

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

Направление подготовки/специальность: 10.03.01 Информационная безопасность

Наименование образовательной программы: Безопасность компьютерных систем

Уровень образования: высшее образование - бакалавриат

Форма обучения: Очная

Рабочая программа дисциплины
ОРГАНИЗАЦИОННОЕ И ПРАВОВОЕ ОБЕСПЕЧЕНИЕ
ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Блок:	Блок 1 «Дисциплины (модули)»
Часть образовательной программы:	Обязательная
№ дисциплины по учебному плану:	Б1.О.20
Трудоемкость в зачетных единицах:	3 семестр - 5; 4 семестр - 5; всего - 10
Часов (всего) по учебному плану:	360 часов
Лекции	3 семестр - 32 часа; 4 семестр - 32 часа; всего - 64 часа
Практические занятия	3 семестр - 48 часа; 4 семестр - 32 часа; всего - 80 часов
Лабораторные работы	не предусмотрено учебным планом
Консультации	3 семестр - 2 часа; 4 семестр - 18 часов; всего - 20 часов
Самостоятельная работа	3 семестр - 97,5 часа; 4 семестр - 93,2 часа; всего - 190,7 часа
в том числе на КП/КР	не предусмотрено учебным планом
Иная контактная работа	4 семестр - 4 часа;
включая: Контрольная работа Мозговой штурм Семинар Кейс (решение конкретных производственных ситуаций)	
Промежуточная аттестация:	
Экзамен	3 семестр - 0,5 часа;
Экзамен	4 семестр - 0,8 часа;
Защита курсовой работы	4 семестр - 0 часов; всего - 1,3 часа

Москва 2025

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	Баронов О.Р.
	Идентификатор	R90d76356-BaronovOR-7bf8fd7e

О.Р. Баронов

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: освоение общекультурных и профессиональных компетенций, заключающихся в общей готовности и способности осуществлять мероприятия по правовой и организационной защите информации в интересах обеспечения информационной безопасности предприятия (организации).

Задачи дисциплины

- изучение теоретических основ обеспечения информационной безопасности на предприятии (в организации);
- формирование готовности и способности к активной профессиональной деятельности в условиях информационного противоборства;
- знание основных нормативных актов в области информационной безопасности, умение осуществлять поиск необходимой правовой информации;
- умение формировать политику информационной безопасности предприятий, исходя из фактического процесса обработки информации на предприятии;;
- умение работать в команде по разработке основных требований в области информационной безопасности предприятия..

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-1 Способен оценивать роль информации, информационных технологий и информационной безопасности в современном обществе, их значение для обеспечения объективных потребностей личности, общества и государства	ИД-1 _{ОПК-1} Понимает значение информации в развитии современного общества, применять информационные технологии для поиска и обработки информации	уметь: - применять информационные технологии для поиска и обработки информации, в том числе информационно-правовые системы.
ОПК-5 Способен применять нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации в сфере профессиональной деятельности	ИД-2 _{ОПК-5} Использует нормативные правовые акты в профессиональной деятельности	знать: - требования нормативных актов в области защиты информации.
ОПК-8 Способен осуществлять подбор, изучение и общение научно-технической литературы, нормативных и методических	ИД-1 _{ОПК-8} Выполняет подбор, изучение и обобщение научно-технической литературы, нормативных и методических материалов,	уметь: - выполнять подбор, изучение и обобщение научно-технической литературы, нормативных и методических материалов, составляет обзор по вопросам обеспечения информационной безопасности по

Код и наименование компетенции	Код и наименование индикатора достижения компетенции	Запланированные результаты обучения
документов в целях решения задач профессиональной деятельности	составляет обзор по вопросам обеспечения информационной безопасности по профилю своей профессиональной деятельности	профилю своей профессиональной деятельности.
ОПК-10 Способен в качестве технического специалиста принимать участие в формировании политики информационной безопасности, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации на объекте защиты	ИД-1 _{ОПК-10} Участвует в работах по реализации политики информационной безопасности, применяет комплексный подход к обеспечению информационной безопасности объекта защиты	<p>знать:</p> <ul style="list-style-type: none"> - требования нормативных актов по формированию политики информационной безопасности. <p>уметь:</p> <ul style="list-style-type: none"> - применять комплексный подход к обеспечению информационной безопасности объекта защиты.
ОПК-10 Способен в качестве технического специалиста принимать участие в формировании политики информационной безопасности, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации на объекте защиты	ИД-2 _{ОПК-10} Принимает участие в формировании, организации и поддержании выполнения комплекса мер по обеспечению информационной безопасности, управляет процессом их реализации	<p>уметь:</p> <ul style="list-style-type: none"> - управлять процессом реализации мер защиты информации.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ ВО

Дисциплина относится к основной профессиональной образовательной программе Безопасность компьютерных систем (далее – ОПОП), направления подготовки 10.03.01 Информационная безопасность, уровень образования: высшее образование - бакалавриат.

