	4	Лабораторные работы выполняются по тематике практических за 4 балла – лабораторная работа выполнена, но имеет некоторые нет 2 балла - лабораторная работа в целом выполнена, однако в проце
		Тестирование(контрольный срез)	2	Тест состоит из 15 вопросов. 2 балла – студент правильно отвечает на 50-100% вопросов в тесте 1 балл - студент правильно отвечает на 25-50% вопросов в тесте. Менее 25% правильных ответов баллов не дает
		Практиче	2	Практические задания выполняются по тематике практических занятий. 2 баллов – практическое задание выполнено в полном объёме, студент свободно владеет материалом, демонстрирует глубокие, систематизированные знания, свободно отвечает на вопросы используя профессиональную терминологию 1 балла – практическое задание выполнено, но имеет некоторые неточности выполнения, студент владеет представленным материалом, отвечает на заданные вопросы
4.	Функцион	Защита	4	Лабораторные работы выполняются по тематике практических за 4 балла – лабораторная работа выполнена в полном объёме, студен 3 балла – лабораторная работа выполнена, но имеет некоторые нет 2 балла - лабораторная работа в целом выполнена, однако в проце
		Рефер	6	6 баллов – реферат выполнен обучающимся самостоятельно, в пол соответствии с правилами ГОСТа 5 баллов – во введение четко сформулированы основные позиции 3-4 балла – во введение основные позиции реферата сформулиров 1-2 балла – текст реферата представляет несамостоятельное (комп
		Практиче	2	Практические задания выполняются по тематике практических занятий. 2 баллов – практическое задание выполнено в полном объёме, студент свободно владеет материалом, демонстрирует глубокие, систематизированные знания, свободно отвечает на вопросы используя профессиональную терминологию 1 балла – практическое задание выполнено, но имеет некоторые неточности выполнения, студент владеет представленным материалом, отвечает на заданные вопросы
5.	Способы обес	Защита	6	Лабораторные работы выполняются по тематике практических за 6 баллов – лабораторная работа выполнена в полном объёме, студе 4 балла – лабораторная работа выполнена, но имеет некоторые нет 2 балла - лабораторная работа в целом выполнена, однако в проце

		Собесе	6	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 6 баллов – студент умеет сопоставить полученную при подготовке 3 баллов - студент умеет применять полученную при подготовке к 2 балла – студент владеет теоретическим материалом по теме прак Если студент не владеет проблематикой практического занятия, не
6.	Обеспечение б	Защита	6	Лабораторные работы выполняются по тематике практических за 6 баллов – лабораторная работа выполнена в полном объёме, студе 4 балла – лабораторная работа выполнена, но имеет некоторые нет 2 балла - лабораторная работа в целом выполнена, однако в проце
7.	Обеспечение б	Собесе	6	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 6 баллов – студент умеет сопоставить полученную при подготовке 3 баллов - студент умеет применять полученную при подготовке к 2 балла – студент владеет теоретическим материалом по теме прак Если студент не владеет проблематикой практического занятия, не
8.	Посещаемость		10	10 баллов – стопроцентное посещение занятий студентом 8-6 баллов – посещаемость студента составляет не менее 80 % зан 4-3 баллов – посещаемость студента составляет не менее 50 % зан 2-1 балла – посещаемость студента составляет не менее 25 % заня
9.	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
10.	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
11.	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

Защита лабораторных работ

Тема 1. Законодательно-правовые и организационные основы обеспечения информационной безопасности предприятия

1. Разработать частную модель угроз безопасности распределенной информационной системы персональных данных (ИС ПДн) с подключением к сети международного информационного обмена по следующим исходным данным:

- локальная ИС ПДн, развернута в пределах нескольких близко расположенных зданий;
- имеет многоточечный выход в сеть общего пользования;
- позволяет запись, удаление, сортировку ПДн;
- имеют доступ определенные перечнем сотрудники организации, являющейся владельцем ИСПДн;
- используется одна база ПДн, принадлежащая организации - владельцу данной ИСПДн;
- данные обезличиваются только при передаче в другие организации и не обезличены при предоставлении пользователю в организации;
- предоставляются сторонним пользователям ИС ПДн без предварительной обработки только часть ПДн.

2.Определить уровень базовый уровень защищенности ИС ПДн по следующим исходным данным:

- обработка ПДн сотрудников организации; - категории биометрических и иных персональных данных;
- объем обработки менее 100000 субъектов персональных данных;
- возможны угрозы 2 типа. 3.

