

федеральное государственное бюджетное образовательное учреждение
высшего образования
РОССИЙСКИЙ ГОСУДАРСТВЕННЫЙ ГИДРОМЕТЕОРОЛОГИЧЕСКИЙ
УНИВЕРСИТЕТ

Кафедра Информационных технологий и систем безопасности

Рабочая программа по дисциплине

**ОРГАНИЗАЦИОННОЕ И ПРАВОВОЕ ОБЕСПЕЧЕНИЕ
ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ**

Основная профессиональная образовательная программа
высшего образования программы специалитета по специальности

10.05.02 «Информационная безопасность телекоммуникационных систем»

Специализация:

Разработка защищенных телекоммуникационных систем

Квалификация:

Специалист

Форма обучения

Очная

Согласовано
Руководитель ОПОП
«Информационная безопасность
телекоммуникационных систем»


Бурлов В.Г.

Утверждаю
Председатель УМС  И.И. Палкин

Рекомендована решением

Учебно-методического совета

 2018 г., протокол № 4

Рассмотрена и утверждена на заседании кафедры

 2018 г., протокол № 5

Зав. кафедрой  Бурлов В.Г.

Авторы-разработчики:

 Богданов П.Ю.

1. Цели освоения дисциплины

Целью освоения дисциплины «Организационно-правовое обеспечение информационной безопасности» является изучение основ правового регулирования в информационной сфере, конституционных гарантий прав граждан на получение информации и механизм их реализации, видов защищаемой информации по законодательству Российской Федерации, системы защиты государственной тайны, основы правового регулирования отношений в области интеллектуальной собственности и способов защиты этой собственности.

2. Место дисциплины в структуре ОПОП

«Организационное и правовое обеспечение информационной безопасности» входит в базовую часть Блока 1 Дисциплины (Модули).

Для успешного усвоения данной дисциплины необходимо, чтобы обучаемые владели знаниями, умениями и навыками, сформированными в процессе изучения следующих дисциплин:

«Основы информационной безопасности»;

«Технические средства и методы защиты информации»

«Правоведение»

«Информационные технологии»

3. Компетенции обучающегося, формируемые в результате освоения дисциплины

Процесс изучения дисциплины направлен на формирование следующих компетенций:

Код компетенции	Компетенция
ОПК-7	способностью применять нормативные правовые акты в своей профессиональной деятельности
ПК-1	способностью осуществлять анализ научно-технической информации, нормативных и методических материалов по методам обеспечения информационной безопасности телекоммуникационных систем
ПК-5	способностью проектировать защищённые телекоммуникационные системы и их элементы, проводить анализ проектных решений по обеспечению заданного уровня безопасности и требуемого качества обслуживания, разрабатывать необходимую техническую документацию с учетом действующих нормативных и методических документов
ПК-6	способностью применять технологии обеспечения информационной безопасности телекоммуникационных систем и нормы их интеграции в государственную и международную информационную среду
ПК-9	способностью участвовать в проведении аттестации телекоммуникационных систем по требованиям защиты информации

ПК-10	способностью оценивать выполнение требований нормативных правовых актов и нормативных методических документов в области информационной безопасности при проверке защищенных телекоммуникационных систем, выполнять подготовку соответствующих заключений
ПК-13	способностью организовывать выполнение требований режима защиты информации ограниченного доступа, разрабатывать проекты документов, регламентирующих работу по обеспечению информационной безопасности телекоммуникационных систем

В результате освоения компетенций в рамках дисциплины

«Организационное и правовое обеспечение информационной безопасности» обучающийся должен:

Код компетенции	Результаты обучения
ОПК-7	<p>Знать: необходимые для профессиональной деятельности нормативно-правовые документы</p> <p>Уметь: применять нормативно-правовые акты в профессиональной деятельности</p> <p>Владеть: навыками работы с нормативными правовыми актами</p>
ПК-1	<p>Знать: основные нормативные правовые акты в области информационной безопасности и защиты информации; основные технические стандарты и спецификации; состояние правового обеспечения информационной безопасности в РФ; сущность информационных процессов в системах связи и управления.</p> <p>Уметь: осуществлять анализ научно-технической информации, нормативных и методических материалов; пользоваться нормативными документами; ориентироваться в правовом обеспечении информационной безопасности в РФ в области информационной инфраструктуры;</p> <p>Владеть: навыками работы с нормативными правовыми актами; навыками анализа функционирования телекоммуникационных систем; навыками сравнения научно-технической информации, нормативных и методических материалов;</p>
ПК-5	<p>Знать: методы проектирования защищенных телекоммуникационных систем и их элементов; действующую нормативную и правовую документацию; состав рабочего проекта ЗТКС,</p> <p>Уметь: проводить анализ проектных решений по обеспечению заданного уровня безопасности; разрабатывать необходимую техническую документацию</p> <p>Владеть: способностью проводить анализ проектных решений по обеспечению заданного уровня безопасности, разрабатывать необходимую техническую документацию с учетом действующих нормативных и правовых документов; навыками выработки требований к системам защиты ТКС;</p>

