МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РФ
Федеральное государственное бюджетное образовательное учреждение высшего образования
«ДАГЕСТАНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»
Юридический институт
Кафедра информационного права и информатики

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

ОРГАНИЗИЦИОННО-ПРАВОВОЕ ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Кафедра информационного права и информатики

Юридического института

Образовательная программа
40.04.01 Юриспруденция

Направленность (профиль) программы
Информационное право и информационная безопасность

Уровень высшего образования
магистратура

Форма обучения
Очная, заочная

Статус дисциплины: **входит в часть, формируемую участниками образовательных отношений**

Махачкала 2021

Рабочая программа дисциплины «Организационно-правовое обеспечение информационной безопасности» составлена в 2021 году в соответствии с требованиями ФГОС ВО-магистратура по направлению подготовки **40.04.01** Юриспруденция от 25 ноября 2020 г. N 1451.

Разработчик(и): кафедра «Информационного права и информатики»
Абдусаламов Руслан Абдусаламович, к.п.н., доцент;
Магдилова Лариса Владимировна, к.э.н., доцент.

Рабочая программа дисциплины одобрена на заседании кафедры информационного права и информатики от «11» 05 2021 г., протокол № 10

Зав. кафедрой _____ Абдусаламов Р.А.

На заседании Методической комиссии юридического института от «19» 05 2021 г., протокол № 10

Председатель _____ Арсланбекова А.З.

Рабочая программа дисциплины согласована с учебно-методическим управлением «09» 07 2021 г. _____

Начальник УМУ _____ Гасангаджиева А.Г.

Аннотация рабочей программы дисциплины

Дисциплина «Организационно-правовое обеспечение информационной безопасности» входит в часть, формируемую участниками образовательных отношений образовательной программы магистратуры по направлению 40.04.01 «Юриспруденция». Дисциплина реализуется в юридическом институте кафедрой информационного права и информатики.

Содержание дисциплины охватывает круг вопросов, связанных с построением систем организационного и правового обеспечения информационной безопасности. Раскрывает вопросы юридической ответственности за правонарушения в области информационной безопасности, а также механизмы защиты прав и законных интересов субъектов информационной сферы.

Дисциплина нацелена на формирование следующих компетенций выпускника: профессиональных –ПК-3, ПК-4.

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

Рабочая программа дисциплины предусматривает проведение следующих видов контроля успеваемости в форме контрольной работы, коллоквиума, тестирования и промежуточный контроль в форме экзамена.

Объем дисциплины 3 зачетные единицы, в том числе в 108 академических часах по видам учебных занятий

Семестр	Учебные занятия							СРС, в том числе экзамен	Форма промежуточной аттестации (зачет, дифференцированный зачет, экзамен)
	в том числе:								
	всего	Контактная работа обучающихся с преподавателем							
		всего	из них						
			Лекции	Лабораторные занятия	Практические занятия	КСР	консультации		
3	108	40	20		20			68	экзамен

Форма обучения: заочная

Семестр	Учебные занятия							СРС, в том числе экзамен	Форма промежуточной аттестации (зачет, дифференцированный зачет, экзамен)
	в том числе:								
	всего	Контактная работа обучающихся с преподавателем							
		всего	из них						
			Лекции	Лабораторные занятия	Практические занятия	КСР	консультации		
4	108	12	10		2			96	зачет

1. Цели освоения дисциплины

Содержание программы учебной дисциплины «Организационно-правовое обеспечение информационной безопасности» направлено на достижение цели: подготовки студентов-магистрантов для работы в органах государственной власти и в других сферах способных представлять интересы в области международного информационного обмена, а также способных ориентироваться в проблемах формирования рынка информационных ресурсов и обеспечивать информационную безопасность государства, общества и личности.

В результате освоения дисциплины обучающийся должен знать: - основные нормативные правовые акты в области информационной безопасности и защиты информации, а также нормативные методические документы Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю в данной области; правовые основы организации защиты государственной тайны и конфиденциальной информации, задачи органов защиты государственной тайны; правовые нормы и стандарты по лицензированию в области обеспечения защиты государственной тайны и сертификации средств защиты информации; организацию ремонтного обслуживания аппаратуры и средств защиты информации; принципы и методы организационной защиты информации, организационное обеспечение информационной безопасности в организации; правовое положение субъектов правоотношений в сфере профессиональной деятельности (включая предпринимательскую деятельность

С учетом этого в рамках данной дисциплины предполагается углубленное изучение студентами-магистрантами вопросов ответственности в области информационной безопасности, в том числе созданием и применением средств и механизмов информационной безопасности.

