

МИНОБРНАУКИ РОССИИ  
Воткинский филиал  
Федерального государственного бюджетного образовательного  
учреждения высшего образования  
«Ижевский государственный технический университет имени М.Т. Калашникова»  
(ВФ ФГБОУ ВО «ИжГТУ имени М.Т. Калашникова»)

УТВЕРЖДАЮ



/Давыдов И.А.

15 марта 2023 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Правовые основы информационной безопасности

направление 09.03.01 «Информатика и вычислительная техника»

профиль «Автоматизированные системы обработки информации и управления»

уровень образования: бакалавриат

форма обучения: заочная

общая трудоемкость дисциплины составляет: 3 зачетных единиц(ы)



Кафедра Естественные науки и информационные технологии

Составитель \_\_\_\_\_

Рабочая программа составлена в соответствии с требованиями федерального государственного образовательного стандарта высшего образования и рассмотрена на заседании кафедры

Протокол от «15» марта 2023 г. № 2

Заведующий кафедрой

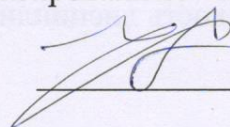
 К.Б. Сентяков

15 марта 2023 г.

**СОГЛАСОВАНО**

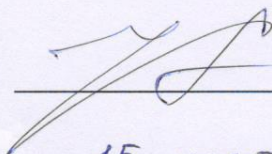
Количество часов рабочей программы и формируемые компетенции соответствуют учебному плану направления 09.03.01 «Информатика и вычислительная техника», профиль «Автоматизированные системы обработки информации и управления»

Председатель учебно-методической комиссии по направлению 09.03.01 «Информатика и вычислительная техника», профиль «Автоматизированные системы обработки информации и управления»

 К.Б. Сентяков

15 марта 2023 г.

Руководитель образовательной программы

 К.Б. Сентяков

15 марта 2023 г.

Аннотация к дисциплине

<b>Название дисциплины</b>	<b>Правовые основы информационной безопасности</b>
<b>Направление подготовки (специальность)</b>	09.03.01 «Информатика и вычислительная техника»
<b>Направленность (профиль/программа/специализация)</b>	«Автоматизированные системы обработки информации и управления»
<b>Место дисциплины</b>	Дисциплина относится к обязательной части Блока 1 «Дисциплины (модули)» ООП
<b>Трудоемкость (з.е. / часы)</b>	3 з.е./108 часов
<b>Цель изучения дисциплины</b>	Формирование способности принимать решения в профессиональной области с учетом нормативно-правовых требований информационной безопасности
<b>Компетенции, формируемые</b>	ОПК-3. Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности; УК-2. Способен определять круг задач в рамках поставленной цели и выбирать оптимальные способы их решения, исходя из действующих правовых норм, имеющихся ресурсов и ограничений
<b>Содержание дисциплины (основные разделы и темы)</b>	Основные направления государственной политики в области защиты информации. Основные понятия нормативно- правового обеспечения информационной безопасности. Ответственность за нарушение режима информационной безопасности. Правовые основы защиты государственной и коммерческой тайн. Правовые основы лицензирования и сертификации в области защиты информации. Правовые основы защиты персональных данных, ГИС (государственных информационных систем), объектов КИИ (критической информационной инфраструктуры). Нормативно – правовое обеспечение в сфере использования криптографических средств защиты информации
<b>Форма промежуточной аттестации</b>	Дифференцированный зачет (6 семестр)

## 1. Цели и задачи дисциплины:

**Целью** освоения дисциплины является формирование способности принимать решения в профессиональной области с учетом требований информационной безопасности

### Задачи дисциплины:

- изучение государственной политики в области защиты информации
- изучение основных нормативно-правовых актов, регламентирующих вопросы защиты информации
- получение навыков в применении нормативно-правовых актов, регламентирующих работу по обеспечению информационной безопасности автоматизированных систем

## 2. Планируемые результаты обучения

В результате освоения дисциплины у студента должны быть сформированы

### Знания, приобретаемые в ходе освоения дисциплины

№ п/п	Знания
1	Государственной политики в области обеспечения информационной безопасности
2	Правовых основ защиты информации ограниченного доступа
3	Видов правонарушений и ответственности в области информационной безопасности

### Умения, приобретаемые в ходе освоения дисциплины

№ п/п	Умения
1	Использовать правовые знания в области информационной безопасности в решении профессиональных задач

### Навыки, приобретаемые в ходе освоения дисциплины

№ п/п	Навыки
1	В применении нормативно - правовых актов и разработке документов, регламентирующих работу по обеспечению информационной безопасности автоматизированных систем

### Компетенции, приобретаемые в ходе освоения дисциплины

Компетенции	Индикаторы	Знания	Умения	Навыки
ОПК-3. Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности;	ОПК-3.1 <b>Знать:</b> принципы, методы и средства решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	1,2	1	1

