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

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

Москва 2025

ПРОГРАММУ СОСТАВИЛ:

Преподаватель	Подписано электронной подписью ФГБОУ ВО «НИУ «МЭИ» Сведения о владельце ЦЭП МЭИ Владелец: Трофимцева С.Ю. Идентификатор: Rdda85afd-TrofimtsevaSY-5aba752	С.Ю. Трофимцева

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 представления о закономерностях генезиса, эволюции и функционирования международной и национальной систем информационной безопасности, о системах международного, зарубежного и российского права и его отраслей, регулирующих информационные отношения и права человека в информационной сфере для последующего применения этих знаний в профессиональной сфере и формирования практических навыков и способности правовыми средствами решать профессиональные задачи

Задачи дисциплины

- проанализировать правовой статус информации и особенности правового регулирования информационных отношений и обеспечения гарантий прав человека в информационной сфере;
- изучить систему информационной безопасности и её составляющие как вид национальной безопасности;
- исследовать структуру федеральных органов власти, обеспечивающих информационную безопасность в РФ;
- проанализировать генезис и эволюцию киберпреступности как угрозу информационной безопасности и механизмы правового противодействия на национальном и международном уровне;
- проанализировать основные виды информации по доступу и видам тайн и особенности международного, зарубежного и российского законодательства, регулирующего оборот защищаемой информации.

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$_{ОПК-3}$ 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: - принципы правового регулирования информационных отношений; - содержание доктринальных документов РФ в сфере информационной безопасности; - обстоятельства возникновения уголовной и административной ответственности при возникновении ИБ-инцидента; - принципы работы с правовыми нормами, относящимися к различным правовым системам и отраслям права, в профессиональных ситуациях в сфере информационной безопасности; - систему нормативного правового регулирования защиты определённого вида информации и прав её обладателя; - структуру, задачи и функции органов, регулирующих деятельность объектов и субъектов в сфере ИБ. уметь: - определять вид правонарушения в киберсфере и перечень требуемых мер при его выявлении;

Код и наименование компетенции	Код и наименование индикатора достижения компетенции	Запланированные результаты обучения
		- определять необходимые правовые нормы для защиты определённого вида информации и формирования политики безопасности информации и защиты информационных прав субъекта в организации; - использовать правовые нормы для разрешения конфликтов и инцидентов 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	Введение в дисциплину. Теоретико-правовой базис регулирования отношений в сфере информационной безопасности	20	2	6	-	10	-	-	-	-	-	4	-	***Подготовка к практическим занятиям:*** Изучение материала по разделу "Введение в дисциплину. Теоретико-правовой базис регулирования отношений в сфере информационной безопасности" подготовка к выполнению заданий на практических занятиях. Студентам необходимо повторить теоретический материал, разобрать примеры, провести анализ правовых норм ***Подготовка курсовой работы:*** Курсовая работа представлена в виде темы по учебному кейсу, охватывающей несколько разделов дисциплины. ***Подготовка к аудиторным занятиям:*** Проработка лекции, выполнение и подготовка к практическому занятию ***Подготовка к текущему контролю:*** Повторение материала по разделу "Введение в дисциплину. Теоретико-правовой базис регулирования отношений в сфере информационной безопасности" ***Самостоятельное изучение теоретического материала:*** Изучение дополнительного материала по разделу "Введение в дисциплину. Теоретико-правовой базис регулирования отношений в сфере информационной безопасности" ***Изучение материалов литературных***
1.1	Введение в дисциплину	4		2	-	-	-	-	-	-	-	2	-	
1.2	Теоретико-правовой базис регулирования отношений в сфере информационной безопасности	16		4	-	10	-	-	-	-	-	2	-	

														источников: [8], 15-45
2	Правовой статус информации. правовое регулирование информационных отношений	14		4	-	6	-	-	-	-	-	4	-	***Самостоятельное изучение теоретического материала:*** Изучение дополнительного материала по разделу "Правовой статус информации. правовое регулирование информационных отношений"
2.1	Правовой статус информации	6		2	-	2	-	-	-	-	-	2	-	***Подготовка к практическим занятиям:*** Изучение материала по разделу "Правовой статус информации. правовое регулирование информационных отношений" подготовка к выполнению заданий на практических занятиях. Студентам необходимо повторить теоретический материал, разобрать примеры, провести анализ правовых норм ***Подготовка курсовой работы:*** Курсовая работа представлена в виде темы по учебному кейсу, охватывающей несколько разделов дисциплины. ***Подготовка к аудиторным занятиям:*** Проработка лекции, выполнение и подготовка к практическому занятию ***Подготовка к текущему контролю:*** Повторение материала по разделу "Правовой статус информации. правовое регулирование информационных отношений" ***Изучение материалов литературных источников:*** [2], 3-50 [3], 17-201 [7], 10-120
2.2	Правовое регулирование информационных отношений	8		2	-	4	-	-	-	-	-	2	-	
3	Информационная безопасность в системе национальной безопасности	18		6	-	8	-	-	-	-	-	4	-	***Подготовка к практическим занятиям:*** Изучение материала по разделу "Информационная безопасность в системе национальной безопасности" подготовка к выполнению заданий на практических занятиях. Студентам необходимо повторить теоретический материал, разобрать примеры,
3.1	Национальная безопасность: содержание, виды	8		2	-	4	-	-	-	-	-	2	-	

