

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РФ
Федеральное государственное образовательное учреждение
высшего образования
«ДАГЕСТАНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»
ЮРИДИЧЕСКИЙ ИНСТИТУТ
КАФЕДРА ИНФОРМАЦИОННОГО ПРАВА И ИНФОРМАТИКИ

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

ОРГАНИЗАЦИОННОЕ И ПРАВОВОЕ ОБЕСПЕЧЕНИЕ
ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Образовательная программа
09.04.03 Прикладная информатика

Магистерская программа
Прикладная информатика в аналитической
экономике

Уровень высшего образования
магистратура

Форма обучения
очная

Статус дисциплины: вариативная

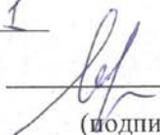
Махачкала 2018 год

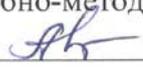
Рабочая программа дисциплины «Организационное и правовое обеспечение информационной безопасности» составлена в 2018 году в соответствии с требованиями ФГОС ВО по направлению подготовки 09.04.03 Прикладная информатика (уровень магистратуры) от «30» октября 2014 г. №1404.

Разработчик(и): кафедра «Информационного права и информатики», Везиров Тельман Тимурович, кандидат педагогических наук, доцент.

Рабочая программа дисциплины одобрена:
на заседании кафедры информационного права и информатики
от «15» 06 2018 г., протокол № 11 .
Зав. кафедрой  Абдусаламов Р.А.
(подпись)

на заседании Методической комиссии юридического института
от «31» 08 2018 г., протокол № 1 .
Председатель  Арсланбекова А.З.
(подпись)

Рабочая программа дисциплины согласована на заседании учебно-методической комиссии факультета информатики и ИТ от «31» 08 2018 г.,
протокол № 1 .
Председатель  Камиллов К.Б.
(подпись)

Рабочая программа дисциплины согласована с учебно-методическим управлением «31» 08 2018 г. 
(подпись)

Аннотация рабочей программы дисциплины

Дисциплина *Организационное и правовое обеспечение информационной безопасности* относится к базовой части образовательной программы магистратуры по направлению *09.04.03 Прикладная информатика*.

Дисциплина реализуется на факультете *информатики и информационных технологий* кафедрой *информационного права и информатики*.

Содержание дисциплины охватывает круг вопросов, связанных с основы правового регулирования отношений в информационной сфере, конституционные гарантии прав граждан на получение информации и механизм их реализации, понятия и виды защищаемой информации по законодательству РФ, систему защиты государственной тайны, основы правового регулирования отношений в области интеллектуальной собственности и способы защиты этой собственности, а также понятие и виды компьютерных преступлений.

Дисциплина нацелена на формирование следующих компетенций выпускника: общекультурных – **ОК-3**, общепрофессиональных – **ОПК-1, ОПК-2**.

Преподавание дисциплины предусматривает проведение следующих видов учебных занятий: *лекции, практические занятия, самостоятельная работа*.

Рабочая программа дисциплины предусматривает проведение следующих видов контроля успеваемости в форме *коллоквиума* и промежуточный контроль в форме *зачета, экзамена*.

Объем дисциплины **5** зачетных единиц, в том числе в академических часах по видам учебных занятий

Се- местр	Учебные занятия							Форма промежуточной аттестации (зачет, дифференцированный зачет, экзамен)
	в том числе							
	Контактная работа обучающихся с преподавателем						СРС	
	Все го	из них						
Лек- ции		Лабора- торные занятия	Практи- ческие занятия	КСР	Кон- троль			
А	36	8		14	4		10	Зачет
В	144	8		36	4	36	60	Экзамен

1. Цели освоения дисциплины

Целями освоения дисциплины *Организационное и правовое обеспечение информационной безопасности* являются дать основы информационного законодательства Российской Федерации; системы защиты государственной тайны; правил лицензирования и сертификации в области защиты информации; международного законодательства в области защиты информации; знаний о компьютерных преступлениях; организации службы безопасности объекта и работы с кадрами; организационного обеспечения защиты информации.

2. Место дисциплины в структуре ОПОП магистратуры

Дисциплина *Организационное и правовое обеспечение информационной безопасности* входит в вариативную часть образовательной программы магистратуры по направлению 09.04.03 Прикладная информатика.

Для успешного освоения данного курса студент должен иметь знания по курсу «Информационное общество и проблемы прикладной информатики». Освоение данной дисциплины необходимо как предшествующее при изучении следующих профессиональных дисциплин: «Техническая защита информации», «Управление информационной безопасностью».

3. Компетенции обучающегося, формируемые в результате освоения дисциплины (перечень планируемых результатов обучения).

Компетенции	Формулировка компетенции из ФГОС ВО	Планируемые результаты обучения (показатели достижения заданного уровня освоения компетенций)
ОК-3	Готовность к саморазвитию, самореализации, использованию творческого потенциала	<p>Знать: понятия «самостоятельная работа студентов», «самоорганизация», «самоконтроль», «самообразование»; формы, технологии организации самостоятельной работы; пути достижения образовательных результатов и способы оценки результатов обучения; виды, формы контроля успеваемости в вузе.</p> <p>Уметь: системно анализировать, обобщать информацию, формулировать цели и самостоятельно находить пути их достижения; использовать в образовательном процессе разнообразные ресурсы; работать самостоятельно и в коллективе, руководить людьми и подчинять личные интересы общей цели; формулировать результат; публично представить собственные и известные научные результаты.</p>

		<p>Владеть: способностью к самоорганизации и к самообразованию; навыками самостоятельной научно - исследовательской работы; способностью формулировать результат.</p>
ОПК-1	Способность к коммуникации в устной и письменной формах на русском и иностранном языках для решения задач профессиональной деятельности	<p>Знать: основные нормативные правовые документы; особенности правового регулирования будущей профессиональной деятельности; значение законности и правопорядка в современном обществе.</p> <p>Уметь: отыскивать необходимые нормативные правовые акты и информационно-правовые нормы в системе действующего законодательства, в том числе с помощью систем правовой информации; применять действующую законодательную базу в области информационной безопасности; разрабатывать проекты нормативных материалов, регламентирующих работу по защите информации, а также положений, инструкций и других организационно-распорядительных документов; применять нормативные правовые акты и нормативные методические документы в области обеспечения информационной безопасности; разрабатывать проекты нормативных и организационно-распорядительных документов, регламентирующих работу по защите информации.</p> <p>Владеть: навыками адекватного реагирования в ситуациях бытового, академического и профессионального общения; навыками поиска нестандартных решений, участвовать в принятии решений, брать на себя ответственность за их последствия; способностью осуществлять действия и поступки на основе выбранных целей.</p>
ОПК-2	Способен руководить коллективом в сфере своей профессиональной	<p>Знать: навыки готовности руководить коллективом в сфере своей профессиональной деятельности, толерантно воспринимая социальные, этнические,</p>

	деятельности, толерантно воспринимаемая социальные, этнические, конфессиональные и культурные различия	<p>конфессиональные и культурные различия.</p> <p>Уметь: использовать знание навыками готовности руководить коллективом в сфере своей профессиональной деятельности, толерантно воспринимаемая социальные, этнические, конфессиональные и культурные различия.</p> <p>Владеть: навыками готовности руководить коллективом в сфере своей профессиональной деятельности, толерантно воспринимаемая социальные, этнические, конфессиональные и культурные различия.</p>
--	--	--

4. Объем, структура и содержание дисциплины.