ПК-6	<p>Знать: о технологии обеспечения информационной безопасности телекоммуникационных систем и нормы их интеграции в государственную и международную информационную среду; принципы и методы организационной защиты информации; основные стандарты защиты информации в ведущих зарубежных странах;</p> <p>Уметь: применять технологии обеспечения информационной безопасности телекоммуникационных систем и нормы их интеграции в государственную и международную информационную среду; анализировать и оценивать угрозы информационной безопасности телекоммуникационных систем; пользоваться нормативными документами по защите информации; применять отечественные и зарубежные нормы и стандарты обеспечения информационной безопасности телекоммуникационных систем;</p> <p>Владеть: способностью применять технологии обеспечения информационной безопасности телекоммуникационных систем и нормы их интеграции в государственную и международную информационную среду; навыками поиска актуальной нормативной и правовой зарубежной информации, необходимой для профессиональной деятельности</p>
ПК-9	<p>Знать: основы документационного обеспечения работ по аттестации телекоммуникационных систем, нормативные документы по защите информации; методы аттестации телекоммуникационных систем и нормативные требования по защите информации</p> <p>Уметь: использовать нормативные правовые документы в своей профессиональной деятельности; производить работы по аттестации телекоммуникационных систем по защите информации</p> <p>Владеть: навыками разработки организационно-распорядительных документов, формирования актов по результатам аттестации ТКС, нормативными требованиями по защите информации</p>
ПК-10	<p>Знать: основные международные и отечественные технические стандарты, а также нормативно-правовые документы, связанные с обеспечением информационной безопасности</p> <p>Уметь: использовать нормативно-правовые документы и отечественные стандарты, связанные с обеспечением информационной безопасности на объектах защиты; производить работы по аттестации телекоммуникационных систем по защите информации</p> <p>Владеть: нормативными требованиями по защите информации; навыками работы с нормативно-правовыми документами, международными и отечественными стандартами, связанными с обеспечением информационной безопасности</p>
ПК-13	<p>Знать: основные нормативные правовые акты в области информационной безопасности и защиты информации; принципы управления системами обеспечения информационной безопасности предприятий</p> <p>Уметь: осуществлять меры противодействия нарушениям информационной безопасности; разрабатывать проекты документов, регламентирующих работу по обеспечению информационной безопасности</p> <p>Владеть: навыками доступа к документации, определяющей правила эксплуатации систем управления информационной безопасности</p>

Основные признаки проявленности формируемых компетенций в результате освоения дисциплины ««Организационно-правовое обеспечение информационной безопасности»» сведены в таблице.

Соответствие уровней освоения компетенции планируемым результатам обучения и критериям их оценивания

Уровень освоения компетенции	Результат обучения	Результат обучения	Результат обучения
	ОПК-7	ПК-1	ПК-5
минимальный	основы Российской правовой системы и законодательства, правового статуса личности, организации и деятельности органов государственной власти в Российской Федерации; основы организационного и правового обеспечения информационной безопасности.	основы российской правовой системы и законодательства; правовые основы обеспечения национальной безопасности Российской Федерации	действующую нормативную и правовую документацию
	использовать в практической деятельности правовые знания; анализировать и составлять правовые акты и осуществлять правовую оценку информации; предпринимать необходимые меры по восстановлению нарушенных прав	осуществлять анализ научно-технической информации, нормативных и методических материалов;	Разрабатывать проектные решения по обеспечению заданного уровня безопасности;
	навыками поиска нормативной правовой информации, необходимой для профессиональной деятельности; навыками работы с нормативными правовыми актами;	навыками работы с нормативными правовыми актами;	способностью проводить анализ проектных решений по обеспечению заданного уровня безопасности
базовый	основы Российской правовой системы и законодательства, правового статуса личности, организации и деятельности органов государственной власти в Российской Федерации; основы организационного и правового обеспечения информационной безопасности; нормативные методические документы ФСБ России и ФСТЭК России в области защиты информации.	основы российской правовой системы и законодательства; правовые основы обеспечения национальной безопасности Российской Федерации; состояние правового обеспечения информационной безопасности в РФ	действующую нормативную и правовую документацию; методы проектирования защищенных телекоммуникационных систем и их элементов
	использовать в практической деятельности правовые знания; анализировать и составлять правовые акты и осуществлять правовую оценку информации; предпринимать необходимые меры по восстановлению нарушенных прав; применять нормативные правовые акты и нормативные	осуществлять анализ научно-технической информации, нормативных и методических материалов; пользоваться нормативными документами	Разрабатывать проектные решения по обеспечению заданного уровня безопасности; проводить анализ проектных решений по обеспечению заданного уровня безопасности;