3.2	Информационная безопасность как вид национальной безопасности и её элементы. Структура федеральных органов власти, обеспечивающих информационную безопасность РФ	10		4	-	4	-	-	-	-	-	2	-	провести анализ правовых норм ***Самостоятельное изучение теоретического материала:*** Изучение дополнительного материала по разделу "Информационная безопасность в системе национальной безопасности" ***Подготовка курсовой работы:*** Курсовая работа представлена в виде темы по учебному кейсу, охватывающей несколько разделов дисциплины. ***Подготовка к аудиторным занятиям:*** Проработка лекции, выполнение и подготовка к практическому занятию ***Подготовка к текущему контролю:*** Повторение материала по разделу "Информационная безопасность в системе национальной безопасности" ***Изучение материалов литературных источников:*** [1], 5-65 [6], 130-136
4	Киберпреступления. Основные механизмы противодействия киберпреступности	18		6	-	8	-	-	-	-	-	4	-	***Самостоятельное изучение теоретического материала:*** Изучение дополнительного материала по разделу "Киберпреступления. Основные механизмы противодействия киберпреступности" ***Подготовка к практическим занятиям:*** Изучение материала по разделу "Киберпреступления. Основные механизмы противодействия киберпреступности" подготовка к выполнению заданий на практических занятиях. Студентам необходимо повторить теоретический материал, разобрать примеры, провести анализ правовых норм ***Подготовка курсовой работы:*** Курсовая работа представлена в виде темы по учебному кейсу, охватывающей несколько разделов дисциплины.
4.1	Генезис киберпреступности. Современные проблемы эффективного противодействия киберпреступлениям	4		2	-	-	-	-	-	-	-	2	-	
4.2	Уголовно-правовое и уголовно-процессуальное противодействие киберпреступности на международном и национальном	14		4	-	8	-	-	-	-	-	2	-	

	уровнях													***Подготовка к аудиторным занятиям:*** Проработка лекции, выполнение и подготовка к практическому занятию ***Подготовка к текущему контролю:*** Повторение материала по разделу "Киберпреступления. Основные механизмы противодействия киберпреступности"
5	Классификация информации по доступу и видам тайн	34		10	-	16	-	-	-	-	-	8	-	***Подготовка к текущему контролю:*** Повторение материала по разделу "Классификация информации по доступу и видам тайн"
5.1	Виды классификаций информации по доступу и распространению. Информация, свободно распространяемая, негативная информация	8		2	-	4	-	-	-	-	-	2	-	***Подготовка к аудиторным занятиям:*** Проработка лекции, выполнение и подготовка к практическому занятию ***Самостоятельное изучение теоретического материала:*** Изучение дополнительного материала по разделу "Классификация информации по доступу и видам тайн"
5.2	Защищаемая информация ограниченного доступа, не содержащая тайну	6		2	-	2	-	-	-	-	-	2	-	***Подготовка к практическим занятиям:*** Изучение материала по разделу "Классификация информации по доступу и видам тайн" подготовка к выполнению заданий на практических занятиях. Студентам необходимо повторить теоретический материал, разобрать примеры, провести анализ правовых норм ***Подготовка курсовой работы:*** Курсовая работа представлена в виде темы по учебному кейсу, охватывающей несколько разделов дисциплины. ***Изучение материалов литературных источников:*** [4], 15-730 [5], 11-701
5.3	Защищаемая информация в режиме тайн	20		6	-	10	-	-	-	-	-	4	-	
	Экзамен	35.9		-	-	-	-	2	-	-	0.4	-	33.5	
	Курсовая работа (КР)	40.1		-	-	-	16	-	4	-	0.4	19.7	-	
	Всего за семестр	**180.0**		**32**	**-**	**48**	**16**	**2**	**4**	**-**	**0.8**	**43.7**	**33.5**	
	Итого за семестр	**180.0**		**32**	**-**	**48**	**18**		**4**		**0.8**	**77.2**		

Примечание: Лек – лекции; Лаб – лабораторные работы; Пр – практические занятия; КПР – 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. Введение в дисциплину. Теоретико-правовой базис регулирования отношений в сфере информационной безопасности

1.1. Введение в дисциплину

Введение в дисциплину. Юриспруденция и её функции в сфере информационной безопасности. Государство и его функции по обеспечению национальной безопасности.

1.2. Теоретико-правовой базис регулирования отношений в сфере информационной безопасности

Права человека в информационной сфере и механизмы их обеспечения. Международное обеспечение прав человека в информационной сфере (Всеобщая декларация прав человека ООН, 1948 г., Римская конвенция СЕ о защите прав человека и его основных свобод, 1950 г., Пакт ООН о гражданских и политических правах, 1966 г., Ниццкая хартия ЕС об основных правах, Страсбургская декларация СЕ о свободе обмена информацией в Интернете, 2003 г.). Механизмы обеспечения прав сотрудников организации в информационной сфере. Информационная безопасность организации и обеспечение негативных универсальных прав человека в информационной сфере. Понятие «право». Системы права, регулирующие сферу информационной безопасности. Международное право, национальное право и их отрасли. Информационное / цифровое право как комплексное право. Правовая норма. Нормативный правовой акт. Иерархия нормативных правовых актов в сфере регулирования информационных отношений. Федеральная и региональная компетенция в сфере информационной безопасности. Документы по стандартизации в сфере информационной безопасности и их правовой статус. Объекты правоотношений. Виды правонарушений. Субъекты правонарушений в сфере информационной безопасности. Особенности правонарушений в информационной сфере.

