МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное бюджетное образовательное учреждение высшего образования

«Воронежский государственный технический университет»

УТВЕРЖДАЮ

Декан факультета ФИТКБ

_____/Гусев П.Ю./

28.02.2023 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

«Организационное и правовое обеспечение информационной безопасности»

Специальность 10.05.03 Информационная безопасность автоматизированных систем

Специализация специализация N 7 "Анализ безопасности информационных систем"

Квалификация выпускника специалист по защите информации

Нормативный период обучения 5 лет и 6 м.

Форма обучения очная

Год начала подготовки 2023

Автор программы _____ Л.В. Паринова

Заведующий кафедрой Систем информационной безопасности _____ А.Г. Остапенко

Руководитель ОПОП _____ А.Г. Остапенко

Воронеж 2023

1. ЦЕЛИ И ЗАДАЧИ ДИСЦИПЛИНЫ

1.1. Цели дисциплины

усвоение законодательно-правовых основ правового обеспечения информационной безопасности, принципов построения систем обеспечения информационной безопасности, анализа и оценки угроз информационной безопасности объектов, средств и методов физической защиты объектов, изучение лицензионной и сертификационной деятельности в области защиты информации.

1.2. Задачи освоения дисциплины

1) получение представления об информационном законодательстве Российской Федерации;

2) освоение системы защиты государственной тайны;

3) ознакомление с правилами лицензирования и сертификации в области защиты информации.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП

Дисциплина «Организационное и правовое обеспечение информационной безопасности» относится к дисциплинам части, формируемой участниками образовательных отношений блока Б.1 учебного плана.

3. ПЕРЕЧЕНЬ ПЛАНИРУЕМЫХ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ

Процесс изучения дисциплины «Организационное и правовое обеспечение информационной безопасности» направлен на формирование следующих компетенций:

Компетенция	Результаты обучения, характеризующие сформированность компетенции
ОПК-5. Способен применять нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации	знает основы: российской правовой системы и законодательства, правового статуса личности, организации и деятельности органов государственной власти в Российской Федерации
	знает основные понятия и характеристику основных отраслей права, применяемых в профессиональной деятельности организации
	знает основы законодательства Российской Федерации, нормативные правовые акты, нормативные и методические документы в области информационной безопасности и защиты информации, правовые основы организации защиты государственной тайны и конфиденциальной информации, правовую характеристику преступлений в сфере компьютерной информации и меры правовой и дисциплинарной ответственности за разглашение защищаемой информации

	знает правовые основы организации защиты персональных данных и охраны результатов интеллектуальной деятельности
	знает основы: российской правовой системы и законодательства, правового статуса личности, организации и деятельности органов государственной власти в Российской Федерации
	знает нормативные документы в области технической защиты информации
	знает основные документы по стандартизации в сфере управления ИБ
	знает принципы формирования политики информационной безопасности в автоматизированных системах
	знает требования информационной безопасности при эксплуатации автоматизированной системы
	знает условные графические обозначения видов проводки, материалов конструкций, электронных компонентов в соответствии с требованиями ЕСПД и ЕСКД
	умеет обосновывать решения, связанные с реализацией правовых норм по защите информации в пределах должностных обязанностей, предпринимать необходимые меры по восстановлению нарушенных прав
	умеет анализировать и разрабатывать проекты локальных правовых актов, инструкций, регламентов и организационно-распорядительных документов, регламентирующих работу по обеспечению информационной безопасности в организации
	умеет формулировать основные требования при лицензировании деятельности в области защиты информации, сертификации и аттестации по требованиям безопасности информации
	умеет формулировать основные требования информационной безопасности при эксплуатации автоматизированной системы
	умеет формулировать основные требования по защите конфиденциальной информации, персональных данных и охране результатов интеллектуальной деятельности в организации
	умеет формировать политики информационной безопасности организации
	умеет выполнять полный объем работ, связанных с реализацией частных политик информационной безопасности автоматизированной системы
	умеет использовать программные средства для построения графических схем и алгоритмов в соответствии с требованиями ЕСПД и ЕСКД

4. ОБЪЕМ ДИСЦИПЛИНЫ

Общая трудоемкость дисциплины «Организационное и правовое обеспечение информационной безопасности» составляет 6 зачетных единиц.

Распределение трудоемкости дисциплины по видам занятий

Очная форма обучения

Вид учебной работы	Всего часов	Семестры	
		1	2
Аудиторные занятия (всего)	90	54	36
В том числе:			
Лекции	36	18	18
Практические занятия (ПЗ)	54	36	18
Лабораторные работы (ЛР)	0	0	0
Самостоятельная работа	144	36	108
Курсовой проект(работа) (есть, нет)		нет	нет
Контрольная работа (есть, нет)		нет	есть
Вид промежуточной аттестации (зачет, зачет с оценкой, экзамен)		зачет с оценкой	зачет с оценкой
Общая трудоемкость час	234	90	144
зач. ед.	6	2	4

5. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

5.1 Содержание разделов дисциплины и распределение трудоемкости по видам занятий

очная форма обучения

№ п/п	Наименование темы	Содержание раздела	Лекц	Прак зан.	СРС	Всего, час
1	Введение	Содержание и задачи дисциплины. Особенности дисциплины и ее связь с другими дисциплинами. Методические рекомендации по изучению.	4	0	0	4
2	Правовое обеспечение	Основные понятия в области организационно-правового обеспечения информационной безопасности. Законодательство РФ в области информационной безопасности, защиты государственной тайны и конфиденциальной информации. Защита информации. Процесс ЗИ, обеспечение и обслуживание процесса ЗИ, управление процессом ЗИ, координация деятельности в области ЗИ. Системы защиты информации. Государственная система ЗИ (ГСЗИ). Целевые (объектные) и функциональные подсистемы ЗИ. Системы систем подготовки кадров в области ЗИ, систем лицензирования, сертификации, аттестования, проведения НИОКР, оказания услуг в области ЗИ. Система документов в области ЗИ. Основы теории государства и права как фундаментальной дисциплины для изучения организационно-правового обеспечения информационной безопасности Место теории государства и права в системе юридических наук. Основные понятия теории государства и права. Правовые отношения. Виды правовых отношений в сфере ЗИ. Правовые нормы. Методы правового регулирования общественных отношений. Право, ограничение права, обязанность, ответственность в сфере информационных отношений. Классификация отраслей права. Система законодательного регулирования общественных отношений в области обеспечения информационной безопасности. Концепция построения системы законодательного регулирования общественных отношений в области обеспечения информационной	14	28	72	114

		безопасности. Роль и место Конституции РФ, конституционных законов, Гражданского Уголовного кодексов, Кодекса об административных правонарушениях, Кодекса законов о труде, других общих и специальных законов в области ЗИ, защиты интеллектуальной собственности в регулировании общественных отношений в процессе создания, распространения и использования информации, информатизации и защиты информации. Конституционные основы обеспечения информационной безопасности в РФ. Основы конституционного строя. Права и свободы человека и гражданина как важнейшего субъекта ЗИ. Федеративное устройство России и его влияние на организацию ЗИ. Функции Президента РФ, Федерального Собрания, Правительства РФ, федеральных органов исполнительной власти, органов судебной власти, органов государственной власти субъектов РФ, органов местного самоуправления в решении вопросов обеспечения информационной безопасности. Регламентация вопросов обеспечения информационной безопасности в Гражданском кодексе РФ Информация как объект гражданских прав. Виды информации, подлежащие защите в процессе обычного гражданского оборота. Регламентация вопросов защиты служебной, коммерческой и банковской тайны, интеллектуальной собственности. Использование электронно-цифровой подписи при совершении сделок. Регламентация вопросов обеспечения информационной безопасности в Уголовном кодексе РФ виды ответственности за преступления в информационной сфере. Ответственность в сфере компьютерной информации: за неправомерный доступ к компьютерной информации, за создание, использование и распространение вредоносных программ для ЭВМ, а также за нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети. Закон РФ «О государственной тайне» Система защиты государственной тайны. Перечень сведений, составляющих государственную тайну. Отнесение сведений к государственной тайне и их засекречивание. Рассекречивание сведений и их носителей. Распоряжение сведениями, составляющими государственную тайну. Правовой режим защиты государственной тайны. Финансирование мероприятий по защите государственной тайны. Федеральные законы «Об информации, информатизации и защите информации» и «Об участии в международном информационном обмене». Информационные ресурсы как объект защиты. Классификация информационных ресурсов. Государственные и негосударственные информационные ресурсы. Персональные данные. Пользование информационными ресурсами. Информатизация, информационные системы и средства их обеспечения. Защита информации и прав субъектов информационных отношений. Системы защиты информационных ресурсов. Законы РФ «Об авторском праве и смежных правах», «О правовой охране программ для электронно-вычислительных машин и баз данных». Предмет регулирования авторского права. Сфера действия авторского права. Объект авторского права. Смежные права. Сфера действия смежных прав. Субъекты смежных прав. Нарушение авторских и смежных прав. Защита авторских и смежных прав. Регламентация вопросов ЗИ в Федеральных законах общего характера Основные нормы и требования по ЗИ, содержащиеся в законах: «О безопасности», «Об обороне», «Об органах федеральной службы безопасности в Российской Федерации», «О федеральных органах правительственной связи и информации», «О внешней разведке», «О милиции»», «О конверсии				

