

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.О.19 Информационная безопасность телекоммуникационных сетей

Направление подготовки/специальность: 11.03.02 - Инфокоммуникационные технологии и системы связи

Профиль/направленность/специализация: Системы и устройства подвижной радиосвязи

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 11.03.02 - Инфокоммуникационные технологии и системы связи (уровень бакалавриата) (приказ Министерства образования и науки РФ от «19» сентября 2017 г. № 930).

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.....	5
3. Объем и содержание дисциплины.....	5
4. Контроль знаний обучающихся и типовые оценочные средства.....	8
5. Методические указания для обучающихся по освоению дисциплины (модуля).....	14
6. Учебно-методическое и информационное обеспечение дисциплины.....	16
7. Материально-техническое обеспечение дисциплины, программное обеспечение, профессиональные базы данных и информационные справочные системы.....	16

## 1. Цели и задачи дисциплины

### 1.1 Цель дисциплины – формирование компетенций:

ОПК-3 Способен применять методы поиска, хранения, обработки, анализа и представления в требуемом формате информации из различных источников и баз данных, соблюдая при этом основные требования информационной безопасности

ПК-4 Способен составлять нормативную документацию (инструкции) по эксплуатационно-техническому обслуживанию сетей и оборудования связи

### 1.2 Типы задач профессиональной деятельности, к которым готовятся обучающиеся в рамках освоения дисциплины:

- научно-исследовательский
- технологический

1.3 Дисциплина ориентирована на подготовку обучающихся к профессиональной деятельности в сферах: 01 Образование и наука (в сфере общего, профессионального и дополнительного профессионального образования; в сфере научных исследований), 06 Связь, информационные и коммуникационные технологии (в сфере разработки, проектирования, исследования и эксплуатации радиоэлектронных средств и радиоэлектронных систем различного назначения; в сфере обороны и безопасности государства и правоохранительной деятельности)

### 1.4 В результате освоения дисциплины у обучающихся должны быть сформированы:

Обобщенные трудовые функции / трудовые функции / трудовые или профессиональные действия (при наличии профстандарта)	Код и наименование компетенции ФГОС ВО, необходимой для формирования трудового или профессионального действия	Индикаторы достижения компетенций
	ОПК-3 Способен применять методы поиска, хранения, обработки, анализа и представления в требуемом формате информации из различных источников и баз данных, соблюдая при этом основные требования информационной безопасности	Анализирует современные подходы к технологиям и методам обеспечения информационной безопасности, работает с программными средствами общего назначения; готов применить навыки работы в локальных и глобальных компьютерных сетях
- В/01.6 Проведение измерений параметров и проверки качества работы оборудования связи (телекоммуникаций)	ПК-4 Способен составлять нормативную документацию (инструкции) по эксплуатационно-техническому обслуживанию сетей и оборудования связи	Разрабатывает нормативы обеспечения информационной безопасности сетей и каналов связи

### 1.5 Согласование междисциплинарных связей дисциплин, обеспечивающих освоение компетенций:

ОПК-3 Способен применять методы поиска, хранения, обработки, анализа и представления в требуемом формате информации из различных источников и баз данных, соблюдая при этом основные требования информационной безопасности

№ п/п	Наименование дисциплин, определяющих междисциплинарные	Форма обучения	
		Очная (семестр)	Заочная (семестр)

	междисциплинарные связи	1	2	6	1	2	6
1	Вычислительная техника и информационные технологии			+			+
2	Информатика и информационные характеристики каналов систем связи	+	+		+	+	

ПК-4 Способен составлять нормативную документацию (инструкции) эксплуатационно-техническому обслуживанию сетей и оборудования связи

№ п/п	Наименование дисциплин, определяющих междисциплинарные связи	Форма обучения			
		Очная (семестр)		Заочная (семестр)	
		6	7	6	7
1	Основы построения инфокоммуникационных систем и сетей	+	+	+	+
2	Системы и сети связи с подвижными объектами		+		+
3	Технологическая (проектно-технологическая) практика	+		+	

## 2. Место дисциплины в структуре ОП бакалавриата:

Дисциплина «Информационная безопасность телекоммуникационных сетей» относится к обязательной части учебного плана ОП по направлению подготовки 11.03.02 - Инфокоммуникационные технологии и системы связи.

