

**Министерство науки и высшего образования РФ**  
**Федеральное государственное бюджетное образовательное учреждение**  
**высшего образования**  
**«Национальный исследовательский университет «МЭИ»**

---

Направление подготовки/специальность: 10.04.01 Информационная безопасность

Наименование образовательной программы: Управление информационной безопасностью

Уровень образования: высшее образование - магистратура

Форма обучения: Очная

**Рабочая программа дисциплины**  
**ОРГАНИЗАЦИОННО-ПРАВОВЫЕ МЕХАНИЗМЫ ОБЕСПЕЧЕНИЯ**  
**ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ**

<b>Блок:</b>	Блок 1 «Дисциплины (модули)»
<b>Часть образовательной программы:</b>	Обязательная
<b>№ дисциплины по учебному плану:</b>	Б1.О.08
<b>Трудоемкость в зачетных единицах:</b>	2 семестр - 5;
<b>Часов (всего) по учебному плану:</b>	180 часов
<b>Лекции</b>	2 семестр - 32 часа;
<b>Практические занятия</b>	2 семестр - 48 часа;
<b>Лабораторные работы</b>	не предусмотрено учебным планом
<b>Консультации</b>	2 семестр - 18 часов;
<b>Самостоятельная работа</b>	2 семестр - 77,2 часа;
<b>в том числе на КП/КР</b>	2 семестр - 19,7 часов;
<b>Иная контактная работа</b>	2 семестр - 4 часа;
<b>включая:</b> Контрольная работа Решение задач Семинар	
<b>Промежуточная аттестация:</b>	
<b>Защита курсовой работы</b>	2 семестр - 0,4 часа;
<b>Экзамен</b>	2 семестр - 0,4 часа; всего - 0,8 часа

**Москва 2023**

**ПРОГРАММУ СОСТАВИЛ:**

Преподаватель

	Подписано электронной подписью ФГБОУ ВО «НИУ «МЭИ»	
	Сведения о владельце ЦЭП МЭИ	
	Владелец	Туркина А.А.
	Идентификатор	R9001f342-TurkinaAA-3bcc47d9

А.А. Туркина

**СОГЛАСОВАНО:**

Руководитель  
образовательной программы

	Подписано электронной подписью ФГБОУ ВО «НИУ «МЭИ»	
	Сведения о владельце ЦЭП МЭИ	
	Владелец	Минзов А.С.
	Идентификатор	R17801759-MinzovAS-e8de8907

А.С. Минзов

Заведующий выпускающей  
кафедрой

	Подписано электронной подписью ФГБОУ ВО «НИУ «МЭИ»	
	Сведения о владельце ЦЭП МЭИ	
	Владелец	Невский А.Ю.
	Идентификатор	R4bc65573-NevskyAY-0b6e493d

А.Ю. Невский

## 1. ЦЕЛИ И ЗАДАЧИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

**Цель освоения дисциплины:** формирование у обучаемых знаний о закономерностях функционирования и развития государственной системы информационной безопасности, о системе российского права и его отраслей, которые регулируют вопросы информационной безопасности с последующим применением этих знаний в профессиональной сфере и практических навыков по формированию способности человека правовыми средствами решать те или иные профессиональные задачи

### Задачи дисциплины

- изучение закономерностей функционирования и развития государственной системы информационной безопасности;;
- изучение структуры системы российского права и его отраслей, которые регулируют вопросы информационной безопасности..

Формируемые у обучающегося **компетенции** и запланированные **результаты обучения** по дисциплине, соотнесенные с **индикаторами достижения компетенций**:

Код и наименование компетенции	Код и наименование индикатора достижения компетенции	Запланированные результаты обучения
ОПК-3 Способен разрабатывать организационно-распорядительные документы по обеспечению информационной безопасности	ИД-1 <sub>оПК-3</sub> Организует работу по созданию или модернизации систем, средств и технологий обеспечения информационной безопасности в соответствии с правовыми нормативными актами и нормативными методическими документами ФСБ России, ФСТЭК России	знать: - структуру, задачи и функции органов, регулирующих деятельность объектов и субъектов в сфере ИБ; - методику анализа нормативно-правовых актов при организации системы ИБ; - технологи работы с правовыми базами данных в профессиональных ситуациях в сфере информационной безопасности.