Требования к входным знаниям и умениям:

- знать Дисциплина базируется на следующих дисциплинах: «Правоведение», «Основы информационной безопасности», «Теория 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 10 зачетных единиц, 360 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. Система права и система законодательства	40	3	8	-	12	-	-	-	-	-	20	-	<p><u>Подготовка к практическим занятиям:</u> Изучение материала по разделу "Правовое обеспечение информационной безопасности Российской Федерации. Система права и система законодательства" подготовка к выполнению заданий на практических занятиях</p> <p><u>Самостоятельное изучение теоретического материала:</u> Изучение дополнительного материала по разделу "Правовое обеспечение информационной безопасности Российской Федерации. Система права и система законодательства"</p> <p><u>Изучение материалов литературных источников:</u> [2], 1-169</p>
1.1	Правовое обеспечение информационной безопасности Российской Федерации.	16		4	-	4	-	-	-	-	-	8	-	
1.2	Система права и система законодательства	12		2	-	4	-	-	-	-	-	6	-	
1.3	Основные функции государственных органов в области информационной безопасности	12		2	-	4	-	-	-	-	-	6	-	
2	Правовое регулирование отношений в области информации, информационных технологий и защиты информации	20		4	-	8	-	-	-	-	-	8	-	
2.1	Понятие информации,	10	2	-	4	-	-	-	-	-	4	-	<p><u>Подготовка к практическим занятиям:</u> Изучение материала по разделу "Правовое</p>	

	основы правового регулирования информации в РФ													регулирование отношений в области информации, информационных технологий и защиты информации" подготовка к выполнению заданий на практических занятиях
2.2	Основы правового регулирования сети "Интернет" в РФ	10	2	-	4	-	-	-	-	-	4	-	-	<u>Подготовка к контрольной работе:</u> Изучение материалов по разделу Правовое регулирование отношений в области информации, информационных технологий и защиты информации и подготовка к контрольной работе <u>Подготовка к текущему контролю:</u> Повторение материала по разделу "Правовое регулирование отношений в области информации, информационных технологий и защиты информации" <u>Изучение материалов литературных источников:</u> [2], 1-169
3	Правовое регулирование отдельных видов информации: государственная тайна, служебная информация, профессиональная тайна и т.д.	42	10	-	16	-	-	-	-	-	16	-	-	<u>Самостоятельное изучение теоретического материала:</u> Изучение дополнительного материала по разделу "Правовое регулирование отдельных видов информации: государственная тайна, служебная информация, профессиональная тайна и т.д." <u>Подготовка к практическим занятиям:</u> Изучение материала по разделу "Правовое регулирование отдельных видов информации: государственная тайна, служебная информация, профессиональная тайна и т.д." подготовка к выполнению заданий на практических занятиях
3.1	Законодательство в области государственной тайны.	12	4	-	4	-	-	-	-	-	4	-	-	регулирование отдельных видов информации: государственная тайна, служебная информация, профессиональная тайна и т.д." подготовка к выполнению заданий на практических занятиях
3.2	Правовое регулирование коммерческой тайны и служебной информации ограниченного распространения	10	2	-	4	-	-	-	-	-	4	-	-	<u>Подготовка к контрольной работе:</u> Изучение материалов по разделу Правовое регулирование отдельных видов информации: государственная тайна, служебная информация, профессиональная тайна и т.д. и подготовка к контрольной

3.3	Правовое регулирование обработки персональных данных	10	2	-	4	-	-	-	-	-	4	-	работе <u>Подготовка к текущему контролю:</u> Повторение материала по разделу "Правовое регулирование отдельных видов информации: государственная тайна, служебная информация, профессиональная тайна и т.д." <u>Изучение материалов литературных источников:</u> [2], 1-169
3.4	Особенности защиты отдельных видов профессиональной тайны	10	2	-	4	-	-	-	-	-	4	-	
4	Правовое регулирование объектов интеллектуальной собственности и их защита	18	4	-	6	-	-	-	-	-	8	-	<u>Подготовка к практическим занятиям:</u> Изучение материала по разделу "Правовое регулирование объектов интеллектуальной собственности и их защита" подготовка к выполнению заданий на практических занятиях <u>Самостоятельное изучение теоретического материала:</u> Изучение дополнительного материала по разделу "Правовое регулирование объектов интеллектуальной собственности и их защита" <u>Подготовка к текущему контролю:</u> Повторение материала по разделу "Правовое регулирование объектов интеллектуальной собственности и их защита" <u>Изучение материалов литературных источников:</u> [3], 1-574
4.1	Правовое регулирование авторского и смежного права	10	2	-	4	-	-	-	-	-	4	-	
4.2	Правовое регулирование объектов промышленной собственности	8	2	-	2	-	-	-	-	-	4	-	
5	Юридическая ответственность субъектов информационной сферы	24	6	-	6	-	-	-	-	-	12	-	<u>Самостоятельное изучение теоретического материала:</u> Изучение дополнительного материала по разделу "Юридическая ответственность субъектов информационной сферы" <u>Подготовка к практическим занятиям:</u> Изучение материала по разделу "Юридическая ответственность субъектов информационной сферы" подготовка к выполнению заданий на практических
5.1	Правовое регулирование уголовной ответственности в области	8	2	-	2	-	-	-	-	-	4	-	

	информационной безопасности												занятиях <u>Подготовка к текущему контролю:</u> Повторение материала по разделу "Юридическая ответственность субъектов информационной сферы" <u>Изучение материалов литературных источников:</u> [1], 1-79
5.2	Правовое регулирование административной ответственности в области информационной безопасности	8		2	-	2	-	-	-	-	-	4	-
5.3	Гражданско-правовая и дисциплинарная ответственности в области информационной безопасности	8		2	-	2	-	-	-	-	-	4	-
	Экзамен	36.0		-	-	-	-	2	-	-	0.5	-	33.5
	Всего за семестр	180.0		32	-	48	-	2	-	-	0.5	64	33.5
	Итого за семестр	180.0		32	-	48	2	-	-	-	0.5	97.5	
6	Организация защиты информации на предприятии. Разработка системы защиты информации предприятия	48	4	12	-	12	-	-	-	-	-	24	-
6.1	Общая характеристика организации защиты информации на предприятии	14		4	-	4	-	-	-	-	-	6	-
6.2	Сертификация средств защиты информации	14		4	-	4	-	-	-	-	-	6	-
6.3	Порядок организации аттестации объектов информатизации	10		2	-	2	-	-	-	-	-	6	-
6.4	Лицензирование деятельности в области информационной безопасности	10		2	-	2	-	-	-	-	-	6	-
													<u>Самостоятельное изучение теоретического материала:</u> Изучение дополнительного материала по разделу "Организация защиты информации на предприятии. Разработка системы защиты информации предприятия" <u>Подготовка к практическим занятиям:</u> Изучение материала по разделу "Организация защиты информации на предприятии. Разработка системы защиты информации предприятия" подготовка к выполнению заданий на практических занятиях <u>Подготовка к текущему контролю:</u> Повторение материала по разделу "Организация защиты информации на предприятии. Разработка системы защиты информации предприятия" <u>Изучение материалов литературных источников:</u> [3], 1-574