Дисциплина «Информационная безопасность телекоммуникационных сетей» изучается в 5 семестре.

## 3. Объем и содержание дисциплины

3.1. Объем дисциплины: 3 з.е.

Очная: 3 з.е.

Заочная: 3 з.е.

Вид учебной работы	Очная (всего часов)	Заочная (всего часов)
<b>Общая трудоёмкость дисциплины</b>	<b>108</b>	<b>108</b>
Контактная работа	52	14
Лекции (Лекции)	18	6
Лабораторные (Лаб. раб.)	34	8
Самостоятельная работа (СР)	56	90
Зачет	-	4

3.2. Содержание курса:

№ темы	Название раздела/темы	Вид учебной работы, час.			Формы текущего контроля
		Лекции	Лаб. раб.	СР	

		О	З	О	З	О	З	
5 семестр								
1	Введение в ИБ. Доктрина ИБ в РФ	3	1	-	-	12	18	Собеседование
2	Основные составляющие национальных интересов РФ в информационной среде	3	1	-	-	10	18	Собеседование
3	Информация. Основные свойства и характеристика безопасности ее применение	3	2	-	-	10	18	Собеседование
4	Угрозы ИБ	3	1	-	-	10	18	Собеседование
5	Системное обеспечение защиты информации	6	1	34	8	14	18	Защита лабораторных работ

### Тема 1. Введение в ИБ. Доктрина ИБ в РФ (ОПК-3)

#### Лекция.

1. Дайте определение понятию «информационная безопасность».
2. Перечислите основные составляющие информационной безопасности.
3. Каково значение составляющих для субъектов информационных отношений?
4. Каковы интересы РФ в информационной сфере?
5. Определите источники угроз информационной безопасности РФ и постройте их классификацию.
6. Перечислите основные методы обеспечения информационной безопасности РФ.
7. Каковы основные проблемы международного сотрудничества в настоящее время?
8. Каковы основные документы в области международной информационной безопасности.

#### Задания для самостоятельной работы.

Задания для самостоятельной работы

Проанализируйте Доктрину ИБ РФ и постройте схему органов государственной власти и местного самоуправления, отвечающих за информационную безопасность. Определите их функциональные обязанности.

Сформулируйте положения государственной политики в области обеспечения информационной безопасности, определите первоочередные мероприятия по обеспечению информационной безопасности, дайте им оценку.

### Тема 2. Основные составляющие национальных интересов РФ в информационной среде (ОПК-3)

#### Лекция.

1. Дайте определение понятию «защита информации».
2. Что понимается под термином «безопасность информации»?
3. Что включает в себя защита информации?
4. Каковы цели защиты информации?
5. Какое место занимает защита информации в информационной безопасности?
6. Каковы уровни обеспечения информационной безопасности?
7. Дайте определение понятию «политика информационной безопасности организации».
8. Что входит в анализ информационных рисков?

### **Задания для самостоятельной работы.**

Задания для самостоятельной работы

Проанализируйте структуру местного предприятия, схему информационных потоков, рассмотрите виды информации и ее носители, используемые в его подразделениях. Сформулируйте цели защиты информации на данном предприятии. Определите возможные угрозы безопасности для информационных процессов на данном предприятии.

## **Тема 3. Информация. Основные свойства и характеристика безопасности ее применение (ОПК-3)**

### **Лекция.**

1. Определите предмет защиты информации.
2. Каковы основные свойства информации, как предмета защиты.
3. Что относится к конфиденциальной информации?
4. Каковы основные уровни секретности государственной тайны?
5. В чем сущность основных подходов к измерению количества информации?
6. В чем сущность информации как объекта права собственности?

### **Задания для самостоятельной работы.**

Задания для самостоятельной работы

Используя данные предыдущей практической работы, проанализируйте особенности каждого из носителей информации. Сформулируйте достоинства и недостатки каждого из типов носителей, условия их хранения и обработки.

