

МИНОБРНАУКИ РОССИИ



Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Российский государственный гуманитарный университет»
(ФГБОУ ВО «РГГУ»)

ИНСТИТУТ ИНФОРМАЦИОННЫХ НАУК И ТЕХНОЛОГИЙ БЕЗОПАСНОСТИ
Факультет информационных систем и безопасности
Кафедра информационной безопасности

ОРГАНИЗАЦИОННОЕ И ПРАВОВОЕ ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

ПРАВОВОЕ ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

По направлению подготовки 10.03.01 «Информационная безопасность»
профили Организация и технология защиты информации, Безопасность
автоматизированных систем
Уровень квалификации выпускника (*бакалавр*)

Форма обучения (*очная*)

РПД адаптирована для лиц
с ограниченными возможностями
здоровья и инвалидов

Москва 2021

Организационное и правовое обеспечение
информационной безопасности.
Правовое обеспечение информационной безопасности

Рабочая программа дисциплины
Составитель:
к.и.н., доцент, заведующая кафедрой
информационной безопасности Г.А. Шевцова

УТВЕРЖДЕНО
Протокол заседания кафедры информационной безопасности
№ 10 от 20.05.2021

ОГЛАВЛЕНИЕ

1. Пояснительная записка

1.1 Цель и задачи дисциплины (*модуля*)

1.2. Перечень планируемых результатов обучения по дисциплине (*модулю*), соотнесенных с индикаторами достижения компетенций

1.3. Место дисциплины в структуре образовательной программы

2. Структура дисциплины (*модуля*)

3. Содержание дисциплины (*модуля*)

4. Образовательные технологии

5. Оценка планируемых результатов обучения

5.1. Система оценивания

5.2. Критерии выставления оценок

5.3. Оценочные средства (материалы) для текущего контроля успеваемости, промежуточной аттестации обучающихся по дисциплине (*модулю*)

6. Учебно-методическое и информационное обеспечение дисциплины

6.1. Список источников и литературы

6.2. Перечень ресурсов информационно-телекоммуникационной сети «Интернет»

7. Материально-техническое обеспечение дисциплины (*модуля*)

8. Обеспечение образовательного процесса для лиц с ограниченными возможностями здоровья и инвалидов

9. Методические материалы

9.1. Планы практических (семинарских, лабораторных) занятий

9.2. Методические рекомендации по подготовке письменных работ

9.3. Иные материалы

Приложения

Приложение 1. Аннотация дисциплины

Приложение 2. Лист изменений

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

1. Пояснительная записка

1.1. Цель и задачи дисциплины (модуля)

Цель дисциплины (модуля): формирование культуры информационной безопасности (ИБ) в социальной среде.

Задачи дисциплины:

- изучение основных угроз ИБ в социальной среде;
- формирование знаний у обучающихся о правовых и организационных принципах обеспечения ИБ в социальной среде;
- выработка у обучающихся практических умений по использованию методов обеспечения ИБ.

Цель курса: сформировать взгляд на правовое обеспечение информационной безопасности как на системную научно-практическую деятельность, одну из основ которой составляет работа по нормативно-правовому обеспечению информационной безопасности.

Задачи курса:

- изучить конституционные гарантии прав граждан на доступ к информации, в том числе права свободно искать, получать, передавать, производить и распространять информацию любым законным способом с учетом особенностей реализации этих прав в отношении информации ограниченного доступа;
- освоить основы правового регулирования отношений в информационной сфере, меры и средства организационно-правового обеспечения информационной безопасности и защиты информации ограниченного доступа, в том числе основополагающие государственные стандарты РФ в области информационной безопасности и защиты информации;
- рассмотреть понятие тайны как правового режима ограничения доступа к информации, в том числе правового режима государственной тайны и иных видов тайн, особенности правового регулирования отношений в сфере обращения информации о персональных данных граждан;
- изучить правовые основы и порядок сертификации средств защиты информации и практику правового регулирования лицензионной деятельности в области информационной безопасности и защиты информации ограниченного доступа.

1.2. Формируемые компетенции, соотнесённые с планируемыми результатами обучения по дисциплине (модулю):

Компетенция (код и наименование)	Индикаторы компетенций (код и наименование)	Результаты обучения
УК-2 - Способен определять круг задач в рамках поставленной цели и выбирать оптимальные способы их решения, исходя из действующих правовых норм, имеющих ресурсы и ограничений	УК-2.1 Уметь анализировать имеющиеся ресурсы и ограничения, оценивать и выбирать оптимальные способы решения поставленных задач	Знать особенности государственно-конституционного устройства и правовые основы современного Российского государства, соотношения прав отдельных личностей, общества и государства в целом, а также характеристики и содержание основных отраслей права; Уметь: оформлять рабочую техническую документацию с учетом действующих нормативных и методических документов Владеть: навыками использовать основы правовых знаний в различных сферах деятельности
	УК-2.2 Уметь использовать знаний о важнейших нормах, институтах и отраслях действующего российского права для определения круга задач и оптимальных способов их решения.	
УК-10 - Способен формировать нетерпимое отношение к коррупционному поведению	УК-10.1 Знает сущность коррупционного поведения и его взаимосвязь с социальными, экономическими, политическими и иными условиями	Знать: закономерности развития предприятий различного типа и организацию их функционирования с целью достижения максимальной эффективности при минимальных затратах ресурсов. Уметь: оформлять рабочую техническую документацию с учетом действующих нормативных и методических документов Владеть: навыками использовать основы правовых знаний в различных сферах деятельности
	УК-10.2 Умеет анализировать, толковать и правильно применять правовые нормы о противодействии коррупционному поведению	
	УК-10.3 Владеет навыками работы с законодательными и другими нормативными правовыми актами	
ОПК-5 - Способен применять нормативные правовые акты, нормативные и методические документы,	ОПК-5.1 Уметь применять нормативные правовые акты, нормативные и методические документы, регламентирующие	Знать особенности государственно-конституционного устройства и правовые основы современного Российского государства, соотношения прав отдельных

регламентирующие деятельность по защите информации в сфере профессиональной деятельности;	деятельность по защите информации в сфере профессиональной деятельности	личностей, общества и государства в целом, а также характеристики и содержание основных отраслей права; Уметь: оформлять рабочую техническую документацию с учетом действующих нормативных и методических документов Владеть: навыками использовать основы правовых знаний в различных сферах деятельности
	ОПК-5.2 Уметь обосновывать решения, связанные с реализацией правовых норм по защите информации в пределах должностных обязанностей, предпринимать необходимые меры по восстановлению нарушенных прав	
	ОПК-5.3 Владеть навыками разрабатывать проекты локальных правовых документов, регламентирующих работу по обеспечению информационной безопасности в организации	
ОПК-6 - Способен при решении профессиональных задач организовывать защиту информации ограниченного доступа в соответствии с нормативными правовыми актами, нормативными и методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю;	ОПК-6.1 Знать нормативные, руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации	Знать особенности государственно-конституционного устройства и правовые основы современного Российского государства, соотношения прав отдельных личностей, общества и государства в целом, а также характеристики и содержание основных отраслей права; Уметь: оформлять рабочую техническую документацию с учетом действующих нормативных и методических документов Владеть: навыками использовать основы правовых знаний в различных сферах деятельности
	ОПК-6.2 Умеет разрабатывать проекты локальных нормативных документов, регламентирующих защиту информации ограниченного доступа в организации	
	ОПК-6.3 Владеет навыками по разработке политики безопасности объекта информатизации	

1.1. Место дисциплины в структуре основной образовательной программы

Дисциплина (модуль) «Правовое обеспечение информационной безопасности» входит в базовую часть цикла дисциплин подготовки студентов по направлению подготовки 10.03.01 «Информационная безопасность». Дисциплина реализуется кафедрой Информационной безопасности.

Для освоения дисциплины (модуля) необходимы знания, умения и владения, сформированные в ходе изучения следующих дисциплин и прохождения практик: «Основы информационной безопасности», «Специальное документоведение и документационное обеспечение управления».

В результате освоения дисциплины (модуля) формируются знания, умения и владения, необходимые для прохождения дисциплин «Организационное обеспечение информационной безопасности» и «Правовая охрана результатов интеллектуальной деятельности».

2. Структура дисциплины (модуля) для очной формы обучения

Общая трудоемкость дисциплины составляет 2 з. е., 76 ч., в том числе контактная работа обучающихся с преподавателем 48 ч., самостоятельная работа обучающихся 28 ч.