	ОПК-3.2 <b>Уметь:</b> решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	1,2,3	1	1
	ОПК-3.3 <b>Владеть:</b> навыками подготовки обзоров, аннотаций, составления рефератов, научных докладов, публикаций и библиографии по научно-исследовательской работе с учетом требований информационной безопасности	1,2,3	1	1
УК-2. Способен определять круг задач в рамках поставленной цели и выбирать оптимальные способы их решения, исходя из действующих правовых норм, имеющихся ресурсов и ограничений	УК-2.1 <b>Знать:</b> виды ресурсов и ограничений для решения профессиональных задач; основные методы оценки разных способов решения задач; действующее законодательство и правовые нормы, регулирующие профессиональную деятельность	1,2,3	1	1
	УК-2.2 <b>Уметь:</b> проводить анализ поставленной цели и формулировать задачи, которые необходимо решить для ее достижения; анализировать альтернативные варианты решений для достижения намеченных результатов; использовать нормативно-правовую документацию в сфере профессиональной деятельности	1,2,3	1	1
	УК-2.3 <b>Владеть:</b> методами разработки цели и задач проекта; методами оценки потребности в ресурсах, продолжительности и стоимости проекта, навыками работы с нормативно-правовой документацией	1,2,3	1	

### 3. Место дисциплины в структуре ООП

Дисциплина относится к обязательной части Блока 1 «Дисциплины (модули)» ООП. Дисциплина изучается на 3 курсе в 6 семестре.

Изучение дисциплины базируется на знаниях, умениях и навыках, полученных при освоении дисциплин (модулей): Информатика, Правоведение

Перечень последующих дисциплин (модулей), для которых необходимы знания, умения и навыки, формируемые данной учебной дисциплиной (модулем): "Защита информации", "Проектирование автоматизированных систем обработки информации и управления"

### 4. Структура и содержание дисциплины

#### 4.1 Структура дисциплины

№ п/п	Раздел дисциплины. Форма промежуточной аттестации	Всего часов на раздел	Семестр	Распределение трудоемкости раздела (в часах) по видам учебной работы					СРС	Содержание самостоятельной работы
				контактная				СРС		
				лек	пр	лаб	КЧА			
1	2	3	4	5	6	7	8	10	11	
1	Введение. Основные направления государственной политики в области защиты информации	15,5	6	1	0,5	-			14	[1,2] Подготовка к устному опросу. Практическая работа. Подготовка к вопросам по практической работе
2	Основные понятия нормативно-правового обеспечения информационной безопасности	16,75	6	0,25	0,5	-			16	[1,2] Практическая работа. Подготовка к вопросам по практической работе
3	Правовые основы защиты государственной и коммерческой тайн.	18	6	1	1	-			16	[1,3] Практическая работа. Подготовка к вопросам по практической работе. Подготовка к контрольной работе
4	Правовые основы лицензирования и сертификации в области защиты информации	14,75	6	0,25	0,5	-			14	[1,3] Практическая работа. Подготовка к вопросам по практической работе. Подготовка к тестированию
5	Правовые основы защиты персональных данных, ГИС (государственных информационных систем), объектов КИИ (критической информационной инфраструктуры)	26	6	3	1	-			22	[1] Практическая работа. Подготовка к вопросам по практической работе

6	Нормативно – правовое обеспечение в сфере использования криптографических средств защиты информации	15	6	0,5	0,5	-		14	[1,3] Практическая работа. Подготовка к вопросам по практической работе
	Дифференцированный зачет	2	6	–	–	–	0,4	1,6	Зачет выставляется по совокупности результатов текущего контроля успеваемости
	<b>Итого:</b>	<b>108</b>		<b>6</b>	<b>4</b>	<b>-</b>	<b>0,4</b>	<b>97,6</b>	

#### 4.2 Содержание разделов курса и формируемых в них компетенций

№ п/п	Раздел дисциплины	Коды компетенции и индикаторов	Знания	Умения	Навыки	Форма контроля
1	Введение. Основные направления государственной политики в области защиты информации	ОПК-3.1, ОПК3.2, ОПК-3.3, УК-2.1, УК-2.2, УК2.3	1,2,3	1	1	Устный опрос Практическое занятие
2	Основные понятия нормативно- правового обеспечения информационной безопасности	ОПК-3.1, ОПК-2.1, УК-2.2, УК-2.3, ОПК-3.1, ОПК-3.2, ОПК-3.3	1,2,3	1	1	Практическое занятие
3	Правовые основы защиты государственной и коммерческой тайн.	ОПК-3.1, ОПК3.2, ОПК-3.3, УК-2.1, УК-2.2, УК2.3	1,2,3	1	1	Практические занятия. Контрольная работа
4	Правовые основы лицензирования и сертификации в области защиты информации	ОПК-3.1, ОПК3.2, ОПК-3.3, УК-2.1, УК-2.2, УК2.3	1,2,3	1	1	Практические занятия. Тест
5	Правовые основы защиты персональных данных, ГИС (государственных информационных систем), объектов КИИ (критической информационной инфраструктуры)	ОПК-3.1, ОПК3.2, ОПК-3.3, УК-2.1, УК-2.2, УК2.3	1,2,3	1	1	Практические занятия.
6	Нормативно – правовое обеспечение в сфере использования криптографических средств защиты информации	ОПК-3.1, ОПК3.2, ОПК-3.3, УК-2.1, УК-2.2, УК2.3	1,2,3	1	1	Практическое занятие