В процессе изучения дисциплины рассматриваются проблемы теории ответственности в информационном праве, совершенствования законодательства и практики применения мер в этой области.

2.Место дисциплины в структуре ОПОП магистратуры

Дисциплина «Организационно-правовое обеспечение информационной безопасности» входит в часть, формируемую участниками образовательных отношений образовательной программы юридических дисциплин и является обязательной для изучения в рамках магистерской программы «Информационного права и информационной безопасности» по кафедре информационного права и информатики.

Магистрант, изучающий дисциплину «Организационно-правовое обеспечение информационной безопасности», должен знать основные общенаучные методы и приемы познания, закономерности экономического и

общественно-политического развития общества и государства, знать основные положения теории права и отдельных отраслей права.

Для полноценного усвоения дисциплины необходима предшествующая теоретическая подготовка по следующим дисциплинам: актуальные проблемы информационного права, информационные технологии в юридической деятельности, конституционные и международные основы информационного права, правовое регулирование государственного управления в информационной сфере.

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

Код и наименование профессиональной компетенции	Код и наименование индикатора достижения профессиональной компетенции	Планируемые результаты обучения	**Процедура освоения**
ПК-3 Способен квалифицированно применять нормативные правовые акты в конкретных сферах юридической деятельности, реализовывать нормы материального и процессуального права в профессиональной деятельности	ПК-3.1. Способен принимать решения и совершать юридические действия в точном соответствии с законом	**Знает:** национальное законодательство, виды правовых актов, функции и полномочия органов исполнительной власти, сферу их деятельности **Умеет:** пользоваться нормами отечественного законодательства, применять их в своей профессиональной деятельности **Владеет:** навыками применения нормативно-правовых актов, работы с информационно-поисковыми системами	Фронтальный опрос, контрольная работа или тестирование
	ПК-3.2. Способен осуществлять юридические процедуры	**Знает:** виды, сроки и цели юридических процедур, формы и правила оформления процессуальных документов, виды документов, новые информационные технологии, программные системы, позволяющие вести электронный документооборот. **Умеет:** осуществлять	

		юридические процедуры, составлять документы, пользоваться электронными ресурсами **Владеет:** навыками осуществления и оформления юридических процедур	
	ПК-3.3. Способен составлять процессуальные документы и совершать необходимые процессуальные действия	**Знает:** сущность и значение информации, содержащейся в служебной документации, основные требования режима секретности служебной документации **Умеет:** применять меры по обеспечению информационной безопасности **Владеет:** навыками засекречивания информации, обеспечения режима секретности	
ПК-4 Способен соблюдать в профессиональной деятельности требования правовых актов в области защиты государственной тайны и информационной безопасности, обеспечивать соблюдение режима секретности	ПК-4.1 Способен понимать сущность и значение информации в развитии современного общества, соблюдать основные требования информационной безопасности, в т.ч. защиты государственной тайны	**Знает:** виды угроз национальной безопасности РФ, методы противодействия возникающим угрозам **Умеет:** выявлять признаки возникающих угроз национальной безопасности РФ, применять меры по предупреждению и пресечению возникших угроз **Владеет:** навыками борьбы и предупреждения возникающих угроз национальной безопасности РФ	Фронтальный опрос, контрольная работа или тестирование

	ПК-4.2. Способен сознавать опасности и угрозы, возникающие в обществе	**Знает:** должностные обязанности работников в области обеспечения законности и правопорядка **Умеет:** правильно исполнять их в своей профессиональной деятельности **Владеет:** методиками исполнения должностных обязанностей по обеспечению законности и правопорядка, безопасности личности, общества, государства; способен осуществлять профессиональную деятельность по обеспечению исполнения полномочий федеральных органов исполнительной власти, органов исполнительной власти субъектов РФ, лиц, замещающих государственные должности РФ, лиц, замещающих государственные должности субъектов РФ, и лиц, замещающих муниципальные должности, а также выполнять должностные обязанности по участию в осуществлении государственного контроля (надзора), муниципального контроля и общественного контроля.	
	ПК-4.3. Способен к выполнению должностных обязанностей по обеспечению законности и правопорядка, безопасности	Знает: должностные обязанности работников в области обеспечения законности и правопорядка Умеет: правильно исполнять их в своей профессиональной деятельности Владеет:	

	личности, общества, государства	методиками исполнения должностных обязанностей по обеспечению законности и правопорядка, безопасности личности, общества, государства; способен осуществлять профессиональную деятельность по обеспечению исполнения полномочий федеральных органов исполнительной власти, органов исполнительной власти субъектов РФ, лиц, замещающих государственные должности РФ, лиц, замещающих государственные должности субъектов РФ, и лиц, замещающих муниципальные должности, а также выполнять должностные обязанности по участию в осуществлении государственного контроля (надзора), муниципального контроля и общественного контроля.	