№ п/п	Раздел дисциплины/темы	Семестр	Виды учебной работы (в часах)					Самостоятельная работа	Формы текущего контроля успеваемости, форма промежуточной аттестации (по семестрам)
			контактная						
			Лекции	Семинар	Практические занятия	Лабораторные занятия	Промежуточная аттестация		
1	Введение. Информационная безопасность как определяющий компонент национальной безопасности России	3	2		4			2	
2	Право на информацию. Право на доступ к информации	3	2		4			2	Опрос
3	Информационная сфера как объект правовых отношений	3	2		4			2	Опрос
4	Закон РФ «Об информации, информационных технологиях и защите информации» как организационно-правовая основа регулирования правоотношений в информационной сфере	3	2		4			2	Опрос
5	Правовое обеспечение защиты документированной информации с ограниченным доступом. Стандарты информационной	3	2		4			2	Опрос Ситуационная задача

	безопасности							
6	Тайна как правовой режим ограничения доступа к информации – государственная тайна, служебная тайна, коммерческая тайна, профессиональные тайны	3	2	4			2	Опрос Тестирование
7	Правовое регулирование отношений в сфере обращения информации о персональных данных граждан	3	2	4			4	Опрос
8	Правовые особенности сертификации средств защиты информации и правовое регулирование лицензионной деятельности в области защиты информации	3	2	4			4	Опрос Ситуационная задача
9	Зачёт с оценкой	3					8	Итоговая контрольная работа
	Итого		16	32			28	

3. Содержание дисциплины (модуля)

№	Наименование раздела дисциплины	Содержание
	Тема 1. Введение. Информационная безопасность как определяющий компонент национальной безопасности России.	<p>Предмет и содержание дисциплины, методы ее изучения, источники и литература, контроль освоения.</p> <p>Направления государственной политики РФ по обеспечению информационной безопасности личности, общества и государства. Доктрина информационной безопасности РФ.</p> <p>Понятия «правовое обеспечение информационной безопасности» и «правовая защита информации». Определение указанных понятий по целям, функциям, структуре.</p>
	Тема 2. Право на информацию. Право на доступ к информации.	<p>Составляющие права на информацию. Законодательство о праве на информацию.</p> <p>Право на доступ к информации, в том числе к информации о деятельности органов государственной власти и местного самоуправления.</p>

	<p>Тема 3. Информационная сфера как объект правовых отношений.</p>	<p>Понятие информационной сферы и ее составляющие. Информация как объект гражданско-правовых отношений. Правовые принципы защиты информации. Информационные системы как объекты правовых отношений.</p> <p>Место правовой защиты информации в системе комплексной защиты информации.</p>
	<p>Тема 4. Закон РФ «Об информации, информационных технологиях и защите информации» как организационно-правовая основа регулирования правоотношений в информационной сфере.</p>	<p>Сфера действия Закона. Основные понятия, используемые в Законе. Права обладателя информации. Порядок распространения или предоставления информации.</p> <p>Порядок документирования информации.</p> <p>Государственное регулирование в сфере применения информационных технологий.</p> <p>Порядок обеспечения защиты информации.</p>
	<p>Тема 5. Правовое обеспечение защиты документированной информации с ограниченным доступом. Стандарты информационной безопасности.</p>	<p>Принципы правового обеспечения защиты документированной информации с ограниченным доступом.</p> <p>Меры и средства организационно-правовой защиты информации ограниченного доступа как необходимое условие обеспечения информационной безопасности для организации любой формы собственности.</p> <p>Основополагающие государственные стандарты РФ в области информационной безопасности и защиты информации</p> <p>Документационное обеспечение защиты информации в организации любой формы собственности.</p>
	<p>Тема 6. Тайна как правовой режим ограничения доступа к информации.</p>	<p>Разновидности правового режима информации. Правовой режим ограниченного доступа к информации. Виды информации ограниченного доступа. Виды конфиденциальной информации.</p> <p>Понятие государственной тайны, основные положения законодательства о государственной тайне.</p> <p>Правовое регулирование режимов коммерческой тайны, служебной тайны, банковской тайны и профессиональных тайн.</p>

		Право на секрет производства (ноу-хау). Служебный секрет производства
	Тема 7. Правовое регулирование отношений в сфере обращения информации о персональных данных граждан.	<p>Основные понятия законодательства о персональных данных, разница между понятиями «неприкосновенность частной жизни» и «персональные данные» как объектов права. Общедоступные источники персональных данных. Специальные категории персональных данных. Биометрические персональные данные.</p> <p>Принципы и условия обработки персональных данных. Права субъекта персональных данных. Обязанности оператора при обработке персональных данных. Права уполномоченного органа по защите прав субъектов персональных данных.</p> <p>Классификация информационных систем персональных данных. Основные методы и способы защиты информации в информационных системах персональных данных для различных классов этих систем.</p>
	Тема 8. Правовые особенности сертификации средств защиты информации и правовое регулирование лицензионной деятельности в области защиты информации.	<p>Понятие сертификации и общие положения о сертификации средств защиты информации.</p> <p>Технические регламенты и стандарты. Подтверждение соответствия. Информация о нарушении требований технических регламентов и стандартов.</p> <p>Порядок лицензирования деятельности по технической защите конфиденциальной информации и по разработке и/или производству средств защиты конфиденциальной информации.</p>

4. Образовательные технологии

При реализации рабочей программы дисциплины «Правовое обеспечение информационной безопасности» используются следующие образовательные технологии:

№ п/п	Наименование раздела	Виды учебных занятий	Образовательные технологии
1	2	3	4
1	Введение. Информационная безопасность как определяющий компонент	Лекция 1	Вводная лекция с использованием презентационного материала

№ п/п	Наименование раздела	Виды учебных занятий	Образовательные технологии
1	2	3	4
	национальной безопасности России		
2	Право на информацию. Право на доступ к информации	Лекция 2 Практические занятия 1-2	Лекция-дискуссия с использованием презентационного материала
3	Информационная сфера как объект правовых отношений	Лекция 3 Практическое занятие 3	Лекция-дискуссия с использованием презентационного материала
4	Закон РФ «Об информации, информационных технологиях и защите информации» как организационно-правовая основа регулирования правоотношений в информационной сфере	Лекция 4 Практические занятия 4	Лекция-дискуссия с использованием презентационного материала р
5	Правовое обеспечение защиты документированной информации с ограниченным доступом. Стандарты информационной безопасности	Лекция 5 Практические занятия 5-6	Лекция-дискуссия с использованием презентационного материала Тестирование
6	Тайна как правовой режим ограничения доступа к информации – государственная тайна, служебная тайна, коммерческая тайна, профессиональные тайны	Лекции 6-11 Практические занятия 7-14	Лекция с использованием презентационного материала Тестирование
7	Правовое регулирование отношений в сфере обращения информации о персональных данных граждан	Лекция 12 Практические занятия 15-16	Лекция-дискуссия Консультирование и проверка домашних заданий посредством электронных носителей
8	Правовые особенности сертификации средств защиты информации и правовое регулирование лицензионной деятельности в области защиты информации	Практические занятия 17-18	Консультирование и проверка домашних заданий посредством электронных носителей

5. Оценка планируемых результатов обучения

5.1. Система оценивания

Система текущего и промежуточного контроля знаний по дисциплине «Правовое обеспечение информационной безопасности» предусматривает:

проведение текущего контроля знаний в устной форме (опрос);

выполнение самостоятельной работы и тестирование в письменной форме (возможно с помощью компьютерных технологий);

проведение промежуточной аттестации (зачет с оценкой) в форме письменного ответа на вопросы заданий.