4.1. Объем дисциплины составляет 5 зачетных единиц, 180 академических часов.

4.2. Структура дисциплины.

№ п/п	Разделы и темы дисциплины	Семестр	Неделя семестра	Виды учебной работы, включая самостоятельную работу студентов и трудоемкость (в часах)				Самостоятельная работа	Формы текущего контроля успеваемости (по неделям семестра) Форма промежуточной аттестации (по семестрам)
				Лекции	Практ-е зан.	Контроль	КСР		
1	2	3	4	5	6	7	8	9	10
Модуль 1. Направления государственное политики и правового регулирования в сфере информационной безопасности									
1.	Основные положения информационной безопасности.	A	1	2			1		
		A	2		2			1	Устный опрос
		A	3		2			1	Письменный опрос
2.	Направления государственной политики России в информационной сфере и сфере информационной безопасности.	A	4	2			1		
		A	5		2			1	Устный опрос
		A	6		2			1	Письменный опрос
3.	Государственная система правового регулирования в области информационной безопасности.	A	7	2			1		
		A	8		2			1	Устный опрос
		A	9		2			1	Письменный опрос

4.	Государственное регулирование деятельности по лицензированию и сертификации в области информационной безопасности.	A	10	2			1		
		A	11		2			4	Мини-конференция
	<i>Итого по модулю 1:</i>	A		8	14		4	10	
	ИТОГО:	A		8	14		4	10	Зачет
1	2	3	4	5	6	7	8	9	10
Модуль 2. Законодательная база правового регулирования в информационной сфере и сфере информационной безопасности									
1.	Законодательная база правового регулирования в информационной сфере и сфере информационной безопасности.	B	1	2			1		
		B	2		4			6	Устный и письменный опрос
		B	3		2			6	Практические задания
		B	4		4			11	Контрольная работа
	<i>Итого по модулю 2:</i>			2	10		1	23	
Модуль 3. Законодательство РФ в сфере информационной безопасности и интеллектуальной собственности									
1.	Законодательство об интеллектуальной собственности. Юридическая ответственность за нарушения правовых норм в области информационной безопасности.	B	5	2			1		
		B	6		4			6	Устный и письменный опрос
		B	7		2			6	Практические задания
		B	8		4			11	Коллоквиум
	<i>Итого по модулю 3:</i>			2	10		1	23	
Модуль 4. Организационное обеспечение защиты информации									
1.	Организация допуска и доступа персонала к конфиденциальной информации. Организация внутриобъектового и пропускного режимов на предприятии.	B	9	2			2		
			10		4			2	Устный и письменный опрос
		B	11		2			2	Практические задания
2.	Организация защиты информации при проведении конфиденциальных совещаний, в ходе издательской, рекламной деятельности и представлении ее в средствах массовой информации. Основы организации защиты	B	12	2	2			2	Устный опрос
			13		2			2	Письменный опрос
		B	14		4			2	Устный и письменный опрос
		B	15		2			4	Мини-конференция

	информации при осуществлении международного сотрудничества и выезде персонала предприятия за границу.								
	<i>Итого по модулю 4:</i>			4	16		2	14	
	Модуль 5. Подготовка к экзамену								
	<i>Подготовка к экзамену</i>					36			
	ИТОГО:	В		8	36	36	4	60	Экзамен

4.3. Содержание дисциплины, структурированное по темам (разделам).

Модуль 1. Направления государственной политики и правового регулирования в сфере информационной безопасности

Тема 1. Основные положения информационной безопасности

Исторический очерк о возникновении органов защиты информации. Концептуальные основы информационной безопасности. Основные понятия, виды и источники информации, подлежащей защите. Угрозы, вероятные каналы утечки конфиденциальной информации: причины возникновения, характеристики, классификация.

Понятие и место информационной безопасности в системе национальной безопасности России. Содержание и функции организационного и правового регулирования информационной безопасности и ее место в системе комплексной защиты информации. Отнесение сведений к конфиденциальной информации, засекречивание и рассекречивание сведений.

Тема 2. Направления государственной политики России в информационной сфере и сфере информационной безопасности

Защита интересов личности, общества и государства в информационной сфере. Направления государственной политики Российской Федерации в сфере информатизации и информационной безопасности. Основы государственной политики российской федерации в области международной информационной безопасности на период до 2020 года. Основные направления защиты интересов личности, общества и государства в информационной сфере. Пути развития правовой информатизации и информационной безопасности. Концепция правовой информатизации Российской Федерации как основа информационной безопасности личности, общества, государства.

Тема 3. Государственная система правового регулирования в области информационной безопасности

Формирование государственной системы правового регулирования информационной безопасности в Российской Федерации. Международный опыт и правовое регулирование информационной безопасности при международном сотрудничестве. Источники нормативно-правового регулирования при международном информационном обмене. Порядок международно-правового регулирования информационной безопасности: классификация и определение источников опасности при международном информационном обмене; меры по обеспечению информационной безопасности РФ в сфере международного информационного обмена

Тема 4. Государственное регулирование деятельности по лицензированию и сертификации в области информационной безопасности

Система лицензирования в области защиты конфиденциальной информации. Система сертификации средств защиты информации. Особенности сертификации средств защиты информации по требованиям безопасности.

Аккредитация испытательных лабораторий и органов сертификации средств защиты информации. Аттестация объектов информатизации по требованиям безопасности информации.

Модуль 2. Законодательная база правового регулирования в информационной сфере и сфере информационной безопасности

Тема 5. Законодательная база правового регулирования в информационной сфере и сфере информационной безопасности

Классификация и структура нормативных правовых актов по информационной безопасности. Основные нормы Конституции РФ и ГК РФ о правах и обязанностях граждан России в сфере информационной безопасности. Основное содержание законов Российской Федерации в сфере информационной безопасности.

Модуль 3. Законодательство РФ в сфере информационной безопасности и интеллектуальной собственности

Тема 6. Законодательство об интеллектуальной собственности. Юридическая ответственность за нарушения правовых норм в области информационной безопасности

Защита интеллектуальной собственности в системе правового регулирования информационной безопасности. Основные положения патентного права. Законодательство о ноу-хау. Особенности договорных отношений. Особенности трудовых соглашений.

Понятие и виды юридической ответственности за нарушение правовых норм в области информационной безопасности. Уголовная ответственность за нарушения правовых норм в сфере информационной безопасности. Административная ответственность за нарушения правовых норм в сфере информационной безопасности. Особенности юридической ответственности за нарушение правовых норм информационной безопасности в области трудовых и гражданско-правовых отношений. Проведение административного расследования по фактам нарушения установленного порядка обеспечения информационной безопасности.

Модуль 4. Организационное обеспечение защиты информации

Тема 7. Организация допуска и доступа персонала к конфиденциальной информации. Организация внутриобъектового и пропускного режимов на предприятии

Основные принципы и условия организационной защиты информации. Основные подходы и требования к организации системы защиты информации. Основные силы и средства, используемые для организации защиты информации. Организационные структуры государственной системы обеспечения информационной безопасности федеральных органов исполнительной власти. Организационные структуры системы обеспечения информационной безопасности предприятия (организации). Физическая защита.

Основные положения допуска персонала предприятия к конфиденциальной информации. Порядок оформления и переоформления допуска к государственной тайне. Формы допуска. Основания для отказа должностному лицу или гражданину в допуске к государственной тайне и условия прекращения допуска. Организация доступа персонала предприятия к сведениям, составляющим государственную тайну. Порядок доступа к конфиденциальной информации командированных лиц. Основные направления и методы работы с персоналом предприятия, допущенным к конфиденциальной информации.