4. Объем, структура и содержание дисциплины

4.1. Объем дисциплины составляет 3 зачетные единицы, 108академических часов.

4.2. Структура дисциплины

4.2.1. Структура дисциплины в очной форме

Раздел	семестр	**Виды учебной работы, включая самостоятельную работу студентов (в часах)**					Формы текущего контроля успеваемости Формы промежуточного контроля
		Лекции	**Практические занятия**	**Лабораторные занятия**	**…**	**Самостоятельная работа в т.ч. экзамен**	
Модуль 1							

1	Основы обеспечения информационной безопасности	3	2	2			12	Устный опрос,
2	Организационно-правовые проблемы международной информационной безопасности	3	4	4			12	Фронтальный опрос, контрольная работа или тестирование
	Итого за 1 модуль		6	6			24	36
Модуль 2								
3	Правовой режим обеспечения безопасности информации ограниченного доступа	3	2	2			13	Рефераты, контрольная работа или тестирование
4	Правовое и организационное обеспечение безопасности в сети Интернет	3	4	4			11	Устный опрос, контрольная работа или тестирование
	Итого за 2 модуль		6	6			24	36
Модуль 3								
5	Организационно-правовое обеспечение защиты информационных систем	3	4	4			10	Фронтальный опрос, контрольная работа или тестирование
6	Юридическая ответственность за правонарушения в информационной сфере	3	4	4			10	Рефераты, контрольная работа или тестирование
	Итого за 3 модуль		8	8			20	36
	Итого:		20	20			68	108

4.2.2. Структура дисциплины в заочной форме

Раздел	семестр	**Виды учебной работы, включая самостоятельную работу студентов (в часах)**	Формы текущего контроля успеваемости

			Лекции	**Практические занятия**	**Лабораторные занятия**	**…**	**Самостоятельная работа в т.ч. экзамен**	Формы промежуточного контроля
	Модуль 1							
1	Основы обеспечения информационной безопасности	4	2	2			15	Устный опрос,
2	Организационно-правовые проблемы международной информационной безопасности	4	1				16	Фронтальный опрос, контрольная работа или тестирование
	Итого за 1 модуль		3	2			31	36
Модуль 2								
3	Правовой режим обеспечения безопасности информации ограниченного доступа	4	1				17	Рефераты, контрольная работа или тестирование
4	Правовое и организационное обеспечение безопасности в сети Интернет	4	2				16	Устный опрос, контрольная работа или тестирование
	Итого за 2 модуль		3				33	36
Модуль 3								
5	Организационно-правовое обеспечение защиты информационных систем	4	2				10	Фронтальный опрос, контрольная работа или тестирование
6	Юридическая ответственность за правонарушения в информационной сфере	4	2				12	Рефераты, контрольная работа или тестирование
	Итого за 3 модуль		4				32	36
	Итого:		10	2			96	108

4.3. Содержание дисциплины, структурированное по темам (разделам)

Модуль 1

Тема 1. Основы обеспечения информационной безопасности

Понятие и основные признаки информационной безопасности. Субъекты и объекты правоотношений в области информационной безопасности. Система нормативных правовых актов, регулирующие обеспечение информационной безопасности в Российской Федерации. Правовые средства обеспечения информационной безопасности.

Правовое обеспечение информационной безопасности. Организационное обеспечение информационной безопасности.

Тема 2. Организационно-правовые проблемы международной информационной безопасности

Понятие международной информационной безопасности. Международные правовые акты в области обеспечения информационной безопасности. Основные угрозы международной информационной безопасности.

Зарубежный опыт правового обеспечения информационной безопасности.

Модуль 2

Тема 3. Правовой режим обеспечения безопасности информации ограниченного доступа

Понятие и виды информации ограниченного доступа. Правовые режимы тайн. Правовой режим защиты государственной тайны: понятие и признаки. Отнесение сведений к государственной тайне. Контроль и надзор за обеспечением защиты государственной тайны.