3.Определить состав и содержание организационных и технических мер по защите ИС ПДн в соответствии с уровнем защищенности, руководствуясь последовательностью действий:

- определить базовый набор мер для третьего уровня защищенности ПДн;
- адаптировать базовый набор мер, с учетом характеристик распределенной информационной системы;
- подготовить предложения для уточнения адаптированного базового набора мер для различных вариантов ИС ПДн. Подобрать необходимый для заданного уровня защищенности ПДн состав средств защиты информации.

4. Разработать структуру технического задания на создание автоматизированной системы в защищенном исполнении. Составить технический паспорт на автоматизированную систему в защищенном исполнении, включающий:

- общие сведения об автоматизированной системе;
- состав оборудования автоматизированной системы (состав основных и вспомогательных средств и систем);
- состав средств защиты информации.

Тема 3. Моделирование КСЗИ

Лабораторная работа. Перечень персональных данных.

Тема 4. Функционирование КСЗИ

Лабораторная работа. Определение уровня исходной защищенности ИСДн.

Тема 5. Способы обеспечения информационной безопасности информационных систем

Лабораторная работа. Определение актуальности угроз безопасности персональных данных в ИСПДН.

Тема 6. Обеспечение безопасности персональных данных, обрабатываемых в информационных системах

Лабораторная работа. Расчет рисков информационной системы на основе модели угроз и уязвимостей. Расчет рисков по угрозе информационной безопасности.

Защита лабораторных работ

Тема 2. Принципы организации и этапы разработки КСЗИ

Лабораторная работа. Определение защищенности информации при несанкционированном доступе.

1. Подсчитать вероятности событий 1-8 при T=500 часов.

2. Найти вероятности сложных событий:

P{Д(1) + E}=P{Д(1)} + P{E} - P{Д(1)}□P{E},

P{Д(2) + E}=P{Д(2)} + P{E} - P{Д(2)}□P{E},

P{CB(1) A(1)}=P{C}□P{B(1)}□P{A(1)},

P{CB(2) A(2)}=P{C}□P{B(2)}□P{A(2)},

P{CB(1) A(1) + CB(2) A(2)}=1 - (1 - P{CB(1) A(1)})(1 - P{CB(2) A(2)}),

P{E + CB(1) A(1) + CB(2) A(2)}=1 - (1 - P{E})(1 - P{CB(1) A(1)})(1 -

-P{CB(2) A(2)}).

Практическое задание для практической подготовки

Тема 3. Моделирование КСЗИ

1. Основной проблемой реализации систем защиты явля-ется:

a) исключение случайного 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 создавать заметных неудобств пользователям в ходе их работы с ресурсами системы.

d) все вышеперечисленное.

Тема 4. Функционирование КСЗИ

Определить уровень исходной защищенности ИСПДн выбранного объекта (организация, фирма, предприятие и т.д.).

Реферат

Тема 4. Функционирование КСЗИ

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. Законодательно-правовые и организационные основы обеспечения информационной безопасности предприятия

1. Понятие распределенной информационной системы и её безопасности. Отличительные свойства распределенной информационной системы по отношению к нераспределенной. Классификация распределенных информационных систем.
2. Классификация угроз для распределенных информационных систем. Внутренние и внешние угрозы. Основные факторы, характерные для распределенных информационных систем, реализующие угрозы.

3. Методы сбора информации о распределенной информационной системе. Принципы работы приложений для сбора и информации об распределенной информационной системе. Анализ топологии системы, включенных в неё устройств, и внутренних сервисов и приложений.

4. Классификация уязвимостей в распределенных информационных системах по сетевой модели ISO/OSI (с физического по представительский уровни).

5. Классификация уязвимостей в распределенных информационных системах по сетевой модели ISO/OSI (прикладной уровень). Классификация уязвимостей по типам приложений (сетевой сервис, веб-приложение, СУБД и др).

6. Технические и программные методы и средства атак на типовые уязвимости распределенных информационных систем.

7. Технические и программные средства и методы противодействия анализу распределенной информационной системы.

8. Технические и программные средства для обнаружения вторжений в распределенную информационную систему.

9. Программные средства для мониторинга работоспособности и целостности распределенной информационной системы. Средства аудита безопасности распределенной информационной системы.

10. Программные средства для мониторинга целостности и неизменности распределенной информационной системы. Защитные системы контроля версий.

11. Внутренние способы защиты. Особенности проектирования и разработки защищаемых сервисов и приложений для распределенной информационной системы. Принципы защиты от реализации атак на сервис и приложение на уровне программного кода.