	методические документы в области информационной безопасности.		
	навыками поиска нормативной правовой информации, необходимой для профессиональной деятельности; навыками работы с нормативными правовыми актами; методами организации и управления деятельностью служб защиты информации на предприятии.	навыками работы с нормативными правовыми актами; навыками анализа функционирования телекоммуникационных систем;	способностью проводить анализ проектных решений по обеспечению заданного уровня безопасности; навыками выработки требований к системам защиты ТКС
продвинутый	основы Российской правовой системы и законодательства, правового статуса личности, организации и деятельности органов государственной власти в Российской Федерации; основы организационного и правового обеспечения информационной безопасности; нормативные методические документы ФСБ России и ФСТЭК России в области защиты информации; организацию работы и нормативные правовые акты и стандарты по лицензированию деятельности в области защиты информации.	основы российской правовой системы и законодательства; правовые основы обеспечения национальной безопасности Российской Федерации; состояние правового обеспечения информационной безопасности в РФ сущность информационных процессов в системах связи и управления.	методы проектирования защищенных телекоммуникационных систем и их элементов; действующую нормативную и правовую документацию; состав рабочего проекта ЗТКС,
	использовать в практической деятельности правовые знания; анализировать и составлять правовые акты и осуществлять правовую оценку информации; предпринимать необходимые меры по восстановлению нарушенных прав; применять нормативные правовые акты и нормативные методические документы в области информационной безопасности; разрабатывать проекты нормативных и организационно-распорядительных документов, регламентирующих работу по защите информации.	осуществлять анализ научно-технической информации, нормативных и методических материалов; пользоваться нормативными документами; ориентироваться в правовом обеспечении информационной безопасности в РФ в области информационной инфраструктуры;	Разрабатывать проектные решения по обеспечению заданного уровня безопасности; проводить анализ проектных решений по обеспечению заданного уровня безопасности; разрабатывать необходимую техническую документацию
	навыками поиска нормативной правовой информации, необходимой для профессиональной деятельности; навыками работы с нормативными правовыми актами; методами организации и управления деятельностью служб защиты	навыками работы с нормативными правовыми актами; навыками анализа функционирования телекоммуникационных систем; навыками сравнения научно-	способностью проводить анализ проектных решений по обеспечению заданного уровня безопасности; навыками выработки требований к системам защиты

	информации на предприятии; методами формирования требований по защите информации	технической информации, нормативных и методических материалов;	ТКС; умением разрабатывать необходимую техническую документацию с учетом действующих нормативных и правовых документов;
--	--	--	---

Уровень освоения компетенции	Результат обучения	Результат обучения	Результат обучения
	ПК-6	ПК-9	ПК-10
минимальный	о технологии обеспечения информационной безопасности телекоммуникационных систем и нормы их интеграции в государственную и международную информационную среду	цели, задачи, принципы и основные направления обеспечения информационной безопасности государства; основные термины по проблематике информационной безопасности;	основные отечественные технические стандарты, связанные с обеспечением информационной безопасности
	применять технологии обеспечения информационной безопасности телекоммуникационных систем и нормы их интеграции в государственную и международную информационную среду;	пользоваться современной научно-технической информацией по исследуемым проблемам и задачам;	искать нормативно-правовые документы и отечественные стандарты, связанные с обеспечением информационной безопасности на объектах защиты;
	навыками поиска актуальной нормативной и правовой зарубежной информации, необходимой для профессиональной деятельности	навыками формальной постановки и решения задачи обеспечения информационной безопасности информации.	нормативными требованиями по защите информации;
базовый	о технологии обеспечения информационной безопасности телекоммуникационных систем и нормы их интеграции в государственную и международную информационную среду; принципы и методы организационной защиты информации;	цели, задачи, принципы и основные направления обеспечения информационной безопасности государства; основные термины по проблематике информационной безопасности; роль и место информационной безопасности в системе национальной безопасности.	основные международные и отечественные технические стандарты, связанные с обеспечением информационной безопасности
	применять технологии обеспечения информационной безопасности телекоммуникационных систем и нормы их	пользоваться современной научно-технической информацией по исследуемым проблемам и задачам;	использовать нормативно-правовые документы и отечественные стандарты, связанные с обеспечением

	интеграции в государственную и международную информационную среду; анализировать и оценивать угрозы информационной безопасности телекоммуникационных систем;	определять комплекс мер для обеспечения информационной безопасности;	информационной безопасности на объектах защиты;
	навыками поиска актуальной нормативной и правовой зарубежной информации, необходимой для профессиональной деятельности; способностью применять технологии обеспечения информационной безопасности телекоммуникационных систем;	навыками формальной постановки и решения задачи обеспечения информационной безопасности; навыками анализа информационной инфраструктуры информационной системы и ее безопасности.	нормативными требованиями по защите информации; навыками работы с нормативно-правовыми документами связанными с обеспечением информационной безопасности
продвинутый	о технологии обеспечения информационной безопасности телекоммуникационных систем и нормы их интеграции в государственную и международную информационную среду; принципы и методы организационной защиты информации; основные стандарты защиты информации в ведущих зарубежных странах;	цели, задачи, принципы и основные направления обеспечения информационной безопасности государства; основные термины по проблематике информационной безопасности; методологию создания систем защиты информации; роль и место информационной безопасности в системе национальной безопасности	основные международные и отечественные технические стандарты, а также нормативно-правовые документы, связанные с обеспечением информационной безопасности
	применять технологии обеспечения информационной безопасности телекоммуникационных систем и нормы их интеграции в государственную и международную информационную среду; анализировать и оценивать угрозы информационной безопасности телекоммуникационных систем; пользоваться нормативными документами по защите информации; применять отечественные и зарубежные нормы и стандарты обеспечения информационной безопасности	пользоваться современной научно-технической информацией по исследуемым проблемам и задачам; определять комплекс мер для обеспечения информационной безопасности; организовать проведение и сопровождение аттестации объекта на соответствие требованиям государственных предприятий и корпоративных в том числе.	использовать нормативно-правовые документы и отечественные стандарты, связанные с обеспечением информационной безопасности на объектах защиты; производить работы по аттестации телекоммуникационных систем по защите информации