## 2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ ВО

Дисциплина относится к основной профессиональной образовательной программе Управление информационной безопасностью (далее – ОПОП), направления подготовки 10.04.01 Информационная безопасность, уровень образования: высшее образование - магистратура.

Требования к входным знаниям и умениям:

- знать Дисциплина базируется на следующих дисциплинах бакалавриата: «Основы информационной безопасности», «Организационное и правовое обеспечение информационной безопасности».

Результаты обучения, полученные при освоении дисциплины, необходимы при выполнении выпускной квалификационной работы.

### 3. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

#### 3.1 Структура дисциплины

Общая трудоемкость дисциплины составляет 5 зачетных единиц, 180 часов.

№ п/п	Разделы/темы дисциплины/формы промежуточной аттестации	Всего часов на раздел	Семестр	Распределение трудоемкости раздела (в часах) по видам учебной работы										Содержание самостоятельной работы/ методические указания	
				Контактная работа							СР				
				Лек	Лаб	Пр	Консультация		ИКР		ПА	Работа в семестре	Подготовка к аттестации /контроль		
КПР	ГК	ИККП	ТК												
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	
1	Правовое обеспечение информационной безопасности Российской Федерации. Основные функции государственных органов в области информационной безопасности	18	2	6	-	8	-	-	-	-	-	4	-	<b><u>Изучение материалов литературных источников:</u></b> [1], 1-344	
1.1	Правовое обеспечение информационной безопасности Российской Федерации	8		2	-	4	-	-	-	-	-	2	-		
1.2	Основные функции государственных органов в области информационной безопасности	10		4	-	4	-	-	-	-	-	2	-		
2	Организация защиты информации на предприятии. Разработка системы защиты информации предприятия	18		6	-	8	-	-	-	-	-	4	-		<b><u>Изучение материалов литературных источников:</u></b> [1], 1-344
2.1	Организация защиты информации на	8		2	-	4	-	-	-	-	-	2	-		

	предприятия.													
2.2	Разработка системы защиты информации предприятия	10	4	-	4	-	-	-	-	-	2	-		
3	Особенности организации работы с персоналом и контрагентами	16	4	-	8	-	-	-	-	-	4	-	<b><u>Изучение материалов литературных источников:</u></b> [1], 1-344	
3.1	Особенности организации работы с персоналом	8	2	-	4	-	-	-	-	-	2	-		
3.2	Особенности организации работы с контрагентами	8	2	-	4	-	-	-	-	-	2	-		
4	Юридическая ответственность субъектов информационной сферы. Расследование инцидентов информационной безопасности на предприятии	24	6	-	12	-	-	-	-	-	6	-		<b><u>Изучение материалов литературных источников:</u></b> [2], 1-124
4.1	Порядок и особенности применения уголовной ответственности за преступления в области информационной безопасности	8	2	-	4	-	-	-	-	-	2	-		
4.2	Порядок и особенности применения административной ответственности за проступки в области информационной	8	2	-	4	-	-	-	-	-	2	-		

	безопасности												
4.3	Порядок и особенности применения гражданско-правовой и дисциплинарной ответственности	8	2	-	4	-	-	-	-	-	2	-	
5	Правовое регулирование отдельных видов информации: государственная тайна, служебная информация, профессиональная тайна и т.д.	28	10	-	12	-	-	-	-	-	6	-	<i><u>Изучение материалов литературных источников:</u></i> [2], 1-124
5.1	Законодательство в области государственной тайны.	10	4	-	4	-	-	-	-	-	2	-	
5.2	Законодательство в области служебной и коммерческой тайны	8	2	-	4	-	-	-	-	-	2	-	
5.3	Правовое регулирование иных видов конфиденциальной информации	10	4	-	4	-	-	-	-	-	2	-	
	Экзамен	35.9	-	-	-	-	2	-	-	0.4	-	33.5	
	Курсовая работа (КР)	40.1	-	-	-	16	-	4	-	0.4	19.7	-	
	<b>Всего за семестр</b>	<b>180.0</b>	<b>32</b>	<b>-</b>	<b>48</b>	<b>16</b>	<b>2</b>	<b>4</b>	<b>-</b>	<b>0.8</b>	<b>43.7</b>	<b>33.5</b>	
	<b>Итого за семестр</b>	<b>180.0</b>	<b>32</b>	<b>-</b>	<b>48</b>	<b>18</b>		<b>4</b>		<b>0.8</b>	<b>77.2</b>		