### 4.3 Наименование тем лекций, их содержание и объем в часах

№ п/п	№ раздела дисциплины	Наименование лекций	Трудоемкость (час)
1.	1	1. Цели и задачи курса. Основные понятия и определения. Национальные интересы и безопасность России. Доктрина информационной безопасности РФ. Стратегия развития информационного общества. 2. Государственная система защиты информации в РФ. Полномочия, права и обязанности органов государственной власти в области защиты информации.	1
2.	2	1. Правовые основы защиты информации. Уровни правового обеспечения информационной безопасности 2. Основные законодательные акты в области защиты информации 3. Информация как объект правовых отношений. 4. Категории информации по условиям доступа к ней 5. Ответственность за нарушение режима информационной безопасности	0,25
3.	3	1. Основные понятия в области защиты государственной тайны. Государственная система защиты гостайны в РФ. Межведомственная комиссия по защите гостайны. Грифы секретности в РФ. Порядок засекречивания и рассекречивания сведений, составляющих государственную тайну. Порядок допуска граждан и должностных лиц к государственной тайне 2. Правовые основы защиты коммерческой тайны. Порядок отнесения информации к коммерческой тайне.	1
	4	1. Лицензирование деятельности по защите информации ограниченного доступа и разработке и производству средств защиты информации 2. Сертификация средств защиты информации. Основные понятия и законодательное регулирование	0,25
	5	2. 1. Законодательство в области защиты персональных данных Классификация информационных систем персональных данных. Реализация мероприятий по защите персональных данных. Определение набора мер по защите персональных данных 3. Законодательство в области защиты государственных информационных систем 4. Классификация государственных информационных систем и требования к их защищенности 5. Основные требования законодательства к безопасности критической информационной инфраструктуры (КИИ) РФ.Классификация информационных систем КИИ.	3
	6	1. Нормативно – правовое обеспечение в сфере связи и криптографической защиты 2. Государственное регулирование вопросов использования криптографических средств и ЭЦП	0,5
	<b>Всего</b>		<b>6</b>



#### 4.4 Наименование тем практических занятий, их содержание и объем в часах

№ п/п	№ раздела дисциплины	Наименование практических работ	Трудоемкость (час)
1.	1	Анализ терминов и определений информационной безопасности . Национальные интересы РФ в области ИБ, приоритетные направления в области защиты информации. Органы, обеспечивающие национальную безопасность РФ	0,5
2.	2	Ответственность за правонарушения в области информационной безопасности	0,5
3.	3	Законодательство в области защиты государственной тайны. Перечень сведений, отнесенных к государственной тайне. Анализ нормативно -правовых документов в области защиты государственной тайны.	0,5
4.	3	Законодательство в области конфиденциальной информации. Анализ нормативно- правовых актов в области защиты коммерческой тайны. Ответственность за нарушение законодательства в области защиты коммерческой тайны. Составление нормативно-правовых актов в области защиты конфиденциальной информации на предприятии.	0,5
5.	4	Анализ и подбор сертифицированных средств защиты информации .Ответственность за использование несертифицированных СЗИ.	0,5
6.	5	Составления акта классификации информационной системы персональных данных. Классификация ГИС. Ответственность оператора персональных данных за нарушение законодательства.	0,5
7.	5	Анализ законодательства в области защиты КИИ. Категорирование объектов КИИ. Составление акта категорирования объекта КИИ	0,5
8.	6	Законодательство в области криптографической защиты информации. Ответственность в области криптографической защиты информации.	0,5
	<b>Всего</b>		<b>4</b>

#### 4.5 Наименование тем лабораторных работ, их содержание и объем в часах

Лабораторные работы учебным планом не предусмотрены

#### 5. Оценочные материалы для текущего контроля успеваемости и промежуточной аттестации по дисциплине

Для контроля результатов освоения дисциплины проводятся :

- контрольная работа
- тесты
- вопросы для устного опроса
- зачет

*Примечание:* оценочные материалы (типовые варианты тестов, контрольных работ и др.) приведены в приложении к рабочей программе дисциплины.