	телекоммуникационных систем;		
	способностью применять технологии обеспечения информационной безопасности телекоммуникационных систем и нормы их интеграции в государственную и международную информационную среду; навыками поиска актуальной нормативной и правовой зарубежной информации, необходимой для профессиональной деятельности	навыками формальной постановки и решения задачи обеспечения информационной безопасности информации; навыками анализа информационной инфраструктуры информационной системы и ее безопасности; навыками участия в экспертизе состояния защищенности информации на объекте защиты.	нормативными требованиями по защите информации; навыками работы с нормативно-правовыми документами, международными и отечественными стандартами, связанными с обеспечением информационной безопасности

Уровень освоения компетенции	Результат обучения		
	ОПК-13		
минимальный	правила эксплуатации систем управления информационной безопасности		
	осуществлять меры противодействия нарушениям информационной безопасности		
	навыками доступа к документации, определяющей правила эксплуатации систем управления информационной безопасности		
базовый	правила эксплуатации систем управления информационной безопасности основные нормативные правовые акты в области информационной безопасности и защиты информации		
	осуществлять меры противодействия нарушениям информационной безопасности; разрабатывать проекты документов, регламентирующих работу по обеспечению информационной безопасности		
	навыками доступа к документации, определяющей правила эксплуатации систем управления информационной безопасности; способностью организовывать выполнение требований режима защиты информации ограниченного доступа		
продвинутый	основные нормативные правовые акты в области информационной безопасности и защиты информации; принципы управления системами обеспечения информационной безопасности предприятий		
	осуществлять меры противодействия нарушениям информационной безопасности; разрабатывать проекты документов, регламентирующих работу по обеспечению информационной безопасности		
	навыками доступа к документации, определяющей правила эксплуатации систем управления информационной безопасности; способностью организовывать выполнение требований режима защиты информации ограниченного доступа; навыками разработки регламентов по обеспечению информационной безопасности		

4. Структура и содержание дисциплины

Общая трудоемкость дисциплины составляет 4 зачетные единицы, 144 часа.

*Объем дисциплины (модуля) по видам учебных занятий
в академических часах)*

Объем дисциплины	Всего часов
	Очная форма обучения
Общая трудоемкость дисциплины	144
Контактная работа обучающихся с преподавателям (по видам аудиторных учебных занятий) – всего:	72
в том числе:	
лекции	36
Практические занятия	36
семинарские занятия	
Самостоятельная работа (СРС) – всего:	72
в том числе:	
курсовая работа	
контрольная работа	
Вид промежуточной аттестации (зачет/экзамен)	экзамен

4.1. Структура дисциплины

Очная форма обучения

№ п/п	Раздел и тема дисциплины	Семестр	Виды учебной работы, в т.ч. самостоятельная работа студентов, час.			Формы текущего контроля успеваемости	Занятия в активной и интерактивной форме, час.	Формируемые компетенции
			Лекции	Семинар Практич.	Самост. работа			
1	Раздел 1. Правовое обеспечение информационной безопасности							

1.1	Информационные отношения как объект правового регулирования	9	2	2	8	Опрос, практические занятия	3	ОПК7, ПК1, ПК5, ПК6, ПК9, ПК10, ПК13
1.2	Правовой режим защиты государственной тайны	9	4	4	8	Опрос, практические занятия	3	ОПК7, ПК1, ПК5, ПК6, ПК9, ПК10, ПК13
1.3	Правовые режимы защиты информации конфиденциального характера	9	6	6	8	Опрос, практические занятия	3	ОПК7, ПК1, ПК5, ПК6, ПК9, ПК10, ПК13
1.4	Государственное регулирование деятельности в области защиты информации	9	2	2	8	Опрос, практические занятия		ОПК7, ПК1, ПК5, ПК6, ПК9, ПК10, ПК13
1.5	Правовая охрана результатов интеллектуальной деятельности	9	2	2	8	Опрос, практические занятия		ОПК7, ПК1, ПК5, ПК6, ПК9, ПК10, ПК13
1.6	Преступления в сфере компьютерной информации	9	2	2	8	Опрос, практические занятия		ОПК7, ПК1, ПК5, ПК6, ПК9, ПК10, ПК13
	Раздел 2. Организационное обеспечение информационной безопасности							ОПК7, ПК1, ПК5, ПК6, ПК9, ПК10, ПК13
2.1	Понятие организационной защиты информации	9	2	2	8	Опрос, практические занятия		ОПК7, ПК1, ПК5, ПК6, ПК9, ПК10, ПК13
2.2	Методы обеспечения физической безопасности	9	2	2	6	Опрос, практические занятия		ОПК7, ПК1, ПК5, ПК6, ПК9, ПК10, ПК13
2.3	Организация работы службы безопасности предприятия.	9	4	4	8	Опрос, практические занятия	3	ОПК7, ПК1, ПК5, ПК6, ПК9, ПК10, ПК13
2.4	Организация объектовых режимов безопасности	9	4	4	6	Опрос, практические занятия	3	ОПК7, ПК1, ПК5, ПК6, ПК9, ПК10, ПК13
2.5	Управление персоналом на	9	2	2	4	Опрос, практические	3	ОПК7, ПК1, ПК5, ПК6, ПК

предприятия					ские занятия		9,ПК10,ПК13
ИТОГО	9	32	32	80		18	

4.2. Содержание разделов дисциплины

4.2.1 Правовое обеспечение информационной безопасности

4.2.1.1 Информационные отношения как объект правового регулирования.