2. Правовой статус информации. правовое регулирование информационных отношений

2.1. Правовой статус информации

Информация как общенаучное понятие. Информация как данные. Семиотический анализ информации. Свойства информации как данных. Свойства информации как сведений. Нормы-дефиниции термина «информация» в российском и международном праве. Понятие «электронное сообщение» в российском праве. Формы представления информации в российском праве. Понятие «документированная информация» и «электронный документ». Правовое регламентирование электронного документооборота в международном, зарубежном и российском праве. Электронная подпись и её виды. Механизмы регулирования правового статуса информации в организации в РФ. Понятие «охраняемая законом информация». Основные атрибуты защищаемой информации. Дефиниции терминов «целостность», «доступность» и «конфиденциальность» защищаемой информации. Требования ведомственных актов регуляторов (ФСБ, ФСТЭК, РКН, Министерства цифрового развития) к защите информации. Угрозы безопасности информации (УБИ) и их классификация.

2.2. Правовое регулирование информационных отношений

Информационные отношения как вид общественных отношений. Информация как объект правоотношений. Объекты правоотношений в российском праве. Признаки информации как объекта правоотношений. Трансформация экономической роли информации в постиндустриальную эпоху. Правовая проблема отнесения информации к предметам собственности. Собственник информации, обладатель информации. Цифровые права в российском праве. Законодательство РФ в области правового регулирования

информационных отношений. Конституция России и её юридический статус в системе регулирования информационных отношений. Нормы международного права как часть российской правовой системы. Законодательство в области защиты прав человека в инфосфере. Законодательство по интеллектуальной собственности. Законодательство, регулирующее обмен данными и дальнюю связь. Законодательство по общим вопросам информационной безопасности. Законодательство по защите информации и информационных ресурсов (в том числе, законодательство о тайнах).

3. Информационная безопасность в системе национальной безопасности

3.1. Национальная безопасность: содержание, виды

Термин «национальная безопасность и его дефиниции. Документы, содержащие официальные взгляды на проблемы национальной безопасности РФ: Концепция НБ 2000 г., Стратегии НБ 2009 г., 2015 г., 2021 г.: сравнительный анализ. Виды национальной безопасности по доктринальным документам РФ. Стратегические национальные приоритеты. Информационная безопасность как стратегический национальный приоритет.

3.2. Информационная безопасность как вид национальной безопасности и её элементы. Структура федеральных органов власти, обеспечивающих информационную безопасность РФ

«Информационная безопасность: два основных значения термина. Документы, содержащие официальные взгляды на проблемы информационной безопасности: Доктрина информационной безопасности 2000 г., 2016 г.: сравнительный анализ. Основные элементы информационной безопасности: информационно-техническая безопасность - информационно-психологическая безопасность, безопасность информации, информационных ресурсов и систем - информационно-психологическая безопасность - правовое обеспечение информационной безопасности. Понятие «безопасность информации [данных]». Локальные нормативные акты ФСТЭК и ФСБ по обеспечению безопасности информации. Понятие «угроза защищаемой информации». Виды угроз защищаемой информации. Угрозы защищаемой информации по банку данных ФСТЭК (УБИ). Понятие «информационно-психологическая безопасность. Классификация видов информационно-психологического воздействия: ситуативные («спектакль», «игра», перфоманс, стратагема), вербально-образные (манипуляции, пропаганда. Целевые мишени ИПВ. Социальная инженерия как технология ИПВ. Способы социальной инженерии: фишинг, картинг, спуфинг, фрикинг, претексинг и т. п. Обеспечение информационно-психологической безопасности персонала организаций. Структура федеральных органов власти, обеспечивающих информационную безопасность РФ. Федеральное собрание РФ, президент РФ и их функции. Правительство РФ (Министерство печати, связи и информации: Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций, Министерство внутренних дел: Управление «Э», Бюро специальных технических мероприятий (Управление «К»), Министерство обороны: Главное управление Генерального штаба ВС) и их функции. Служба внешней разведки и её функции. Федеральная служба безопасности и её функции. Федеральная служба по техническому и экспортному контролю и её функции. Федеральная служба охраны и её функции. Следственный комитет: Отдел по расследованию киберпреступлений и его функции. Совет безопасности и его функции.

4. Киберпреступления. Основные механизмы противодействия киберпреступности

4.1. Генезис киберпреступности. Современные проблемы эффективного противодействия киберпреступлениям

Проблема определения времени зарождения киберпреступности. Факторы, способствовавшие эскалации киберпреступлений. Общественная опасность киберпреступлений. Современные проблемы эффективного противодействия киберпреступлениям. Проблемы на уровне национальных правовых систем. Проблемы на уровне международного права. Правовые проблемы, связанные с транснациональным характером киберпреступлений и необходимость их решения..

4.2. Уголовно-правовое и уголовно-процессуальное противодействие киберпреступности на международном и национальном уровнях

Особенности начала криминализации кибердеяний в национальных правовых системах. Рекомендации ООН по противодействию киберпреступности. Резолюции конгрессов и генеральных ассамблей ООН по противодействию использованию информационно-коммуникационных технологий в преступных целях. Кодификатор киберпреступлений МОУП «Интерпол». Проект конвенции ООН противодействии использованию информационно-коммуникационных технологий в преступных целях (2019 г., РФ). Организационно-правовое противодействие киберпреступности на общеевропейском уровне. Специальные комитеты СЕ и их функции. Рекомендации Комитета министров стран - членов Совета Европы. Классификация киберпреступлений в наднациональном праве Европы. Конвенция Совета Европы «О киберпреступности» (г. Будапешт, 2001) и дополнительные протоколы. Рекомендации Будапештской конвенции и Страсбургского протокола в области материального права и процессуального права. Специфика уголовно-правового противодействия киберпреступности в праве государств, ратифицировавших Будапештскую конвенцию. Проблемы, связанные с гармонизацией национального права ратификантов Будапештской конвенции. Уголовно-правовые и уголовно-процессуальные рекомендации по противодействию киберпреступности на уровне СНГ. Рекомендации Модельного уголовного кодекса СНГ (1996 г.). Рекомендации Душанбинского соглашения о сотрудничестве государств - участников СНГ в борьбе с преступлениями в сфере информационных технологий (2019 г.) в области материального и процессуального права. Рекомендации Модельного закона СНГ о противодействии киберпреступности (2023 г.). Специфика уголовно-правового противодействия киберпреступности в праве государств - членов СНГ. Компьютерные преступления, преступления, вязанные с компьютерами, преступления, связанные с содержанием данных в уголовном праве РФ и их особенности. Организация противодействия киберпреступности в организации. Особенности защиты компьютерной информации, сетей и систем в организации..

