

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



Н. Л. Королева  
«04» июля 2022 г.

## **РАБОЧАЯ ПРОГРАММА**

по дисциплине Б1.О.10 Основы информационной безопасности

Направление подготовки/специальность: 10.03.01 - Информационная безопасность

Профиль/направленность/специализация: Безопасность компьютерных систем

Уровень высшего образования: бакалавриат

Квалификация: Бакалавр

год набора: 2022

Тамбов, 2022

**Автор программы:**

Анурьева Мария Сергеевна

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 «17» ноября 2020 г. № 1427).

Рабочая программа принята на заседании Кафедры математического моделирования и информационных технологий «29» июня 2022 г. Протокол № 12

Рассмотрена и одобрена на заседании Ученого совета Института математики, физики и информационных технологий, Протокол от «04» июля 2022 г. № 6.

## СОДЕРЖАНИЕ

1. Цели и задачи дисциплины.....	4
2. Место дисциплины в структуре ОП бакалавра.....	4
3. Объем и содержание дисциплины.....	4
4. Контроль знаний обучающихся и типовые оценочные средства.....	10
5. Методические указания для обучающихся по освоению дисциплины (модуля).....	36
6. Учебно-методическое и информационное обеспечение дисциплины.....	38
7. Материально-техническое обеспечение дисциплины, программное обеспечение, профессиональные базы данных и информационные справочные системы.....	39

## 1. Цели и задачи дисциплины

1.1 Цель дисциплины – формирование компетенций:

ОПК-8 Способен осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических документов в целях решения задач профессиональной деятельности

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

- организационно-управленческий

1.3 Дисциплина ориентирована на подготовку обучающихся к профессиональной деятельности в сфере: 06 Связь, информационные и коммуникационные технологии (в сфере техники и технологии, охватывающей совокупность проблем, связанных с обеспечением защищенности объектов информатизации в условиях существования угроз в информационной сфере)

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-8 Способен осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических документов в целях решения задач профессиональной деятельности	Осуществляет подбор, изучение и обобщение научно-технической литературы, нормативных и методических документов в целях решения задач профессиональной деятельности в области информационной безопасности

1.5 Согласование междисциплинарных связей дисциплин, обеспечивающих освоение компетенций:

## 2. Место дисциплины в структуре ОП бакалавриата:

Дисциплина «Основы информационной безопасности» относится к обязательной части учебного плана ОП по направлению подготовки 10.03.01 - Информационная безопасность.

Дисциплина «Основы информационной безопасности» изучается в 2 семестре.

## 3. Объем и содержание дисциплины

3.1. Объем дисциплины: 5 з.е.

Очная: 5 з.е.

Вид учебной работы	Очная (всего часов)
<b>Общая трудоёмкость дисциплины</b>	<b>180</b>
Контактная работа	96
Лекции (Лекции)	64
Лабораторные (Лаб. раб.)	32
Самостоятельная работа (СР)	48
Экзамен	36

## 3.2.Содержание курса:

№ темы	Название раздела/темы	Вид учебной работы, час.			Формы текущего контроля
		Лек ции	Лаб · раб.	СР	
		О	О	О	
2 семестр					
1	Введение. Стратегия национальной безопасности РФ. Доктрина информационной безопасности РФ.	4	2	2	Защита лаболаторных работ; Собеседование; Тестирование
2	Понятие национальной безопасности, виды безопасности. Информационная безопасность РФ.	6	2	3	Защита лаболаторных работ; Собеседование; Тестирование
3	Терминологически е основы информационной безопасности. Основные понятия и определения.	6	2	4	Защита лаболаторных работ; Собеседование; Тестирование
4	Проблемы обеспечения информационной безопасности	6	2	4	Защита лаболаторных работ; Собеседование
5	Основы теории защиты информации	6	4	6	Защита лаболаторных работ; Собеседование; Реферат
6	Общеметодологиче ские принципы теории информационной безопасности. Комплексность.	6	4	6	Защита лаболаторных работ; Собеседование; Тестирование
7	Угрозы. Классификация и анализ угроз информационной безопасности.	6	4	6	Защита лаболаторных работ; Собеседование; Тестирование

8	Методы нарушения конфиденциальности, целостности и доступности информации.	8	4	6	Защита лабораторных работ; Собеседование; Тестирование
9	Причины, виды, каналы утечки и искажения информации.	8	2	4	Собеседование; Тестирование
10	Функции и задачи защиты информации. Проблемы региональной информационной безопасности.	4	2	3	Собеседование; Тестирование
11	Развитие теории и практики защиты информации	4	4	4	Защита лабораторных работ; Собеседование; Тестирование

## **Тема 1. Введение. Стратегия национальной безопасности РФ. Доктрина информационной безопасности РФ. (ОПК-8)**

### **Лекция.**

Россия в современном мире. Национальные интересы и стратегические национальные приоритеты. Национальные интересы РФ в информационной сфере и их обеспечение. Виды угроз информационной безопасности РФ. Источники угроз информационной безопасности РФ. Состояние информационной безопасности РФ и основные задачи по ее обеспечению. Методы обеспечения информационной безопасности РФ. Особенности обеспечения информационной безопасности РФ в различных сферах общественной жизни. Международное сотрудничество РФ в области обеспечения информационной безопасности. Основные положения государственной политики обеспечения информационной безопасности РФ и первоочередные мероприятия по ее реализации. Организационная основа системы обеспечения информационной безопасности РФ.

### **Лабораторные работы.**

Анализ Доктрины информационной безопасности Российской Федерации.

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

- 1 Изучить Стратегию национальной безопасности РФ (2015 года).
- 2 Изучить Доктрину информационной безопасности РФ (2016 года). Провести сравнительный анализ Доктрин ИБ 2016 г. и 2000 г.

## **Тема 2. Понятие национальной безопасности, виды безопасности. Информационная безопасность РФ. (ОПК-8)**

### **Лекция.**

Органы, обеспечивающие национальную безопасность РФ, цели, задачи. Национальные интересы РФ в информационной сфере. Приоритетные направления в области защиты информации в РФ. Тенденции развития информационной политики государств и ведомств. Государственная тайна. Правовое обеспечение защиты информации.

### **Лабораторные работы.**

Лабораторная работа по программно-аппаратным методам защиты информации.

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

- 1 Подготовка к практическим занятиям, повторение изучения лекционного материала;
- 2 Подготовка к лекциям, повторение учебного материала предыдущих лекций;
- 3 Изучение материалов лекционного курса по заданиям на самостоятельную проработку, выдаваемых преподавателем на занятиях;
- 4 Составление отчета по лабораторной работе.

## **Тема 3. Терминологические основы информационной безопасности. Основные понятия и определения. (ОПК-8)**

### **Лекция.**

Понятие информации, информатизации, информационных систем и смежных с ними: информационная безопасность, информационная война, информационная агрессия, информационное оружие, информационные процессы, информационная система, информационная сфера. Понятия автора и собственника информации, взаимодействие субъектов в информационном обмене. Защита информации, тайна, средства защиты информации, угрозы - определения, сопоставление.

### **Лабораторные работы.**

Анализ терминов и определений информационной безопасности.

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

- 1 Подготовка к практическим занятиям, повторение изучения лекционного материала;
- 2 Подготовка к лекциям, повторение учебного материала предыдущих лекций;
- 3 Изучение материалов лекционного курса по заданиям на самостоятельную проработку, выдаваемых преподавателем на занятиях;
- 4 Составление отчета по лабораторной работе.

## **Тема 4. Проблемы обеспечения информационной безопасности (ОПК-8)**

### **Лекция.**

Определение и место информационной безопасности в общей совокупности информационных проблем современного общества. Ретроспективный анализ развития подходов к защите информации. Современная постановка задачи защиты информации. Сущность, необходимость, пути и условия перехода к интенсивным способам защиты информации.

### **Лабораторные работы.**

Определение коэффициентов важности, полноты, адекватности, релевантности, толерантности информации.

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

- 1 Подготовка к практическим занятиям, повторение изучения лекционного материала;
- 2 Подготовка к лекциям, повторение учебного материала предыдущих лекций;
- 3 Изучение материалов лекционного курса по заданиям на самостоятельную проработку, выдаваемых преподавателем на занятиях;
- 4 Составление отчета по лабораторной работе.

## **Тема 5. Основы теории защиты информации (ОПК-8)**

### **Лекция.**

Особенности и состав научно-методологического базиса решения задач защиты информации. Общеметодологические принципы формирования теории защиты информации. Методологический базис теории защиты информации. Принципы автоформализации профессиональных знаний эксперта-аналитика. Моделирование процессов защиты информации. Основное содержание теории защиты информации.

### **Лабораторные работы.**

Лабораторная работа по программно-аппаратным методам защиты информации.

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

- 1 Подготовка к практическим занятиям, повторение изучения лекционного материала;
- 2 Подготовка к лекциям, повторение учебного материала предыдущих лекций;
- 3 Изучение материалов лекционного курса по заданиям на самостоятельную проработку, выдаваемых преподавателем на занятиях;
- 4 Составление отчета по лабораторной работе.