7	Корпоративная нормативная база по защите информации. Политика безопасности	40	12	-	8	-	-	-	-	-	-	20	-	<p><u>Самостоятельное изучение теоретического материала:</u> Изучение дополнительного материала по разделу "Корпоративная нормативная база по защите информации. Политика безопасности"</p> <p><u>Подготовка к практическим занятиям:</u> Изучение материала по разделу "Корпоративная нормативная база по защите информации. Политика безопасности" подготовка к выполнению заданий на практических занятиях</p> <p><u>Подготовка к текущему контролю:</u> Повторение материала по разделу "Корпоративная нормативная база по защите информации. Политика безопасности"</p>
7.1	Особенности работы с персоналом для обеспечения защиты информации	12	4	-	2	-	-	-	-	-	-	6	-	
7.2	Политика информационной безопасности	12	4	-	2	-	-	-	-	-	-	6	-	
7.3	Основные организационно-распорядительные документы, определяющие порядок и особенности работы с конфиденциальной информацией на предприятии	8	2	-	2	-	-	-	-	-	-	4	-	
7.4	Особенности защиты информации при организации электронного документооборота	8	2	-	2	-	-	-	-	-	-	4	-	
8	Особенности защиты информации на отдельных объектах информатизации	35.7	8	-	12	-	-	-	-	-	-	15.7	-	
8.1	Особенности защиты информации при проведении совещаний и переговоров	10	2	-	4	-	-	-	-	-	-	4	-	<p><u>Подготовка к практическим занятиям:</u> Изучение материала по разделу "Особенности защиты информации на отдельных объектах информатизации" подготовка к выполнению заданий на практических занятиях</p> <p><u>Самостоятельное изучение теоретического материала:</u> Изучение</p>
8.2	Особенности защиты информации при работе с	10	2	-	4	-	-	-	-	-	-	4	-	

	контрагентами, связанной с передачей конфиденциальной информации												дополнительного материала по разделу "Особенности защиты информации на отдельных объектах информатизации"
8.3	Особенности защиты информации на предприятиях топливно-энергетического комплекса	15.7		4	-	4	-	-	-	-	-	7.7	-
	Экзамен	36.3		-	-	-	-	2	-	-	0.8	-	33.5
	Курсовая работа (КР)	20		-	-	-	16	-	4	-	-	-	-
	Всего за семестр	180.0		32	-	32	16	2	4	-	0.8	59.7	33.5
	Итого за семестр	180.0		32	-	32	18		4		0.8	93.2	
	ИТОГО	360.0	-	64	-	80	20		4		1.3	190.7	

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. Правовое обеспечение информационной безопасности Российской Федерации. Система права и система законодательства

1.1. Правовое обеспечение информационной безопасности Российской Федерации.

Предмет, задачи и содержание курса «Организационное и правовое обеспечение защиты информации». Место курса среди других дисциплин. Структура курса. Наименование тем и их распределение по видам аудиторных занятий. Форма проведения семинаров и практических занятий. Формы проверки знаний. Анализ нормативных источников и литературы по дисциплине. Методика самостоятельной работы студентов по изучению дисциплины. Компетенции студентов, которые должны быть получены в результате изучения дисциплины. Информационные технологии изучения дисциплины..

1.2. Система права и система законодательства

Понятие «право». Субъективное, объективное и естественное право. Формы и признаки позитивного права. Публичное и частное право. Нормы права, правоотношения, субъекты и объекты права, юридические факты. Источники права. Содержание и структура законодательства. Порядок принятия законодательных актов. Национальная безопасность Российской Федерации. Государственная политика в области обеспечения безопасности. Понятие информационной безопасности. Национальные интересы России в информационной сфере. Основные источники угроз информационной безопасности Российской Федерации. Основные положения государственной политики обеспечения информационной безопасности Российской Федерации и первоочередные мероприятия по ее реализации..

1.3. Основные функции государственных органов в области информационной безопасности

Полномочия федеральных органов государственной власти, функции органов государственной власти субъектов Российской Федерации и органов местного самоуправления в области обеспечения безопасности. Статус Совета Безопасности. Составляющие национальной безопасности. Основные характеристики состояния национальной безопасности. Основные функции ФСТЭК и ФСБ России в области обеспечения информационной безопасности. Основные полномочия данных служб в области информационной безопасности, история их создания, структуры данных государственных органов. Функции ФСО, МВД, Роскомнадзора и других федеральных органов в области обеспечения информационной безопасности РФ. Организационная основа системы обеспечения информационной безопасности Российской Федерации..

2. Правовое регулирование отношений в области информации, информационных технологий и защиты информации

2.1. Понятие информации, основы правового регулирования информации в РФ

Понятие информации и правового обеспечения защиты информации (информационного права). Предмет, методы информационного права и его место в системе российского права. Содержание и структура правового обеспечения. Содержание и структура законодательства в области информационной безопасности. Понятие обладателя информации. Общедоступная информация и информация ограниченного доступа..