Правовой режим информации. Правовой статус обладателя информации. Конституционные гарантии прав граждан в информационной сфере и механизм их реализации.. Правовой режим информационных технологий информационная безопасность и ее обеспечение. Защита информации. Роль информационной безопасности в национальной безопасности. Обеспечение информационной безопасности Российской Федерации. Содержание и структура законодательства в области информационной безопасности.

4.2.1.2 Правовой режим защиты государственной тайны

Государственная тайна как особый вид защищаемой информации и ее характерные признаки. Порядок отнесения сведений к государственной тайне. Порядок засекречивания и рассекречивания. Порядок распоряжения сведениями, составляющими государственную тайну. Система защиты сведений, составляющих государственную тайну

4.2.1.3 Правовые режимы защиты информации конфиденциального характера

Понятие информации конфиденциального характера по российскому законодательству. Основные виды конфиденциальной информации. Законодательство о персональных данных. Принципы и условия обработки персональных данных, их конфиденциальность. Права субъектов персональных данных. Обязанности оператора при обработке персональных данных. Контроль и надзор. Законодательство о коммерческой тайне. Порядок отнесения информации к коммерческой тайне. Порядок охраны коммерческой тайны. Порядок предоставления информации, составляющей коммерческую тайну. Правовые основы защиты служебной тайны. Защита служебной тайны в соответствии с «Положением о порядке обращения со служебной информацией ограниченного распространения в федеральных органах исполнительной власти». Правовые основы защиты профессиональной тайны. Ответственность за нарушение законодательства.

4.2.1.4 Государственное регулирование деятельности в области защиты информации

Понятие лицензирования по российскому законодательству. Виды деятельности подлежащие лицензированию. Правовая регламентация лицензионной деятельности в области обеспечения информационной

безопасности. Правовые основы сертификации в области защиты информации. Законодательство об электронной цифровой подписи. Особенности использования цифровой подписи.

4.2.1.5 Правовая охрана результатов интеллектуальной деятельности

Общие положения. Авторское право и смежные права. Патентное право. Право на топологии интегральных микросхем. Право на секрет производства. Право на средства индивидуальных юридических лиц, товаров, работ, услуг и предприятий.

4.2.1.6. Преступления в сфере компьютерной информации

Дисциплинарная и административная ответственность. Уголовная ответственность. Особенности правонарушений в информационной сфере. Преступления в сфере компьютерной информации. Основы расследования преступлений в сфере компьютерной информации. Правовая защита информационных систем.

4.2.2 Организационное обеспечение информационной безопасности

4.2.2.1 Понятие организационной защиты информации

Введение в организационное обеспечение информационной безопасности. Сущность организационных методов защиты информации. Соотношение организационных мер защиты информации с мерами правового и технического характера. Организационные структуры государственной системы обеспечения информационной безопасности федеральных органов исполнительной власти. Организационные структуры государственной системы обеспечения информационной безопасности организаций.

4.2.2.2 Методы обеспечения физической безопасности

Объекты охраны: территория, здания, помещения, персонал, информационные ресурсы, материальные и физические ценности. Особенности их охраны. Понятие о рубежах охраны. Противопожарная безопасность. Контроль доступа. Видеонаблюдение. Охранная сигнализация.

4.2.2.3 Организация работы службы безопасности предприятия.

Концепция безопасности предприятия и ее содержание. Политика информационной безопасности. Подразделения, обеспечивающие ИБ предприятия: основные функции, содержание деятельности, структура, обязанности сотрудников. Варианты организационных структур, обеспечивающих защиту информации. Основные документы службы информационной безопасности.

4.2.2.4. Организация объектовых режимов безопасности

Организация пропускного режима. Основные положения инструкции об организации пропускного режима. Контрольно-пропускные пункты, их оборудование и организация работы. Организация внутриобъектового режима. Порядок проведения служебных расследований.

4.2.2.5 Управление персоналом на предприятии

Подбор и расстановка кадров. Направления и методы работы с персоналом, обладающим конфиденциальной информацией. Мотивация добросовестной деятельности. Организация подготовки кадров в области обеспечения информационной безопасности. Основные формы обучения и методы контроля знаний. Методы проверки персонала. Организация служебного расследования по фактам разглашения персоналом конфиденциальной информации. Организационные меры по защите информации при увольнении сотрудника.

4.3. Практические занятия, их содержание

№ п/п	№ раздела дисциплины	Тематика практических занятий	Форма проведения	Формируемые компетенции
1	1	Функции и полномочия ФСТЭК России, ФСБ России, Межведомственной комиссии по защите государственной тайны.	практическое занятие	ОПК1, ПК1ПК6
2	1	Законодательство РФ в области защиты информации конфиденциального характера	практическое занятие	ОПК1, ПК1
3	1	Правовая защита служебной, профессиональной и коммерческой тайны	практическое занятие	ОПК1, ПК1
4	1	Правовая защита персональных данных	практическое занятие	ОПК1, ПК1
5	2	Служба безопасности предприятия	практическое занятие	ОПК1, ПК1 ПК13
6	2	Классификация автоматизированных систем	практическое занятие	ОПК1, ПК1
7	2	Аттестация объектов информатизации	практическое занятие	ПК9, ПК13,ОПК1, ПК1
8	2	Контроль доступа и средства поиска и досмотра. Системы контроля доступа	практическое занятие	ПК13

5. Учебно-методическое обеспечение самостоятельной работы студентов и оценочные средства для текущего контроля успеваемости, промежуточной аттестации по итогам освоения дисциплины

5.1. Текущий контроль

Устный опрос, выполнение практических работ

5.3. Промежуточный контроль: экзамен

Перечень вопросов к экзамену

- 1) Структура информационной сферы, характеристика ее элементов.