**Примечание:** Лек – лекции; Лаб – лабораторные работы; Пр – практические занятия; КПП – аудиторные консультации по курсовым проектам/работам; ИККП – индивидуальные консультации по курсовым проектам/работам; ГК- групповые консультации по разделам дисциплины; СР – самостоятельная работа студента; ИКР – иная контактная работа; ТК – текущий контроль; ПА – промежуточная аттестация

### **3.2 Краткое содержание разделов**

#### 1. Правовое обеспечение информационной безопасности Российской Федерации. Основные функции государственных органов в области информационной безопасности

##### 1.1. Правовое обеспечение информационной безопасности Российской Федерации

Основные термины и определения в сфере правового обеспечения ИБ. Анализ нормативных источников и литературы по дисциплине. Понятие информации и правового обеспечения защиты информации (информационного права). Предмет, методы информационного права и его место в системе российского права. Содержание и структура законодательства в области информационной безопасности. Структура нормативно-правовых актов, регулирующих деятельность в сфере ИБ..

##### 1.2. Основные функции государственных органов в области информационной безопасности

Понятие механизма правового регулирования. Элементы механизма правового регулирования. Реализация механизмов правового регулирования в области информационной безопасности. Понятие обладателя информации. Общедоступная информация и информация ограниченного доступа. Правила распространения или предоставления информации..

#### 2. Организация защиты информации на предприятии. Разработка системы защиты информации предприятия

##### 2.1. Организация защиты информации на предприятии.

Понятие сертификации. Нормативные правовые акты Российской Федерации и национальные стандарты, регламентирующие порядок проведения сертификации средств защиты информации и использования технических средств защиты информации. Выбор средств защиты информации для обеспечения безопасности объектов информатизации. Понятие аттестации объектов информатизации. Порядок проведения аттестации объектов информатизации. Другие виды оценки соответствия объектов информатизации..

##### 2.2. Разработка системы защиты информации предприятия

Реализация механизмов правового регулирования при формировании системы защиты информации на предприятии. Организация пропускного режима. Организация внутриобъектового режима. Выявление и определение объектов информатизации, обрабатывающих информацию ограниченного доступа на предприятии. Обеспечение конфиденциальности информации при проведении заседаний, совещаний, переговоров..

#### 3. Особенности организации работы с персоналом и контрагентами

##### 3.1. Особенности организации работы с персоналом

Анализ реализации правовых механизмов воздействия на работников предприятия при реализации требований в области ИБ. Регулирование отношений по использованию информации ограниченного доступа с работниками организации. Обязанности работодателя по охране конфиденциальности информации в рамках трудовых отношений. Обязанности работников, получивших доступ к документам, содержащим информацию ограниченного доступа. Учёт лиц, получивших доступ к информации. Особенности оформления трудовых и гражданско-правовых отношений с лицами, получающими доступ к информации. Порядок проведения служебных расследований. Особенности определения взысканий при выявлении нарушений в области информационной безопасности..

### 3.2. Особенности организации работы с контрагентами

Особенности отражения требований по защите информации в гражданско-правовых договорах с клиентами и контрагентами. Порядок согласования общего режима конфиденциальности информации между несколькими организациями. Особенности организации и проведения переписки, содержащей конфиденциальную информацию..

## 4. Юридическая ответственность субъектов информационной сферы. Расследование инцидентов информационной безопасности на предприятии

### 4.1. Порядок и особенности применения уголовной ответственности за преступления в области информационной безопасности

Правовые механизмы привлечения к ответственности за нарушение требований в области ИБ. Понятие юридической ответственности. Правосстановительная ответственность. Публичная и частная ответственность. Уголовная ответственность. Порядок применения уголовной ответственности на территории РФ. Виды наказаний в УК РФ. Состав преступления: объект, субъект, объективная и субъективная сторона. Мотив к совершению преступления как важная часть для квалификации деяния. Основные составы преступлений в области информационной безопасности..