Правовой режим обеспечения безопасности персональных данных: понятие и виды. Принципы и условия обработки персональных данных. Обязанности оператора по обеспечению безопасности персональных данных.

Тема 4. Правовое и организационное обеспечение безопасности в сети Интернет

Информационная безопасность в сети интернет. Ответственность за распространение экстремистских материалов. Пропаганда, незаконная реклама наркотических средств и психотропных веществ. Клевета в сети Интернет. Мошенничество, связанное с блокированием программного обеспечения компьютеров пользователей сети Интернет. Хищения, совершаемые с помощью сети Интернет и компьютерной техники. Распространение персональных данных и сведений о частной жизни в сети Интернет. Нарушение авторских прав в сети Интернет.

Защита детей от вредной информации. Информационная безопасность детей.

Блокирование доступа к информации в сети Интернет. Идентификация пользователей сети Интернет. Охрана прав субъекта персональных данных в сети Интернет. Информационный посредник.

Модуль 3

Тема 5. Организационно-правовое обеспечение защиты информационных систем

Основные объекты обеспечения информационной безопасности в сфере создания и функционирования общегосударственных информационных систем. Требования при создании системы защиты информации автоматизированных систем. Несанкционированный доступ к информации автоматизированных систем. Утечка защищаемой информации по техническим каналам.

Программное и техническое обеспечение информационной безопасности. Политика информационной безопасности.

Тема 6. Юридическая ответственность за правонарушения в информационной сфере

Понятие и виды юридической ответственности в области обеспечения информационной безопасности. Субъекты и объекты правоотношений в области обеспечения информационной безопасности.

Гражданско-правовая ответственность за информационные правонарушения. Основания для наступления гражданско-правовой ответственности.

Административно-правовая ответственность за информационные правонарушения.

Уголовная ответственность за преступления в информационной сфере.

Ответственность за преступления в сфере компьютерной информации. Международный опыт борьбы с преступлениями в сфере компьютерной информации.

Криминалистическая характеристика преступлений в сфере компьютерной информации.

Темы практических и семинарских занятий

Тема 1. Основы обеспечения информационной безопасности

1. Понятие и основные признаки информационной безопасности.
2. Субъекты и объекты правоотношений в области информационной безопасности.
3. Законодательство в области обеспечения информационной безопасности.
4. Средства и методы защиты информации

Тема 2. Организационно-правовые проблемы международной информационной безопасности

1. Понятие и основные угрозы международной информационной безопасности.

2. Международные правовые акты в области обеспечения информационной безопасности.

3. Международное сотрудничество в борьбе с киберпреступностью

Тема 3. Правовой режим обеспечения безопасности информации ограниченного доступа

1. Понятие и виды информации ограниченного доступа.
2. Правовой режим защиты государственной тайны.
3. Правовой режим коммерческой тайны.
4. Правовой режим персональных данных.

Тема 4. Правовое и организационное обеспечение безопасности в сети Интернет

1. Защита детей от информации, причиняющей вред их здоровью и развитию
2. Правила доступа к информации в сети интернет
3. Охрана прав субъектов персональных данных в сети Интернет.

Тема 5. Организационно-правовое обеспечение защиты информационных систем

1. Политика информационной безопасности информационных систем.

2. Основные функции информационной безопасности автоматизированных систем.

3. Обеспечение информационной безопасности информационных систем в сфере судопроизводства.

Тема 6. Юридическая ответственность за правонарушения в информационной сфере

1. Понятие и виды юридической ответственности в области обеспечения информационной безопасности.

2. Гражданская ответственность за правонарушения в информационной сфере.

3. Административная ответственность за правонарушения в информационной сфере.

4. Уголовная ответственность за правонарушения в информационной сфере.

5. **Образовательные технологии**

При проведении занятий могут быть использованы традиционные академические и интерактивные методы обучения:

- дискуссии;
- работа в малых группах;
- творческие задания;
- ролевая игра;
- тестирование;
- вопрос-вопрос;
- лекция-презентация;
- лекция-пресс-конференция;
- решение задач;
- лекция с ошибками;
- лекция – тандем (напр.: лектор+госслужащий)

Использование в лекциях элементов проблемного обучения, на семинарских занятиях – мозгового штурма, решение задач практического характера, разбор конкретных ситуаций, деловые и ролевые игры, психологический тренинг. Проведение занятий в интерактивной форме. Организация встреч студентов учеными и практиками государственных и общественных организаций.

