

Министерство науки и высшего образования РФ Ульяновский государственный университет Ф – Рабочая программа дисциплины	Форма	
--	-------	--



**УТВЕРЖДЕНО**

решием Ученого совета факультета математики, информационных и авиационных технологий  
«21» 05 2024г., протокол № 5/24  
Председатель \_\_\_\_\_ Волков М.А.  
«21» 05 2024 г.

## РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Дисциплина	<b>Организационное и правовое обеспечение информационной безопасности</b>
Факультет	Факультет математики, информационных и авиационных технологий
Кафедра	Кафедра информационной безопасности и теории управления
Курс	3

Направление (специальность): 10.05.03 Информационная безопасность автоматизированных систем

Направленность (профиль/специализация): Безопасность открытых информационных систем

Форма обучения: очная

Дата введения в учебный процесс УлГУ: 01.09.2024 г.

Программа актуализирована на заседании кафедры: протокол № 10 от 15.04 2024 г.

Программа актуализирована на заседании кафедры: протокол № \_\_\_\_\_ от \_\_\_\_\_ 20\_\_ г.

Программа актуализирована на заседании кафедры: протокол № \_\_\_\_\_ от \_\_\_\_\_ 20\_\_ г.

Сведения о разработчиках:

ФИО	КАФЕДРА	Должность, ученая степень, звание
Иванцов Андрей Михайлович	Кафедра информационной безопасности и теории управления	Доцент, Кандидат технических наук, Доцент

## 1. ЦЕЛИ И ЗАДАЧИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

### Цели освоения дисциплины:

Дисциплина «Организационное и правовое обеспечение информационной безопасности» является важной составляющей общей профессиональной подготовки специалистов в области обеспечения информационной безопасности. Дисциплина реализует требования федерального государственного образовательного стандарта высшего профессионального образования по специальности "Информационная безопасность автоматизированных систем".

### Задачи освоения дисциплины:

изучить основные документы по информационной безопасности;

обеспечить освоение студентами практических навыков работы с нормативно-правовой базой в области обеспечения информационной безопасности.

## 2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП

Дисциплина «Организационное и правовое обеспечение информационной безопасности» относится к числу дисциплин блока Б1.О.1, предназначенного для студентов, обучающихся по направлению: 10.05.03 Информационная безопасность автоматизированных систем.

В процессе изучения дисциплины формируются компетенции: ОПК-5, ОПК-6, ОПК-14.

Основные положения дисциплины используются в дальнейшем при изучении таких дисциплин как: Системы управления базами данных, Разработка и эксплуатация автоматизированных систем в защищенном исполнении, Научно-исследовательская работа, Организационное и правовое обеспечение информационной безопасности, Базы данных, Проектная деятельность, Подготовка к сдаче и сдача государственного экзамена, Управление информационной безопасностью, Защита информации от утечки по техническим каналам, Ознакомительная практика, Теория информации, Основы информационной безопасности.

## 3. ПЕРЕЧЕНЬ ПЛАНИРУЕМЫХ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ, СООТНЕСЕННЫХ С ПЛАНИРУЕМЫМИ РЕЗУЛЬТАТАМИ ОСВОЕНИЯ ОСНОВНОЙ ПРОФЕССИОНАЛЬНОЙ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

Код и наименование реализуемой компетенции	Перечень планируемых результатов обучения по дисциплине (модулю), соотнесенных с индикаторами достижения компетенций
ОПК-14 Способен осуществлять разработку, внедрение и эксплуатацию автоматизированных систем с учетом требований по защите информации, проводить подготовку исходных данных для технико-экономического обоснования проектных решений;	<p><b>знать:</b> основные угрозы безопасности информации и модели нарушителя в автоматизированных системах</p> <p><b>уметь:</b> осуществлять разработку, внедрение и эксплуатацию автоматизированных систем с учетом требований по защите информации, проводить подготовку исходных данных для технико-экономического обоснования</p>