### 4.2. Порядок и особенности применения административной ответственности за проступки в области информационной безопасности

Административная ответственность. Порядок применения административной ответственности. Виды наказаний в КоАП РФ. Административная ответственность по законодательству субъектов РФ. Понятие длящегося правонарушения, неоднократность совершения административных правонарушений. Сроки в КоАП РФ. Основные составы административных правонарушений в области информационной безопасности..

### 4.3. Порядок и особенности применения гражданско-правовой и дисциплинарной ответственности

Гражданско-правовая ответственность. Порядок компенсации имущественного (реального) и морального вреда. Порядок оценки причиненного вреда. Дисциплинарная ответственность. Виды ответственности по трудовому законодательству. Порядок применения ответственности к работникам предприятия. Материальная ответственность..

## 5. Правовое регулирование отдельных видов информации: государственная тайна, служебная информация, профессиональная тайна и т.д.

### 5.1. Законодательство в области государственной тайны.

Основные понятия и определения в области государственной тайны. Принципы отнесения сведений к государственной тайне и засекречивания этих сведений. Перечень сведений, составляющих государственную тайну. Сведения, подлежащие отнесению к государственной тайне и засекречиванию. Степени секретности сведений и грифы секретности носителей этих сведений. Реквизиты носителей сведений, составляющих государственную тайну. Порядок и правила отнесения сведений, составляющих государственную тайну, к различным степеням секретности. Перечни сведений в области государственной тайны. Порядок засекречивания сведений и их носителей. Проведение проверки наличия в заявках на выдачу патента на изобретение или полезную модель, сведений, составляющих государственную тайну. Порядок рассекречивания сведений. Взаимная передача сведений, составляющих государственную тайну, органами государственной власти, предприятиями, учреждениями и организациями..



## 5.2. Законодательство в области служебной и коммерческой тайны

Понятие служебной тайны. Порядок допуска сотрудников к информации, составляющей служебную тайну. Порядок учета, хранения документов категории «Для служебного пользования» и обеспечения ограничений к их доступу..

## 5.3. Правовое регулирование иных видов конфиденциальной информации

Законодательство в области профессиональной тайны. Понятие профессиональной тайны. Виды профессиональных тайн. Порядок доступа к различным видам профессиональных тайн. Правовое регулирование персональных данных. Правовое регулирование защиты информации на объектах КИИ.

### 3.3. Темы практических занятий

1. Правовое регулирование отдельных видов защищаемой информации и ответственность за нарушение требований законодательства в области информационной безопасности;
2. Разработка системы защиты информации на предприятии и отдельных видов корпоративных документов в области информационной безопасности;
3. Основные организационно-правовые акты Российской Федерации в области информационной безопасности и функции государственных органов.

### 3.4. Темы лабораторных работ

не предусмотрено

### 3.5 Консультации

### 3.6 Тематика курсовых проектов/курсовых работ

#### 2 Семестр

Курсовая работа (КР)

Темы:

1. Обзор нормативных актов, регулирующих правовые основы защиты информации в организации
2. Анализ правовых основ применения сертифицированных средств защиты информации
3. Особенности и порядок разработки организационно-распорядительных документов, устанавливающих режим обработки персональных данных в организации
4. Особенности и порядок разработки организационно-распорядительных документов, устанавливающих режим обработки банковской тайны
5. Особенности и порядок разработки организационно-распорядительных документов, устанавливающих режим обработки информации в государственной информационной системе
6. Особенности и порядок разработки организационно-распорядительных документов, устанавливающих режим обработки информации на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды
7. Организация и порядок допуска персонала к сведениям конфиденциального характера, а также особенности и основания прекращения допуска персонала к конфиденциальной информации
8. Разработка методики реагирования на запросы государственных органов о предоставлении информации
9. Порядок и особенности регулирования использования информационно-телекоммуникационных сетей в организации
10. Анализ правовых основ ограничения доступа к информации, а также порядок реализации ограничения доступа к информации в организации
11. Сравнительный анализ методик определения численности подразделений информационной безопасности, организация подразделения по информационной безопасности
12. Механизмы реализации вопросов защиты конфиденциальной информации в договорных отношениях
13. Особенности организации и обеспечения безопасности при работе со средствами криптографической

