

Сибирский институт управления – филиал РАНХиГС
Кафедра конституционного и муниципального права

УТВЕРЖДЕНА
кафедрой конституционного и муницип-
ального права
протокол от 24.12.2021 №6

**РАБОЧАЯ ПРОГРАММА
ДИСЦИПЛИНЫ**

**ПРАВОВОЕ ОБЕСПЕЧЕНИЕ
ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ**
(Б1.В.ДВ.06.02)
краткое наименование дисциплины – ПО ИБ

По специальности 40.05.01 Правовое обеспечение национальной
безопасности
специализация: «Гражданско-правовая»
квалификация выпускника: Юрист

формы обучения: очная, заочная

Год набора – 2021

Новосибирск, 2021

Авторы – составители:

Канд. юрид. наук, доцент кафедры конституционного и муниципального права

Раздьяконова Евгения Владимировна ;

Старший преподаватель кафедры конституционного и муниципального права

Дробот Семен Евгеньевич

Заведующий кафедрой конституционного и муниципального права

Е.В. Раздьяконова

СОДЕРЖАНИЕ

1. Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения образовательной программы	4
2. Объем и место дисциплины в структуре ОП ВО	9
3. Содержание и структура дисциплины	10
4. Материалы текущего контроля успеваемости обучающихся и фонд оценочных средств промежуточной аттестации по дисциплине	16
4.1. Формы и методы текущего контроля успеваемости и промежуточной аттестации.	16
4.2. Материалы текущего контроля успеваемости.	17
4.3. Оценочные средства промежуточной аттестации.	22
4.4. Методические материалы промежуточной аттестации.	33
5. Методические указания для обучающихся по освоению дисциплины	33
6. Учебная литература и ресурсы информационно-телекоммуникационной сети "Интернет", включая перечень учебно-методическое обеспечение для самостоятельной работы обучающихся по дисциплине	35
6.1. Основная литература.	35
6.2. Дополнительная литература.	35
6.3. Учебно-методическое обеспечение самостоятельной работы.	35
6.4. Нормативные правовые документы	35
6.5. Интернет-ресурсы.	36
6.6. Иные источники.	36
7. Материально – техническая база, информационные технологии, программное обеспечение и информационные справочные системы	36

1. Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения образовательной программы

1.1. Дисциплина Б1.В.ДВ.06.02 «Правовое обеспечение информационной безопасности» обеспечивает овладение следующими компетенциями с учетом этапа:

Таблица 1.

Код компетенции	Наименование компетенции	Код этапа освоения компетенции	Наименование этапа освоения компетенции
ПКо-ОС 4	Способен использовать современные технологии и методики противодействия угрозам национальной безопасности.	Очная форма обучения –	<p>ПКо ОС – 4.1</p> <p>Способен определить, оценить и проанализировать угрозы национальной безопасности ПКо ОС - 4.2</p> <p>Способен на определение комплекса мер по противодействию угрозам национальной безопасности, включая современные технологии и методики ПКо ОС - 4.3</p> <p>Способен организовать и обеспечить реализацию комплекса мер по противодействию угрозам национальной безопасности ПКо ОС - 4.4</p> <p>Способен применить технические средства и методики в профессиональной, в том числе служебной деятельности на противодействие угрозам национальной безопасности ПКо ОС - 4.5</p> <p>Способен оценить эффективность современных технологий и методик по противодействию угрозам национальной безопасности</p>
		Заочная форма обучения -	<p>ПКо ОС – 4.1</p> <p>Способен определить, оценить и проанализировать угрозы национальной безопасности ПКо ОС - 4.2</p> <p>Способен на определение комплекса мер по противодействию угрозам национальной безопасности, включая современные технологии и методики ПКо ОС - 4.3</p> <p>Способен организовать и обеспечить реализацию комплекса мер по противодействию угрозам национальной безопасности ПКо ОС - 4.4</p> <p>Способен разрабатывать методики по противодействию угрозам национальной безопасно-</p>

			<p>сти. ПКо ОС - 4.5</p> <p>Способен применить технические средства и методики в профессиональной, в том числе служебной деятельности на противодействие угрозам национальной безопасности ПКо ОС - 4.6</p> <p>Способен оценить эффективность современных технологий и методик по противодействию угрозам национальной безопасности</p>
		<p>Заочная форма обучения с применением электронного обучения и дистанционных образовательных технологий¹</p>	<p>ПКо ОС – 4.1</p> <p>Способен определить, оценить и проанализировать угрозы национальной безопасности ПКо ОС - 4.2</p> <p>Способен на определение комплекса мер по противодействию угрозам национальной безопасности, включая современные технологии и методики ПКо ОС - 4.3</p> <p>Способен организовать и обеспечить реализацию комплекса мер по противодействию угрозам национальной безопасности ПКо ОС - 4.4</p> <p>Способен разрабатывать методики по противодействию угрозам национальной безопасности. ПКо ОС - 4.5</p> <p>Способен применить технические средства и методики в профессиональной, в том числе служебной деятельности на противодействие угрозам национальной безопасности ПКо ОС - 4.6</p> <p>Способен оценить эффективность современных технологий и методик по противодействию угрозам национальной безопасности</p>
ПКс-3	Способен использовать специальные познания при представлении в суде интересов лиц, органов и организаций.	Очная форма обучения –	<p>ПКс – 3.1</p> <p>Способен осуществлять коммуникацию в устной и письменной формах на государственном языке, иностранном языке (ах) в различных сферах профессиональной деятельности юриста ПКс – 3.2</p> <p>Способен применять нормативные правовые акты, реализовывать нормы материального и процессуального права в профессиональной</p>

¹ Далее по тексту – ЭО и ДОТ

			<p>деятельности. ПКс – 3.3 Способен правильно и полно отражать результаты профессиональной деятельности в юридической и иной документации ПКс – 3.4 Способен применять нормативные правовые акты, реализовывать нормы материального и процессуального права в профессиональной деятельности. ПКс – 3.5 Владение навыками подготовки юридических документов.</p>
		<p>Заочная форма обучения -</p>	<p>ПКс – 3.1 Способен осуществлять коммуникацию в устной и письменной формах на государственном языке, иностранном языке (ах) в различных сферах профессиональной деятельности юриста ПКс – 3.2 Способен применять нормативные правовые акты ПКс – 3.3 Способен реализовывать нормы материального и процессуального права в профессиональной деятельности. ПКс – 3.4 Способен правильно и полно отражать результаты профессиональной деятельности в юридической и иной документации ПКс – 3.5 Способен применять нормативные правовые акты в профессиональной деятельности. ПКс – 3.6 Способен реализовывать нормы материального и процессуального права в профессиональной деятельности. ПКс – 3.7 Владение навыками подготовки юридических документов.</p>
		<p>Заочная форма обучения с применением электронного обучения и дистанционных образовательных технологий</p>	<p>ПКс – 3.1 Способен осуществлять коммуникацию в устной и письменной формах на государственном языке, иностранном языке (ах) в различных сферах профессиональной деятельности юриста ПКс – 3.2 Способен применять нормативные правовые акты</p>

			<p>ПКс – 3.3 Способен реализовывать нормы материального и процессуального права в профессиональной деятельности.</p> <p>ПКс – 3.4 Способен правильно и полно отражать результаты профессиональной деятельности в юридической и иной документации</p> <p>ПКс – 3.5 Способен применять нормативные правовые акты в профессиональной деятельности.</p> <p>ПКс – 3.6 Способен реализовывать нормы материального и процессуального права в профессиональной деятельности.</p> <p>ПКс – 3.7 Владение навыками подготовки юридических документов.</p>
--	--	--	--

1.2. В результате освоения дисциплины у студентов должны быть сформированы:

Таблица 2.

Профессиональные действия	Код этапа освоения компетенции	Результаты обучения
способность соблюдать в профессиональной деятельности требования нормативных правовых актов в области защиты государственной тайны и информационной безопасности, обеспечивать соблюдение режима секретности	Очная форма обучения, заочная форма обучения, заочная форма обучения с применением электронного обучения и дистанционных образовательных технологий	<p>Знания:</p> <ul style="list-style-type: none"> - перечня сведений, составляющих государственную и иную охраняемую законом тайну; - порядка раскрытия информации, составляющей государственную и иную охраняемую законом тайну; - способов защиты государственной тайны и информационной безопасности в различных областях профессиональной деятельности <p>Умения:</p> <ul style="list-style-type: none"> - Определять применимые в конкретной ситуации способы реагирования на нарушение требований соблюдения режима секретности с учетом сферы деятельности - Формировать перечень необходимых мер по обеспечению соблюдения требований к сохранению тайны в профессиональной деятельности <p>Владения:</p> <ul style="list-style-type: none"> - Способами обеспечения выполнения в конкретной организации требований нормативных правовых актов, устанавливающих требования к защите государственной тайны и обеспечению информационной безопасности, а также соответствующих локальных нормативных актов - Навыками соблюдения требований правовых актов,

		направленных к охране государственной тайны и обеспечению информационной безопасности
--	--	---

2. Объем и место дисциплины в структуре ОП ВО

Объем дисциплины

Общая трудоемкость дисциплины в зачетных единицах: **3 З.Е.**

Количество академических часов, выделенных:

очная форма обучения

на контактную работу с преподавателем – 40 часов (16 часа лекций, 24 часов практических (семинарских) занятий);

на самостоятельную работу обучающихся – 68 часа.

Контроль –

заочная форма обучения

на контактную работу с преподавателем - 12 часов (4 часа лекций, 8 часов практических (семинарских) занятий);

на самостоятельную работу обучающихся – 87 часов.

Контроль - 9 ч.

заочная форма обучения с применением ЭО, ДОТ

на контактную работу с преподавателем - 12 часов (4 часа лекций, 8 часов практических (семинарских) занятий);

на самостоятельную работу обучающихся – 87 часов.

Контроль - 9 ч.

Место дисциплины –

Правовое обеспечение информационной безопасности входит в вариативную часть (дисциплины по выбору) учебного плана и изучается в течение седьмого семестра по очной и 6 курсе по заочной форме обучения.