### **Тема 6. Общеметодологические принципы теории информационной безопасности.**

#### **Комплексность.**

**(ОПК-8)**

#### **Лекция.**

Этапы развития информационной безопасности: 1. Системы безопасности ресурса. 2. Этап развитой защиты (постепенное осознание необходимости комплексирования целей защиты, расширение арсенала используемых средств защиты, стали объединяться в функциональные самостоятельные системы защиты). 3. Этап комплексной защиты. Требования к системе защиты информации. Показатели информации: важность, полнота, адекватность, релевантность, толерантность. Комплексность: целевая, инструментальная, структурная, функциональная, временная.

#### **Лабораторные работы.**

Лабораторная работа по программно-аппаратным методам защиты информации.

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

- 1 Подготовка к практическим занятиям, повторение изучения лекционного материала;
- 2 Подготовка к лекциям, повторение учебного материала предыдущих лекций;
- 3 Изучение материалов лекционного курса по заданиям на самостоятельную проработку, выдаваемых преподавателем на занятиях;
- 4 Составление отчета по лабораторной работе.

### **Тема 7. Угрозы. Классификация и анализ угроз информационной безопасности.**

**(ОПК-8)**

#### **Лекция.**

Понятие угрозы. Виды угроз. Три наиболее выраженные угрозы: 1) подверженность физическому искажению или уничтожению; 2) возможность несанкционированной (случайной или злоумышленной) модификации; 3) опасность несанкционированного (случайного и преднамеренного) получения информации лицами, для которых она не предназначена. Характер происхождения угроз: умышленные факторы, естественные факторы. Источники угроз. Предпосылки появления угроз: объективные, субъективные

#### **Лабораторные работы.**

Лабораторная работа по программно-аппаратным методам защиты информации.

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

- 1 Подготовка к практическим занятиям, повторение изучения лекционного материала;
- 2 Подготовка к лекциям, повторение учебного материала предыдущих лекций;
- 3 Изучение материалов лекционного курса по заданиям на самостоятельную проработку, выдаваемых преподавателем на занятиях;
- 4 Составление отчета по лабораторной работе.

### **Тема 8. Методы нарушения конфиденциальности, целостности и доступности информации.**

**(ОПК-8)**

#### **Лекция.**



Классы каналов несанкционированного получения информации: 1) непосредственно с объекта; 2) с каналов отображения информации; 3) получение по внешним каналам; 4) подключение к каналам получения информации. Причины нарушения целостности информации: субъективные преднамеренные, субъективные непреднамеренные, объективные непреднамеренные. Потенциально возможные злоумышленные действия в автоматизированных системах обработки данных. Функции защиты информации: 4 функции. Стратегии защиты информации: оборонительная стратегия, наступательная стратегия, упреждающая стратегия. Архитектура систем защиты информации. Семирубежная модель защиты информации.

#### **Лабораторные работы.**

Лабораторная работа по программно-аппаратным методам защиты информации.

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

- 1 Подготовка к практическим занятиям, повторение изучения лекционного материала;
- 2 Подготовка к лекциям, повторение учебного материала предыдущих лекций;
- 3 Изучение материалов лекционного курса по заданиям на самостоятельную проработку, выдаваемых преподавателем на занятиях;
- 4 Составление отчета по лабораторной работе.

### **Тема 9. Причины, виды, каналы утечки и искажения информации. (ОПК-8)**

#### **Лекция.**

Три методологических подхода к оценке уязвимости информации: эмпирический, теоретический и теоретико-эмпирический. Модель затрат, разработанная специалистами американской фирмы IBM. Модель защиты - модель системы с полным перекрытием. Последовательность решения задачи защиты информации. Фундаментальные требования, которым должны удовлетворять те вычислительные системы, которые используются для обработки конфиденциальной информации. Требования разделены на три группы: стратегия, подотчетность, гарантии. Классификация автоматизированных систем и требований по защите информации. Факторы, влияющие на требуемый уровень защиты информации.

#### **Лабораторные работы.**

Лабораторная работа по инженерно-техническим средствам защиты информации.

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

- 1 Подготовка к практическим занятиям, повторение изучения лекционного материала;
- 2 Подготовка к лекциям, повторение учебного материала предыдущих лекций;
- 3 Изучение материалов лекционного курса по заданиям на самостоятельную проработку, выдаваемых преподавателем на занятиях;
- 4 Составление отчета по лабораторной работе.

### **Тема 10. Функции и задачи защиты информации. Проблемы региональной информационной безопасности. (ОПК-8)**

#### **Лекция.**

Методы формирования функций защиты. Соккрытие информации о средствах, комплексах, объектах и системах обработки информации. Дезинформация противника. Легендирование. Введение избыточности элементов системы. Резервирование элементов системы. Регулирование доступа к элементам системы и защищаемой информации. Регулирование использования элементов системы и защищаемой информации. Маскировка информации. Регистрация сведений. Уничтожение информации. Обеспечение сигнализации. Обеспечение реагирования. Управление системой защиты информации. Обеспечение требуемого уровня готовности обслуживающего персонала к решению задач информационной безопасности. Защита от информационного воздействия на технические средства обработки. Защита от информационного воздействия на общество. Защита от информационного воздействия на психику человека. Применение криптографии. Региональные компоненты защиты информации. Защита информации предприятия. Проведение анализа защищенности локального объекта.

### Лабораторные работы.

Лабораторная работа по инженерно-техническим средствам защиты информации.

#### Задания для самостоятельной работы.

- 1 Подготовка к практическим занятиям, повторение изучения лекционного материала;
- 2 Подготовка к лекциям, повторение учебного материала предыдущих лекций;
- 3 Изучение материалов лекционного курса по заданиям на самостоятельную проработку, выдаваемых преподавателем на занятиях;
- 4 Составление отчета по лабораторной работе.

## Тема 11. Развитие теории и практики защиты информации (ОПК-8)

### Лекция.

Основные выводы из истории развития теории и практики защиты информации. Перспективы развития теории и практики защиты информации. Проблемы создания и организации работы центров защиты информации. Подготовка кадров в области обеспечения информационной безопасности.

### Лабораторные работы.

Оценка безопасности информации на объектах ее обработки.

#### Задания для самостоятельной работы.

- 1 Подготовка к практическим занятиям, повторение изучения лекционного материала;
- 2 Подготовка к лекциям, повторение учебного материала предыдущих лекций;
- 3 Изучение материалов лекционного курса по заданиям на самостоятельную проработку, выдаваемых преподавателем на занятиях;
- 4 Составление отчета по лабораторной работе.

## 4. Контроль знаний обучающихся и типовые оценочные средства

### 4.1. Распределение баллов:

#### 2 семестр

- посещаемость – 10 баллов
- текущий контроль – 55 баллов
- контрольные срезы – 3 среза: 1 балл, 2 балла, 2 балла
- премиальные баллы – 8 баллов
- ответ на экзамене: не более 30 баллов

#### Распределение баллов по заданиям:

№ те мы	Название темы / вид учебной работы	Формы текущего контроля / срезы	Мак. кол-во баллов	Методика проведения занятия и оценки
1.	Введение. Стратегия национальной безопасности РФ. Доктрина информационной безопасности РФ.	Защита лабораторных работ	2	Лабораторные работы выполняются по текущему разделу или темы дисциплины. 2 балла – лабораторная работа выполнена, но имеет некоторые неточности выполнения, студент владеет представленным материалом, отвечает на заданные вопросы. 1 балл - лабораторная работа в целом выполнена, однако в процессе выполнения лабораторной работы допущены существенны ошибки, студент слабо владеет информацией по теме, при ответе использует заготовленный текст, затрудняется с ответами на задаваемые вопросы.

