

**МИНОБРНАУКИ РОССИИ**

федеральное государственное бюджетное образовательное учреждение  
высшего образования

**«Кузбасский государственный технический университет имени Т. Ф. Горбачева»**  
Институт профессионального образования



**ПОДПИСАНО ЭП КУЗГТУ**

Подразделение: ректорат

Должность: проректор по среднему  
профессиональному образованию

Дата: 15.04.2022 05:51:54

**Попов Иван Павлович**

**Рабочая программа дисциплины**

**Организационно-правовое обеспечение информационной безопасности**

Специальность «10.02.05 Обеспечение информационной безопасности автоматизированных систем»

Присваиваемая квалификация  
"Техник по защите информации"

Формы обучения  
очная

Кемерово 2022 г.

Рабочую программу составил:

**ПОДПИСАНО ЭП КУЗГТУ**

Подразделение: учебно-методическое управление

Должность: начальник управления

Дата: 14.04.2022 03:56:50

**Прокопенко Евгения Викторовна**

Рабочая программа обсуждена на заседании кафедры информационной безопасности

Протокол № 3/1 от 15.04.2022

**ПОДПИСАНО ЭП КУЗГТУ**

Подразделение: учебно-методическое управление

Должность: начальник управления

Дата: 15.04.2022 03:31:33

**Прокопенко Евгения Викторовна**

Согласовано цикловой-методической комиссией по направлению подготовки (специальности)  
10.02.05 Обеспечение информационной безопасности автоматизированных систем

Протокол № 4/1 от 15.04.2022

**ПОДПИСАНО ЭП КУЗГТУ**

Подразделение: учебно-методическое управление

Должность: начальник управления

Дата: 15.04.2022 05:16:54

**Прокопенко Евгения Викторовна**

Согласовано заместителем директора по УР ИПО

**ПОДПИСАНО ЭП КУЗГТУ**

Подразделение: учебно-методическое управление

Должность: Заместитель директора по учебной работе

Дата: 15.04.2022 05:16:54

**Полуэктова Наталья Сергеевна**

Согласовано заместителем директора по МР ИПО

**ПОДПИСАНО ЭП КУЗГТУ**

Подразделение: учебно-методическое управление

Должность: Заместитель директора по методической работе

Дата: 15.04.2022 05:16:54

**Сьянова Татьяна Юрьевна**

## **1. Общая характеристика рабочей программы дисциплины**

### **1.1 Место дисциплины в структуре основной образовательной программы**

Учебная дисциплина «Организационно-правовое обеспечение информационной безопасности» является обязательной частью общепрофессионального цикла основной образовательной программы в соответствии с ФГОС по специальности 10.02.05 «Обеспечение информационной безопасности автоматизированных систем».

Учебная дисциплина «Организационно-правовое обеспечение информационной безопасности» обеспечивает формирование профессиональных и общих компетенций в соответствии с ФГОС по специальности 10.02.05 «Обеспечение информационной безопасности автоматизированных систем».

### **1.2 Цель и планируемые результаты освоения дисциплины, соотнесенные с планируемыми результатами освоения образовательной программы**

Освоение дисциплины направлено на формирование:  
общих компетенций:

ОК 01. Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам.

Знать: правовые основы организации защиты информации, содержащей сведения, составляющие государственную тайну и информации конфиденциального характера, задачи органов защиты государственной тайны; способы решения задач профессиональной деятельности, применительно к различным контекстам и сопутствующие нормативные документы в области обеспечения защиты информации ограниченного доступа; Способы решения задач профессиональной деятельности, применительно к различным контекстам.

Уметь: осуществлять организационное обеспечение информационной безопасности автоматизированных (информационных) систем в рамках должностных обязанностей техника по защите информации;

ОК 02. Осуществлять поиск, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности.

Знать: Способы организации поиск, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности, в том числе основные нормативные правовые акты в области информационной безопасности и защиты информации, а также нормативные методические документы Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю в данной области; правовое положение субъектов правоотношений в сфере профессиональной деятельности (включая предпринимательскую деятельность); способы поиска, анализа и интерпретации информации, необходимой для выполнения задач профессиональной деятельности, в том числе нормативных документов в области обеспечения защиты информации ограниченного доступа; Принципы и методы поиска, анализа и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности - организационное обеспечение информационной безопасности. Способы поиска, анализа и интерпретации информации, необходимой для выполнения задач профессиональной деятельности, в том числе законодательные и нормативные правовые акты, регламентирующие трудовые правоотношения.

Уметь: Осуществлять поиск, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности.

ОК 03. Планировать и реализовывать собственное профессиональное и личностное развитие.

Знать: Применение нормативных методических документы Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю в данной области; Способы самореализации и планирования собственного профессионального и личностного развитие. Способы самореализации и планирования собственного профессионального и личностного развитие. Использование в профессиональной деятельности нормативные документы в области обеспечения защиты информации ограниченного доступа; Способы планирования и реализации собственного профессионального и личностного развития; Способы собственного профессионального и личностного развития, использования в этом процессе законодательные и нормативные правовые акты, регламентирующие трудовые правоотношения.

Уметь: Планировать и реализовывать собственное профессиональное и личностное развитие.

ОК 04. Работать в коллективе и команде, эффективно взаимодействовать с коллегами, руководством, клиентами.

Знать: Принципы работы в коллективе и команде, эффективно взаимодействовать с коллегами, руководством, клиентами. Методики применения при работе в коллективе и команде, эффективно взаимодействовать с коллегами, руководством, клиентами основываясь на законодательных и нормативных правовых актах, регламентирующих трудовые правоотношения.

Уметь: Работать в коллективе и команде, эффективно взаимодействовать с коллегами, руководством, клиентами

ОК 06. Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных общечеловеческих ценностей, применять стандарты антикоррупционного поведения.

Знать: Способы использования и сферы действия нормативных методических документов Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю в данной области; Законодательные и нормативные правовые акты обеспечение информационной безопасности. Нормативные правовые акты и нормативные методические документы в области защиты информации; законодательные и нормативные правовые акты, регламентирующие трудовые правоотношения.

Уметь: применять нормативные правовые акты и нормативные методические документы в области защиты информации; Защищать свои права в соответствии с трудовым законодательством;

ОК 09. Использовать информационные технологии в профессиональной деятельности.

Знать: Информационные технологии в профессиональной деятельности, в том числе для правовое обеспечение информационной безопасности; Принципы использования информационных технологий в профессиональной деятельности для работы с нормативными документами в области обеспечения защиты информации ограниченного доступа; Способы работы с законодательными и нормативными правовыми актами, регламентирующие трудовые правоотношения с использованием информационных технологий в профессиональной деятельности.

Уметь: Использовать информационные технологии в профессиональной деятельности. профессиональных компетенций:

ПК 1.4. Осуществлять проверку технического состояния, техническое обслуживание и текущий ремонт, устранять отказы и восстанавливать работоспособность автоматизированных (информационных) систем в защищенном исполнении.

Знать: Основную документацию по регламентации мероприятий и оказанию услуг в области защиты информации; Уметь: Осуществлять проверку технического состояния, техническое обслуживание и текущий ремонт, устранять отказы и восстанавливать работоспособность автоматизированных (информационных) систем в защищенном исполнении; Оформлять документацию по регламентации мероприятий и оказанию услуг в области защиты информации; Иметь практический опыт: проверки технического состояния, техническое обслуживание и текущий ремонт, устранять отказы и восстанавливать работоспособность автоматизированных (информационных) систем в защищенном исполнении; Оформления документации по регламентации мероприятий и оказанию услуг в области защиты информации;

ПК 2.1. Осуществлять установку и настройку отдельных программных, программно-аппаратных средств защиты информации.

Знать: Организационное обеспечение информационной безопасности Уметь: Осуществлять установку и настройку отдельных программных, программно-аппаратных средств защиты информации. Иметь практический опыт: установки и настройки отдельных программных, программно-аппаратных средств защиты информации.

ПК 2.4. Осуществлять обработку, хранение и передачу информации ограниченного доступа. Знать: Документацию по правовому обеспечению информационной безопасности; Нормативные документы в области обеспечения защиты информации ограниченного доступа для обеспечения обработки, хранения и передачи информации ограниченного доступа; Нормативные методические документы, регламентирующие порядок выполнения мероприятий по защите информации, обрабатываемой в автоматизированной (информационной) системе; Уметь: Осуществлять обработку, хранение и передачу информации ограниченного доступа; Осуществлять обработку, хранение и передачу информации ограниченного доступа согласно нормативным документам в области обеспечения защиты информации ограниченного доступа; Осуществлять обработку, хранение и передачу информации ограниченного доступа; Иметь практический опыт: обработки, хранения и передачи информации ограниченного доступа; обработки, хранения и передачи информации ограниченного доступа согласно нормативным документам в области обеспечения защиты информации ограниченного доступа; обработки, хранения и передачи информации ограниченного доступа;

ПК 3.2. Осуществлять эксплуатацию технических средств защиты информации в соответствии с требованиями эксплуатационной документации. Знать: Нормативные документы в области обеспечения защиты информации ограниченного доступа для эксплуатации технических средств защиты информации в соответствии с требованиями эксплуатационной документации; Организацию ремонтного обслуживания аппаратуры и средств защиты информации; Уметь: Осуществлять эксплуатацию технических средств защиты информации в соответствии с требованиями эксплуатационной документации и нормативными документами в области обеспечения защиты информации ограниченного доступа; Осуществлять эксплуатацию технических средств защиты информации в соответствии с требованиями эксплуатационной документации. Иметь практический опыт: Эксплуатации технических средств защиты информации в соответствии с требованиями эксплуатационной документации и нормативными документами в области обеспечения защиты информации ограниченного доступа; эксплуатации технических средств защиты информации в соответствии с требованиями эксплуатационной документации.

ПК 3.5. Организовывать отдельные работы по физической защите объектов информатизации. Знать: Нормативные документы в области обеспечения защиты информации ограниченного доступа для организации работ по физической защите объектов информатизации. Принципы и методы организационной защиты информации, организационное обеспечение информационной безопасности в организации; Уметь: Организовывать отдельные работы по физической защите объектов информатизации на основе нормативных документов в области обеспечения защиты информации ограниченного доступа; контролировать соблюдение персоналом требований по защите информации при ее обработке с использованием средств вычислительной техники; Иметь практический опыт: Организации работ по физической защите объектов информатизации на основе нормативных документов в области обеспечения защиты информации ограниченного доступа; контролирования за соблюдением персоналом требований по защите информации при ее обработке с использованием средств вычислительной техники;

#### **В результате освоения дисциплины обучающийся в общем по дисциплине должен**

Знать:

- правовые основы организации защиты информации, содержащей сведения, составляющие государственную тайну и информации конфиденциального характера, задачи органов защиты государственной тайны; способы решения задач профессиональной деятельности, применительно к различным контекстам и сопутствующие нормативные документы в области обеспечения защиты информации ограниченного доступа; Способы решения задач профессиональной деятельности, применительно к различным контекстам.

- Способы организации поиска, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности, в том числе основные нормативные правовые акты в области информационной безопасности и защиты информации, а также нормативные методические документы Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю в данной области; правовое положение субъектов правоотношений в сфере профессиональной деятельности (включая предпринимательскую деятельность); способы поиска, анализа и интерпретации информации, необходимой для выполнения задач профессиональной деятельности, в том числе нормативных документов в области обеспечения защиты информации ограниченного доступа; Принципы и методы поиска, анализа и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности - организационное обеспечение информационной безопасности. Способы поиска, анализа и интерпретации информации,

необходимой для выполнения задач профессиональной деятельности, в том числе законодательные и нормативные правовые акты, регламентирующие трудовые правоотношения.

- Применение нормативных методических документов Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю в данной области; Способы самореализации и планирования собственного профессионального и личностного развития. Способы самореализации и планирования собственного профессионального и личностного развития. Использование в профессиональной деятельности нормативные документы в области обеспечения защиты информации ограниченного доступа; Способы планирования и реализации собственного профессионального и личностного развития; Способы собственного профессионального и личностного развития, использования в этом процессе законодательные и нормативные правовые акты, регламентирующие трудовые правоотношения.