2.2. Основы правового регулирования сети "Интернет" в РФ

Правила распространения или предоставления информации. Особенности распространения информации в сети «Интернет». Государственное регулирование в сфере применения информационных технологий. Понятие информационных систем.

Использование информационно-телекоммуникационных сетей. Организационно-правовые меры, препятствующие распространению запрещенной информации в сети «Интернет». Порядок ограничения доступа к информации, распространяемой с нарушением авторских и (или) смежных прав. Порядок ограничения доступа к информации, распространяемой с нарушением закона. Порядок ограничения доступа к информационному ресурсу организатора распространения информации в сети «Интернет». Порядок ограничения доступа к информации, обрабатываемой с нарушением законодательства Российской Федерации в области персональных данных. Порядок ограничения доступа к сайтам в сети «Интернет», на которых неоднократно и неправомерно размещалась информация, содержащая объекты авторских и (или) смежных прав. Внесудебные меры по прекращению нарушения авторских и (или) смежных прав в информационно-телекоммуникационных сетях. Понятие защиты информации..

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

3.1. Законодательство в области государственной тайны.

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. Степени секретности сведений и грифы секретности носителей этих сведений. Порядок рассекречивания сведений. Взаимная передача сведений, составляющих государственную тайну, органами государственной власти, предприятиями, учреждениями и организациями. Органы защиты государственной тайны. Допуск и доступ к информации, составляющей государственную тайну. Социальные гарантии лицам, допущенным к государственной тайне на постоянной основе. Государственная аттестация руководителей организаций. Организация доступа к сведениям, составляющим государственную тайну..

3.2. Правовое регулирование коммерческой тайны и служебной информации ограниченного распространения

Законодательство в области служебной тайны. Понятие служебной тайны. Порядок допуска сотрудников к информации, составляющей служебную тайну. Законодательство в области коммерческой тайны. Понятие коммерческой тайны и режима коммерческой тайны. Ответственность за нарушение законодательства Российской Федерации о коммерческой тайне..

3.3. Правовое регулирование обработки персональных данных

Законодательство в области персональных данных. Понятие персональных данных. Категории персональных данных. Обработка персональных данных без использования средств автоматизации. Условия обработки персональных данных. Обработка персональных данных с письменного согласия субъекта персональных данных. Меры по обеспечению безопасности персональных данных при их обработке. Уведомление об обработке персональных данных. Типы угроз и уровни защищенности персональных данных. Порядок определения набора мер по обеспечению безопасности персональных данных. Контроль и надзор в области персональных данных..

3.4. Особенности защиты отдельных видов профессиональной тайны

Законодательство в области профессиональной тайны. Понятие профессиональной тайны. Виды профессиональных тайн. Порядок доступа к различным видам профессиональных тайн. Правовое регулирование банковской тайны.

4. Правовое регулирование объектов интеллектуальной собственности и их защита

4.1. Правовое регулирование авторского и смежного права

Законодательство в области интеллектуальной собственности. Общие положения. Авторское право и смежные права. Права на программное обеспечение.

4.2. Правовое регулирование объектов промышленной собственности

Патентное право. Изобретение, полезная модель и промышленный образец, созданные в связи с выполнением служебного задания или при выполнении работ по договору. Получение патента. Защита прав авторов и патентообладателей. Право на топологии интегральных микросхем. Право на секрет производства (ноу-хау). Права на средства индивидуализации юридических лиц, товаров, работ, услуг и предприятий. Право использования результатов интеллектуальной деятельности в составе единой технологии..

5. Юридическая ответственность субъектов информационной сферы

5.1. Правовое регулирование уголовной ответственности в области информационной безопасности

Понятие юридической ответственности. Правовосстановительная 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..

5.2. Правовое регулирование административной ответственности 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..

5.3. Гражданско-правовая и дисциплинарная ответственности в области информационной безопасности

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. Суды общей юрисдикции, арбитражные суды, третейские суды, суд по интеллектуальным правам. Процедура обращения в суд за судебной защитой..

6. Организация защиты информации на предприятии. Разработка системы защиты информации предприятия

6.1. Общая характеристика организации защиты информации на предприятии

Организация пропускного режима. Организация внутриобъектового режима. Выявление и определение объектов информатизации, обрабатывающих информацию ограниченного доступа на предприятии. Порядок учета, хранения документов ограниченного доступа и обеспечение ограничений к их доступу..

6.2. Сертификация средств защиты информации

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..

6.3. Порядок организации аттестации объектов информатизации

Понятие аттестации объектов информатизации. Порядок проведения аттестации объектов информатизации. Иные виды оценки соответствия объектов информатизации..

6.4. Лицензирование деятельности в области информационной безопасности

Понятие лицензирования. Нормативные правовые акты Российской Федерации, регламентирующие порядок лицензирования в области защиты информации. Лицензируемые виды деятельности в области защиты информации. Требования к персоналу, осуществляющему лицензируемые виды деятельности. Требования к оборудованию и программному обеспечению необходимым для осуществления лицензируемых видов деятельности. Особенности и порядок получения литературы для осуществления лицензируемых видов деятельности..

7. Корпоративная нормативная база по защите информации. Политика безопасности

7.1. Особенности работы с персоналом для обеспечения защиты информации

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..

7.2. Политика информационной безопасности

Установление порядка обращения с информацией ограниченного доступа на предприятии. Порядок определения перечня информации, составляющей коммерческую тайну или иной информации ограниченного доступа. Условия и организация доступа к информации. Понятие и состав грифа конфиденциальности документов. Порядок принятия решения об отнесении документов к информации ограниченного доступа..