Освоение дисциплины опирается на минимально необходимый объем теоретических знаний в области закономерностей развития общества, государства и права, методов и приемов критического мышления, а также методов работы с информацией.

Дисциплина реализуется после изучения дисциплин:

На очной форме обучения:

Б1.Б.09	Теория государства и права
---------	----------------------------

На заочной форме обучения:

Б1.Б.35.05	Право интеллектуальной собственности
Б1.Б.35.09	Наследственное право и нотариальная практика

На заочной форме обучения с применением ЭО, ДОТ:

Б1.Б.35.05	Право интеллектуальной собственности
Б1.Б.35.09	Наследственное право и нотариальная практика

3. Содержание и структура дисциплины

Таблица 3

№ п/п	Наименование тем, модулей (разделов)	Объем дисциплины, час.						Форма текущего контроля успеваемости, промежуточной аттестации
		Всего	Контактная работа обучающегося с преподавателем по видам учебных занятий				СР	
			л	лр	пз	ксп		
Очная форма обучения								
Тема 1	Информационная безопасность (ИБ) РФ и задачи по ее обеспечению.	8	1		1		6	О – 1; ПЗ-1
Тема 2	Нормативно-правовая база обеспечения ИБ в России.	7	1				6	О – 2; ПЗ-2
Тема 3	Информация как объект правового регулирования и защиты.	8	1		1		6	О – 3; ПЗ-3
Тема 4	Система субъектов обеспечения ИБ в России и их правовой статус.	9	1		1		7	О – 4; ПЗ-4
Тема 5	Преступность в информационной сфере и ее криминологическая и уголовно-правовая характеристика.	9	1		1		7	О – 5; ПЗ-5
Тема 6	Правовая защита личности в информационной сфере.	9	1		1		7	О – 6; ПЗ-6
Тема 7	Правовой режим государственной тайны и меры по ее обеспечению.	9	1		1		7	О – 7; ПЗ-7
Тема 8	Правовые и организационные способы защиты информации в сфере высоких технологий.	8	1		1		6	О – 8; ПЗ-8
Тема 9	Правовое обеспечение права интеллектуальной собственности (ПИС).	8	1		1		6	О – 9; ПЗ-9
Тема 10	Правовая защита коммерческой тайны (КТ).	9	1		1		7	О – 10; ПЗ-11
Тема 11	Правовое регулирование отношений в сфере лицензирования и сертификации.	8			1		7	О – 11; ПЗ-12
Тема 12	Предупреждение преступлений в информационной сфере в современной России.	8			1		7	О – 12; ПЗ-12
Тема 13	Юридическая ответственность за правонарушения в сфере ИБ.	8			1		7	О – 13; ПЗ-13

Промежуточная аттестация:							
зачёт							
Всего:	108	10		12		86	

Таблица 4

№ п/п	Наименование тем, модулей (разделов)	Объем дисциплины, час.						Форма текущего контроля успеваемости, промежуточной аттестации
		Всего	Контактная работа обучающегося с преподавателем по видам учебных занятий				СР	
			Л	ЛР	ПЗ	КСР		
Заочная форма обучения								
Тема 1	Информационная безопасность (ИБ) РФ и задачи по ее обеспечению.	8			1		7	О – 1; ПЗ-1
Тема 2	Нормативно-правовая база обеспечения ИБ в России.	8			1		7	О – 2; ПЗ-2
Тема 3	Информация как объект правового регулирования и защиты.	9	1		1		7	О – 3; ПЗ-3
Тема 4	Система субъектов обеспечения ИБ в России и их правовой статус.	9	1		1		7	О – 4; ПЗ-4
Тема 5	Преступность в информационной сфере и ее криминологическая и уголовно-правовая характеристика.	9	1		1		7	О – 5; ПЗ-5
Тема 6	Правовая защита личности в информационной сфере.	8			1		7	О – 6; ПЗ-6
Тема 7	Правовой режим государственной тайны и меры по ее обеспечению.	9	1		1		7	О – 7; ПЗ-7
Тема 8	Правовые и организационные способы защиты информации в сфере высоких технологий.	8			1		7	О – 8; ПЗ-8
Тема 9	Правовое обеспечение права интеллектуальной собственности (ПИС).	7					7	О – 9; ПЗ-9
Тема 10	Правовая защита коммерческой тайны (КТ).	7					7	О – 10; ПЗ-10
Тема 11	Правовое регулирование отношений в сфере лицензирования и	7					7	О – 11; ПЗ-11

	сертификации.							
Тема 12	Предупреждение преступлений в информационной сфере в современной России.	7					7	О – 12; ПЗ-12
Тема 13	Юридическая ответственность за правонарушения в сфере ИБ.	4					4	О – 13; ПЗ-13
Промежуточная аттестация: зачёт		9						
Всего:		108	4		8		87	

Таблица 5

№ п/п	Наименование тем, модулей (разделов)	Объем дисциплины, час.						Форма текущего контроля успеваемости, промежуточной аттестации
		Всего	Контактная работа обучающегося с преподавателем по видам учебных занятий				СР	
			Л	ЛР	ПЗ	КСР		
Заочная форма обучения с применением ЭО, ДОТ								
Тема 1	Информационная безопасность (ИБ) РФ и задачи по ее обеспечению.	8			1		7	О – 1; ПЗ-1
Тема 2	Нормативно-правовая база обеспечения ИБ в России.	8			1		7	О – 2; ПЗ-2
Тема 3	Информация как объект правового регулирования и защиты.	8	1		1		7	О – 3; ПЗ-3
Тема 4	Система субъектов обеспечения ИБ в России и их правовой статус.	8	1		1		7	О – 4; ПЗ-4
Тема 5	Преступность в информационной сфере и ее криминологическая и уголовно-правовая характеристика.	9	1		1		7	О – 5; ПЗ-5
Тема 6	Правовая защита личности в информационной сфере.	8			1		7	О – 6; ПЗ-6
Тема 7	Правовой режим государственной тайны и меры по ее обеспечению.	19	1		1		7	О – 7; ПЗ-7
Тема 8	Правовые и организационные способы защиты информации в сфере высоких технологий.	8			1		7	О – 8 ; ПЗ-8
Тема	Правовое обеспечение права ин-	7					7	О – 9;

9	теллектуальной собственности (ПИС).							ПЗ-9
Тема 10	Правовая защита коммерческой тайны (КТ).	7					7	О – 10; ПЗ-10
Тема 11	Правовое регулирование отношений в сфере лицензирования и сертификации.	7					7	О – 11; ПЗ-11
Тема 12	Предупреждение преступлений в информационной сфере в современной России.	7					7	О – 12; ПЗ-12
Тема 13	Юридическая ответственность за правонарушения в сфере ИБ.	4					4	О – 13; ПЗ-13
Промежуточная аттестация: зачёт		9						
Всего:		108	4		8		87	

Содержание дисциплины

Тема 1. Информационная безопасность (ИБ) РФ и задачи по ее обеспечению.

Понятие ИБ и информационного общества. Цели, задачи и принципы обеспечения ИБ. Угроза национальной безопасности и их виды. Информационные войны и информационное оружие. Информационный терроризм. Информационное общество в РФ и его характеристики. Информационная сфера и ее области. Национальные интересы России в информационной сфере. Государственная политика РФ в сфере обеспечения ИБ и ее принципы.

Тема 2. Нормативно-правовая база обеспечения ИБ в России.

Понятие правового обеспечения и правовой защиты. История формирования законодательства РФ об информации и ее защите. Система нормативно-правовых актов России, регулирующих отношения в сфере ИБ. Международно-правовые нормы и стандарты в сфере ИБ. Место Окинавской Хартии глобального информационного общества в системе международно-правовых актов обеспечения ИБ. Предмет и метод правового регулирования в сфере ИБ страны. Информационное право. Информационные отношения. Виды ведомственных и корпоративных норм и их место в системе правового регулирования ИБ в РФ. Правовое регулирование деятельности средств массовой информации. Основные тенденции развития законодательства РФ в сфере ИБ. Особенности стандартизации нормативной базы в сфере ИБ в современном мире.

Тема 3. Информация как объект правового регулирования и защиты.

Информация, ее виды и признаки. Информация как объект юридической защиты. Информационная сфера общества и ее характеристики. Информационные ресурсы. Понятие и виды. Виды и источники информации, подлежащие защите. Правовой режим защиты государственной тайны. Способы обеспечения сохранности информации, составляющей государственную тайну и система контроля за состоянием ее защиты. Основные принципы засекречивания информации. Конфиденциальная информация и возможные каналы ее утечки. Информационная инфраструктура и информационная среда. Их структура и характеристики. Международный опыт деятельности по правовому обеспечению ИБ и основные направления его развития. Государственная политика РФ в сфере правового обеспечения ИБ.

Тема 4. Система субъектов обеспечения ИБ в России и их правовой статус.

Понятие государственного управления в сфере обеспечения ИБ. Система органов государственной власти, обеспечивающая ИБ и особенности их компетентности. Правовой статус и система органов государственной власти, обеспечивающая право доступа к информации. Особенности правового статуса и организация работы органов государственной власти, обеспечивающих защиту информации, обрабатываемой техническими средствами. Служба Специальной связи и информации Федеральной службы охраны РФ, ее задачи и правовой статус.

Тема 5. Преступность в информационной сфере и ее криминологическая и уголовно-правовая характеристика.

Понятие и виды преступности в информационной сфере. Основные этапы и тенденции развития компьютерной преступности в России. Особенности детерминации преступлений, совершаемых в информационной сфере. Криминологическая и криминалистическая характеристики основных способов мошенничества, совершаемых с помощью сети Интернет. Понятие преступления в сфере компьютерной информации. Виды преступлений в сфере компьютерной информации. Уголовно-правовая характеристика преступлений в сфере компьютерной информации. Особенности объективных признаков компьютерных преступлений. Основные способы их совершения. Субъективные признаки компьютерных преступлений. Характерные мотивы и цели их совершения. Криминологическая и уголовно-правовая характеристика лиц, совершающих преступления в сфере компьютерной информации.

Тема 6. Правовая защита личности в информационной сфере.