- Принципы работы в коллективе и команде, эффективно взаимодействовать с коллегами, руководством, клиентами. Методики применения при работе в коллективе и команде, эффективно взаимодействовать с коллегами, руководством, клиентами основываясь на законодательных и нормативных правовых актах, регламентирующих трудовые правоотношения.

- Способы использования и сферы действия нормативных методических документов Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю в данной области; Законодательные и нормативные правовые акты обеспечение информационной безопасности. Нормативные правовые акты и нормативные методические документы в области защиты информации; законодательные и нормативные правовые акты, регламентирующие трудовые правоотношения.

- Информационные технологии в профессиональной деятельности, в том числе для правовое обеспечение информационной безопасности; Принципы использования информационных технологии в профессиональной деятельности для работы с нормативными документами в области обеспечения защиты информации ограниченного доступа; Способы работы с законодательными и нормативными правовыми актами, регламентирующие трудовые правоотношения с использованием информационных технологий в профессиональной деятельности.

- Основную документацию по регламентации мероприятий и оказанию услуг в области защиты информации;

- Организационное обеспечение информационной безопасности

- Документацию по правовому обеспечению информационной безопасности; Нормативные документы в области обеспечения защиты информации ограниченного доступа для обеспечения обработки, хранения и передачи информации ограниченного доступа; Нормативные методические документы, регламентирующие порядок выполнения мероприятий по защите информации, обрабатываемой в автоматизированной (информационной) системе;

- Нормативные документы в области обеспечения защиты информации ограниченного доступа для эксплуатации технических средств защиты информации в соответствии с требованиями эксплуатационной документации; Организацию ремонтного обслуживания аппаратуры и средств защиты информации;

- Нормативные документы в области обеспечения защиты информации ограниченного доступа для организации работ по физической защите объектов информатизации. Принципы и методы организационной защиты информации, организационное обеспечение информационной безопасности в организации;

- Уметь:

- осуществлять организационное обеспечение информационной безопасности автоматизированных (информационных) систем в рамках должностных обязанностей техника по защите информации;

- Осуществлять поиск, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности.

- Планировать и реализовывать собственное профессиональное и личностное развитие.

- Работать в коллективе и команде, эффективно взаимодействовать с коллегами, руководством, клиентами

- применять нормативные правовые акты и нормативные методические документы в области защиты информации; Защищать свои права в соответствии с трудовым законодательством;

- Использовать информационные технологии в профессиональной деятельности.

- Осуществлять проверку технического состояния, техническое обслуживание и текущий ремонт, устранять отказы и восстанавливать работоспособность автоматизированных (информационных) систем в защищенном исполнении; Оформлять документацию по регламентации мероприятий и оказанию

услуг в области защиты информации;

- Осуществлять установку и настройку отдельных программных, программно-аппаратных средств защиты информации.

- Осуществлять обработку, хранение и передачу информации ограниченного доступа; Осуществлять обработку, хранение и передачу информации ограниченного доступа согласно нормативным документам в области обеспечения защиты информации ограниченного доступа; Осуществлять обработку, хранение и передачу информации ограниченного доступа;

- Осуществлять эксплуатацию технических средств защиты информации в соответствии с требованиями эксплуатационной документации и нормативными документами в области обеспечения защиты информации ограниченного доступа; Осуществлять эксплуатацию технических средств защиты информации в соответствии с требованиями эксплуатационной документации.

- Организовывать отдельные работы по физической защите объектов информатизации на основе нормативных документов в области обеспечения защиты информации ограниченного доступа; контролировать соблюдение персоналом требований по защите информации при ее обработке с использованием средств вычислительной техники;

Иметь практический опыт:

- проверки технического состояния, техническое обслуживание и текущий ремонт, устранять отказы и восстанавливать работоспособность автоматизированных (информационных) систем в защищенном исполнении; Оформление документации по регламентации мероприятий и оказанию услуг в области защиты информации;

- установки и настройки отдельных программных, программно-аппаратных средств защиты информации.

- обработки, хранения и передачи информации ограниченного доступа; обработки, хранения и передачи информации ограниченного доступа согласно нормативным документам в области обеспечения защиты информации ограниченного доступа; обработки, хранения и передачи информации ограниченного доступа;

- Эксплуатации технических средств защиты информации в соответствии с требованиями эксплуатационной документации и нормативными документами в области обеспечения защиты информации ограниченного доступа; эксплуатации технических средств защиты информации в соответствии с требованиями эксплуатационной документации.

- Организации работ по физической защите объектов информатизации на основе нормативных документов в области обеспечения защиты информации ограниченного доступа; контролироля за соблюдением персоналом требований по защите информации при ее обработке с использованием средств вычислительной техники;

## 2. Структура и содержание дисциплины

### 2.1 Объем дисциплины и виды учебной работы

Форма обучения	Количество часов		
	ОФ	ЗФ	ОЗФ
<b>Курс 2 / Семестр 4</b>			
<b>Объем дисциплины</b>	104		
в том числе:			
<i>лекции, уроки</i>	40		
<i>лабораторные работы</i>			
<i>практические занятия</i>	40		
Консультации			
Самостоятельная работа	24		
Промежуточная аттестация			
Индивидуальное проектирование			
<b>Форма промежуточной аттестации</b>	дифференцированный зачет		

### 2.2 Тематический план и содержание дисциплины

Наименование разделов и тем	Содержание учебного материала и формы организации деятельности обучающихся	Объем в часах
<b>Раздел 1. Правовое обеспечение информационной безопасности</b>		
<b>Тема 1.1. Введение в правовое обеспечение информационной безопасности</b>		
<i>Лекции</i>		
	Лекция 1.1.1. Информационная безопасность государства. Нормативные правовые акты Российской Федерации в области информации, информационных технологий и защиты информации. Конституционные права граждан на информацию и возможности их ограничения	1
<b>Тема 1.2. Государственная система защиты информации в Российской Федерации, ее организационная структура и функции</b>		
<i>Лекции</i>		
	Лекция 1.2.1. Федеральная служба по техническому и экспортному контролю, ее задачи, полномочия и права в области защиты информации	1
<b>Тема 1.3. Информация как объект правового регулирования</b>		
<i>Лекции</i>		
	Лекция 1.3.1. Информация как объект правовых отношений. Субъекты и объекты правовых отношений в информационной сфере.	1
	Лекция 1.3.2. Виды информации по законодательству Российской Федерации.	1
	Лекция 1.3.3. Нормы законодательства Российской Федерации, определяющие защиту информации.	1
<i>Практические занятия</i>		
	Практическое занятие 1.3.1. Работа с нормативными документами	2
	Практическое занятие 1.3.2. Защита информации, содержащейся в информационных системах общего пользования	2
<b>Тема 1.4. Правовой режим защиты государственной тайны</b>		
<i>Лекции</i>		

Наименование разделов и тем	Содержание учебного материала и формы организации деятельности обучающихся	Объем в часах
	Лекция 1.4.1. Государственная тайна как особый вид защищаемой информации. Законодательство Российской Федерации в области защиты государственной тайны.	1
	Лекция 1.4.2. Основные понятия, используемые в Законе Российской Федерации «О государственной тайне», и их определения. Степени секретности сведений, составляющих государственную тайну. Отнесение сведений к государственной тайне. Засекречивание и рассекречивание.	1
	Лекция 1.4.3. Документирование сведений, составляющих государственную тайну. Реквизиты носителей сведений, составляющих государственную тайну.	1
	Лекция 1.4.4. Допуск к государственной тайне и доступ к сведениям, составляющим государственную тайну.	1
	Лекция 1.4.5. Органы защиты государственной тайны в Российской Федерации.	1
	Лекция 1.4.6. Ответственность за нарушения правового режима защиты государственной тайны	1
<b>Тема 1.5. Правовые режимы защиты конфиденциальной информации</b>		
<i>Лекции</i>		
	Лекция 1.5.1. Законодательство Российской Федерации в области защиты конфиденциальной информации. Виды конфиденциальной информации по законодательству Российской Федерации. Отнесение сведений к конфиденциальной информации.	1
	Лекция 1.5.2. Нормативно-правовое содержание Федерального закона «О персональных данных». Документирование сведений конфиденциального характера. Защита конфиденциальной информации. Ответственность за нарушение режима защиты конфиденциальной информации.	1
<i>Практические занятия</i>		
	Практическое занятие 1.5.1. Разработка базового блока документов для обеспечения информационной безопасности ИСПДн: Составление перечня ПДн	2
	Практическое занятие 1.5.2. Разработка базового блока документов для обеспечения информационной безопасности ИСПДн: Составление перечня защищаемых ресурсов ПДн	2
	Практическое занятие 1.5.3. Разработка базового блока документов для обеспечения информационной безопасности ИСПДн: Классификация ИСПДн.	2
Самостоятельная работа обучающихся		8
<b>Раздел 2. Лицензирование и сертификация в области защиты информации</b>		
<b>Тема 2.1. Лицензирование деятельности в области защиты информации</b>		

Наименование разделов и тем	Содержание учебного материала и формы организации деятельности обучающихся	Объем в часах
<i>Лекции</i>		
	Лекция 2.1.1. Основные понятия в области лицензирования и их определения. Нормативные правовые акты, регламентирующие лицензирование деятельности в области защиты информации. Виды деятельности в области защиты информации, подлежащие лицензированию. Участники лицензионных отношений в области защиты информации. Порядок получения лицензий на деятельность в области защиты информации.	3
<i>Практические занятия</i>		
	Практическое занятие 2.1.1. Подготовка документов к получению лицензии	8
<b>Тема 2.2. Сертификация и аттестация по требованиям безопасности информации</b>		
<i>Лекции</i>		
	Лекция 2.2.1. Аттестация объектов информатизации по требованиям безопасности информации. Основные понятия в области аттестации по требованиям безопасности информации и их определения. Системы сертификации средств защиты информации по требованиям безопасности информации	2
<i>Практические занятия</i>		
	Практическое занятие 2.2.1. Подготовки документов к сертификации	8
	Практическое занятие 2.2.2. Подготовка документов к аттестации объектов информатизации	8
<b>Раздел 3. Организационное обеспечение информационной безопасности</b>		
<b>Тема 3.1. Допуск лиц и сотрудников к сведениям, составляющим государственную тайну и конфиденциальную информацию</b>		
<i>Лекции</i>		
	Лекция 3.1.1. Особенности подбора персонала на должности, связанные с работой с конфиденциальной информацией. Должности, составляющие с точки зрения защиты информации «группы риска».	2
	Лекция 3.1.2. Понятие «допуск». Формы допусков, их назначение и классификация. Номенклатура должностей работников, подлежащих оформлению на допуск и порядок ее составления, утверждения.	2
	Лекция 3.1.3. Работа по обучению персонала, допускаемому к конфиденциальной информации	2
<b>Тема 3.2. Организация пропускного и внутриобъектового режимов</b>		
<i>Лекции</i>		

Наименование разделов и тем	Содержание учебного материала и формы организации деятельности обучающихся	Объем в часах
	Лекция 3.2.1. Понятие «охрана». Организация охраны территории, зданий, помещений и персонала. Цели и задачи охраны. Объекты охраны. Виды и способы охраны.	2
	Лекция 3.2.2. Понятие пропускного режима. Цели и задачи пропускного режима. Организация пропускного режима. Основные положения инструкции об организации пропускного режима и работе бюро пропусков. Понятие пропуска. Понятие внутриобъектового режима. Общие требования внутриобъектового режима	2
	Лекция 3.2.3. Требования к помещениям, в которых ведутся работы с конфиденциальной информацией, конфиденциальные переговоры.	2
<b>Тема 3.3. Организация ремонтного обслуживания аппаратуры и средств защиты</b>		
	Лекция 3.3.1. Изъятие компьютерной техники и носителей информации. Инструкция изъятия компьютерной техники.	2
	Лекция 3.3.2. Исследование компьютерной техники и носителей информации. Оформление результатов исследования	2
<b>Раздел 4. Основы трудового права</b>		
<b>Тема 4.1. Законодательные и нормативные правовые акты, регламентирующие трудовые правоотношения.</b>		
<i>Лекции</i>		
	Лекция 4.1.1. Законодательные и нормативные правовые акты, регламентирующие трудовые правоотношения.	2
	Лекция 4.1.2. Понятие, стороны и содержание трудового договора. Виды трудовых договоров. Заключение трудового договора.	2
	Лекция 4.1.3. Испытательный срок. Правовые гарантии в области оплаты труда.	2
<i>Практические занятия</i>		
	Практическое занятие 4.1.1. Составление трудового договора сотрудника службы информационной безопасности	6
Самостоятельная работа обучающихся		16
<b>Всего</b>		<b><u>104</u></b>

### **3 Материально-техническое и учебно-методическое обеспечение дисциплины (модуля)**

#### **3.1 Специальные помещения для реализации программы**

Для реализации программы учебной дисциплины должны быть предусмотрены следующие специальные помещения:

1. Специальное помещение № 1406 представляет собой учебную аудиторию для проведения занятий лекционного типа, занятий семинарского типа, групповых и индивидуальных консультаций,

текущего контроля и промежуточной аттестации.