По каждому виду и форме контроля предусмотрено следующее распределение баллов:

Форма контроля	Максимальное количество баллов	
	За одну работу	Всего
Текущий контроль: - опрос по темам 2-8; - тестирование по темам 5, 6; - самостоятельной работы на семинаре по теме 8;	4 балл 10 баллов 12 баллов	28 баллов 20 баллов 12 баллов
Промежуточная аттестация (зачет с оценкой)	40 баллов	
Итого за семестр (дисциплину):	100 баллов	

Перечень компетенций с указанием этапов их формирования в процессе освоения дисциплины представляется в виде таблицы:

<i>№ п/п</i>	<i>Контролируемые разделы дисциплины</i>	<i>Код контролируемой компетенции</i>	<i>Наименование оценочного средства</i>
1.	1-3	УК-2; УК-10; ОПК-5; ОПК-6	План практического занятия
2.	4-5	УК-2; УК-10; ОПК-5; ОПК-6	План практического занятия
3.	6-8	УК-2; УК-10; ОПК-5; ОПК-6	Тест План практического занятия Контрольная работа

Полученный совокупный результат конвертируется в традиционную шкалу оценок и в шкалу оценок Европейской системы переноса и накопления кредитов (European Credit Transfer System; далее – ECTS) в соответствии с таблицей:

100-балльная шкала	Традиционная шкала		Шкала ECTS
95 – 100	отлично	зачтено	А
83 – 94			В
68 – 82			хорошо

56 – 67	удовлетворительно		D
50 – 55			E
20 – 49	неудовлетворительно	не зачтено	FX
0 – 19			F

5.2. Критерии выставления оценки по дисциплине

Баллы/ Шкала ECTS	Оценка по дисциплине	Критерии оценки результатов обучения по дисциплине
100-83/ A,B	зачтено	<p>Выставляется обучающемуся, если он глубоко и прочно усвоил теоретический и практический материал, может продемонстрировать это на занятиях и в ходе промежуточной аттестации.</p> <p>Обучающийся исчерпывающе и логически стройно излагает учебный материал, умеет увязывать теорию с практикой, справляется с решением задач профессиональной направленности высокого уровня сложности, правильно обосновывает принятые решения. Свободно ориентируется в учебной и профессиональной литературе.</p> <p>Оценка по дисциплине выставляется обучающемуся с учётом результатов текущей и промежуточной аттестации. Компетенции, закреплённые за дисциплиной, сформированы на уровне – «высокий».</p>
82-68/ C	зачтено	<p>Выставляется обучающемуся, если он знает теоретический и практический материал, грамотно и по существу излагает его на занятиях и в ходе промежуточной аттестации, не допуская существенных неточностей.</p> <p>Обучающийся правильно применяет теоретические положения при решении практических задач профессиональной направленности разного уровня сложности, владеет необходимыми для этого навыками и приёмами.</p> <p>Достаточно хорошо ориентируется в учебной и профессиональной литературе.</p> <p>Оценка по дисциплине выставляется обучающемуся с учётом результатов текущей и промежуточной аттестации. Компетенции, закреплённые за дисциплиной, сформированы на уровне – «хороший».</p>
67-50/ D, E	зачтено	<p>Выставляется обучающемуся, если он знает на базовом уровне теоретический и практический материал, допускает отдельные ошибки при его изложении на занятиях и в ходе промежуточной аттестации.</p> <p>Обучающийся испытывает определённые затруднения в применении теоретических положений при решении практических задач профессиональной направленности стандартного уровня сложности, владеет необходимыми для этого базовыми навыками и приёмами.</p> <p>Демонстрирует достаточный уровень знания учебной литературы по дисциплине.</p>

Баллы/ Шкала ECTS	Оценка по дисциплине	Критерии оценки результатов обучения по дисциплине
		Оценка по дисциплине выставляются обучающемуся с учётом результатов текущей и промежуточной аттестации. Компетенции, закреплённые за дисциплиной, сформированы на уровне – «достаточный».
49-0/ F, FX	не зачтено	Выставляется обучающемуся, если он не знает на базовом уровне теоретический и практический материал, допускает грубые ошибки при его изложении на занятиях и в ходе промежуточной аттестации. Обучающийся испытывает серьёзные затруднения в применении теоретических положений при решении практических задач профессиональной направленности стандартного уровня сложности, не владеет необходимыми для этого навыками и приёмами. Демонстрирует фрагментарные знания учебной литературы по дисциплине. Оценка по дисциплине выставляются обучающемуся с учётом результатов текущей и промежуточной аттестации. Компетенции на уровне «достаточный», закреплённые за дисциплиной, не сформированы.

5.3. Оценочные средства (материалы) для текущего контроля успеваемости, промежуточной аттестации обучающихся по дисциплине (модулю)

Текущий контроль (примерное ситуационное задание для самостоятельной работы по теме 5, 8) - проверка сформированности компетенций - УК-2; УК-10; ОПК-5; ОПК-6

В качестве специалиста в области организации и технологии защиты информации Вы вступили в должность начальника отдела защиты информации (службы безопасности) в ранее созданной и успешно работающей в настоящее время организации. Эта организация _____ подведомственна _____ . Основным видом деятельности этой организации в течение ряда лет являлась разработка _____

На эту организацию в ближайшие три-четыре месяца будет возложена дополнительная обязанность по разработке и серийному производству средств защиты _____

Перечислите и обоснуйте последовательность Ваших организационно-правовых действий, необходимых для успешного выполнения поставленной задачи, в том числе:

- необходимость получения лицензии на указанный вид новой деятельности и наименование организации, в которую Вы будете обращаться для получения лицензии;
- порядок Вашего взаимодействия с этой организацией и перечень документов, которые должны быть представлены Вами в эту организацию;
- основные лицензионные требования и условия, которые должны быть выполнены Вами для получения лицензии и срок действия получаемой лицензии;
- необходимость создания нового подразделения в рамках отдела по защите информации;
- необходимость организации сертификации производимых Вами средств защиты информации, система сертификации, в которую Вы должны будете обратиться и схема проведения сертификации этих средств.

Текущий контроль (примерный тест по теме 6) – проверка сформированности компетенций - УК-2; УК-10; ОПК-5; ОПК-6

Укажите номер правильного ответа

1.. Доступ к сведениям, составляющим государственную тайну это?

1.1. Санкционированное полномочным должностным лицом ознакомление конкретного лица со сведениями, составляющими государственную тайну.

1.2. Процедура оформления права граждан на доступ к сведениям, составляющим государственную тайну, а предприятий, учреждений и организаций - на проведение работ с использованием таких сведений.

1.3. Процедура оформления права граждан на доступ к сведениям, составляющим государственную тайну.

1.4. Санкционированное ознакомление конкретного лица со сведениями, составляющими государственную тайну.

Укажите номер правильного ответа

2. На основании чего устанавливается порядок доступа должностного лица или гражданина к сведениям, составляющим государственную тайну?

2.1. На основании нормативных документов, утвержденных Правительством Российской Федерации.

2.2. На основании нормативных документов, утвержденных Федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности.

2.3. На основании нормативных документов, утвержденных руководителем предприятия.

2.4. На основании нормативных документов, утвержденных руководителем подразделения по защите государственной тайны.

Укажите номер правильного ответа

3. Кто осуществляет законодательное регулирование отношений в области государственной тайны?

3.1. Органы судебной власти.

3.2. Правительство Российской Федерации.

3.3. Палаты Федерального Собрания.

3.4. Органы государственной власти Российской Федерации.

Укажите номер правильного ответа

4. Информацию в зависимости от порядка ее предоставления или распространения подразделяют?

- 4.1. На свободно распространяемую.
- 4.2. На распространяемую между Федеральными органами исполнительной власти.
- 4.3. На распространяемую только в особых случаях.
- 4.4. На информацию перечисленную во всех вышеперечисленных пунктах.

Укажите номер правильного ответа

5. Кто вносит в полномочные органы государственной власти предложения по совершенствованию системы защиты государственной тайны?

- 5.1. Президент Российской Федерации.
- 5.2. Правительство Российской Федерации.
- 5.3. Палаты Федерального Собрания.
- 5.4. Органы государственной власти Российской Федерации.

Укажите номер правильного ответа

6. Владелец информации, составляющей коммерческую тайну, имеет право?

6.1. Защищать в установленном законом порядке свои права в случае незаконного использования третьими лицами информации, составляющей коммерческую тайну.

6.2. Запрещать доступ к информации, составляющей коммерческую тайну.

6.3. Требовать от лиц, получивших доступ к информации, составляющей коммерческую тайну, в результате действий, совершенных случайно или по ошибке, охраны конфиденциальности этой информации.

6.4. Использовать все права указанные выше.

Укажите номер правильного ответа

7. Исключительное право на результат интеллектуальной деятельности это?

7.1. Охраняемая правом возможность правообладателя по своему усмотрению любым не противоречащим закону способом использовать объект интеллектуальной собственности, результат интеллектуальной деятельности или средство индивидуализации, распоряжаться им, разрешать или запрещать другим лицам его использование.

7.2. Охраняемая правом возможность правообладателя по своему усмотрению использовать объект интеллектуальной собственности, результат интеллектуальной деятельности или средство индивидуализации, распоряжаться им, разрешать или запрещать другим лицам его использование.

7.3. Охраняемая правом возможность использовать объект интеллектуальной собственности, результат интеллектуальной деятельности или средство индивидуализации, распоряжаться им, разрешать или запрещать его использование.