Система и структура нормативных актов, обеспечивающих защиту прав личности в информационной сфере. Конституционные гарантии правовой охраны прав личности в информационной сфере. Правовые средства защиты права на доступ к информации и неприкосновенности частной жизни. Правовой механизм защиты права на неприкосновенность частной жизни. Врачебная тайна как институт защиты интересов личности. Защита права на личную информацию с ограниченным доступом. Персональная тайна и ее виды. Обработка и правовая охрана персональных данных. Правовая база обеспечения защиты личности от воздействия «вредной» информации. Российская и зарубежная модели обеспечения защиты личности от воздействия «вредной» информации.

Тема 7. Правовой режим государственной тайны и меры по ее обеспечению.

Понятие государственной тайны и правового режима ее обеспечения. Принципы и механизм отнесения сведений к государственной тайне (ГТ). Процедура засекречивания и рассекречивания сведений, составляющих государственную тайну. Субъекты обеспечения режима государственной тайны и их правовой статус. Организационно-правовые меры защиты ГТ. Допуск и доступ к ГТ. Обеспечение ИБ при международном обмене информацией. Система контроля за режимом обеспечения ГТ. Особенности юридической ответственности за нарушение режима обеспечения ГТ.

Тема 8. Правовые и организационные способы защиты информации в сфере высоких технологий.

Правовое обеспечение защиты информации, обрабатываемой вычислительной техникой и передаваемой по компьютерным цепям. Организационно-управленческие меры обеспечения защиты информации в сфере высоких технологий. Компьютерные преступления и особенности их идентификации и предупреждения. Правовые основы применения «электронной цифровой подписи» (ЭЦП). Криптографическая защита информации (КЗИ). Правовые и организационные способы обеспечения КЗИ в России и других странах современного мира. Контроль за разработкой, производством и применением криптографических средств. КЗИ и их правовая основа. Органы лицензирования и сертификации и их правовой статус.

Тема 9. Правовое обеспечение права интеллектуальной собственности (ПИС).

Понятие интеллектуальной собственности и ее правовой статус. Законодательство РФ об авторских и смежных правах. Особенности правоотношений, обеспечивающих ПИС. Объекты и субъекты ПИС. Правовой механизм обеспечения защиты авторских и смежных прав.

Государственная регистрация ПИС. Особенности правовой защиты программ для электронных вычислительных машин и баз данных. Патентное право и патентные правоотношения. Правовой статус участников. Сфера действия патентного законодательства. Показатели и условия патентоспособности. Правовой статус автора и патентообладателя. Механизм правовой защиты прав автора и патентообладателей. Товарный знак и механизм его правовой защиты. Государственная регистрация товарного знака. Прекращение права на товарный знак. Программы для ЭВМ и механизм их правовой защиты. Правовое регулирование договорных отношений в сфере ПИС.

Тема 10. Правовая защита коммерческой тайны (КТ).

Понятие КТ и ее правовой статус. Признаки КТ. Защита КТ и патентование как способы правового закрепления права собственности на промышленный образец и полезную модель. Объекты защиты КТ. Особенности правового обеспечения режима КТ. Промышленный шпионаж и его объекты. Критерии определения секретности при определении режима КТ. Организационные меры обеспечения защиты КТ и особенности их реализации в рамках гражданско-правовых (договорных) и трудовых отношений. Режим представления информации, составляющей КТ органам государственной власти. Юридическая ответственность за нарушение режима обеспечения КТ.

Тема 11. Правовое регулирование отношений в сфере лицензирования и сертификации.

Правовое обеспечение деятельности организаций по лицензированию и сертификации в сфере ИБ. Понятие лицензирования по российскому законодательству. Виды деятельности, подлежащие лицензированию в сфере ИБ. Система государственного лицензирования в сфере ИБ и ее функции. Субъекты лицензирования в сфере ИБ и их правовой статус. Порядок лицензирования, приостановления или аннулирования действия лицензии. Специальная экспертиза предприятия и государственная аттестация их руководителей. Контроль за условиями обеспечения ИБ лицензиатами. Понятие сертификации средств защиты информации (ССЗИ) и ее правовая основа в РФ. Цели создания системы ССЗИ. Организационная структура системы ССЗИ и особенности правового статуса ее субъектов. Объекты сертификационной деятельности и режимы сертификации. Особенности аттестации и контроля за деятельностью объектов обработки особо важной информации. Юридическая ответственность за нарушением правил лицензирования и сертификации.

Тема 12. Предупреждение преступлений в информационной сфере в современной России.

Информационная безопасность России и задачи по ее обеспечению. Система детерминант преступности в информационной сфере. Уровневый подход. Мотивационная сфера лиц, совершающих правонарушения в сфере ИБ. Субъекты деятельности по обеспечению противодействия правонарушениям в сфере ИБ и их правовой статус. Оперативно-розыскные и криминалистические мероприятия по борьбе с преступлениями в сфере ИБ. Особенности расследования преступлений в сфере ИБ. Совершенствование правовых норм как средство обеспечения профилактического воздействия на отношения в сфере ИБ. Зарубежный опыт борьбы с преступностью в сфере ИБ.

Тема 13. Юридическая ответственность за правонарушения в сфере ИБ.

Понятие и виды юридической ответственности (ЮО) за правонарушения в сфере ИБ. Уголовная ответственность за правонарушения в сфере ИБ и ее особенности. Объективные и субъективные признаки составов преступлений, посягающих на ИБ страны. Уголовная ответственность за компьютерные преступления и особенности их реализации в современной России. Правовое регулирование отношений, связанных с привлечением к ответственности лиц, совершивших административные правонарушения в сфере ИБ. Составы административных правонарушений, посягающих на ИБ страны. Органы государственной власти и должностные лица, уполномоченные рассматривать административные правонарушения в сфере защиты информации и их правовой статус.

4. Материалы текущего контроля успеваемости обучающихся и фонд оценочных средств промежуточной аттестации по дисциплине

4.1. Формы и методы текущего контроля успеваемости обучающихся и промежуточной аттестации.

4.1.1. В ходе реализации дисциплины Б.1.В.ДВ. 05. 02 «Правовое обеспечение информационной безопасности» используются следующие методы текущего контроля успеваемости обучающихся:

Таблица 6.

Для проведения занятий по очной, заочной формам обучения

№ п/п	тема (раздел)	Методы текущего контроля успеваемости
Тема 1	Информационная безопасность (ИБ) РФ и задачи по ее обеспечению.	Устный/письменный ответ на вопросы
Тема 2	Нормативно-правовая база обеспечения ИБ в России.	Устный/письменный ответ на вопросы
Тема 3	Информация как объект правового регулирования и защиты.	Устный/письменный ответ на вопросы
Тема 4	Система субъектов обеспечения ИБ в России и их правовой статус.	Устный/письменный ответ на вопросы
Тема 5	Преступность в информационной сфере и ее криминологическая и уголовно-правовая характеристика.	Устный/письменный ответ на вопросы
Тема 6	Правовая защита личности в информационной сфере.	Устный/письменный ответ на вопросы
Тема 7	Правовой режим государственной тайны и меры по ее обеспечению.	Устный/письменный ответ на вопросы
Тема 8	Правовые и организационные способы защиты информации в сфере высоких технологий.	Устный/письменный ответ на вопросы
Тема 9	Правовое обеспечение права интеллектуальной собственности (ПИС).	Устный/письменный ответ на вопросы
Тема 10	Правовая защита коммерческой тайны (КТ).	Устный/письменный ответ на вопросы
Тема 11	Правовое регулирование отношений в сфере лицензирования и сертификации.	Устный/письменный ответ на вопросы
Тема 12	Предупреждение преступлений в информационной сфере в современной России.	Устный/письменный ответ на вопросы
Тема 13	Юридическая ответственность за правонарушения в сфере ИБ.	Устный/письменный ответ на вопросы

Таблица 7.

Для проведения занятий по заочной форме обучения с применением ЭО, ДОТ

№ п/п	тема (раздел)	Методы текущего контроля успеваемости
Тема 1	Информационная безопасность (ИБ) РФ и задачи по ее обеспечению.	Устный/письменный ответ на вопросы
Тема 2	Нормативно-правовая база обеспечения ИБ в России.	Устный/письменный ответ на вопросы
Тема 3	Информация как объект правового регулирования и защиты.	Устный/письменный ответ на вопросы
Тема 4	Система субъектов обеспечения ИБ в России и их правовой статус.	Устный/письменный ответ на вопросы
Тема 5	Преступность в информационной сфере и ее криминологическая и уголовно-правовая характеристика.	Устный/письменный ответ на вопросы
Тема 6	Правовая защита личности в информационной сфере.	Устный/письменный ответ на вопросы
Тема 7	Правовой режим государственной тайны и меры по ее обеспечению.	Устный/письменный ответ на вопросы
Тема 8	Правовые и организационные способы защиты информации в сфере высоких технологий.	Устный/письменный ответ на вопросы
Тема 9	Правовое обеспечение права интеллектуальной собственности (ПИС).	Устный/письменный ответ на вопросы
Тема 10	Правовая защита коммерческой тайны (КТ).	Устный/письменный ответ на вопросы
Тема 11	Правовое регулирование отношений в сфере лицензирования и сертификации.	Устный/письменный ответ на вопросы
Тема 12	Предупреждение преступлений в информационной сфере в современной России.	Устный/письменный ответ на вопросы
Тема 13	Юридическая ответственность за правонарушения в сфере ИБ.	Устный/письменный ответ на вопросы

В ходе реализации дисциплины по заочной форме обучения с применением ЭО, ДОТ используются следующие методы текущего контроля успеваемости обучающихся:

- письменный ответ на письменные задания.

4.1.2. Зачет проводится с применением следующих методов (средств): устное собеседование по вопросам билета с письменным выполнением заданий билета либо полностью письменный ответ на вопросы билета с письменным выполнением заданий билета.

4.2. Материалы текущего контроля успеваемости

Полный перечень материалов текущего контроля находится на кафедре конституционного и муниципального права.

ТИПОВЫЕ ВОПРОСЫ И ЗАДАНИЯ ДЛЯ ОПРОСА

Тема 1. Информационная безопасность (ИБ) РФ и задачи по ее обеспечению.