Перечень основного оборудования:

Комплект мебели (столы и стулья). Проектор. Персональный компьютер.

Перечень программного обеспечения: Libre Office. Mozilla Firefox. Google Chrome. 7-zip .Microsoft Windows. ESET NOD32 Smart Security Business Edition. Kaspersky Endpoint Security. Браузер Спутник.

2. Специальное помещение № 1147 представляет собой помещение для групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации, а также помещения для самостоятельной работы, мастерские и лаборатории, оснащенные оборудованием, техническими средствами обучения и материалами, учитывающими требования международных, национальных и межгосударственных стандартов в области защиты информации.

Перечень основного оборудования:

Специализированная мебель (столы и стулья); Коммутаторы, Металлические рольставни с пружинным механизмом, белые 1650мм\*2270мм; Сейф металлический; Системные блоки ITS (i3-10100/H410M/8 Gb/SSD 240Gb/БП AA500W); Точка доступа D-link; Мониторы 23.6" AOC 24B1H VA 1920x1080 (16:9), 250кд/м2, 5мс, VGA, HDMI, черные; Системные блоки MasteroMiddleMC05, IntelCorei510400 2.9GHz, 8GbRAM, 240GbSSD, DOS, программно-аппаратный комплекс для обнаружения компьютерных атак VipNet, средство доверенной загрузки (СДЗ) Соболев

3. Помещение для самостоятельной работы обучающихся:

Специальное помещение № 1237 представляет собой помещения для самостоятельной работы, оснащенные компьютерной техникой с возможностью подключения к информационно-телекоммуникационной сети Интернет и обеспечением доступа в электронную информационно-образовательную среду образовательной организации:

Перечень основного оборудования:

Комплект мебели (столы и стулья). Персональные компьютеры. Коммутатор AlliedTelesynLayer 2 SmartSwitch,

Перечень программного обеспечения: LibreOffice. MozillaFirefox. Google Chrome. 7-zip .Microsoft Windows. ESET NOD32 Smart Security Business Edition. Kaspersky Endpoint Security. БраузерСпутник.

4. Помещение для самостоятельной работы обучающихся:

Специальное помещение № 1211 представляет собой помещения для самостоятельной работы, оснащенные компьютерной техникой с возможностью подключения к информационно-телекоммуникационной сети Интернет и обеспечением доступа в электронную информационно-образовательную среду образовательной организации:

Перечень основного оборудования:

Специализированная мебель (столы и стулья); компьютерная техника с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду КузГТУ, в том числе:

проектор, экран настенный моторизованный.

Перечень программного обеспечения: LibreOffice. Mozilla Firefox. Google Chrome. 7-zip .Microsoft Windows. ESET NOD32 Smart Security Business Edition. Kaspersky Endpoint Security. БраузерСпутник.

5. Специальное помещение №1134 представляет собой компьютерный класс оснащенный современной вычислительной техникой из расчета одно рабочее место на каждого обучающегося при проведении учебных занятий в данных классах:

Перечень основного оборудования:

Специализированная мебель (столы и стулья), лабораторное оборудование, персональные компьютеры

Перечень программного обеспечения: СПРУТ, Autodesk AutoCAD 2017, Autodesk

Inventor, СПРУТ-ТП, SprutCAD, Autodesk AutoCAD 2018, КОМПАС-3D, Microsoft Windows, SprutCAM,

СПРУТ-ОКП.

## **3.2 Информационное обеспечение реализации программы**

### **3.2.1 Основная литература**

1. Полякова, Т. А. Организационное и правовое обеспечение информационной безопасности.: учебник и практикум для СПО / Полякова Т. А., Стрельцов А. А., Чубукова С. Г., Ниесов В. А. ; Отв. ред. Полякова Т. А., Стрельцов А. А. - Москва : Юрайт, 2020. - 325 с. - ISBN 978-5-534-00843-2. - URL: <https://urait.ru/book/organizacionnoe-i-pravovoe-obespechenie-informacionnoy-bezopasnosti-451933> (дата

обращения: 26.09.2023). – Текст : электронный.

2. Белов, Е. Б. Организационно-правовое обеспечение информационной безопасности : учебник для студентов, обучающихся по специальности укрупненной группы специальностей среднего профессионального образования "Информационная безопасность" / Е. Б. Белов, В. Н. Пржегорлинский. – 2-е изд., испр. и доп. – Москва : Академия, 2020. – 333 с. – (Профессиональное образование). – URL: <https://academia-library.ru/catalogue/4831/473794/> (дата обращения: 26.09.2023). – Текст : электронный.

### **3.2.2 Дополнительная литература**

1. Организационное и правовое обеспечение информационной безопасности.: учебник и практикум для вузов / Под ред. Поляковой Т.А., Стрельцова А.А.. – Москва : Юрайт, 2021. – 325 с. – ISBN 978-5-534-03600-8. – URL: <https://urait.ru/book/organizacionnoe-i-pravovoe-obespechenie-informacionnoy-bezopasnosti-469235> (дата обращения: 26.09.2023). – Текст : электронный.

### **3.2.3 Методическая литература**

1. Организационно-правовое обеспечение информационной безопасности : методические материалы для обучающихся направления подготовки 10.02.05 "Обеспечение информационной безопасности автоматизированных систем" / Кузбасский государственный технический университет им. Т. Ф. Горбачева ; Кафедра информационной безопасности, составители: Е. В. Прокопенко, А. В. Медведев, А. Г. Киренберг. – Кемерово : КузГТУ, 2020. – 9 с. – URL: <http://library.kuzstu.ru/meto.php?n=9960> (дата обращения: 26.09.2023). – Текст : электронный.

### **3.2.4 Интернет ресурсы**

1. ЭИОС КузГТУ:

а) Электронная библиотека КузГТУ. – Текст: электронный // Научно-техническая библиотека Кузбасского государственного технического университета им. Т. Ф. Горбачева : сайт. – Кемерово, 2001 – . – URL: <https://elib.kuzstu.ru/> . – Текст: электронный.

б) Портал.КузГТУ : Автоматизированная Информационная Система (АИС) : [сайт] / Кузбасский государственный технический университет им. Т. Ф. Горбачева. – Кемерово : КузГТУ, [б. г.]. – URL: <https://portal.kuzstu.ru/>. – Режим доступа: для авториз. пользователей. – Текст: электронный.

с) Электронное обучение : [сайт] / Кузбасский государственный технический университет им. Т. Ф. Горбачева. – Кемерово : КузГТУ, [б. г.]. – URL: <https://el.kuzstu.ru/> . – Режим доступа: для авториз. пользователей КузГТУ. – Текст: электронный.

2. ФСТЭК России : Федеральная служба по техническому и экспортному контролю : официальный сайт / ФАУ «ГНИИИ ПТЗИ ФСТЭК России». – Москва, 2004 – . – URL: [www.fstec.ru](http://www.fstec.ru). – Текст: электронный.

3. SecurityLab.ru : информационный портал по безопасности : сайт. – Москва. – URL: <https://www.securitylab.ru/> . – Текст: электронный.

4. Департамент образования Вологодской области : официальный сайт. – Вологда. – URL: <http://depobr.gov35.ru/> . – Текст: электронный.

5. BIOMETRICS.RU : Российский биометрический портал : сайт. – Москва, 2000 – . – URL: [www.biometrics.ru](http://www.biometrics.ru) . – Текст: электронный.

6. InformationSecurity/Информационная безопасность : сайт. – Москва. – URL: <http://www.itsec.ru>. – Текст: электронный.

7. eLIBRARY.RU : научная электронная библиотека : сайт. – Москва, 2000 – . – URL: <https://elibrary.ru>. – Режим доступа: для зарегистрир. пользователей. – Текст: электронный.

8. Гарант. ру : информационно-правовой портал : сайт. – Москва, 1990 – . – URL: <https://www.garant.ru/> . – Текст: электронный.

9. КонсультантПлюс : компьютерная справочно-правовая система : сайт. – Москва, 1992 – . – URL: [www.consultant.ru](http://www.consultant.ru) . – Текст: электронный.

10. Единое окно доступа к образовательным ресурсам : информационная система : сайт / ФГАУ ГНИИ ИТТ «Информика» . – Москва, 2005 – . – URL: <http://window.edu.ru/> . – Текст: электронный.

11. Российское образование. Федеральный образовательный портал : сайт / ФГАОУ ДПО ЦРГОП и ИТ. – Москва, 2002 – . – URL: [www.edu.ru](http://www.edu.ru) . – Текст: электронный.

#### 4. Организация самостоятельной работы обучающихся

Самостоятельная работа обучающихся осуществляется в объеме, установленном в разделе 2 настоящей программы дисциплины (модуля).

Для самостоятельной работы обучающихся предусмотрены специальные помещения, оснащенные компьютерной техникой с возможностью подключения к информационно-телекоммуникационной сети "Интернет" с обеспечением доступа в электронную информационно-образовательную среду КузГТУ.

#### 5. Фонд оценочных средств для проведения текущего контроля, промежуточной аттестации обучающихся по дисциплине

##### 5.1 Паспорт фонда оценочных средств

Планируемые результаты обучения по дисциплине.

Дисциплина направлена на формирование следующих компетенций выпускника:

##### 5.1 Паспорт фонда оценочных средств

№	Наименование разделов дисциплины	Содержание (темы) раздела	Код компетенции	Знания, умения, практический опыт, необходимые для формирования соответствующей компетенции	Форма текущего контроля знаний, умений, практического опыта, необходимых для формирования соответствующей компетенции
1.	Раздел 1. Правовое обеспечение информационной безопасности	Тема 1.1. Основные правовые понятия. Источники права. Основы государственного устройства РФ. Введение в правовое обеспечение информационной безопасности Тема 1.2. Государственная система защиты информации в Российской Федерации, ее организационная структура и функции Тема 1.3. Информация как объект правового регулирования Тема 1.4. Правовой режим защиты государственной тайны Тема 1.5. Правовые режимы защиты конфиденциальной информации	ОК 02.	Знать: Способы организации поиска, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности, в том числе основные нормативные правовые акты в области информационной безопасности и защиты информации, а также нормативные методические документы Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю в данной области; Уметь: Осуществлять поиск, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности.	опрос обучающихся по контрольным вопросам, защита отчетов по практическим заданиям, тестирование
			ОК 03.	Знать: Применение нормативных методических документов Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю в данной области; Уметь: Планировать и реализовывать собственное профессиональное и личностное развитие.	
			ОК 06.	Знать: Способы использования и сферы действия нормативных методических документов Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю в данной области	
			ОК 01.	Знать: правовые основы организации защиты информации, содержащей сведения, составляющие государственную тайну и информации конфиденциального характера, задачи органов защиты государственной тайны;	
			ОК 02.	Знать: правовое положение субъектов правоотношений в сфере профессиональной деятельности (включая предпринимательскую деятельность);	
			ОК 03.	Знать: Способы самореализации и планирования собственного профессионального и личностного развития.	
			ОК 06.	Знать: Законодательные и нормативные правовые акты обеспечение информационной безопасности.	
			ОК 09.	Знать: Информационные технологии в профессиональной деятельности, в том числе для правовое обеспечение информационной безопасности; Уметь: Использовать информационные технологии в профессиональной деятельности.	
			ПК 2.4.	Знать: Документацию по правовому обеспечению информационной безопасности Уметь: Осуществлять обработку, хранение и передачу информации ограниченного доступа; Иметь практический опыт: обработки, хранения и передачи информации ограниченного доступа;	