7.4. Охраняемая правом возможность правообладателя по своему усмотрению использовать объект интеллектуальной собственности, результат интеллектуальной деятельности, распоряжаться им, разрешать или запрещать другим лицам его использование.

Укажите номер правильного ответа

8. Информационные технологии, представляющие собой процессы и (или) методы

поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов являются?

- 8.1. Субъектом правового режима.
- 8.2. Объектом правового режима.
- 8.3. Техническими средствами информационных систем.
- 8.4. Всеми перечисленными определениями.

Укажите номер правильного ответа

9. Право на средства индивидуализации предприятий включает?

- 9.1. Право на коммерческое обозначение.
- 9.2. Право на оборот товара независимо от его места происхождения.
- 9.3. Право на знак качества.
- 9.4. Все вышеперечисленные права.

Укажите номер правильного ответа

10. Правоприменительная деятельность это?

10.1. Установление определенных правовых норм осуществления наиболее важных общественных отношений и охраны этих норм от нарушения с использованием государственного принуждения.

10.2. Подготовка, принятие и издание законодательными органами нормативных правовых актов, регулирующих отношения в области удовлетворения национальных интересов в информационной сфере, а также создающих условия для предотвращения реализации угроз информационной безопасности.

10.3. Реализация функции государства по обеспечению правосудия в процессе выполнения задач противодействия угрозам информационной безопасности.

10.4. Основанная на законодательстве оперативная, повседневная реализация органами исполнительной власти (государственного управления) функций государства в области обеспечения информационной безопасности.

Примерные контрольные вопросы к зачету по курсу – проверка сформированности компетенций - УК-2; УК-10; ОПК-5; ОПК-6

1. Понятие «национальная безопасность». Информационная безопасность как составная часть национальной безопасности.

2. Понятие «информационная сфера», ее структура. Объекты отношений в информационной сфере. Понятие «информация». Понятия «сведения» и «сообщения» в информационных отношениях. Особенности информации как объекта права. Правовые принципы защиты информации.

3. Сфера действия Закона РФ «Об информации, информационных технологиях и защите информации» и основные понятия, используемые в этом Законе.

4. Правовое обеспечение защиты документированной информации с ограниченным доступом, меры и средства, используемые для организации защиты такой информации.

5. Документационное обеспечение защиты документированной информации ограниченного доступа в организации любой формы собственности.

6. Понятие «информационная система» в Законе РФ «Об информации, информационных технологиях и защите информации». Информационная система (ИС) как объект защиты информации.

7. Основные принципы разработки и реализации политики информационной безопасности в информационной системе. основополагающие стандарты в области информационной безопасности и защите информации.

8. Классификация информации по режиму доступа к ней. Понятие правового режима обращения информации. Правовые режимы свободного доступа к информации.

9. Правовой режим ограниченного доступа к информации, реализуемый на основе понятия «тайна». Тайна как правовая категория и её соотношение с понятием информация. Общий признак всех видов тайн.

10. Определение понятия «государственная тайна». Сфера действия федерального закона «О государственной тайне». Объект и субъекты правоотношений в области государственной тайны.

11. Принципы отнесения сведений к государственной тайне и их засекречивания. Основной критерий выбора степени секретности. Сведения, не подлежащие засекречиванию. Система перечней сведений, составляющих государственную тайну, их роль в системе засекречивания.

12. Иерархия органов защиты государственной тайны и их основные функции. Основные права государства в отношении сведений, относящихся к государственной тайне.

13. Порядок допуска должностных лиц и граждан к сведениям, составляющим государственную тайну, Основания для отказа в получении допуска. Формы допуска в соответствии со степенями секретности. Правовые последствия оформления допуска. Субъекты особого порядка допуска.

14. Развитие российского законодательства о служебной тайне. Признаки, необходимые для отнесения информации к служебной тайне. Основные объекты служебной тайны. Перечень сведений, которые не могут быть отнесены к служебной тайне. .

15. Порядок правовой охраны конфиденциальной информации, переданной в государственный орган исполнительной власти юридическими или физическими лицами – субъектами предпринимательской или иной деятельности. Приведите примеры.

16. Права руководителя федерального государственного органа исполнительной власти в качестве обладателя в отношении собственной служебной тайны и способ реализации этих прав.

17. Основные понятия федерального закона «О коммерческой тайне». Информация, которая может быть отнесена к коммерческой тайне. Законодательно установленный перечень информации, которая не может быть отнесена к коммерческой тайне.

18. Обязательные и факультативные составляющие, используемые для установления режима коммерческой тайны субъектами предпринимательской деятельности. Обязанности работника и работодателя в сфере коммерческой тайны. Виды ответственности за правонарушения в сфере коммерческой тайны.

19. Понятие «профессиональная тайна» и признаки, необходимые для отнесения информации к профессиональной тайне. Субъекты правоотношений для основных видов профессиональных тайн, приведите примеры.

20. Банковская тайна как вид профессиональной тайны и законодательное определение этого понятия. Место банковской тайны в числе иных видов тайн в массиве конфиденциальной информации, которая накапливается, хранится и используется в банковской деятельности.

21. Определение понятий «банковская тайна» и «коммерческая тайна банка», принципиальные различия между этими понятиями. Основные права обладателя банковской тайны (клиента банка) в отношении информации, составляющей его банковскую тайну.

22. Обязанности банка по сохранению и защите конфиденциальной информации обладателей банковской тайны – клиентов банка, которая была получена банком в качестве пользователя этой информацией на законных основаниях. Возможные случаи ограничения прав клиентов банка на защиту такой информации.

23. Основные понятия, используемые в федеральном законе «О персональных данных». Разница между понятиями «неприкосновенность частной жизни» и «персональные данные» как объектов права.

24. Понятие конфиденциальности персональных данных. Общедоступные источники персональных данных. Специальные категории персональных данных. Биометрические персональные данные.

25. Право субъекта персональных данных на доступ к своим персональным данным. Обязанности оператора по обеспечению безопасности персональных данных при

их обработке. Порядок уведомления оператором уполномоченного органа по защите прав субъектов персональных данных.

26. Понятие информационной системы персональных данных. Классификация информационных систем персональных данных.

27. Общие положения законодательства о лицензировании определенных видов деятельности, достоинства и недостатки любой системы лицензирования. Лицензирование деятельности в защиты информации как правовая форма обеспечения информационной безопасности.

28. Правовые особенности лицензирования деятельности по технической защите конфиденциальной информации и по разработке и (или) производству средств защиты конфиденциальной информации.

29. Правовые основы лицензирования деятельности организаций по проведению работ, связанных с использованием сведений, составляющих государственную тайну.

30. Основные понятия ФЗ РФ «О техническом регулировании» (сертификация, стандарт, технический регламент, форма подтверждения соответствия). Организация государственной сертификации средств защиты информации (ЗИ). Органы исполнительной власти, создающие системы сертификации средств ЗИ, участники любой системы сертификации средств ЗИ. Испытательные лаборатории их права и обязанности.

6. Учебно-методическое и информационное обеспечение дисциплины

6.1. Список источников и литературы

Источники

Конституция Российской Федерации (принята всенародным голосованием 12.12.1993), Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_28399/

Гражданский кодекс Российской Федерации. Часть первая, от 30.11.1994 N 51-ФЗ
Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_5142/

Уголовный кодекс Российской Федерации от 13.06.1996 N 63-ФЗ, Режим доступа:
http://www.consultant.ru/document/cons_doc_LAW_10699/

Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Режим доступа:
http://www.consultant.ru/document/cons_doc_LAW_61798/

Закон Российской Федерации от 21.07.93 № 5485-1 “О государственной тайне”,
Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_2481/

Федеральный закон от 29.07.2004 № 98-ФЗ «О коммерческой тайне», Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_48699/

Федеральный закон от 28.12.2010 №390-ФЗ «О безопасности», Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_108546/

Федеральный закон от 04.05.2011 № 99-ФЗ «О лицензировании отдельных видов деятельности», Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_113658/

Федеральный закон от 27.07.2006 N 152-ФЗ «О персональных данных», Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_61801/

Федеральный закон от 27.12.2002 № 184-ФЗ «О техническом регулировании», Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_40241/

Указ Президента Российской Федерации от 06.03.97 № 188 “Об утверждении перечня сведений конфиденциального характера”, Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_13532/

Постановление Правительства Российской Федерации от 15.04.1995 № 333 «О лицензировании деятельности предприятий, учреждений и организаций по проведению работ, связанных с использованием сведений, составляющих государственную тайну, созданием средств защиты информации, а также с осуществлением мероприятий и (или) оказанием услуг по защите государственной тайны», Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_6387/