Тема 5. Способы обеспечения информационной безопасности информационных систем

1. Законодательно-правовые и организационные основы обеспечения информационной безопасности предприятия.

2. Задачи комплексной системы защиты информации (КСЗИ) на предприятии.

3. Определение объектов защиты и нормативное закрепление состава защищаемой информации предприятия.

4. Определение функций КСЗИ по защите информации предприятия.

Тема 7. Обеспечение безопасности информации в ключевых системах информационной инфраструктуры

1. Современные технические средства несанкционированного доступа к информации.

2. Анализ и оценка угроз безопасности информации.

3. Выявление и оценка источников, способов и результатов дестабилизирующего воздействия на информацию.

4. Современные технические средства охраны и защиты информации.

5. Выбор методов и способов предотвращения угроз безопасности информации.

6. Определение условий функционирования КСЗИ.

7. Определение компонентов КСЗИ

8. Технологическое и организационное построение КСЗИ.

9. Кадровое, материально-техническое обеспечение функционирования КСЗИ.

Тестирование

Тема 3. Моделирование КСЗИ

1. Из перечисленных разделов, криптография включает:

а) управление ключами

б) системы электронной подписи

в) асимметричные криптосистемы г) симметричные криптосистемы

д) стеганография

2. Из перечисленного для аутентификации по личной подписи терминальных пользователей используются методы:

а) исследование траектории движения руки

б) исследование динамических характеристик движения руки

в) визуальное сканирование

г) фрагментарное сканирование

3. Если средство защиты способно противостоять отдельным атакам, то согласно "Европейским критериям" безопасность считается:

а) стандартной

б) базовой

в) средней

г) низкой

4. Полномочия ядра безопасности ОС ассоциируются с:

а) приложениями

б) процессами

в) пользователями

г) периферийными устройствами

5. Согласно "Оранжевой книге" дискреционную защиту имеет группа критериев:

а) B

б) A

в) D

г) C

6. Два ключа используются в криптосистемах:

а) двойного шифрования

б) симметричных

в) с закрытым ключом

г) с открытым ключом

7. На многопользовательские системы с информацией одного уровня конфиденциальности согласно "Оранжевой книге" рассчитан класс:

а) C2

б) B2

в) C1

г) B1

8. Согласно "Оранжевой книге" с объектами должны быть ассоциированы:

а) уровни доступа

б) электронные подписи

в) метки безопасности

г) типы операций

9. Административные действия в СУБД позволяют выполнять привилегии:

а) безопасности

б) чтения

в) доступа

г) тиражирования

10. Как предотвращение неавторизованного использования ресурсов определена услуга защиты:

а) причастность

б) аутентификация

в) контроль доступа

г) целостность

4.3 Промежуточная аттестация по дисциплине проводится в форме экзамена

Типовые вопросы экзамена (ОК-2, ПК-4, ПК-7, ПК-13)

1. Законодательно-правовые и организационные основы обеспечения информационной безопасности предприятия.
2. Задачи комплексной системы защиты информации (КСЗИ) на предприятии.
3. Определение объектов защиты и нормативное закрепление состава защищаемой информации предприятия.
4. Определение функций КСЗИ по защите информации предприятия.
5. Современные технические средства несанкционированного доступа к информации.
6. Анализ и оценка угроз безопасности информации.
7. Выявление и оценка источников, способов и результатов дестабилизирующего воздействия на информацию.
8. Современные технические средства охраны и защиты информации.
9. Выбор методов и способов предотвращения угроз безопасности информации.
10. Определение условий функционирования КСЗИ.
11. Разработка модели КСЗИ.
12. Определение компонентов КСЗИ, технологическое и организационное построение КСЗИ.
13. Кадровое, материально-техническое и нормативно-методическое обеспечение функционирования КСЗИ.
14. Назначение, структура и содержание системы управления КСЗИ.
15. Принципы и методы планирования функционирования КСЗИ.
16. Сущность и содержание контроля функционирования КСЗИ.
17. Управление КСЗИ в условиях чрезвычайных ситуаций.
18. Методы оценки эффективности КСЗИ.

Типовые задания для экзамена (ОК-2, ПК-4, ПК-7, ПК-13)

1. Основной проблемой реализации систем защиты явля-ется:

a) исключение случайного 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 создавать заметных неудобств пользователям в ходе их работы 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 научных, 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.