5. Классификация информации по доступу и видам тайн

5.1. Виды классификаций информации по доступу и распространению. Информация, свободно распространяемая, негативная информация

Основные виды классификаций информации по доступу и распространению: информация свободного доступа, информация ограниченного доступа, информация, свободно распространяемая, информация, предоставляемая по соглашению лиц, участвующих в соответствующих отношениях, информация, которая в соответствии с федеральными законами подлежит предоставлению или распространению, информацию, распространение которой в Российской Федерации ограничивается или запрещается – проблемы отнесения конкретной информации к определённому классу. Сводная классификация информации по доступу, распространению и видам тайн. Информация свободного распространения: основные виды и правовые требования к её обороту. Основные параметры свободно распространяемой информации. Международные документы, гарантирующие право человека на информацию: правовые гарантии ООН, СЕ, ЕС. Правовые гарантии права человека на информацию в Конституции России. Право человека на доступ к ресурсам

Интернета. Интернет как коммуникативное пространство. Страсбургская декларация СЕ о свободе обмена информацией в Интернете, 2003 г. Основные проблемы распространения информации в Интернете. Модели стиля регулирования Интернета. Свободно распространяемая информация в организациях: информация, распространяемая во внешней среде, информация, распространяемая во внутренней среде. Основные документы, регламентирующие оборот свободно распространяемой информации в организации, в РФ. Понятие «негативной» информации (информации, от которой нужно защищать субъектов информационных отношений) и её виды. Негативная информация в связи со способом её распространения. Правовые требования к распространению рекламной информации организациями. Запрет и ограничения на рекламирование отдельных видов товаров и услуг коммерческими компаниями и индивидуальными предпринимателями. Административная ответственность за рекламирование некоторых товаров и услуг в РФ. Негативная информация по признакам её содержания. Виды информации, запрещённой к распространению в РФ. Уголовная и административная ответственность за распространение информации, запрещённой в РФ..

5.2. Защищаемая информация ограниченного доступа, не содержащая тайну

Право интеллектуальной собственности. Защита информации, относящейся к объектам интеллектуальной собственности. Уровни правового регулирования интеллектуальной собственности. Авторское право. Генезис института авторского права. Международное регулирование авторского и смежных прав (Бернская конвенция о защите литературных и художественных произведений, 1886 г., Всемирная (Женевская) конвенция по авторскому праву, 1952 г., Маракешское соглашение по интеллектуальной собственности и торговле (ТРИПС), 1994 г.). Виды и типы объектов авторских и смежных прав, и их признаки. Программа для ЭВМ и её правовая защита в режиме охраны литературного произведения. Виды авторских прав. Сроки действия авторских прав. Правовые проблемы свободного использования объектов авторских прав. Служебное произведение и особенности его правового регулирования и использования в организациях. Нетрадиционные объекты авторских прав. Произведения, не являющиеся объектами авторских прав. Произведения, не являющиеся объектами исключительных прав. Правовое регулирование авторских прав в РФ. Смежное право. Международное регулирование смежных прав (Римская конвенция об охране прав исполнителей, изготовителей фонограмм и вещательных организаций, 1961, Женевская конвенция об охране интересов производителей фонограмм от незаконного воспроизводства их фонограмм, 1971 г.). Правовое противодействие нарушению авторских и смежных прав (Маракешское соглашение по интеллектуальной собственности и торговле (ТРИПС), 1994 г., Международное торговое соглашение по борьбе с контрафактом (АСТА), 2001 г.). Правовое регулирование смежных прав в РФ. Уголовная и административная ответственность за нарушение авторских и смежных прав в РФ. Объекты патентных прав. Генезис правового института патентных прав. Международное правовое регулирование патентных прав (Парижская конвенция по охране промышленной собственности, 1883 г., Стокгольмская конвенция, учреждающая Всемирную организацию интеллектуальной собственности (ВОИС), 1967 г., Международная патентная система (РСТ), 1978, Женевский договор о патентном праве, 2000 г.). Критерии объектов патентных прав. Виды объектов патентных прав. Виды прав на объекты. Служебное изобретение (полезная модель, промышленный образец) и особенности его правового регулирования и использования в организациях. Нетрадиционные объекты патентных прав. Правовые проблемы защиты ноу-хау. Правовое регулирование патентных прав в РФ. Уголовная и административная ответственность за нарушение патентных прав в РФ. Служебная информация ограниченного распространения в РФ. Чиновничье право, «чиновничьи секреты» в зарубежном праве. Служебная информация ограниченного распространения в РФ: особенности правового регулирования и правовые проблемы. Сфера оборота служебной информации ограниченного распространения в РФ. Признаки служебной информации как несекретной информации.

Требования к документообороту служебной информации ограниченного распространения в РФ..