защиты информации, не составляющей государственную тайну 14. Особенности организации применения электронной подписи в организации для внутреннего и внешнего электронного документооборота 15. Особенности организации обработки и хранения информации с использованием виртуальных инфраструктур 16. Порядок подтверждения и расследования инцидентов информационной безопасности 17. Организация подтверждения соответствия объекта информатизации требованиям в области информационной безопасности 18. Особенности и методика проведения подготовительных мероприятий заказчиком по аттестации объекта информатизации 19. Разработка и внедрение системы защиты от несанкционированного доступа к информации ограниченного доступа в организации (организационные аспекты) 20. Организация системы резервирования и восстановления информации, формирование плана реагирования на возникновение чрезвычайных ситуаций (в части сохранности конфиденциальной информации) 21. Методика организации хранения, уничтожения и выдачи отчуждаемых носителей конфиденциальной информации 22. Особенности подготовки к лицензированию ФСТЭК России по технической защите конфиденциальной информации (или разработке и производству средств защиты информации. 23. Особенности подготовки к лицензированию ФСБ России по деятельности по разработке, производству, распространению шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств 24. Порядок разработки в организации технического задания на комплексную систему защиты информации 25. Анализ видов ответственности и порядок ее применения за правонарушения в сфере информации, информационных технологий и защиты информации

#### **График выполнения курсового проекта**

Неделя	1 - 4	5 - 8	9 - 12	Зачетная
Раздел курсового проекта	1	2	3	Защита курсового проекта
Объем раздела, %	30	30	40	-
Выполненный объем нарастающим итогом, %	30	60	100	-

Номер раздела	Раздел курсового проекта
1	Введение, Глава 1
2	Глава 2
3	Глава 3, Заключение, Список литературы

### 3.7. Соответствие разделов дисциплины и формируемых в них компетенций

Запланированные результаты обучения по дисциплине (в соответствии с разделом 1)	Коды индикаторов	Номер раздела дисциплины (в соответствии с п.3.1)					Оценочное средство (тип и наименование)
		1	2	3	4	5	
<b>Знать:</b>							
технологии работы с правовыми базами данных в профессиональных ситуациях в сфере информационной безопасности	ИД-1опк-3					+	Семинар/Правовое регулирование отдельных видов защищаемой информации и ответственность за нарушение требований законодательства в области информационной безопасности  Семинар/Правовое регулирование отдельных видов информации: государственная тайна, служебная информация, профессиональная тайна и т.д.
методику анализа нормативно-правовых актов при организации системы ИБ	ИД-1опк-3		+	+			Контрольная работа/Правовое обеспечение информационной безопасности Российской Федерации. Основные функции государственных органов в области информационной безопасности  Решение задач/Разработка системы защиты информации на предприятии и отдельных видов корпоративных документов в области информационной безопасности
структуру, задачи и функции органов, регулирующих деятельность объектов и субъектов в сфере ИБ	ИД-1опк-3	+				+	Контрольная работа/Правовое обеспечение информационной безопасности Российской Федерации. Основные функции государственных органов в области информационной безопасности  Семинар/Правовое регулирование отдельных видов защищаемой информации и ответственность за нарушение требований законодательства в области информационной безопасности

#### **4. КОМПЕТЕНТНОСТНО-ОРИЕНТИРОВАННЫЕ ОЦЕНОЧНЫЕ СРЕДСТВА ДЛЯ КОНТРОЛЯ ОСВОЕНИЯ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ (ТЕКУЩИЙ КОНТРОЛЬ УСПЕВАЕМОСТИ, ПРОМЕЖУТОЧНАЯ АТТЕСТАЦИЯ ПО ДИСЦИПЛИНЕ)**

##### **4.1. Текущий контроль успеваемости**

**2 семестр**

Форма реализации: Защита задания

1. Правовое регулирование отдельных видов защищаемой информации и ответственность за нарушение требований законодательства в области информационной безопасности (Семинар)
2. Правовое регулирование отдельных видов информации: государственная тайна, служебная информация, профессиональная тайна и т.д. (Семинар)

Форма реализации: Письменная работа

1. Правовое обеспечение информационной безопасности Российской Федерации. Основные функции государственных органов в области информационной безопасности (Контрольная работа)

Форма реализации: Проверка задания

1. Разработка системы защиты информации на предприятии и отдельных видов корпоративных документов в области информационной безопасности (Решение задач)

Балльно-рейтинговая структура дисциплины является приложением А.