## **Тема 4. Угрозы ИБ (ОПК-3)**

### **Лекция.**

1. Составьте классификацию угроз информационной безопасности.
2. Охарактеризуйте группы преднамеренных угроз информационной безопасности.
3. Дайте определение понятию «несанкционированный доступ к информации».
4. Как строится модель нарушителя информационной безопасности?

### **Задания для самостоятельной работы.**

Задания для самостоятельной работы

На основе целей защиты информации и носителей информации, определите список угроз информационной безопасности, характерных для данного предприятия.

Проанализируйте риски, определите степень их допустимости.

Составьте модели нарушителей информационной безопасности, актуальных для данного предприятия.

## **Тема 5. Системное обеспечение защиты информации (ОПК-3)**

### **Лекция.**

1. Каковы основные принципы построения систем защиты информации?
2. Перечислите основные модели защиты информации и их особенности.
3. В чем заключается сущность методов защиты от случайных угроз?
4. Дайте определение понятиям «идентификация» и «аутентификация».
5. Перечислите основные виды аутентификации.
6. Как обеспечивается повышение надежности и отказоустойчивости информационных систем?
7. Какова роль подготовленности персонала в построении системы защиты информации?
8. Какие методы и средства используются для организации противодействия традиционным методам шпионажа и диверсий?
9. Каковы особенности построения защиты от несанкционированного доступа?
10. Какие методы защиты информации относятся к криптографическим?

### **Лабораторные работы.**

## Лабораторные занятия

Лабораторная работа №1. Резервное копирование и восстановление данных.

Ознакомление со способами резервного копирования информации

Лабораторная работа №2 . Подсистема безопасности WINDOWS.

Ознакомление с подсистемой безопасности Windows

Лабораторная работа №3 . Определение защищенности информации при несанкционированном доступе

Определить показатели защищенности (уязвимости) информации при несанкционированном доступе. Провести анализ зависимости показателя уязвимости информации от параметров системы ЗИ

Лабораторная работа №4 Стандарт управления информационной безопасностью ГОСТ Р ИСО/МЭК 27002-2012

Ознакомиться с требованиями стандарта ГОСТ Р ИСО/МЭК 27002-2012 для комплексного подхода к обеспечению ИБ

Лабораторная работа № 5.KasperskyKryptoStorage 1.0.

Дать практические навыки по работе с криптоконтейнером Kaspersky

Лабораторная работа № 6. Win Lock Professional v 4.53.

Дать практические навыки по работе с сервисной программой Win Lock.

## 4. Контроль знаний обучающихся и типовые оценочные средства

### 4.1. Распределение баллов:

#### 5 семестр

- посещаемость – 10 баллов
- текущий контроль – 30 баллов
- контрольные срезы – 1 срез по 60 баллов каждый
- премиальные баллы – 20 баллов

#### Распределение баллов по заданиям:

№ те мы	Название темы / вид учебной работы	Формы текущего контроля / срезы	Мах. кол-во баллов	Методика проведения занятия и оценки
1.	Введение в ИБ. Доктрина ИБ в РФ	Собеседование	5	<p>5 баллов – студент умеет сопоставить полученную при подготовке к практическому занятию информацию, сравнивать разные точки зрения на анализируемую проблему, уметь четко формулировать свои вопросы и отвечать на задаваемые ему вопросы, вести дискуссию с использованием терминологии современной физики и химии</p> <p>3 балла - студент умеет применять полученную при подготовке к практическому занятию информацию, отвечать на большинство вопросов, вести дискуссию с использованием терминологии современной физики и химии.</p> <p>1 балл – студент владеет теоретическим материалом по теме практического занятия, иногда затрудняется при ответе на вопросы, не умеет сформулировать свою точку зрения на обсуждаемую проблему</p> <p>Если студент не владеет проблематикой практического занятия, не может отвечать на вопросы – ответ баллами не оценивается.</p>