2	Раздел 2. Лицензирование и сертификация в области защиты информации	Тема 2.1. Лицензирование деятельности в области защиты информации Тема 2.2. Сертификация и аттестация по требованиям безопасности информации	OK 01.	Знать: способы решения задач профессиональной деятельности, применительно к различным контекстам и отсутствующие нормативные документы в области обеспечения защиты информации ограниченного доступа;	опрос обучающихся по контрольным вопросам, защита отчетов по практическим заданиям, тестирование
			OK 02.	Знать: способы поиска, анализа и интерпретации информации, необходимой для выполнения задач профессиональной деятельности, в том числе нормативных документов в области обеспечения защиты информации ограниченного доступа;	
			OK 03.	Знать: Способы самореализации и планирования собственного профессионального и личностного развития. Использование в профессионально деятельности нормативные документы в области обеспечения защиты информации ограниченного доступа;	
			OK 09.	Знать: Принципы использования информационные технологии в профессиональной деятельности для работы с нормативными документами в области обеспечения защиты информации ограниченного доступа;	
			ПК 2.4.	Знать: Нормативные документы в области обеспечения защиты информации ограниченного доступа для обеспечения обработки, хранения и передачи информации ограниченного доступа; Уметь: Осуществлять обработку, хранение и передачу информации ограниченного доступа согласно нормативным документам в области обеспечения защиты информации ограниченного доступа; Иметь практический опыт: обработки, хранения и передачи информации ограниченного доступа согласно нормативным документам в области обеспечения защиты информации ограниченного доступа;	
			ПК 3.2.	Знать: Нормативные документы в области обеспечения защиты информации ограниченного доступа для эксплуатации технических средств защиты информации в соответствии с требованиями эксплуатационной документации; Уметь: Осуществлять эксплуатацию технических средств защиты информации в соответствии с требованиями эксплуатационной документации и нормативными документами в области обеспечения защиты информации ограниченного доступа; Иметь практический опыт: Эксплуатации технических средств защиты информации в соответствии с требованиями эксплуатационной документации и нормативными документами в области обеспечения защиты информации ограниченного доступа;	
			ПК 3.5	Знать: Нормативные документы в области обеспечения защиты информации ограниченного доступа для организации работ по физической защите объектов информатизации. Уметь: Организовывать отдельные работы по физической защите объектов информатизации на основе нормативных документов в области обеспечения защиты информации ограниченного доступа; Иметь практический опыт: Организации работ по физической защите объектов информатизации на основе нормативных документов в области обеспечения защиты информации ограниченного доступа;	
3	Раздел 3. Организационное обеспечение информационной безопасности	Тема 3.1. Допуск лиц и сотрудников к сведениям, составляющим государственную тайну и конфиденциальную информацию Тема 3.2. Организация пропускного и внутриобъектового режимов Тема 3.3. Организация ремонтного обслуживания аппаратуры и средств защиты	OK 01.	Знать: Способы решения задач профессиональной деятельности, применительно к различным контекстам. Уметь: осуществлять организационное обеспечение информационной безопасности автоматизированных (информационных) систем в рамках должностных обязанностей техника по защите информации;	опрос обучающихся по контрольным вопросам, тестирование
			OK 02.	Знать: Принципы и методы поиска, анализа и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности - организационное обеспечение информационной безопасности.	
			OK 03.	Знать: Способы планирования и реализации собственного профессионального и личностного развития;	
			OK 04.	Знать: Принципы работы в коллективе и команде, эффективно взаимодействовать с коллегами, руководством, клиентами. Уметь: Работать в коллективе и команде, эффективно взаимодействовать с коллегами, руководством, клиентами	
			OK 06.	Знать: Нормативные правовые акты и нормативные методические документы в области защиты информации; Уметь: применять нормативные правовые акты и нормативные методические документы в области защиты информации;	
			ПК 1.4.	Знать: Основную документацию по регламентации мероприятий и оказанию услуг в области защиты информации; Уметь: Осуществлять проверку технического состояния, техническое обслуживание и текущий ремонт, устранять отказы и восстанавливать работоспособность автоматизированных (информационных) систем в защищенном исполнении; Оформлять документацию по регламентации мероприятий и оказанию услуг в области защиты информации; Иметь практический опыт: проверки технического состояния, техническое обслуживание и текущий ремонт, устранять отказы и восстанавливать работоспособность автоматизированных (информационных) систем в защищенном исполнении; Оформления документации по регламентации мероприятий и оказанию услуг в области защиты информации;	
			ПК 2.1.	Знать: Организационное обеспечение информационной безопасности Уметь: Осуществлять установку и настройку отдельных программных, программно-аппаратных средств защиты информации. Иметь практический опыт: установки и настройки отдельных программных, программно-аппаратных средств защиты информации.	
			ПК 2.4.	Знать: Нормативные методические документы, регламентирующие порядок выполнения мероприятий по защите информации, обрабатываемой в автоматизированной (информационной) системе; Уметь: Осуществлять обработку, хранение и передачу информации ограниченного доступа; Иметь практический опыт: обработки, хранения и передачи информации ограниченного доступа;	
			ПК 3.2.	Знать: Организацию ремонтного обслуживания аппаратуры и средств защиты информации; Уметь: Осуществлять эксплуатацию технических средств защиты информации в соответствии с требованиями эксплуатационной документации. Иметь практический опыт: эксплуатации технических средств защиты информации в соответствии с требованиями эксплуатационной документации.	
			ПК 3.5.	Знать: Принципы и методы организационной защиты информации, организационное обеспечение информационной безопасности в организации; Уметь: контролировать соблюдение персоналом требований по защите информации при ее обработке с использованием средств вычислительной техники; Иметь практический опыт: контролировала за соблюдением персоналом требований по защите информации при ее обработке с использованием средств вычислительной техники;	

4	Раздел 4. Основы трудового права	Тема 4.1. Законодательные и нормативные правовые акты, регламентирующие трудовые правоотношения.	OK 02.	Знать: Способы поиска, анализа и интерпретации информации, необходимой для выполнения задач профессиональной деятельности, в том числе законодательные и нормативные правовые акты, регламентирующие трудовые правоотношения.	опрос обучающихся по контрольным вопросам, защита отчетов по практическим заданиям, тестирование
			OK 03.	Знать: Способы собственного профессионального и личного развития, использования в этом процессе законодательные и нормативные правовые акты, регламентирующие трудовые правоотношения.	
			OK 04.	Знать: Методики применения при работе в коллективе и команде, эффективно взаимодействовать с коллегами, руководством, клиентами основываясь на законодательных и нормативных правовых актах, регламентирующих трудовые правоотношения.	
			OK 06.	Знать: законодательные и нормативные правовые акты, регламентирующие трудовые правоотношения. Уметь: Защищать свои права в соответствии с трудовым законодательством;	
			OK 09.	Знать: Способы работы с законодательными и нормативными правовыми актами, регламентирующие трудовые правоотношения с использованием информационных технологий в профессиональной деятельности.	

## 5.2 Типовые контрольные задания или иные материалы

Текущий контроль успеваемости и аттестационные испытания обучающихся могут быть организованы с использованием ресурсов ЭИОС КузГТУ. Полный перечень оценочных материалов расположен в ЭИОС КузГТУ.: <https://el.kuzstu.ru/login/index.php>.

Текущий контроль успеваемости и аттестационные испытания могут проводиться в письменной и (или) устной, и (или) электронной форме.

### 5.2.1 Оценочные средства при текущем контроле

Текущий контроль по темам дисциплины заключается в опросе обучающихся по контрольным вопросам, защите отчетов по лабораторным и(или) практическим заданиям, тестировании.

#### **Опрос по контрольным вопросам:**

При проведении текущего контроля обучающимся будет письменно, либо устно задано два вопроса, на которые они должны дать ответы.

Например:

1. Общественные отношения в чем регулирует конституционное право?
2. Чем, с позиции конституционного права, обеспечивается единство общества?

Критерии оценивания:

- 90-100 баллов – при правильном и полном ответе на два вопроса;
- 80-89баллов – при правильном и полном ответе на один из вопросов и правильном, но не полном ответе на другой из вопросов;
- 60-79 баллов – при правильном и неполном ответе только на один из вопросов;
- 0-59 баллов – при отсутствии правильных ответов на вопросы.

Количество баллов	0-59	60-79	80-89	90-100
Шкала оценивания	неуд	удовл	хорошо	отлично

#### **Примерный перечень контрольных вопросов:**

**Введение. Основные правовые понятия. Источники права. Основы государственного устройства РФ.**

1. Общественные отношения в чем регулирует конституционное право?
2. Чем, с позиции конституционного права, обеспечивается единство общества?
3. Что представляют собой основы конституционного строя?
4. Что такое конституционное право?
5. В чем заключаются основные принципы правового государства?
6. Может ли в правовом государстве отдельная личность (ассоциации индивидов, народ) выступать в качестве объектов и субъектов власти одновременно?
7. Какие разделения государственной власти существуют в Российской Федерации?
8. В чем проявляется непосредственное действие прав и свобод?
9. По каким признакам, согласно Конституции Российской Федерации, запрещаются ограничения прав граждан?
10. Кто или какие структуры осуществляют государственную власть в Российской Федерации?

### **Раздел 1. Правовое обеспечение информационной безопасности**

### **Тема 1.1. Введение в правовое обеспечение информационной безопасности**

1. Что является основным нормативно-правовым документом, защищающим права, свободы и безопасность человека в системе информационных отношений, в РФ?
2. В каком нормативном документе представлены совокупность официальных взглядов на цели, задачи, принципы и основные направления обеспечения информационной безопасности РФ ?
3. В каком году произошло становление отечественного законодательства по информатизации?
4. Каким нормативным документом определены на международном уровне пределы вмешательства в частную жизнь со стороны государства и других субъектов ?
5. Какая часть Уголовного кодекса посвящается преступлениям в сфере компьютерной информации?

### **Тема 1.2. Государственная система защиты информации в Российской Федерации, ее организационная структура и функции**

1. Каким законом определяется система защиты государственных секретов?
2. Какая информация относится к государственной тайне?
3. Назовите Федеральный закон, который регулирует отношения, возникающие при обеспечении защиты информации?
4. Перечислите принципы, на которых основывается правовое регулирование отношений, возникающих в сфере информации, информационных технологий и защиты информации?
5. Какой коллегиальный орган осуществляет в соответствии с Указом Президента Российской Федерации № 212 от 19.02.99 г., межотраслевую координацию и функциональное регулирование деятельности по обеспечению защиты (не-криптографическими методами) информации, содержащей сведения, составляющие государственную и служебную тайну?

### **Тема 1.3. Информация как объект правового регулирования**

1. Укажите какие меры защиты информации используются в организациях?
2. Каким нормативным документом введена защита компьютерной информации?
3. Какая подсистема является частью системы обеспечения национальной безопасности страны, призванной к реализации государственной политики в информационной сфере?
4. Как называется требование не передавать определенную информацию третьим лицам без согласия ее обладателя?
5. Какие признаки не свойственны информации как объекту правоотношений?

### **Тема 1.4. Правовой режим защиты государственной тайны**

1. Какие сведения составляют Государственную тайну ?
2. Какие сведения, защищаемые государством не относятся к государственной тайне?
3. Какое ведомство рассматривает административные дела в сфере нарушений требований защиты информации, составляющей государственную тайну?
4. В отношении допуска к каким сведениям, составляющих государственную тайну, не проводятся проверочные мероприятия?
5. Какие принципы относятся к числу основных причисления информации к государственной тайне в соответствии с ФЗ «О государственной тайне» ?