Роль и место внутриобъектового и пропускного режимов в общей системе защиты информации на предприятии. Основные цели, подходы и принципы организации внутриобъектового режима. Силы и средства, используемые при организации внутриобъектового режима. Цели и задачи пропускного режима. Основные элементы системы организации пропускного режима, используемые силы и средства. Организация охраны предприятия.

Тема 8. Организация защиты информации при проведении конфиденциальных совещаний, в ходе издательской, рекламной деятельности и представлении ее в средствах массовой информации. Основы организации защиты информации при осуществлении международного сотрудничества и выезде персонала предприятия за границу

Планирование мероприятий по защите информации при подготовке к проведению совещания. Организация допуска участников совещания к обсуждаемым вопросам. Подготовка места проведения совещания. Порядок проведения совещания и использования его материалов. Основы организации защиты информации в ходе издательской и рекламной деятельности. Организация подготовки материалов к открытому опубликованию. Основы организации защиты информации в ходе взаимодействия со средствами массовой информации.

Порядок передачи различных видов конфиденциальной информации иностранным государствам. Организация подготовки к передаче сведений, составляющих государственную тайну, другим государствам. Ограничения прав гражданина, осведомленного в сведениях, составляющих государственную тайну, на выезд за границу. Работа должностных лиц предприятия по оформлению документов на выезд сотрудников в служебные командировки и по частным делам. Организация аналитической работы и контроля состояния и защиты конфиденциальной информации. Организация и проведение слу-

жебного расследования в случае разглашения сведений конфиденциального характера или утраты носителей сведений.

Практические занятия

Модуль 1. Направления государственной политики и правового регулирования в сфере информационной безопасности

Тема 1. Основные положения информационной безопасности (4 часа)

1. Исторический очерк о возникновении органов защиты информации.
2. Концептуальные основы информационной безопасности.
3. Основные понятия, виды и источники информации, подлежащей защите.
4. Угрозы, вероятные каналы утечки конфиденциальной информации: причины возникновения, характеристики, классификация.
5. Понятие и место информационной безопасности в системе национальной безопасности России.
6. Содержание и функции организационного и правового регулирования информационной безопасности и ее место в системе комплексной защиты информации.
7. Отнесение сведений к конфиденциальной информации, засекречивание и рассекречивание сведений.

Тема 2. Направления государственной политики России в информационной сфере и сфере информационной безопасности (4 часа)

1. Защита интересов личности, общества и государства в информационной сфере.
2. Направления государственной политики Российской Федерации в сфере информатизации и информационной безопасности.
3. Основы государственной политики российской федерации в области международной информационной безопасности на период до 2020 года.
4. Основные направления защиты интересов личности, общества и государства в информационной сфере.
5. Пути развития правовой информатизации и информационной безопасности.
6. Концепция правовой информатизации Российской Федерации как основа информационной безопасности личности, общества, государства.

Тема 3. Государственная система правового регулирования в области информационной безопасности (4 часа)

1. Формирование государственной системы правового регулирования информационной безопасности в Российской Федерации.
2. Международный опыт и правовое регулирование информационной безопасности при международном сотрудничестве.
3. Источники нормативно-правового регулирования при международном информационном обмене.

4. Порядок международно-правового регулирования информационной безопасности: классификация и определение источников опасности при международном информационном обмене; меры по обеспечению информационной безопасности РФ в сфере международного информационного обмена

Тема 4. Государственное регулирование деятельности по лицензированию и сертификации в области информационной безопасности (2 часа)

1. Система лицензирования в области защиты конфиденциальной информации.

2. Система сертификации средств защиты информации.

3. Особенности сертификации средств защиты информации по требованиям безопасности.

4. Аккредитация испытательных лабораторий и органов сертификации средств защиты информации.

5. Аттестация объектов информатизации по требованиям безопасности информации.

Модуль 2. Законодательная база правового регулирования в информационной сфере и сфере информационной безопасности

Тема 5. Законодательная база правового регулирования в информационной сфере и сфере информационной безопасности (10 часов)

1. Классификация и структура нормативных правовых актов по информационной безопасности.

2. Основные нормы Конституции РФ и ГК РФ о правах и обязанностях граждан России в сфере информационной безопасности.

3. Основное содержание законов Российской Федерации в сфере информационной безопасности.

Модуль 3. Законодательство РФ в сфере информационной безопасности и интеллектуальной собственности

Тема 6. Законодательство об интеллектуальной собственности. Юридическая ответственность за нарушения правовых норм в области информационной безопасности (10 часов)

1. Защита интеллектуальной собственности в системе правового регулирования информационной безопасности.

2. Основные положения патентного права.

3. Законодательство о ноу-хау.

4. Особенности договорных отношений.

5. Особенности трудовых соглашений.

6. Понятие и виды юридической ответственности за нарушение правовых норм в области информационной безопасности.

7. Уголовная ответственность за нарушения правовых норм в сфере информационной безопасности.

8. Административная ответственность за нарушения правовых норм в сфере информационной безопасности.

9. Особенности юридической ответственности за нарушение правовых норм информационной безопасности в области трудовых и гражданско-правовых отношений.

10. Проведение административного расследования по фактам нарушения установленного порядка обеспечения информационной безопасности.

Модуль 4. Организационное обеспечение защиты информации

Тема 7. Организация допуска и доступа персонала к конфиденциальной информации. Организация внутриобъектового и пропускного режимов на предприятии (6 часов)

1. Основные принципы и условия организационной защиты информации.

2. Основные подходы и требования к организации системы защиты информации.

3. Основные силы и средства, используемые для организации защиты информации.

4. Организационные структуры государственной системы обеспечения информационной безопасности федеральных органов исполнительной власти.

5. Организационные структуры системы обеспечения информационной безопасности предприятия (организации). Физическая защита.

6. Основные положения допуска персонала предприятия к конфиденциальной информации.

7. Порядок оформления и переоформления допуска к государственной тайне. Формы допуска.

8. Основания для отказа должностному лицу или гражданину в допуске к государственной тайне и условия прекращения допуска.

9. Организация доступа персонала предприятия к сведениям, составляющим государственную тайну.

10. Порядок доступа к конфиденциальной информации командированных лиц.

11. Основные направления и методы работы с персоналом предприятия, допущенным к конфиденциальной информации.

12. Роль и место внутриобъектового и пропускного режимов в общей системе защиты информации на предприятии.

13. Основные цели, подходы и принципы организации внутриобъектового режима.

14. Силы и средства, используемые при организации внутриобъектового режима.

15. Цели и задачи пропускного режима.

16. Основные элементы системы организации пропускного режима, используемые силы и средства.

17. Организация охраны предприятия.