Код и наименование реализуемой компетенции	Перечень планируемых результатов обучения по дисциплине (модулю), соотнесенных с индикаторами достижения компетенций
	<p>типовых проектных решений</p> <p><b>владеть:</b> навыками осуществления разработки, внедрения и эксплуатации автоматизированных систем с учетом требований по защите информации</p>
<p>ОПК-5 Способен применять нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации;</p>	<p><b>знать:</b> основы российской правовой системы и законодательства, правового статуса личности, организации и деятельности органов государственной власти в Российской Федерации основы законодательства Российской Федерации, нормативные правовые акты, нормативные и методические документы в области информационной безопасности и защиты информации, правовые основы организации защиты государственной тайны и конфиденциальной информации, правовую характеристику преступлений в сфере компьютерной информации и меры правовой и дисциплинарной ответственности за разглашение защищаемой информации правовые основы организации защиты персональных данных и охраны результатов интеллектуальной деятельности</p> <p><b>уметь:</b> обосновывать решения, связанные с реализацией правовых норм по защите информации в пределах должностных обязанностей, предпринимать необходимые меры по восстановлению нарушенных прав анализировать и разрабатывать проекты локальных право-вых актов, инструкций, регламентов и организационно-распорядительных документов, регламентирующих работу по обеспечению информационной безопасности в организации формулировать основные требования при лицензировании деятельности в области защиты информации, сертификации и аттестации по требованиям безопасности информации формулировать основные требования информационной безопасности при эксплуатации автоматизированной системы формулировать основные требования по защите конфиденциальной информации, персональных данных и охране результатов интеллектуальной деятельности в организации</p> <p><b>владеть:</b> навыками применения нормативных правовых актов, нормативных и методических документов, регламентирующих деятельность по защите информации</p>
<p>ОПК-6 Способен при решении профессиональных задач организовывать защиту информации ограниченного доступа в автоматизированных системах в соответствии с нормативными правовыми актами, нормативными и методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю;</p>	<p><b>знать:</b> систему нормативных правовых актов и стандартов по лицензированию в области обеспечения защиты государственной тайны, технической защиты конфиденциальной информации, по аттестации объектов информатизации и сертификации средств защиты информации</p> <p><b>уметь:</b></p>

Код и наименование реализуемой компетенции	Перечень планируемых результатов обучения по дисциплине (модулю), соотнесенных с индикаторами достижения компетенций
	<p>организовывать защиту информации ограниченного доступа в автоматизированных системах в соответствии с нормативными правовыми актами, нормативными и методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю</p> <p><b>владеть:</b> навыками организации защиты информации ограниченного доступа в автоматизированных системах в соответствии с нормативными правовыми актами</p>

#### 4. ОБЩАЯ ТРУДОЕМКОСТЬ ДИСЦИПЛИНЫ

##### 4.1. Объем дисциплины в зачетных единицах (всего): 3 ЗЕТ

##### 4.2. Объем дисциплины по видам учебной работы (в часах): 108 часов

Форма обучения: очная

Вид учебной работы	Количество часов (форма обучения <u>очная</u> )	
	Всего по плану	В т.ч. по семестрам
		5
<b>1</b>	<b>2</b>	<b>3</b>
Контактная работа обучающихся с преподавателем в соответствии с УП	54	54
Аудиторные занятия:	54	54
Лекции	18	18
Семинары и практические занятия	36	36
Лабораторные работы, практикумы	-	-
Самостоятельная работа	54	54
Форма текущего контроля знаний и контроля самостоятельной работы: тестирование, контр. работа, коллоквиум, реферат и др. (не менее 2 видов)	Оценивание реферата, Тестирование	Оценивание реферата, Тестирование
Курсовая работа	-	-
Виды промежуточной аттестации (экзамен, зачет)	Зачет (-18)	Зачет
Всего часов по дисциплине	108	108

##### 4.3. Содержание дисциплины. Распределение часов по темам и видам учебной работы

Форма обучения: очная

Название разделов и тем	Всего	Виды учебных занятий					Форма текущего контроля знаний
		Аудиторные занятия			Занятия в интерактивной форме	Самостоятельная работа	
		Лекции	Практические занятия, семинары	Лабораторные работы, практикумы			
1	2	3	4	5	6	7	8
<b>Раздел 1. Правовое обеспечение информационной безопасности</b>							
Тема 1.1. Информационные отношения как объект правового регулирования. Закон одательства РФ в области информационной безопасности. Правовая охрана результатов интеллектуальной деятельности	12	2	4	0	0	6	Тестирование, Оценивание реферата
Тема 1.2. Правовые режимы защиты коммерческой, профессиональной тайн и служебной информации	12	2	4	0	0	6	Тестирование, Оценивание реферата
Тема 1.3. Законодательство Российской Федерации по вопросам защиты персональных данных	12	2	4	0	0	6	Тестирование, Оценивание реферата

Название разделов и тем	Всего	Виды учебных занятий					Форма текущего контроля знаний
		Аудиторные занятия			Занятия в интерактивной форме	Самостоятельная работа	
		Лекции	Практические занятия, семинары	Лабораторные работы, практикумы			
1	2	3	4	5	6	7	8
Тема 1.4. Государственная система лицензирования и сертификации в области защиты информации	12	2	4	0	0	6	Тестирование, Оценивание реферата
<b>Раздел 2. Организационное обеспечение информационной безопасности</b>							
Тема 2.1. Методы обеспечения физической безопасности. Особенности защиты компьютерной информации	12	2	4	0	0	6	Тестирование, Оценивание реферата
Тема 2.2. Организация режима секретности. Допуск к государственной тайне	12	2	4	0	0	6	Тестирование, Оценивание реферата
<b>Раздел 3. Обеспечение безопасности значимых объектов критической информационной инфраструктуры</b>							
Тема 3.1. Основы обеспечения безопасности объектов критической информационной ин	12	2	4	0	0	6	Тестирование, Оценивание реферата