2.	Основные составляющие национальных интересов РФ в информационной среде	Собеседование	5	<p>5 баллов – студент умеет сопоставить полученную при подготовке к практическому занятию информацию, сравнивать разные точки зрения на анализируемую проблему, уметь четко формулировать свои вопросы и отвечать на задаваемые ему вопросы, вести дискуссию с использованием терминологии современной физики и химии</p> <p>3 балла - студент умеет применять полученную при подготовке к практическому занятию информацию, отвечать на большинство вопросов, вести дискуссию с использованием терминологии современной физики и химии.</p> <p>1 балл – студент владеет теоретическим материалом по теме практического занятия, иногда затрудняется при ответе на вопросы, не умеет сформулировать свою точку зрения на обсуждаемую проблему</p> <p>Если студент не владеет проблематикой практического занятия, не может отвечать на вопросы – ответ баллами не оценивается.</p>
3.	Информация. Основные свойства и характеристика безопасности ее применение	Собеседование	10	<p>10 баллов – студент умеет сопоставить полученную при подготовке к практическому занятию информацию, сравнивать разные точки зрения на анализируемую проблему, уметь четко формулировать свои вопросы и отвечать на задаваемые ему вопросы, вести дискуссию с использованием терминологии современной физики и химии</p> <p>8 баллов - студент умеет применять полученную при подготовке к практическому занятию информацию, отвечать на большинство вопросов, вести дискуссию с использованием терминологии современной физики и химии.</p> <p>3 балла – студент владеет теоретическим материалом по теме практического занятия, иногда затрудняется при ответе на вопросы, не умеет сформулировать свою точку зрения на обсуждаемую проблему</p> <p>Если студент не владеет проблематикой практического занятия, не может отвечать на вопросы – ответ баллами не оценивается.</p>
4.	Угрозы ИБ	Собеседование	10	<p>10 баллов – студент умеет сопоставить полученную при подготовке к практическому занятию информацию, сравнивать разные точки зрения на анализируемую проблему, уметь четко формулировать свои вопросы и отвечать на задаваемые ему вопросы, вести дискуссию с использованием терминологии современной физики и химии</p> <p>8 баллов - студент умеет применять полученную при подготовке к практическому занятию информацию, отвечать на большинство вопросов, вести дискуссию с использованием терминологии современной физики и химии.</p> <p>3 балла – студент владеет теоретическим материалом по теме практического занятия, иногда затрудняется при ответе на вопросы, не умеет сформулировать свою точку зрения на обсуждаемую проблему</p> <p>Если студент не владеет проблематикой практического занятия, не может отвечать на вопросы – ответ баллами не оценивается.</p>
5.	Системное обеспечение защиты информации	<b>Защита лабораторных работ(контрольный срез)</b>	60	<p>10 баллов – студент выполнил лабораторную работу правильно, расчеты по работе произведены верно, ответил на контрольные вопросы преподавателя после выполнения лабораторной работы.</p> <p>6 баллов – студент выполнил лабораторную работу с ошибками, расчеты по работе содержат неточности, ответил на контрольные вопросы преподавателя после выполнения лабораторной работы.</p> <p>3 балла – студент выполнил лабораторную работу с грубыми ошибками, не смог правильно провести расчеты и ответить на контрольные вопросы.</p> <p>0 баллов – студент не выполнил лабораторную работу.</p>

6.	Посещаемость	10	10 баллов – студент посетил все 100% занятий 7-9 баллов – студент посетил не менее 80% занятий 4-6 баллов – студент посетил не менее 50% занятий 1-3 балла – студент посетил не менее 25% занятий Если студент посетил менее 25% занятий, баллы не начисляются
7.	Премияльные баллы	20	Дополнительные премиальные баллы могут быть начислены: - за проект, выполненный по заказу работодателя и реализованный на практике – 10 баллов; - постоянная активность во время практических занятий – 10 баллов; - полностью подготовленная к публикации статья по тематике в рамках дисциплины – 10 баллов; - победа в межрегиональной олимпиаде по социологии образования – 10 баллов; - участие с докладом во всероссийской олимпиаде по тематике изучаемой дисциплины – 10 баллов; - участие в выставке по тематике изучаемой дисциплины – 10 баллов; - публикация статьи по тематике изучаемой дисциплины в сборнике студенческих работ / материалах всероссийской конференции / журнале из перечня ВАК – 10
8.	Индивидуальные задания, с помощью которых можно набрать дополнительные баллы на экзамене	20	Добор: студент может предоставить все задания текущего контроля и контрольные срезы
9.	Итого за семестр	100	