6. Учебно-методическое обеспечение самостоятельной работы студентов

Нормативные акты

1. Конституция Российской Федерации: принята всенар. голосованием 12.12.1993 г. // Собр. законодательства Рос. Федерации. – 2014. – № 31. – Ст. 4398.
2. Арбитражный процессуальный кодекс Российской Федерации: федеральный закон от 24.07.2002 № 95-ФЗ: в ред. от 29.06.2015 №195-ФЗ // СЗ РФ. – 2002. – № 30. – Ст. 3012.; СЗ РФ. – 2015. – № 27. – Ст. 3986.
3. Гражданский кодекс РФ (часть 4): Федеральный закон от 18.12.2006 N 230-ФЗ //СЗ РФ. – 2006. - №52. – Ст. 5496.
4. Гражданский процессуальный кодекс Российской Федерации от 14.11.2002 № 138-ФЗ (ред. от 30.12.2015) (с изм. и доп., вступ. в силу с 01.01.2016) // Собрание законодательства РФ. – 2002. – № 46. – Ст. 4532.
5. Кодекс Российской Федерации об административных правонарушениях// Российская газета. — 2001. — № 256.
6. О безопасности: Федеральный закон от 28.12.2010 № 390-ФЗ // "Российская газета", N 295, 29.12.2010
7. О гарантиях равенства парламентских партий при освещении их деятельности государственными общедоступными телеканалами и радиоканалами: Федеральный закон от 12.05.2009 N 95-ФЗ (принят ГД ФС РФ 24.04.2009) // "Собрание законодательства РФ", 18.05.2009, N 20, ст. 2392.

8. О порядке освещения деятельности органов государственной власти в государственных средствах массовой информации: Федеральный закон от 13.01.1995 N 7-ФЗ (ред. от 12.05.2009) (принят ГД ФС РФ 15.12.1994) // "Собрание законодательства РФ", 16.01.1995, N 3, ст. 170.
9. О порядке рассмотрения обращений граждан Российской Федерации: Федеральный закон от 02.05.2006 № 59 – ФЗ (ред. от 29.06.2010) //Парламентская газета. — 2006. — № 70–71.
10. О рекламе: Федеральный закон от 13 марта 2006 г.№ 38 – ФЗ //СЗ РФ . - 2006. - №12. - ст. 1232.
11. О рекламе: Федеральный Закон РФ от 13.03.2006 № 38 - ФЗ (ред. от 08.03.2015) //Собрание Законодательства РФ. - 2006. - №12. - ст. 1232.
12. О средствах массовой информации: Закон РФ от 27.12.1991 №2124-1. // Ведомости РФ СНД и ВС РФ, 13.02.1992, № 7, ст. 300.
13. О Судебном департаменте при Верховном Суде Российской Федерации: Федеральный закон от 8 января 1998 г. № 7-ФЗ (в ред. От 05.10.2015) // СЗ РФ. – 1998. – № 2. – Ст. 223.
14. Об информации, информационных технологиях и о защите информации: Федеральный закон от 27 июля 2006 г. № 149 – ФЗ // СЗ РФ. – 2006. - №31 (1ч.). – Ст. 3448.
15. Об обеспечении доступа к информации о деятельности государственных органов и органов местного самоуправления: Федеральный закон от 09.02.2009 № 8-ФЗ «» // Собрание законодательства Российской Федерации, 16.02.2009, № 7, ст. 776.
16. Об обеспечении доступа к информации о деятельности судов в Российской Федерации: Федеральный закон от 22.12.2008 № 262 – ФЗ (ред. от 28.06.2010) //Парламентская газета. — 2008. — № 90.
17. Уголовно–процессуальный кодекс Российской Федерации //Российская газета. — 2001. — № 249.
18. Уголовный кодекс РФ //СЗ РФ. – 1996. - №25. – Ст. 2954.

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

7.1. Типовые контрольные задания

Примерная тематика рефератов (творческих работ)

1. Преступления против неприкосновенности личной жизни.
2. Нарушение авторских и смежных прав.
3. Неправомерный доступ к компьютерной информации.
4. Незаконное получение и разглашение сведений, составляющих коммерческую, налоговую или банковскую тайну.