Название разделов и тем	Всего	Виды учебных занятий					Форма текущего контроля знаний
		Аудиторные занятия			Занятия в интерактивной форме	Самостоятельная работа	
		Лекции	Практические занятия, семинары	Лабораторные работы, практикумы			
1	2	3	4	5	6	7	8
фраструктуры							
Тема 3.2. Организация работ по обеспечению безопасности значимого объекта критической информационной инфраструктуры	12	2	4	0	0	6	Тестирование, Оценивание реферата
Тема 3.3. Контроль за обеспечением безопасности значимого объекта критической информационной инфраструктуры	12	2	4	0	0	6	Тестирование, Оценивание реферата
<b>Итого подлежит изучению</b>	108	18	36	0	0	54	

## 5. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

### Раздел 1. Правовое обеспечение информационной безопасности

#### Тема 1.1. Информационные отношения как объект правового регулирования. Законодательство РФ в области информационной безопасности. Правовая охрана результатов интеллектуальной деятельности

Структура информационной сферы и характеристика ее элементов. Субъекты и объекты правоотношений в области информационной безопасности. Информация как объект

Министерство науки и высшего образования РФ Ульяновский государственный университет Ф – Рабочая программа дисциплины	Форма	
--	-------	--

правоотношений. Категории информации по условиям доступа к ней и распространения. Информация ограниченного доступа. Система нормативных правовых актов, регулирующих обеспечение информационной безопасности в Российской Федерации Понятие и виды защищаемой информации по законодательству РФ. Правовая охрана результатов интеллектуальной деятельности Законодательство РФ об интеллектуальных правах. Понятие и виды интеллектуальных прав. Объекты и субъекты авторского права. Авторские права (личные неимущественные права и исключительное право). Правовая охрана баз данных, топологий интегральных микросхем и единых технологий. Защита интеллектуальных прав. Юридическая ответственность за нарушение авторских прав.

### **Тема 1.2. Правовые режимы защиты коммерческой, профессиональной тайн и служебной информации**

Понятие коммерческой, профессиональной тайн и служебной информации по российскому законодательству. Коммерческая, профессиональная тайны. Служебная тайна. Правовые режимы тайн. Юридическая ответственность за нарушения правовых режимов информации ограниченного доступа (дисциплинарная, гражданско-правовая, административная, уголовная).

### **Тема 1.3. Законодательство Российской Федерации по вопросам защиты персональных данных**

Основные мероприятия по вопросам защиты информации и документы, разрабатываемые на предприятии в соответствии с Федеральным законом РФ «О персональных данных».

### **Тема 1.4. Государственная система лицензирования и сертификации в области защиты информации**

В данной теме рассмотрены основные руководящие документы, определяющие порядок лицензирования и сертификации в области защиты информации, виды деятельности, подлежащие лицензированию, основные принципы и правила системы лицензирования; сертификация средств защиты информации.

## **Раздел 2. Организационное обеспечение информационной безопасности**

### **Тема 2.1. Методы обеспечения физической безопасности. Особенности защиты компьютерной информации**

Объекты обеспечения физической безопасности: сооружения, предметы, люди. Методы и средства технической охраны объектов информатизации. Сигнализация. Противостояние взлому: двери, замки, запоры, ограждения. Безопасность при транспортировке носителей информации. Инженерная защита. Пропускной режим. Особенности защиты компьютерной информации. Технологическая схема обработки информации. Основные каналы утечки информации при обработке на компьютерах. Аппаратные закладки. Виброакустический канал утечки информации. Визуальный канал утечки информации. Программные и аппаратные средства защиты от несанкционированного доступа. Парольная система доступа. Защита на различных уровнях: операционная система, прикладные программы. Программные закладки. Разграничение доступа.

Министерство науки и высшего образования РФ Ульяновский государственный университет Ф – Рабочая программа дисциплины	Форма	
--	-------	--

Регистрация. Остаточная информация. Защита от копирования.

## **Тема 2.2. Организация режима секретности. Допуск к государственной тайне**

Организационные меры, направленные на защиту государственной тайны. Режим секретности как основной порядок деятельности в сфере защиты государственной тайны. Виды представления информации. Пути прохождения информации. Учет получения, перемещения, преобразования, хранения и уничтожения информации. Первые отделы. Категорирование объектов. Подбор и расстановка кадров. Порядок допуска и доступа к государственной тайне. Основные принципы допускной работы. Номенклатура должностей работников, подлежащих оформлению на допуск и порядок ее составления и утверждения. Документальное оформление для отправки на согласование. Процедура оформления и переоформления допусков и ее документирование, подлежащие согласованию с органами государственной безопасности. Особенности инструктажа и документальное оформление контракта об оформлении допуска к государственной тайне. Понятие правового режима защиты государственной тайны. Система нормативных правовых актов, регламентирующих обеспечение сохранности сведений, составляющих государственную тайну в Российской Федерации. Государственная тайна как особый вид защищаемой информации и ее характерные признаки. Принципы и механизмы отнесения сведений к государственной тайне, их засекречивания и рассекречивания. Органы защиты государственной тайны и их компетенция. Система контроля за состоянием защиты государственной тайны.