5.3. Защищаемая информация в режиме тайн

Классификация защищаемой информации в режиме тайн в РФ: информация в режиме государственной тайны и информация конфиденциального характера. Информация в режиме государственной тайны. Правовой институт государственной тайны в СССР и его специфика. Правовой институт государственной тайны в РФ. Сферы присутствия информации в режиме государственной тайны в РФ. Информация, которая не может быть засекречена в режиме государственной тайны в РФ. Порядок допуска должностных лиц и граждан к информации в режиме государственной тайны в РФ. Степени секретности информации и реквизиты на материальных носителях информации в режиме государственной тайны в РФ. Порядок отнесения информации к государственной тайне, сроки засекречивания, условия рассекречивания информации в режиме государственной тайны в РФ. Уголовная ответственность за нарушение секретности информации в режиме государственной тайны в РФ. Информация в режиме коммерческой тайны. Основные причины генезиса правового института коммерческой тайны. Промышленно-экономический шпионаж и бизнес-разведка как виды деятельности по получения защищаемой коммерческой информации. Особенности эволюции правового института коммерческой тайны в зарубежном праве. Признаки информации в режиме коммерческой тайны. Международное правовое регулирования защиты информации в режиме коммерческой тайны (Североамериканское соглашение о свободной торговле (NAFTA), 1992, USMCA, 2020, Маракешское соглашение по интеллектуальной собственности и торговле (ТРИПС), 1994 г., соглашения ВТО). Генезис правового института регулирования коммерческой тайны в РФ и его специфика. Информация, которая не может быть отнесена к коммерческой тайне в РФ. Основные законодательные требования к введению режима коммерческой тайны в коммерческих организациях и индивидуальными предпринимателями в РФ. Обязательные реквизиты на материальных носителях, содержащих информацию в режиме коммерческой тайны в РФ. Основные рекомендации по документальному обеспечению коммерческой тайны и по процедуре доступа работников и контрагентов коммерческих компаний в РФ. Уголовная и административная ответственность за нарушение конфиденциальности информации в режиме коммерческой тайны в РФ. Информация в режиме служебной тайны в области обороны в РФ. Служебная тайна в СССР: специфика правового регулирования. Попытки введения служебной тайны в РФ в 1990-х гг. Информация в режиме служебной тайны в области обороны с 2021 г. в РФ и её признаки. Требования к документообороту информации в режиме служебной тайны в области обороны в РФ. Административная ответственность за нарушение конфиденциальности информации в режиме служебной тайны в области обороны в РФ. Информация о частной жизни (личная и семейная тайна). Генезис идеи и правового института защиты частной жизни человека и тайны его коммуникации (Декларация прав человека и гражданина, Билль о правах). Международное правовое обеспечения права человека на защиту частной жизни, личную и семейную тайну, тайну коммуникации (Всеобщая декларация прав человека ООН, 1948 г., Римская конвенция о защите прав человека и его основных свобод СЕ, 1950 г., Пакт ООН о защите гражданских и политических прав, 1966 г., Ниццкая хартия ЕС об основных правах, 2000 г.). Права человека на защиту частной жизни, личную и семейную тайну, тайну коммуникации в Конституции России. Проблемы правоприменительной практики при обеспечении права человека на защиту частной жизни, личную и семейную тайну, тайну коммуникации, в РФ. Уголовная ответственность за нарушение тайны частной жизни и тайны коммуникации в РФ. Правовая защита персональных данных. Генезис правового института персональных данных. Понятие «персональные данные» в зарубежном праве. Международное правовое регулирование оборота персональных данных (Директива о защите неприкосновенности частной жизни и международных обменов персональными данными ОЭСР, 1980 г., Страсбургская конвенция

СЕ «О защите физических лиц при автоматизированной обработке персональных данных», 1981 г., Общий регламент по защите данных ЕС 2016/679, Модельный закон «О персональных данных» СНГ, 2021 г.). Особенности защиты персональных данных за рубежом. Правовые требования к защите персональных данных в РФ. Права субъекта персональных данных. Формы согласий на обработку персональных данных. Обязанности оператора персональных данных. Порядок трансграничной передачи персональных данных. Категории персональных данных. Специальные персональные данные. Биометрические персональные данные. Правовые требования к биометрическим персональным данным. Условия получения биометрических данных. Требования к сбору и хранению биометрических данных. Требования к информационным системам, обрабатывающим персональные данные. Основные документы оператора персональных данных. Нормативные требования по государственному контролю за обработкой персональных данных. Административная ответственность за нарушение правил оборота и защиты персональных данных в РФ. Информация в режиме профессиональных тайн. Виды профессиональных тайн в РФ. Правовые требования к защите врачебной тайны. Особенности защиты информации в режиме нотариальной, адвокатской, банковской, налоговой тайны. Специфика конфиденциальности информации в режиме журналистской тайны. Административная и уголовная ответственность за нарушение режима отдельных видов профессиональных тайн. Информация в режиме процессуальной тайны: данные предварительного расследования, тайна совещания судей, тайна совещания присяжных заседателей. Уголовная ответственность за нарушение режима процессуальных тайн..

3.3. Темы практических занятий

1. Информационное / цифровое право как комплексное право;
2. Электронная подпись и её использование в правоотношениях;
3. Требования ведомственных актов регуляторов (ФСБ, ФСТЭК, РКН, Министерства цифрового развития) к защите информации. Угрозы безопасности информации (УБИ) и их классификация;
4. Доктринальные документы РФ в сфере национальной и информационной безопасности РФ;
5. Административно-правовое и уголовно-правовое противодействие распространению негативной информации в РФ;
6. Уголовно-правовое и уголовно-процессуальное противодействие киберпреступности: сравнительный анализ норм УК РФ, рекомендаций документов СНГ и СЕ;
7. Правовая защита нетрадиционных объектов интеллектуальной собственности в РФ;
8. Правовое регулирование требований к защите информации в режиме отдельных видов тайн;
9. Структура нормативных правовых актов в сфере обеспечения информационной безопасности;
10. Функции органов, регулирующих правовые отношения в сфере информационной безопасности. Правовой статус Совета безопасности в сфере обеспечения национальной и информационной безопасности РФ;
11. Права человека в информационной сфере.