Тема 8. Организация защиты информации при проведении конфиденциальных совещаний, в ходе издательской, рекламной деятельности и представлении ее в средствах массовой информации. Основы организации защиты информации при осуществлении международного сотрудничества и выезде персонала предприятия за границу (10 часов)

1. Планирование мероприятий по защите информации при подготовке к проведению совещания.
2. Организация допуска участников совещания к обсуждаемым вопросам.
3. Подготовка места проведения совещания.
4. Порядок проведения совещания и использования его материалов.
5. Основы организации защиты информации в ходе издательской и рекламной деятельности.
6. Организация подготовки материалов к открытому опубликованию.
7. Основы организации защиты информации в ходе взаимодействия со средствами массовой информации.
8. Порядок передачи различных видов конфиденциальной информации иностранным государствам.
9. Организация подготовки к передаче сведений, составляющих государственную тайну, другим государствам.
10. Ограничения прав гражданина, осведомленного в сведениях, составляющих государственную тайну, на выезд за границу.
11. Работа должностных лиц предприятия по оформлению документов на выезд сотрудников в служебные командировки и по частным делам.
12. Организация аналитической работы и контроля состояния и защиты конфиденциальной информации.
13. Организация и проведение служебного расследования в случае разглашения сведений конфиденциального характера или утраты носителей сведений.

5. Образовательные технологии

В соответствии с требованиями ФГОС ВО по направлению подготовки в рамках изучения данной дисциплины для реализации компетентностного подхода предусмотрено все проводимые занятия, в том числе самостоятельная работа магистранта, сочетать передовые методические приемы с новыми образовательными информационными технологиями и достижениями науки и техники.

№ п/п	Вид учебной работы	Образовательные технологии
1.	Лекции	<ul style="list-style-type: none">• Вводная лекция• Лекция-информация с визуализацией• Проблемная лекция
2.	Практические занятия	<ul style="list-style-type: none">• Семинар-дискуссия, семинар-дебаты по актуальным проблемам информационной безопасности• Выполнение практических работ• Решение проблемных ситуаций из области информационной безопасности• Семинар-конференция по студенческим докладам и эссе• Имитационные (ситуативные) технологии• Проектные технологии• Ролевые игры• Технология учебного исследования
3.	Самостоятельная работа	<ul style="list-style-type: none">• Письменные и устные домашние задания• Консультации преподавателя• Поиск и анализ информации в справочных правовых системах и сети Интернет• Внеаудиторная работа студентов (освоение теоретического материала, подготовка к семинарским занятиям, выполнение домашних заданий, выполнение творческой работы, работа с электронным учебно-методическим комплексом, подготовка к текущему и итоговому контролю)
4.	Контроль	<ul style="list-style-type: none">• Выступление на семинарах• Выполнение практических заданий• Защита рефератов• Устный опрос• Письменный опрос

6. Учебно-методическое обеспечение самостоятельной работы студентов.

Самостоятельная работа – вид индивидуальной деятельности магистранта, основанный на собственных познавательных ресурсах. Целью самостоятельной работы магистрантов является обучение навыкам работы с научной литературой и практическими материалами, необходимыми для углубленного изучения курса наследственного права, а также развитие у них устойчивых способностей к самостоятельному (без помощи преподавателя) изучению и изложению полученной информации. В связи с этим основными задачами самостоятельной работы магистрантов, изучающих дисциплину «*Организационные и правовые основы информационной безопасности*», являются:

- во-первых, продолжение изучения дисциплины в домашних условиях по программе, предложенной преподавателем;
- во-вторых, привитие магистрантам интереса к юридической литературе, правотворческому процессу.

Изучение и изложение информации, полученной в результате изучения научной литературы и практических материалов, предполагает развитие у магистрантов как владения навыками устной речи, так и способностей к четкому письменному изложению материала.

Виды и порядок выполнения самостоятельной работы:

№ п/п	Вид самостоятельной работы	Вид контроля	Учебно-методическое обеспечение
1.	Подготовка реферата (до 5 страниц), презентации и доклада (7-10 минут)	Прием реферата, презентации, доклада и оценка качества их исполнения на мини-конференции	См. приложение А данного документа
2.	Освоение теоретического материала	Устный и письменный опрос	См. приложение А данного документа
3.	Подготовка к практическим занятиям	Практические задания	См. приложение А данного документа
4.	Подготовка к текущему контролю	Контрольная работа. Коллоквиум	См. приложение А данного документа
5.	Подготовка к экзамену	Промежуточная аттестация в форме экзамена.	См. приложение А данного документа

Нормативно-правовые акты

1. Конституция Российской Федерации (принята всенародным голосованием 12.12.1993) (с учетом поправок, внесенных Законами Российской Федерации о поправках к Конституции Российской Федерации от 30.12.2008 N 6-ФКЗ, от 30.12.2008 N 7-ФКЗ, от 05.02.2014 N 2-ФКЗ, от 21.07.2014 N 11-ФКЗ).

2. Федеральный конституционный закон от 17.12.1997 № 2-ФКЗ «О Правительстве Российской Федерации» (ред. от 12.03.2014).
3. Федеральный закон от 02.12.1990 № 395-1 (ред. от 21.07.2014) «О банках и банковской деятельности».
4. Закон Российской Федерации от 27.12.1991 № 2124-1 (ред. от 02.07.2013) «О средствах массовой информации» (с изм. и доп., вступившими в силу с 01.09.2013).
5. Закон Российской Федерации от 11.03.1992 №2487-1 (ред. от 23.06.2014, изм. от 21.07.2014) «О частной детективной и охранной деятельности в Российской Федерации».
6. Закон Российской Федерации от 21.07.1993 № 5485-1 (ред. от 21.12.2013) «О государственной тайне».
7. Федеральный закон от 13.01.1995 № 7-ФЗ (ред. от 12.03.2014) «О порядке освещения деятельности органов государственной власти в государственных средствах массовой информации».
8. Федеральный закон от 03.04.1995 № 40-ФЗ (ред. от 28.06.2014) «О Федеральной службе безопасности».
9. Федеральный закон от 15.07.1995 № 101-ФЗ (ред. от 12.03.2014) «О международных договорах Российской Федерации».
10. Федеральный закон от 12.08.1995 № 144-ФЗ (ред. от 21.03.13) «Об оперативно-розыскной деятельности».
11. Федеральный закон от 10.01.1996 № 5-ФЗ (ред. от 08.12.2011) «О внешней разведке».
12. Федеральный закон от 15.08.1996 № 114-ФЗ (ред. от 20.04.2014, с изм. от 04.06.2014) «О порядке выезда из Российской Федерации и въезда в Российскую Федерацию».
13. Федеральный закон от 14.04.1999 № 77-ФЗ (ред. от 21.07.2014) «О ведомственной охране».
14. Федеральный закон от 27.07.2004 № 79-ФЗ (ред. от 02.04.2014) «О государственной гражданской службе Российской Федерации».
15. Федеральный закон от 29.07.2004 № 98-ФЗ (ред. от 11.07.2011) «О коммерческой тайне».
16. Федеральный закон от 13.03.2006 № 38-ФЗ (ред. от 21.07.2014) «О рекламе» (с изм. и доп., в силу с 06.08.2014).
17. Федеральный закон от 27.07.2006 № 149-ФЗ (ред. от 21.07.2014) «Об информации, информационных технологиях и о защите информации».
18. Федеральный закон от 27.07.2006 № 152-ФЗ (ред. от 04.06.2014) «О персональных данных».
19. Федеральный закон от 04.05.2011 № 99-ФЗ (ред. от 21.07.2014) «О лицензировании отдельных видов деятельности».
20. Гражданский кодекс Российской Федерации (часть первая) от 30.11.1994 § № 51-ФЗ (ред. от 05.05.2014) (с изм. и доп., вступ. в силу с 01.09.2014).

21. Гражданский кодекс Российской Федерации (часть вторая) от 26.01.1996 № 14-ФЗ (ред. от 21.07.2014) (с изм. и доп., вступ. в силу с 01.10.2014).