		Собеседование	1	<p>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. Устный опрос может применяться в различных формах: фронтальный, индивидуальный, комбинированный. Основные качества устного ответа подлежащего оценке:</p> <ul style="list-style-type: none"> <li>- правильность ответа по содержанию;</li> <li>- полнота и глубина ответа;</li> <li>- сознательность ответа;</li> <li>- логика изложения материала;</li> <li>- рациональность использованных приемов и способов решения поставленной учебной задачи;</li> <li>- своевременность и эффективность использования наглядных пособий и технических средств при ответе;</li> <li>- использование дополнительного материала;</li> <li>- рациональность использования времени, отведенного на задание.</li> </ul> <p>1 балл - студент умеет применять полученную при подготовке к практическому занятию информацию, отвечать на большинство вопросов, вести дискуссию.</p> <p>Если студент не владеет проблематикой практического занятия, не может отвечать на вопросы, зачитывает ответ по напечатанному тексту – ответ баллами не оценивается</p>
		Тестирование	1	<p>Оценка теста по текущему разделу или теме дисциплины</p> <p>1 балл – студент правильно отвечает на 50-100% вопросов в тесте.</p> <p>0 баллов - студент правильно отвечает на 25-50% вопросов в тесте.</p>
2.	Понятие национальной безопасности, виды безопасности. Информационная безопасность РФ.	Защита лабораторных работ	2	<p>Лабораторные работы выполняются по текущему разделу или теме дисциплины.</p> <p>2 балла – лабораторная работа выполнена, но имеет некоторые неточности выполнения, студент владеет представленным материалом, отвечает на заданные вопросы.</p> <p>1 балл - лабораторная работа в целом выполнена, однако в процессе выполнения лабораторной работы допущены существенны ошибки, студент слабо владеет информацией по теме, при ответе использует заготовленный текст, затрудняется с ответами на задаваемые вопросы.</p>

		Собеседование(контрольный срез)	1	<p>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. Устный опрос может применяться в различных формах: фронтальный, индивидуальный, комбинированный. Основные качества устного ответа подлежащего оценке:</p> <ul style="list-style-type: none"> <li>- правильность ответа по содержанию;</li> <li>- полнота и глубина ответа;</li> <li>- сознательность ответа;</li> <li>- логика изложения материала;</li> <li>- рациональность использованных приемов и способов решения поставленной учебной задачи;</li> <li>- своевременность и эффективность использования наглядных пособий и технических средств при ответе;</li> <li>- использование дополнительного материала;</li> <li>- рациональность использования времени, отведенного на задание.</li> </ul> <p>1 балл – 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</p> <p>Если студент не владеет проблематикой практического занятия, не может отвечать на вопросы, зачитывает ответ по напечатанному тексту – ответ баллами не оценивается</p>
		Тестирование	1	<p>Оценка теста по текущему разделу или теме дисциплины</p> <p>1 балл – студент правильно отвечает на 50-100% вопросов в тесте.</p> <p>0 баллов - студент правильно отвечает на 25-50% вопросов в тесте.</p>
		Защита лабораторных работ	2	<p>Лабораторные работы выполняются по текущему разделу или теме дисциплины.</p> <p>2 балла – лабораторная работа выполнена, но имеет некоторые неточности выполнения, студент владеет представленным материалом, отвечает на заданные вопросы.</p> <p>1 балл - лабораторная работа в целом выполнена, однако в процессе выполнения лабораторной работы допущены существенны ошибки, студент слабо владеет информацией по теме, при ответе использует заготовленный текст, затрудняется с ответами на задаваемые вопросы.</p>
3.	Терминологические основы информационной безопасности. Основные понятия и определения.			

		Собеседование	1	<p>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. Устный опрос может применяться в различных формах: фронтальный, индивидуальный, комбинированный. Основные качества устного ответа подлежащего оценке:</p> <ul style="list-style-type: none"> <li>- правильность ответа по содержанию;</li> <li>- полнота и глубина ответа;</li> <li>- сознательность ответа;</li> <li>- логика изложения материала;</li> <li>- рациональность использованных приемов и способов решения поставленной учебной задачи;</li> <li>- своевременность и эффективность использования наглядных пособий и технических средств при ответе;</li> <li>- использование дополнительного материала;</li> <li>- рациональность использования времени, отведенного на задание.</li> </ul> <p>1 балл - студент умеет применять полученную при подготовке к практическому занятию информацию, отвечать на большинство вопросов, вести дискуссию.</p> <p>Если студент не владеет проблематикой практического занятия, не может отвечать на вопросы, зачитывает ответ по напечатанному тексту – ответ баллами не оценивается</p>
		Тестирование	1	<p>Оценка теста по текущему разделу или теме дисциплины</p> <p>1 балл – студент правильно отвечает на 50-100% вопросов в тесте.</p> <p>0 баллов - студент правильно отвечает на 25-50% вопросов в тесте.</p>
		Защита лабораторных работ	2	<p>Лабораторные работы выполняются по текущему разделу или теме дисциплины.</p> <p>2 балла – лабораторная работа выполнена, но имеет некоторые неточности выполнения, студент владеет представленным материалом, отвечает на заданные вопросы.</p> <p>1 балл - лабораторная работа в целом выполнена, однако в процессе выполнения лабораторной работы допущены существенны ошибки, студент слабо владеет информацией по теме, при ответе использует заготовленный текст, затрудняется с ответами на задаваемые вопросы.</p>
4.	Проблемы обеспечения информационной безопасностью	Защита лабораторных работ	2	

		Собеседование	2	<p>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. Устный опрос может применяться в различных формах: фронтальный, индивидуальный, комбинированный. Основные качества устного ответа подлежащего оценке:</p> <ul style="list-style-type: none"> <li>- правильность ответа по содержанию;</li> <li>- полнота и глубина ответа;</li> <li>- сознательность ответа;</li> <li>- логика изложения материала;</li> <li>- рациональность использованных приемов и способов решения поставленной учебной задачи;</li> <li>- своевременность и эффективность использования наглядных пособий и технических средств при ответе;</li> <li>- использование дополнительного материала;</li> <li>- рациональность использования времени, отведенного на задание.</li> </ul> <p>2 балла – 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</p> <p>1 балл - студент умеет применять полученную при подготовке к практическому занятию информацию, отвечать на большинство вопросов, вести дискуссию .</p> <p>Если студент не владеет проблематикой практического занятия, не может отвечать на вопросы, зачитывает ответ по напечатанному тексту – ответ баллами не оценивается</p>
5.	Основы теории защиты информации	Защита лабораторных работ	2	<p>Лабораторные работы выполняются по текущему разделу или темы дисциплины.</p> <p>2 балла – лабораторная работа выполнена, но имеет некоторые неточности выполнения, студент владеет представленным материалом, отвечает на заданные вопросы.</p> <p>1 балл - лабораторная работа в целом выполнена, однако в процессе выполнения лабораторной работы допущены существенны ошибки, студент слабо владеет информацией по теме, при ответе использует заготовленный текст, затрудняется с ответами на задаваемые вопросы.</p>

	Собеседование	2	<p>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. Устный опрос может применяться в различных формах: фронтальный, индивидуальный, комбинированный. Основные качества устного ответа подлежащего оценке:</p> <ul style="list-style-type: none"> <li>- правильность ответа по содержанию;</li> <li>- полнота и глубина ответа;</li> <li>- сознательность ответа;</li> <li>- логика изложения материала;</li> <li>- рациональность использованных приемов и способов решения поставленной учебной задачи;</li> <li>- своевременность и эффективность использования наглядных пособий и технических средств при ответе;</li> <li>- использование дополнительного материала;</li> <li>- рациональность использования времени, отведенного на задание.</li> </ul> <p>2 балла – 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</p> <p>1 балл - студент умеет применять полученную при подготовке к практическому занятию информацию, отвечать на большинство вопросов, вести дискуссию .</p> <p>Если студент не владеет проблематикой практического занятия, не может отвечать на вопросы, зачитывает ответ по напечатанному тексту – ответ баллами не оценивается</p>
	Реферат	8	<p>8-10 баллов – реферат выполнен обучающимся самостоятельно, в полном объеме, с соблюдением необходимых технических параметров; стиль изложения отвечает специфике жанра научной работы; во введении логично, объективно и аргументировано характеризуется научная проблема; содержание реферата включает самостоятельное исследование, а заключение содержат выводы, логично вытекающие из содержания основной части; список литературы оформлен в соответствии с правилами ГОСТа</p> <p>6-7 баллов – во введение четко сформулированы основные позиции реферата, а содержание соответствует теме реферата; в содержании реферата логично, связно, но недостаточно полно излагается теоретическая или практическая часть; заключение содержит выводы, логично вытекающие из содержания основной части; стиль изложения соответствует специфике жанра научной работы; в оформлении списка литературы встречаются незначительные погрешности</p> <p>3-5 балла – во введение основные позиции реферата сформулированы нечетко или не вполне соответствуют теме исследования; в основной части реферата (теоретической и эмпирической главах) исследование выполнено недостаточно логично (убедительно) и последовательно; выводы в заключение отражают содержание глав не полностью или неточно; в оформлении списка литературы нет единообразия; стиль изложения не отвечает специфике жанра научной работы</p> <p>1-2 балла – текст реферата представляет несамостоятельное (компиляция; плагиат) научное исследование; реферат написан с несоблюдением технических и научных требований</p>

6.	Общеметодологические принципы теории информационной безопасности. Комплексность	Защита лабораторных работ	2	Лабораторные работы выполняются по текущему разделу или теме дисциплины. 2 балла – лабораторная работа выполнена, но имеет некоторые неточности выполнения, студент владеет представленным материалом, отвечает на заданные вопросы. 1 балл - лабораторная работа в целом выполнена, однако в процессе выполнения лабораторной работы допущены существенные ошибки, студент слабо владеет информацией по теме, при ответе использует заготовленный текст, затрудняется с ответами на задаваемые вопросы.
		Собеседование(контрольный срез)	2	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. 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. 2 балла – 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 1 балл - студент умеет применять полученную при подготовке к практическому занятию информацию, отвечать на большинство вопросов, вести дискуссию. Если студент не владеет проблематикой практического занятия, не может отвечать на вопросы, зачитывает ответ по напечатанному тексту – ответ баллами не оценивается
		Тестирование	2	Оценка теста по текущему разделу или теме дисциплины 2 балла – студент правильно отвечает на 50-100% вопросов в тесте. 1 балл - студент правильно отвечает на 25-50% вопросов в тесте.
7.	Угрозы. Классификация и анализ угроз информационной безопасности.	Защита лабораторных работ	2	Лабораторные работы выполняются по текущему разделу или теме дисциплины. 2 балла – лабораторная работа выполнена, но имеет некоторые неточности выполнения, студент владеет представленным материалом, отвечает на заданные вопросы. 1 балл - лабораторная работа в целом выполнена, однако в процессе выполнения лабораторной работы допущены существенные ошибки, студент слабо владеет информацией по теме, при ответе использует заготовленный текст, затрудняется с ответами на задаваемые вопросы.