Постановление Правительства Российской Федерации от 06.02.2010 № 63 «Об утверждении Инструкции о порядке допуска должностных лиц и граждан Российской Федерации к государственной тайне», Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_97474/

Постановление Правительства Российской Федерации от 03.11.94 № 1233 «Об утверждении Положения о порядке обращения со служебной информацией ограниченного распространения в федеральных органах исполнительной власти», Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_54870/

Федеральный закон от 09.02.2009 N 8-ФЗ "Об обеспечении доступа к информации о деятельности государственных органов и органов местного самоуправления" Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_84602/

Федеральный закон от 31.05.2002 N 63-ФЗ "Об адвокатской деятельности и адвокатуре в Российской Федерации" Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_36945/

Постановление Правительства РФ от 26.06.1995 N 608 (ред. от 21.04.2010) "О сертификации средств защиты информации" Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_7054/

ГОСТ Р ИСО/МЭК 17799-2005 "Информационная технология. Практические правила управления информационной безопасностью" (утв. Приказом Ростехрегулирования от 29.12.2005 N 447-ст), Режим доступа: <http://www.consultant.ru/cons/cgi/online.cgi?req=doc;base=EXP;n=447600#013921417480764586>

ГОСТ Р 50922-2006. Защита информации. Основные термины и определения. (утв. Приказом Ростехрегулирования от 27.12.2006 N 373-ст), Режим доступа: <http://www.consultant.ru/cons/cgi/online.cgi?req=doc;base=EXP;n=418509#08480021357350149>

Основная литература

Ельчанинова, Н.Б. Правовые основы защиты информации с ограниченным доступом: учебное пособие / Н.Б. Ельчанинова ; Южный федеральный университет. - Ростов-на-Дону - Таганрог : Издательство Южного федерального университета, 2017. - 76 с. - ISBN 978-5-9275-2501-0. - Текст : электронный. - URL: <https://new.znaniium.com/catalog/product/1021578>

Дополнительная литература

Организационно-правовое обеспечение информационной безопасности: [учеб. пособие] / [А. А. Стрельцов и др.] ; под ред. А. А. Стрельцова. – М.: Академия, 2008. – 248с. 10 э.

Государственная тайна и ее защита в Российской Федерации: учеб. пособие для студентов вузов / П. П. Аникин [и др.]; под общ. ред.: М. А. Вуса и А. В. Федорова. – 3-е изд., испр. и доп. – СПб.: Юрид. центр Пресс, 2007. – 745с.

Информационная безопасность предприятия: Учебное пособие / Гришина Н.В., - 2-е изд., доп - М.:Форум, НИЦ ИНФРА-М, 2016. - 240 с.: 60x90 1/16. - (Высшее образование: Бакалавриат) (Обложка. КБС) ISBN 978-5-00091-007-8 - Режим доступа: <http://znaniium.com/catalog/product/544554>

Правовое обеспечение информационной безопасности: Учебник / [авт.-ред. В. А. Минаев и др.]. – Изд. 2-е, расширенное и доп. – М.: Маросейка, 2008. – С. 120-124.

Перечень БД и ИСС

№п/п	Наименование
	Международные реферативные наукометрические БД, доступные в рамках национальной подписки в 2017 г.

	Web of Science Scopus
	Профессиональные полнотекстовые БД, доступные в рамках национальной подписки в 2017 г. Журналы Oxford University Press ProQuest Dissertation & Theses Global SAGE Journals Журналы Taylor and Francis
	Компьютерные справочные правовые системы Консультант Плюс, Гарант

7. Материально-техническое обеспечение дисциплины/модуля

Материально-техническая база включает учебные аудитории для проведения занятий лекционного типа, занятий семинарского типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации.

Современный компьютерный класс оснащен

Перечень ПО

№п /п	Наименование ПО	Производитель	Способ распространения (лицензионное или свободно распространяемое)
1	Microsoft Office 2010	Microsoft	лицензионное
2	Windows XP	Microsoft	лицензионное
3	Kaspersky Endpoint Security	Kaspersky	лицензионное

включающий наряду с компьютерами, подключёнными к сети Интернет, экран и проектор.

Для проведения занятий лекционного типа предлагаются тематические иллюстрации в формате презентаций PowerPoint.

8. Обеспечение образовательного процесса для лиц с ограниченными возможностями здоровья и инвалидов

В ходе реализации дисциплины используются следующие дополнительные методы обучения, текущего контроля успеваемости и промежуточной аттестации обучающихся в зависимости от их индивидуальных особенностей:

- для слепых и слабовидящих:
 - лекции оформляются в виде электронного документа, доступного с помощью компьютера со специализированным программным обеспечением;
 - письменные задания выполняются на компьютере со специализированным программным обеспечением, или могут быть заменены устным ответом;
 - обеспечивается индивидуальное равномерное освещение не менее 300 люкс;
 - для выполнения задания при необходимости предоставляется увеличивающее устройство; возможно также использование собственных увеличивающих устройств;

- письменные задания оформляются увеличенным шрифтом;
- экзамен и зачёт проводятся в устной форме или выполняются в письменной форме на компьютере.

- для глухих и слабослышащих:
 - лекции оформляются в виде электронного документа, либо предоставляется звукоусиливающая аппаратура индивидуального пользования;

- письменные задания выполняются на компьютере в письменной форме;
- экзамен и зачёт проводятся в письменной форме на компьютере; возможно проведение в форме тестирования.

- для лиц с нарушениями опорно-двигательного аппарата:
 - лекции оформляются в виде электронного документа, доступного с помощью компьютера со специализированным программным обеспечением;

- письменные задания выполняются на компьютере со специализированным программным обеспечением;

- экзамен и зачёт проводятся в устной форме или выполняются в письменной форме на компьютере.

При необходимости предусматривается увеличение времени для подготовки ответа.

Процедура проведения промежуточной аттестации для обучающихся устанавливается с учётом их индивидуальных психофизических особенностей. Промежуточная аттестация может проводиться в несколько этапов.

При проведении процедуры оценивания результатов обучения предусматривается использование технических средств, необходимых в связи с индивидуальными особенностями обучающихся. Эти средства могут быть предоставлены университетом, или могут использоваться собственные технические средства.

Проведение процедуры оценивания результатов обучения допускается с использованием дистанционных образовательных технологий.

Обеспечивается доступ к информационным и библиографическим ресурсам в сети Интернет для каждого обучающегося в формах, адаптированных к ограничениям их здоровья и восприятия информации:

- для слепых и слабовидящих:
 - в печатной форме увеличенным шрифтом;
 - в форме электронного документа;
 - в форме аудиофайла.

- для глухих и слабослышащих:
 - в печатной форме;
 - в форме электронного документа.

- для обучающихся с нарушениями опорно-двигательного аппарата:
 - в печатной форме;
 - в форме электронного документа;
 - в форме аудиофайла.

Учебные аудитории для всех видов контактной и самостоятельной работы, научная библиотека и иные помещения для обучения оснащены специальным оборудованием и учебными местами с техническими средствами обучения:

- для слепых и слабовидящих:
 - устройством для сканирования и чтения с камерой SARA CE;
 - дисплеем Брайля PAC Mate 20;
 - принтером Брайля EmBraille ViewPlus;
- для глухих и слабослышащих:
 - автоматизированным рабочим местом для людей с нарушением слуха и слабослышащих;
 - акустический усилитель и колонки;
- для обучающихся с нарушениями опорно-двигательного аппарата:

- передвижными, регулируемые эргономическими партами СИ-1;
- компьютерной техникой со специальным программным обеспечением.

9. Методические материалы

9.1. Планы практических занятий - проверка сформированности компетенций - УК-2; УК-10; ОПК-5; ОПК-6

Практическое занятие 1, тема 2. (2 часа). Право на доступ к информации - Вопросы для изучения и обсуждения:

1. Теоретические основы и границы права на информацию.
2. Законодательство о праве на информацию. Субъекты права на информацию.
3. Содержание права граждан на информацию.
4. Право на доступ к информации о деятельности органов государственной власти и местного самоуправления.

Контрольные вопросы:

1. Назовите основные принципы обеспечения права на доступ к информации.
2. Приведите основные формы реализации конституционного права граждан на доступ к информации.
3. Перечислите законодательно установленные способы обеспечения доступа к информации о деятельности государственных и органов местного самоуправления.
4. Перечислите основное содержание информации о деятельности государственных и органов местного самоуправления в Интернете.