Итоговая оценка по зачету 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
50 - 100 баллов	Зачтено
0 - 49 баллов	Не зачтено

#### 4.2 Типовые оценочные средства текущего контроля

### Защита лабораторных работ

#### Тема 5. Системное обеспечение защиты информации

##### Лабораторная работа №1. Резервное копирование и восстановление данных.

Ознакомление со способами резервного копирования информации

##### Лабораторная работа №2 . Подсистема безопасности WINDOWS.

Ознакомление с подсистемой безопасности Windows

##### Лабораторная работа №3 . Определение защищенности информации при несанкционированном доступе

Определить показатели защищенности (уязвимости) информации при несанкционированном доступе. Провести анализ зависимости показателя уязвимости информации от параметров системы ЗИ

##### Лабораторная работа №4 Стандарт управления информационной безопасностью ГОСТ Р ИСО/МЭК 27002-2012

Ознакомиться с требованиями стандарта ГОСТ Р ИСО/МЭК 27002-2012 для комплексного подхода к обеспечению ИБ

### Лабораторная работа № 5. Kaspersky KryptoStorage 1.0.

Дать практические навыки по работе с криптоконтейнером Kaspersky

### Лабораторная работа № 6. Win Lock Professional v 4.53.

Дать практические навыки по работе с сервисной программой Win Lock.

Примерные вопросы тестирования

1. К техническим средствам приема, обработки, хранения и передачи информации (ТСПИ) относятся:
  - а) (!) средства и системы информатизации;
  - б) средства открытой телефонной связи;
  - в) системы пожарной и охранной сигнализации;
2. К вспомогательным техническим средствам и системам (ВТСС) относятся:
  - а) средства и системы информатизации;
  - б) (!) средства открытой телефонной связи;
  - в) программные средства (операционные системы, системы управления базами данных, другое общесистемное и прикладное программное обеспечение).
3. Опасной зоной 2 называется:
  - а) (!) зона, в пределах которой отношение “информационный сигнал/помеха” превышает допустимое нормированное значение
  - б) пространство вокруг ТСПИ, в пределах которого на случайных антеннах наводится информационный сигнал выше допустимого (нормированного) уровня
4. Опасной зоной 2 называется:
  - а) зона, в пределах которой отношение “информационный сигнал/помеха” превышает допустимое нормированное значение;
  - б) (!) пространство вокруг ТСПИ, в пределах которого на случайных антеннах наводится информационный сигнал выше допустимого (нормированного) уровня.
5. Сосредоточенная случайная антенна это:
  - а) (!) компактное техническое средство;
  - б) кабели, провода, металлические трубы.

## Собеседование

### Тема 1. Введение в ИБ. Доктрина ИБ в РФ

Типовые задания собеседования

Проанализируйте Доктрину ИБ РФ и постройте схему органов государственной власти и местного самоуправления, отвечающих за информационную безопасность. Определите их функциональные обязанности.

Сформулируйте положения государственной политики в области обеспечения информационной безопасности, определите первоочередные мероприятия по обеспечению информационной безопасности, дайте им оценку.

Проанализируйте структуру местного предприятия, схему информационных потоков, рассмотрите виды информации и ее носители, используемые в его подразделениях. Сформулируйте цели защиты информации на данном предприятии. Определите возможные угрозы безопасности для информационных процессов на данном предприятии

Используя данные предыдущей практической работы, проанализируйте особенности каждого из носителей информации. Сформулируйте достоинства и недостатки каждого из типов носителей, условия их хранения и обработки

### Тема 2. Основные составляющие национальных интересов РФ в информационной среде

Типовые задания собеседования

Проанализируйте Доктрину ИБ РФ и постройте схему органов государственной власти и местного самоуправления, отвечающих за информационную безопасность. Определите их функциональные обязанности.