3.4. Темы лабораторных работ

не предусмотрено

3.5 Консультации

Аудиторные консультации по курсовому проекту/работе (КПР)

1. Консультации направлены на выполнение разделов курсовой работы под руководством преподавателя. В рамках часов на групповые консультации разбираются наиболее важные части правовых проблем раздела "Правовой статус информации. правовое регулирование информационных отношений"
2. Консультации направлены на выполнение разделов курсовой работы под руководством преподавателя. В рамках часов на групповые консультации разбираются наиболее важные части правовых проблем раздела "Информационная безопасность в системе национальной безопасности"
3. Консультации направлены на выполнение разделов курсовой работы под руководством преподавателя. В рамках часов на групповые консультации разбираются наиболее важные части правовых проблем раздела "Киберпреступления. Основные механизмы противодействия киберпреступности"
4. Консультации направлены на выполнение разделов курсовой работы под руководством преподавателя. В рамках часов на групповые консультации разбираются наиболее важные части правовых проблем раздела "Классификация информации по доступу и видам тайн"

Групповые консультации по разделам дисциплины (ГК)

1. Обсуждение материалов по кейсам раздела "Введение в дисциплину. Теоретико-правовой базис регулирования отношений в сфере информационной безопасности"
2. Обсуждение материалов по кейсам раздела "Правовой статус информации. правовое регулирование информационных отношений"
3. Обсуждение материалов по кейсам раздела "Информационная безопасность в системе национальной безопасности"
4. Обсуждение материалов по кейсам раздела "Киберпреступления. Основные механизмы противодействия киберпреступности"
5. Обсуждение материалов по кейсам раздела "Классификация информации по доступу и видам тайн"

Индивидуальные консультации по курсовому проету /работе (ИККП)

1. Консультации проводятся по разделу "Правовой статус информации. правовое регулирование информационных отношений"
2. Консультации проводятся по разделу "Информационная безопасность в системе национальной безопасности"
3. Консультации проводятся по разделу "Киберпреступления. Основные механизмы противодействия киберпреступности"
4. Консультации проводятся по разделу "Классификация информации по доступу и видам тайн"

Текущий контроль (ТК)

1. Консультации направлены на анализ группового задания для выполнения контрольных мероприятий по разделу "Введение в дисциплину. Теоретико-правовой базис регулирования отношений в сфере информационной безопасности"
2. Консультации направлены на анализ группового задания для выполнения контрольных мероприятий по разделу "Правовой статус информации. правовое регулирование информационных отношений"
3. Консультации направлены на анализ группового задания для выполнения контрольных мероприятий по разделу "Информационная безопасность в системе национальной безопасности"
4. Консультации направлены на анализ группового задания для выполнения контрольных мероприятий по разделу "Киберпреступления. Основные механизмы противодействия киберпреступности"

5. Консультации направлены на анализ группового задания для выполнения контрольных мероприятий по разделу "Классификация информации по доступу и видам тайн"

3.6 Тематика курсовых проектов/курсовых работ

2 Семестр

Курсовая работа (КР)

Темы:

- 1. Особенности обеспечения правовой защиты внутренней информации неконфиденциального характера коммерческой организации в РФ
- 2. Правовые проблемы использования биометрических персональных данных в РФ
- 3. Возможности фальсификации биометрических персональных данных и правовые механизмы противодействия в РФ
- 4. Специфика и основные механизмы защиты информации, составляющей врачебную тайну, в РФ
- 5. Правовые и организационные механизмы защиты тайны частной жизни в социальных сетях в российском и зарубежном правовом поле
- 6. Организация защиты личной информации в социальных сетях и разработка рекомендаций для пользователей сетей
- 7. Организация режима защиты персональных данных клиентов в коммерческой организации (на примере организации).
- 8. Организация и порядок допуска персонала к защищаемым персональным данным в организации, и основания его прекращения (на примере организации).
- 9. Механизмы и порядок защиты персональных данных, полученных работодателем в рамках трудовых отношений (на примере организации).
- 10. Механизмы и порядок защиты персональных данных обучающихся, полученных образовательной организацией в рамках оказания образовательных услуг (на примере организации).
- 11. Организация и порядок допуска персонала к информации, составляющей коммерческую тайну, и основания его прекращения (на примере организации).
- 12. Организационно-правовая защита коммерческой компании от промышленно-экономического шпионажа и бизнес-разведки (на примере организации).
- 13. Особенности организации применения электронной подписи в организации для внутреннего и внешнего электронного документооборота (на примере организации).
- 14. Особенности защиты информации литературных произведений и авторских прав на них в Интернет-пространстве в российском и международном правовом поле.
- 15. Особенности защиты информации видеопродукции и авторских прав на них в Интернет-пространстве в российском и международном правовом поле.
- 16. Особенности защиты информации музыкальных произведений и авторских прав на них в Интернет-пространстве в российском и международном правовом поле.
- 17. Правовое регулирование оборота свободно распространяемой информации в РФ.
- 18. Организация и порядок оборота свободно распространяемой информации в организации (на примере организации).
- 19. Проблемы классификации киберпреступлений в российском и международном праве.
- 20. Специфика уголовно-правового противодействия компьютерным преступлениям в России и странах СНГ (сравнительный анализ) и разработка рекомендаций по совершенствованию киберзаконодательства.
- 21. Специфика уголовно-правового противодействия преступлениям, связанным с компьютерами, в России и странах СНГ (сравнительный анализ) и разработка рекомендаций по совершенствованию киберзаконодательства.