1. Понятие ИБ и информационного общества. Цели, задачи и принципы обеспечения ИБ.
2. Угроза национальной безопасности и их виды.
3. Информационное общество в РФ и его характеристики. Информационная сфера и ее области.
4. Национальные интересы России в информационной сфере. Государственная политика РФ в сфере обеспечения ИБ и ее принципы.

Тема 2. Нормативно-правовая база обеспечения ИБ в России.

1. История формирования законодательства РФ об информации и ее защите.
2. Система нормативно-правовых актов России, регулирующих отношения в сфере ИБ.
3. Предмет и метод правового регулирования в сфере ИБ страны. Информационное право. Информационные отношения.
4. Правовое регулирование деятельности средств массовой информации.
5. Основные тенденции развития законодательства РФ в сфере ИБ. Особенности стандартизации нормативной базы в сфере ИБ в современном мире.

Тема 3. Информация как объект правового регулирования и защиты.

1. Информация, ее виды и признаки.
2. Информационная сфера общества и ее характеристики. Информационные ресурсы: понятие и виды.
4. Виды и источники информации, подлежащие защите.
5. Правовой режим защиты государственной тайны. Способы обеспечения сохранности информации, составляющей государственную тайну и система контроля за состоянием ее защиты.
6. Основные принципы засекречивания информации. Конфиденциальная информация и возможные каналы ее утечки.

Тема 4. Система субъектов обеспечения ИБ в России и их правовой статус.

1. Понятие государственного управления в сфере обеспечения ИБ. Система органов государственной власти, обеспечивающая ИБ и особенности их компетентности.
2. Правовой статус и система органов государственной власти, обеспечивающая право доступа к информации.
3. Особенности правового статуса и организация работы органов государственной власти, обеспечивающих защиту информации, обрабатываемой техническими средствами.

Тема 5. Преступность в информационной сфере и ее криминологическая и уголовно-правовая характеристика.

1. Понятие и виды преступности в информационной сфере.
2. Криминологическая и криминалистическая характеристики основных способов мошенничества, совершаемых с помощью сети Интернет.
3. Понятие преступления в сфере компьютерной информации. Виды преступлений в сфере компьютерной информации. Уголовно-правовая характеристика преступлений в сфере компьютерной информации.
4. Особенности объективных признаков компьютерных преступлений. Основные способы их совершения.
5. Субъективные признаки компьютерных преступлений. Мотивы и цели совершения компьютерных преступлений.
6. Криминологическая и уголовно-правовая характеристика лиц, совершающих преступления в сфере компьютерной информации.

Тема 6. Правовая защита личности в информационной сфере.

1. Система и структура нормативных актов, обеспечивающих защиту прав личности в информационной сфере.
2. Конституционные гарантии правовой охраны прав личности в информационной сфере.
3. Правовые средства защиты права на доступ к информации и неприкосновенности частной жизни.
4. Правовой механизм защиты права на неприкосновенность частной жизни.
5. Врачебная тайна как институт защиты интересов личности.
6. Персональная тайна и ее виды. Обработка и правовая охрана персональных данных.
7. Правовая база обеспечения защиты личности от воздействия «вредной» информации.

Тема 7. Правовой режим государственной тайны и меры по ее обеспечению.

1. Понятие государственной тайны и правового режима ее обеспечения. Принципы и механизм отнесения сведений к государственной тайне (ГТ).
2. Процедура засекречивания и рассекречивания сведений, составляющих государственную тайну.
3. Субъекты обеспечения режима государственной тайны и их правовой статус.
4. Организационно-правовые меры защиты ГТ. Допуск и доступ к ГТ.
5. Обеспечение ИБ при международном обмене информацией.
6. Система контроля за режимом обеспечения ГТ.
7. Особенности юридической ответственности за нарушение режима обеспечения ГТ.

Тема 8. Правовые и организационные способы защиты информации в сфере высоких технологий.

1. Правовое обеспечение защиты информации, обрабатываемой вычислительной техникой и передаваемой по компьютерным цепям.
2. Организационно-управленческие меры обеспечения защиты информации в сфере высоких технологий.
3. Компьютерные преступления и особенности их идентификации и предупреждения.
4. Криптографическая защита информации (КЗИ). Правовые и организационные способы обеспечения КЗИ в России и других странах современного мира. Контроль за разработкой, производством и применением криптографических средств.
5. КЗИ и их правовая основа. Органы лицензирования и сертификации и их правовой статус.

Тема 9. Правовое обеспечение права интеллектуальной собственности (ПИС).

1. Понятие интеллектуальной собственности и ее правовой статус. Законодательство РФ об авторских и смежных правах.
2. Особенности правоотношений, обеспечивающих ПИС. Объекты и субъекты ПИС.
3. Правовой механизм обеспечения защиты авторских и смежных прав.
4. Государственная регистрация ПИС.
5. Особенности правовой защиты программ для электронных вычислительных машин и баз данных.
6. Патентное право и патентные правоотношения. Правовой статус участников. Сфера действия патентного законодательства. Показатели и условия патентоспособности.
7. Правовой статус автора и патентообладателя. Механизм правовой защиты прав автора и патентообладателей.
8. Товарный знак и механизм его правовой защиты. Государственная регистрация товарного знака. Прекращение права на товарный знак.
9. Программы для ЭВМ и механизм их правовой защиты.

Тема 10. Правовая защита коммерческой тайны (КТ).

1. Понятие КТ и ее правовой статус. Признаки КТ. Защита КТ и патентование как способы правового закрепления права собственности на промышленный образец и полезную модель.
2. Объекты защиты КТ. Особенности правового обеспечения режима КТ.
3. Промышленный шпионаж и его объекты.
4. Критерии определения секретности при определении режима КТ. Организационные меры обеспечения защиты КТ и особенности их реализации в рамках гражданско-правовых (договорных) и трудовых отношений.
5. Режим представления информации, составляющей КТ органам государственной власти.
6. Юридическая ответственность за нарушения режима обеспечения КТ.

Тема 11. Правовое регулирование отношений в сфере лицензирования и сертификации.

1. Правовое обеспечение деятельности организаций по лицензированию и сертификации в сфере ИБ.
2. Понятие лицензирования по российскому законодательству. Виды деятельности, подлежащие лицензированию в сфере ИБ. Система государственного лицензирования в сфере ИБ и ее функции.
3. Субъекты лицензирования в сфере ИБ и их правовой статус. Порядок лицензирования, приостановления или аннулирования действия лицензии.
4. Специальная экспертиза предприятия и государственная аттестация их руководителей. Контроль за условиями обеспечения ИБ лицензиатами.
5. Понятие сертификации средств защиты информации (ССЗИ) и ее правовая основа в РФ. Цели создания системы ССЗИ.
6. Организационная структура системы ССЗИ и особенности правового статуса ее субъектов.
7. Объекты сертификационной деятельности и режимы сертификации. Особенности аттестации и контроля за деятельностью объектов обработки особо важной информации.
8. Юридическая ответственность за нарушением правил лицензирования и сертификации.

Тема 12. Предупреждение преступлений в информационной сфере в современной России.

1. Информационная безопасность России и задачи по ее обеспечению.
2. Мотивационная сфера лиц, совершающих правонарушения в сфере ИБ.
3. Субъекты деятельности по обеспечению противодействия правонарушениям в сфере ИБ и их правовой статус.
4. Оперативно-розыскные и криминалистические мероприятия по борьбе с преступлениями в сфере ИБ.
5. Особенности расследования преступлений в сфере ИБ.

Тема 13. Юридическая ответственность за правонарушения в сфере ИБ.

1. Понятие и виды юридической ответственности (ЮО) за правонарушения в сфере ИБ.
2. Уголовная ответственность за правонарушения в сфере ИБ и ее особенности.
3. Объективные и субъективные признаки составов преступлений, посягающих на ИБ страны.
4. Правовое регулирование отношений, связанных с привлечением к ответственности лиц, совершивших административные правонарушения в сфере ИБ.
5. Составы административных правонарушений, посягающих на ИБ страны.
6. Органы государственной власти и должностные лица, уполномоченные рассматривать административные правонарушения в сфере защиты информации и их правовой статус.

ТИПОВЫЕ ПРАКТИЧЕСКИЕ ЗАДАНИЯ

Тема 1. Информационная безопасность (ИБ) РФ и задачи по ее обеспечению.

Подготовьте доклад на тему: Информационные войны и информационное оружие. Информационный терроризм.

Тема 2. Нормативно-правовая база обеспечения ИБ в России.

С использованием правовой системы подобрать нормативные акты по тематике информационной безопасности.

Тема 3. Информация как объект правового регулирования и защиты.

Подготовьте доклад на тему: Виды ведомственных и корпоративных норм и их место в системе правового регулирования ИБ в РФ.

Тема 4. Система субъектов обеспечения ИБ в России и их правовой статус.

Подготовьте доклад на тему: Государственная политика РФ в сфере правового обеспечения ИБ.

Тема 5. Преступность в информационной сфере и ее криминологическая и уголовно-правовая характеристика.

Подготовьте доклад на тему: Основные этапы и тенденции развития компьютерной преступности в России.

Тема 6. Правовая защита личности в информационной сфере.

Подготовьте доклад на тему: Российская и зарубежная модели обеспечения защиты личности от воздействия «вредной» информации.

Тема 7. Правовой режим государственной тайны и меры по ее обеспечению.

С использованием ресурсов <https://sudact.ru>; <https://sudrf.ru> ознакомиться с решениями судов, где предметом разбирательства явились отношения в сфере защиты государственной тайны.

Тема 8. Правовые и организационные способы защиты информации в сфере высоких технологий.

Подготовьте доклад на тему: Правовые основы применения «электронной цифровой подписи» (ЭЦП).

Тема 9. Правовое обеспечение права интеллектуальной собственности (ПИС).

Подготовьте доклад на тему: Правовое регулирование договорных отношений в сфере ПИС.

Тема 10. Правовая защита коммерческой тайны (КТ).

С использованием ресурсов <https://sudact.ru>; <https://sudrf.ru> ознакомиться с решениями судов, где предметом разбирательства явились отношения в сфере защиты коммерческой тайны.

Тема 11. Правовое регулирование отношений в сфере лицензирования и сертификации.