Сформулируйте положения государственной политики в области обеспечения информационной безопасности, определите первоочередные мероприятия по обеспечению информационной безопасности, дайте им оценку.

Проанализируйте структуру местного предприятия, схему информационных потоков, рассмотрите виды информации и ее носители, используемые в его подразделениях. Сформулируйте цели защиты информации на данном предприятии. Определите возможные угрозы безопасности для информационных процессов на данном предприятии

Используя данные предыдущей практической работы, проанализируйте особенности каждого из носителей информации. Сформулируйте достоинства и недостатки каждого из типов носителей, условия их хранения и обработки

### Тема 3. Информация. Основные свойства и характеристика безопасности ее применение

Типовые задания собеседования

Проанализируйте Доктрину ИБ РФ и постройте схему органов государственной власти и местного самоуправления, отвечающих за информационную безопасность. Определите их функциональные обязанности.

Сформулируйте положения государственной политики в области обеспечения информационной безопасности, определите первоочередные мероприятия по обеспечению информационной безопасности, дайте им оценку.

Проанализируйте структуру местного предприятия, схему информационных потоков, рассмотрите виды информации и ее носители, используемые в его подразделениях. Сформулируйте цели защиты информации на данном предприятии. Определите возможные угрозы безопасности для информационных процессов на данном предприятии

Используя данные предыдущей практической работы, проанализируйте особенности каждого из носителей информации. Сформулируйте достоинства и недостатки каждого из типов носителей, условия их хранения и обработки

### Тема 4. Угрозы ИБ

Типовые задания собеседования

Проанализируйте Доктрину ИБ РФ и постройте схему органов государственной власти и местного самоуправления, отвечающих за информационную безопасность. Определите их функциональные обязанности.

Сформулируйте положения государственной политики в области обеспечения информационной безопасности, определите первоочередные мероприятия по обеспечению информационной безопасности, дайте им оценку.

Проанализируйте структуру местного предприятия, схему информационных потоков, рассмотрите виды информации и ее носители, используемые в его подразделениях. Сформулируйте цели защиты информации на данном предприятии. Определите возможные угрозы безопасности для информационных процессов на данном предприятии

Используя данные предыдущей практической работы, проанализируйте особенности каждого из носителей информации. Сформулируйте достоинства и недостатки каждого из типов носителей, условия их хранения и обработки

### 4.3 Промежуточная аттестация по дисциплине проводится в форме зачета

#### Типовые вопросы зачета (ОПК-3, ПК-4)

Типовые вопросы зачета

1. Понятие информационной безопасности
2. Основные составляющие информационной безопасности.

3. Значение информационной безопасности для субъектов информационных отношений
4. Информационная безопасность в системе национальной безопасности РФ
5. Общее содержание защиты информации
6. Понятие и сущность защиты информации.
7. Цели защиты информации
8. Место защиты информации в информационной безопасности
9. Модели защиты информации
10. Современная концепция обеспечения информационной безопасности
11. Предмет и объект защиты информации
12. Предмет защиты информации
13. Информация как объект права собственности
14. Объект защиты информации
15. Угрозы информационной безопасности
16. Случайные угрозы
17. Преднамеренные угрозы
18. Модель нарушителя информационной безопасности
19. Системное обеспечение защиты информации
20. Основные принципы построения системы защиты
21. Методы защиты информации
22. Минимизация ущерба от аварий и стихийных бедствий
23. Дублирование информации
24. Повышение надежности информационной системы
25. Создание отказоустойчивых информационных систем
26. Оптимизация взаимодействия пользователей и обслуживающего персонала
27. Методы и средства защиты информации от традиционного шпионажа и диверсий
28. Методы и средства защиты от электромагнитных излучений и наводок
29. Защита информации от несанкционированного доступа
30. Криптографические методы защиты информации

#### **Типовые задания для зачета (ОПК-3, ПК-4)**

Проанализируйте Доктрину ИБ РФ и постройте схему органов государственной власти и местного самоуправления, отвечающих за информационную безопасность. Определите их функциональные обязанности.