### **Тема 1.5. Правовые режимы защиты конфиденциальной информации**

1. В отношении каких сведений не устанавливается режим защиты информации?
2. Что такое режим документированной информации?
3. Для какой информации или сведений устанавливается режим общественного достояния?
4. Какие виды тайн или сведений входят в правовой режим документированной информации?
5. Какие существуют режимы доступа к конфиденциальной информации?

## **Раздел 2. Лицензирование и сертификация в области защиты информации**

### **Тема 2.1. Лицензирование деятельности в области защиты информации**

1. Какие органы занимаются лицензированием в области защиты информации?
2. Какой орган занимается лицензированием деятельности в области защиты конфиденциальной информации?
3. Какие лицензии выдаются ФСТЭК России?
4. В каких случаях требуется лицензия ФСБ на деятельность по разработке / производству средств

- защиты конфиденциальной информации?
5. В каких случаях требуется переоформление лицензии ФСТЭК?

### **Тема 2.2. Сертификация и аттестация по требованиям безопасности информации**

1. Какой из действующих федеральных законов является базовым в области сертификации средств защиты информации?
2. Какой характер носит процесс проведения сертификации?
3. С какими органами, уполномоченными в сфере защиты информации должно согласовываться положение о сертификации в сфере защиты информации, составляющей государственную тайну?
4. На сколько этапов условно разбивается процедура аттестации объектов информатизации?
5. Кто утверждает паспорт на объект информатизации, прошедший аттестацию?

## **Раздел 3. Организационное обеспечение информационной безопасности**

### **Тема 3.1. Допуск лиц и сотрудников к сведениям, составляющим государственную тайну и конфиденциальную информацию**

1. Кто принимает решение о допуске гражданина к сведениям, составляющим государственную тайну?
2. Каким образом осуществляется замена формы допуска к сведениям, составляющим государственную тайну на более низкую?
3. Какой нормативный документ определяет правила и порядок допуска должностных лиц, граждан и организаций к государственной тайне?
4. Кто допускается к государственной тайне в особом порядке (без проведения проверочных мероприятий)?
5. Какие существуют и как называются формы допуска к государственной тайне должностных лиц и граждан в соответствии со степенями секретности сведений, составляющих государственную тайну?

### **Тема 3.2. Организация пропускного и внутриобъектового режимов**

1. В каких случаях работники охраны предприятия имеют право требовать от персонала и посетителей объектов охраны соблюдения внутриобъектового и пропускного режимов?
2. Какие задачи должен решать пропускной режим?
3. Чем должен обеспечиваться внутриобъектовый режим?
4. Кто утверждает пропускной и внутриобъектовый режим в учреждении?
5. Кто разрабатывает пропускной и внутриобъектовый режим в учебном учреждении?

### **Тема 3.3. Организация ремонтного обслуживания аппаратуры и средств защиты**

1. Какое лицо возглавляет службу ремонта на предприятии?
2. Какой ремонт выполняется при полной разборке оборудования?
3. Какие работники относятся к оперативному персоналу?
4. Что понимается под термином «кондуктивная электромагнитная помеха в системе энергоснабжения»?
5. Кто отвечает за правильную эксплуатацию и своевременный контроль за состоянием средств защиты, выданных в индивидуальное пользование?

## **Раздел 4. Основы трудового права**

### **Тема 4.1. Законодательные и нормативные правовые акты, регламентирующие трудовые правоотношения.**

1. В связи с заключением какого трудового документа регулирует отношения трудовое законодательство?
2. Какие нормативные акты являются источниками трудового права?
3. Как применяются и применяются ли вообще нормы вновь принятого федерального закона, содержащего нормы трудового права, если они противоречат ТК РФ?
4. Что не регулирует трудовое законодательство?
5. Что указано в Трудовом кодексе Российской Федерации?

### **Отчеты по лабораторным и (или) практическим заданиям(далее вместе - задания):**

По каждой работе обучающиеся самостоятельно оформляют отчеты в электронном формате  
Содержание отчета:

1. Тема работы.

2. Задачи задания.
3. Краткое описание хода выполнения.
4. Ответы на задания или полученные результаты по окончании выполнения работы (в зависимости от задач, поставленных в п. 2).
5. Выводы

Критерии оценивания:

- 60 - 100 баллов - при раскрытии всех разделов в полном объеме

- 0 - 59 баллов - при раскрытии не всех разделов, либо при оформлении разделов в неполном объеме.

Количество баллов	0-59	60-100
Шкала оценивания	Не зачтено	Зачтено

**Процедура защиты отчетов по заданиям:**

Оценочными средствами для текущего контроля по защите отчетов являются контрольные вопросы. Обучающимся будет устно задано два вопроса, на которые они должны дать ответы.

Например:

1. Как применяются и применяются ли вообще нормы вновь принятого федерального закона, содержащего нормы трудового права, если они противоречат ТК РФ?
2. Что не регулирует трудовое законодательство?

Критерии оценивания:

- 90-100 баллов - при правильном и полном ответе на два вопроса;

- 80-89 баллов - при правильном и полном ответе на один из вопросов и правильном, но не полном ответе на другой из вопросов;

- 60-79 баллов - при правильном и неполном ответе только на один из вопросов;

- 0-59 баллов - при отсутствии правильных ответов на вопросы.

Количество баллов	0-59	60-79	80-89	90-100
Шкала оценивания	неуд	удовл	хорошо	отлично

**Примерный перечень заданий:**

**1.Задание к практическому занятию 1.3.1. Работа с нормативными документами**

Задание 1. Используя «Руководство пользователя» (РК) по работе со справочной правовой системой «КонсультантПлюс», познакомиться со структурой интерфейса программы, процессами запуска системы, назначением вкладок.

Задание 2. Найти ФЗ-152.

Задание 3. Найти статьи УК РФ, относящиеся к правонарушениям в сфере информационных технологий.

Задание 4. Определите дату принятия Доктрины информационной безопасности РФ.

Задание 5. Найти информацию о наказании за разработку вредоносного программного обеспечения.

Задание 6. Найти последний законодательный акт, принятый в сфере информационной безопасности.

Задание 7. Найти статью «Правовая защита цифрового контента от пиратства в сети Интернет и ее влияние на развитие телевизионной и киноотрасли».

Задание 8. Провести сравнение редакций закона «О связи».

Задание 9. Найти форму приказа на увольнение.

Результаты зафиксировать в отчете.

**2. Задание к практическому занятию 1.3.2. Защита информации, содержащейся в информационных системах общего пользования**

Задание 1. Проведите анализ специальных понятий: «социальная информация», «документальная информация», «правовая информация», «научная информация» и приведите примеры информации, которая может быть отнесена к данным понятиям.

Задание 2. Определите, к какому виду информации в зависимости от порядка ее предоставления или распространения относится информация в конкретных ситуациях: а) юридическое лицо заключило с таможенным представителем договор представлять свои интересы при оформлении таможенной декларации и помещении товаров под определённую таможенную процедуру, при перемещении товаров через таможенную границу Таможенного союза, и предоставил ему информацию о себе, товаре

и его назначении;

б) государственный фонд данных государственного экологического мониторинга (государственного мониторинга окружающей среды) включает в себя:

1. информацию, содержащуюся в базах данных подсистем единой системы государственного экологического мониторинга (государственного мониторинга окружающей среды);
2. результаты производственного контроля в области охраны окружающей среды и государственного экологического надзора;
3. данные государственного учета объектов, оказывающих негативное воздействие на окружающую среду;

в) при принятии бюджета на 2017 год и плановый период на 2018–2019 годы Комитет Государственной Думы по бюджетному планированию рассмотрел источник доходов и размеры финансирования на обеспечения обороноспособности страны с подробным указанием всех статей расходов.

Задание 3. Доступ на территорию организации осуществляется через пост вневедомственной охраны с проходом через турникет и фиксацией времени входа-выхода сотрудников. Посетители проходят по пропускам при предъявлении документа, удостоверяющего личность. Однако это не регламентировано никаким документом, с которым под роспись ознакомлены ответственные должностные лица, а также не определены мероприятия по контролю соблюдения установленных требований. Как вы считаете, приняты ли все организационные меры, направленные на физическую защиту объекта в данной организации?

Задание 4. Разработать систему защиты информации в информационной системе на предприятии (выбор системы и предприятия произвольно), содержащую следующие основные пункты:

1. проблемная ситуация в сфере информационной безопасности;
2. механизмы обеспечения информационной безопасности предприятия;
3. мероприятия по реализации мер информационной безопасности предприятия;
4. программа создания системы информационной безопасности предприятия.

Задание 5. Проанализируйте Доктрину информационной безопасности Российской Федерации, утвержденной Президентом РФ от 5 декабря 2016 г. № 646 и определите основные направления обеспечения информационной безопасности в экономической сфере России.

Результаты зафиксировать в отчете.

**3 -4.Задание к практическому занятию 1.5.1. Разработка базового блока документов для обеспечения информационной безопасности ИСПДн: Составление перечня ПДн и Задание к практическому занятию 1.5.2. Разработка базового блока документов для обеспечения информационной безопасности ИСПДн: Составление перечня защищаемых ресурсов ПДн**

На основе исходных данных, предоставленных преподавателем, провести анализ ИСПДн и подготовить отчет о практической работе, содержащий: Перечень персональных данных, обрабатываемых в ИСПДн и подлежащих защите (для каждой ИСПДн).

Результаты зафиксировать в отчете.

**5. Задание к практическому занятию 1.5.3. Разработка базового блока документов для обеспечения информационной безопасности ИСПДн: Классификация ИСПДн.**

Задание 1. На основе исходных данных, предоставленных преподавателем, провести анализ ИСПДн и подготовить отчет о практической работе, содержащий: Перечень ИСПДн и их основные характеристики.

Результаты зафиксировать в отчете.

**6. Задание к практическому занятию 2.1.1. Подготовка документов к получению лицензии**

Задание 1. Используя справочно-правовые системы ознакомиться с нормативно-правовыми актами, регулирующими лицензирование отдельных видов предпринимательской деятельности.

Задание 2. Используя открытые источники, в том числе интернет-источники, выяснить расценки на лицензии конкретных видов деятельности.

Задание 3. Составить заявление о предоставлении лицензии на деятельность по технической защите конфиденциальной информации юридическому лицу.

Результаты зафиксировать в отчете.

**8. Задание к практическому занятию 2.2.2. Подготовка документов к аттестации объектов информатизации**

Задание 1. Приведите объекты информатизации, которые подлежат обязательной аттестации.

Задание 2. Опишите порядок проведения аттестации объектов информатизации по требованиям безопасности информации.

Задание 3. Приведите сведения, на основании которых разрабатывается программа аттестационных испытаний.

Задание 4. Перечислите сведения об объекте, представленные в техническом паспорте объекта информатизации.

Задание 5. Перечислите виды аттестации помещений по требованиям безопасности информации.

Задание 6. Ознакомьтесь с "Положением об аттестации объектов информатизации по требованиям безопасности". Составьте заявление на аттестацию объекта информатизации по требованиям безопасности.

Результаты зафиксировать в отчете.

**9. Задание к практическому занятию 4.1.1. Составление трудового договора сотрудника службы информационной безопасности**

Задание 1. Оформить документы о приеме на работу сотрудника службы информационной безопасности:

1. заявление о приеме на работу;
2. резюме работника;
3. приказ руководителя предприятия о приеме на работу; в тексте приказа обязательно должно быть указано несколько существенных условий договора. Как правило: дата начала работы, место работы, должность, размер оплаты труда, условия об испытательном сроке, режим работы.

Задание 2. Составить и оформить трудовой договор с сотрудником службы информационной безопасности в полном соответствии с законодательством РФ.

Результаты зафиксировать в отчете.

**Тестирование:**

Критерии оценивания при тестировании:

- 90-100 баллов - при правильном и полном ответе на 10 вопроса;
- 80...89 баллов - при правильном ответе на 8-9 вопросов;
- 60...79 баллов - при правильном ответе на 5-7 вопросов;
- 0...59 - при правильном ответе только на 4 вопроса;

Количество баллов	0-59	60-79	80-89	90-100
Шкала оценивания	неуд	удовл	хорошо	отлично

*Пример тестовых заданий:*

**Введение. Основные правовые понятия. Источники права. Основы государственного устройства РФ**

1. Конституционное право регулирует общественные отношения, складывающиеся:

1. исключительно в политической сфере жизни общества;
2. исключительно в экономической сфере жизни общества;
3. исключительно в социальной сфере жизни общества;
4. во всех без исключения сферах жизнедеятельности общества.