22. Уголовный кодекс Российской Федерации от 13.06.1996 № 63-ФЗ (ред. от 21.07.2014) (с изм. и доп., вступ. в силу с 04.08.2014).

23. Налоговый кодекс Российской Федерации (часть первая) от 31.07.1998 № 146-ФЗ (ред. от 28.06.2014).

24. Уголовно-процессуальный кодекс Российской Федерации от 18.12.2001 № 174-ФЗ (ред. от 21.07.2014) (с изм. и доп., вступ. в силу с 06.08.2014).

25. Кодекс Российской Федерации об административных правонарушениях от 30.12.2001 № 195-ФЗ (ред. от 21.07.2014) (с изм. и доп., вступ. в силу с 06.08.2014).

26. Трудовой кодекс Российской Федерации от 30.12.2001 № 197-ФЗ (ред. от 28.06.2014).

27. «Арбитражный процессуальный кодекс Российской Федерации» от 24.07.2002 № 95-ФЗ (ред. от 28.06.2014).

28. Гражданский процессуальный кодекс Российской Федерации от 14.11.2002 № 138-ФЗ (ред. от 21.07.2014) (с изм. и доп., вступ. в силу с 06.08.2014).

29. Гражданский кодекс Российской Федерации (часть четвертая) от 18.12.2006 № 230-ФЗ (ред. от 12.03.2014).

30. Указ Президента РФ от 30.11.1995 № 1203 (ред. от 01.09.2014) «Об утверждении Перечня сведений, отнесенных к государственной тайне».

31. Указ Президента РФ от 06.03.1997 № 188 (ред. от 23.09.2005) «Об утверждении Перечня сведений конфиденциального характера».

32. Указ Президента РФ от 11.08.2003 № 960 (ред. от 07.03.2014) «Вопросы Федеральной службы безопасности Российской Федерации».

33. Указ Президента РФ от 11.07.2004 № 865 (ред. от 21.12.2013) «Вопросы Министерства иностранных дел Российской Федерации».

34. Указ Президента РФ от 16.08.2004 № 1082 (ред. от 12.6.2014) «Вопросы Министерства обороны Российской Федерации».

35. Указ Президента РФ от 16.08.2004 № 1085 (ред. от 01.9.2014) «Вопросы Федеральной службы по техническому и экспортному контролю» (Выписка).

36. Указ Президента РФ от 06.10.2004 № 1286 (ред. от 11.08.2014) «Вопросы Межведомственной комиссии по защите государственной тайны».

37. Указ Президента РФ от 26.02.2009 № 228 (ред. от 11.08.2014) «Вопросы Межведомственной комиссии по защите государственной тайны».

38. Указ Президента РФ от 12.05.2009 № 537 (ред. от 01.07.2014) «О Стратегии национальной безопасности Российской Федерации до 2020 года».

39. Доктрина информационной безопасности Российской Федерации (утверждена Президентом РФ 09.09.2000 № Пр-1895).

40. Распоряжение Президента РФ от 16.04.2005 № 151-рп (ред. от 27.06.2014) «О перечне должностных лиц органов государственной власти и организаций, наделяемых полномочиями по отнесению сведений к государственной тайне».

41. Постановление Правительства РСФСР от 05.12.1991 № 35 (ред. от 03.10.2002) «О перечне сведений, которые не могут составлять коммерческую тайну».

42. Постановление Правительства РФ от 03.11.1994 № 1233 (ред. от 20.07.2012) «Об утверждении Положения о порядке обращения со служебной информацией ограниченного распространения в федеральных органах исполнительной власти».

43. Постановление Правительства РФ от 20.02.1995 № 170 (ред. от 07.09.2011) «Об установлении порядка рассекречивания и продления сроков засекречивания архивных документов Правительства СССР».

44. Постановление Правительства РФ от 15.04.1995 № 333 (ред. от 05.05.2012) «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».

45. Постановление Правительства РФ от 04.09.1995 № 870 (ред. от 22.05.2008) «Об утверждении Правил отнесения сведений, составляющих государственную тайну, к различным степеням секретности».

46. Постановление Правительства РФ от 02.08.1997 № 973 (ред. от 06.04.2013) «Об утверждении Положения о подготовке к передаче сведений, составляющих государственную тайну, другим государствам или Международным организациям».

47. Постановление Правительства РФ от 01.06.2004 № 260 (ред. от 30.07.2014) «О Регламенте Правительства Российской Федерации и Положении об Аппарате Правительства Российской Федерации».

48. Постановление Правительства РФ от 30.06.2004 № 331 (ред. от 26.08.2014) «Об утверждении Положения о Федеральной антимонопольной службе».

49. Постановление Правительства РФ от 18.09.2006 № 573 (ред. от 25.03.2013) «О предоставлении социальных гарантий гражданам, допущенным к государственной тайне на постоянной основе, и сотрудникам структурных подразделений по защите государственной тайны» (вместе с «Правилами выплаты ежемесячных процентных надбавок к должностному окладу (тарифной ставке) граждан, допущенных к государственной тайне на постоянной основе, и сотрудников структурных подразделений по защите государственной тайны»).

50. Постановление Правительства РФ от 06.02.2010 № 63 (ред. от 01.11.2012) «Об утверждении Инструкции о порядке допуска должностных лиц и граждан Российской Федерации к государственной тайне».

51. Приказ Минздравсоцразвития РФ от 26.08.2011 N 989н «Об утверждении перечня медицинских противопоказаний для работы с использованием сведений, составляющих государственную тайну, порядка получения и формы справки об отсутствии медицинских противопоказаний для работы с использованием сведений, составляющих государственную тайну» (Зарегистрировано в Минюсте РФ 11.10.2011 N 22016).

52. «Защита информации. Основные термины и определения. ГОСТ Р 509222006» (утв. Приказом Ростехрегулирования от 27.12.2006 № 373-ст).

Примеренная тематика рефератов

1. Информация как объект правовой защиты.
2. Виды защищаемой информации и правовые основы ее защиты.
3. Государственная политика в области информатизации и обеспечения информационной безопасности российского государства.
4. Нормативно-правовое регулирование вопросов информационной безопасности.
5. Предмет и метод информационного права.
6. Способы и формы правовой защиты информации.
7. Информационные права и свободы граждан и их ограничения.
8. Право граждан Российской Федерации на неприкосновенность частной жизни.
9. Персональные данные как институт охраны права на неприкосновенность частной жизни.
10. Тайна как социальное и правовое явление.
11. Правовая защита государственной тайны Российской Федерации.
12. Органы защиты государственной тайны.
13. Лицензирование предприятий, работающих с государственными секретами.
14. Правовые аспекты проблемы оценки ущерба наносимого безопасности Российской Федерации следствии несанкционированного (противоправного) распространения информации, составляющей государственную тайну.
15. Ответственность, установленная за неправомерное обращение со сведениями, составляющими государственную тайну.
16. Проблемы формирования института коммерческой тайны.
17. Особенности правовой охраны и защиты коммерческой тайны.
18. Институт банковской тайны.
19. Сущность банковской тайны и отличие от иных видов тайн.
20. Проблемы формирования института кредитных историй.
21. Тайна переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений.
22. Институт врачебной тайны.
23. Институт адвокатской тайны.
24. Правовая охрана и защита нотариальной тайны.
25. Правовая охрана и защита страховой тайны.