Промежуточная аттестация по итогам освоения дисциплины – зачет с оценкой

## 6. Учебно-методическое и информационное обеспечение дисциплины:

### 1. а) Основная литература

№ п/п	Наименование книги	Год издания
1	Кубанков, А. Н. Система обеспечения информационной безопасности Российской Федерации: организационно-правовой аспект [Электронный ресурс] : учебное пособие / А. Н. Кубанков, Н. Н. Куняев ; под ред. А. В. Морозов. — Электрон. текстовые данные. — М. : Всероссийский государственный университет юстиции(РПА Минюста России), 2014. — 78 с. — 978-5-89172-850-9. — Режим доступа: <a href="http://www.iprbookshop.ru/47262.html">http://www.iprbookshop.ru/47262.html</a>	2014
2	Основы информационной безопасности [Электронный ресурс] : учебник для студентов вузов, обучающихся по направлению подготовки «Правовое обеспечение национальной безопасности» / В. Ю. Rogozin, И. Б. Галушкин, В. К. Новиков, С. Б. Вепрев. — Электрон. текстовые данные. — М. : ЮНИТИ-ДАНА, 2017. — 287 с. — 978-5-238-02857-6. — Режим доступа: <a href="http://www.iprbookshop.ru/72444.html">http://www.iprbookshop.ru/72444.html</a>	2017

### б) Дополнительная литература

№ п/п	Наименование	Год издания
1	Морозов, А. В. Информационное право и информационная безопасность. Часть 2 [Электронный ресурс] : учебник для магистров и аспирантов / А. В. Морозов, Л. В. Филатова, Т. А. Полякова. — Электрон. текстовые данные. — Москва, Саратов : Всероссийский государственный университет юстиции (РПА Минюста России), Ай Пи Эр Медиа, 2016. — 604 с. — 978-5-00094-297-0. — Режим доступа: <a href="http://www.iprbookshop.ru/66771.html">http://www.iprbookshop.ru/66771.html</a>	2016
2	Нестеров С.А., Основы информационной безопасности [Электронный ресурс] : учебное пособие / Нестеров С.А.. — Электрон. текстовые данные. — СПб. : Санкт-Петербургский политехнический университет Петра Великого, 2014. — 322 с. — 978-5-7422-4331-1. — Режим доступа: <a href="http://www.iprbookshop.ru/43960.html">http://www.iprbookshop.ru/43960.html</a>	2014

### в) перечень ресурсов информационно-коммуникационной сети Интернет

1. Электронно-библиотечная система IPRbooks  
<http://istu.ru/material/elektronno-bibliotechnaya-sistema-iprbooks>
2. Электронный каталог научной библиотеки ИжГТУ имени М.Т. Калашникова Web ИРБИС  
[http://94.181.117.43/cgi-bin/irbis64r\\_12/cgiirbis\\_64.exe?LNG=&C21COM=F&I21DBN=IBIS&P21DBN=IBIS](http://94.181.117.43/cgi-bin/irbis64r_12/cgiirbis_64.exe?LNG=&C21COM=F&I21DBN=IBIS&P21DBN=IBIS)
3. Национальная электронная библиотека - <http://нэб.рф>
4. Мировая цифровая библиотека - <http://www.wdl.org/ru>
5. Международный индекс научного цитирования Web of Science - <http://webofscience.com>
6. Научная электронная библиотека eLIBRARY.RU – <https://elibrary.ru/defaultx.asp>

### г) программное обеспечение:

1. Microsoft Office Standard 2007
2. Doctor Web Enterprise Suite

### д) методические указания:

1. Оформление контрольных работ, рефератов, курсовых работ и проектов, отчетов по практике, выпускных квалификационных работ: методические указания/сост.: А.Ю. Уразбахтина, Р.М. Бакиров, В.А. Смирнов – Воткинск: Изд. ВФ ИжГТУ имени М.Т. Калашникова, 2018–25с. -

Режимдоступа:[http://vfistu.ru/images/files/Docs/metodichka\\_po\\_oformleiu\\_v3.pdf](http://vfistu.ru/images/files/Docs/metodichka_po_oformleiu_v3.pdf)

2. Учебно-методическое пособие по организации самостоятельной работы обучающихся: для обучающихся по направлению подготовки 15.03.05 – конструкторско-

## **7. Материально-техническое обеспечение дисциплины:**

### **1. Лекционные занятия.**

Учебные аудитории для лекционных занятий укомплектованы мебелью и техническими средствами обучения, служащими для представления учебной информации большой аудитории (наборы демонстрационного оборудования (проектор, экран, компьютер/ноутбук).

### **2. Практические занятия.**

Учебные аудитории для практических занятий укомплектованы специализированной мебелью и техническими средствами обучения (проектор, экран, компьютер/ноутбук).

### **3. Самостоятельная работа.**

Помещения для самостоятельной работы оснащены компьютерной техникой с возможностью подключения к сети «Интернет» и доступом к электронной информационно-образовательной среде ВФ ФГБОУ ВО «ИжГТУ имени М.Т. Калашникова»:

помещения для самостоятельной работы обучающихся (ауд.№ 224, адрес: 427430, Удмуртская Республика, г. Воткинск, ул. П.И. Шувалова, д. 1).