		Собеседование	2	<p>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. Устный опрос может применяться в различных формах: фронтальный, индивидуальный, комбинированный. Основные качества устного ответа подлежащего оценке:</p> <ul style="list-style-type: none"> <li>- правильность ответа по содержанию;</li> <li>- полнота и глубина ответа;</li> <li>- сознательность ответа;</li> <li>- логика изложения материала;</li> <li>- рациональность использованных приемов и способов решения поставленной учебной задачи;</li> <li>- своевременность и эффективность использования наглядных пособий и технических средств при ответе;</li> <li>- использование дополнительного материала;</li> <li>- рациональность использования времени, отведенного на задание.</li> </ul> <p>2 балла – 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</p> <p>1 балл - студент умеет применять полученную при подготовке к практическому занятию информацию, отвечать на большинство вопросов, вести дискуссию .</p> <p>Если студент не владеет проблематикой практического занятия, не может отвечать на вопросы, зачитывает ответ по напечатанному тексту – ответ баллами не оценивается</p>
		Тестирование	2	<p>Оценка теста по текущему разделу или теме дисциплины</p> <p>2 балла – студент правильно отвечает на 50-100% вопросов в тесте.</p> <p>1 балл - студент правильно отвечает на 25-50% вопросов в тесте.</p>
8.	Методы нарушения конфиденциальности, целостности и доступности информации.	Защита лабораторных работ	2	<p>Лабораторные работы выполняются по текущему разделу или теме дисциплины.</p> <p>2 балла – лабораторная работа выполнена, но имеет некоторые неточности выполнения, студент владеет представленным материалом, отвечает на заданные вопросы.</p> <p>1 балл - лабораторная работа в целом выполнена, однако в процессе выполнения лабораторной работы допущены существенны ошибки, студент слабо владеет информацией по теме, при ответе использует заготовленный текст, затрудняется с ответами на задаваемые вопросы.</p>

		Собеседование	2	<p>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. Устный опрос может применяться в различных формах: фронтальный, индивидуальный, комбинированный. Основные качества устного ответа подлежащего оценке:</p> <ul style="list-style-type: none"> <li>- правильность ответа по содержанию;</li> <li>- полнота и глубина ответа;</li> <li>- сознательность ответа;</li> <li>- логика изложения материала;</li> <li>- рациональность использованных приемов и способов решения поставленной учебной задачи;</li> <li>- своевременность и эффективность использования наглядных пособий и технических средств при ответе;</li> <li>- использование дополнительного материала;</li> <li>- рациональность использования времени, отведенного на задание.</li> </ul> <p>2 балла – 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</p> <p>1 балл - студент умеет применять полученную при подготовке к практическому занятию информацию, отвечать на большинство вопросов, вести дискуссию .</p> <p>Если студент не владеет проблематикой практического занятия, не может отвечать на вопросы, зачитывает ответ по напечатанному тексту – ответ баллами не оценивается</p>
		Тестирование	2	<p>Оценка теста по текущему разделу или теме дисциплины</p> <p>2 балла – студент правильно отвечает на 50-100% вопросов в тесте.</p> <p>1 балл - студент правильно отвечает на 25-50% вопросов в тесте.</p>
9.	Причины, виды, каналы утечки и искажения информации.	Собеседование(контрольный срез)	2	<p>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. Устный опрос может применяться в различных формах: фронтальный, индивидуальный, комбинированный. Основные качества устного ответа подлежащего оценке:</p> <ul style="list-style-type: none"> <li>- правильность ответа по содержанию;</li> <li>- полнота и глубина ответа;</li> <li>- сознательность ответа;</li> <li>- логика изложения материала;</li> <li>- рациональность использованных приемов и способов решения поставленной учебной задачи;</li> <li>- своевременность и эффективность использования наглядных пособий и технических средств при ответе;</li> <li>- использование дополнительного материала;</li> <li>- рациональность использования времени, отведенного на задание.</li> </ul> <p>2 балла – 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</p> <p>1 балл - студент умеет применять полученную при подготовке к практическому занятию информацию, отвечать на большинство вопросов, вести дискуссию .</p> <p>Если студент не владеет проблематикой практического занятия, не может отвечать на вопросы, зачитывает ответ по напечатанному тексту – ответ баллами не оценивается</p>

		Тестирование	2	Оценка теста по текущему разделу или теме дисциплины 2 балла – студент правильно отвечает на 50-100% вопросов в тесте. 1 балл - студент правильно отвечает на 25-50% вопросов в тесте.
10.	Функции и задачи защиты информации. Проблемы региональной информационной безопасности.	Собеседование	2	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. 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. 2 балла – 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 1 балл - студент умеет применять полученную при подготовке к практическому занятию информацию, отвечать на большинство вопросов, вести дискуссию . Если студент не владеет проблематикой практического занятия, не может отвечать на вопросы, зачитывает ответ по напечатанному тексту – ответ баллами не оценивается
		Тестирование	2	Оценка теста по текущему разделу или теме дисциплины 2 балла – студент правильно отвечает на 50-100% вопросов в тесте. 1 балл - студент правильно отвечает на 25-50% вопросов в тесте.
11.	Развитие теории и практики защиты информации	Защита лабораторных работ	2	Лабораторные работы выполняются по текущему разделу или теме дисциплины. 2 балла – лабораторная работа выполнена, но имеет некоторые неточности выполнения, студент владеет представленным материалом, отвечает на заданные вопросы. 1 балл - лабораторная работа в целом выполнена, однако в процессе выполнения лабораторной работы допущены существенны ошибки, студент слабо владеет информацией по теме, при ответе использует заготовленный текст, затрудняется с ответами на задаваемые вопросы.

		Собеседование	2	<p>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. Устный опрос может применяться в различных формах: фронтальный, индивидуальный, комбинированный. Основные качества устного ответа подлежащего оценке:</p> <ul style="list-style-type: none"> <li>- правильность ответа по содержанию;</li> <li>- полнота и глубина ответа;</li> <li>- сознательность ответа;</li> <li>- логика изложения материала;</li> <li>- рациональность использованных приемов и способов решения поставленной учебной задачи;</li> <li>- своевременность и эффективность использования наглядных пособий и технических средств при ответе;</li> <li>- использование дополнительного материала;</li> <li>- рациональность использования времени, отведенного на задание.</li> </ul> <p>2 балла – 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</p> <p>1 балл - студент умеет применять полученную при подготовке к практическому занятию информацию, отвечать на большинство вопросов, вести дискуссию .</p> <p>Если студент не владеет проблематикой практического занятия, не может отвечать на вопросы, зачитывает ответ по напечатанному тексту – ответ баллами не оценивается</p>
		Тестирование	2	<p>Оценка теста по текущему разделу или теме дисциплины</p> <p>2 балла – студент правильно отвечает на 50-100% вопросов в тесте.</p> <p>1 балл - студент правильно отвечает на 25-50% вопросов в тесте.</p>
12.	Посещаемость		10	<p>10 баллов – стопроцентное посещение занятий студентом</p> <p>8 баллов – посещаемость студента составляет не менее 80 % занятий</p> <p>6 баллов – посещаемость студента составляет не менее 50 % занятий</p> <p>4 балла – посещаемость студента составляет не менее 25 % занятий</p>
13.	Премияльные баллы		8	<p>Дополнительные премияльные баллы могут быть начислены:</p> <ul style="list-style-type: none"> <li>- за проект, выполненный по заказу работодателя и реализованный на практике – 8 баллов;</li> <li>- постоянная активность во время практических занятий – 6 баллов;</li> <li>- полностью подготовленная к публикации статья по тематике в рамках дисциплины – 6 баллов;</li> <li>- участие с докладом во всероссийской олимпиаде по тематике изучаемой дисциплины – 8 баллов;</li> <li>- участие в выставке по тематике изучаемой дисциплины – 8 баллов;</li> <li>- публикация статьи по тематике изучаемой дисциплины в сборнике студенческих работ / материалах всероссийской конференции / журнале из перечня ВАК – 10 / 15 / 20</li> </ul>

14.	Ответ на экзамене	30	<p>Оценка «удовлетворительно»- студент имеет достаточный минимальный объем знаний по дисциплине; студентом усвоена основная литература, рекомендованная учебной программой; студент умеет ориентироваться в основных теориях, концепциях и направлениях по дисциплине и давать им оценку; студент умеет делать выводы без существенных ошибок;</p> <p>Оценка «хорошо» – «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.</p> <p>- Оценка «отлично» – систематизированные и полные знания по всем разделам дисциплины, а также по основным вопросам, выходящим за пределы учебной программы; точное использование научной терминологии систематически грамотное и логически правильное изложение ответа на вопросы; 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; активное участие в групповых обсуждениях.</p>
15.	Итого за семестр	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. Введение. Стратегия национальной безопасности РФ. Доктрина информационной безопасности РФ.