С использованием ресурсов <https://sudact.ru>; <https://sudrf.ru> ознакомиться с решениями судов (период – последние 3 года), где предметом разбирательства явились отношения с участием СМИ.

Тема 12. Предупреждение преступлений в информационной сфере в современной России.

Подготовьте доклад на тему: Зарубежный опыт борьбы с преступностью в сфере ИБ.

Тема 13. Юридическая ответственность за правонарушения в сфере ИБ.

Подготовьте доклад на тему: Уголовная ответственность за компьютерные преступления и особенности их реализации в современной России.

4.3. Оценочные средства для промежуточной аттестации

4.1. Перечень компетенций с указанием этапов их формирования в процессе освоения образовательной программы. Показатели и критерии оценивания компетенций с учетом этапа их формирования

Таблица 8.

Код компетенции	Наименование компетенции	Код этапа освоения компетенции	Наименование этапа освоения компетенции
ПКо-ОС 4	Способен использовать современные технологии и методики противодействия угрозам национальной безопасности.	ПКо ОС – 4.1	Способен определить, оценить и проанализировать угрозы национальной безопасности
		ПКо ОС - 4.2	Способен на определение комплекса мер по противодействию угрозам национальной безопасности, включая современные технологии и методики
		ПКо ОС - 4.3	Способен организовать и обеспечить реализацию комплекса мер по противодействию угрозам национальной безопасности
		ПКо ОС - 4.4	Способен применить технические средства и методики в профессиональной, в том числе служебной деятельности на противодействие угрозам национальной безопасности
		ПКо ОС - 4.5	Способен оценить эффективность современных технологий и методик по противодействию угрозам национальной безопасности
ПКс-3	Способен использовать специальные познания при представлении в суде интересов лиц, органов и организаций.	ПКс – 3.1	Способен осуществлять коммуникацию в устной и письменной формах на государственном языке, иностранном языке (ах) в различных сферах профессиональной деятельности юриста
		ПКс – 3.2	Способен применять нормативные правовые акты, реализовывать нормы материального и процессуального права в профессиональной деятельности.
		ПКс – 3.3	Способен правильно и полно отра-

		жать результаты профессиональной деятельности в юридической и иной документации
	ПКс – 3.4	Способен применять нормативные правовые акты, реализовывать нормы материального и процессуального права в профессиональной деятельности.
	ПКс – 3.5	Владение навыками подготовки юридических документов.

Таблица 9.

Очная форма

Этап освоения компетенции	Показатель оценивания	Критерий оценивания
ПКо ОС – 4.1 Способен определить, оценить и проанализировать угрозы национальной безопасности	Способен определить, оценить и проанализировать угрозы национальной безопасности	Правильно определяет, дает оценку и анализирует угрозы национальной безопасности
ПКо ОС - 4.2 Способен на определение комплекса мер по противодействию угрозам национальной безопасности, включая современные технологии и методики	Осуществляет определение комплекса мер по противодействию угрозам национальной безопасности, включая современные технологии и методики. Изучает современные технологии и методики, разработанные для противодействия угрозам национальной безопасности. Выработывает тактику применения современных технологий и методик, разработанных для противодействия угрозам национальной безопасности.	Демонстрирует верный выбор мер по противодействию угрозам национальной безопасности, включая современные технологии и методики. Изучил современные технологии и методики, разработанные для противодействия угрозам национальной безопасности. Выработал тактику применения современных технологий и методик, разработанных для противодействия угрозам национальной безопасности.
ПКо ОС - 4.3 Способен организовать и обеспечить реализацию комплекса мер по противодействию угрозам национальной безопасности	Способен организовывать и обеспечить реализацию комплекса мер по противодействию угрозам национальной безопасности. Разрабатывает методики по противодействию угрозам национальной безопасности. Осуществляет взаимодействие с подразделениями и ОГВ по противодействию угрозам национальной	Организовывает и обеспечивает реализацию комплекса мер по противодействию угрозам национальной безопасности. Разрабатывает методики по противодействию угрозам национальной безопасности. Осуществляет взаимодействие с подразделениями и ОГВ по противодействию угрозам национальной безопасности.
ПКо ОС - 4.4 Способен применить технические средства и методики в профессиональной, в том числе служебной деятельности на противодействие угрозам национальной безопасно-	Применяет технические средства и методики в профессиональной деятельности, в том числе служебной деятельности на противодействие угрозам национальной безопасности	Правильно применяет технические средства и методики в профессиональной деятельности, в том числе служебной деятельности на противодействие угрозам национальной безопасности.

сти		
<p>ПКо ОС - 4.5</p> <p>Способен оценить эффективность современных технологий и методик по противодействию угрозам национальной безопасности</p>	<p>Демонстрирует знание современных технологий и методик противодействия угрозам национальной безопасности и соотносит характер угроз со средствами противодействия им.</p>	<p>Применяет современные технологии и методики противодействия угрозам национальной безопасности.</p> <p>Правильно соотносит характер угроз со средствами противодействия им.</p> <p>Оценивает эффективность примененных современных технологий и методик.</p>
<p>ПКс – 3.1</p> <p>Способен осуществлять коммуникацию в устной и письменной формах на государственном языке, иностранном языке (ах) в различных сферах профессиональной деятельности юриста</p>	<p>Осуществляет коммуникации в устной и письменной формах на государственном языке, иностранном языке (ах) с соблюдением норм профессиональной речи юриста.</p> <p>Способен подготовить публичное выступление в соответствии с основными правилами юридической риторики, и выступить перед аудиторией</p>	<p>Свободно осуществляет коммуникации в устной и письменной формах на государственном языке, иностранном языке (ах) с соблюдением норм профессиональной речи юриста.</p> <p>Грамотно разрабатывает план публичного выступления, в соответствии с основными правилами юридической риторики, осуществляет публичное выступление на различные темы.</p>
<p>ПКс – 3.2</p> <p>Способен применять нормативные правовые акты, реализовывать нормы материального и процессуального права в профессиональной деятельности.</p>	<p>Анализирует юридические факты и возникающие в связи с ними административно-процессуальные отношения.</p> <p>Анализирует и правильно применяет нормативно-правовые акты, регламентирующие административный процесс.</p> <p>Представляет квалифицированные юридические заключения и консультации в сфере административно-процессуального регулирования.</p>	<p>Проанализированы юридические факты и возникающие в связи с ними административно-процессуальные отношения.</p> <p>Проанализированы и правильно применены нормативно-правовые акты, регламентирующие административный процесс.</p> <p>Представлены квалифицированные юридические заключения и консультации в сфере административно-процессуального регулирования.</p>
<p>ПКс – 3.3</p> <p>Способен правильно и полно отражать результаты профессиональной деятельности в юридической и иной документации</p>	<p>Выбирает вид юридического документа и оформляет процессуальные действия и решения в проекте процессуальных и иных документов; избирает правильную форму обращения в суд и судебный акт, составляет и правильно оформляет проект процессуального документа.</p>	<p>Выбран вид юридического документа и оформлены процессуальные действия и решения в проекте процессуальных и иных документов; избрана правильная форма обращения в суд и судебный акт, составлен и правильно оформлен проект процессуального документа.</p>
<p>ПКс – 3.4</p> <p>Способен применять нормативные правовые акты, реализовывать нормы материального и процессуального права в профессиональной деятельности.</p>	<p>Определяет необходимое процессуальное действие и принимает необходимое процессуальное решение.</p>	<p>Правильно определено необходимое процессуальное действие и принято необходимое процессуальное решение</p>

ПКс – 3.5 Владение навыками подготовки юридических документов.	Прогнозирует и анализирует возможные последствия создания юридического документа, редактирует юридический документ и приводит его в требуемую форму.	Спрогнозированы и проанализированы возможные последствия создания юридического документа, отредактирован юридический документ и приведен в требуемую форму.
---	--	---

Таблица 10.

Заочная форма

Этап освоения компетенции	Показатель оценивания	Критерий оценивания
ПКо ОС – 4.1 Способен определить, оценить и проанализировать угрозы национальной безопасности	Способен определить, оценить и проанализировать угрозы национальной безопасности	Правильно определяет, дает оценку и анализирует угрозы национальной безопасности
ПКо ОС - 4.2 Способен на определение комплекса мер по противодействию угрозам национальной безопасности, включая современные технологии и методики	Осуществляет определение комплекса мер по противодействию угрозам национальной безопасности, включая современные технологии и методики. Изучает современные технологии и методики, разработанные для противодействия угрозам национальной безопасности. Вырабатывает тактику применения современных технологий и методик, разработанных для противодействия угрозам национальной безопасности.	Демонстрирует верный выбор мер по противодействию угрозам национальной безопасности, включая современные технологии и методики. Изучил современные технологии и методики, разработанные для противодействия угрозам национальной безопасности. Выработал тактику применения современных технологий и методик, разработанных для противодействия угрозам национальной безопасности.
ПКо ОС - 4.3 Способен организовать и обеспечить реализацию комплекса мер по противодействию угрозам национальной безопасности	Способен организовывать и обеспечить реализацию комплекса мер по противодействию угрозам национальной безопасности. Осуществляет взаимодействие с подразделениями и ОГВ по противодействию угрозам национальной безопасности.	Организовывает и обеспечивает реализацию комплекса мер по противодействию угрозам национальной безопасности. Осуществляет взаимодействие с подразделениями и ОГВ по противодействию угрозам национальной безопасности.
ПКо ОС - 4.4 Способен разрабатывать методики по противодействию угрозам национальной безопасности.	Разрабатывает методики по противодействию угрозам национальной безопасности.	Разработаны методики по противодействию угрозам национальной безопасности.
ПКо ОС - 4.5 Способен применить технические средства и методики в профессиональной, в том числе служебной деятельности на противодействие угро-	Применяет технические средства и методики в профессиональной деятельности, в том числе служебной деятельности на противодействие угрозам национальной	Правильно применяет технические средства и методики в профессиональной деятельности, в том числе служебной деятельности на противодействие угрозам национальной безопас-