При необходимости рабочая программа дисциплины (модуля) может быть адаптирована для обеспечения образовательного процесса инвалидов и лиц с ограниченными возможностями здоровья, в том числе для обучения с применением дистанционных образовательных технологий. Для этого требуется заявление студента (его законного представителя) и заключение психолого-медико-педагогической комиссии (ПМПК).

## Лист согласования рабочей программы дисциплины на учебный год

Рабочая программа дисциплины (модуля) «Правовые основы информационной безопасности» по направлению подготовки 09.03.01 «Информатика и вычислительная техника»

по профилю «Автоматизированные системы обработки информации и управления»

согласована на ведение учебного процесса в учебном году:

<b>Учебный год</b>	<b>«Согласовано»: заведующий кафедрой, ответственной за РПД (подпись и дата)</b>
2022 – 2023	
2023 – 2024	
2024 – 2025	
2025 - 2026	



МИНОБРНАУКИ РОССИИ  
Воткинский филиал  
Федерального государственного бюджетного образовательного  
учреждения высшего образования  
«Ижевский государственный технический университет имени М.Т. Калашникова»  
(ВФ ФГБОУ ВО «ИжГТУ имени М.Т. Калашникова»)

**Оценочные средства  
по дисциплине**

Правовые основы информационной безопасности

направление 09.03.01 «Информатика и вычислительная техника»

профиль «Автоматизированные системы обработки информации и управления»

уровень образования: бакалавриат

форма обучения: заочная

общая трудоемкость дисциплины составляет: 3 зачетных единиц(ы)

## 1.Оценочные средства

Оценивание формирования компетенций производится на основе результатов обучения, приведенных в п. 2 рабочей программы и ФОС. Связь разделов компетенций, индикаторов и форм контроля (текущего и промежуточного) указаны в таблице 4.2 рабочей программы дисциплины.

Оценочные средства соотнесены с результатами обучения по дисциплине и индикаторами достижения компетенций, представлены ниже.

№ п/п	Коды компетенции и индикаторов	Результат обучения (знания, умения и навыки)	Формы текущего и промежуточного контроля
1	ОПК-3.1 <b>Знать:</b> принципы, методы и средства решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационнокоммуникационных технологий и с учетом основных требований информационной безопасности	31. Государственной политики в области обеспечения информационной безопасности 32. Правовых основ защиты информации ограниченного доступа У1..Использовать правовые знания в области информационной безопасности в решении профессиональных задач Н1. В применении нормативно - правовых актов и разработке документов, регламентирующих работу по обеспечению информационной безопасности автоматизированных систем	Устный опрос Практические работы Контрольная работа тестирование Зачет
	ОПК-3.2 <b>Уметь:</b> решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационнокоммуникационных технологий и с учетом основных требований информационной безопасности	31. Государственной политики в области обеспечения - информационной безопасности 32. Правовых основ защиты информации ограниченного доступа 33. Видов правонарушений и ответственности в области информационной безопасности У1..Использовать правовые знания в области информационной безопасности в решении профессиональных задач Н1. В применении нормативно – правовых актов и разработке документов, регламентирующих работу по обеспечению информационной безопасности автоматизированных систем	Устный опрос Практические работы Контрольная работа тестирование Зачет
	ОПК-3.3 <b>Владеть:</b> навыками подготовки обзоров, аннотаций, составления рефератов, научных докладов, публикаций и библиографии по научно-исследовательской работе с учетом требований информационной безопасности	31. Государственной политики в области обеспечения информационной безопасности 32. Правовых основ защиты информации ограниченного доступа 33. Видов правонарушений и ответственности в области информационной безопасности У1..Использовать правовые знания в области информационной безопасности в решении профессиональных задач Н1. В применении нормативно - правовых актов и разработке документов, регламентирующих работу по обеспечению информационной безопасности автоматизированных систем	Устный опрос Практические работы Контрольная работа тестирование Зачет

2	УК-2.1 Знать: виды ресурсов и ограничений для решения профессиональных задач; основные методы оценки разных способов решения задач; действующее законодательство и правовые нормы, регулирующие профессиональную деятельность	31. Государственной политики в области обеспечения информационной безопасности 32. Правовых основ защиты информации ограниченного доступа 33. Видов правонарушений и ответственности в области информационной безопасности У1..Использовать правовые знания в области информационной безопасности в решении профессиональных задач Н1. В применении нормативно - правовых актов и разработке документов, регламентирующих работу по обеспечению информационной безопасности автоматизированных систем	Устный опрос Практические работы Контрольная работа тестирование Зачет
	УК-2.2 Уметь: проводить анализ поставленной цели и формулировать задачи, которые необходимо решить для ее достижения; анализировать альтернативные варианты решений для достижения намеченных результатов; использовать нормативно-правовую документацию в сфере профессиональной деятельности	31. Государственной политики в области обеспечения информационной безопасности 32. Правовых основ защиты информации ограниченного доступа 33. Видов правонарушений и ответственности в области информационной безопасности У1..Использовать правовые знания в области информационной безопасности в решении профессиональных задач Н1. В применении нормативно - правовых актов и разработке документов, регламентирующих работу по обеспечению информационной безопасности автоматизированных систем	Устный опрос Практические работы Контрольная работа тестирование Зачет
	УК-2.3 Владеть: методиками разработки цели и задач проекта; методами оценки потребности в ресурсах, продолжительности и стоимости проекта, навыками работы с нормативно-правовой документацией	31. Государственной политики в области обеспечения информационной безопасности 32. Правовых основ защиты информации ограниченного доступа 33. Видов правонарушений и ответственности в области информационной безопасности У1..Использовать правовые знания в области информационной безопасности в решении профессиональных задач Н1. В применении нормативно - правовых актов и разработке документов, регламентирующих работу по обеспечению информационной безопасности автоматизированных систем	Устный опрос Практические работы Контрольная работа тестирование Зачет