2. Чем, с позиции конституционного права, обеспечивается единство общества?

1. лежащими в его основе принципами, выражающими его качественную определенность, формы организации и функционирования;
2. механизмом, посредством которого осуществляется управление всеми сферами жизнедеятельности общества, сохраняется его целостность;
3. естественному стремлению людей к объединению;

3. Основы конституционного строя - это

1. определенный набор норм и правил функционирования общества и государства;
2. совокупность основополагающих общественных отношений, определяющих устройство государства, общества, закрепляющие их нормы в действующей Конституции России;
3. совокупность форм взаимодействия общества и государства;
4. нет верного варианта ответа.

4. . Конституционное право - это

1. отрасль права России, представляющая собой совокупность правовых норм, закрепляющих и регулирующих общественные отношения, через которые обеспечивается организационное и функциональное единство общества как целостной социальной системы;
2. отрасль права России, регулирующая общественные отношения в сфере управленческой деятельности органов и должностных лиц по исполнению публичных функций государства и муниципальных образований;
3. это отрасль права России, представляющая собой совокупность правовых норм, регулирующих общественные отношения в сфере налогообложения;
4. отрасль права России, объединяющая правовые нормы, регулирующие имущественные, а также связанные и несвязанные с ними личные неимущественные отношения, которые основаны на независимости имущественной самостоятельности и юридическом равенстве сторон в целях создания наиболее благоприятных условий для удовлетворения частных потребностей, а также норм развития экономических отношений.

5. Основные принципы правового государства:

1. легитимность публичной власти, разделение властей;
2. взаимная ответственность государства и личности;
3. тенденция сближения права и морали;

6. Может ли в правовом государстве отдельная личность (ассоциации индивидов, народ) выступать в качестве объектов и субъектов власти одновременно?

1. да, могут выступать;
2. нет, они выступают только в качестве объектов власти;
3. нет, они выступают только в качестве субъектов власти;
4. они не являются ни субъектами, ни объектами власти.

7. В Российской Федерации предусмотрено следующее разделение государственной власти:

1. на федеральную, региональную и местную;
2. на законотворческую, инициативную и контрольную;
3. на судебную, исполнительную, законодательную;
4. нет верного варианта ответа.

8. В чем проявляется непосредственное действие прав и свобод?

1. они подлежат обеспечению правосудием (пользуются напрямую судебной защитой);
2. возможно принятие нормативных решений, при которых незначительная часть прав и свобод человека и гражданина находится вне правовой защиты;
3. исключается возможность нормативных решений, при которых права и свободы, хотя бы только в определенной части, оказывались вне правовой защиты;

9. По каким признакам, согласно Конституции Российской Федерации, запрещаются ограничения прав граждан?

1. социальной и расовой принадлежности;
2. национальной и языковой принадлежности;
3. религиозной принадлежности;
4. по всем перечисленным признакам.

10. Государственную власть в Российской Федерации осуществляют:

1. Президент Российской Федерации;
2. Федеральное Собрание (Совет Федерации и Государственная Дума);

3. Правительство Российской Федерации;
4. суды Российской Федерации;
5. все варианты ответов верны.

### **Раздел 1. Правовое обеспечение информационной безопасности**

#### **Тема 1.1. Введение в правовое обеспечение информационной безопасности**

1. Основным нормативно-правовым документом, защищающим права, свободы и безопасность человека в системе информационных отношений, в РФ является:

1. Стратегия национальной безопасности РФ до 2020 года
2. ФЗ "О государственной тайне"
3. Конституция
4. Уголовный кодекс
5. Доктрина информационной безопасности РФ

2. Совокупность официальных взглядов на цели, задачи, принципы и основные направления обеспечения информационной безопасности РФ представлены

1. в Доктрине информационной безопасности РФ
2. в Концепции национальной безопасности РФ
3. в Конституции РФ
4. в Билле о надзоре за данными
5. в ФЗ РФ "Об информации, информационных технологиях и о защите информации"

3. Становление отечественного законодательства по информатизации произошло

1. в конце 60-х гг
2. в конце 70-х гг
3. в конце 80-х гг
4. в начале 90-х гг
5. в начале 70-х гг

4. На международном уровне пределы вмешательства в частную жизнь со стороны государства и других субъектов определены

1. Законом о тайне частной информации
2. Стандартом ISO 15408
3. Оранжевой книгой
4. Декларацией прав человека
5. Биллем о надзоре за данными

5. Преступлениям в сфере компьютерной информации в Уголовном кодексе посвящается

1. глава
2. раздел
3. статья
4. пункт
5. часть

#### **Тема 1.2. Государственная система защиты информации в Российской Федерации, ее организационная структура и функции**

1. Система защиты государственных секретов определяется Законом

1. "Об информации, информатизации и защите информации"
2. "Об органах ФСБ"
3. "О государственной тайне"
4. "О безопасности"

2. К государственной тайне относится...

1. информация в военной области
2. информация о внешнеполитической и внешнеэкономической деятельности государства
3. информация в области экономики, науки и техники и сведения в области разведывательной и

оперативно-розыскной деятельности

4. все выше перечисленное

3. Назовите Федеральный закон, который регулирует отношения, возникающие при обеспечении защиты информации?

1. Федеральный закон Российской Федерации от 27 июля 2006 г. N 149-ФЗ Об информации, информационных технологиях и о защите информации.
2. Федеральный закон Российской Федерации от 27 июля 2006 г. N 152-ФЗ О персональных данных.
3. ДОКТРИНА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ РОССИЙСКОЙ ФЕДЕРАЦИИ от 9 сентября 2000 г. N Пр-1895

4. Перечислите принципы, на которых основывается правовое регулирование отношений, возникающих в сфере информации, информационных технологий и защиты информации?

1. свобода поиска, получения, передачи, производства и распространения информации любым законным способом;
2. установление ограничений доступа к информации только федеральными законами;
3. открытость информации о деятельности государственных органов и органов местного самоуправления и свободный доступ к такой информации, кроме случаев, установленных федеральными законами;
4. равноправие языков народов Российской Федерации при создании информационных систем и их эксплуатации;
5. обеспечение безопасности Российской Федерации при создании информационных систем, их эксплуатации и защите содержащейся в них информации;
6. достоверность информации и своевременность ее предоставления;
7. неприкосновенность частной жизни, недопустимость сбора, хранения, использования и распространения информации о частной жизни лица без его согласия;
8. недопустимость установления нормативными правовыми актами каких-либо преимуществ применения одних информационных технологий перед другими

5. Выберите правильный ответ. В соответствии с Указом Президента Российской Федерации № 212 от 19.02.99 г., межотраслевую координацию и функциональное регулирование деятельности по обеспечению защиты (некриптографическими методами) информации, содержащей сведения, составляющие государственную и служебную тайну, осуществляет коллегиальный орган:

1. ФАПСИ
2. ФСБ
3. Гостехкомиссия
4. Главная научно-исследовательская организация по защите информации

### **Тема 1.3. Информация как объект правового регулирования**

1. Укажите какие меры защиты информации используются в организациях: выбрать все верные

1. государственные
2. нормативные
3. технические
4. правовые
5. организационные
6. коммерческие

2. Защита компьютерной информации введена...

1. Семейным кодексом РФ
2. Конституцией РФ
3. Гражданским кодексом РФ
4. Уголовным кодексом РФ

3. Частью системы обеспечения национальной безопасности страны, призванной к реализации государственной политики в информационной сфере является система...

1. Государственных органов
2. Обеспечения информационной безопасности

3. Обеспечения экологической безопасности
4. Оборона страны

4. Требование не передавать определенную информацию третьим лицам без согласия ее обладателя называется...

1. Сбережением информации
2. Запретом информации
3. Конфиденциальностью информации
4. Защитой информации

5. Информации как объекту правоотношений не свойственны следующие признаки:

1. количественная неопределенность;
2. физический износ;
3. секретные сведения

#### **Тема 1.4. Правовой режим защиты государственной тайны**

1. Государственную тайну составляют сведения...

1. В области учета населения
2. В области здравоохранения
3. В военной области
4. В области образования

2. К государственной тайне не относятся сведения, защищаемые государством ...

1. распространение которых может нанести ущерб государству;
2. в экономической области;
3. в контрразведывательной деятельности;
4. в оперативно-розыскной деятельности;
5. о частной жизни политических деятелей.

3. Административные дела в сфере нарушений требований защиты информации, составляющей государственную тайну, рассматривает:

1. Федеральная служба безопасности;
2. Полиция
3. Следственный комитет РФ
4. Межведомственная комиссия по защите государственной тайны

4. В отношении допуска к каким сведениям, составляющих государственную тайну, не проводятся проверочные мероприятия:

1. секретных сведений;
2. коммерческих сведений
3. публичных сведений
4. личных сведений
5. служебных сведений

5. В соответствии с ФЗ «О государственной тайне» к числу основных принципов отнесения информации к государственной тайне относятся...

1. Законность, демократизм и гуманизм
2. Законность, формализм и объективизм
3. Законность, демократизм и объективизм
4. Законность, обоснованность и своевременность

#### **Тема 1.5. Правовые режимы защиты конфиденциальной информации**

1. Режим защиты информации не устанавливается в отношении сведений, относящихся к ...

1. государственной тайне
2. деятельности государственных деятелей
3. конфиденциальной информации

4. персональным данным

2. Режим документированной информации - это ...

1. выделенная информация по определенной цели
2. электронный документ с электронно-цифровой подписью
3. выделенная информация в любой знаковой форме
4. электронная информация, позволяющая ее идентифицировать

3. Режим общественного достояния устанавливается для ...

1. любой общедоступной информации
2. сведений, которые являются уникальными, незаменимыми по своей природе
3. любой общественной организации
4. для государственных органов и муниципальных образований

4. В правовой режим документированной информации входит ...

1. государственная тайна
2. тайна частной жизни
3. банковская тайна
4. электронная цифровая подпись
5. персональные данные

5. Какие режимы доступа к конфиденциальной информации существуют: (выбрать все верные)

1. общественного достояния
2. исключительных прав
3. массовой информации
4. конфиденциальной информации
5. свободного доступа
6. неограниченного доступа

**Раздел 2. Лицензирование и сертификация в области защиты информации**

**Тема 2.1. Лицензирование деятельности в области защиты информации**

1. Какие органы занимаются лицензированием в области защиты информации?

1. Роскомнадзор
2. МВД
3. ФАПСИ
4. Гостехкомиссия РФ

2. Какой орган занимается лицензированием деятельности в области защиты конфиденциальной информации?

1. Роскомнадзор
2. МВД
3. ФАПСИ
4. Гостехкомиссия РФ

3. Какие лицензии выдаются ФСТЭК России? (выбрать все верные)

1. на деятельность в области разработки и производства средств защиты конфиденциальной информации;
2. на деятельность в области технической защиты конфиденциальной информации
3. на деятельность в области программной защиты конфиденциальной информации
4. на деятельность в области антивирусной защиты информации

4. В каких случаях требуется лицензия ФСБ на деятельность по разработке / производству средств защиты конфиденциальной информации? (выбрать все верные)

1. если средства защиты будут разрабатываться для эксплуатации в Администрации президента РФ
2. если средства защиты будут разрабатываться для эксплуатации в Совбез РФ
3. если средства защиты будут разрабатываться для эксплуатации в правительстве РФ

4. если средства защиты будут разрабатываться для эксплуатации в Верховном и Высшем арбитражном судах РФ
5. если средства защиты будут разрабатываться для эксплуатации в ФСБ РФ
6. если средства защиты будут разрабатываться для эксплуатации в банковской сфере
7. если средства защиты будут разрабатываться для эксплуатации в военной сфере

5. В каких случаях требуется переоформление лицензии ФСТЭК?