5. Заведомо ложное сообщение об акте терроризма.
6. Сокрытие информации об обстоятельствах, создающих опасность для жизни или здоровья людей.
7. Информационные барьеры.
8. Окинавская Хартия глобального информационного общества.
9. Информационные войны.
10. Особенности правоотношений, возникающих при производстве, распространении и потреблении массовой информации.
11. Особенности сети Интернет как средства распространения информации.
12. Особенности следственных действий при выявлении информационных преступлений.
13. Сговор при ограничении доступа к открытой информации.
14. Разглашение государственной тайны.
15. Полномочия законодателя субъекта по установлению административной ответственности.
16. Особенности административной ответственности специальных субъектов
17. Административный штраф как вид административного наказания.
18. Компетенция органов административной юрисдикции по рассмотрению дел об административных правонарушениях.
19. Использование несертифицированных средств связи либо предоставление несертифицированных услуг связи.
20. Развитие законодательства в области сбора, хранения, использования или распространения информации о гражданах (персональных данных).
21. Воспрепятствование распространению продукции средства массовой информации.
22. Административная ответственность за нарушение порядка изготовления или распространения продукции средства массовой информации.
23. К вопросу о расширении представляемой информации о деятельности государственных органов и органов местного самоуправления в сети "Интернет».
24. Ответственности без вины в гражданском праве.
25. Основания освобождения от ответственности без вины.
26. Соотношение возмещения убытков с иными формами гражданско-правовой ответственности.
27. Роль судебной практики в определении и возмещении убытков.
28. Принцип полного возмещения убытков как ограничитель ответственности, с одной стороны, и как компенсационный - с другой.
29. Определение предмета доказывания и распределение бремени доказывания по делам о возмещении убытков.
30. Методика доказывания и необходимые доказательства по делам о возмещении убытков.
31. Компенсация морального вреда при нарушении договора. Тенденции развития законодательства.
32. Особенности компенсации морального вреда в США.

33. Компенсация морального вреда в Германии.
34. Компенсация морального вреда во Франции.

35. Требования, предъявляемые к организации защиты конфиденциальной информации.
36. Виды компьютерных преступлений.
37. Особенности квалификации компьютерных преступлений.
38. Преступления имущественного характера, которые совершаются с применением или в отношении средств компьютерной техники.
39. Доктрина информационной безопасности РФ об основных угрозах в информационной сфере и их источниках.

Примерные тестовые задания для проведения текущего и промежуточного контроля

1. Правовой режим информации - это

) объектный режим, вводимый законодательным актом и позволяющий обеспечить комплексность воздействия в информационной сфере посредством совокупности регулятивных, охранительных, процессуально-процедурных средств, характеризующих особое сочетание дозволений, запретов и обязываний, а также гарантий по его соблюдению
) порядок регулирования, выраженный в комплексе правовых средств, которые характеризуют особое сочетание взаимодействующих между собой дозволений, запретов, а также позитивных обязываний и создают особую направленность регулирования
) государственный строй, совокупность средств, методов, способов осуществления власти

2. Правовой режим объекта правоотношения может быть
) общим (или первичным) и специальным (или вторичным)
) императивным и диспозитивным
) открытым и ограниченным
) публичноправовым и частноправовым

3. Специальный (или вторичный) правовой режим – это режим
) вносящий либо особые льготы и преимущества, либо особые ограничения, которые заключаются в дополнительных запретах и обязываниях
) при котором участники отношений не могут изменить по своему усмотрению установленные правила поведения
) при котором участники отношений могут менять по своему усмотрению правила поведения
) который выражает общие, исходные способы правового регулирования

4. Правовой режим информации определяется нормами, устанавливающими:
) порядок документирования информации; право собственности на отдельные документы и отдельные массивы документов, документы и массивы документов в информационных системах; категорию информации по уровню доступа к ней; порядок правовой защиты информации