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);

4.4. Шкала оценивания промежуточной аттестации

Оценка	Компете	Дескрипторы (уровни) – основные признак
«отлично» (85 - 100 балл	ОК-2	Студент показывает не только высокий уровень теоретических знаний по дисциплине, но и прослеживает междисциплинарные связи. Умеет увязывать знания, полученные при изучении различных дисциплин, анализировать практические ситуации, принимать соответствующие решения. Ответ, построен логично, материал излагается четко, ясно, хорошим языком, аргументировано, уместно используется информационный и иллюстративный материал (примеры из практики, таблицы, графики и т.д.). На вопросы отвечает кратко, аргументировано, уверенно, по существу. • безупречное владение инструментарием учебной дисциплины, умение его эффективно использовать в постановке научных и практических задач; • выраженная способность самостоятельно и творчески решать сложные проблемы и нестандартные ситуации; • полное и глубокое усвоение основной и дополнительной литературы, рекомендованной учебной программой по дисциплине; • умение ориентироваться в теориях, концепциях и направлениях дисциплины и давать им критическую оценку, используя научные достижения других дисциплин; • творческая самостоятельная работа на практических/семинарских/лабораторных занятиях, активное участие в групповых обсуждениях, высокий уровень культуры исполнения заданий; высокий уровень сформированностизаявленных в рабочей программе компетенций.
	ПК-4	Демонстрирует высокий уровень знаний теории Анализирует значимые проблемы, дает оценку основным тенденциям развития. Ответ построен логично, материал излагается четко, ясно, хорошим языком, аргументировано.
	ПК-7	Свободно ориентируется в основных целях, задачах, методах контроля за обеспечением защиты информации, в том числе сведений, составляющих государственную тайну, анализирует эффективность системы защиты информации. На вопросы отвечает кратко, аргументировано, уверенно, по существу.

	ПК-13	Демонстрирует высокий уровень знаний методологического базиса решения поставленных задач защиты информации. Анализирует существующие методики определений требования к защите информации. Свободно ориентируется в законодательстве РФ по защите информации. Ответ построен логично, материал излагается четко, ясно, хорошим языком, аргументировано. На вопросы отвечает кратко, аргументировано, уверенно, по существу.
«хорошо» (70 - 84 балло	ОК-2	Достаточно полные и систематизированные знания по дисциплине; • умение ориентироваться в основном теориях, концепциях и направлениях дисциплины и давать им критическую оценку; • использование научной терминологии, лингвистически и логически правильное изложение ответа на вопросы, умение делать обоснованные выводы; • владение инструментарием по дисциплине, умение его использовать в постановке и решении научных и профессиональных задач;¶• усвоение основной и дополнительной литературы, рекомендованной учебной программой по дисциплине; • самостоятельная работа на практических занятиях, участие в групповых обсуждениях, высокий уровень культуры исполнения заданий; средний уровень сформированности заявленных в рабочей программе компетенций.
	ПК-4	Демонстрирует достаточный уровень знаний теории. Достаточно ориентируется в проблемах, дает оценку основным тенденциям развития Ответ не всегда логично выстроен,
	ПК-7	Достаточно ориентируется в основных целях, задачах, методах контроля за обеспечением защиты информации, в том числе сведений, составляющих государственную тайну, анализирует эффективность системы защиты информации. Достаточно ориентируется в информационном и иллюстративном материале.Вопросы, задаваемые преподавателем, вызывают затруднения.
	ПК-13	Демонстрирует достаточный уровень знаний методологичес базиса решения задач защиты информации. Анализир существующие методики определений требования к зац информации. Достаточно свободно ориентируется в законодатели РФ по защите информации. Ответ построен логично, матер излагается хорошим языком. Вопросы, задаваемые преподавате не вызывают существенных затруднений.
	ОК-2	Достаточный минимальный объем знаний по дисциплине; • усвоение основной литературы, рекомендованной учебной программой; • умение ориентироваться в основных теориях, концепциях и направлениях по дисциплине и давать им оценку; • использование научной терминологии, стилистическое и логическое изложение ответа на вопросы, умение делать выводы без существенных ошибок; • владение инструментарием учебной дисциплины, умение его использовать в решении типовых задач; • умение под руководством преподавателя решать стандартные задачи; • работа под руководством преподавателя на практических занятиях, допустимый уровень культуры исполнения заданий; достаточный минимальный уровень сформированности заявленных в рабочей программе компетенций.