#### 1. Модель нарушителя информационной безопасности

Задачи практической работы:

- Дать характеристики основных групп нарушителей;
- Определить возможных нарушителей защиты рассматриваемого объекта информатизации;
- Определить каналы, используемые нарушителем для доступа к защищаемым ресурсам ИС

## Тема 2. Понятие национальной безопасности, виды безопасности. Информационная безопасность РФ.

Повышение надежности информационной системы.

Цель работы: Закрепление знаний по теме “Понятие национальной безопасности”

Самостоятельная работа студента под контролем преподавателя: При выполнении лабораторной работы, студент, опираясь на теоретический материал и “Рекомендации по выполнению лабораторных работ по дисциплине “Понятие национальной безопасности”, необходимо написать проект ИС, обладающей свойствами надежности. Для этого используется проектирование сверху вниз. Студентам необходимо разбить проект на модули. Каждому модулю написать входные и выходные параметры. Каждому модулю составляется спецификация. Последовательность действий: сформулировать требования, далее сформулировать цели, представить предварительный внешний проект, далее детальный внешний проект, проект архитектуры программы. Затем написать внешние проекты модулей и проекты логики модулей. Форма отчетности: проект ИС, состоящей из взаимосвязанных модулей, обладающей свойствами надёжности

## Тема 3. Терминологические основы информационной безопасности. Основные понятия и определения.

Анализ терминов и определений информационной безопасности.

Цель: Познакомить студентов с проблемами информационной безопасности и основными направлениями их решения; дать представление о принципах и подходах к решению задач защиты информации; выработать навыки разработки политики информационной безопасности, применения современных методов и средств защиты информационных ресурсов предприятий.

- Основные понятия. Информационная безопасность и ее составные части. Понятия целостности, конфиденциальности, аутентичности и доступности информации. Защищенность информационных ресурсов, систем и технологий.
- Основы информационной безопасности. Концепция и общие направления обеспечения информационной безопасности. Угрозы безопасности, стратегия и тактика защиты информации.
- Современное состояние проблемы информационной безопасности. Категории информационной безопасности. Модели защиты информации (Biba, Goguen-Mesenguer, Clark-Wilson). Технологии несанкционированного доступа к информационным ресурсам и системам. Принципы построения систем защиты информации. Стандарты безопасности информационных систем.
- Программно-аппаратные методы защиты информации. Структура подсистем безопасности операционных систем (Windows, UNIX), их функции: идентификация, разграничение доступа, аудит, защита обмена данных. Критерии защищенности ОС. Защита РС: ограничение доступа, хранение ключевой информации, привязка программного обеспечения к аппаратному окружению и физическим носителям.
- Криптографические методы защиты информации. Классификация алгоритмов шифрования информации. Криптографические стандарты.
- Безопасность компьютерных сетей. Защита серверов, рабочих станций, среды передачи информации, узлов коммутации сетей. Защита от вирусов, межсетевые экраны (Firewall), анализ трафика.

- Системы обеспечения корпоративной безопасности информации. Комплексный подход к проблеме защиты информации. Уровни (административный, процедурный, программно-технический) и приоритеты политики безопасности. Анализ рисков, исследование защищенности информации. Обзор новейших технологий защиты информации.

#### Тема 4. Проблемы обеспечения информационной безопасности

Определение коэффициентов важности, полноты, адекватности, релевантности, толерантности информации.

Цель работы: работа в тестовой программе (Aida или CPU-z); основные настройки базовой системы ввода вывода. Оборудование: учебный персональный компьютер.

Практическое задание. Оцените результат поиска в сети Интернет и ответьте на вопросы:

1. Какую поисковую систему ты использовал?
2. Адрес сайта, который ты изучал.
3. Название сайта.
4. Долго ли загружается страница?
5. Привлекательно ли она выглядит?
6. Легко ли читается?
7. Есть ли изображения? Какого качества?
8. Несут ли изображения дополнительную информацию?
9. Указаны ли имя и адрес электронной почты автора сайта?
10. Есть ли указание, когда был подготовлен (обновлен) сайт?
11. Есть ли возможность при переходе на следующие страницы автоматически вернуться на первую?
12. Достаточно ли полно заглавие сайта раскрывает его содержание?
13. Смог бы ты получить больше информации из печатного справочника?
14. Во всем ли ты согласен с автором?
15. Не попадалась ли тебе неверная информация?
16. Достаточно ли актуальна предложенная информация?
17. Есть ли на сайте отсылки к другим сайтам с похожей информацией?

Отчет. Отчет должен содержать:

1. наименование работы;
2. цель работы;
3. задание;
4. последовательность выполнения работы;
5. ответы на контрольные вопросы;
6. вывод о проделанной работе.

Контрольные вопросы

1. Назовите причины недоверия информации?
2. Каким требованиям должна соответствовать оценочная информация?

#### Тема 5. Основы теории защиты информации

Создание отказоустойчивых информационных систем

Обеспечение защиты информации по угрозе отказ в обслуживании

Методы обеспечения защиты информации по угрозе отказ в обслуживании

Как обеспечивается защита информации в сети Интернет?

Опишите организационные средства защиты информации.

Тема 6. Общеметодологические принципы теории информационной безопасности. Комплексность. Методы и средства защиты информации от традиционного шпионажа и диверсий

Определение шпионажа

Определение диверсии

Методы борьбы со шпионажем

Методы борьбы с диверсиями

Тема 7. Угрозы. Классификация и анализ угроз информационной безопасности.

Защита информации от инсайдерских угроз

- 1 Подготовка к практическим занятиям, повторение изучения лекционного материала;
- 2 Подготовка к лекциям, повторение учебного материала предыдущих лекций;
- 3 Изучение материалов лекционного курса по заданиям на самостоятельную проработку, выдаваемых преподавателем на занятиях;
- 4 Составление отчета по лабораторной работе.

Тема 8. Методы нарушения конфиденциальности, целостности и доступности информации.

Наиболее распространенные угрозы доступности, целостности и конфиденциальности.

Цель работы:

Изучить наиболее распространенные угрозы, а также уязвимые места защиты, которые эти угрозы обычно эксплуатируют. Получить навыки выбора наиболее экономичных средств обеспечения безопасности.

Порядок выполнения работы

1. Ознакомиться с содержанием лабораторной работы .
2. Выполнить практическое задание.
3. Ответить на контрольные вопросы.

Практические задания

- 1 Разработать интерфейс пользователя « Наиболее распространенные угрозы доступности».
- 2 Разработать интерфейс пользователя «Основные угрозы целостности».
- 3 Разработать интерфейс пользователя «Основные угрозы конфиденциальности».

Контрольные вопросы

Вариант 1

1. Окно опасности — это:
  - промежуток времени
  - часть пространства
  - плохо закрепленная деталь строительной конструкции
2. Самыми опасными угрозами являются:
  - непреднамеренные ошибки штатных сотрудников
  - вирусные инфекции
  - атаки хакеров
3. Дублирование сообщений является угрозой:
  - доступности
  - конфиденциальности
  - целостности
4. Melissa - это:
  - бомба
  - вирус
  - червь

Вариант 2



1. Окно опасности появляется, когда:
  - становится известно о средствах использования уязвимости
  - появляется возможность использовать уязвимость
  - устанавливается новое ПО
2. Самыми опасными источниками угроз являются:
  - внутренние
  - внешние
  - пограничные
3. Перехват данных является угрозой:
  - доступности
  - конфиденциальности
  - целостности
4. Melissa - это:
  - макровирус для файлов MS-Word
  - макровирус для файлов PDF
  - макровирус для файлов Postscript

#### Тема 11. Развитие теории и практики защиты информации

Оценка безопасности информации на объектах ее обработки.

Опишите функции, задачи и структуру центров защиты информации.

Опишите структуру среды защиты.

Как происходит подготовка кадров в области обеспечения информационной безопасности?