		оборонной промышленности в Российской Федерации», «О закрытом административно-территориальном образовании», «О связи», «О рекламе», «О недрах» и др. Международное законодательство в области обеспечения информационной безопасности и защиты информации. Принципы правового регулирования вопросов обеспечения информационной безопасности и ЗИ в США, Франции, Великобритании, ФРГ и других государствах. Краткая характеристика основных законодательно-правовых документов в области ЗИ, действующих в указанных государствах. Основы организации обеспечения информационной безопасности и ЗИ. Основные положения концепции обеспечения информационной безопасности РФ. Основные положения концепции ЗИ в РФ. Распределение полномочий по обеспечению информационной безопасности в РФ. Научно-технические проблемы, требующие скоординированных действий различных органов государственной власти. Система документов в области обеспечения информационной безопасности и защиты информации. Обоснование необходимой и достаточной системы документов в области ЗИ. Общегосударственные документы. Организационно-распорядительные документы. Специальные нормативные документы Гостехкомиссии России по вопросам защиты информации от технических разведок, несанкционированного доступа и несанкционированных воздействий на информацию. Нормативные документы государственной системы стандартизации. Плановые документы. Информационные документы.				
3	Организационное обеспечение	Определение целей и задач обеспечения информационной безопасности и защиты информации Классификация объектов обеспечения информационной безопасности и защиты информации. Структуризация понятия «объект защиты». Составные части объекта защиты. Виды защищаемой информации, носителей информации и информационных процессов. Характеристика промышленных предприятий, учреждений, информационно-телекоммуникационных систем как объектов защиты. Лицензирование деятельности в области ЗИ. Правовые основы лицензирование деятельности в области ЗИ. Структура системы лицензирования, функции ее органов. Порядок проведения лицензирования. Распределений полномочий по лицензированию деятельности в области ЗИ между федеральными органами государственной власти. Сертификация средств ЗИ Правовые основы сертификации ЗИ. Структура системы сертификации, функции ее органов. Порядок сертификации ЗИ. Распределений полномочий по сертификации средств ЗИ между федеральными органами государственной власти. Аттестование объектов по выполнению требований обеспечения защиты информации. Правовые основы аттестования объектов по выполнению требований обеспечения защиты информации. Структура системы аттестования, функции ее органов. Порядок аттестования объектов органов управления, промышленных объектов, систем информатизации и связи. Распределений полномочий по аттестованию между федеральными органами государственной власти. Подготовка (переподготовка) и повышение квалификации специалистов в области ЗИ Правовые основы подготовки специалистов в области ЗИ. Система учебных заведений. Перечень специальностей. Основные нормативные документы по подготовке специалистов в области ЗИ. Организация контроля состояния ЗИ. Правовые основы контроля состояния ЗИ. Основные организационно-распорядительные и нормативные документы по контролю состояния ЗИ. Цели и задачи контроля. Формы	18	26	72	116

		контроля: межведомственный контроль; ведомственный контроль; контроль, осуществляемый собственником информации. Органы контроля. Контроль организации и эффективности ЗИ. Методы контроля: информационно-логический; расчетный; инструментальный; инструментально-расчетный; программный. Нарушения установленных требований и норм ЗИ. Организация ЗИ на объектах органов государственной власти и управления. Требования к содержанию Руководств по ЗИ на объекте. Цели и задачи ЗИ. Определение защищаемых информационных ресурсов. Оценка возможностей технических разведок и других источников угроз безопасности информации. Разработка организационных и технических мероприятий по ЗИ. Аттестование объектов.				
		Итого	36	54	114	234

5.2 Перечень лабораторных работ

Не предусмотрено учебным планом

6. ПРИМЕРНАЯ ТЕМАТИКА КУРСОВЫХ ПРОЕКТОВ (РАБОТ) И КОНТРОЛЬНЫХ РАБОТ

Не предусмотрено учебным планом

7. ОЦЕНОЧНЫЕ МАТЕРИАЛЫ ДЛЯ ПРОВЕДЕНИЯ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ОБУЧАЮЩИХСЯ ПО ДИСЦИПЛИНЕ

7.1. Описание показателей и критериев оценивания компетенций на различных этапах их формирования, описание шкал оценивания

7.1.1 Этап текущего контроля

Результаты текущего контроля знаний и межсессионной аттестации оцениваются по следующей системе:

«аттестован»;

«не аттестован».

Компетенция	Результаты обучения, характеризующие сформированность компетенции	Критерии оценивания	Аттестован	Не аттестован
ОПК-5	знает основы: российской правовой системы и законодательства, правового статуса личности, организации и деятельности органов государственной власти в Российской Федерации	Соответствие результатам обучения, характеризующим сформированность компетенций	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах

	знает основные понятия и характеристику основных отраслей права, применяемых в профессиональной деятельности организации	Соответствие результатам обучения, характеризующим сформированность компетенций	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
	знает основы законодательства Российской Федерации, нормативные правовые акты, нормативные и методические документы в области информационной безопасности и защиты информации, правовые основы организации защиты государственной тайны и конфиденциальной информации, правовую характеристику преступлений в сфере компьютерной информации и меры правовой и дисциплинарной ответственности за разглашение защищаемой информации	Соответствие результатам обучения, характеризующим сформированность компетенций	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
	знает правовые основы организации защиты персональных данных и охраны результатов интеллектуальной деятельности	Соответствие результатам обучения, характеризующим сформированность компетенций	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
	знает основы: российской правовой системы и законодательства, правового статуса личности, организации и деятельности органов государственной власти в Российской Федерации	Соответствие результатам обучения, характеризующим сформированность компетенций	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
	знает нормативные документы в области технической защиты информации	Соответствие результатам обучения, характеризующим сформированность компетенций	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
	знает основные документы по стандартизации в сфере управления ИБ	Соответствие результатам обучения, характеризующим сформированность компетенций	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
	знает принципы формирования политики информационной безопасности в автоматизированных системах	Соответствие результатам обучения, характеризующим сформированность компетенций	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
	знает требования информационной безопасности при эксплуатации автоматизированной системы	Соответствие результатам обучения, характеризующим сформированность компетенций	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах

	знает условные графические обозначения видов проводки, материалов конструкций, электронных компонентов в соответствии с требованиями ЕСПД и ЕСКД	Соответствие результатам обучения, характеризующим сформированность компетенций	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
	умеет обосновывать решения, связанные с реализацией правовых норм по защите информации в пределах должностных обязанностей, предпринимать необходимые меры по восстановлению нарушенных прав	Соответствие результатам обучения, характеризующим сформированность компетенций	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
	умеет анализировать и разрабатывать проекты локальных правовых актов, инструкций, регламентов и организационно-распорядительных документов, регламентирующих работу по обеспечению информационной безопасности в организации	Соответствие результатам обучения, характеризующим сформированность компетенций	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
	умеет формулировать основные требования при лицензировании деятельности в области защиты информации, сертификации и аттестации по требованиям безопасности информации	Соответствие результатам обучения, характеризующим сформированность компетенций	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
	умеет формулировать основные требования информационной безопасности при эксплуатации автоматизированной системы	Соответствие результатам обучения, характеризующим сформированность компетенций	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
	умеет формулировать основные требования по защите конфиденциальной информации, персональных данных и охране результатов интеллектуальной деятельности в организации	Соответствие результатам обучения, характеризующим сформированность компетенций	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
	умеет формировать политики информационной безопасности организации	Соответствие результатам обучения, характеризующим сформированность компетенций	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
	умеет выполнять полный объем работ, связанных с реализацией частных политик информационной безопасности автоматизированной системы	Соответствие результатам обучения, характеризующим сформированность компетенций	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах

	умеет использовать программные средства для построения графических схем и алгоритмов в соответствии с требованиями ЕСПД и ЕСКД	Соответствие результатам обучения, характеризующим сформированность компетенций	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах

7.1.2 Этап промежуточного контроля знаний

Результаты промежуточного контроля знаний оцениваются во 2 семестре:

«отлично»;

«хорошо»;

«удовлетворительно»;

«неудовлетворительно»

Компетенция	Результаты обучения, характеризующие сформированность компетенции	Критерии оценивания	Отлично	Хорошо	Удовл	Неудовл
ОПК-5	знает основы: российской правовой системы и законодательства, правового статуса личности, организации и деятельности органов государственной власти в Российской Федерации	Тест	Выполнение теста на 90-100%	Выполнение теста на 80-90%	Выполнение теста на 70-80%	В тесте менее 70% правильных ответов
	знает основные понятия и характеристику основных отраслей права, применяемых в профессиональной деятельности организации	Тест	Выполнение теста на 90-100%	Выполнение теста на 80-90%	Выполнение теста на 70-80%	В тесте менее 70% правильных ответов
	знает основы законодательства Российской Федерации, нормативные правовые акты, нормативные и методические документы в области информационной безопасности и защиты информации, правовые основы организации защиты государственной тайны и конфиденциальной информации, правовую характеристику преступлений в сфере компьютерной информации и меры правовой и дисциплинарной ответственности за разглашение защищаемой информации	Тест	Выполнение теста на 90-100%	Выполнение теста на 80-90%	Выполнение теста на 70-80%	В тесте менее 70% правильных ответов
	знает правовые основы организации защиты	Тест	Выполнение теста на 90-	Выполнение теста на 80-	Выполнение теста на 70-	В тесте менее 70%

персональных данных и охраны результатов интеллектуальной деятельности		100%	90%	80%	правильных ответов
знает основы: российской правовой системы и законодательства, правового статуса личности, организации и деятельности органов государственной власти в Российской Федерации	Тест	Выполнение теста на 90-100%	Выполнение теста на 80-90%	Выполнение теста на 70-80%	В тесте менее 70% правильных ответов
знает нормативные документы в области технической защиты информации	Тест	Выполнение теста на 90-100%	Выполнение теста на 80-90%	Выполнение теста на 70-80%	В тесте менее 70% правильных ответов
знает основные документы по стандартизации в сфере управления ИБ	Тест	Выполнение теста на 90-100%	Выполнение теста на 80-90%	Выполнение теста на 70-80%	В тесте менее 70% правильных ответов
знает принципы формирования политики информационной безопасности в автоматизированных системах	Тест	Выполнение теста на 90-100%	Выполнение теста на 80-90%	Выполнение теста на 70-80%	В тесте менее 70% правильных ответов
знает требования информационной безопасности при эксплуатации автоматизированной системы	Тест	Выполнение теста на 90-100%	Выполнение теста на 80-90%	Выполнение теста на 70-80%	В тесте менее 70% правильных ответов
знает условные графические обозначения видов проводки, материалов конструкций, электронных компонентов в соответствии с требованиями ЕСПД и ЕСКД	Тест	Выполнение теста на 90-100%	Выполнение теста на 80-90%	Выполнение теста на 70-80%	В тесте менее 70% правильных ответов
умеет обосновывать решения, связанные с реализацией правовых норм по защите информации в пределах должностных обязанностей, предпринимать необходимые меры по восстановлению нарушенных прав	Тест	Выполнение теста на 90-100%	Выполнение теста на 80-90%	Выполнение теста на 70-80%	В тесте менее 70% правильных ответов
умеет анализировать и разрабатывать проекты локальных правовых актов, инструкций, регламентов и организационно-распорядительных документов,	Тест	Выполнение теста на 90-100%	Выполнение теста на 80-90%	Выполнение теста на 70-80%	В тесте менее 70% правильных ответов