**Наименование:** дифференцированный зачет **Представление в ФОС:**

**Перечень вопросов для проведения зачета:**

1. Основные понятия в области защиты информации. Определение и сравнение терминов «информационная безопасность» и «защита информации»
2. Роль и место ИБ в системе национальной безопасности государства
3. Государственная политика обеспечения ИБ в РФ
4. Права, полномочия и обязанности Президента РФ, Правительства РФ и др. федеральных и муниципальных органов исполнительной власти субъектов РФ в области безопасности
5. Полномочия, задачи, функции и права ФСБ в области защиты информации
6. Полномочия, задачи, функции и права ФСТЭК в области защиты информации
7. Полномочия, обязанности и права Федеральной службы по надзору в сфере связи, массовых коммуникаций и информационных технологий в области защиты информации при обработке персональных данных
8. Информация как объект правовых отношений. Характеристика информационного права

9. Уровни правового обеспечения ИБ. Иерархия нормативных актов в области защиты информации. Сущность и содержание основных нормативно-правовых актов в области ИБ
10. Ответственность за правонарушения в области ИБ
11. Сущность основных понятий в области защиты государственной тайны.
12. Государственная система защиты гостайны, органы защиты гостайны.
13. Межведомственная комиссия по защите гостайны и ее основные задачи в области защиты гостайны.
14. Допуск граждан к государственной тайне. Порядок оформления допуска к гостайне.
15. Правовые основы защиты коммерческой тайны. Понятия «коммерческая тайна», «режим коммерческой тайны»
16. Порядок отнесения информации к коммерческой тайне
17. Права обладателя информации, составляющей коммерческую тайну.
18. Ответственность за нарушение режима коммерческой тайны.
19. Способы охраны конфиденциальной информации. ФЗ «О коммерческой тайне»
20. Цели и задачи и принципы в области лицензирования
21. Полномочия и права лицензирующих органов в области информационной безопасности
22. Процедура получения лицензии. Срок действия лицензии
23. Сертификация в РФ. Процедура сертификации средств защиты информации. Срок действия сертификата.
24. Ответственность за правонарушение в области лицензирования и сертификации
25. Законодательство в области защиты персональных данных
26. Порядок классификации информационных систем персональных данных.
27. Реализация мероприятий по защите персональных данных.
28. Права и обязанности оператора, обрабатывающего персональные данные
29. Права и обязанности субъекта персональных данных
30. Основные требования законодательства к безопасности критической информационной инфраструктуры (КИИ) РФ. Классификация информационных систем КИИ
31. Законодательство в области криптографии и связи
32. Государственное регулирование вопросов использования ЭП. Виды и назначение ЭП
33. Доктрина информационной безопасности Российской Федерации от 05.12.2016г. и ее краткая характеристика
34. Государственная программа Российской Федерации " О стратегии развития информационного общества в Российской Федерации на 2017 - 2030 годы" и ее краткая характеристика
35. Федеральный закон от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации» и его краткая характеристика
36. Федеральный закон «О коммерческой тайне» и его краткая характеристика
37. Закон РФ от 21 июля 1993 г. № 5485-1 «О государственной тайне» и его краткая характеристика
38. Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных» и его краткая характеристика
39. Федеральный закон от 6 апреля 2011 г. № 63-ФЗ «Об электронной подписи» и его краткая характеристика
40. Статья 272 УК РФ (Неправомерный доступ к компьютерной информации). Рассмотреть по составу.
41. Статья 273 УК РФ (Создание, использование и распространение вредоносных компьютерных программ). Рассмотреть по составу.
42. Статья 274 УК РФ (Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей). Рассмотреть по составу.
43. Статья 183 УК РФ (Незаконные получение и разглашение сведений, составляющих коммерческую, налоговую или банковскую тайну).
44. Статья 13.12 КоАП РФ. Нарушение правил защиты информации
45. Статья 13.13 КоАП РФ. Незаконная деятельность в области защиты информации
46. Статья 13.14 КоАП РФ. Разглашение информации с ограниченным доступом