Анализ нормативно-правовых документов по защите информации

### Реферат

#### Тема 5. Основы теории защиты информации

1. Состояние и тенденции развития национальной безопасности Российской Федерации в современном мире.
2. Информационные основы обеспечения информационной безопасности.
3. Сущность и содержание национальной безопасности России.
4. Угрозы национальной и информационной безопасности Российской Федерации.
5. Угрозы информационной безопасности.
6. Модель нарушителя информационной безопасности
7. Правовое регулирование информационной безопасности.
8. Повышение надежности информационной системы.
9. Несанкционированный доступ.
10. Создание отказоустойчивых информационных систем
11. Методы и средства защиты информации от традиционного шпионажа и диверсий
12. Защита информации от инсайдерских угроз
13. Этапы развития информационной безопасности.
14. Комплексный подход защиты информации.
15. Наиболее распространенные угрозы доступности, целостности и конфиденциальности.
16. Показатели уязвимости информационной системы.
17. Виды угроз информационным системам.
18. Причины, виды, каналы утечки и искажения информации.

19. Способы и методы предотвращения утечки информации.
20. Контроль доступа к информационным системам.
21. Защита от информационного воздействия.
22. Избыточность элементов система.
23. Современные вопросы защиты информации.
24. Функции, задачи и структура центров защиты информации.
25. Перспективы развития теории и практики защиты информации.

### **Собеседование**

Тема 1. Введение. Стратегия национальной безопасности РФ. Доктрина информационной безопасности РФ.

- 1 Общие положения стратегии национальной безопасности Российской Федерации.
- 2 Опишите состояние и тенденции развития России в современном мире.
- 3 В чём состоят национальные интересы Российской Федерации в области национальной безопасности?
- 4 Опишите стратегические национальные приоритеты в области национальной безопасности.
- 5 В чём заключается обеспечение национальной безопасности?
- 6 Общие положения Доктрины информационной безопасности РФ.
- 7 Организационные и нормативно-правовые основы обеспечения информационной безопасности.
- 8 Информационные основы обеспечения информационной безопасности.
- 9 Перечислите основные информационные угрозы.
- 10 Основные направления обеспечения информационной безопасности.

Тема 2. Понятие национальной безопасности, виды безопасности. Информационная безопасность РФ.

1. Понятие национальной безопасности.
2. Опишите сущность и содержание национальной безопасности России.
3. Перечислите направления и задачи по обеспечению национальной безопасности.
4. Опишите объект и субъект обеспечения безопасности.
5. Система обеспечения национальной безопасности Российской Федерации: ее назначение и состав.
6. Опишите принципы обеспечения национальной безопасности Российской Федерации.
7. Перечислите и опишите виды национальной безопасности.
8. Понятие информационной безопасности.
9. Что такое информационный ресурс?
10. Перечислите угрозы национальной и информационной безопасности Российской Федерации.

Тема 3. Терминологические основы информационной безопасности. Основные понятия и определения.

1. Определение информационной безопасности.
2. Определение системы информационной безопасности.
3. Перечислите угрозы информационной безопасности.
4. Основные составляющие информационной безопасности.
5. Объекты защиты. Определение и классификация.

Тема 4. Проблемы обеспечения информационной безопасности

1. Составляющие проблемы обеспечения информационной безопасности.
2. Перечислите и опишите причины проблем информационной безопасности.

3. Перечислите источники угроз информационной безопасности.
4. Опишите меры противодействия угрозам информационной безопасности.
5. Что такое целостность данных? Назовите методы обеспечения целостности данных.
6. Что такое конфиденциальность информации?
7. Что такое доступность информации?
8. В чём заключается правовое регулирование информационной безопасности?
9. Что такое региональная политика обеспечения информационной безопасности?
10. Что является предметом политики информационной безопасности?

#### Тема 5. Основы теории защиты информации

1. Понятие теории защиты информации.
2. Назовите принципы формирования теории защиты информации.
3. Перечислите задачи теории защиты информации.
4. В чём заключается комплексный подход к решению задач защиты?
5. Опишите методологический базис теории защиты информации.
6. Сформулируйте модель защиты информации.
7. Что такое несанкционированный доступ? Источники и последствия.
8. Опишите и классифицируйте вредоносные программы и вирусы.

#### Тема 6. Общеметодологические принципы теории информационной безопасности. Комплексность.

1. Опишите этапы развития информационной безопасности.
2. Опишите системы безопасности информационного ресурса.
3. В чём заключаются требования к системе защиты информации?
4. Дайте определение политике безопасности информации.
5. Перечислите показатели информации.
6. Перечислите элементы информации, требующие защиты.
7. В чём заключается комплексный подход защиты информации?
8. Как осуществляется управление информационными ресурсами?
9. Составляющие информационной базы.
10. Как обеспечивается безопасность рабочей станции в сети?

#### Тема 7. Угрозы. Классификация и анализ угроз информационной безопасности.

1. Перечислите классы каналов несанкционированного доступа получения информации.
2. Перечислите показатели уязвимости информационной системы.
3. В чём состоят причины нарушения целостности информации?
4. Сформулируйте модель нарушителя информационных систем.
5. Виды угроз информационным системам

#### Тема 8. Методы нарушения конфиденциальности, целостности и доступности информации.

1. Понятие нарушения конфиденциальности информации.
2. Виды нарушения конфиденциальности.
3. Как обеспечивается конфиденциальность сообщений и данных?
4. Дайте определение политике доступа к информации.
5. Понятие целостности информации.
6. Причины, виды, каналы утечки и искажения информации.
7. Понятие доступности информации.
8. Как происходит нарушение доступности информации?
9. В чём состоит проблема доступа к информации?
10. Опишите методы защиты доступности информации.

### Тема 9. Причины, виды, каналы утечки и искажения информации.

1. Назовите умышленные и непреднамеренные причины искажения информации.
2. Как обеспечивается предотвращение искажения информации?
3. Назовите виды утечки информации.
4. Как происходит и как предотвратить разглашение информации?
5. Опишите несанкционированный доступ как угрозу искажения информации.
6. Перечислите каналы утечки информации.
7. Опишите способы и методы предотвращения утечки информации.
8. Дайте определение и опишите технические средства перехвата информации.
9. В чём состоит проблема доступа к информации?
10. Как обеспечивается контроль доступа?

### Тема 10. Функции и задачи защиты информации. Проблемы региональной информационной безопасности.

1. Опишите методы формирования функций защиты.
2. Как обеспечивается и когда необходимо скрытие информации о средствах, комплексах, объектах и системах обработки информации?
3. Как обеспечивается и когда необходимо введение избыточности элементов системы.
4. Дайте определение и описание процессу резервирования элементов системы.
5. Как обеспечивается регулирование доступа к элементам системы и защищаемой информации?
6. Как происходит регулирование использования элементов системы и защищаемой информации?
7. Дайте определение маскировке информации.
8. Как происходит управление системой защиты информации?
9. В чём состоит обеспечение требуемого уровня готовности обслуживающего персонала к решению задач информационной безопасности?
10. Как обеспечивается защита от информационного воздействия?

### Тема 11. Развитие теории и практики защиты информации

1. В чём заключаются основные вопросы защиты информации в современном понимании?
2. Сформулируйте перспективы развития теории и практики защиты информации.
3. Как обеспечивается совершенствование теоретических основ защиты информации?
4. Как происходит перевод защиты информации на индустриальную тему?
5. Как обеспечивается компьютерная безопасность в современном мире?
6. Как обеспечивается компьютерная безопасность объекта?
7. В чём заключаются проблемы создания и организации работы центров защиты информации?

## Тестирование

### Тема 1. Введение. Стратегия национальной безопасности РФ. Доктрина информационной безопасности РФ.

1. Безопасность это
  - а) Чувство защищенности человека
  - б) Система государственных мер по защищенности человека
  - в) Состояние защищенности жизненно важных интересов личности общества и государства от внешних и внутренних угроз
  - г) Состояние защищенности общества от преступности.
2. Чем является стратегия национальной безопасности Российской Федерации?

- а) федеральным законом
- б) базовым документом стратегического планирования
- в) базовым документом обеспечения безопасности
- г) нормативным правовым актом

3. Под национальной безопасностью РФ понимается:

- а) предотвращение, локализация и нейтрализация военных угроз Российской Федерации
- б) безопасность Российского многонационального народа как носителя суверенитета и единственного источника власти в РФ
- в) совокупность факторов, обеспечивающих жизнеспособность государства и, в первую очередь, его возможность обеспечивать защиту суверенитета, территориальной целостности и экономической независимости
- г) обеспечение состояния защищённости интересов государства

4. Что не относится к объектам обеспечения безопасности?

- а) общество
- б) личность
- в) государство
- г) диаспора

5. Что не относится к принципам обеспечения безопасности?