«удовлетворите (50 - 69 балло	ПК-4	Демонстрирует не достаточный уровень знаний теории Неуверенно определяет проблемы, дает оценку основным тенденциям развития Ответ не всегда логично выстроен, материал излагается без применения научной терминологии.
	ПК-7	Слабо ориентируется в основных целях, задачах, методах контроля за обеспечением защиты информации, в том числе сведений, составляющих государственную тайну, анализирует эффективность системы защиты информации. Вопросы, задаваемые преподавателем, вызывают затруднения. Слабо ориентируется в информационном и иллюстративном материале (примеры из практики, таблицы, графики и т.д.).
	ПК-13	Демонстрирует не достаточный уровень знаний методологического базиса решения задач защиты информации. Не анализирует существующие методики определений требования к защите информации. Слабо ориентируется в законодательстве РФ по защите информации. Практическое задание выполнено не полностью. Ответ не всегда логично выстроен, материал излагается без применения научной терминологии. Вопросы, задаваемые преподавателем, вызывают затруднения.
«неудовлетвори (менее 50 бал	ОК-2	фрагментарные знания по дисциплине;• отказ от ответа (выполнения письменной работы);• знание отдельных источников, рекомендованных учебной программой по дисциплине;• неумение использовать научную терминологию;• наличие грубых ошибок;• низкий уровень культуры исполнения заданий;низкий уровень сформированности заявленных в рабочей программе компетенций.
	ПК-4	Демонстрирует слабый уровень знаний. Не может определить проблемы, дать оценку основным тенденциям развития. Неуверенно и логически непоследовательно излагает материал.
	ПК-7	Не ориентируется в основных целях, задачах, методах контроля за обеспечением защиты информации, в том числе сведений, составляющих государственную тайну, анализа эффективность системы защиты информации. Не ориентируется в информационном и иллюстративном материале (примеры из практики, таблицы, графики и т.д.) Неправильно отвечает на поставленные вопросы или затрудняется с ответом
	ПК-13	Демонстрирует не достаточный уровень знаний методологического базиса решения задач защиты информации. Не анализирует существующие методики определений требования к защите информации. Не способен использовать программные средства. Не ориентируется в законодательстве РФ по защите информации. Неуверенно и логически непоследовательно излагает материал. 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. Шаньгин В.Ф. Комплексная защита информации в корпоративных системах : учеб. пособие. - М.: ИД "Форум", ИНФРА-М, 2013. - 591 с.

2. Соколов, В. П., Тарасова, Н. П. Кодирование в системах защиты информации : учебное пособие. - 2022-04-04; Кодирование в системах защиты информации. - Москва: Московский технический университет связи и информатики, 2016. - 94 c. - Текст : электронный // IPR BOOKS [сайт]. - URL: http://www.iprbookshop.ru/61485.html

6.2 Дополнительная литература:

1. Блок 1: История и современная система защиты информации в России, 2017. - 1 электрон. опт. диск (CD-ROM)

2. Тамб. гос. ун-т им. Г.Р. Державина Комплексная система защиты информации на предприятии : электрон. УМК. - [Тамбов]: Изд-во ТГУ, 2008. - 1 электрон. опт. диск (CD).

3. Аверченков В. И., Рытов М. Ю., Кондрашин Г. В., Рудановский М. В. Системы защиты информации в ведущих зарубежных странах : учебное пособие для вузов. - 4-е изд., стер.. - Москва: Флинта, 2016. - 224 с. - Текст : электронный // ЭБС «Университетская библиотека онлайн» [сайт]. - URL: http://biblioclub.ru/index.php?page=book&id=93351

6.3 Иные источники:

1. Федеральный портал «Российское образование» - http://www.edu.ru/
2. Федеральное хранилище «Единая коллекция цифровых образовательных ресурсов» - http://school-collection.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 Windows 10

Microsoft Office Профессиональный плюс 2007

Профессиональные базы данных и информационные справочные системы:

1. Электронный каталог Фундаментальной библиотеки ТГУ. – URL: http://biblio.tsutmb.ru/elektronnyij-katalog
2. Университетская библиотека онлайн: электронно-библиотечная система. – URL: https://biblioclub.ru
3. Консультант студента. Гуманитарные науки: электронно-библиотечная система. – URL: https://www.studentlibrary.ru
4. Научная электронная библиотека eLIBRARY.ru. – URL: https://elibrary.ru
5. Российская государственная библиотека. – URL: https://www.rsl.ru
6. Российская национальная библиотека. – URL: http://nlr.ru
7. Президентская библиотека имени Б.Н. Ельцина. – URL: https://www.prlib.ru
8. Научная электронная библиотека Российской академии естествознания. – URL: https://www.monographies.ru
9. Электронная библиотека РФФИ. – URL: https://www.rfbr.ru/rffi/ru/library

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.