## **Раздел 3. Обеспечение безопасности значимых объектов критической информационной инфраструктуры**

### **Тема 3.1. Основы обеспечения безопасности объектов критической информационной инфраструктуры**

Правовые основы обеспечения безопасности критической информационной инфраструктуры (КИИ) Российской Федерации. Угрозы безопасности информации, обрабатываемой на объекте КИИ. Анализ угроз безопасности информации и уязвимостей программного обеспечения значимого объекта КИИ с помощью банка данных угроз безопасности информации.

### **Тема 3.2. Организация работ по обеспечению безопасности значимого объекта критической информационной инфраструктуры**

Категорирование объектов КИИ. Требования по обеспечению безопасности значимых объектов КИИ. Система безопасности значимого объекта КИИ. Стадии (этапы) работ по созданию систем безопасности. Выявление управленческих, технологических производственных, финансово-экономических и (или) иных процессов в рамках выполнения функций (полномочий) или осуществления видов деятельности.

### **Тема 3.3. Контроль за обеспечением безопасности значимого объекта критической информационной инфраструктуры**

Разработка документов по результатам внутреннего контроля за обеспечением безопасности значимого объекта КИИ.

Министерство науки и высшего образования РФ Ульяновский государственный университет Ф – Рабочая программа дисциплины	Форма	
--	-------	--

## **6. ТЕМЫ ПРАКТИЧЕСКИХ И СЕМИНАРСКИХ ЗАНЯТИЙ**

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

#### **Тема 1.1. Информационные отношения как объект правового регулирования. Законодательство РФ в области информационной безопасности. Правовая охрана результатов интеллектуальной деятельности**

Вопросы к теме:

Очная форма

1. Информация как объект правоотношений.
2. Виды и содержание тайн.
3. Законодательная база охраны государственной тайны.
4. Законодательная база охраны коммерческой тайны.
5. Законодательная база охраны служебной тайны.
6. Правовая охрана результатов интеллектуальной деятельности.

#### **Тема 1.2. Правовые режимы защиты коммерческой, профессиональной тайн и служебной информации**

Вопросы к теме:

Очная форма

1. Законодательство о коммерческой тайне.
2. Правовые основы защиты служебной тайны.
3. Правовые основы защиты профессиональных тайн.

#### **Тема 1.3. Законодательство Российской Федерации по вопросам защиты персональных данных**

Вопросы к теме:

Очная форма

1. Требования законодательства России по вопросам защиты персональных данных.
2. Основные нормативные документы, разрабатываемые на предприятии по защите персональных данных.

#### **Тема 1.4. Государственная система лицензирования и сертификации в области защиты**

Министерство науки и высшего образования РФ Ульяновский государственный университет Ф – Рабочая программа дисциплины	Форма	
--	-------	--

## **информации**

Вопросы к теме:

Очная форма

1. Основные руководящие документы, определяющие порядок лицензирования и сертификации в области защиты информации.
2. Виды деятельности, подлежащие лицензированию.
3. Основные принципы и правила системы лицензирования:
  - Общие принципы и правила лицензирования;
  - Лицензирование средств криптографической защиты информации
4. Сертификация средств защиты информации

## **Раздел 2. Организационное обеспечение информационной безопасности**

### **Тема 2.1. Методы обеспечения физической безопасности. Особенности защиты компьютерной информации**

Вопросы к теме:

Очная форма

1. Методы и средства технической охраны объектов информатизации.
2. Системы сигнализации. Противостояние взлому: двери, замки, запоры, ограждения.
3. Методы и средства инженерной защиты объектов информатизации.
4. Пропускной режим предприятия.
5. Технологическая схема обработки информации. Основные каналы утечки информации при обработке на компьютерах.

### **Тема 2.2. Организация режима секретности. Допуск к государственной тайне**

Вопросы к теме:

Очная форма

1. Режим секретности как основной порядок деятельности в сфере защиты государственной тайны.
2. Порядок допуска и доступа к государственной тайне.
3. Номенклатура должностей работников, подлежащих оформлению на допуск и порядок ее составления и утверждения.

## **Раздел 3. Обеспечение безопасности значимых объектов критической информационной инфраструктуры**

Министерство науки и высшего образования РФ Ульяновский государственный университет Ф – Рабочая программа дисциплины	Форма	
--	-------	--

### **Тема 3.1. Основы обеспечения безопасности объектов критической информационной инфраструктуры**

Вопросы к теме:

Очная форма

1. Правовые основы обеспечения безопасности критической информационной инфраструктуры (КИИ) Российской Федерации.
2. Угрозы безопасности информации, обрабатываемой на объекте КИИ.
3. Анализ угроз безопасности информации и уязвимостей программного обеспечения значимого объекта КИИ с помощью банка данных угроз безопасности информации.