**Критерии оценки:**

Приведены в разделе 2

**Наименование:** тест **Варианты тестов:**

**1. Какие из утверждений является верными**

- а) сертифицирует средства СЗИ , выдают сертификаты и лицензии на применение знака соответствия с представлением копий в федеральные органы по сертификации и ведут учет
- б) не имеют права представлять по их требованию необходимую информацию
- в) имеет право приостанавливать либо обменять действие выданных ими сертификатов и лицензий на применение знака соответствия

**2. Какие центры по сертификации находятся в УР(г.Ижевск)**

- а) Softjet
- б) Иж-стандарт
- в) НПО Компьютер
- г) УЦС

**3. Участником сертификации средств защиты информации нижеперечисленных являются**

- а) федеральный орган по сертификации
- б) ФСБ
- в) ФСТЭК
- г) испытательные лаборатории
- д) изготовители-продавцы

**4. Каких категорий объектов не существует**

- а) особоважный объект
- б) секретный объект
- в) режимный объект
- г) особорежимный объект

**5. Комплекс мероприятий подтверждает, что объект соответствует требованиям стандартов и иных нормативных документов утвержд. ФСТЭК РФ**

- а) аттестация объекта
- б) организация объекта
- в) лицензирование объекта

**6. Центральный орган системы сертификации:**

- а) организует работы по формированию систем сертификации
- б) координирует деятельность органов
- в) ведет учет входящих в систему сертификации органов по сертификации средств СИ
- г) все варианты верны

**7. федеральный орган по сертификации в пределах своей компетенции**

- а) создает систему сертификации
- б) осуществляет выбор способа подтверждения соответствия средств СИ и требования нормативных документов
- в) выдает сертификат и лицензию на применение знака соответствия
- г) все варианты верны

**8. Сколько выделяют зон безопасности внутри объекта**

- а) 4
- б) 6
- в) 9
- г) 3

**9. К федеральным органам по сертификации относятся**

- а) ФСТЭК
- б) ФСБ

- в) Министерство обороны РФ
- г) ГТК

**10. Обязательной аттестации подлежат объекты информатизации**

- а) коммерческая тайна
- б) гос. тайна
- в) ведение секретных переговоров
- г) нет верного ответа

**11. Что поверяет ФСТЭК у сертифицированных продуктов**

- а) галографическая наклейка
- б) ПО
- в) паспорт на продукт
- г) Все правильно

**12. Укажите, что определяют соответствующие госорганы в области сертификации**

- а) порядок выдачи и приостановки сертификатов
- б) порядок оплаты услуг по сертификации
- в) права и обязанности участника системы сертификации с СИ
- г) все правильно

**Критерии оценки:**

Приведены в разделе 2

**Наименование:** контрольная работа

**Представление в ФОС:** набор вариантов заданий

**Варианты заданий:**

- 1) Назовите грифы секретности материальных носителей
- 2) Назовите формы допуска сотрудников к гостайне
- 3) Опишите как сведения становятся гостайной
- 4) Что такое гриф секретности и куда он наносится?
- 5) Укажите срок засекречивания материальных носителей
- 6) Какие функции выполняет Межведомственная комиссия
- 7) Опишите условия для получения формы допуска к ГТ
- 8) Срок действия допуска к ГТ?
- 9) Кто проводит проверочные мероприятия по допуску сотрудника к ГТ?
- 10) Что такое перечень сведений, отнесенных к ГТ на предприятии, кто его разрабатывает. Актуализирует?
- 11) Какие ограничения могут быть наложены на сотрудника с допуском ГТ?
- 12) Какие преференции имеет сотрудник с допуском ГТ?
- 13) «СС» - это гриф к сведениям в какой области?
- 14) Кто имеет права допуска к ГТ без его оформления?
- 15) Министр УР по информатизации – имеет права допуска к ГТ без оформления?
- 16) Глава УР имеет права допуска к ГТ без оформления?

**Критерии оценки:**

Приведены в разделе 2

**Наименование:** устный опрос

**Представление в ФОС:** перечень заданий или вопросов

**Варианты заданий:**

Задание №1. Проанализируйте Стратегию развития информационного общества 2017-2030г. Ответьте на вопросы:

- Стратегия развития общества на 2017-2030 г. основные цели и ее отличие от Стратегии развития общества от 7.02.2008г. (№Пр-212)?

Задание №2. Объясните следующие понятия:

- Безопасное ПО?
- Интернет вещей?
- Критическая информационная инфраструктура?
- Облачные вычисления, туманные вычисления?
- Приведите примеры объектов с критической информационной инфраструктурой?
- Информационное пространство? Информационное общество? Цифровая экономика? Электронное правительство?
- Индустриальный интернет?