26. Правовая охрана и защита аудиторской тайны.
27. Проблемы формирования института служебной тайны.
28. Тайны в ходе предварительного расследования
29. Тайны в ходе осуществления судопроизводства.
30. Институт налоговой тайны.
31. Лицензирование при осуществлении деятельности по защите информации.
32. Правовое регулирование деятельности служб безопасности на предприятии.
33. Правовые основы деятельности подразделений защиты информации на предприятии.
34. Правовое регулирование деятельности средств массовой информации.
35. Система правовой ответственности за утечку информации и утрату носителей информации.
36. Правовое регулирование взаимоотношений администрации и персонала в области защиты информации.
37. Виды и условия применения правовых норм уголовной ответственности за разглашение защищаемой информации и невыполнение правил ее защиты.
38. Виды и условия применения правовых норм гражданско-правовой ответственности за разглашение защищаемой информации и невыполнение правил ее защиты.
39. Виды и условия применения правовых норм административной и дисциплинарной ответственности за разглашение защищаемой информации и невыполнение правил ее защиты.
40. Правовое регулирование оперативно-розыскной деятельности.
41. Правовое регулирование разведывательной и контрразведывательной деятельности.

7. Фонд оценочных средств для проведения текущего контроля успеваемости, промежуточной аттестации по итогам освоения дисциплины.

7.1. Перечень компетенций с указанием этапов их формирования в процессе освоения образовательной программы.

Перечень компетенций с указанием этапов их формирования приведен в описании образовательной программы.

Компетенция	Знания, умения, навыки	Процедура освоения
ОК-3	Знать: пути достижения образовательных результатов и способы оценки результатов обучения. Уметь: системно анализировать, обобщать информацию, формулировать цели и самостоятельно находить	Устный опрос, письменный опрос, Мини-конференция

	<p>пути их достижения; использовать в образовательном процессе разнообразные ресурсы; работать самостоятельно и в коллективе, руководить людьми и подчинять личные интересы общей цели; формулировать результат; публично представить собственные и известные научные результаты.</p> <p>Владеть: способностью к самоорганизации и к самообразованию; навыками самостоятельной научно - исследовательской работы; способностью формулировать результат.</p>	
ОПК-1	<p>Знать: основные нормативные правовые документы; особенности правового регулирования будущей профессиональной деятельности; значение законности и правопорядка в современном обществе.</p>	<p>Устный опрос, письменный опрос, Мини-конференция</p>
ОПК-1	<p>Уметь: отыскивать необходимые нормативные правовые акты и информационно-правовые нормы в системе действующего законодательства, в том числе с помощью систем правовой информации; применять действующую законодательную базу в области информационной безопасности; разрабатывать проекты нормативных материалов, регламентирующих работу по защите информации, а также положений, инструкций и других организационно-распорядительных документов; применять нормативные правовые акты и нормативные методические документы в области обеспечения информационной безопасности; разрабатывать проекты нормативных и организационно-распорядительных документов, регламентирующих работу по защите информации.</p>	<p>Практические задания, письменный опрос, Мини-конференция.</p>
ОПК-1	<p>Владеть: навыками адекватного реагирования в ситуациях бытового, ака-</p>	<p>Устный опрос, письменный опрос,</p>

	демического и профессионального общения; навыками поиска нестандартных решений, участвовать в принятии решений, брать на себя ответственность за их последствия; способностью осуществлять действия и поступки на основе выбранных целей.	Мини-конференция
ОПК-2	Знать: навыки готовности руководить коллективом в сфере своей профессиональной деятельности, толерантно воспринимая социальные, этнические, конфессиональные и культурные различия.	Устный опрос, письменный опрос, Мини-конференция
ОПК-2	Уметь: использовать знание навыками готовности руководить коллективом в сфере своей профессиональной деятельности, толерантно воспринимая социальные, этнические, конфессиональные и культурные различия.	Устный опрос, письменный опрос, Мини-конференция, Коллоквиум
ОПК-2	Владеть: навыками готовности руководить коллективом в сфере своей профессиональной деятельности, толерантно воспринимая социальные, этнические, конфессиональные и культурные различия.	Устный опрос, письменный опрос, Мини-конференция, Коллоквиум

7.2. Контрольные задания

Контрольные вопросы к зачету и экзамену

1. Что понимается под информацией, подлежащей защите?
2. Назовите категории источников, содержащих конфиденциальную информацию.
3. Назовите возможные пути получения информации злоумышленником.
4. Что является причинами разглашения конфиденциальной информации?
5. Назовите факторы и обстоятельства, приводящие к утечке информации.
6. Назовите причины разглашения конфиденциальной информации.
7. Назовите особенности информации как объекта права собственности.
8. Дайте определение понятия информации как объекта правоотношений.
9. Дайте определение понятия информационной безопасности.

10. Что понимается под информационными угрозами личности, обществу и государству?
11. Назовите основные пути реализации угроз информационным ресурсам и безопасности информации.
12. Назовите основные виды потерь, связанных с угрозами безопасности информации.
13. Определите значение информационной безопасности в системе национальной безопасности Российской Федерации.
14. Назовите классификацию способов и средств защиты информации.
15. Дайте определение понятий методов, форм и средств обеспечения информационной безопасности.
16. Назовите интересы личности, государства, общества в информационной сфере. В чем выражается их защита?
17. Назовите основные направления деятельности государства и принципы обеспечения ИБ.
18. Проанализируйте проблемы и особенности организационного и социально-экономического компонентов процесса правовой информатизации.
19. Каковы особенности научно-технического компонента процесса правовой информатизации?
20. Назовите задачи разработки концепции правовой информатизации субъекта Российской Федерации.
21. Назовите основные нормативные документы, регламентирующие положение доступа к государственным информационным ресурсам.
22. Понятие информации и информационных ресурсов, их соотношение.
23. Понятие правового режима информации.
24. В отношении какой категории сведений устанавливается режим защиты информации?
25. Назовите субъекты, которые обеспечивают защиту государственных информационных ресурсов?
26. Соотношение принципов правового обеспечения информационной безопасности.
27. Направления деятельности государства по защите информационных ресурсов.
28. Охарактеризуйте структуру законодательной базы по вопросам информационной безопасности.
29. Что закрепляет Конституция РФ и ГК РФ о правах, обязанности граждан России в сфере информационной безопасности?
30. Раскройте содержание Закона о государственной тайне.
31. Раскройте основное содержание Закона об информации.
32. Назовите цели принятия Федерального закона «О коммерческой тайне».
33. Охарактеризуйте законодательство РФ по информационной безопасности в области международного сотрудничества.