### **Тема 3.2. Организация работ по обеспечению безопасности значимого объекта критической информационной инфраструктуры**

Вопросы к теме:

Очная форма

1. Категорирование объектов КИИ.
2. Требования по обеспечению безопасности значимых объектов КИИ.
3. Стадии (этапы) работ по созданию систем безопасности.
4. Выявление управленческих, технологических производственных, финансово-экономических и (или) иных процессов в рамках выполнения функций (полномочий) или осуществления видов деятельности.

### **Тема 3.3. Контроль за обеспечением безопасности значимого объекта критической информационной инфраструктуры**

Вопросы к теме:

Очная форма

1. Основные документы по результатам внутреннего контроля за обеспечением безопасности значимого объекта КИИ.
2. Контроль сетевой безопасности (системы обнаружения вторжений и анализа защищенности, сетевые сканеры).
3. Анализ защищенности значимого объекта КИИ на соответствие требованиям по обеспечению безопасности.

## **7. ЛАБОРАТОРНЫЕ РАБОТЫ, ПРАКТИКУМЫ**

Министерство науки и высшего образования РФ Ульяновский государственный университет Ф – Рабочая программа дисциплины	Форма	
--	-------	--

Данный вид работы не предусмотрен УП.

## **8. ТЕМАТИКА КУРСОВЫХ, КОНТРОЛЬНЫХ РАБОТ, РЕФЕРАТОВ**

### **Темы рефератов**

- Тема 1. Законодательство РФ об информационной безопасности
- Тема 2. Требования Федерального закона РФ «Об информации, информационных технологиях и о защите информации»
- Тема 3. Требования Федерального закона РФ «О коммерческой тайне»
- Тема 4. Законодательство РФ в области защиты персональных данных
- Тема 5. Проблемы защиты персональных данных
- Тема 6. Государственная система лицензирования в области защиты информации
- Тема 7. Государственная система сертификации в области защиты информации
- Тема 8. Методы обеспечения физической безопасности объектов информатизации
- Тема 9. Основные каналы утечки информации при обработке на компьютерах
- Тема 10. Программные и аппаратные средства защиты информации от несанкционированного доступа
- Тема 11. Требования Федерального закона РФ «О государственной тайне».
- Тема 12. Допуск к государственной тайне. Мероприятия и документы
- Тема 13. Требования Федерального закона РФ "О безопасности критической информационной инфраструктуры Российской Федерации"
- Тема 14. Правовые основы обеспечения безопасности критической информационной инфраструктуры (КИИ) Российской Федерации
- Тема 15. Анализ угроз безопасности информации и уязвимостей программного обеспечения значимого объекта КИИ с помощью банка данных угроз безопасности информации
- Тема 16. Основные документы по результатам внутреннего контроля за обеспечением безопасности значимого объекта КИИ
- Тема 17. Категорирование объектов КИИ
- Тема 18. Анализ защищенности значимого объекта КИИ на соответствие требованиям по обеспечению безопасности
- Тема 19. Юридическая ответственность за нарушение авторских прав

## **9. ПЕРЕЧЕНЬ ВОПРОСОВ К ЗАЧЕТУ**

1. Информация как объект правоотношений. Законодательство РФ в области информационной безопасности
2. Общие положения в области охраны результатов интеллектуальной деятельности. Авторское право и смежные права
3. Общие положения в области охраны результатов интеллектуальной деятельности. Патентное право. Право на секрет производства (ноу-хау)
4. Юридическая ответственность за нарушение авторских прав

Министерство науки и высшего образования РФ Ульяновский государственный университет	Форма	
Ф – Рабочая программа дисциплины		

5. Виды и содержание тайн. Законодательная база охраны государственной тайны
- 6.
7. Виды и содержание тайн. Законодательная база охраны коммерческой тайны
8. Виды и содержание тайн. Законодательная база охраны служебной тайны
9. Организационные, правовые и технические меры для введения на предприятии режима коммерческой тайны
10. Виды и содержание тайн. Правовые основы защиты профессиональных тайн
11. Порядок предоставления государственным органам сведений, отнесённой к коммерческой тайне предприятия
12. Основные нормативные документы, разрабатываемые на предприятии по защите персональных данных
- 13.
14. Первоочередные мероприятия по созданию системы защиты персональных данных на предприятии
15. Виды и содержание тайн. Законодательная база охраны персональных данных
16. Основные руководящие документы, определяющие порядок лицензирования и сертификации в области защиты информации
17. Виды деятельности, подлежащие лицензированию. Порядок получения лицензии в области защиты информации
18. Сертификация средств защиты информации
19. Методы и средства технической охраны объектов информатизации
20. Системы сигнализации. Противостояние взлому: двери, замки, запоры, ограждения
21. Концепция инженерной защиты и технической охраны объекта
22. Методы и средства инженерной защиты объектов информатизации
23. Основные каналы утечки информации при обработке на компьютерах
24. Виброакустический канал утечки информации. Методы и средства защиты