Балльно-рейтинговая структура курсовой работы является приложением Б.

##### **4.2 Промежуточная аттестация по дисциплине**

Экзамен (Семестр №2)

При формировании итоговой оценки учитывается как результат ответа на экзамене, так и текущая успеваемость студента

Курсовая работа (КР) (Семестр №2)

При выставлении итоговой оценки учитывается выполнение графика написания работы, содержание и оформление работы, а также качества доклада и умение студента аргументированно отстаивать свою точку зрения.

В диплом выставляется оценка за 2 семестр.

**Примечание:** Оценочные материалы по дисциплине приведены в фонде оценочных материалов ОПОП.

#### **5. УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ**

##### **5.1 Печатные и электронные издания:**

1. Тумбинская М. В., Петровский М. В. - "Комплексное обеспечение информационной безопасности на предприятии", Издательство: "Лань", Санкт-Петербург, 2019 - (344 с.)  
<https://e.lanbook.com/book/125739>;
2. Прохорова О. В. - "Информационная безопасность и защита информации", (3-е изд., стер.), Издательство: "Лань", Санкт-Петербург, 2021 - (124 с.)  
<https://e.lanbook.com/book/169817>.

## 5.2 Лицензионное и свободно распространяемое программное обеспечение:

1. СДО "Прометей";
2. Office / Российский пакет офисных программ;
3. Windows / Операционная система семейства Linux;
4. Видеоконференции (Майнд, Сберджаз, ВК и др).

## 5.3 Интернет-ресурсы, включая профессиональные базы данных и информационно-справочные системы:

1. ЭБС Лань - <https://e.lanbook.com/>
2. Электронная библиотека МЭИ (ЭБ МЭИ) - <http://elib.mpei.ru/login.php>
3. Портал открытых данных Российской Федерации - <https://data.gov.ru>
4. Информационно-справочная система «Кодекс/Техэксперт» - <Http://proinfosoft.ru;>  
<http://docs.cntd.ru/>
5. Открытая университетская информационная система «РОССИЯ» - <https://uisrussia.msu.ru>

## 6. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Тип помещения	Номер аудитории, наименование	Оснащение
Учебные аудитории для проведения лекционных занятий и текущего контроля	М-511, Учебная аудитория	парта, стол преподавателя, стул, мультимедийный проектор, экран, доска маркерная, компьютер персональный
	К-601, Учебная аудитория	парта со скамьей, стол преподавателя, стул, трибуна, доска меловая, мультимедийный проектор, экран
Учебные аудитории для проведения практических занятий, КР и КП	М-510, Учебная лаборатория информационно-аналитический технологий - компьютерный класс	стул, стол письменный, мультимедийный проектор, экран, доска маркерная, компьютер персональный, кондиционер
Учебные аудитории для проведения промежуточной аттестации	М-511, Учебная аудитория	парта, стол преподавателя, стул, мультимедийный проектор, экран, доска маркерная, компьютер персональный
	Ж-120, Машинный зал ИВЦ	сервер, кондиционер
Помещения для самостоятельной работы	НТБ-201, Компьютерный читальный зал	стол компьютерный, стул, стол письменный, вешалка для одежды, компьютерная сеть с выходом в Интернет, компьютер персональный, принтер, кондиционер
	К-307, Учебная лаборатория "Открытое программное обеспечение"	стол преподавателя, стол компьютерный, стол учебный, стул, вешалка для одежды, тумба, компьютерная сеть с выходом в Интернет, мультимедийный проектор, экран, доска маркерная, сервер, компьютер персональный, кондиционер