1. если внесены изменения в уставную документацию организации, занимающейся производством средств защиты информации
2. если нужно расширить внесенный в лицензию перечень выполняемых работ
3. если в силу научно-технического прогресса появились новые технологии и методы защиты информации
4. если существующие или подобные средства защиты, произведенные организацией дали сбой и не смогли обеспечить информационную безопасность на объекте

### **Тема 2.2. Сертификация и аттестация по требованиям безопасности информации**

1. Какой из действующих федеральных законов является базовым в области сертификации средств защиты информации?

1. федеральный закон о сертификации
2. федеральный закон о техническом регулировании
3. федеральный закон о персональных данных

2. Какой характер носит процесс проведения сертификации?

1. принудительный
2. добровольный
3. обязательный

3. С какими органами, уполномоченными в сфере защиты информации должно согласовываться положение о сертификации в сфере защиты информации, составляющей государственную тайну?

1. с органами ФСБ
2. с органами ФСТЭК
3. с межведомственной комиссией по защите государственной тайны

4. На сколько этапов условно разбивается процедура аттестации объектов информатизации?

1. на 2
2. на 3
3. на 4

5. Кто утверждает паспорт на объект информатизации, прошедший аттестацию?

1. председатель аттестационной комиссии
2. руководитель организации
3. руководитель органа по сертификации

### **Раздел 3. Организационное обеспечение информационной безопасности**

**Тема 3.1. Допуск лиц и сотрудников к сведениям, составляющим государственную тайну и конфиденциальную информацию**

1. Кто принимает решение о допуске гражданина к сведениям, составляющим государственную тайну?

1. руководитель территориальных органов исполнительной власти, наделенных полномочиями по защите государственной тайны
2. руководитель предприятия, на котором работает гражданин
3. руководитель органа ФСБ, проводившего проверочные мероприятия

2. Каким образом осуществляется замена формы допуска к сведениям, составляющим государственную тайну на более низкую?

1. решением межведомственной комиссии по защите государственной тайны

2. решением руководителя предприятия
3. решением руководителя органа ФСБ

3. Правила и порядок допуска должностных лиц, граждан и организаций к государственной тайне определяет...

1. Федеральный Закон «О государственной тайне»
2. Семейный кодекс Российской Федерации
3. Федеральный Закон «О валютном регулировании и валютном контроле»
4. Федеральный Закон «О банках и банковской деятельности»

4. В особом порядке (без проведения проверочных мероприятий) допускаются к государственной тайне ... (выбрать все верные)

1. члены Совета Федерации, депутаты Государственной Думы, судьи,
2. адвокаты, участвующие в судебном процессе, связанном с государственной тайной
3. Президент РФ
4. послы России за рубежом
5. Председатель и члены Правительства РФ

5. Формами допуска к государственной тайне должностных лиц и граждан соответствующими степеням секретности сведений, составляющих государственную тайну, называются...

1. большой секретности, малой секретности, особо важным
2. средней важности, профессиональной секретности, небольшой секретности
3. особой важности, совершенно секретным, секретным

### **Тема 3.2. Организация пропускного и внутриобъектового режимов**

1. Работники охраны предприятия имеют право требовать от персонала и посетителей объектов охраны соблюдения внутриобъектового и пропускного режимов:

1. При обеспечении внутриобъектового и пропускного режимов, а также при транспортировке охраняемых грузов, денежных средств и иного имущества в пределах объекта охраны
2. При осуществлении обязанностей по защите жизни и здоровья граждан
3. При обеспечении любых охранных мероприятий, предусмотренных законодательством

2. Пропускной режим должен обеспечивать решение следующих задач: (выбрать все верные)

1. предотвращение несанкционированного доступа в контролируемую зону посторонних лиц и транспортных средств;
2. установление порядка доступа работников (транспортных средств) предприятия в контролируемую зону, а также порядок доступа посетителей и транспорта сторонних организаций;
3. строгое ограничение доступа сотрудников предприятия к обслуживаемым объектам;
4. предотвращение незаконного выноса (вывоза) с территории предприятия материальных ценностей, а также вноса (ввоза) на территорию предприятия оружия, взрывчатых и других предметов и веществ, которые могут быть использованы для совершения теракта.
5. контроль за соблюдением рабочего времени сотрудников предприятия

3. Внутриобъектовый режим должен обеспечиваться: (выбрать все верные)

1. установлением регламента работы и взаимодействием производственных участков, цехов, складов и др. объектов с подразделением охраны на предмет принятия объектов под охрану и контроля состояния пожарной безопасности перед закрытием;
2. внедрением автоматических контрольно-пропускных установок (кабин), обеспечивающих контроль времени прохода через КПП, а также введение системы увольнительных записок, для лиц, выходящих из предприятия в течении рабочего дня;
3. оборудованием служебных помещений, предназначенных для хранения документов изделий, доступ к которым ограничен, кодовыми замками и охранной сигнализацией;
4. осуществлением патрулирования нарядами охраны территории предприятия в т.ч. и мест хранения материальных ценностей на предмет выявления и задержания посторонних лиц и пресечения хищения материальных ценностей;
5. установлением маршрутов и правил движения транспортных средств и пешеходов по территории предприятия; ограждение, обозначение и освещение мест, опасных для жизни и здоровья персонала

и посетителей.

- установкой камер видеонаблюдения территории как внутри периметра предприятия, так и внешней прилегающей территории

4. Кто утверждает пропускной и внутриобъектовый режим в учреждении:

- представитель ФСБ
- представитель МВД
- директор учреждения

5. Кто разрабатывает пропускной и внутриобъектовый режим в учебном учреждении:

- директор учреждения
- зам директора по АХЧ
- преподаватель по ОБЖ

### **Тема 3.3. Организация ремонтного обслуживания аппаратуры и средств защиты**

1. Какое лицо возглавляет службу ремонта на предприятии?

- Главный технолог
- Главный механик
- Главный метролог
- специалист по ИБ

2. Какой ремонт выполняется при полной разборке оборудования?

- Текущий
- Средний
- Капитальный

3. Какие работники относятся к оперативному персоналу?

- Работники, специально обученные и подготовленные для оперативного обслуживания в утвержденном объеме закрепленных за ним оборудования
- Работники, выполняющие техническое обслуживание и ремонт, монтаж, наладку и испытание оборудования
- Работники, на которых возложены обязанности по организации технического и оперативного обслуживания, проведения ремонтных, монтажных и наладочных работ с оборудованием
- нет верного ответа

4. Что понимается под термином «кондуктивная электромагнитная помеха в системе энергоснабжения»?

- Электромагнитная помеха, распространяющаяся по элементам электрической сети от потребителей электроэнергии
- Электромагнитная помеха, распространяющаяся по элементам электрической сети
- Электромагнитная помеха, распространяющаяся по элементам электрической сети от источника энергоснабжения
- Электромагнитная помеха, распространяющаяся по элементам электрической сети при повреждениях в ней

5. Кто отвечает за правильную эксплуатацию и своевременный контроль за состоянием средств защиты, выданных в индивидуальное пользование?

- Работник, получивший эти средства защиты в индивидуальное пользование
- Работник, выдающий эти средства защиты в индивидуальное пользование
- Непосредственный руководитель работника, получившего эти средства защиты в индивидуальное пользование
- Специалист по охране труда организации

## **Раздел 4. Основы трудового права**

### **Тема 4.1. Законодательные и нормативные правовые акты, регламентирующие трудовые правоотношения.**

1. Трудовое законодательство регулирует отношения:

1. в связи с заключением трудового контракта;
2. в связи с заключением трудового соглашения;
3. в связи с заключением трудового договора.

2. Какие из перечисленных нормативных актов являются источниками трудового права:

1. Конституция РФ;
2. Приказы Федеральной налоговой службы;
3. Трудовой кодекс РФ

3. Если нормы вновь принятого федерального закона, содержащего нормы трудового права, противоречат ТК РФ, то они:

1. применяются только при условии внесения соответствующих изменений и дополнений в ТК РФ;
2. не применяются;
3. применяются независимо от внесения соответствующих изменений и дополнений.

4. Трудовое законодательство не регулирует:

1. отношения по занятости и трудоустройству;
2. отношения по организации труда и управлению трудом;
3. материальную ответственность работодателей и работников в сфере труда.

5. В Трудовом кодексе Российской Федерации:

1. указаны все принципы трудового права;
2. перечислены некоторые принципы трудового права;
3. принципы трудового права не указаны, поскольку это догматическая категория права.

### 5.2.2 Оценочные средства при промежуточной аттестации

**Формой промежуточной аттестации в четвертом семестре** является дифференцированный зачет, в процессе которого определяется сформированность обозначенных в рабочей программе компетенций.

Инструментом измерения сформированности компетенций являются:

- зачетные отчеты по заданиям,
- ответы на вопросы во время опроса,
- зачетное компьютерное тестирование.

При проведении промежуточного контроля обучающийся отвечает на 10 тестовых заданий, либо отвечает на 2 вопроса выбранных случайным образом, формирующихся случайным образом.

Промежуточная аттестация может проводиться в письменной и (или) устной, и (или) электронной форме. Банк вопросов на тестирование находится в ЭИОС КузГТУ "Moodle".

Критерии оценивания при тестировании:

- 90-100 баллов - при правильном и полном ответе на 10 вопроса;
- 80...89 баллов - при правильном ответе на 8-9 вопросов;
- 60...79 баллов - при правильном ответе на 5-7 вопросов;
- 0...59 - при правильном ответе только на 4 вопроса;

Количество баллов	0-59	60-79	80-89	90-100
Шкала оценивания	неуд	удовл	хорошо	отлично

Пример вариантов тестовых заданий:

#### Вариант 1.

1. Основным нормативно-правовым документом, защищающим права, свободы и безопасность человека в системе информационных отношений, в РФ является:

1. Стратегия национальной безопасности РФ до 2020 года
2. ФЗ "О государственной тайне"
3. Конституция

4. Уголовный кодекс
5. Доктрина информационной безопасности РФ

2. Совокупность официальных взглядов на цели, задачи, принципы и основные направления обеспечения информационной безопасности РФ представлены

1. в Доктрине информационной безопасности РФ
2. в Концепции национальной безопасности РФ
3. в Конституции РФ
4. в Билле о надзоре за данными
5. в ФЗ РФ "Об информации, информационных технологиях и о защите информации"

3. Становление отечественного законодательства по информатизации произошло

1. в конце 60-х гг
2. в конце 70-х гг
3. в конце 80-х гг
4. в начале 90-х гг
5. в начале 70-х гг

4. На международном уровне пределы вмешательства в частную жизнь со стороны государства и других субъектов определены

1. Законом о тайне частной информации
2. Стандартом ISO 15408
3. Оранжевой книгой
4. Декларацией прав человека
5. Биллем о надзоре за данными

5. Преступлениям в сфере компьютерной информации в Уголовном кодексе посвящается

1. глава
2. раздел
3. статья
4. пункт
5. часть

6. Какое лицо возглавляет службу ремонта на предприятии?

1. Главный технолог
2. Главный механик
3. Главный метролог
4. специалист по ИБ

7. Какой ремонт выполняется при полной разборке оборудования?

1. Текущий
2. Средний
3. Капитальный

8. Какие работники относятся к оперативному персоналу?

1. Работники, специально обученные и подготовленные для оперативного обслуживания в утвержденном объеме закрепленных за ним оборудования
2. Работники, выполняющие техническое обслуживание и ремонт, монтаж, наладку и испытание оборудования
3. Работники, на которых возложены обязанности по организации технического и оперативного обслуживания, проведения ремонтных, монтажных и наладочных работ с оборудованием
4. нет верного ответа

9. Что понимается под термином «кондуктивная электромагнитная помеха в системе энергоснабжения»?

1. Электромагнитная помеха, распространяющаяся по элементам электрической сети от потребителей

- электроэнергии
- 2. Электромагнитная помеха, распространяющаяся по элементам электрической сети
- 3. Электромагнитная помеха, распространяющаяся по элементам электрической сети от источника энергоснабжения
- 4. Электромагнитная помеха, распространяющаяся по элементам электрической сети при повреждениях в ней

10. Кто отвечает за правильную эксплуатацию и своевременный контроль за состоянием средств защиты, выданных в индивидуальное пользование?