зам национальной безопасности	безопасности	ности.
ПКо ОС - 4.6 Способен оценить эффективность современных технологий и методик по противодействию угрозам национальной безопасности	Демонстрирует знание современных технологий и методик противодействия угрозам национальной безопасности и соотносит характер угроз со средствами противодействия им.	Применяет современные технологии и методики противодействия угрозам национальной безопасности. Правильно соотносит характер угроз со средствами противодействия им. Оценивает эффективность примененных современных технологий и методик.
ПКс – 3.1 Способен осуществлять коммуникацию в устной и письменной формах на государственном языке, иностранном языке (ах) в различных сферах профессиональной деятельности юриста	Осуществляет коммуникации в устной и письменной формах на государственном языке, иностранном языке (ах) с соблюдением норм профессиональной речи юриста. Способен подготовить публичное выступление в соответствии с основными правилами юридической риторики, и выступить перед аудиторией	Свободно осуществляет коммуникации в устной и письменной формах на государственном языке, иностранном языке (ах) с соблюдением норм профессиональной речи юриста. Грамотно разрабатывает план публичного выступления, в соответствии с основными правилами юридической риторики, осуществляет публичное выступление на различные темы.
ПКс – 3.2 Способен применять нормативные правовые акты	Анализирует юридические факты и возникающие в связи с ними административно-процессуальные отношения.	Проанализированы юридические факты и возникающие в связи с ними административно-процессуальные отношения.
ПКс – 3.3 Способен реализовывать нормы материального и процессуального права в профессиональной деятельности.	Анализирует и правильно применяет нормативно-правовые акты, регламентирующие административный процесс. Представляет квалифицированные юридические заключения и консультации в сфере административно-процессуального регулирования.	Проанализированы и правильно применены нормативно-правовые акты, регламентирующие административный процесс. Представлены квалифицированные юридические заключения и консультации в сфере административно-процессуального регулирования.
ПКс – 3.4 Способен правильно и полно отражать результаты профессиональной деятельности в юридической и иной документации	Выбирает вид юридического документа и оформляет процессуальные действия и решения в проекте процессуальных и иных документов; избирает правильную форму обращения в суд и судебный акт, составляет и правильно оформляет проект процессуального документа.	Выбран вид юридического документа и оформлены процессуальные действия и решения в проекте процессуальных и иных документов; избрана правильная форма обращения в суд и судебный акт, составлен и правильно оформлен проект процессуального документа.
ПКс – 3.5 Способен применять нормативные правовые акты в профессиональной деятельности.	Определяет необходимое процессуальное действие и принимает необходимое процессуальное решение.	Правильно определено необходимое процессуальное действие и принято необходимое процессуальное решение

ПКс – 3.6 Способен реализовывать нормы материального и процессуального права в профессиональной деятельности.	Реализовывает нормы материального и процессуального права в профессиональной деятельности.	Реализованы нормы материального и процессуального права в профессиональной деятельности.
ПКс – 3.7 Владение навыками подготовки юридических документов.	Прогнозирует и анализирует возможные последствия создания юридического документа, редактирует юридический документ и приводит его в требуемую форму.	Спрогнозированы и проанализированы возможные последствия создания юридического документа, отредактирован юридический документ и приведен в требуемую форму.

Таблица 11.

Заочная форма с ЭО и ДОТ

Этап освоения компетенции	Показатель оценивания	Критерий оценивания
ПКо ОС – 4.1 Способен определить, оценить и проанализировать угрозы национальной безопасности	Способен определить, оценить и проанализировать угрозы национальной безопасности	Правильно определяет, дает оценку и анализирует угрозы национальной безопасности
ПКо ОС - 4.2 Способен на определение комплекса мер по противодействию угрозам национальной безопасности, включая современные технологии и методики	Осуществляет определение комплекса мер по противодействию угрозам национальной безопасности, включая современные технологии и методики. Изучает современные технологии и методики, разработанные для противодействия угрозам национальной безопасности. Вырабатывает тактику применения современных технологий и методик, разработанных для противодействия угрозам национальной безопасности.	Демонстрирует верный выбор мер по противодействию угрозам национальной безопасности, включая современные технологии и методики. Изучил современные технологии и методики, разработанные для противодействия угрозам национальной безопасности. Выработал тактику применения современных технологий и методик, разработанных для противодействия угрозам национальной безопасности.
ПКо ОС - 4.3 Способен организовать и обеспечить реализацию комплекса мер по противодействию угрозам национальной безопасности	Способен организовывать и обеспечить реализацию комплекса мер по противодействию угрозам национальной безопасности. Осуществляет взаимодействие с подразделениями и ОГВ по противодействию угрозам национальной безопасности.	Организовывает и обеспечивает реализацию комплекса мер по противодействию угрозам национальной безопасности. Осуществляет взаимодействие с подразделениями и ОГВ по противодействию угрозам национальной безопасности.
ПКо ОС - 4.4 Способен разрабатывать методики по противодействию угрозам национальной безопасности	Разрабатывает методики по противодействию угрозам национальной безопасности.	Разработаны методики по противодействию угрозам национальной безопасности.

опасности.		
ПКо ОС - 4.5 Способен применить технические средства и методики в профессиональной, в том числе служебной деятельности на противодействие угрозам национальной безопасности	Применяет технические средства и методики в профессиональной деятельности, в том числе служебной деятельности на противодействие угрозам национальной безопасности	Правильно применяет технические средства и методики в профессиональной деятельности, в том числе служебной деятельности на противодействие угрозам национальной безопасности.
ПКо ОС - 4.6 Способен оценить эффективность современных технологий и методик по противодействию угрозам национальной безопасности	Демонстрирует знание современных технологий и методик противодействия угрозам национальной безопасности и соотносит характер угроз со средствами противодействия им.	Применяет современные технологии и методики противодействия угрозам национальной безопасности. Правильно соотносит характер угроз со средствами противодействия им. Оценивает эффективность примененных современных технологий и методик.
ПКс – 3.1 Способен осуществлять коммуникацию в устной и письменной формах на государственном языке, иностранном языке (ах) в различных сферах профессиональной деятельности юриста	Осуществляет коммуникации в устной и письменной формах на государственном языке, иностранном языке (ах) с соблюдением норм профессиональной речи юриста. Способен подготовить публичное выступление в соответствии с основными правилами юридической риторики, и выступить перед аудиторией	Свободно осуществляет коммуникации в устной и письменной формах на государственном языке, иностранном языке (ах) с соблюдением норм профессиональной речи юриста. Грамотно разрабатывает план публичного выступления, в соответствии с основными правилами юридической риторики, осуществляет публичное выступление на различные темы.
ПКс – 3.2 Способен применять нормативные правовые акты	Анализирует юридические факты и возникающие в связи с ними административно-процессуальные отношения.	Проанализированы юридические факты и возникающие в связи с ними административно-процессуальные отношения.
ПКс – 3.3 Способен реализовывать нормы материального и процессуального права в профессиональной деятельности.	Анализирует и правильно применяет нормативно-правовые акты, регламентирующие административный процесс. Представляет квалифицированные юридические заключения и консультации в сфере административно-процессуального регулирования.	Проанализированы и правильно применены нормативно-правовые акты, регламентирующие административный процесс. Представлены квалифицированные юридические заключения и консультации в сфере административно-процессуального регулирования.
ПКс – 3.4 Способен правильно и полно отражать результаты профессиональной деятельности в юридической и иной документации	Выбирает вид юридического документа и оформляет процессуальные действия и решения в проекте процессуальных и иных документов; избирает правильную форму обращения в суд и судебный акт, составляет и правильно	Выбран вид юридического документа и оформлены процессуальные действия и решения в проекте процессуальных и иных документов; избрана правильная форма обращения в суд и судебный акт, составлен и правильно

	оформляет проект процессуального документа.	оформлен проект процессуального документа.
ПКс – 3.5 Способен применять нормативные правовые акты в профессиональной деятельности.	Определяет необходимое процессуальное действие и принимает необходимое процессуальное решение.	Правильно определено необходимое процессуальное действие и принято необходимое процессуальное решение
ПКс – 3.6 Способен реализовывать нормы материального и процессуального права в профессиональной деятельности.	Реализовывает нормы материального и процессуального права в профессиональной деятельности.	Реализованы нормы материального и процессуального права в профессиональной деятельности.
ПКс – 3.7 Владение навыками подготовки юридических документов.	Прогнозирует и анализирует возможные последствия создания юридического документа, редактирует юридический документ и приводит его в требуемую форму.	Спрогнозированы и проанализированы возможные последствия создания юридического документа, отредактирован юридический документ и приведен в требуемую форму.

4.3.2. Типовые оценочные средства

Полный перечень вопросов и заданий находится на кафедре конституционного и муниципального права.

ТИПОВЫЕ ВОПРОСЫ И ЗАДАНИЯ ДЛЯ ПОДГОТОВКИ К ЗАЧЕТУ

Типовые вопросы на проверку знаний

1. Понятие ИБ и информационного общества. Цели, задачи и принципы обеспечения ИБ.
2. Угроза национальной безопасности и их виды. Информационные войны и информационное оружие. Информационный терроризм.
3. Информационное общество в РФ и его характеристики. Информационная сфера и ее области.
4. Национальные интересы России в информационной сфере. Государственная политика РФ в сфере обеспечения ИБ и ее принципы.
5. История формирования законодательства РФ об информации и ее защите.
6. Система нормативно-правовых актов России, регулирующих отношения в сфере ИБ.
7. Предмет и метод правового регулирования в сфере ИБ страны. Информационное право. Информационные отношения.
8. Виды ведомственных и корпоративных норм и их место в системе правового регулирования ИБ в РФ.
9. Правовое регулирование деятельности средств массовой информации.
10. Основные тенденции развития законодательства РФ в сфере ИБ. Особенности стандартизации нормативной базы в сфере ИБ в современном мире.
11. Информация, ее виды и признаки.
12. Информационная сфера общества и ее характеристики. Информационные ресурсы: понятие и виды.
13. Виды и источники информации, подлежащие защите.