7.3. Основные организационно-распорядительные документы, определяющие порядок и особенности работы с конфиденциальной информацией на предприятии

Определение и назначение ответственных лиц и подразделений. Определение перечня объектов на которых обрабатывается информация ограниченного доступа для определения режима. Формирование документов, описывающих технический процесс обработки информации и технических паспортов на объекты информатизации. Разработка инструкций, определяющих порядок отдельных видов защиты информации..

7.4. Особенности защиты информации при организации электронного документооборота

Организация внешнего и внутреннего электронного документооборота. Виды электронной подписи и правовые особенности ее применения. Удостоверяющий центр как основа организации электронного документооборота. Особенности создания внутреннего

удостоверяющего центра. Требования к работникам, участвующих в процессе выпуска электронной подписи. Особенности хранения ключей электронной подписи..

8. Особенности защиты информации на отдельных объектах информатизации

8.1. Особенности защиты информации при проведении совещаний и переговоров

Обеспечение конфиденциальности информации при проведении заседаний, совещаний, переговоров. Подготовка помещения для проведения переговоров. Определения круга лиц, приглашаемых на переговоры.

8.2. Особенности защиты информации при работе с контрагентами, связанной с передачей конфиденциальной информации

Порядок учета, хранения документов ограниченного доступа и обеспечение ограничений к их доступу. Обеспечение конфиденциальности информации при работе с контрагентом. Особенности согласования разных режимов конфиденциальности.

8.3. Особенности защиты информации на предприятиях топливно-энергетического комплекса

Особенности защиты информации в государственных и муниципальных информационных системах. Особенности защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды..

3.3. Темы практических занятий

1. 5.Порядок и особенности подготовки к лицензированию ФСТЭК России;
2. 6.Порядок и особенности подготовки к лицензированию ФСБ России;
3. 7.Порядок работы с персоналом по подготовке его к работе с информацией ограниченного доступа;
4. 14.Особенности защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды;
5. 12.Виды объектов промышленной собственности и их правовая защита;
6. 6.Полномочия и функции иных государственных органов в области информационной безопасности;
7. 9.Формирование иных корпоративных документов в области информационной безопасности. Подготовка описания технологического процесса и технического паспорта на объект информатизации;
8. 1.Понятие режима на предприятии и особенности его организации;
9. 2.Особенности выбора сертифицированных средств защиты информации. Реестр сертифицированных средств защиты информации;
10. 13.Особенности организации защиты информации в государственных и муниципальных информационных системах, реализация требований по подключению к ним;
11. 11.Порядок создания внутреннего удостоверяющего центра компании;
12. 15.Особенности применения гражданско-правовой и дисциплинарной ответственности;
13. 14.Особенности применения административной ответственности при совершении правонарушений в области информационной безопасности;
14. 3.Аттестация объектов информатизации: особенности организации и проведения;

15. 3. Отдельные интересы РФ при формировании национальной безопасности. Информационная безопасность. Экономическая безопасность;
16. 8. Формирование корпоративной политики в области информационной безопасности;
17. 1. Понятие права и государства, основные характеристики РФ как государства;
18. 7. Законодательство в области информационной безопасности. Содержание и структура законодательства. Законодательные акты в области защиты информации;
19. 9. Особенности организации на предприятии режима защиты государственной тайны;
20. 10. Особенности организации конфиденциального документооборота с использованием внешнего удостоверяющего центра;
21. 8. Классификация информации по категориям доступа к ней;
22. 11. Виды объектов авторских прав и их правовая защита;
23. 10. Особенности организации на предприятии режима коммерческой тайны;
24. 4. Особенности организации конфиденциальных переговоров на предприятии;
25. 12. Особенности организации защиты персональных данных на предприятии;
26. 13. Особенности применения уголовной ответственности при совершении преступлений в области информационной безопасности;
27. 2. Сравнение Стратегия национальной безопасности РФ до 2020 года и Доктрина информационной безопасности Российской Федерации;
28. 4. Полномочия ФСБ в области информационной безопасности. Структура и история службы;
29. 5. Полномочия ФСТЭК в области информационной безопасности. Структура и история службы.

3.4. Темы лабораторных работ не предусмотрено

3.5 Консультации

Аудиторные консультации по курсовому проекту/работе (КПР)

1. Консультации направлены на выполнение разделов курсового проекта под руководством наставника (преподавателя). В рамках часов на групповые консультации разбираются наиболее важные части расчетных заданий раздела "Правовое обеспечение информационной безопасности Российской Федерации. Система права и система законодательства"
2. Консультации направлены на выполнение разделов курсового проекта под руководством наставника (преподавателя). В рамках часов на групповые консультации разбираются наиболее важные части расчетных заданий раздела "Правовое регулирование отношений в области информации, информационных технологий и защиты информации"
3. Консультации направлены на выполнение разделов курсового проекта под руководством наставника (преподавателя). В рамках часов на групповые консультации разбираются наиболее важные части расчетных заданий раздела "Правовое регулирование отдельных видов информации: государственная тайна, служебная информация, профессиональная тайна и т.д."
4. Консультации направлены на выполнение разделов курсового проекта под руководством наставника (преподавателя). В рамках часов на групповые консультации разбираются наиболее важные части расчетных заданий раздела "Правовое регулирование объектов интеллектуальной собственности и их защита"