	регламентирующих работу по обеспечению информационной безопасности в организации					
	умеет формулировать основные требования при лицензировании деятельности в области защиты информации, сертификации и аттестации по требованиям безопасности информации	Тест	Выполнение теста на 90-100%	Выполнение теста на 80-90%	Выполнение теста на 70-80%	В тесте менее 70% правильных ответов
	умеет формулировать основные требования информационной безопасности при эксплуатации автоматизированной системы	Тест	Выполнение теста на 90-100%	Выполнение теста на 80-90%	Выполнение теста на 70-80%	В тесте менее 70% правильных ответов
	умеет формулировать основные требования по защите конфиденциальной информации, персональных данных и охране результатов интеллектуальной деятельности в организации	Тест	Выполнение теста на 90-100%	Выполнение теста на 80-90%	Выполнение теста на 70-80%	В тесте менее 70% правильных ответов
	умеет формировать политики информационной безопасности организации	Тест	Выполнение теста на 90-100%	Выполнение теста на 80-90%	Выполнение теста на 70-80%	В тесте менее 70% правильных ответов
	умеет выполнять полный объем работ, связанных с реализацией частных политик информационной безопасности автоматизированной системы	Тест	Выполнение теста на 90-100%	Выполнение теста на 80-90%	Выполнение теста на 70-80%	В тесте менее 70% правильных ответов
	умеет использовать программные средства для построения графических схем и алгоритмов в соответствии с требованиями ЕСПД и ЕСКД	Тест	Выполнение теста на 90-100%	Выполнение теста на 80-90%	Выполнение теста на 70-80%	В тесте менее 70% правильных ответов

7.2 Примерный перечень оценочных средств (типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности)

7.2.1 Примерный перечень вопросов для подготовки к зачету

(если предусмотрен учебным планом)

Содержание и задачи дисциплины. Основные понятия в области организационно-правового обеспечения информационной безопасности

Основы теории государства и права как фундаментальной дисциплины для изучения организационно-правового обеспечения информационной безопасности

Система законодательного регулирования общественных отношений в области обеспечения информационной безопасности

Конституционные основы обеспечения информационной безопасности в РФ

Регламентация вопросов обеспечения информационной безопасности в Гражданском кодексе РФ

Регламентация вопросов обеспечения информационной безопасности в Уголовном кодексе РФ

Закон РФ «О государственной тайне»

Федеральные законы «Об информации, информатизации и защите информации» и «Об участии в международном информационном обмене»

Законы РФ «Об авторском праве и смежных правах», «О правовой охране программ для электронно-вычислительных машин и баз данных»

Регламентация вопросов ЗИ в Федеральных законах общего характера

Международное законодательство в области обеспечения информационной безопасности и защиты информации

Основы организации обеспечения информационной безопасности и ЗИ

Система документов в области обеспечения информационной безопасности и защиты информации

Определение целей и задач обеспечения информационной безопасности и защиты информации

Лицензирование деятельности в области ЗИ

Сертификация средств ЗИ.

Аттестование объектов по выполнению требований обеспечения защиты информации

Подготовка (переподготовка) и повышение квалификации специалистов в области ЗИ

Организация контроля состояния ЗИ

Организация ЗИ на объектах органов государственной власти и управления

7.2.2 Примерный перечень заданий для решения стандартных задач

ОПК-5. Способен применять нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации

1. Информационное общество: понятие, структура, признаки.
2. Понятие информационной сферы общества.
3. Информация и ее виды.

4. Ответственность за правонарушения в информационной сфере.

5. Понятие коммерческой тайны. Информация, составляющая коммерческую тайну (секреты производства).

6. Отнесение информации к информации, составляющей коммерческую тайну (секрет производства).

7. Понятие и виды персональных данных.

8. Принципы обработки персональных данных.

9. Порядок и условия обработки персональных данных.

10. Права и обязанности субъекта персональных данных.

11. Понятие и виды электронной подписи.

12. Правовой статус удостоверяющего центра.

13. Полномочия федеральных органов исполнительной власти в сфере использования электронной подписи.

14. Правовое регулирование отношений в сфере библиотечного дела.

15. Правовое регулирование отношений в области формирования обязательного экземпляра документов.

16. Правовое регулирование общественных отношений в сфере формирования, хранения, учета и использования архивов и архивных фондов.

17. Понятие связи, ее структура, принципы функционирования.

18. Общая характеристика отношений в сфере связи и массовых коммуникаций.

19. Государственной регулирование деятельности в области связи.

20. Право и Интернет как социальные явления.

21. Правовое регулирование деятельности в киберпространстве.

22. Сущность конституционного права на информацию и его гарантии.

23. Правовые режимы информации.

24. Понятие информационной безопасности.

25. Понятие правонарушений в информационной сфере.

26. Понятие государственной тайны. Сведения, составляющие государственную тайну.

27. Отнесение сведений к государственной тайне, их засекречивание и рассекречивание.

28. Порядок распоряжения сведениями, составляющими государственную тайну.

29. Защита сведений, составляющих государственную тайну.

30. Содержание и реализация исключительного права на секрет производства.

31. Права и обязанности оператора при обработке персональных данных.

32. Особенности регулирования интернет-отношений.

33.Понятие и виды информационных правоотношений.

34. Субъекты, объекты, содержание информационных правоотношений.

35. Законодательство Российской Федерации в области информационной безопасности.

36. Особенности обеспечения информационной безопасности в различных сферах общественной жизни.

37. Юридическая ответственность за нарушение режима государственной тайны.

38. Ответственность за нарушение положений законодательства о персональных данных.

39. Понятие электронного документа и электронного документооборота.

40. Правовое регулирование и юридические риски электронного документооборота.

41. Общая характеристика законодательства в сфере электронного документооборота.