Список источников и литературы:

Источники:

Конституция Российской Федерации (принята всенародным голосованием 12.12.1993), Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_28399/

Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_61798/

Закон Российской Федерации от 21.07.93 № 5485-1 “О государственной тайне”, Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_2481/

Федеральный закон от 29.07.2004 № 98-ФЗ «О коммерческой тайне», Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_48699/

Федеральный закон от 28.12.2010 №390-ФЗ «О безопасности», Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_108546/

Постановление Правительства Российской Федерации от 15.04.1995 № 333 «О лицензировании деятельности предприятий, учреждений и организаций по проведению работ, связанных с использованием сведений, составляющих государственную тайну, созданием средств защиты информации, а также с осуществлением мероприятий и (или) оказанием услуг по защите государственной тайны», Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_6387/

Основная литература:

Ельчанинова, Н.Б. Правовые основы защиты информации с ограниченным доступом : учебное пособие / Н.Б. Ельчанинова ; Южный федеральный университет. - Ростов-на-Дону - Таганрог : Издательство Южного федерального университета, 2017. - 76 с. - ISBN 978-5-9275-2501-0. - Текст : электронный. - URL: <https://new.znaniium.com/catalog/product/1021578>

Дополнительная литература:

Информационная безопасность предприятия: Учебное пособие / Гришина Н.В., - 2-е изд., доп - М.:Форум, НИЦ ИНФРА-М, 2016. - 240 с.: 60x90 1/16. - (Высшее образование: Бакалавриат) (Обложка. КБС) ISBN 978-5-00091-007-8 - Режим доступа: <http://znaniium.com/catalog/product/544554>

Практические занятия 2, тема 4. (2 часа). Закон РФ «Об информации, информационных технологиях и защите информации» как организационно-правовая основа регулирования правоотношений в информационной сфере

Вопросы для изучения и обсуждения:

1. Основные понятия, используемые в законе.
2. Принципы разделения информации на категории открытого и ограниченного доступа.
3. Порядок распространения информации или предоставления информации.
4. Порядок документирования информации.
5. Информационная система как объект правового регулирования.
6. Государственное регулирование в сфере применения информационных технологий. Государственные информационные системы.
7. Регулирование отношений в сфере защиты информации

Контрольные вопросы:

1. Раскройте на примерах содержание основных понятий, используемых в Законе – информация, конфиденциальность информации, предоставление и распространения информации.

2. Перечислите виды информации, относимой к категории ограниченного доступа, дайте им краткую характеристику.

3. Определите возможный порядок документирования и перечислите формы представления документированной информации.

4. Какие требования предусматривает государственный порядок распространения информации.

5. Перечислите основные признаки информационной системы как объекта правового регулирования.

6. Перечислите обязанности обладателя и пользователя информации, а также оператора информационной системы по защите информации ограниченного доступа.

Список источников и литературы:

Источники:

Гражданский кодекс Российской Федерации. Часть первая, от 30.11.1994 N 51-ФЗ
Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_5142/

Уголовный кодекс Российской Федерации от 13.06.1996 N 63-ФЗ, Режим доступа:
http://www.consultant.ru/document/cons_doc_LAW_10699/

Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Режим доступа:
http://www.consultant.ru/document/cons_doc_LAW_61798/

Практическое занятие 3, тема 5. (2 часа). Правовое обеспечение защиты информации с ограниченным доступом. Стандарты информационной безопасности

Вопросы для изучения и обсуждения:

1. Разновидности правовых режимов информации.
2. Основные законодательно определенные виды информации ограниченного доступа.

3. Меры и средства, используемые для защиты информации с ограниченным доступом.

4. Основные положения Закона РФ «О техническом регулировании» в части стандартизации.

5. Основные положения действующих стандартов РФ в области информационной безопасности и защиты информации.

Контрольные вопросы:

1. Перечислите основные законодательно определенные виды информации ограниченного доступа и дайте им краткую характеристику.

2. Перечислите меры и средства, используемые в рамках известных видов защиты информации (правовой, организационной, инженерно-технической и программно-аппаратной) с целью обеспечения информационной безопасности организации любой формы собственности.

3. Понятие стандартизация, цели стандартизации и виды стандартов.

4. Основные положения стандарта ГОСТ Р 50922-2006. Защита информации. Основные термины и определения. Госстандарт России.

5. Основные положения стандарта ГОСТ Р ИСО/МЭК 17799-2005. Информационная технология. Методы и средства обеспечения безопасности. Практические правила управления информационной безопасностью.

6. Основные положения стандарта ГОСТ Р ИСО/МЭК 27001-2006. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования.

Список источников и литературы:

Источники:

Федеральный закон от 27.12.2002 № 184-ФЗ «О техническом регулировании», Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_40241/

Указ Президента Российской Федерации от 06.03.97 № 188 “Об утверждении перечня сведений конфиденциального характера”, Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_13532/

Постановление Правительства Российской Федерации от 03.11.94 № 1233 «Об утверждении Положения о порядке обращения со служебной информацией ограниченного распространения в федеральных органах исполнительной власти», Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_54870/

Федеральный закон от 09.02.2009 N 8-ФЗ "Об обеспечении доступа к информации о деятельности государственных органов и органов местного самоуправления" Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_84602/

ГОСТ Р ИСО/МЭК 17799-2005 "Информационная технология. Практические правила управления информационной безопасностью" (утв. Приказом Ростехрегулирования от 29.12.2005 N 447-ст), Режим доступа: <http://www.consultant.ru/cons/cgi/online.cgi?req=doc;base=EXP;n=447600#0139214174807645>

ГОСТ Р 50922-2006. Защита информации. Основные термины и определения. (утв. Приказом Ростехрегулирования от 27.12.2006 N 373-ст), Режим доступа: <http://www.consultant.ru/cons/cgi/online.cgi?req=doc;base=EXP;n=418509#08480021357350149>

Основная литература:

Организационно-правовое обеспечение информационной безопасности : [учеб. пособие] / [А. А. Стрельцов и др.] ; под ред. А. А. Стрельцова. - М.: Академия, 2008. – С. 72-82; С. 83-92; С. 116-125; С. 153-165.

Дополнительная литература:

Государственная тайна и ее защита в Российской Федерации: учеб. пособие для студентов вузов / П. П. Аникин [и др.]; под общ. ред.: М. А. Вуса и А. В. Федорова. – 3-е изд., испр. и доп. – СПб.: Юрид. центр Пресс, 2007. – 745с.

Практическое занятие 4, тема 6 (2 часа). Тайна как правовой режим ограничения доступа к информации – государственная тайна (далее ГТ)

Вопросы для изучения и обсуждения:

1. Сфера действия ФЗ РФ «О государственной тайне» (далее Закон) и основные понятия Закона.
2. Понятие о перечнях сведений, составляющих ГТ и степени секретности сведений.
3. Порядок отнесения сведений к ГТ и принципы их засекречивания. Сведения, не подлежащие засекречиванию.
4. Порядок рассекречивания сведений и их носителей.
5. Распоряжение сведениями, составляющими ГТ.
6. Иерархия органов защиты ГТ.
7. Порядок допуска должностных лиц и граждан к ГТ, основания для отказа в допуске и условия прекращения допуска.
8. Лицензирование деятельности, связанной с использованием ГТ, как обязательное условие допуска предприятий, учреждений и организаций к проведению работ, связанных с использованием сведений, составляющих ГТ.
9. Ответственность за нарушение законодательства РФ о ГТ.

Контрольные вопросы:

1. Определение понятия «государственная тайна» (ГТ). Сфера действия закона РФ «О ГТ». Объект правоотношений на ГТ. Субъекты правоотношений в области ГТ.

Принципы отнесения сведений к государственной тайне (ГТ) и засекречивания этих сведений.

2. Понятие о перечнях сведений, составляющих государственную тайну (ГТ). Основной критерий выбора степени секретности. Порядок рассекречивания сведений, относящихся к государственной тайне. Понятие о комиссионном порядке рассекречивания.

3. Иерархия органов защиты государственной тайны и их основные функции. Порядок допуска организаций к проведению работ, связанных с использованием информации, составляющей государственную тайну.

4. Основные права государства в отношении сведений, относящихся к категории государственной тайны.

5. Порядок допуска должностных лиц и граждан к сведениям, составляющим государственную тайну. Основания для отказа в получении допуска. Формы допусков в соответствии с грифами сведений.

6. Разница между понятиями «допуск» и «доступ» должностного лица или гражданина к сведениям, составляющим государственную тайну. Конкретный порядок организации доступа работника к секретным документам.

7. Ответственность за нарушение законодательства о государственной тайне.