- а) Государственный суверенитет
- б) Интеграция с международными системами безопасности
- в) Баланс жизненно важных интересов личности, общества и государства
- г) законность

## Тема 2. Понятие национальной безопасности, виды безопасности. Информационная безопасность РФ.

1. Стратегия национальной безопасности Российской Федерации включает в себя:

- а) стратегические цели
- б) главные стратегические риски и угрозы
- в) противодействия угрозам экономической безопасности
- г) всё из вышеперечисленного

2. За своевременное выявление угроз национальной безопасности РФ, за подготовку оперативных решений по предотвращению чрезвычайных ситуаций и разработку основных направлений стратегии обеспечения национальной безопасности РФ ответственен:

- а) Президент РФ
- б) Совет Федерации и Государственная Дума Федерального Собрания РФ
- в) Правительство РФ
- г) Совет Безопасности РФ

3. Основные направления деятельности государства и общества по обеспечению национальной безопасности Российской Федерации являются все, кроме:

- а) объективный и всесторонний анализ и прогнозирование угроз национальной безопасности во всех сферах;
- б) определение критериев национальной безопасности, выработка комплекса мер и механизмов обеспечения национальной безопасности в различных сферах;
- в) соблюдение норм международного права и российских законов;
- г) поддержание на необходимом уровне стратегических и мобилизационных ресурсов государства.

4. Что представляет собой Доктрина информационной безопасности РФ?

- а) совокупность официальных взглядов на цели, задачи, принципы и основные направления обеспечения информационной безопасности Российской Федерации
- б) совокупность нормативно-правовых норм в области обеспечения информационной безопасности
- в) указ президента РФ о конфиденциальности информации
- г) свод законов об обработке информации на предприятиях

5. К какому виду документов относится Доктрина информационной безопасности РФ?

- а) организационные Нормативно-методические
- б) нормативно-методические
- в) плановые
- г) указ

### Тема 3. Терминологические основы информационной безопасности. Основные понятия и определения.

1. Доктрина необходима для

- а) предотвращения угроз информации, относимой к государственной тайне
- б) формирования государственной политики и выработки мер по совершенствованию системы обеспечения информационной безопасности
- в) осуществления внешней политики в области информационной безопасности
- г) защиты прав граждан на конфиденциальность информации

2. Что является одним из основных негативных факторов, влияющих на состояние информационной безопасности?

- а) незаконное получение, использование, разглашение информации, составляющей коммерческую, служебную или иную охраняемую законом тайну
- б) программно-аппаратные отказы, которые происходят из-за нестабильной работы аппаратного комплекса
- в) наращивание рядом зарубежных стран возможностей информационно-технического воздействия на информационную инфраструктуру в военных целях
- г) нарушение доступности информации

3. К угрозам национальной безопасности относятся все, кроме:

- а) террористическая угроза
- б) угроза распространения наркотических веществ
- в) угроза истощения природных ресурсов и ухудшения экологической ситуации
- г) угроза физическому здоровью нации

4. Основными принципами обеспечения национальной безопасности РФ являются все, кроме:

- а) соблюдение Конституции РФ и законодательства РФ
- б) реальность выдвигаемых задач
- в) приоритетность силовых мер обеспечения национальной безопасности
- г) единство, взаимосвязь и сбалансированность всех видов безопасности

5. Основными принципами обеспечения национальной безопасности Российской Федерации являются все, кроме:

- а) соблюдение Конституции РФ и законодательства РФ;
- б) реальность выдвигаемых задач;
- в) единство, взаимосвязь и сбалансированность всех видов безопасности;

г) приоритетность силовых мер обеспечения национальной безопасности

Тема 6. Общеметодологические принципы теории информационной безопасности. Комплексность.

1. Что такое политики безопасности?

- а) Пошаговые инструкции по выполнению задач безопасности
- б) Общие руководящие требования по достижению определенного уровня безопасности
- в) Широкие, высокоуровневые заявления руководства
- г) Детализированные документы по обработке инцидентов безопасности

2. Кто является основным ответственным за определение уровня классификации информации?

- а) Руководитель среднего звена
- б) Высшее руководство
- в) Владелец
- г) Пользователь

3. Какая категория является наиболее рискованной для компании с точки зрения вероятного мошенничества и нарушения безопасности?

- а) Сотрудники
- б) Хакеры
- в) Атакующие
- г) Контрагенты

4. Что такое политики безопасности?

- а) Пошаговые инструкции по выполнению задач безопасности
- б) Общие руководящие требования по достижению определенного уровня безопасности
- в) Широкие, высокоуровневые заявления руководства
- г) Детализированные документы по обработке инцидентов безопасности

5. Что наиболее важно обеспечить при классификации данных?

- а) Политика доступа для сотрудников, контрагентов и клиентов
- б) Необходимый уровень доступности, целостности и конфиденциальности
- в) Оценка уровня риска и отмена контрмер
- г) Управление доступом, которое должно защищать данные

Тема 7. Угрозы. Классификация и анализ угроз информационной безопасности.

1. Когда целесообразно не предпринимать никаких действий в отношении выявленных рисков?

- а) Никогда. Для обеспечения хорошей безопасности нужно учитывать и снижать все риски
- б) Когда риски не могут быть приняты во внимание по политическим соображениям
- в) Когда необходимые защитные меры слишком сложны
- г) Когда стоимость контрмер превышает ценность актива и потенциальные потери

2. Обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя это

- а) Электронное сообщение
- б) Распространение информации
- в) Предоставление информации
- г) Конфиденциальность информации

3. Все компоненты информационной системы предприятия, в котором накапливаются и обрабатываются персональные данные это:

- а) Информационная система персональных данных
- б) База данных
- в) Централизованное хранилище данных
- г) Сервер

4. К сведениям конфиденциального характера, согласно Указу президента РФ от 6 марта 1997 г., относятся:

- а) Информация о распространении программ
- б) Информация о лицензировании программного обеспечения
- в) Личная тайна
- г) Персональные данные

5. Отношения, связанные с обработкой персональных данных, регулируются законом...

- а) «Об информации, информационных технологиях»
- б) «О защите информации»
- в) Федеральным законом «О персональных данных»
- г) Федеральным законом «О конфиденциальной информации»

Тема 8. Методы нарушения конфиденциальности, целостности и доступности информации.

1. Процесс сообщения субъектом своего имени или номера, с целью получения определённых полномочий (прав доступа) на выполнение некоторых (разрешенных ему) действий в системах с ограниченным доступом:

- а) Авторизация
- б) Аутентификация
- в) Обезличивание
- г) Идентификация

2. Процедура проверки соответствия субъекта и того, за кого он пытается себя выдать, с помощью некой уникальной информации:

- а) Авторизация
- б) Обезличивание
- в) Дегерсонализация
- г) Аутентификация

3. Что такое персональные данные?

- а) Любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу
- б) Фамилия, имя, отчество физического лица
- в) Год, месяц, дата и место рождения, адрес физического лица
- г) Сведения о семейном, социальном, имущественном положении человека, составляющие понятие «профессиональная тайна»

4. Документированная информация, доступ к которой ограничивает в соответствии с законодательством РФ:

- а) Информация составляющая государственную тайну
- б) Информация составляющая коммерческую тайну
- в) Конфиденциальная информация
- г) Документированная информация



5. В каком году был принят закон "О государственной тайне"?

- а) 1982
- б) 1988
- в) 1993
- г) 2005

#### Тема 9. Причины, виды, каналы утечки и искажения информации.

1. Дублирование сообщений является угрозой:

- а) доступности
- б) конфиденциальности
- в) целостности
- г) достоверности

2. Уголовный кодекс РФ не предусматривает наказания за:

- а) создание, использование и распространение вредоносных программ
- б) ведение личной корреспонденции на производственной технической базе
- в) неправомерный доступ к охраняемой законом компьютерной информации
- г) нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации

3. Степень защищенности информации от негативного воздействия на неё с точки зрения нарушения её физической и логической целостности или несанкционированного использования — это

- а) уязвимость информации
- б) надежность информации
- в) защищенность информации
- г) базопасность информации

4. Соответствие средств безопасности решаемым задачам характеризует

- а) эффективность
- б) корректность
- а) адекватность
- г) унификация

5. С помощью закрытого ключа информация

- а) копируется
- б) транслируется
- в) расшифровывается
- г) зашифровывается

#### Тема 10. Функции и задачи защиты информации. Проблемы региональной информационной безопасности.

1. Совокупность свойств, обуславливающих пригодность информации удовлетворять определенные потребности в соответствии с ее назначением, называется

- а) актуальностью информации
- б) доступностью
- в) качеством информации
- г) целостностью

2. Первым этапом разработки системы защиты информационной системы является
  - а) анализ потенциально возможных угроз информации
  - б) изучение информационных потоков
  - в) стандартизация программного обеспечения
  - г) оценка возможных потерь
  
3. Что является угрозой конфиденциальности информации?
  - а) несанкционированная модификация
  - б) искажение
  - в) несанкционированное получение
  - г) уничтожение
  
4. Возможность получения необходимых пользователю данных или сервисов за разумное время
  - а) актуальность
  - б) восстанавливаемость
  - в) детерминированность
  - г) доступность
  
5. Защита информации это:
  - а) преобразование информации, в результате которого содержание информации становится непонятным для субъекта, не имеющего доступа;
  - б) получение субъектом возможности ознакомления с информацией, в том числе при помощи технических средств;
  - в) совокупность правил, регламентирующих порядок и условия доступа субъекта к информации и ее носителям;
  - г) деятельность по предотвращению утечки информации, несанкционированных и непреднамеренных воздействий на неё.