14. Правовой режим защиты государственной тайны. Способы обеспечения сохранности информации, составляющей государственную тайну и система контроля за состоянием ее защиты.
15. Основные принципы засекречивания информации. Конфиденциальная информация и возможные каналы ее утечки.
16. Государственная политика РФ в сфере правового обеспечения ИБ.
17. Понятие государственного управления в сфере обеспечения ИБ. Система органов государственной власти, обеспечивающая ИБ и особенности их компетентности.
18. Правовой статус и система органов государственной власти, обеспечивающая право доступа к информации.
19. Особенности правового статуса и организация работы органов государственной власти, обеспечивающих защиту информации, обрабатываемой техническими средствами.
20. Служба Специальной связи и информации Федеральной службы охраны РФ, ее задачи и правовой статус.
21. Понятие и виды преступности в информационной сфере.
22. Основные этапы и тенденции развития компьютерной преступности в России.
23. Криминологическая и криминалистическая характеристики основных способов мошенничества, совершаемых с помощью сети Интернет.
24. Понятие преступления в сфере компьютерной информации. Виды преступлений в сфере компьютерной информации. Уголовно-правовая характеристика преступлений в сфере компьютерной информации.
25. Особенности объективных признаков компьютерных преступлений. Основные способы их совершения.
26. Субъективные признаки компьютерных преступлений. Мотивы и цели совершения компьютерных преступлений.
27. Криминологическая и уголовно-правовая характеристика лиц, совершающих преступления в сфере компьютерной информации.
28. Система и структура нормативных актов, обеспечивающих защиту прав личности в информационной сфере.

Типовые вопросы на проверку умений

29. Конституционные гарантии правовой охраны прав личности в информационной сфере.
30. Правовые средства защиты права на доступ к информации и неприкосновенности частной жизни.
31. Правовой механизм защиты права на неприкосновенность частной жизни.
32. Врачебная тайна как институт защиты интересов личности.
33. Персональная тайна и ее виды. Обработка и правовая охрана персональных данных.
34. Правовая база обеспечения защиты личности от воздействия «вредной» информации.
35. Российская и зарубежная модели обеспечения защиты личности от воздействия «вредной» информации.
36. Понятие государственной тайны и правового режима ее обеспечения. Принципы и механизм отнесения сведений к государственной тайне (ГТ).
37. Процедура засекречивания и рассекречивания сведений, составляющих государственную тайну.
38. Субъекты обеспечения режима государственной тайны и их правовой статус.
39. Организационно-правовые меры защиты ГТ. Допуск и доступ к ГТ.
40. Обеспечение ИБ при международном обмене информацией.
41. Система контроля за режимом обеспечения ГТ.
42. Особенности юридической ответственности за нарушение режима обеспечения ГТ.
43. Правовое обеспечение защиты информации, обрабатываемой вычислительной техникой и передаваемой по компьютерным цепям.

44. Организационно-управленческие меры обеспечения защиты информации в сфере высоких технологий.
45. Компьютерные преступления и особенности их идентификации и предупреждения.
46. Правовые основы применения «электронной цифровой подписи» (ЭЦП).
47. Криптографическая защита информации (КЗИ). Правовые и организационные способы обеспечения КЗИ в России и других странах современного мира. Контроль за разработкой, производством и применением криптографических средств.
48. КЗИ и их правовая основа. Органы лицензирования и сертификации и их правовой статус.
49. Понятие интеллектуальной собственности и ее правовой статус. Законодательство РФ об авторских и смежных правах.
50. Особенности правоотношений, обеспечивающих ПИС. Объекты и субъекты ПИС.
51. Правовой механизм обеспечения защиты авторских и смежных прав.
52. Государственная регистрация ПИС.
53. Особенности правовой защиты программ для электронных вычислительных машин и баз данных.
54. Патентное право и патентные правоотношения. Правовой статус участников. Сфера действия патентного законодательства. Показатели и условия патентоспособности.
55. Правовой статус автора и патентообладателя. Механизм правовой защиты прав автора и патентообладателей.
56. Товарный знак и механизм его правовой защиты. Государственная регистрация товарного знака. Прекращение права на товарный знак.

Типовые вопросы на проверку навыков

57. Программы для ЭВМ и механизм их правовой защиты.
58. Правовое регулирование договорных отношений в сфере ПИС.
59. Понятие КТ и ее правовой статус. Признаки КТ. Защита КТ и патентование как способы правового закрепления права собственности на промышленный образец и полезную модель.
60. Объекты защиты КТ. Особенности правового обеспечения режима КТ.
61. Раскройте сущность промышленного шпионажа и охарактеризуйте его объекты.
62. Раскройте критерии определения секретности при определении режима КТ. Перечислите организационные меры обеспечения защиты КТ и особенности их реализации в рамках гражданско-правовых (договорных) и трудовых отношений.
63. Режим представления информации, составляющей КТ органам государственной власти.
64. Юридическая ответственность за нарушения режима обеспечения КТ.
65. Правовое обеспечение деятельности организаций по лицензированию и сертификации в сфере ИБ.
66. Понятие лицензирования по российскому законодательству. Виды деятельности, подлежащие лицензированию в сфере ИБ. Система государственного лицензирования в сфере ИБ и ее функции.
67. Субъекты лицензирования в сфере ИБ и их правовой статус. Порядок лицензирования, приостановления или аннулирования действия лицензии.
68. Специальная экспертиза предприятия и государственная аттестация их руководителей. Контроль за условиями обеспечения ИБ лицензиатами.
69. Понятие сертификации средств защиты информации (ССЗИ) и ее правовая основа в РФ. Цели создания системы ССЗИ.
70. Организационная структура системы ССЗИ и особенности правового статуса ее субъектов.
71. Объекты сертификационной деятельности и режимы сертификации. Особенности аттестации и контроля за деятельностью объектов обработки особо важной информации.
72. Юридическая ответственность за нарушением правил лицензирования и сертификации.

73. Информационная безопасность России и задачи по ее обеспечению.
74. Мотивационная сфера лиц, совершающих правонарушения в сфере ИБ.
75. Субъекты деятельности по обеспечению противодействия правонарушениям в сфере ИБ и их правовой статус.
76. Оперативно-розыскные и криминалистические мероприятия по борьбе с преступлениями в сфере ИБ.
77. Особенности расследования преступлений в сфере ИБ.
78. Понятие и виды юридической ответственности (ЮО) за правонарушения в сфере ИБ.
79. Уголовная ответственность за правонарушения в сфере ИБ и ее особенности.
80. Объективные и субъективные признаки составов преступлений, посягающих на ИБ страны.
81. Уголовная ответственность за компьютерные преступления и особенности их реализации в современной России.
82. Правовое регулирование отношений, связанных с привлечением к ответственности лиц, совершивших административные правонарушения в сфере ИБ.
83. Составы административных правонарушений, посягающих на ИБ страны.
84. Органы государственной власти и должностные лица, уполномоченные рассматривать административные правонарушения в сфере защиты информации и их правовой статус.

Шкала оценивания

Таблица 12.

Очная форма обучения, очно-заочная, заочная, заочная форма обучения с применением ЭО и ДОТ

Зачет с оценкой	Критерии оценки
зачтено	<ul style="list-style-type: none"> - ответ логически и лексически грамотно изложен, содержательный и аргументированный, подкрепленный знанием литературы и источников по теме опроса; - умение отвечать на дополнительно заданные вопросы; - незначительное нарушение логики изложения материала, периодическое использование разговорной лексики, допущение не более одной ошибки в содержании ответа, а также не более одной неточности при аргументации своей позиции; - неполные или неточные ответы на дополнительно заданные вопросы; - незначительное нарушение логики изложения материала, периодическое использование разговорной лексики при допущении не более двух ошибок в содержании ответа, а также не более двух неточностей при аргументации своей позиции, неполные или неточные ответы на дополнительно заданные вопросы.
незачтено	<ul style="list-style-type: none"> - в ответе допущено существенное нарушение логики изложения материала, систематическое использование разговорной лексики, допущение не более двух ошибок в содержании ответа, а также не более двух неточностей при аргументации своей позиции, неправильные ответы на дополнительно заданные вопросы; - существенное нарушение логики изложения материала, постоянное использование разговорной лексики, допущение не более трех ошибок в содержании ответа, а также не более трех неточностей при аргументации своей позиции, неправильные ответы на дополнительно заданные вопросы;

- полное отсутствие логики изложения материала, постоянное использование разговорной лексики, допущение более трех ошибок в содержании ответа, а также более трех неточностей при аргументации своей позиции, полное незнание литературы и источников по теме вопроса, отсутствие ответов на дополнительно заданные вопросы.
--

4.4. Методические материалы промежуточной аттестации

Зачет включает ответы на теоретические вопросы.

Ответы на теоретические вопросы могут даваться в устной форме или в форме электронного тестирования.

Студент при подготовке к ответу по билету формулирует ответ на вопрос.

При подготовке ответа на вопрос стоит использовать соответствующий дисциплине понятийный аппарат, основываться на действующем законодательстве и изученных актах судебной практики, отвечать с пояснениями, полно и аргументированно.

При сравнении явлений необходимо представить аргументы, представляющие их сходства и различия.

Давать односложные ответы нежелательно.

Нет необходимости при ответе приводить номера статей нормативных правовых актов, но содержание ответа должно основываться на действующем законодательстве.

При ответе студент должен полно и аргументированно ответить на вопрос билета, демонстрируя знания либо умения в его рамках.

При демонстрации выполненного задания студент должен аргументировать свое решение (формулировку текста и т.д.), демонстрируя знания, умения либо навыки в полной мере.

Для студентов, обучающихся на заочной форме обучения с применением ЭО и ДОТ выполнение письменного контрольного задания позволяет оценить умения и навыки по дисциплине и осуществляется в течении семестра.

Проверка знаний также осуществляется с помощью тестовых заданий. Тестирование проводится в СДО "Академия" в соответствии с установленными требованиями. Итоговый тест формируется на аппаратном уровне с использованием банка тестовых заданий по дисциплине. Проверка результатов тестирования осуществляется автоматически.

5. Методические указания для обучающихся по освоению дисциплины

При изучении курса «Правовое обеспечение информационной безопасности» применяются лекции, практические занятия, выполнение практических заданий по темам и контрольной работы по всему курсу, самостоятельная работа с источниками и др.