Список источников и литературы:

Источники:

Гражданский кодекс Российской Федерации. Часть первая, от 30.11.1994 N 51-ФЗ
Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_5142/

Уголовный кодекс Российской Федерации от 13.06.1996 N 63-ФЗ, Режим доступа:
http://www.consultant.ru/document/cons_doc_LAW_10699/

Закон Российской Федерации от 21.07.93 № 5485-1 “О государственной тайне”,
Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_2481/

Федеральный закон от 29.07.2004 № 98-ФЗ «О коммерческой тайне», Режим
доступа: http://www.consultant.ru/document/cons_doc_LAW_48699/

Федеральный закон от 27.07.2006 N 152-ФЗ «О персональных данных», Режим
доступа: http://www.consultant.ru/document/cons_doc_LAW_61801/

Указ Президента Российской Федерации от 06.03.97 № 188 “Об утверждении
перечня сведений конфиденциального характера”, Режим доступа:
http://www.consultant.ru/document/cons_doc_LAW_13532/

Основная литература:

Ельчанинова, Н.Б. Правовые основы защиты информации с ограниченным доступом: учебное пособие / Н.Б. Ельчанинова ; Южный федеральный университет. - Ростов-на-Дону - Таганрог : Издательство Южного федерального университета, 2017. - 76 с. - ISBN 978-5-9275-2501-0. - Текст : электронный. - URL: <https://new.znaniium.com/catalog/product/1021578>

Правовое обеспечение информационной безопасности: Учебник / [авт.-ред. В. А. Минаев и др.]. – Изд. 2-е, расширенное и доп. – М.: Маросейка, 2008. – С. 120-124.

Дополнительная литература:

Организационно-правовое обеспечение информационной безопасности : [учеб. пособие] / [А. А. Стрельцов и др.] ; под ред. А. А. Стрельцова. - М.: Академия, 2008. – С. 126-141.

Государственная тайна и ее защита в Российской Федерации: учеб. пособие для студентов вузов / П. П. Аникин [и др.]; под общ. ред.: М. А. Вуса и А. В. Федорова. – 3-е изд., испр. и доп. – СПб.: Юрид. центр Пресс, 2007. – 745с.

Практическое занятие 5, тема 7 (2 часа). Правовое регулирование отношений в сфере обращения информации о персональных данных граждан (далее ПДн)

Вопросы для изучения и обсуждения:

1. Общие положения и основные понятия, используемые в Законе РФ «О персональных данных».
2. Принципы и условия обработки ПДн.
3. Классификация ПДн – общедоступные, специальные, биометрические.
4. Основные права субъекта ПДн.
5. Основные обязанности оператора ПДн.
6. Государственный контроль и надзор за обработкой ПДн, ответственность за нарушение требований законодательства о ПДн.
7. Понятие информационной системы обработки ПДн.

Контрольные вопросы:

1. Определите разницу между понятиями «неприкосновенность частной жизни» и «персональные данные» как объектов права.
2. Конфиденциальность ПДн как основной принцип их обработки.
3. Определите разницу между понятиями «обработка ПДн» и «оборот ПДн».
4. Перечислите права субъекта на получение информации, касающейся обработки его ПДн и возможные случаи ограничения этих прав.
5. Перечислите меры по обеспечению безопасности ПДн, принимаемые оператором ПДн при их обработке.

6. Порядок уведомления оператором органа по защите прав субъектов ПДн о намерении их обработки, и случаи законодательно установленного права оператора на обработку ПДн без такого уведомления.

7. Принципы классификации информационных систем обработки ПДн.

Список источников и литературы:

Источники:

Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_61798/

Федеральный закон от 04.05.2011 № 99-ФЗ «О лицензировании отдельных видов деятельности», Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_113658/

Федеральный закон от 27.07.2006 N 152-ФЗ «О персональных данных», Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_61801/

Федеральный закон от 27.12.2002 № 184-ФЗ «О техническом регулировании», Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_40241/

Указ Президента Российской Федерации от 06.03.97 № 188 “Об утверждении перечня сведений конфиденциального характера”, Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_13532/

Постановление Правительства РФ от 26.06.1995 N 608 (ред. от 21.04.2010) "О сертификации средств защиты информации" Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_7054/

Дополнительная литература:

Организационно-правовое обеспечение информационной безопасности : [учеб. пособие] / [А. А. Стрельцов и др.] ; под ред. А. А. Стрельцова. - М.: Академия, 2008. – С. 83-92.

Практическое занятие 6, тема 8 (2 часа). Правовое регулирование лицензионной деятельности в области защиты информации

Вопросы для изучения и обсуждения:

1. Лицензирование предпринимательской деятельности: достоинства и недостатки
1. Сфера применения закона РФ «О лицензировании отдельных видов деятельности» и основные понятия этого Закона.
2. Общие правовые принципы осуществления лицензионной деятельности.
3. Лицензирования деятельности в области защиты информации как необходимое условие обеспечения информационной безопасности.
4. Ответственность за нарушение условий, предусмотренных лицензией на осуществление деятельности в области защиты информации.

Контрольные вопросы:

1. Перечислите органы исполнительной власти, уполномоченные лицензировать деятельность в области технической защиты, а также в области разработки и производства средств защиты конфиденциальной информации.

2. Перечислите виды работ и услуг по технической защите конфиденциальной информации, осуществляемых юридическими лицами и индивидуальными предпринимателями и подлежащих лицензированию.

3. Перечислите виды работ, выполняемых юридическими лицами и индивидуальными предпринимателями при разработке и (или) производству средств защиты конфиденциальной информации и подлежащих лицензированию.

Список источников и литературы:

Источники:

Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_61798/

Федеральный закон от 04.05.2011 № 99-ФЗ «О лицензировании отдельных видов деятельности», Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_113658/

Постановление Правительства Российской Федерации от 15.04.1995 № 333 «О лицензировании деятельности предприятий, учреждений и организаций по проведению работ, связанных с использованием сведений, составляющих государственную тайну, созданием средств защиты информации, а также с осуществлением мероприятий и (или) оказанием услуг по защите государственной тайны», Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_6387/

Основная литература:

Ельчанинова, Н.Б. Правовые основы защиты информации с ограниченным доступом: учебное пособие / Н.Б. Ельчанинова ; Южный федеральный университет. - Ростов-на-Дону - Таганрог : Издательство Южного федерального университета, 2017. - 76 с. - ISBN 978-5-9275-2501-0. - Текст : электронный. - URL: <https://new.znaniium.com/catalog/product/1021578>

Дополнительная литература

Информационная безопасность предприятия: Учебное пособие / Гришина Н.В., - 2-е изд., доп - М.:Форум, НИЦ ИНФРА-М, 2016. - 240 с.: 60x90 1/16. - (Высшее образование: Бакалавриат) (Обложка. КБС) ISBN 978-5-00091-007-8 - Режим доступа: <http://znaniium.com/catalog/product/544554>

Государственная тайна и ее защита в Российской Федерации: учеб. пособие для студентов вузов / П. П. Аникин [и др.]; под общ. ред.: М. А. Вуса и А. В. Федорова. – 3-е изд., испр. и доп. – СПб.: Юрид. центр Пресс, 2007. – 745с.

10. Методические рекомендации по организации самостоятельной работы

Трудоемкость освоения дисциплины «Правовое обеспечение информационной безопасности» составляет 76 часов, из них 36 часов отведены на самостоятельную работу студента (СР).