42. Ответственность за нарушение исключительного права на секрет производства.

43. Контроль и надзор за обработкой персональных данных.

44. Киберпреступления: понятие, основные черты, формы проявления.

45. Понятие и распространение массовой информации.

46. Понятие и правовой статус средства массовой информации.

47. Правовые формы организации деятельности средств массовой информации.

48. Общие принципы работы средств массовой информации.

49. Правовые формы организации деятельности средств массовой информации.

50. Специальная редакционная ответственность средств массовой информации.

7.2.3 Примерный перечень заданий для решения прикладных задач

ОПК-5. Способен применять нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации

1. Кто является основным ответственным за определение уровня классификации информации?

Варианты ответа:

Руководитель среднего звена

Высшее руководство

Владелец

Пользователь

2. Какая категория является наиболее рискованной для компании с точки зрения вероятного мошенничества и нарушения безопасности?

Варианты ответа:

Сотрудники

Хакеры

Атакующие

Контрагенты (лица, работающие по договору)

3. Если различным группам пользователей с различным уровнем доступа требуется доступ к одной и той же информации, какое из указанных ниже действий следует предпринять руководству?

Варианты ответа:

Снизить уровень безопасности этой информации для обеспечения ее доступности и удобства использования

Требовать подписания специального разрешения каждый раз, когда человеку требуется доступ к этой информации

Улучшить контроль за безопасностью этой информации

Снизить уровень классификации этой информации

4. Что самое главное должно продумать руководство при классификации данных?

Варианты ответа:

Типы сотрудников, контрагентов и клиентов, которые будут иметь доступ к данным

Необходимый уровень доступности, целостности и конфиденциальности

Оценить уровень риска и отменить контрмеры

Управление доступом, которое должно защищать данные

5. Кто в конечном счете несет ответственность за гарантии того, что данные классифицированы и защищены?

Варианты ответа:

Владельцы данных

Пользователи

Администраторы

Руководство

6. Когда целесообразно не предпринимать никаких действий в отношении выявленных рисков?

Варианты ответа:

Никогда. Для обеспечения хорошей безопасности нужно учитывать и снижать все риски

Когда риски не могут быть приняты во внимание по политическим соображениям

Когда необходимые защитные меры слишком сложны

Когда стоимость контрмер превышает ценность актива и потенциальные потери

7. Что такое политики безопасности?

Варианты ответа:

Пошаговые инструкции по выполнению задач безопасности

Общие руководящие требования по достижению определенного уровня безопасности

Широкие, высокоуровневые заявления руководства

Детализированные документы по обработке инцидентов безопасности

7.2.4 Примерный перечень вопросов для подготовки к зачету

Основные понятия в области организационно-правового обеспечения информационной безопасности. Законодательство РФ в области информационной безопасности, защиты государственной тайны и конфиденциальной информации. Защита информации. Процесс ЗИ,

обеспечение и обслуживание процесса ЗИ, управление процессом ЗИ, координация деятельности в области ЗИ. Системы защиты информации. Государственная система ЗИ (ГСЗИ). Целевые (объектные) и функциональные подсистемы ЗИ. Системы систем подготовки кадров в области ЗИ, систем лицензирования, сертификации, аттестования, проведения НИОКР, оказания услуг в области ЗИ. Система документов в области ЗИ. Основы теории государства и права как фундаментальной дисциплины для изучения организационно-правового обеспечения информационной безопасности Место теории государства и права в системе юридических наук. Основные понятия теории государства и права. Правовые отношения. Виды правовых отношений в сфере ЗИ. Правовые нормы. Методы правового регулирования общественных отношений. Право, ограничение права, обязанность, ответственность в сфере информационных отношений. Классификация отраслей права. Система законодательного регулирования общественных отношений в области обеспечения информационной безопасности. Концепция построения системы законодательного регулирования общественных отношений в области обеспечения информационной безопасности. Роль и место Конституции РФ, конституционных законов, Гражданского Уголовного кодексов, Кодекса об административных правонарушениях, Кодекса законов о труде, других общих и специальных законов в области ЗИ, защиты интеллектуальной собственности в регулировании общественных отношений в процессе создания, распространения и использования информации, информатизации и защиты информации.

Конституционные основы обеспечения информационной безопасности в РФ. Основы конституционного строя. Права и свободы человека и гражданина как важнейшего субъекта ЗИ. Федеративное устройство России и его влияние на организацию ЗИ. Функции Президента РФ, Федерального Собрания, Правительства РФ, федеральных органов исполнительной власти, органов судебной власти, органов государственной власти субъектов РФ, органов местного самоуправления в решении вопросов обеспечения информационной безопасности. Регламентация вопросов обеспечения информационной безопасности в Гражданском кодексе РФ Информация как объект гражданских прав. Виды информации, подлежащие защите в процессе обычного гражданского оборота. Регламентация вопросов защиты служебной, коммерческой и банковской тайны, интеллектуальной собственности. Использование электронно-цифровой подписи при совершении сделок.

Регламентация вопросов обеспечения информационной безопасности в Уголовном кодексе РФ виды ответственности за преступления в информационной сфере. Ответственность в сфере компьютерной информации: за неправомерный доступ к компьютерной информации, за создание, использование и распространение вредоносных программ для ЭВМ, а также за нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети.