**Критерии оценки:**

Приведены в разделе 2

**Наименование:** практические работы

**Представление в ФОС:** набор вариантов заданий

**Варианты заданий:**

- Познакомиться с нормативной базой по допуску граждан к ГТ
- Оформить карточку допуска (форма 1) (ознакомиться с формой карточки и выписать основные данные, которые необходимы для заполнения карточки допуска)
- **Ответить на вопросы:**
- 1) Кто проводит проверочные мероприятия?
- 2) Могут ли запрашивать при проверочных мероприятиях сведения, касающиеся личной и семейной тайны?
- 3) Нужно ли оформлять допуск гражданину для работы с информацией грифа «Служебная тайна»

**Критерии оценки:**

Приведены в разделе 2

## 2. Критерии и шкалы оценивания

Для контрольных мероприятий (текущего контроля) устанавливается минимальное и максимальное количество баллов в соответствии с таблицей. Контрольное мероприятие считается пройденным успешно при условии набора количества баллов не ниже минимального.

Результат обучения по дисциплине считается достигнутым при успешном прохождении обучающимся всех контрольных мероприятий, относящихся к данному результату обучения.

Разделы дисциплины	Форма контроля	Количество баллов	
		min	max
1	Устный опрос	3	5
1	Выполнение практической работы, ответ на вопросы	7	10
2	Выполнение практической работы, ответ на вопросы	7	10
3	Выполнение практической работы, ответ на вопросы	7	10
3	Выполнение практической работы, ответ на вопросы	6	10
3	Контрольная работа	5	10
4	Выполнение практической работы, ответ на вопросы	5	10
4	тест	5	10
5	Выполнение практической работы, ответ на вопросы	5	7

5	Выполнение практической работы, ответ на вопросы	5	8
6	Выполнение практической работы, ответ на вопросы	5	10

При оценивании результатов обучения по дисциплине в ходе текущего контроля успеваемости используются следующие критерии. Минимальное количество баллов выставляется обучающемуся при выполнении всех показателей, допускаются несущественные неточности в изложении и оформлении материала.

<b>Наименование, обозначение</b>	<b>Показатели выставления минимального количества баллов</b>
Практическая работа	Задания выполнены более чем наполовину. Присутствуют серьезные ошибки. Продемонстрирован удовлетворительный уровень владения материалом. Проявлены низкие способности применять знания и умения к выполнению конкретных заданий.
<b>Наименование, обозначение</b>	<b>Показатели выставления минимального количества баллов</b>
	На защите практической работы даны правильные ответы не менее чем на 50% заданных вопросов
Контрольная работа	Продемонстрирован удовлетворительный уровень владения материалом. Правильно решено не менее 50% заданий
Тест	Правильно решено не менее 50% тестовых заданий
Устный опрос	Даны правильные ответы не менее чем на 50% заданных вопросов. Продемонстрированы знания основного учебно-программного материала

Промежуточная аттестация по дисциплине проводится в форме дифференцированного зачета

Итоговая оценка выставляется с использованием следующей шкалы.

<b>Оценка</b>	<b>Набрано баллов</b>
«отлично»	88-100
«хорошо»	76-87
«удовлетворительно»	61-75
«неудовлетворительно»	менее 60

При оценивании результатов обучения по дисциплине в ходе промежуточной аттестации используются следующие критерии и шкала оценки:

<b>Оценка</b>	<b>Критерии оценки</b>
«отлично»	Обучающийся показал всестороннее, систематическое и глубокое знание учебного материала, предусмотренного программой, умение уверенно применять на их практике при решении задач (выполнении заданий), способность полно, правильно и аргументировано отвечать на вопросы и делать необходимые выводы. Свободно использует основную литературу и знаком с дополнительной литературой, рекомендованной программой
«хорошо»	Обучающийся показал полное знание теоретического материала, владение основной литературой, рекомендованной в программе, умение самостоятельно решать задачи (выполнять задания), способность аргументировано отвечать на вопросы и делать необходимые выводы, допускает единичные ошибки, исправляемые после замечания преподавателя. Способен к самостоятельному пополнению и обновлению знаний в ходе дальнейшей учебной работы и профессиональной деятельности



«удовлетворительно»	Обучающийся демонстрирует неполное или фрагментарное знание основного учебного материала, допускает существенные ошибки в его изложении, испытывает затруднения и допускает ошибки при выполнении заданий (решении задач), выполняет задание при подсказке преподавателя, затрудняется в формулировке выводов. Владеет знанием основных разделов, необходимых для дальнейшего обучения, знаком с основной и дополнительной литературой, рекомендованной программой
«неудовлетворительно»	Обучающийся при ответе демонстрирует существенные пробелы в знаниях основного учебного материала, допускает грубые ошибки в формулировании основных понятий и при решении типовых задач (при выполнении типовых заданий), не способен ответить на наводящие вопросы преподавателя. Оценка ставится обучающимся, которые не могут продолжить обучение или приступить к профессиональной деятельности по окончании образовательного учреждения без дополнительных занятий по рассматриваемой дисциплине