- 2) Информация как объект правоотношений, категории информации.
- 3) Система правовой защиты информации.
- 4) Понятие и виды защищаемой информации.
- 5) Особенности государственной тайны как защищаемой информации.
- 6) Система защиты государственной тайны.
- 7) Засекречивание информации, отнесенной к государственной тайне.
- 8) Защита сведений отнесенных к государственной тайне.
- 9) Понятие информации конфиденциального характера
- 10) Основные виды конфиденциальной информации, в соответствии с требованиями российской нормативно-правовой базы.
- 11) Правовой режим конфиденциальной информации
- 12) Основные требования, предъявляемые к организации защиты конфиденциальной информации
- 13) Понятие и характеристика служебной тайны
- 14) Нормативно-правовые основы защиты служебной тайны
- 15) Порядок обращения с документами, содержащими служебную информацию ограниченного распространения.
- 16) Правовые основы защиты коммерческой тайны.
- 17) Виды информации, составляющей коммерческую тайну
- 18) Основные угрозы коммерческой тайны
- 19) Правовые основы защиты банковской тайны.
- 20) Нарушение банковской тайны и ответственность за подобные нарушения
- 21) Нотариальная тайна и ее особенности. Тайна завещания.
- 22) Врачебная тайна и ее особенности.
- 23) Адвокатская тайна и ее особенности
- 24) Тайна страхования и ее особенности
- 25) Тайна связи и ее особенности. Тайна переписки, почтовых, телеграфных и иных сообщений
- 26) Тайна усыновления (удочерения). Тайна исповеди.
- 27) Формирование российского законодательства в области защиты персональных данных.
- 28) Основные понятия и содержание закона РФ «О персональных данных»
- 29) Подзаконные нормативно-правовые документы о порядке правовой защиты персональных данных

- 30) Государственный надзор и контроль обработки персональных данных, ответственность за нарушения законодательства в данной области.
- 31) Правовые основы лицензирования в области защиты информации.
- 32) Правовые основы сертификации в области защиты информации.
- 33) Особенности правонарушений в информационной сфере
- 34) Преступления в сфере компьютерной информации: виды, состав.
- 35) Основы расследования преступлений в сфере компьютерной информации
- 36) Правовая защита результатов интеллектуальной деятельности
- 37) Соотношение организационных мер защиты информации с мерами правового и технического характера
- 38) Основные термины, связанные с организацией информации
- 39) Организационные меры, направленные на защиту государственной тайны
- 40) Распределение между уровнями государственного управления полномочий, управленческих функций и задач по защите государственной тайны.
- 41) Установление и изменение степени секретности сведений, отнесенных к государственной тайне
- 42) Понятие «рассекречивание сведений». Основания для рассекречивания сведений.
- 43) Порядок допуска и доступа к государственной тайне. Основные принципы допускной работы.
- 44) Объекты охраны: территория, здания, помещения, персонал, информационные ресурсы, материальные и финансовые ценности. Особенности их охраны
- 45) Понятие о рубежах охраны. Многорубежная система охраны
- 46) Подбор и расстановка кадров
- 47) Направления и методы работы с персоналом, обладающим конфиденциальной информацией. Организация обучения персонала
- 48) Основные формы обучения и методы контроля знаний
- 49) Основные формы воздействия на персонал как методы мотивации: вознаграждение, управление карьерой, профессиональная этика
- 50) Организация служебного расследования по фактам разглашения персоналом конфиденциальной информации
- 51) Основные требования, предъявляемые к подготовке и проведению конфиденциальных переговоров
- 52) Подготовка помещения для проведения конфиденциальных переговоров
- 53) Концепция безопасности предприятия и ее содержание. Политика информационной безопасности

- 54) Подразделения, обеспечивающие ИБ предприятия: основные функции, содержание деятельности, структур, обязанностей сотрудников
- 55) Основные документы службы информационной безопасности

Критерии оценивания:

Оценка «отлично» ставится студенту, ответ которого содержит:

- глубокое знание программного материала, а также основного содержания и новаций лекционного курса по сравнению с учебной литературой;
- знание концептуально-понятийного аппарата всего курса; а также свидетельствует о способности:
- самостоятельно критически оценивать основные положения курса;
- увязывать теорию с практикой.

Оценка «отлично» не ставится в случаях систематических пропусков студентом семинарских и лабораторных занятий по неуважительным причинам, а также неправильных ответов на дополнительные вопросы преподавателя.

Оценка «хорошо» ставится студенту, ответ которого свидетельствует о полном знании материала по программе, а также содержит в целом правильное, но не всегда точное и аргументированное изложение материала.

Оценка «хорошо» не ставится в случаях систематических пропусков студентом семинарских и практических занятий по неуважительным причинам, а также неправильных ответов на дополнительные вопросы преподавателя.