Министерство науки и высшего образования РФ Ульяновский государственный университет Ф – Рабочая программа дисциплины	Форма	
--	-------	--

25. Визуальный канал утечки информации. Методы и средства защиты
26. Программные и аппаратные средства защиты от несанкционированного доступа
27. Порядок отнесения сведений к государственной тайне
28. Система защиты сведений, составляющих государственную тайну
29. Пропускной режим предприятия
30. Порядок допуска и доступа к государственной тайне
31. Номенклатура должностей работников, подлежащих оформлению на допуск и порядок ее составления и утверждения
32. Правовые основы обеспечения безопасности критической информационной инфраструктуры (КИИ) Российской Федерации
33. Угрозы безопасности информации, обрабатываемой на объекте КИИ
34. Анализ угроз безопасности информации и уязвимостей программного обеспечения значимого объекта КИИ с помощью банка данных угроз безопасности информации
35. Категорирование объектов КИИ. Требования по обеспечению безопасности значимых объектов КИИ
36. Система безопасности значимого объекта КИИ. Стадии (этапы) работ по созданию систем безопасности
37. Основные документы по результатам внутреннего контроля за обеспечением безопасности значимого объекта КИИ

## **10. САМОСТОЯТЕЛЬНАЯ РАБОТА ОБУЧАЮЩИХСЯ**

*Содержание, требования, условия и порядок организации самостоятельной работы обучающихся с учетом формы обучения определяются в соответствии с «Положением об организации самостоятельной работы обучающихся», утвержденным Ученым советом УлГУ (протокол №8/268 от 26.03.2019г.).*

*По каждой форме обучения: очная/заочная/очно-заочная заполняется отдельная таблица*

Форма обучения: очная

Министерство науки и высшего образования РФ Ульяновский государственный университет Ф – Рабочая программа дисциплины	Форма	
--	-------	--

<b>Название разделов и тем</b>	<b>Вид самостоятельной работы (проработка учебного материала, решение задач, реферат, доклад, контрольная работа, подготовка к сдаче зачета, экзамена и др).</b>	<b>Объем в часах</b>	<b>Форма контроля (проверка решения задач, реферата и др.)</b>
<b>Раздел 1. Правовое обеспечение информационной безопасности</b>			
Тема 1.1. Информационные отношения как объект правового регулирования. Законодательство РФ в области информационной безопасности. Правовая охрана результатов интеллектуальной деятельности	Проработка учебного материала с использованием ресурсов учебно-методического и информационного обеспечения дисциплины.	6	Тестирование, Оценивание реферата
Тема 1.2. Правовые режимы защиты коммерческой, профессиональной тайн и служебной информации	Проработка учебного материала с использованием ресурсов учебно-методического и информационного обеспечения дисциплины.	6	Тестирование, Оценивание реферата
Тема 1.3. Законодательство Российской Федерации по вопросам защиты персональных данных	Проработка учебного материала с использованием ресурсов учебно-методического и информационного обеспечения дисциплины.	6	Тестирование, Оценивание реферата
Тема 1.4. Государственная система лицензирования и сертификации в области защиты информации	Проработка учебного материала с использованием ресурсов учебно-методического и информационного обеспечения дисциплины.	6	Тестирование, Оценивание реферата
<b>Раздел 2. Организационное обеспечение информационной безопасности</b>			
Тема 2.1. Методы обеспечения физической безопасности. Особенности защиты компьютерной информации	Проработка учебного материала с использованием ресурсов учебно-методического и информационного обеспечения дисциплины.	6	Тестирование, Оценивание реферата
Тема 2.2. Организация режима секретности. Допуск к государственной тайне	Проработка учебного материала с использованием ресурсов учебно-методического и информационного обеспечения дисциплины.	6	Тестирование, Оценивание реферата
<b>Раздел 3. Обеспечение безопасности значимых объектов критической информационной инфраструктуры</b>			
Тема 3.1. Основы обеспечения безопасности объектов критической информационной инфраструктуры	Проработка учебного материала с использованием ресурсов учебно-методического и информационного обеспечения дисциплины.	6	Тестирование, Оценивание реферата

Министерство науки и высшего образования РФ Ульяновский государственный университет Ф – Рабочая программа дисциплины	Форма	
--	-------	--

Название разделов и тем	Вид самостоятельной работы (проработка учебного материала, решение задач, реферат, доклад, контрольная работа, подготовка к сдаче зачета, экзамена и др).	Объем в часах	Форма контроля (проверка решения задач, реферата и др.)
Тема 3.2. Организация работ по обеспечению безопасности значимого объекта критической информационной инфраструктуры	Проработка учебного материала с использованием ресурсов учебно-методического и информационного обеспечения дисциплины.	6	Тестирование, Оценивание реферата
Тема 3.3. Контроль за обеспечением безопасности значимого объекта критической информационной инфраструктуры	Проработка учебного материала с использованием ресурсов учебно-методического и информационного обеспечения дисциплины.	6	Тестирование, Оценивание реферата