Закон РФ «О государственной тайне» Система защиты государственной тайны. Перечень сведений, составляющих государственную тайну. Отнесение сведений к государственной тайне и их засекречивание. Рассекречивание

сведений и их носителей. Распоряжение сведениями, составляющими государственную тайну. Правовой режим защиты государственной тайны. Финансирование мероприятий по защите государственной тайны. Федеральные законы «Об информации, информатизации и защите информации» и «Об участии в международном информационном обмене». Информационные ресурсы как объект защиты. Классификация информационных ресурсов. Государственные и негосударственные информационные ресурсы. Персональные данные. Пользование информационными ресурсами. Информатизация, информационные системы и средства их обеспечения. Защита информации и прав субъектов информационных отношений. Системы защиты информационных ресурсов. Законы РФ «Об авторском праве и смежных правах», «О правовой охране программ для электронно-вычислительных машин и баз данных». Предмет регулирования авторского права. Сфера действия авторского права. Объект авторского права. Смежные права. Сфера действия смежных прав. Субъекты смежных прав. Нарушение авторских и смежных прав. Защита авторских и смежных прав.

Регламентация вопросов ЗИ в Федеральных законах общего характера Основные нормы и требования по ЗИ, содержащиеся в законах: «О безопасности», «Об обороне», «Об органах федеральной службы безопасности в Российской Федерации», «О федеральных органах правительственной связи и информации», «О внешней разведке», «О милиции»», «О конверсии оборонной промышленности в Российской Федерации», «О закрытом административно-территориальном образовании», «О связи», «О рекламе», «О недрах» и др.

Международное законодательство в области обеспечения информационной безопасности и защиты информации. Принципы правового регулирования вопросов обеспечения информационной безопасности и ЗИ в США, Франции, Великобритании, ФРГ и других государствах. Краткая характеристика основных законодательно-правовых документов в области ЗИ, действующих в указанных государствах.

Основы организации обеспечения информационной безопасности и ЗИ. Основные положения концепции обеспечения информационной безопасности РФ. Основные положения концепции ЗИ в РФ. Распределение полномочий по обеспечению информационной безопасности в РФ. Научно-технические проблемы, требующие скоординированных действий различных органов государственной власти. Система документов в области обеспечения информационной безопасности и защиты информации. Обоснование необходимой и достаточной системы документов в области ЗИ. Общегосударственные документы. Организационно-распорядительные документы. Специальные нормативные документы Гостехкомиссии России по вопросам защиты информации от технических разведок, несанкционированного доступа и несанкционированных воздействий на информацию. Нормативные документы государственной системы стандартизации. Плановые документы. Информационные документы.

Определение целей и задач обеспечения информационной безопасности и защиты информации

Классификация объектов обеспечения информационной безопасности и защиты информации. Структуризация понятия «объект защиты». Составные части объекта защиты. Виды защищаемой информации, носителей информации и информационных процессов. Характеристика промышленных предприятий, учреждений, информационно-телекоммуникационных систем как объектов защиты. Лицензирование деятельности в области ЗИ. Правовые основы лицензирование деятельности в области ЗИ. Структура системы лицензирования, функции ее органов. Порядок проведения лицензирования. Распределений полномочий по лицензированию деятельности в области ЗИ между федеральными органами государственной власти. Сертификация средств ЗИ

Правовые основы сертификации ЗИ. Структура системы сертификации, функции ее органов. Порядок сертификации ЗИ. Распределений полномочий по сертификации средств ЗИ между федеральными органами государственной власти. Аттестование объектов по выполнению требований обеспечения защиты информации. Правовые основы аттестования объектов по выполнению требований обеспечения защиты информации. Структура системы аттестования, функции ее органов. Порядок аттестования объектов органов управления, промышленных объектов, систем информатизации и связи. Распределений полномочий по аттестованию между федеральными органами государственной власти. Подготовка (переподготовка) и повышение квалификации специалистов в области ЗИ

Правовые основы подготовки специалистов в области ЗИ. Система учебных заведений. Перечень специальностей. Основные нормативные документы по подготовке специалистов в области ЗИ. Организация контроля состояния ЗИ. Правовые основы контроля состояния ЗИ. Основные организационно-распорядительные и нормативные документы по контролю состояния ЗИ. Цели и задачи контроля. Формы контроля: межведомственный контроль; ведомственный контроль; контроль, осуществляемый собственником информации. Органы контроля. Контроль организации и эффективности ЗИ. Методы контроля: информационно-логический; расчетный; инструментальный; инструментально-расчетный; программный. Нарушения установленных требований и норм ЗИ. Организация ЗИ на объектах органов государственной власти и управления. Требования к содержанию Руководств по ЗИ на объекте. Цели и задачи ЗИ. Определение защищаемых информационных ресурсов. Оценка возможностей технических разведок и других источников угроз безопасности информации. Разработка организационных и технических мероприятий по ЗИ. Аттестование объектов.

7.2.5 Примерный перечень заданий для решения прикладных задач

Не предусмотрено учебным планом

7.2.6 Методика выставления оценки при проведении промежуточной аттестации

(Например: Зачет проводится по тест-билетам, каждый из которых содержит 10 вопросов и задачу. Каждый правильный ответ на вопрос в тесте оценивается 1 баллом, задача оценивается в 10 баллов (5 баллов верное решение и 5 баллов за верный ответ). Максимальное количество набранных баллов – 20.

1. Оценка «Неудовлетворительно» ставится в случае, если студент набрал менее 6 баллов.