#### Тема 11. Развитие теории и практики защиты информации

1. Преднамеренная угроза безопасности информации
  - а) наводнение
  - б) кража
  - в) повреждение кабеля, по которому идет передача, в связи с погодными условиями
  - г) ошибка разработчика
  
2. Концепция системы защиты от информационного оружия не должна включать...
  - а) средства нанесения контратаки с помощью информационного оружия
  - б) механизмы защиты пользователей от различных типов и уровней угроз для национальной информационной инфраструктуры
  - в) признаки, сигнализирующие о возможном нападении
  - г) процедуры оценки уровня и особенностей атаки против национальной инфраструктуры в целом и отдельных пользователей
  
3. Принцип, по которому субъекты информационного права обязаны строго соблюдать Конституцию РФ и законодательство РФ
  - а) Принцип ответственности
  - б) Принцип законности
  - в) Принцип свободного доступа
  - г) Принцип оборотоспособности информации

4. В чем заключается метод защиты информации - разграничение доступа?

- а) В создании некоторой физической замкнутой преграды вокруг объекта защиты с организацией функциональными обязанностями
- б) В том, что из числа допущенных к ней должностных лиц выделяется группа, которой предоставляется доступ только при одновременном предъявлении полномочий всех членов группы
- в) В разделении информации, циркулирующей в объекте защиты, на части и организации доступа к ней должностных лиц в соответствии с их функциональными обязанностями и полномочиями
- г) В преобразовании информации с помощью специальных алгоритмов либо аппаратных решений и кодов ключей, т.е. в приведении её к неявному виду

5. Что означает термин "правовые меры защиты информации"?

- а) Действующие в стране законы, указы и другие нормативные акты, регламентирующие правила обращения с информацией и ответственность за их нарушения.
- б) Традиционно сложившиеся в стране или обществе нормы поведения и правила обращения с информацией.
- в) Меры, регламентирующие процессы функционирования системы обработки данных, использования её ресурсов.
- г) Правила разграничения доступа к информации для определённых групп лиц

4.3 Промежуточная аттестация по дисциплине проводится в форме экзамена

#### **Типовые вопросы экзамена (ОПК-8)**

- 1 Теория защиты информации. Основные направления
- 2 Виды угроз. Основные нарушения.
- 3 Общая модель воздействия на информацию.
- 4 Общая модель процесса нарушения физической целостности информации.
- 5 Методы определения требований к защите информации.
- 6 Допущения в моделях оценки уязвимости информации.
- 7 Классификация требований к средствам защиты информации.
- 8 Способы и средства защиты информации.
- 9 Способы «абсолютной системы защиты».

#### **Типовые задания для экзамена (ОПК-8)**

- 1 Содержание интересов личности, общества и государства в информационной сфере.
- 2 Источники и содержание угроз в информационной сфере.
- 3 Классы информационных ресурсов.
- 4 Перечислите категории информации.
- 5 Носители информации. Понятие и классификация.
- 6 Средства защиты информации. Понятие и классификация.
- 7 Законодательный уровень информационной безопасности.
- 8 Перечислите органы, обеспечивающие информационную безопасность.

4.4. Шкала оценивания промежуточной аттестации

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

<p>«отлично» (85 - 100 баллов)</p>	ОПК-8	<p>Демонстрирует высокий уровень теоретических знаний в области основ информационной безопасности.</p> <p>Анализирует существующие методики определений требования к защите информации.</p> <p>Демонстрирует знание принципов обеспечения защиты информации и источников угроз ИБ.</p> <p>Способен продемонстрировать современные подходы к технологиям и методам обеспечения ИБ.</p> <p>Способен осуществлять подробный подбор научно-технической литературы, нормативных и методических документов в целях решения задач профессиональной деятельности.</p>
<p>«хорошо» (70 - 84 баллов)</p>	ОПК-8	<p>Демонстрирует достаточный уровень теоретических знаний в области основ информационной безопасности.</p> <p>Анализирует существующие методики определений требования к защите информации.</p> <p>Демонстрирует знание принципов обеспечения защиты информации и источников угроз ИБ.</p> <p>Способен продемонстрировать современные подходы к технологиям и методам обеспечения ИБ.</p> <p>Способен осуществлять подбор научно-технической литературы, нормативных и методических документов в целях решения задач профессиональной деятельности.</p>
<p>«удовлетворительно» (50 - 69 баллов)</p>	ОПК-8	<p>Демонстрирует слабый уровень знаний в области основ информационной безопасности.</p> <p>Анализирует существующие методики определений требования к защите информации.</p> <p>Демонстрирует слабый уровень знаний принципов обеспечения защиты информации и источников угроз ИБ.</p> <p>Не способен продемонстрировать современные подходы к технологиям и методам обеспечения ИБ.</p> <p>Способен осуществлять частичный подбор, научно-технической литературы, нормативных и методических документов в целях решения задач профессиональной деятельности.</p>
<p>«неудовлетворительно» (менее 50 баллов)</p>	ОПК-8	<p>Не имеет знаний в области основ информационной безопасности.</p> <p>Не анализирует существующие методики определений требования к защите информации.</p> <p>Не способен продемонстрировать знания принципов обеспечения защиты информации и источников угроз ИБ.</p> <p>Не способен продемонстрировать современные подходы к технологиям и методам обеспечения ИБ.</p> <p>Не способен осуществлять подбор, научно-технической литературы, нормативных и методических документов в целях решения задач профессиональной деятельности.</p>

## 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. Тамб. гос. ун-т им. Г.Р. Державина, Ин-т математики, физики и информатики Техническая защита информации : учеб. пособие. - Тамбов: [Б.и.], 2014. - 1 электрон. опт. диск (CD-ROM)

### 6.2 Дополнительная литература:

1. Загинайлов Ю. Н. Основы информационной безопасности: курс визуальных лекций : учебное пособие. - Москва|Берлин: Директ-Медиа, 2015. - 105 с. - Текст : электронный // ЭБС «Университетская библиотека онлайн» [сайт]. - URL: <http://biblioclub.ru/index.php?page=book&id=362895>
2. Загинайлов Ю. Н. Теория информационной безопасности и методология защиты информации : учебное пособие. - Москва|Берлин: Директ-Медиа, 2015. - 253 с. - Текст : электронный // ЭБС «Университетская библиотека онлайн» [сайт]. - URL: <http://biblioclub.ru/index.php?page=book&id=276557>
3. Аверченков В. И., Рытов М. Ю., Кувыклин А. В., Рудановский М. В. Аудит информационной безопасности органов исполнительной власти : учебное пособие. - 4-е изд., стер.. - Москва: Флинта, 2016. - 100 с. - Текст : электронный // ЭБС «Университетская библиотека онлайн» [сайт]. - URL: <http://biblioclub.ru/index.php?page=book&id=93259>
4. Аверченков, В. И., Рытов, М. Ю., Кувыклин, А. В., Рудановский, М. В. Аудит информационной безопасности органов исполнительной власти : учебное пособие. - Весь срок охраны авторского права; Аудит информационной безопасности органов исполнительной власти. - Брянск: Брянский государственный технический университет, 2012. - 100 с. - Текст : электронный // IPR BOOKS [сайт]. - URL: <http://www.iprbookshop.ru/6992.html>

5. Комплексное обеспечение информационной безопасности автоматизированных систем : лабораторный практикум. - Ставрополь: Северо-Кавказский Федеральный университет (СКФУ), 2016. - 242 с. - Текст : электронный // ЭБС «Университетская библиотека онлайн» [сайт]. - URL: <http://biblioclub.ru/index.php?page=book&id=458012>

### 6.3 Иные источники:

1. Курс «Стандарты информационной безопасности» - <https://www.intuit.ru/studies/courses/30/30/info>
2. Курс «Основы информационной безопасности» - <https://www.intuit.ru/studies/courses/10/10/info>

## 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

Операционная система Microsoft Windows 10

Adobe Reader XI (11.0.08) - Russian Adobe Systems Incorporated 10.11.2014 187,00 MB 11.0.08

7-Zip 9.20

Microsoft Office Профессиональный плюс 2007

Профессиональные базы данных и информационные справочные системы:

1. Электронный каталог Фундаментальной библиотеки ТГУ. – URL: <http://biblio.tsutmb.ru/elektronnyj-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. Научная электронная библиотека Российской академии естествознания. – URL: <https://www.monographies.ru>
8. Президентская библиотека имени Б.Н. Ельцина. – URL: <https://www.prilib.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](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.