) порядок производства, передачи и распространения информации
) порядок создания и применения информации, информационных систем и механизмов информационной безопасности
) все верны
5. Основными направлениями правового регулирования отношений в Интернет являются
) защита от вредной и незаконной информации; соблюдение авторских и смежных прав; вопросы электронного документооборота; вопросы киберэкономики; информационная безопасность; правонарушения
) информационная безопасность; вопросы разработки сетевых программ и техники; повышение производительности каналов сети; вопросы электронного документооборота; вопросы киберэкономики; правонарушения
) использование электронной подписи и электронных денег; ограничение права доступа к информации; охрана прав несовершеннолетних
6. При правовом регулировании отношений в Интернет важно соблюдение баланса
) между свободой слова и интересами несовершеннолетних; свободы доступа к информации и информационной безопасностью; свободы производства информации и ограничения производства и распространения опасной информации
) между свободой слова и интересами несовершеннолетних; между свободой слова и цензурой; свободы к государственным ресурсам и их безопасностью
) свободы производства информации и ограничения производства и распространения опасной информации; между использованием различных видов каналов (кабельных, спутниковых, радиопоисковых и т.п.); между программными и техническими средствами защиты информации
7. К публично-правовым отношениям в Интернет относятся:
) все верны
) отношения, возникающие при создании и функционировании "электронного правительства"
) отношения по лицензированию деятельности провайдеров, удостоверяющих центров и иных субъектов, по регистрации электронных СМИ и сертификации технических средств; отношения по привлечению к ответственности за преступления и правонарушения, совершенные с использованием Интернета
) в сфере электронной коммерции - отношения типа B2A - BusinesstoAdministration
8. В законе РФ «О безопасности» безопасность определяется как
) как состояние защищенности жизненно важных интересов личности, общества и государства от внутренних и внешних угроз
) совокупность потребностей, удовлетворение которых обеспечивает существование и возможности прогрессивного развития личности, общества, государства
) проведение единой государственной политики в этой сфере и система мер экономического, политического, организационного и иного характера,

адекватных угрозам жизненно важным интересам личности, общества и государства, направленных на выявление и предупреждение угроз
9. По определению, данному Г.В. Емельяновым и А.А. Стрельцовым, под информационной войной понимается
) «особый вид отношений между государствами, при котором для разрешения существующих межгосударственных противоречий используются методы, средства и технологии силового воздействия на информационную сферу этих государств»
) совокупность запланированных, взаимосвязанных информационных операции, успешное выполнение которых приводит к достижению цели, как правило, заключающейся во взятии под контроль системы управления противника (государства) или слому этой системы управления и замены ее на другую — контролируемую
) «специальные средства, технологии и информацию, позволяющие осуществлять «силовое» воздействие на информационное пространство общества и привести к значительному ущербу политическим, оборонным, экономическим и другим жизненно важным интересам государства»
10. С.П. Расторгуев определяет понятие «информационное оружие»
) как «открытые и скрытые целенаправленные информационные воздействия информационных систем друг на друга с целью получения определенного выигрыша в материальной сфере»
) как «специальные средства, технологии и информацию, позволяющие осуществлять «силовое» воздействие на информационное пространство общества и привести к значительному ущербу политическим, оборонным, экономическим и другим жизненно важным интересам государства»
) как совокупность запланированных, взаимосвязанных информационных операции, успешное выполнение которых приводит к достижению цели, как правило, заключающейся во взятии под контроль системы управления противника (государства) или слому этой системы управления и замены ее на другую — контролируемую
11. Информационные правонарушения обладают следующими признаками, имеющими существенное значение для этого класса правонарушений
) общими и специальными
) регулятивными и охранительными
) абсолютными и относительными
) императивными и диспозитивными
12. Информационное правонарушение определяется как
) общественно опасное (вредное), противоправное, виновное деяние (действия или бездействия) деликтоспособного лица, совершенное в информационной сфере и (или) с использованием информационных средств и технологий работы с информацией независимо от ее формы, либо в иной области человеческой деятельности в условиях информационной среды
) юридический факт (наряду с событием и действием), действия, противоречащие нормам права (антипод правомерному поведению)

) виновное общественно опасное деяние, запрещенное законодательством РФ под угрозой наказания, совершенное в области информационных правоотношений

13. Юридическая ответственность за информационные правонарушения - это

) применение к виновному лицу, совершившему правонарушение, мер воздействия, предусмотренных санкцией нарушенной нормы информационного права в определенном регламентированном порядке

) применение к виновному лицу, совершившему правонарушение, установленного законом порядка сбора, хранения, использования или распространения информации о гражданах (персональных данных) и правил защиты информации, мер воздействия, предусмотренных санкцией нарушенной нормы информационного права в определенном регламентированном порядке

) ответственность работников, по вине которых предприятие, учреждение, организация понесли расходы по возмещению вреда

) применение принудительных мер к виновному лицу, который в результате несоблюдения соответствующих норм информационного права, причинен вред предприятиям, учреждениям, организациям и гражданам