## 11. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

### а) Список рекомендуемой литературы

#### основная

1. Суворова Галина Михайловна. Информационная безопасность : учебное пособие для вузов / Г.М. Суворова ; Г. М. Суворова. - Москва : Юрайт, 2023. - 253 с. - (Высшее образование). - URL: <https://urait.ru/bcode/519780> (дата обращения: 10.02.2023). - Режим доступа: Электронно-библиотечная система Юрайт, для авториз. пользователей. - Электрон. дан. - ISBN 978-5-534-13960-0 : 1039.00. / .— ISBN 0\_490325

2. Гродзенский Я.С. Информационная безопасность : учебное пособие / Я.С. Гродзенский ; Гродзенский Я.С. - Москва : РГ-Пресс, 2020. - 144 с. - URL: <https://www.studentlibrary.ru/book/ISBN9785998808456.html>. - Режим доступа: ЭБС "Консультант студента"; по подписке. - ISBN 978-5-9988-0845-6. / .— ISBN 0\_260443

#### дополнительная

1. Доктрина информационной безопасности Российской Федерации (Указ Президента РФ от 05.12.2016 N 646 "Об утверждении Доктрины информационной безопасности Российской Федерации"). - URL: [http://www.consultant.ru/document/cons\\_doc\\_LAW\\_208191/](http://www.consultant.ru/document/cons_doc_LAW_208191/). - Режим доступа: СПС Консультант Плюс. - Текст : электронный. / .— ISBN 0\_476279

2. Федеральный закон от 27.07.2006 № 152-ФЗ "О персональных данных". - URL: [http://www.consultant.ru/document/cons\\_doc\\_LAW\\_61801](http://www.consultant.ru/document/cons_doc_LAW_61801). - Режим доступа: Некоммерческая интернет-версия СПС Консультант Плюс. - Текст : электронный. / .— ISBN 0\_476252

3. Федеральный закон от 29.07.2004 № 98-ФЗ "О коммерческой тайне". - URL: [http://www.consultant.ru/document/cons\\_doc\\_LAW\\_48699](http://www.consultant.ru/document/cons_doc_LAW_48699). - Режим доступа: Некоммерческая

Министерство науки и высшего образования РФ Ульяновский государственный университет Ф – Рабочая программа дисциплины	Форма	
--	-------	--

интернет-версия СПС Консультант Плюс. - Текст : электронный. / .— ISBN 0\_476253

4. Федеральный закон "О безопасности критической информационной инфраструктуры Российской Федерации" от 26.07.2017 N 187-ФЗ. - URL: [http://www.consultant.ru/document/cons\\_doc\\_LAW\\_220885/](http://www.consultant.ru/document/cons_doc_LAW_220885/). - Режим доступа: СПС Консультант Плюс. - Текст : электронный. / .— ISBN 0\_476631

5. Галатенко В.А. Стандарты информационной безопасности : учебник / В.А. Галатенко ; Галатенко В.А. - Москва : ИНТУИТ, 2016. - . - URL: <https://www.studentlibrary.ru/book/ISBN5955600531.html>. - Режим доступа: ЭБС "Консультант студента"; по подписке. - ISBN 5-9556-0053-1. / .— ISBN 0\_257176

### **учебно-методическая**

1. Иванцов А. М. Методические указания для самостоятельной работы студентов по дисциплине «Организационное и правовое обеспечение информационной безопасности» для студентов специалитета по специальностям 10.05.01 и 10.05.03 очной формы обучения / А. М. Иванцов ; УлГУ, Фак. математики, информ. и авиац. технологий. - 2020. - Загл. с экрана. - Неопубликованный ресурс. - Электрон. текстовые дан. (1 файл : 329 КБ). - Режим доступа: ЭБС УлГУ. - Текст : электронный. / .— ISBN 0\_37895.

### **б) Программное обеспечение**

- Операционная система "Альт образование"
- Офисный пакет "Мой офис"

### **в) Профессиональные базы данных, информационно-справочные системы**

#### **1. Электронно-библиотечные системы:**

1.1. Цифровой образовательный ресурс IPRsmart : электронно-библиотечная система : сайт / ООО Компания «Ай Пи Ар Медиа». - Саратов, [2024]. – URL: <http://www.iprbookshop.ru>. – Режим доступа: для зарегистрир. пользователей. - Текст : электронный.

1.2. Образовательная платформа ЮРАЙТ : образовательный ресурс, электронная библиотека : сайт / ООО Электронное издательство ЮРАЙТ. – Москва, [2024]. - URL: <https://urait.ru>. – Режим доступа: для зарегистрир. пользователей. - Текст : электронный.

1.3. База данных «Электронная библиотека технического ВУЗа (ЭБС «Консультант студента») : электронно-библиотечная система : сайт / ООО Политехресурс. – Москва, [2024]. – URL: <https://www.studentlibrary.ru/cgi-bin/mb4x>. – Режим доступа: для зарегистрир. пользователей. – Текст : электронный.