Студентам рекомендуется вести две специальные тетради: для записи основных положений лекций (конспектов) и для самостоятельной работы при подготовке к практическим занятиям.

Студент обязательно должен посетить первые лекции, на которых излагается цель, задачи и содержание курса, выдается задание на контрольную работу, приводятся рекомендации и критерии оценивания.

На практических занятиях у студентов формируются навыки публичного выступления, анализа материала, умение грамотно и обоснованно отвечать на поставленные вопросы и применять полученные теоретические знания к практическим ситуациям, а также умение выполнять (решать) практические задания (задачи).

При необходимости в период самостоятельной подготовки студенты могут получить индивидуальные консультации преподавателя по учебной дисциплине.

Для подготовки к занятиям по курсу «Правовое обеспечение информационной безопасности» следует начинать с ознакомления с содержанием темы, вопросами к теме, подбора рекомендованной литературы. Затем необходимо перечитать конспект лекции, ознакомиться с основной литературой. При этом нужно иметь соответствующие нормативные акты в действующей редакции, в частности, Конституцию РФ. Рекомендуется внимательно изучать ма-

териалы справочных правовых систем для уточнения действующих редакций нормативных актов, которые в сфере конституционного права очень часто обновляются.

Особенностью освоения данной дисциплины по заочной форме является минимизация устных форм опроса и выполнения практических заданий из-за небольшого объема аудиторных занятий. Основным методом обучения на заочной форме выступает собственно самостоятельная работа, которая выполняется индивидуально в произвольном режиме времени в удобные для обучающегося часы, часто вне аудитории - внеаудиторная самостоятельная работа.

Опрос в рамках изучаемой темы может проходить как в устной, так и в письменной форме.

Опрос проводится только после изучения материала темы и направлен на ее закрепление.

Вопросы могут быть направлены как на закрепление знаний, например, нормативно-правовых актов, составляющих источники информации и подлежащих применению, так и на формирование умений, например, сопоставлять правовые нормы с конкретной ситуацией, давать правовую оценку установленным фактам и обстоятельствам и т.д.

Для успешного ответа на вопросы вполне достаточно изучения действующего законодательства, относящегося к курсу, а также основных источников литературы.

Решение практических заданий нацелено на формирование у студента соответствующих компетентностных практических умений и владений.

При решении задач ответ должен быть дан конкретно на поставленный вопрос либо ситуацию (казус), при этом обязательным является формулировка ответа с использованием профессиональных терминов и ссылка на статьи гражданско-правового нормативного источника.

При составлении схемы надо иметь в виду основные требования к выделению видов (классов) явлений и процессов по какому-то отдельному основанию, а также ссылки на статьи нормативного источника (как нормативного, так и литературного).

При заполнении таблиц необходимо придерживаться установленных в задании требований, например, по количеству рассматриваемых примеров.

Ссылки нужны для подтверждения достоверности представленных сведений, а также оценки умения пользоваться действующим законодательством. Именно эти умения и навыки являются ценными для профессиональной работы выпускника по специальности 40.05.01 «Правовое обеспечение национальной безопасности».

6. Учебная литература и ресурсы информационно-телекоммуникационной сети «интернет», учебно-методическое обеспечение для самостоятельной работы обучающихся по дисциплине

6.1. Основная литература

1. Организационное и правовое обеспечение информационной безопасности : учебник и практикум для вузов / под редакцией Т. А. Поляковой, А. А. Стрельцова. — Москва : Издательство Юрайт, 2021. — 325 с. — (Высшее образование). — ISBN 978-5-534-03600-8. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: <https://urait.ru/bcode/469235>

2. Внуков, А. А. Защита информации : учебное пособие для вузов / А. А. Внуков. — 3-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2021. — 161 с. — (Высшее образование). — ISBN 978-5-534-07248-8. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: <https://urait.ru/bcode/470131>

6.2. Дополнительная литература

3. Информационные технологии. Базовый курс : учебник / А. В. Костюк, С. А. Бобонец, А. В. Флегонтов, А. К. Черных. — 2-е изд., стер. — Санкт-Петербург : Лань, 2019. — 604 с. — ISBN 978-5-8114-4065-8. — URL: <https://e.lanbook.com/book/114686> (дата обращения: 17.02.2021). — Режим доступа: электрон.-библ. система «Лань», требуется авторизация.

4. Кармановский, Н. С. Организационно-правовое и методическое обеспечение информационной безопасности : учебное пособие / Н. С. Кармановский, О. В. Михайличенко, Н. Н. Прохожев. — Санкт-Петербург : Университет ИТМО, 2016. — 169 с. — ISBN 2227-8397. — URL: <http://www.iprbookshop.ru/67452.html> (дата обращения: 17.02.2021). — Режим доступа: электрон.-библ. система «IPRbooks», требуется авторизация. — То же электрон. версия на сайте URL: <https://e.lanbook.com/book/91449> (дата обращения: 17.02.2021). — Режим доступа: электрон.-библ. система «Лань», требуется авторизация.

5. Организационное и правовое обеспечение информационной безопасности : учебник и практикум для вузов / Т. А. Полякова, А. А. Стрельцов, С. Г. Чубукова, В. А. Ниесов ; под ред. Т. А. Поляковой, А. А. Стрельцова. — Москва : Юрайт, 2020. — 325 с. — (Высшее образование). — ISBN 978-5-534-03600-8. — URL: <https://urait.ru/bcode/450371> (дата обращения: 17.02.2021). — Режим доступа: электрон.-библ. система «Юрайт», требуется авторизация.

6. Прохорова, О. В. Информационная безопасность и защита информации : учебник / О. В. Прохорова. — 2-е изд., испр. — Санкт-Петербург : Лань, 2020. — 124 с. — ISBN 978-5-8114-4404-5. — URL: <https://e.lanbook.com/book/133924> (дата обращения: 17.02.2021). — Режим доступа: электрон.-библ. система «Лань», требуется авторизация.

6.3. Учебно-методическое обеспечение самостоятельной работы

6.4. Нормативные правовые документы

1. Конституция Российской Федерации (принята всенародным голосованием 12.12.1993) (с учетом поправок, внесенных Законами РФ о поправках к Конституции РФ от 30.12.2008 N 6-ФКЗ, от 30.12.2008 N 7-ФКЗ, от 05.02.2014 N 2-ФКЗ, от 01.07.2020 N 11-ФКЗ) // Российская газета. - 2020. - 4 июля. - № 144.
2. Конвенция о защите прав человека и основных свобод от 4 ноября 1950 г. // Собр. законодательства РФ. - 2001. - №2. - Ст. 163.
3. О Конституционном Суде Российской Федерации: федеральный конституционный закон от 21 июля 1994 № 1-ФКЗ (в ред. федер. конст. закона от 04.06.2014) // Собр. законодательства РФ. - 1994. - № 13. - ст. 1447.
4. Об информации, информационных технологиях, и о защите информации: федеральный закон от 27 июля 2006 года № 149-ФЗ // Рос. газета. - 29.07.2006. - № 165.
5. О государственной тайне: закон Российской Федерации от 21 июля 1993 года № 5481-1 // Рос. газета. - 21.09.1993. - № 18.

Акты судебных органов

- По делу о проверке конституционности статей 1 и 21 Закона Российской Федерации от 21 июля 1993 года "О государственной тайне" в связи с жалобами граждан В.М. Гурджиянца, В.Н. Синцова, В.Н. Бугрова и А.К. Никитина: Постановление Конституционного Суда РФ от 27.03.1996 N 8-П // Рос. газета. – 04.04.1996. - № 64.

6.5. Интернет-ресурсы

- Официальный сайт Конституционного Суда Российской Федерации [Электронный ресурс]. - Режим доступа: www.ksrf.ru
- Министерство юстиции РФ <http://minjust.ru/ru/activity/development>
- Министерство цифрового развития, связи и массовых коммуникаций РФ <https://digital.gov.ru/ru/>
- Роскомнадзор России <https://rkn.gov.ru/>
- ФСБ России <http://www.fsb.ru/>
- ФСТЭК России <https://fstec.ru/>
- Совет Безопасности РФ <http://www.scrf.gov.ru/>
- Правительство РФ: <http://www.government.ru>
- Единый портал раскрытия информации о проектах нормативных актов федеральных органов исполнительной власти <http://regulation.gov.ru/>

7. Материально-техническая база, информационные технологии, программное обеспечение и информационные справочные системы

Учебная аудитория для проведения учебных занятий (занятий лекционного типа), оснащенная оборудованием и техническими средствами обучения: комплект специализированной учебной мебели (столы и кресла – рабочие места обучающихся и преподавателя); доска аудиторная; экран; персональный компьютер; звуковая система; проектор; веб-камера. Выход в Интернет и доступ в электронную информационно-образовательную среду организации.

Учебная аудитория для проведения учебных занятий (занятий семинарского типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации), оснащенная оборудованием и техническими средствами обучения: комплект специализированной учебной мебели (столы и стулья – рабочие места обучающихся и преподавателя); доска аудиторная; персональный компьютер; телевизор; веб-камера. Выход в Интернет и доступ в электронную информационно-образовательную среду организации.

Компьютерный класс, учебная аудитория для проведения учебных занятий (занятий семинарского типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации), оснащенная оборудованием и техническими средствами обучения: комплект специализированной учебной мебели (столы и стулья - рабочие места обучающихся и преподавателя), доска аудиторная; персональные компьютеры моноблоки; проектор; веб-камера; экран. Выход в Интернет и доступ в электронную информационно-образовательную среду организации, в том числе с рабочих мест обучающихся. Программное обеспечение: операционная система Microsoft Windows; пакеты лицензионных программ: MS Office, MS Teams, СПС КонсультантПлюс, лицензионное антивирусное программное обеспечение.

Помещение для самостоятельной работы обучающихся (Информационно-ресурсный центр) оснащенное комплектом специализированной учебной мебели, компьютерной техникой с возможностью подключения к сети Интернет и обеспечено доступом в электронную информационно-образовательную среду организации.

Программное обеспечение: ОС Microsoft Windows, Пакет Microsoft Office (Word, Excel, PowerPoint), Microsoft Teams, лицензионное антивирусное программное обеспечение.