Оценка «удовлетворительно» ставится студенту, ответ которого содержит:

- поверхностные знания важнейших разделов программы и содержания лекционного курса;
- затруднения с использованием научно-понятийного аппарата и терминологии курса;
- стремление логически четко построить ответ, а также свидетельствует о возможности последующего обучения.

Оценка «неудовлетворительно» ставится студенту, имеющему существенные пробелы в знании основного материала по программе, а также допустившему принципиальные ошибки при изложении материала.

6. Учебно-методическое и информационное обеспечение дисциплины

а) основная литература:

- 1) Организационное и правовое обеспечение информационной безопасности : учебник и практикум для бакалавриата и магистратуры / Т. А. Полякова, А. А. Стрельцов, С. Г. Чубукова, В. А. Ниесов ; под ред. Т. А. Поляковой, А. А. Стрельцова. — М. : Издательство Юрайт, 2018. — 325 с. — (Серия : Бакалавр и магистр. Академический курс). — ISBN 978-5-534-03600-8. — Режим доступа : www.biblio-online.ru/book/D056DF3D-E22B-4A93-8B66-E6BAEF354847.

- 2) Внуков, А. А. Защита информации : учебное пособие для бакалавриата и магистратуры / А. А. Внуков. — 2-е изд., испр. и доп. — М. : Издательство Юрайт, 2018. — 261 с. — (Серия : Бакалавр и магистр. Академический курс). — ISBN 978-5-534-01678-9. — Режим доступа : www.biblio-online.ru/book/73BEF88E-FC6D-494A-821C-D213E1A984E1.

б) дополнительная литература:

1) Куняев, Н. Н. Правовое обеспечение национальных интересов Российской Федерации в информационной сфере [Электронный ресурс] / Н. Н. Куняев. - М.: Логос, 2010. - 348 с. - ISBN 978-5-98704-513-8. - Режим доступа: <http://znanium.com/bookread2.php?book=469026>

2) Организационно-правовое обеспечение информационной безопасности: Учебное пособие/ Богданов П.Ю. Яготинцева Н.В., СПб.: «Андреевский издательский дом», 2015 г. – 169 стр.

3) Информационная безопасность: нормативно-правовые аспекты: Учебное пособие / Ю.А. Родичев, –СПб.: Питер, 2010 г. -272с. – Электронное издание.

4) Информационная безопасность: нормативно-правовые аспекты: Учебное пособие / Ю.А. Родичев, –СПб.: Питер, 2010 г. -272с. – Электронное издание.

в) программное обеспечение и Интернет-ресурсы:

Программное обеспечение:

- windows 7
- office 2007
- dr Web

Интернет-ресурсы

- <https://biblio-online.ru> – ЭБС Юрайт
- <http://znanium.com> – ЭБС Знаниум
- <http://www.prospektnauki.ru> – ЭБС Проспект науки
- <http://elib.rshu.ru> ЭБС ГидроМетеоОнлайн
- <https://нэб.рф> - Национальная электронная библиотека
- www.fstec.ru Федеральная служба технического и экспортного контроля
- <http://www.consultant.ru> справочная система" Консультант Плюс"
- <http://www.garant.ru> справочная система"Гарант"

7. Методические указания для обучающихся по освоению дисциплины

В настоящее время в рамках учебного процесса по данной дисциплине все большее значение приобретает самостоятельная работа студентов. Это объясняется, прежде всего, тем, что постоянно возрастает количество учебного и научно-теоретического материала, которым необходимо овладеть студенту в

процессе изучения данной дисциплины. В ходе проведения аудиторных занятий по дисциплине возникает проблема нехватки времени на углубленное изучение определенных вопросов, связанных с рассмотрением различных вопросов Информационной безопасности.

Самостоятельная работа дает возможность студентам проверить, а преподавателю решить задачи контроля уровня усвоения вопросов изучения организационного и правового обеспечения информационной безопасности, выявить пробелы в знаниях и наметить пути их устранения. Самостоятельная работа способствует выработке у студентов умений грамотно и четко формировать и излагать свои мысли, вести творческую дискуссию, отстаивать свои мнения и убеждения. По темам дисциплины дан перечень наиболее важных вопросов курса, а также список литературы.

Важным этапом самостоятельной подготовки является изучение соответствующих разделов в учебниках и учебных пособиях, и только после этого, когда уже имеется теоретическая база для уяснения более сложного материала, нужно приступить к изучению литературы, содержащей информацию по проблемным вопросам темы.