2. Оценка «Удовлетворительно» ставится в случае, если студент набрал от 6 до 10 баллов

3. Оценка «Хорошо» ставится в случае, если студент набрал от 11 до 15 баллов.

4. Оценка «Отлично» ставится, если студент набрал от 16 до 20 баллов.)

7.2.7 Паспорт оценочных материалов

№ п/п	Контролируемые разделы (темы) дисциплины	Код контролируемой компетенции (или ее части)	Наименование оценочного средства
1	Введение	ОПК-5	Тест
2	Правовое обеспечение	ОПК-5	Тест
3	Организационное обеспечение	ОПК-5	Тест

7.3. Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности

Тестирование осуществляется, либо при помощи компьютерной системы тестирования, либо с использованием выданных тест-заданий на бумажном носителе. Время тестирования 30 мин. Затем осуществляется проверка теста экзаменатором и выставляется оценка согласно методики выставления оценки при проведении промежуточной аттестации.

Решение стандартных задач осуществляется, либо при помощи компьютерной системы тестирования, либо с использованием выданных задач на бумажном носителе. Время решения задач 30 мин. Затем осуществляется проверка решения задач экзаменатором и выставляется оценка, согласно методики выставления оценки при проведении промежуточной аттестации.

8 УЧЕБНО МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Основная

1. Жигулин Г.П. Организационное и правовое обеспечение информационной безопасности [Электронный ресурс]: учебное пособие/ Жигулин Г.П.— Электрон. текстовые данные.— Санкт-Петербург: Университет ИТМО, 2014.— 174 с.— Режим доступа: http://www.iprbookshop.ru/67451.html.

2.Ажмухамедов И.М. Основы организационно-правового обеспечения информационной безопасности [Электронный ресурс]: учебное пособие/ Ажмухамедов И.М., Князева О.М.— Электрон. текстовые данные.— Санкт-Петербург: Интермедия, 2017.— 264 с.— Режим доступа: http://www.iprbookshop.ru/73643.html.

Дополнительная

1.Пахомова, А.С. Организационное и правовое обеспечение информационной безопасности [Электронный ресурс]: Учеб. пособие. - Электрон. текстовые, граф. дан. (390 Кб). - Воронеж: ФГБОУ ВПО "Воронежский государственный технический университет».

8.2 Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине, включая перечень лицензионного программного обеспечения, ресурсов информационно-телекоммуникационной сети «Интернет», современных профессиональных баз данных и информационных справочных систем:

Официальный сайт ФСТЭК России [Электронный ресурс] / ФАУ «ГНИИИ ПТЗИ ФСТЭК России». – Режим доступа: http://fstec.ru/, свободный.

Банк данных угроз безопасности информации [Электронный ресурс] / ФАУ «ГНИИИ ПТЗИ ФСТЭК России». – Режим доступа: http://bdu.fstec.ru/, свободный.

Каталог национальных стандартов [Электронный ресурс] / Федеральное агентство по техническому регулированию и метрологии. – Режим доступа: http://www.gost.ru/, свободный.

9 МАТЕРИАЛЬНО-ТЕХНИЧЕСКАЯ БАЗА, НЕОБХОДИМАЯ ДЛЯ ОСУЩЕСТВЛЕНИЯ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА

Специализированная лекционная аудитория, оснащенная оборудованием для лекционных демонстраций и проекционной аппаратурой.

10 МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ (МОДУЛЯ)

По дисциплине «Организационное и правовое обеспечение информационной безопасности» читаются лекции, проводятся практические занятия.

Основой изучения дисциплины являются лекции, на которых излагаются наиболее существенные и трудные вопросы, а также вопросы, не нашедшие отражения в учебной литературе.

Большое значение по закреплению и совершенствованию знаний имеет самостоятельная работа студентов. Информацию о всех видах самостоятельной работы студенты получают на занятиях.

Практические занятия направлены на приобретение практических навыков.

Вид учебных занятий	Деятельность студента
Лекция	Написание конспекта лекций: кратко, схематично, последовательно фиксировать основные положения, выводы, формулировки, обобщения; помечать важные мысли, выделять ключевые слова, термины. Проверка терминов, понятий с помощью энциклопедий, словарей, справочников с выписыванием толкований в тетрадь. Обозначение вопросов, терминов, материала, которые вызывают трудности, поиск ответов в рекомендуемой литературе. Если самостоятельно не удается разобраться в материале, необходимо сформулировать вопрос и задать преподавателю на лекции или на практическом занятии.
Практическое занятие	Конспектирование рекомендуемых источников. Работа с конспектом лекций, подготовка ответов к контрольным вопросам, просмотр рекомендуемой литературы. Прослушивание аудио- и видеозаписей по заданной теме, выполнение расчетно-графических заданий, решение задач по алгоритму.
Самостоятельная работа	Самостоятельная работа студентов способствует глубокому усвоения учебного материала и развитию навыков самообразования. Самостоятельная работа предполагает следующие составляющие: - работа с текстами: учебниками, справочниками, дополнительной литературой, а также проработка конспектов лекций; - работа над темами для самостоятельного изучения; - участие в работе студенческих научных конференций, олимпиад.
Подготовка к дифференцированному зачету	При подготовке к зачету необходимо ориентироваться на конспекты лекций, рекомендуемую литературу и решение задач на практических занятиях.