34. Каковы отличительные особенности определения понятия интеллектуальной собственности?
35. Способы защиты интеллектуальной собственности.
36. Какова структура и содержание законодательства об интеллектуальной собственности?
37. К какой отрасли права относится авторское право?
38. Каково содержание законодательства об авторском праве и смежных правах?
39. Содержание объекта, субъекты авторского права.
40. Какую ответственность может понести нарушитель авторского права?
41. Что входит в структуру законодательства о правовой охране программ для ЭВМ и баз данных?
42. Каковы отличительные особенности правовой охраны элементов вычислительной техники?
43. Что относится к основным объектам промышленной собственности?
44. В чем сущность показателей патентоспособности объектов промышленной собственности?
45. Каково содержание формулы изобретения?
46. Каковы механизмы патентной защиты?
47. Какие существуют типы договоров и место в нем договоров в области защиты информации?
48. Каково содержание и порядок заключения (расторжения) договора?
49. Каковы особенности трудовых соглашений в области защиты информации?
50. Охарактеризуйте структуру системы государственного лицензирования деятельности в области защиты информации.
51. Назовите полномочия органов государственного лицензирования по защите информации.
52. Назовите нормативные правовые акты по сертификации средств защиты информации.
53. Охарактеризуйте организационную структуру системы сертификации средств защиты информации по требованиям ее безопасности.
54. В каком порядке проводится сертификация и контроль средств защиты информации?
55. Охарактеризуйте организационную структуру системы аттестации объектов информатизации по требованиям безопасности информации.
56. В каком порядке проводится аттестация объектов информатизации по требованиям безопасности информации?
57. Назовите классификацию видов противоправных деяний в отношении компьютерной информации.
58. Назовите особенности компьютерных преступлений.
59. Дайте определение понятия компьютерных преступлений

60. Назовите классы компьютерных преступников.
61. Назовите способы и механизмы совершения компьютерных преступлений.
62. Назовите способы несанкционированного доступа к ЭВТ.
63. Какие виды юридической ответственности предусмотрены за нарушение правовых норм по защите информации?
64. Проведите классификация характера сохраняемой тайны.
65. Укажите проблемы уголовной ответственности за нарушение правовых норм по защите информации.
66. Какая уголовная ответственность установлена за нарушение правовых норм защиты информации?
67. Какая административная ответственность установлена за нарушение правовых норм защиты информации?
68. Какие виды административного наказания предусмотрены за нарушение правовых норм по защите информации?
69. Назовите этапы проведения административного расследования по фактам нарушения установленного порядка защиты информации.
70. Какие типовые организационные структуры входят в государственную систему защиты информации?
71. Какие функции в области обеспечения безопасности и защиты информации выполняют службы контроля и надзора органа государственной власти?
72. В чем состоит специфика государственного регулирования деятельности специализированных предприятий — разработчиков комплексов и средств обеспечения безопасности?
73. Как классифицируются услуги организационно-технологического характера в соответствии с этапами жизненного цикла систем обеспечения информационной безопасности?
74. В чем состоит специфика деятельности сертификационно-испытательных центров (лабораторий) и механизмов ее государственного регулирования?
75. Какие функции выполняет служба безопасности предприятия для решения задачи физической защиты?
76. Какие функции выполняет служба безопасности предприятия для решения задачи обеспечения информационной безопасности?
77. Как строится структура полномасштабной системы обеспечения безопасности и защиты информации?
78. Какова специфика организации и выполнения охранных функций?
79. Какие специальные мероприятия и действия должны предпринимать сотрудники службы безопасности по организации объектовых режимов?
80. В чем состоит основное назначение корпоративной нормативной базы?
81. Какова структура корпоративной нормативной базы?

82. Какие разделы содержит типовой формат положений о структурных подразделениях службы безопасности?
83. Дайте перечень нормативных документов процедурного уровня.
84. Чем определяется срок жизненного цикла корпоративной нормативной базы по информационной безопасности?
85. Объясните различие в определениях политики информационной безопасности.
86. В чем состоит отличие нормативно-методических документов политики безопасности от нормативных документов процедурного уровня?
87. Какие существуют особенности документального оформления политики безопасности, и чем они объясняются?
88. Изложите типовое содержание политики безопасности, оформленной в виде единого документа.
89. В чем состоит назначение Концепции обеспечения информационной безопасности организации? Изложите общее содержание Концепции.
90. Каковы цель и задача аудита информационной безопасности?
91. Какова методология деятельности по обеспечению безопасности объекта на основе политики безопасности?
92. Дайте перечень контрольных мероприятий и действий по оценке уровня безопасности объекта.
93. Дайте определение понятия «режимный объект» и видов обеспечения его безопасности.
94. Каковы цель и задачи организации пропускного режима?
95. Что является нормативной основой организации пропускного режима и каково ее общее содержание?
96. Что определяет порядок пропуска (прохода) физических лиц на территорию режимного объекта?
97. Что предусматривают правила въезда (выезда) транспортных средств на территорию режимного объекта?
98. Каковы особенности организации охраны режимного объекта?
99. Каковы суть и содержание нормативной основы организации охранных мероприятий?
100. Назовите действия охраны при тревоге и других чрезвычайных ситуациях.
101. Каковы цель и задачи организационного обеспечения внутриобъектового режима?
102. В чем состоит содержание организационного обеспечения режима секретности?
103. Каким образом организуется конфиденциальное делопроизводство?
104. Какие организационные процедуры включает обеспечение режима секретности?
105. Как организуется засекречивание сведений, составляющих государственную тайну?

106. Как организуются допуск и доступ к сведениям, составляющим государственную тайну?
107. Каковы правила обращения секретных документов?
108. Перечислите основные правила организации секретного делопроизводства.
109. Что предусматривает организационный режим делопроизводства и обращения документов с грифом «Для служебного пользования» (ДСП)?
110. Расскажите об особенностях современных систем автоматизированного документооборота.
111. В чем принципиальные отличия технологии workflow от традиционных систем автоматизации управленческой деятельности?
112. В чем состоит суть и содержание работ по противодействию технической разведке?
113. Дайте определение понятия «аттестация объектов информатизации».
114. Назовите основной перечень работ по аттестации объектов информатизации.
115. Каковы цель и задачи проведения служебных расследований инцидентов нарушений информационной безопасности?
116. Как проводится служебное расследование инцидентов при реализации угрозы информационной безопасности?
117. Чем определяется эффективность менеджмента в области информационной безопасности?
118. Опишите суть и содержание использования организационных схем и профессиограмм при подборе кадров.
119. Что является нормативно-правовой основой для введения дополнительных ограничений по контролю за деятельностью персонала?
120. Перечислите организационные процедуры для составления психологического портрета работника.
121. В чем состоят особенности верификации сведений о работнике при его приеме на работу?
122. Дайте описание методов психологического тестирования и графологической экспертизы.
123. Опишите специфику использования метода психофизиологического тестирования.
124. Какова цель ранжирования должностей по степени риска управления бизнес-процессами?
125. Опишите участие службы безопасности в процедурах увольнения сотрудников.
126. Дайте определение мотивации как метода управления персоналом.
127. Опишите суть и содержание метода положительного стимулирования.
128. В чем состоят особенности метода отрицательного стимулирования.
129. Что предполагает создание ориентирующих условий?

130. Что определяет актуальность вопросов самообучения и повышения квалификации?

131. Перечислите основные специальности, по которым осуществляется подготовка кадров в области обеспечения информационной безопасности, и основные направления образовательной деятельности в этой области.

7.3. Критерии оценивания.

Общий результат выводится как интегральная оценка, складывающаяся из текущего контроля - 70% и промежуточного контроля - 30%.

Текущий контроль по дисциплине включает:

- посещение занятий - 10 баллов,
- участие на практических занятиях - 30 баллов,
- выполнение домашних (аудиторных) контрольных работ - 30 баллов.

Промежуточный контроль по дисциплине включает:

- устный опрос - 15 баллов,
- письменная контрольная работа - 15 баллов,

8. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины.

а) основная литература:

1. Борисов М.А. Основы организационно-правой защиты информации: учеб. пособие / М.А. Борисов, О.А. Романов. – М.: URSS, 2013. – 202 с.