8. Информационные технологии, используемые при осуществлении образовательного процесса по дисциплине, включая перечень программного обеспечения и информационных справочных систем (при необходимости)

Тема (раздел) дисциплины	Образовательные и информационные технологии	Перечень программного обеспечения и информационных справочных систем
Информационные отношения как объект правового регулирования	Лекции, практические работы, презентации	https://biblio-online.ru http://znanium.com http://www.prospektnauki.ru http://elib.rshu.ru https://нэб.пф windows 7 office 2007 dr Web www.fstec.ru http://www.consultant.ru http://www.garant.ru
Правовой режим защиты государственной тайны	Лекции, практические работы, презентации	https://biblio-online.ru http://znanium.com

		http://www.prospektnauki.ru http://elib.rshu.ru https://нэб.пф windows 7 office 2007 dr Web www.fstec.ru http://www.consultant.ru http://www.garant.ru
Правовые режимы защиты информации конфиденциального характера	Лекции, практические работы, презентации	https://biblio-online.ru http://znanium.com http://www.prospektnauki.ru http://elib.rshu.ru https://нэб.пф windows 7 office 2007 dr Web www.fstec.ru http://www.consultant.ru http://www.garant.ru
Государственное регулирование деятельности в области защиты информации	Лекции, практические работы, презентации	https://biblio-online.ru http://znanium.com http://www.prospektnauki.ru http://elib.rshu.ru https://нэб.пф windows 7 office 2007 dr Web www.fstec.ru http://www.consultant.ru http://www.garant.ru
Правовая охрана результатов интеллектуальной деятельности	Лекции, практические работы, презентации	https://biblio-online.ru http://znanium.com http://www.prospektnauki.ru http://elib.rshu.ru https://нэб.пф windows 7 office 2007 dr Web www.fstec.ru http://www.consultant.ru http://www.garant.ru
Преступления в сфере компьютерной информации	Лекции, практические работы, презентации	https://biblio-online.ru http://znanium.com http://www.prospektnauki.ru http://elib.rshu.ru https://нэб.пф windows 7 office 2007 dr Web www.fstec.ru http://www.consultant.ru http://www.garant.ru

Раздел 2. Организационное обеспечение информационной безопасности	Лекции, практические работы, презентации	https://biblio-online.ru http://znanium.com http://www.prospektnauki.ru http://elib.rshu.ru https://нэб.пф windows 7 office 2007 dr Web www.fstec.ru http://www.consultant.ru http://www.garant.ru
Понятие организационной защиты информации	Лекции, практические работы, презентации	https://biblio-online.ru http://znanium.com http://www.prospektnauki.ru http://elib.rshu.ru https://нэб.пф windows 7 office 2007 dr Web www.fstec.ru http://www.consultant.ru http://www.garant.ru
Методы обеспечения физической безопасности	Лекции, практические работы, презентации	https://biblio-online.ru http://znanium.com http://www.prospektnauki.ru http://elib.rshu.ru https://нэб.пф windows 7 office 2007 dr Web www.fstec.ru http://www.consultant.ru http://www.garant.ru
Организация работы службы безопасности предприятия.	Лекции, практические работы, презентации	https://biblio-online.ru http://znanium.com http://www.prospektnauki.ru http://elib.rshu.ru https://нэб.пф windows 7 office 2007 dr Web www.fstec.ru http://www.consultant.ru http://www.garant.ru
Организация объектовых режимов безопасности	Лекции, практические работы, презентации	https://biblio-online.ru http://znanium.com http://www.prospektnauki.ru http://elib.rshu.ru https://нэб.пф windows 7 office 2007 dr Web www.fstec.ru http://www.consultant.ru

		http://www.garant.ru
Управление персоналом на предприятии	Лекции, практические работы, презентации	https://biblio-online.ru http://znanium.com http://www.prospektnauki.ru http://elib.rshu.ru https://нэб.рф windows 7 office 2007 dr Web www.fstec.ru http://www.consultant.ru http://www.garant.ru

9. Особенности освоения дисциплины для инвалидов и лиц с ограниченными возможностями здоровья

Обучение обучающихся с ограниченными возможностями здоровья при необходимости осуществляется на основе адаптированной рабочей программы с использованием специальных методов обучения и дидактических материалов, составленных с учетом особенностей психофизического развития, индивидуальных возможностей и состояния здоровья таких обучающихся (обучающегося).

При определении формы проведения занятий с обучающимся-инвалидом учитываются рекомендации, содержащиеся в индивидуальной программе реабилитации инвалида, относительно рекомендованных условий и видов труда.

При необходимости для обучающихся из числа инвалидов и лиц с ограниченными возможностями здоровья создаются специальные рабочие места с учетом нарушенных функций и ограничений жизнедеятельности.

10. Материально-техническое обеспечение дисциплины

Учебная аудитория для проведения занятий лекционного типа – укомплектована специализированной (учебной) мебелью, проектором и экраном для демонстрации иллюстрированных презентаций.

Учебная аудитория для проведения практических работ и занятий семинарского типа - укомплектована специализированной (учебной) мебелью, персональными компьютерами, служащими для выполнения практических работ и поиска информации. .

Учебная аудитория для групповых и индивидуальных консультаций - укомплектована специализированной (учебной) мебелью, техническими средствами обучения, служащими для представления учебной информации.

Учебная аудитория для текущего контроля и промежуточной аттестации - укомплектована специализированной (учебной) мебелью, техническими

средствами обучения, служащими для представления учебной информации.

Помещение для самостоятельной работы – укомплектовано специализированной (учебной) мебелью, оснащено компьютерной техникой с возможностью подключения к сети "Интернет" и обеспечено доступом в электронную информационно-образовательную среду организации

Рассмотрено и рекомендовано к использованию в учебном процессе на
2019/2020 учебный год с изменениями (смотри лист изменений)

Протокол заседания кафедры ИТиСБ от 07.05.2019 №5

Лист Изменений

Изменения, внесенные протоколом заседания кафедры ИТиСБ
от 07.05.2019 №5

1. Дисциплина перенесена на 7 семестр.