- 1. Работник, получивший эти средства защиты в индивидуальное пользование
- 2. Работник, выдающий эти средства защиты в индивидуальное пользование
- 3. Непосредственный руководитель работника, получившего эти средства защиты в индивидуальное пользование
- 4. Специалист по охране труда организации

#### **Вариант 2.**

1. Какие органы занимаются лицензированием в области защиты информации?

- 1. Роскомнадзор
- 2. МВД
- 3. ФАПСИ
- 4. Гостехкомиссия РФ

2. Какой орган занимается лицензированием деятельности в области защиты конфиденциальной информации?

- 1. Роскомнадзор
- 2. МВД
- 3. ФАПСИ
- 4. Гостехкомиссия РФ

3. Какие лицензии выдаются ФСТЭК России? (выбрать все верные)

- 1. на деятельность в области разработки и производства средств защиты конфиденциальной информации;
- 2. на деятельность в области технической защиты конфиденциальной информации
- 3. на деятельность в области программной защиты конфиденциальной информации
- 4. на деятельность в области антивирусной защиты информации

4. В каких случаях требуется лицензия ФСБ на деятельность по разработке / производству средств защиты конфиденциальной информации? (выбрать все верные)

- 1. если средства защиты будут разрабатываться для эксплуатации в Администрации президента РФ
- 2. если средства защиты будут разрабатываться для эксплуатации в Совбез РФ
- 3. если средства защиты будут разрабатываться для эксплуатации в правительстве РФ
- 4. если средства защиты будут разрабатываться для эксплуатации в Верховном и Высшем арбитражном судах РФ
- 5. если средства защиты будут разрабатываться для эксплуатации в ФСБ РФ
- 6. если средства защиты будут разрабатываться для эксплуатации в банковской сфере
- 7. если средства защиты будут разрабатываться для эксплуатации в военной сфере

5. В каких случаях требуется переоформление лицензии ФСТЭК?

- 1. если внесены изменения в уставную документацию организации, занимающейся производством средств защиты информации
- 2. если нужно расширить внесенный в лицензию перечень выполняемых работ
- 3. если в силу научно-технического прогресса появились новые технологии и методы защиты информации
- 4. если существующие или подобные средства защиты, произведенные организацией дали сбой и не смогли обеспечить информационную безопасность на объекте

6. Работники охраны предприятия имеют право требовать от персонала и посетителей объектов

охраны соблюдения внутриобъектового и пропускного режимов:

1. При обеспечении внутриобъектового и пропускного режимов, а также при транспортировке охраняемых грузов, денежных средств и иного имущества в пределах объекта охраны
2. При осуществлении обязанностей по защите жизни и здоровья граждан
3. При обеспечении любых охраняемых мероприятий, предусмотренных законодательством

7. Пропускной режим должен обеспечивать решение следующих задач: (выбрать все верные)

1. предотвращение несанкционированного доступа в контролируруемую зону посторонних лиц и транспортных средств;
2. установление порядка доступа работников (транспортных средств) предприятия в контролируемую зону, а также порядок доступа посетителей и транспорта сторонних организаций;
3. строгое ограничение доступа сотрудников предприятия к обслуживаемым объектам;
4. предотвращение незаконного выноса (вывоза) с территории предприятия материальных ценностей, а также вноса (ввоза) на территорию предприятия оружия, взрывчатых и других предметов и веществ, которые могут быть использованы для совершения теракта.
5. контроль за соблюдением рабочего времени сотрудников предприятия

8. Внутриобъектовый режим должен обеспечиваться: (выбрать все верные)

1. установлением регламента работы и взаимодействием производственных участков, цехов, складов и др. объектов с подразделением охраны на предмет принятия объектов под охрану и контроля состояния пожарной безопасности перед закрытием;
2. внедрением автоматических контрольно-пропускных установок (кабин), обеспечивающих контроль времени прохода через КПП, а также введение системы увольнительных записок, для лиц, выходящих из предприятия в течение рабочего дня;
3. оборудованнием служебных помещений, предназначенных для хранения документов изделий, доступ к которым ограничен, кодовыми замками и охранной сигнализацией;
4. осуществлением патрулирования нарядами охраны территории предприятия в т.ч. и мест хранения материальных ценностей на предмет выявления и задержания посторонних лиц и пресечения хищения материальных ценностей;
5. установлением маршрутов и правил движения транспортных средств и пешеходов по территории предприятия; ограждение, обозначение и освещение мест, опасных для жизни и здоровья персонала и посетителей.
6. установкой камер видеонаблюдения территории как внутри периметра предприятия, так и внешней прилегающей территории

9. Кто утверждает пропускной и внутриобъектовый режим в учреждении:

1. представитель ФСБ
2. представитель МВД
3. директор учреждения

10. Кто разрабатывает пропускной и внутриобъектовый режим в учебном учреждении:

1. директор учреждения
2. зам директора по АХЧ
3. преподаватель по ОБЖ

### **Вариант 3.**

1. Кто принимает решение о допуске гражданина к сведениям, составляющим государственную тайну?

1. руководитель территориальных органов исполнительной власти, наделенных полномочиями по защите государственной тайны
2. руководитель предприятия, на котором работает гражданин
3. руководитель органа ФСБ, проводившего проверочные мероприятия

2. Каким образом осуществляется замена формы допуска к сведениям, составляющим государственную тайну на более низкую?

1. решением межведомственной комиссии по защите государственной тайны

2. решением руководителя предприятия
3. решением руководителя органа ФСБ

3. Правила и порядок допуска должностных лиц, граждан и организаций к государственной тайне определяет...

1. Федеральный Закон «О государственной тайне»
2. Семейный кодекс Российской Федерации
3. Федеральный Закон «О валютном регулировании и валютном контроле»
4. Федеральный Закон «О банках и банковской деятельности»

4. В особом порядке (без проведения проверочных мероприятий) допускаются к государственной тайне ... (выбрать все верные)

1. члены Совета Федерации, депутаты Государственной Думы, судьи,
2. адвокаты, участвующие в судебном процессе, связанном с государственной тайной
3. Президент РФ
4. послы России за рубежом
5. Председатель и члены Правительства РФ

5. Формами допуска к государственной тайне должностных лиц и граждан соответствующими степеням секретности сведений, составляющих государственную тайну, называются...

1. большой секретности, малой секретности, особо важным
2. средней важности, профессиональной секретности, небольшой секретности
3. особой важности, совершенно секретным, секретным

6. Государственную тайну составляют сведения...

1. В области учета населения
2. В области здравоохранения
3. В военной области
4. В области образования

7. К государственной тайне не относятся сведения, защищаемые государством ...

1. распространение которых может нанести ущерб государству;
2. в экономической области;
3. в контрразведывательной деятельности;
4. в оперативно-розыскной деятельности;
5. о частной жизни политических деятелей.

8. Административные дела в сфере нарушений требований защиты информации, составляющей государственную тайну, рассматривает:

1. Федеральная служба безопасности;
2. Полиция
3. Следственный комитет РФ
4. Межведомственная комиссия по защите государственной тайны

9. В отношении допуска к каким сведениям, составляющих государственную тайну, не проводятся проверочные мероприятия:

1. секретных сведений;
2. коммерческих сведений
3. публичных сведений
4. личных сведений
5. служебных сведений

10. В соответствии с ФЗ «О государственной тайне» к числу основных принципов отнесения информации к государственной тайне относятся...

1. Законность, демократизм и гуманизм

2. Законность, формализм и объективизм
3. Законность, демократизм и объективизм
4. Законность, обоснованность и своевременность

**Ответ на вопросы:**

Критерии оценивания при ответе на вопросы:

- 90-100 баллов - при правильном и полном ответе на два вопроса;
- 80-89 баллов - при правильном и полном ответе на один из вопросов и правильном, но не полном ответе на другой из вопросов;
- 60-79 баллов - при правильном и неполном ответе только на один из вопросов;
- 0-59 баллов - при отсутствии правильных ответов на вопросы.

Количество баллов	0-59	60-79	80-89	90-100
Шкала оценивания	неуд	удовл	хорошо	отлично

*Примерный перечень вопросов к зачету:*

1. Угрозы безопасности информации.
2. Система защиты информации.
3. Законодательно - правовые и организационные основы обеспечения защиты информации.
4. Организация защиты информации на предприятии.
5. Политика безопасности предприятия.
6. Структура системы государственного лицензирования.
7. Порядок проведения лицензирования.
8. Основные лицензионные требования и условия.
9. Порядок проведения аттестации и контроля объектов информатизации.
10. Объекты защиты.
11. Структура системы сертификации.
12. Перечень видов деятельности в области защиты информации, подлежащих лицензированию.
13. Государственная аттестация руководителей предприятий.
14. Организационные и технические способы защиты государственной тайны.
15. Организационное управление защитой информации.
16. Перечень сведений конфиденциального характера.
17. Мероприятия по защите конфиденциальной информации.
18. Законодательство РФ о ГТ. Полномочия органов государственной власти и должностных лиц.
19. Перечень сведений, составляющих ГТ. Отнесение сведений к ГТ.
20. Порядок засекречивания сведений и их носителей.
21. Порядок рассекречивания сведений и их носителей.
22. Распоряжение сведениями, составляющими ГТ.
23. Органы защиты ГТ.
24. Порядок допуска к ГТ.
25. Контроль за обеспечением защиты государственной тайны.
26. Правила отнесения сведений, составляющих ГТ, к различным степеням секретности.
27. Организация допуска должностных лиц и граждан к государственной тайне.
28. Информация как объект правового регулирования.
29. Виды информации, защищаемой законодательством РФ.
30. Государственная тайна как особый вид защищаемой информации.
31. Система защиты государственной тайны.
32. Организационное управление защитой информации. (Принципы ИБ предприятия. Направления
33. (методическое, организационной, техническое) и этапы по созданию комплексной системы
34. безопасности. Уровни ПБ предприятия.)
35. Структура организационной защиты информации. (Объекты защиты. Структура организации
36. защиты информации (СЗИ; мероприятия по ЗИ; мероприятия по контролю эффективности защиты
37. информации.)
38. Организация и порядок проведения специальных экспертиз предприятий.
39. Порядок оформления запроса на лицензирование по видам деятельности.
40. Порядок отнесения сведений к коммерческой тайне. (Закон о КТ).
41. Информация, которая не подлежит засекречиванию.
42. Обеспечение сохранности документов, дел и изданий.

43. Обязанности лиц, допущенных к сведениям, составляющих коммерческую тайну.
44. Организация контроля за обеспечением режима при работе со сведениями, содержащими
45. коммерческую тайну.
46. Обязанности персонала организации по сохранению коммерческой тайны.
47. Состав и структура системы безопасности предприятия.
48. Правовые основы деятельности службы безопасности.
49. Организационное обеспечение информационной безопасности при проведении закрытых
50. мероприятий.
51. Организация информационно - аналитической работы.
52. Организация охраны предприятий.
53. Основные задачи организации режима и охраны.
54. Организация пропускного режима.
55. Пропускные документы.
56. Требования внутриобъектового режима.
57. Основные документы, разрабатываемые на охраняемых объектах.
58. Организация информационной безопасности и защиты информации.

### **5.2.3 Методические материалы, определяющие процедуры оценивания знаний, умений, практического опыта деятельности, характеризующие этапы формирования компетенций**

Порядок организации проведения текущего контроля и промежуточной аттестации представлен в Положении о проведении текущего контроля и промежуточной аттестации обучающихся, осваивающих образовательные программы среднего профессионального образования в КузГТУ (Ип 06/10

### **6. Иные сведения и (или) материалы**

1. Образовательный процесс осуществляется с использованием как традиционных, так и современных интерактивных технологий. При контактной работе педагогического работника с обучающимися применяются следующие элементы интерактивных технологий:

- совместный разбор проблемных ситуаций;

- совместное выявление причинно-следственных связей вещей и событий, происходящих в повседневной жизни, и их сопоставление с учебным материалом.

2. Проведение групповых и индивидуальных консультаций осуществляется в соответствии с расписанием консультаций по темам, заявленным в рабочей программе дисциплины, в период освоения дисциплины и перед промежуточной аттестацией с учетом результатов текущего контроля.