5. Консультации направлены на выполнение разделов курсового проекта под руководством наставника (преподавателя). В рамках часов на групповые консультации разбираются наиболее важные части расчетных заданий раздела "Юридическая ответственность субъектов информационной сферы"
6. Консультации направлены на выполнение разделов курсового проекта под руководством наставника (преподавателя). В рамках часов на групповые консультации разбираются наиболее важные части расчетных заданий раздела "Организация защиты информации на предприятии. Разработка системы защиты информации предприятия"
7. Консультации направлены на выполнение разделов курсового проекта под руководством наставника (преподавателя). В рамках часов на групповые консультации разбираются наиболее важные части расчетных заданий раздела "Корпоративная нормативная база по защите информации. Политика безопасности"
8. Консультации направлены на выполнение разделов курсового проекта под руководством наставника (преподавателя). В рамках часов на групповые консультации разбираются наиболее важные части расчетных заданий раздела "Особенности защиты информации на отдельных объектах информатизации"

Групповые консультации по разделам дисциплины (ГК)

1. Обсуждение материалов по кейсам раздела "Правовое обеспечение информационной безопасности Российской Федерации. Система права и система законодательства"
2. Обсуждение материалов по кейсам раздела "Правовое регулирование отношений в области информации, информационных технологий и защиты информации"
3. Обсуждение материалов по кейсам раздела "Правовое регулирование отдельных видов информации: государственная тайна, служебная информация, профессиональная тайна и т.д."
4. Обсуждение материалов по кейсам раздела "Правовое регулирование объектов интеллектуальной собственности и их защита"
5. Обсуждение материалов по кейсам раздела "Юридическая ответственность субъектов информационной сферы"
6. Обсуждение материалов по кейсам раздела "Организация защиты информации на предприятии. Разработка системы защиты информации предприятия"
7. Обсуждение материалов по кейсам раздела "Корпоративная нормативная база по защите информации. Политика безопасности"
8. Обсуждение материалов по кейсам раздела "Особенности защиты информации на отдельных объектах информатизации"

Индивидуальные консультации по курсовому проекту /работе (ИККП)

1. Консультации проводятся по разделу "Правовое обеспечение информационной безопасности Российской Федерации. Система права и система законодательства"
2. Консультации проводятся по разделу "Правовое регулирование отношений в области информации, информационных технологий и защиты информации"
3. Консультации проводятся по разделу "Правовое регулирование отдельных видов информации: государственная тайна, служебная информация, профессиональная тайна и т.д."
4. Консультации проводятся по разделу "Правовое регулирование объектов интеллектуальной собственности и их защита"
5. Консультации проводятся по разделу "Юридическая ответственность субъектов информационной сферы"
6. Консультации проводятся по разделу "Организация защиты информации на предприятии. Разработка системы защиты информации предприятия"
7. Консультации проводятся по разделу "Корпоративная нормативная база по защите информации. Политика безопасности"

8. Консультации проводятся по разделу "Особенности защиты информации на отдельных объектах информатизации"

Текущий контроль (ТК)

1. Консультации направлены на получение индивидуального задания для выполнения контрольных мероприятий по разделу "Правовое обеспечение информационной безопасности Российской Федерации. Система права и система законодательства"
2. Консультации направлены на получение индивидуального задания для выполнения контрольных мероприятий по разделу "Правовое регулирование отношений в области информации, информационных технологий и защиты информации"
3. Консультации направлены на получение индивидуального задания для выполнения контрольных мероприятий по разделу "Правовое регулирование отдельных видов информации: государственная тайна, служебная информация, профессиональная тайна и т.д."
4. Консультации направлены на получение индивидуального задания для выполнения контрольных мероприятий по разделу "Правовое регулирование объектов интеллектуальной собственности и их защита"
5. Консультации направлены на получение индивидуального задания для выполнения контрольных мероприятий по разделу "Юридическая ответственность субъектов информационной сферы"
6. Консультации направлены на получение индивидуального задания для выполнения контрольных мероприятий по разделу "Организация защиты информации на предприятии. Разработка системы защиты информации предприятия"
7. Консультации направлены на получение индивидуального задания для выполнения контрольных мероприятий по разделу "Корпоративная нормативная база по защите информации. Политика безопасности"
8. Консультации направлены на получение индивидуального задания для выполнения контрольных мероприятий по разделу "Особенности защиты информации на отдельных объектах информатизации"

3.6 Тематика курсовых проектов/курсовых работ

4 Семестр

Курсовая работа (КР)

Темы:

- 1. Обзор нормативно-правовых актов по обеспечению защиты информации в организации
2. Основные направления государственной политики России в сфере информационной безопасности
3. Понятие информации и ее виды по порядку организации доступа к ней
4. Основные элементы организационной основы системы обеспечения информационной безопасности России
5. Полномочия в области информационной безопасности и история создания ФСТЭК России
6. Полномочия в области информационной безопасности и история создания ФСБ России
7. Полномочия МВД России, ФСО России, Службы внешней разведки и Федеральная служба войск национальной гвардии в области информационной безопасности
8. Организация лицензирования деятельности в области защиты информации, осуществляемое ФСТЭК России
9. Организация лицензирования деятельности в области защиты информации, осуществляемое ФСБ России
10. Понятие «коммерческая тайна», особенности ее установления на предприятии
11. Понятие «служебная информация», особенности определения режима её обработки
12. Информация, относимая к секрету производства, особенности ее правовой и организационной защиты
13. Особенности правового регулирования объектов интеллектуальной собственности и порядок их защиты
14. Банковская тайна и порядок ее определения и защиты
15. Профессиональная информация ограниченного доступа и порядок ее защиты
16. Персональные данные и иная личная информация ограниченного доступа и порядок ее защиты
17. Ответственность за нарушение законодательства в сфере защиты информации и особенности ее применения
18. Правовое