- 22. Специфика уголовно-правового противодействия преступлениям, связанным с содержанием данных, в России и странах СНГ (сравнительный анализ) и разработка рекомендаций по совершенствованию киберзаконодательства.
- 23. Анализ пробелов уголовного законодательства национальных правовых систем и международного права в сфере противодействия злонамеренным деяниям в киберсреде при подготовке специалистов по компьютерной безопасности.
- 24. Особенности защиты информации видеоигр и авторских прав на них в Интернет-пространстве в российском правовом поле.
- 25. Правовое регулирование аспектов информационной безопасности в «Интернете вещей» как нового направления электронной коммерции.

График выполнения курсового проекта

Неделя	1 - 4	5 - 8	9 - 12	13 - 15	Зачетная
Раздел курсового проекта	1	2	3	4	Защита курсового проекта
Объем раздела, %	10	40	40	10	-
Выполненный объем нарастающим итогом, %	10	50	90	100	-

Номер раздела	Раздел курсового проекта
1	Введение
2	Глава 1
3	Глава 2
4	Заключение

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	
Знать:							
структуру, задачи и функции органов, регулирующих деятельность объектов и субъектов в сфере ИБ	ИД-1$_{ОПК-3}$			+			Тестирование/Правовой статус информации. правовое регулирование информационных отношений
систему нормативного правового регулирования защиты определённого вида информации и прав её обладателя	ИД-1$_{ОПК-3}$					+	Тестирование/Классификация информации по доступу и видам тайн
принципы работы с правовыми нормами, относящимися к различным правовым системам и отраслям права, в профессиональных ситуациях в сфере информационной безопасности	ИД-1$_{ОПК-3}$	+					Тестирование/Введение в дисциплину. Теоретико-правовой базис регулирования отношений в сфере информационной безопасности
обстоятельства возникновения уголовной и административной ответственности при возникновении ИБ-инцидента	ИД-1$_{ОПК-3}$				+		Тестирование/Киберпреступления. Основные механизмы противодействия киберпреступности
содержание доктринальных документов РФ в сфере информационной безопасности	ИД-1$_{ОПК-3}$			+			Тестирование/Правовой статус информации. правовое регулирование информационных отношений
принципы правового регулирования информационных отношений	ИД-1$_{ОПК-3}$		+				Тестирование/Классификация информации по доступу и видам тайн Тестирование/Правовой статус информации. правовое регулирование информационных отношений
Уметь:							
использовать правовые нормы для разрешения конфликтов и инцидентов в сфере информационной безопасности	ИД-1$_{ОПК-3}$					+	Тестирование/Классификация информации по доступу и видам тайн

определять необходимые правовые нормы для защиты определённого вида информации и формирования политики безопасности информации и защиты информационных прав субъекта в организации	ИД-1$_{ОПК-3}$					+	Тестирование/Классификация информации по доступу и видам тайн
определять вид правонарушения в киберсфере и перечень требуемых мер при его выявлении	ИД-1$_{ОПК-3}$				+		Тестирование/Киберпреступления. Основные механизмы противодействия киберпреступности

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: Компьютерное задание

1. Введение в дисциплину. Теоретико-правовой базис регулирования отношений в сфере информационной безопасности (Тестирование)
2. Киберпреступления. Основные механизмы противодействия киберпреступности (Тестирование)
3. Классификация информации по доступу и видам тайн (Тестирование)
4. Правовой статус информации. правовое регулирование информационных отношений (Тестирование)

Балльно-рейтинговая структура дисциплины является приложением А.
Балльно-рейтинговая структура курсовой работы является приложением Б.

4.2 Промежуточная аттестация по дисциплине

Экзамен (Семестр №2)

Оценка определяется в соответствии с Положением о балльно-рейтинговой системе для студентов НИУ «МЭИ» на основании семестровой и экзаменационной составляющих.

Курсовая работа (КР) (Семестр №2)

При выставлении итоговой оценки учитывается выполнение графика написания работы, содержание и оформление работы, а также умение студента анализировать нормативные правовые акты и работать с научной литературой по теме.

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. № 28(313) : Национальные интересы: приоритеты и безопасность = National interests : журнал / ред. сов. О. Н. Беленов ; изд. ООО «Информационный центр «Финансы и кредит» ; гл. ред. В. Л. Макаров ; учред. ООО «Издательский дом ФИНАНСЫ и КРЕДИТ» . – Москва : Финансы и кредит, 2015 . – 68 с. : ил., табл., схем. – Режим доступа: электронная библиотечная система «Университетская библиотека ONLINE», требуется авторизация . - Библиогр. в кн . - ISSN 2311-875X .;
2. Александров, А. С. Система контроля документооборота ограниченного распространения в корпоративных информационных системах : магистерская диссертация / А. С. Александров, Нац. исслед. ун-т "МЭИ", Кафедра информационной и экономической безопасности . – М., 2017 . – 55 с. - диссертация только в электронном виде, для чтения перейдите в электронную библиотеку МЭИ .
http://elib.mpei.ru/elib/view.php?id=9179;
3. Артемов, А. В. Информационная безопасность: курс лекций : курс лекций / Межрегиональная академия безопасности и выживания . – Орел : Межрегиональная