	К-302, Учебная лаборатория "Информационно-аналитические технологии"	стол преподавателя, стол компьютерный, стул, мультимедийный проектор, экран, доска маркерная, сервер, компьютер персональный, кондиционер
Помещения для консультирования	М-510, Учебная лаборатория информационно-аналитический технологий - компьютерный класс	стул, стол письменный, мультимедийный проектор, экран, доска маркерная, компьютер персональный, кондиционер
Помещения для хранения оборудования и учебного инвентаря	К-202/2, Склад кафедры БИТ	стеллаж для хранения инвентаря, стол, стул, шкаф для документов, шкаф для хранения инвентаря, тумба, запасные комплектующие для оборудования

## БАЛЛЬНО-РЕЙТИНГОВАЯ СТРУКТУРА ДИСЦИПЛИНЫ

### Организационно-правовые механизмы обеспечения информационной безопасности

(название дисциплины)

#### 2 семестр

**Перечень контрольных мероприятий текущего контроля успеваемости по дисциплине:**

- КМ-1 Правовое обеспечение информационной безопасности Российской Федерации. Основные функции государственных органов в области информационной безопасности (Контрольная работа)
- КМ-2 Разработка системы защиты информации на предприятии и отдельных видов корпоративных до-кументов в области информационной безопасности (Решение задач)
- КМ-3 Правовое регулирование отдельных видов защищаемой информации и ответственность за нарушение требований законодательства в области информационной безопасности (Семинар)
- КМ-4 Правовое регулирование отдельных видов информации: государственная тайна, служебная информация, профессиональная тайна и т.д. (Семинар)

**Вид промежуточной аттестации – Экзамен.**

Номер раздела	Раздел дисциплины	Индекс КМ:	КМ-1	КМ-2	КМ-3	КМ-4
		Неделя КМ:	4	8	12	15
1	Правовое обеспечение информационной безопасности Российской Федерации. Основные функции государственных органов в области информационной безопасности					
1.1	Правовое обеспечение информационной безопасности Российской Федерации		+		+	
1.2	Основные функции государственных органов в области информационной безопасности		+		+	
2	Организация защиты информации на предприятии. Разработка системы защиты информации предприятия					
2.1	Организация защиты информации на предприятии.		+	+		
2.2	Разработка системы защиты информации предприятия		+	+		
3	Особенности организации работы с персоналом и контрагентами					
3.1	Особенности организации работы с персоналом		+	+		
3.2	Особенности организации работы с контрагентами		+	+		
4	Юридическая ответственность субъектов информационной сферы. Расследование инцидентов информационной безопасности на предприятии					

4.1	Порядок и особенности применения уголовной ответственности за преступления в области информационной безопасности	+		+	
4.2	Порядок и особенности применения административной ответственности за проступки в области информационной безопасности	+		+	
4.3	Порядок и особенности применения гражданско-правовой и дисциплинарной ответственности	+		+	
5	Правовое регулирование отдельных видов информации: государственная тайна, служебная информация, профессиональная тайна и т.д.				
5.1	Законодательство в области государственной тайны.			+	+
5.2	Законодательство в области служебной и коммерческой тайны			+	+
5.3	Правовое регулирование иных видов конфиденциальной информации			+	+
Вес КМ, %:		25	25	25	25



**БАЛЛЬНО-РЕЙТИНГОВАЯ СТРУКТУРА  
КУРСОВОГО ПРОЕКТА/РАБОТЫ ПО ДИСЦИПЛИНЕ**

**Организационно-правовые механизмы обеспечения информационной безопасности**

(название дисциплины)

**2 семестр**

**Перечень контрольных мероприятий текущего контроля успеваемости по курсовой работе:**

- КМ-1 соблюдение графика выполнения КР; оценка выполнения разделов КР  
 КМ-2 соблюдение графика выполнения КР; оценка выполнения разделов КР;  
 КМ-3 соблюдение графика выполнения КР; качество оформления КР

**Вид промежуточной аттестации – защита КР.**

Номер раздела	Раздел курсового проекта/курсовой работы	Индекс КМ:	КМ-1	КМ-2	КМ-3
		Неделя КМ:	4	8	12
1	Введение, Глава 1		+		
2	Глава 2			+	
3	Глава 3, Заключение, Список литературы				+
Вес КМ, %:			30	30	40