регулирование применения электронной подписи 19. Понятие и виды электронной подписи, порядок применения электронной подписи во внутреннем (внешнем) документообороте 20. Особенности подтверждения соответствия средств защиты информации установленным нормативным требованиям. 21. Система сертификации средств защиты информации в России 22. Аттестация объектов информатизации, как способ подтверждения соответствия систем установленным требованиям 23. Порядок организации защиты информации на предприятии 24. Особенности разработки положения о пропускном режиме на предприятии 25. Особенности хранения материальных носителей, содержащих информацию ограниченного распространения 26. Организация доступа и допуска персонала к информации ограниченного распространения 27. Особенности защиты информации при проведении совещаний 28. Особенности организации публикации различной информации, на предприятиях, обрабатывающих информацию ограниченного распространения 29. Организация внутриобъектового режима на предприятии 30. Планирование мероприятий по защите информации на предприятии 31. Организация контроля за состоянием защиты информации на предприятии 32. Порядок подключения операторов к Единой Биометрической Системе (ЕБС) 33. Порядок защиты информации в государственной информационной системе на примере конкретной государственной информационной системы (ГИС) 34. Особенности обработки и защиты персональных данных при создании системы «Умный город» 35. Особенности привлечения к ответственности за киберпреступления в России 36. Правовое регулирование веб-приложений и программного обеспечения, обрабатывающего персональные данные 37. Сравнение законодательства России в области ПДн с европейским GDPR 38. Правовое регулирование интернета в России

График выполнения курсового проекта

Неделя	1 - 8	9 - 15	Зачетная
Раздел курсового проекта	1	2	Защита курсового проекта
Объем раздела, %	50	50	-
Выполненный объем нарастающим итогом, %	50	100	-

Номер раздела	Раздел курсового проекта
1	Соблюдение графика выполнения КП/КР
2	Применение в работе судебной практики и подзаконных нормативных актов

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	6	7	8	
Знать:										
требования нормативных актов в области защиты информации	ИД-2 _{ОПК-5}	+								Контрольная работа/Основные функции государственных органов в области информационной безопасности
требования нормативных актов по формированию политики информационной безопасности	ИД-1 _{ОПК-10}		+							Контрольная работа/Правовое регулирование отношений в области информации, информационных технологий и защиты информации
Уметь:										
применять информационные технологии для поиска и обработки информации, в том числе информационно-правовые системы	ИД-1 _{ОПК-1}			+	+					Мозговой штурм/Правовое регулирование отдельных видов информации: государственная тайна, служебная информация, профессиональная тайна и т.д.
выполнять подбор, изучение и обобщение научно-технической литературы, нормативных и методических материалов, составляет обзор по вопросам обеспечения информационной безопасности по профилю своей профессиональной деятельности	ИД-1 _{ОПК-8}					+				Семинар/Юридическая ответственность субъектов информационной сферы
применять комплексный подход к обеспечению информационной безопасности объекта защиты	ИД-1 _{ОПК-10}						+	+		Кейс (решение конкретных производственных ситуаций)/Корпоративная нормативная база по защите информации. Особенности защиты информации при организации электронного документооборота Семинар/Лицензирование деятельности в области информационной безопасности. Особенности работы с персоналом для обеспечения защиты информации

											Контрольная работа/Организация защиты информации на предприятии. Разработка системы защиты информации предприятия
управлять процессом реализации мер защиты информации	ИД-2опк-10							+	+		Семинар/Особенности защиты информации на отдельных объектах информатизации

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

4.1. Текущий контроль успеваемости

3 семестр

Форма реализации: Письменная работа

1. Основные функции государственных органов в области информационной безопасности (Контрольная работа)
2. Правовое регулирование отношений в области информации, информационных технологий и защиты информации (Контрольная работа)

Форма реализации: Проверка задания

1. Юридическая ответственность субъектов информационной сферы (Семинар)

Форма реализации: Устная форма

1. Правовое регулирование отдельных видов информации: государственная тайна, служебная информация, профессиональная тайна и т.д. (Мозговой штурм)

4 семестр

Форма реализации: Письменная работа

1. Организация защиты информации на предприятии. Разработка системы защиты информации предприятия (Контрольная работа)
2. Особенности защиты информации на отдельных объектах информатизации (Семинар)

Форма реализации: Проверка задания

1. Корпоративная нормативная база по защите информации. Особенности защиты информации при организации электронного документооборота (Кейс (решение конкретных производственных ситуаций))
2. Лицензирование деятельности в области информационной безопасности. Особенности работы с персоналом для обеспечения защиты информации (Семинар)

Балльно-рейтинговая структура дисциплины является приложением А.

Балльно-рейтинговая структура курсовой работы является приложением Б.

4.2 Промежуточная аттестация по дисциплине

Экзамен (Семестр №3)

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

Экзамен (Семестр №4)

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

Курсовая работа (КР) (Семестр №4)

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 4 семестр.

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

5. УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

5.1 Печатные и электронные издания:

1. Т. А. Гульятеева- "Основы информационной безопасности", Издательство: "Новосибирский государственный технический университет", Новосибирск, 2018 - (79 с.)
<https://biblioclub.ru/index.php?page=book&id=574729>;
2. С. А. Комаров, Е. В. Мицкая- "Правовое регулирование обеспечения информационной безопасности и защиты персональных данных", Санкт-Петербург, 2018 - (169 с.)
<https://biblioclub.ru/index.php?page=book&id=564652>;
3. В.А. Сердюк- "Организация и технологии защиты информации: обнаружение и предотвращение информационных атак в автоматизированных системах предприятий", Издательство: "Издательский дом Высшей школы экономики", Москва, 2015 - (574 с.)
<http://biblioclub.ru/index.php?page=book&id=440285>.