Сформулируйте положения государственной политики в области обеспечения информационной безопасности, определите первоочередные мероприятия по обеспечению информационной безопасности, дайте им оценку.

Проанализируйте структуру местного предприятия, схему информационных потоков, рассмотрите виды информации и ее носители, используемые в его подразделениях. Сформулируйте цели защиты информации на данном предприятии. Определите возможные угрозы безопасности для информационных процессов на данном предприятии.

Используя данные предыдущей практической работы, проанализируйте особенности каждого из носителей информации. Сформулируйте достоинства и недостатки каждого из типов носителей, условия их хранения и обработки.

#### **4.4. Шкала оценивания промежуточной аттестации**

Оценка	Компетенции	Дескрипторы (уровни) – основные признаки освоения (показатели достижения результата)
--------	-------------	--

«зачтено» (50 - 100 баллов)	ОПК-3	Свободно ориентируется в направлениях исследований в области информационной безопасности. В полном объеме владеет практическими навыками современных исследовательских методов Демонстрирует знание и понимание современного отечественного и зарубежного опыта в области ИБ Определяет основные цели, задачи, методы научных исследований
	ПК-4	
«не зачтено» (0 - 49 баллов)	ОПК-3	Не ориентируется в направлениях исследований ИБ Не ориентируется в информационном и иллюстративном материале (примеры из практики, таблицы, графики и т.д.), не может анализировать и обобщать результаты научных исследований в области ИБ Неправильно отвечает на поставленные вопросы или затрудняется с ответом
	ПК-4	

## 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 презентации, 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. Передков В.М., Митрошкин А.Г. Информационная безопасность и защита информации. - Тамбов: [Б.и.], 2014. - 1 электрон. опт. диск (CD-ROM)
2. Лопатин Д.В., Калинина Ю.В. Безопасные информационные технологии : электрон. учеб. пособие. - Тамбов: [Б.и.], 2014. - 1 электрон. опт. диск (CD-ROM)
3. Аверченков, В. И. Аудит информационной безопасности : учебное пособие для вузов. - Весь срок охраны авторского права; Аудит информационной безопасности. - Брянск: Брянский государственный технический университет, 2012. - 268 с. - Текст : электронный // IPR BOOKS [сайт]. - URL: <http://www.iprbookshop.ru/6991.html>

### **6.2 Иные источники:**

1. Университетская библиотека онлайн: электронно-библиотечная система - <http://www.biblioclub.ru>
2. Консультант студента. Гуманитарные науки: электронно-библиотечная система - <http://www.studentlibrary.ru>
3. Российская национальная библиотека - [www.nlr.ru](http://www.nlr.ru)
4. Научная электронная библиотека Российской академии естествознания - [www.monographies.ru](http://www.monographies.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 и свободно распространяемое программное обеспечение:

Kaspersky Endpoint Security для бизнеса - Стандартный Russian Edition. 1500-2499 Node 1 year Educational Renewal Licence

Microsoft Office Профессиональный плюс 2007

7-Zip 9.20

Операционная система Microsoft Windows 10

Adobe Reader XI - Russian

Профессиональные базы данных и информационные справочные системы:

1. Электронная библиотека ТГУ. – URL: <https://elibrary.tsutmb.ru/>

2. Электронный каталог Фундаментальной библиотеки ТГУ. – URL: <http://biblio.tsutmb.ru/elektronnyij-katalog>
3. Научная электронная библиотека eLIBRARY.ru. – URL: <https://elibrary.ru>
4. Российская государственная библиотека. – URL: <https://www.rsl.ru>
5. Российская национальная библиотека. – URL: <http://nlr.ru>
6. Президентская библиотека имени Б.Н. Ельцина. – URL: <https://www.prlib.ru>
7. 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](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.