2. Кармановский Н.С. Организационно-правовое и методическое обеспечение информационной безопасности / Н.С. Кармановский, О.В. Михайличенко, С.В. Савков // Учебное пособие. – СПб: НИУ ИТМО, 2013. – 148 с.

3. Организационно-правовое обеспечение информационной безопасности: учеб. пособие для студ. высш. учеб. заведений / А. А. Стрельцов [и др.]; под ред. А. А. Стрельцова. — М.: Издательский центр «Академия», 2008. — 256 с. ISBN 978-5-7695-4240-4.

б) дополнительная литература:

1. Камышев Э.Н. Информационная безопасность и защита информации: Учебное пособие. - Томск: ТПУ, 2009. - 95 с.

2. Парошин А.А. Нормативно-правовые аспекты защиты информации: Учебное пособие / А.А. Парошин. – Владивосток: Изд-во Дальневост. федер. ун-та, 2010. – 116 с.

3. Развитие правового обеспечения информационной безопасности (монография) / (А.А. Стрельцов и др.); под редакцией А.А. Стрельцова; Фонд Гражданских инициатив в Политике Интернет. – М.: Престиж, 2005.

4. Романов О.А. Основы организационно-правовой защиты информации: учеб. пособие / О.А. Романов, М.А. Борисов; Моск. гос. универ. им. М.В. Ломоносова, Фак. вычисл. математики и кибернетики М.: МАКС-ПРЕСС, 2007.

5. Семкин С.Н. Основы организационного обеспечения информационной безопасности объектов информатизации: Учебное пособие / С.Н. Сем-

кин, Э.В. Беляков, С.В. Козачек // М.: Гелиос АРВ, 2005.

9. Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины.

1. eLIBRARY.RU [Электронный ресурс]: электронная библиотека / Науч. электронн. б-ка. – Москва, 1999 - . Режим па: <http://elibrary.ru/default.asp> (дата обращения: 01.04.2017). – яз. рус., англ.

2. Moodle [Электронный ресурс]: система виртуального обучения: [база данных] / Даг. Гос. ун-т. – Махачкала, г. – Доступ из сети ДГУ или, после регистрации из сети ун-та, из любой точки, имеющей доступ в интернет. – URL: <http://moodle.dgu.ru/> (дата обращения: 22.03.2018).

3. Электронный каталог НБ ДГУ [Электронный ресурс]: база данных содержит сведения о всех видах литературы, поступающих в фонд НБ ДГУ / Дагестанский гос. ун-т. – Махачкала, 2010 – режим доступа: <http://elib.dgu.ru>, свободный (дата обращения: 21.03.2018).

4. <http://edu.icc.dgu.ru> - Сайт образовательных ресурсов Даггосуниверситета.

5. <http://www.scrf.gov.ru/documents/6/114.html> - Совет Безопасности Российской Федерации.

6. <http://www.fsb.ru> – Федеральная служба безопасности (ФСБ) России.

7. <http://fstec.ru> – Федеральная служба по техническому и экспортному контролю (ФСТЭК) России.

8. <http://mvd.ru> – Министерство внутренних дел (МВД) Российской Федерации.

10. Методические указания для обучающихся по освоению дисциплины.

Для эффективного усвоения программного материала по дисциплине «*Организационно-правовые основы информационной безопасности*», как и по любой другой дисциплине, предусмотрены разнообразные формы аудиторной и внеаудиторной самостоятельной работы студентов, в том числе:

- прослушивание лекционного курса в аудитории с написанием конспекта;
- подготовка и индивидуальное активное участие на семинарских занятиях;
- выполнение самостоятельных работ с использованием рекомендованной литературы и Интернет-ресурсов;
- подготовка рефератов, участие на студенческих научно-практических конференциях с докладами по тематике дисциплины;
- выполнение тестовых заданий.

В процессе подготовки к семинару студенты могут воспользоваться консультациями преподавателя. Примерные темы докладов, сообщений, вопросов для обсуждения приведены в настоящих рекомендациях. Кроме указан-

ных в настоящих учебно-методических материалах тем, студенты могут по согласованию с преподавателем избирать и другие темы.

Самостоятельная работа необходима студентам для подготовки к семинарским занятиям и подготовки рефератов на выбранную тему с использованием материалов преподаваемого курса, лекций и рекомендованной литературы.

Самостоятельная работа включает глубокое изучение монографий, научных статей и работ, учебных пособий по дисциплине, а также нормативных правовых актов.

Самостоятельную работу над дисциплиной следует начинать с изучения программы, которая содержит основные требования к знаниям, умениям, навыкам обучаемых. Обязательно следует выполнять рекомендации преподавателя, данные в ходе установочных занятий. Затем приступить к изучению отдельных разделов и тем в порядке, предусмотренном программой.

Получив представление об основном содержании раздела, темы, необходимо изучить материал с помощью учебника. Целесообразно составить краткий конспект или схему, отображающую смысл и связи основных понятий данного раздела, включенных в него тем. Затем необходимо изучить соответствующее законодательство. Обязательно следует записывать возникшие вопросы, на которые не удалось ответить самостоятельно. При самостоятельных занятиях студенты осуществляют тематические подборки нормативных правовых актов из различных баз данных по законодательству, в том числе и в удаленном доступе. Кроме того, формой самостоятельной работы студента является подготовка реферата, в которых студент дает анализ законодательства и изученной литературы при рассмотрении какой-либо проблемы. Примерная тематика рефератов приведена в настоящем пособии. Студент может выбрать и другую тему, согласовав ее с преподавателем.

Реферат - это научно-исследовательская работа студента, и которой он делает анализ источников права и изученной литературы по выбранной теме.

Реферат является отражением знания студента выбранной темы. Работа проводится под руководством преподавателя: согласовывается план работы, определяются источники и литература, обсуждаются возможные методы исследования вопросов выбранной темы. Объем реферата 15-20 страниц печатного текста (размер шрифта (кегель) - 14, междустрочный интервал полуторный).

На титульном листе указываются: принадлежность к ФГБОУ ДГУ; тема реферата; фамилия, имя, отчество автора, курс, учебная группа, год написания. На втором листе помещается план реферата, включающий введение, основные вопросы, заключение.

Изложение материала в письменной работе (реферат) делится на три логические части: введение, основная часть, заключение. Введение содержит обоснование темы. Основная часть также делится на логически завершенные части исследуемой темы (разделы, главы, параграфы). Заключение должно содержать выводы, к которым пришел автор. В работе должны быть сноски

на цитируемую литературу, малоизвестные факты, статистические данные. В конце работы приводится список использованной литературы в алфавитном порядке (фамилия, инициалы автора; заголовок использованного учебника, монографии, статьи и т.п.; издательство, год издания, страницы).

Нормативные правовые акты излагаются по видам актов: международно-правовые акты, Конституция РФ, конституционные федеральные законы, федеральные законы (законы Российской Федерации), указы, распоряжения Президента РФ, постановления, распоряжения Правительства РФ, нормативные правовые акты федеральных органов исполнительной власти, правовые акты субъектов Российской Федерации, правовые акты органов местного самоуправления и по датам их принятия.

11. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине, включая перечень программного обеспечения и информационных справочных систем.

1. Операционная система Windows7.
2. Текстовый процессор Microsoft Word 2010.
3. СПС КонсультантПлюс
4. СПС Гарант

12. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине.

- Аудиторный класс.
- Компьютерный класс.
- Ноутбук, мультимедиа проектор для презентаций, экран.