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. Научная электронная библиотека - <https://elibrary.ru/>
3. Национальная электронная библиотека - <https://rusneb.ru/>
4. ЭБС "Консультант студента" - <http://www.studentlibrary.ru/>
5. Электронная библиотека МЭИ (ЭБ МЭИ) - <http://elib.mpei.ru/login.php>
6. Портал открытых данных Российской Федерации - <https://data.gov.ru>
7. Информационно-справочная система «Кодекс/Техэксперт» - [Http://proinfosoft.ru](Http://proinfosoft.ru;);
<http://docs.cntd.ru/>
8. Национальный портал онлайн обучения «Открытое образование» - <https://openedu.ru>
9. 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	Н-204, Учебная аудитория	парта со скамьей, стол преподавателя, стул, трибуна, доска меловая, колонки звуковые, мультимедийный проектор, экран
	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	К-301, Учебная аудитория	стол преподавателя, стол учебный, стул, мультимедийный проектор, экран, доска маркерная, кондиционер
Учебные аудитории для	Ж-120, Машинный	сервер, кондиционер

проведения промежуточной аттестации	зал ИВЦ	
	К-301, Учебная аудитория	стол преподавателя, стол учебный, стул, мультимедийный проектор, экран, доска маркерная, 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
Помещения для консультирования	А-300, Учебная аудитория "А"	кресло рабочее, парта, стеллаж, стол преподавателя, стол учебный, стул, трибуна, микрофон, мультимедийный проектор, экран, доска маркерная, колонки, техническая аппаратура, кондиционер, телевизор
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

Организационное и правовое обеспечение информационной безопасности

(название дисциплины)

3 семестр

Перечень контрольных мероприятий текущего контроля успеваемости по дисциплине:

- КМ-1 Основные функции государственных органов в области информационной безопасности (Контрольная работа)
- КМ-2 Правовое регулирование отдельных видов информации: государственная тайна, служебная информация, профессиональная тайна и т.д. (Мозговой штурм)
- КМ-3 Правовое регулирование отношений в области информации, информационных технологий и защиты информации (Контрольная работа)
- КМ-4 Юридическая ответственность субъектов информационной сферы (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. Система права и система законодательства					
1.1	Правовое обеспечение информационной безопасности Российской Федерации.		+			
1.2	Система права и система законодательства		+			
1.3	Основные функции государственных органов в области информационной безопасности		+			
2	Правовое регулирование отношений в области информации, информационных технологий и защиты информации					
2.1	Понятие информации, основы правового регулирования информации в РФ				+	
2.2	Основы правового регулирования сети "Интернет" в РФ				+	
3	Правовое регулирование отдельных видов информации: государственная тайна, служебная информация, профессиональная тайна и т.д.					
3.1	Законодательство в области государственной тайны.			+		
3.2	Правовое регулирование коммерческой тайны и служебной информации ограниченного распространения			+		
3.3	Правовое регулирование обработки персональных данных			+		
3.4	Особенности защиты отдельных видов профессиональной тайны			+		

4	Правовое регулирование объектов интеллектуальной собственности и их защита				
4.1	Правовое регулирование авторского и смежного права		+		
4.2	Правовое регулирование объектов промышленной собственности		+		
5	Юридическая ответственность субъектов информационной сферы				
5.1	Правовое регулирование уголовной ответственности в области информационной безопасности				+
5.2	Правовое регулирование административной ответственности в области информационной безопасности				+
5.3	Гражданско-правовая и дисциплинарная ответственности в области информационной безопасности				+
Вес КМ, %:		20	30	30	20

4 семестр

Перечень контрольных мероприятий текущего контроля успеваемости по дисциплине:

- КМ-1 Лицензирование деятельности в области информационной безопасности. Особенности работы с персоналом для обеспечения защиты информации (Семинар)
- КМ-2 Организация защиты информации на предприятии. Разработка системы защиты информации предприятия (Контрольная работа)
- КМ-3 Корпоративная нормативная база по защите информации. Особенности защиты информации при организации электронного документооборота (Кейс (решение конкретных производственных ситуаций))
- КМ-4 Особенности защиты информации на отдельных объектах информатизации (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	Организация защиты информации на предприятии. Разработка системы защиты информации предприятия					
1.1	Общая характеристика организации защиты информации на предприятии		+	+	+	
1.2	Сертификация средств защиты информации		+	+	+	
1.3	Порядок организации аттестации объектов информатизации		+	+	+	
1.4	Лицензирование деятельности в области информационной безопасности		+	+	+	
2	Корпоративная нормативная база по защите информации. Политика безопасности					
2.1	Особенности работы с персоналом для обеспечения защиты информации		+	+	+	
2.2	Политика информационной безопасности		+	+	+	

2.3	Основные организационно-распорядительные документы, определяющие порядок и особенности работы с конфиденциальной информацией на предприятии	+	+	+	
2.4	Особенности защиты информации при организации электронного документооборота				+
3	Особенности защиты информации на отдельных объектах информатизации				
3.1	Особенности защиты информации при проведении совещаний и переговоров				+
3.2	Особенности защиты информации при работе с контрагентами, связанной с передачей конфиденциальной информации				+
3.3	Особенности защиты информации на предприятиях топливно-энергетического комплекса				+
Вес КМ, %:		25	25	25	25

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

Организационное и правовое обеспечение информационной безопасности

(название дисциплины)

4 семестр

Перечень контрольных мероприятий текущего контроля успеваемости по курсовой работе:

КМ-1 Соблюдение графика выполнения КП/КР

КМ-2 Применение в работе судебной практики и подзаконных нормативных актов

Вид промежуточной аттестации – защита КР.

Номер раздела	Раздел курсового проекта/курсовой работы	Индекс КМ:	КМ-1	КМ-2
		Неделя КМ:	8	15
1	Соблюдение графика выполнения КП/КР		+	
2	Применение в работе судебной практики и подзаконных нормативных актов			+
Вес КМ, %:			50	50