академия безопасности и выживания, 2014 . – 257 с. : табл., схем. – Режим доступа: электронная библиотечная система «Университетская библиотека ONLINE», требуется авторизация .;
4. Бабаш, А. В. Информационная безопасность. История защиты информации в России / А. В. Бабаш, Е. К. Баранова, Д. А. Ларин . – М. : КДУ, 2013 . – 736 с. - ISBN 978-5-98227-928-6 .;
5. Бачило, И. Л. Информационное право : учебник для вузов по направлению "Юриспруденция", специальностям "Юриспруденция", "Правохранительная деятельность" / И. Л. Бачило, В. Н. Лопатин, М. А. Федотов ; Ред. Б. Н. Топорнин ; Ин-т государства и права Рос. акад. наук . – 2-е изд., с изм. и доп . – СПб. : Р. Асланов "Юридический центр Пресс", 2005 . – 725 с. – (Учебники и учебные пособия) . - ISBN 5-942014-33-7 .;
6. Володенков, С. В. Информационно-психологические войны и массовое сознание / С. В. Володенков . – 2003 // Вестник МГУ: Политические науки . – 03/2003 . – N3 . – с.130-136 . - Автор анализирует понятие информационно-психологические войны как феномен, описывающий определнный тип взаимоотношений между различными государственными и общественными системами.;
7. А. Б. Арзуманян- "Международные стандарты правовой защиты информации и информационных технологий", Издательство: "Южный федеральный университет", Ростов-на-Дону, Таганрог, 2020 - (140 с.)
https://biblioclub.ru/index.php?page=book&id=612162;
8. авторы-составители Л. Э.,Трофимов М. С.- "Информационное право и информационные технологии: Практикум", Издательство: "СКФУ", Ставрополь, 2017 - (79 с.)
https://e.lanbook.com/book/307070.

5.2 Лицензионное и свободно распространяемое программное обеспечение:
1. СДО "Прометей";
2. Office / Российский пакет офисных программ;
3. Windows / Операционная система семейства Linux.

5.3 Интернет-ресурсы, включая профессиональные базы данных и информационно-справочные системы:
1. **ЭБС Лань** - https://e.lanbook.com/
2. **ЭБС "Университетская библиотека онлайн"** - http://biblioclub.ru/index.php?page=main_ub_red
3. **Научная электронная библиотека** - https://elibrary.ru/
4. **База данных Web of Science** - http://webofscience.com/
5. **База данных Scopus** - http://www.scopus.com
6. **Национальная электронная библиотека** - https://rusneb.ru/
7. **ЭБС "Консультант студента"** - http://www.studentlibrary.ru/
8. **База данных диссертаций ProQuest Dissertations and Theses Global** - https://search.proquest.com/pqdtglobal/index
9. **Электронная библиотека МЭИ (ЭБ МЭИ)** - http://elib.mpei.ru/login.php
10. **Портал открытых данных Российской Федерации** - https://data.gov.ru
11. **Информационно-справочная система «Кодекс/Техэксперт»** - Http:\\proinfosoft.ru; http://docs.cntd.ru/
12. **Национальный портал онлайн обучения «Открытое образование»** - https://openedu.ru
13. **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

Приложение А

БАЛЛЬНО-РЕЙТИНГОВАЯ СТРУКТУРА ДИСЦИПЛИНЫ

Организационно-правовые механизмы обеспечения информационной безопасности

(название дисциплины)

2 семестр

Перечень контрольных мероприятий текущего контроля успеваемости по дисциплине:

КМ-1 Введение в дисциплину. Теоретико-правовой базис регулирования отношений в сфере информационной безопасности (Тестирование)

КМ-2 Правовой статус информации. правовое регулирование информационных отношений (Тестирование)

КМ-3 Киберпреступления. Основные механизмы противодействия киберпреступности (Тестирование)

КМ-4 Классификация информации по доступу и видам тайн (Тестирование)

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	Введение в дисциплину. Теоретико-правовой базис регулирования отношений в сфере информационной безопасности					
1.1	Введение в дисциплину		+			
1.2	Теоретико-правовой базис регулирования отношений в сфере информационной безопасности		+			
2	Правовой статус информации. правовое регулирование информационных отношений					
2.1	Правовой статус информации			+		+
2.2	Правовое регулирование информационных отношений			+		+
3	Информационная безопасность в системе национальной безопасности					
3.1	Национальная безопасность: содержание, виды			+		
3.2	Информационная безопасность как вид национальной безопасности и её элементы. Структура федеральных органов власти, обеспечивающих информационную безопасность РФ			+		
4	Киберпреступления. Основные механизмы противодействия киберпреступности					
4.1	Генезис киберпреступности. Современные проблемы эффективного противодействия киберпреступлениям				+	

4.2	Уголовно-правовое и уголовно-процессуальное противодействие киберпреступности на международном и национальном уровнях			+	
5	Классификация информации по доступу и видам тайн				
5.1	Виды классификаций информации по доступу и распространению. Информация, свободно распространяемая, негативная информация				+
5.2	Защищаемая информация ограниченного доступа, не содержащая тайну				+
5.3	Защищаемая информация в режиме тайн				+
	Вес КМ, %:	10	25	30	35

Приложение Б

БАЛЛЬНО-РЕЙТИНГОВАЯ СТРУКТУРА КУРСОВОГО ПРОЕКТА/РАБОТЫ ПО ДИСЦИПЛИНЕ

Организационно-правовые механизмы обеспечения информационной безопасности

(название дисциплины)

2 семестр

Перечень контрольных мероприятий <u>текущего контроля</u> успеваемости по курсовой работе:

КМ-1 Введение
КМ-2 Глава 1
КМ-3 Глава 2
КМ-4 Заключение

Вид промежуточной аттестации – защита КР.

Номер раздела	Раздел курсового проекта/курсовой работы	Индекс КМ:	КМ-1	КМ-2	КМ-3	КМ-4
		Неделя КМ:	4	8	12	15
1	Введение		+			
2	Глава 1			+		
3	Глава 2				+	
4	Заключение					+
		Вес КМ, %:	10	40	40	10