Вид работы	Содержание (перечень вопросов)	СР (в часах)	Рекомендации
Тема 2. Право на информацию. Право на доступ к информации			
Подготовка к практическому занятию 1.	См. содержание темы в разделе 3 и план практического занятия 1 в разделе 9 РПД.	2	См. конспект лекции по теме 2 и план практического занятия 1 в разделе 9. Следует обратить внимание на основные формы реализации конституционного права граждан на доступ к информации.
Тема 4. Закон «Об информации...» как организационно-правовая основа регулирования правоотношений в информационной сфере			
Подготовка к практическому занятию 2.	См. содержание темы в разделе 3 и планы практического занятия 2 в разделе 9 РПД.	2	См. конспект лекции по теме 4 и планы практического занятия 2 в разделе 9. Следует обратить внимание на принципы разделения информации по категориям открытого и ограниченного доступа при проведении практического занятия 2 и на особенности информационных систем как объектов правового регулирования при проведении практического занятия 2.
Тема 5. Правовое обеспечение защиты документированной информации с ограниченным доступом. Стандарты информационной безопасности			
Подготовка к практическому занятию 3.	См. содержание темы в разделе 3 и планы практического занятия 3 в разделе 9 РПД.	4	См. конспект лекции по теме 5 и планы практического занятия 3 в разделе 9. Следует обратить внимание на перечень мер и средств, используемых для защиты информации с ограниченным доступом на практическом занятии 3 и на основные положения действующих стандартов РФ в области информационной безопасности и защиты информации при проведении практического занятия 3.
Тема 6. Тайна как правовой режим ограничения доступа к информации – государственная тайна (ГТ), служебная тайна (СТ), коммерческая тайна (КТ), профессиональные тайны (ПрТ)			
Подготовка к тестированию и практическому занятию 4	См. содержание темы в разделе 3 и планы практического занятия 4 в разделе 9 РПД.	16	См. конспекты лекций по теме 6 и планы практического занятия 4 в разделе 9. Следует обратить внимание: - на практику использования перечней сведений, составляющих ГТ, принципы засекречивания сведений,

Вид работы	Содержание (перечень вопросов)	СР (в часах)	Рекомендации
			<p>иерархии органов защиты ГТ и основные права государства в отношении сведений, относящихся к ГТ - при проведении практического занятия 4;</p> <p>- на понятие СТ, признаки, необходимые для отнесения информации к СТ и общие положения о порядке обращения со служебной информацией ограниченного распространения в федеральных органах исполнительной власти - при проведении практического занятия 4;</p> <p>- на общий порядок охраны конфиденциальности информации, относимой к КТ, в том числе в рамках трудовых отношений, и на виды ответственности за нарушение законодательства о КТ - при проведении практического занятия 4;</p> <p>- на требования к информации для возможности ее отнесения к профессиональной тайне, на основные субъекты правоотношений в области профессиональных тайн – при проведении практического занятия 4;</p> <p>- на понятие «банковская тайна», как одного из видов профессиональных тайн и на место банковской тайны в числе иных видов информации ограниченного доступа в массиве информации, которая накапливается, хранится и используется в банковской деятельности - при проведении практического занятия 4.</p>
Тема 7. Правовое регулирование отношений в сфере обращения информации о персональных данных граждан (ПДн)			
Подготовка к практического занятия 5.	См. содержание темы в разделе 3 и планы практического занятия 5 в разделе 9 РПД.	6	<p>См. конспект лекции по теме 7 и планы практического занятия 5 в разделе 9. Следует обратить внимание:</p> <p>- на классификацию ПДн, права субъекта ПДн и обязанности оператора ПДн – при проведении практического занятия 5;</p> <p>- на Государственный контроль и</p>

Вид работы	Содержание (перечень вопросов)	СР (в часах)	Рекомендации
			надзор за обработкой ПДн и ответственность за нарушение требований законодательства о ПДн, а также на понятие информационной системы обработки ПДн – при проведении практического занятия 5.
Тема 8. Правовые особенности сертификации средств защиты информации и правовое регулирование лицензионной деятельности в области защиты информации			
Подготовка к практического занятия 6 и самостоятельно й работе	См. содержание темы в разделе 3, планы практического занятия 6 в разделе 9 РПД и примерное содержание практической работы по теме 8 в разделе 6 РПД.	4	См. конспект лекций по теме 8, примерное задание для выполнения практической работы по теме 8 в разделе 6. Следует обратить внимание: - на лицензирование деятельности в области защиты информации, как необходимое условие обеспечения информационной безопасности, и ответственность за нарушение условий, предусмотренных лицензией на осуществление деятельности в области защиты информации - при проведении практического занятия 2; - на особенностях системы сертификации средств защиты информации, ее участниках и их обязанностях в рамках деятельности по сертификации средств защиты информации – при проведении практического занятия 2, 3
Промежуточная аттестация (зачет с оценкой)			
Подготовка к ответу на вопросы заданий	См. цели и задачи дисциплины в разделе 1 и содержание дисциплины в разделе 3 РПД.	8	См. конспекты лекции по дисциплине, примерные контрольные вопросы по курсу в разделе 6 и список источников и литературы в разделе 6 РПД.
Итого		44	

АННОТАЦИЯ ДИСЦИПЛИНЫ

Дисциплина «Правовое обеспечение информационной безопасности» реализует в соответствии с требованиями федерального государственного образовательного стандарта высшего образования по направлению подготовки 10.03.01 «Информационная безопасность» (квалификация (степень) «бакалавр»), утвержденного и введенного в действие приказом Министерства образования и науки РФ от 01 декабря 2016 г. № 1515.

Дисциплина «Правовое обеспечение информационной безопасности» входит в базовую часть цикла дисциплин подготовки студентов по направлению подготовки 10.03.01 «Информационная безопасность».

Дисциплина реализуется на факультете информационных систем и безопасности кафедрой информационной безопасности Института информационных наук и технологий безопасности.

Содержание курса дисциплины «Правовое обеспечение информационной безопасности» охватывает круг вопросов, связанных с целями, функциями и структурой государственной системы правового регулирования в области информационной безопасности личности, общества и государства, правовым обеспечением информационной безопасности при использовании мер и средств организационно-правовой защиты информации, структурой законодательства по правовому обеспечению информационной безопасности, а также порядком сертификации средств защиты информации и правовому регулированию лицензионной деятельности в области защиты информации. Рассматривается понятие тайны как правового режима ограничения доступа к информации, в том числе правовые режимы государственной тайны, коммерческой тайны, служебной тайны, различных видов профессиональных тайн, а также особенности правового регулирования отношений в сфере обращения информации о персональных данных граждан.

Цель курса: сформировать взгляд на правовое обеспечение информационной безопасности как на системную научно-практическую деятельность, одну из основ которой составляет работа по нормативно-правовому обеспечению информационной безопасности.

Задачи курса:

- изучить конституционные гарантии прав граждан на доступ к информации, в том числе права свободно искать, получать, передавать, производить и распространять

информацию любым законным способом с учетом особенностей реализации этих прав в отношении информации ограниченного доступа;

- освоить основы правового регулирования отношений в информационной сфере, меры и средства организационно-правового обеспечения информационной безопасности и защиты информации ограниченного доступа, в том числе основополагающие государственные стандарты РФ в области информационной безопасности и защиты информации;

- рассмотреть понятие тайны как правового режима ограничения доступа к информации, в том числе правового режима государственной тайны и иных видов тайн, особенности правового регулирования отношений в сфере обращения информации о персональных данных граждан;

- изучить правовые основы и порядок сертификации средств защиты информации и практику правового регулирования лицензионной деятельности в области информационной безопасности и защиты информации ограниченного доступа.

Дисциплина направлена на формирование следующих компетенций:

- УК-2 - Способен определять круг задач в рамках поставленной цели и выбирать оптимальные способы их решения, исходя из действующих правовых норм, имеющихся ресурсов и ограничений

В результате освоения дисциплины обучающийся должен:

- Уметь анализировать имеющиеся ресурсы и ограничения, оценивать и выбирать оптимальные способы решения поставленных задач
- Уметь использовать знаний о важнейших нормах, институтах и отраслях действующего российского права для определения круга задач и оптимальных способов их решения.
- УК-10 - Способен формировать нетерпимое отношение к коррупционному поведению

В результате освоения дисциплины обучающийся должен:

- Знает сущность коррупционного поведения и его взаимосвязь с социальными, экономическими, политическими и иными условиями
- Умеет анализировать, толковать и правильно применять правовые нормы о противодействии коррупционному поведению
- Владеет навыками работы с законодательными и другими нормативными правовыми актами
- ОПК-5 - Способен применять нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации в сфере профессиональной деятельности;

В результате освоения дисциплины обучающийся должен:

- Уметь применять нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации в сфере профессиональной деятельности
- Уметь обосновывать решения, связанные с реализацией правовых норм по защите информации в пределах должностных обязанностей, предпринимать необходимые меры по восстановлению нарушенных прав
- Владеть навыками разрабатывать проекты локальных правовых документов, регламентирующих работу по обеспечению информационной безопасности в организации
- ОПК-6 - Способен при решении профессиональных задач организовывать защиту информации ограниченного доступа в соответствии с нормативными правовыми актами, нормативными и методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю;

В результате освоения дисциплины обучающийся должен:

- Знать нормативные, руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации
- Умеет разрабатывать проекты локальных нормативных документов, регламентирующих защиту информации ограниченного доступа в организации
- Владеет навыками по разработке политики безопасности объекта информатизации

Рабочей программой предусмотрены следующие виды контроля: текущий контроль успеваемости в форме тестирования, промежуточная аттестация в форме зачета с оценкой

Общая трудоемкость освоения дисциплины составляет 2 зачетные единицы.