1.4. Консультант врача. Электронная медицинская библиотека : база данных : сайт / ООО Высшая школа организации и управления здравоохранением-Комплексный медицинский консалтинг. – Москва, [2024]. – URL: <https://www.rosmedlib.ru>. – Режим доступа: для зарегистрир. пользователей. – Текст : электронный.

Министерство науки и высшего образования РФ Ульяновский государственный университет Ф – Рабочая программа дисциплины	Форма	
--	-------	--

1.5. Большая медицинская библиотека : электронно-библиотечная система : сайт / ООО Букап. – Томск, [2024]. – URL: <https://www.books-up.ru/ru/library/> . – Режим доступа: для зарегистрир. пользователей. – Текст : электронный.

1.6. ЭБС Лань : электронно-библиотечная система : сайт / ООО ЭБС Лань. – Санкт-Петербург, [2024]. – URL: <https://e.lanbook.com>. – Режим доступа: для зарегистрир. пользователей. – Текст : электронный.

1.7. ЭБС **Znanium.com** : электронно-библиотечная система : сайт / ООО Знаниум. - Москва, [2024]. - URL: <http://znanium.com> . – Режим доступа : для зарегистрир. пользователей. - Текст : электронный.

**2. КонсультантПлюс** [Электронный ресурс]: справочная правовая система. /ООО «Консультант Плюс» - Электрон. дан. - Москва : КонсультантПлюс, [2024].

**3. eLIBRARY.RU:** научная электронная библиотека : сайт / ООО «Научная Электронная Библиотека». – Москва, [2024]. – URL: <http://elibrary.ru>. – Режим доступа : для авториз. пользователей. – Текст : электронный

**4. Федеральная государственная информационная система «Национальная электронная библиотека» :** электронная библиотека : сайт / ФГБУ РГБ. – Москва, [2024]. – URL: <https://нэб.рф>. – Режим доступа : для пользователей научной библиотеки. – Текст : электронный.

**5. Российское образование :** федеральный портал / учредитель ФГАУ «ФИЦТО». – URL: <http://www.edu.ru>. – Текст : электронный.

**6. Электронная библиотечная система УлГУ :** модуль «Электронная библиотека» АБИС Мега-ПРО / ООО «Дата Экспресс». – URL: <http://lib.ulsu.ru/MegaPro/Web>. – Режим доступа : для пользователей научной библиотеки. – Текст : электронный.

## 12. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ:

Аудитории для проведения лекций, семинарских занятий, для выполнения лабораторных работ и практикумов, для проведения текущего контроля и промежуточной аттестации, курсового проектирования, групповых и индивидуальных консультаций (*выбрать необходимое*)

Аудитории укомплектованы специализированной мебелью, учебной доской. Аудитории для проведения лекций оборудованы мультимедийным оборудованием для представления информации большой аудитории. Помещения для самостоятельной работы оснащены компьютерной техникой с возможностью подключения к сети «Интернет» и обеспечением доступа к электронной информационно-образовательной среде, электронно-библиотечной системе. Перечень оборудования, используемого в учебном процессе:

- Мультимедийное оборудование: компьютер/ноутбук, экран, проектор/телевизор
- Компьютерная техника

Министерство науки и высшего образования РФ Ульяновский государственный университет Ф – Рабочая программа дисциплины	Форма	
--	-------	--

### **13. СПЕЦИАЛЬНЫЕ УСЛОВИЯ ДЛЯ ОБУЧАЮЩИХСЯ С ОГРАНИЧЕННЫМИ ВОЗМОЖНОСТЯМИ ЗДОРОВЬЯ**

В случае необходимости, обучающимся из числа лиц с ограниченными возможностями здоровья (по заявлению обучающегося) могут предлагаться одни из следующих вариантов восприятия информации с учетом их индивидуальных психофизических особенностей:

- для лиц с нарушениями зрения: в печатной форме увеличенным шрифтом; в форме электронного документа; в форме аудиофайла (перевод учебных материалов в аудиоформат); в печатной форме на языке Брайля; индивидуальные консультации с привлечением тифлосурдопереводчика; индивидуальные задания и консультации;

- для лиц с нарушениями слуха: в печатной форме; в форме электронного документа; видеоматериалы с субтитрами; индивидуальные консультации с привлечением сурдопереводчика; индивидуальные задания и консультации;

- для лиц с нарушениями опорно-двигательного аппарата: в печатной форме; в форме электронного документа; в форме аудиофайла; индивидуальные задания и консультации.

В случае необходимости использования в учебном процессе частично/исключительно дистанционных образовательных технологий, организация работы ППС с обучающимися с ОВЗ и инвалидами предусматривается в электронной информационно-образовательной среде с учетом их индивидуальных психофизических особенностей.

Разработчик	Доцент, Кандидат технических наук, Доцент	Иванцов Андрей Михайлович
	Должность, ученая степень, звание	ФИО