14. Состав информационного правонарушения включает в себя следующие элементы (признаки)

) объект, объективную сторону, субъект и субъективную сторону

) объект, субъект, поведение, право, обязанность, ответственность

) общественные отношения, физические и юридические лица, ответственность

) объект, объективную сторону, субъект, субъективную сторону, ответственность

15. Российская правовая система предусматривает следующие виды ответственности физических лиц за правонарушения в информационной сфере

) дисциплинарную (включая материальную), административную, гражданско-правовую (имущественную) и уголовную

) дисциплинарную (включая материальную), гражданско-правовую (имущественную) и уголовную

) дисциплинарную (включая материальную), административную, уголовную

) административную, гражданско-правовую (имущественную) и уголовную

16. Российская правовая система предусматривает следующие виды ответственности юридических лиц (предприятия, учреждения и организации) за правонарушения в информационной сфере

) административную и гражданско-правовую

) административную, гражданско-правовую и уголовную

) дисциплинарную (включая материальную), административную, гражданско-правовую (имущественную) и уголовную

) гражданско-правовую и уголовную

Вопросы к экзамену

1. Понятие информационной безопасности и основные принципы ее обеспечения.
2. Субъекты и объекты правоотношений в области информационной безопасности.
3. Законодательство в области обеспечения информационной безопасности.
4. Средства и методы защиты информации.
5. Национальные интересы в информационной сфере.
6. Основные информационные угрозы.
7. Основные направления обеспечения информационной безопасности.
8. Понятие и основные угрозы международной информационной безопасности.
9. Международные правовые акты в области обеспечения информационной безопасности.
10. Международное сотрудничество в борьбе с киберпреступностью
11. Понятие и виды информации ограниченного доступа.
12. Источники угроз информационной безопасности РФ
13. Основные положения государственной информационной политики Российской Федерации
14. Понятие и виды персональных данных.
15. Принципы и условия обработки персональных данных.
16. Обязанности оператора по обеспечению безопасности персональных данных.
17. Защита детей от информации, причиняющей вред их здоровью и развитию
18. Правила доступа к информации в сети интернет.
19. Охрана прав субъектов персональных данных в сети Интернет.
20. Угрозы информационной безопасности на предприятии.
21. Разработка политики информационной безопасности.
22. Политика информационной безопасности информационных систем.
23. Основные функции информационной безопасности автоматизированных систем.
24. Понятие и виды юридической ответственности в области обеспечения информационной безопасности.
25. Гражданская ответственность за правонарушения в информационной сфере.
26. Административная ответственность за правонарушения в информационной сфере.

27. Уголовная ответственность за правонарушения в информационной сфере.
28. Ответственность за распространение сведений, порочащих честь, достоинство или деловую репутацию.
29. Особенности ответственности информационного посредника.
30. Гражданско-правовая ответственность за разглашение коммерческой, служебной тайны и тайны частной жизни.
31. Административная ответственность за правонарушения в области связи.
32. Глава 28 УК РФ «Преступления в сфере компьютерной информации».
33. Требования, предъявляемые к организации защиты конфиденциальной информации.

7.2. Методические материалы, определяющие процедуру оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций.

Общий результат выводится как интегральная оценка, складывающая из текущего контроля и промежуточного контроля.

Текущий контроль по дисциплине включает:
- посещение занятий - 5 баллов,
- наличие конспектов – 5 баллов,
- участие на практических занятиях - 5 баллов,
- самостоятельная работа – 5 баллов,
- контрольная работа – 10 баллов.

Промежуточный контроль по дисциплине включает:
- устный опрос - 10 баллов,
- письменная контрольная работа - 20 баллов,
- тестирование – 10 баллов
- коллоквиум – 30 баллов.

8. Учебно-методическое обеспечение дисциплины

Основная литература

1. Актуальные проблемы информационного права [Электронный ресурс]: учебник / коллектив авторов: под ред. И.Л. Бачило, М.А. Лариной. – М.: ЮСТИЦИЯ, 2016. – 534 с. – (Магистратура и аспирантура). – URL: http://нэб.рф/catalog/000199_000009_008242836/- ЭБС «НЭБ».
2. Городов О.А. Информационное право [Электронный ресурс]: учебник для бакалавров. – М.: Издательство Проспект, 2016. – 303 с. – URL: http://нэб.рф/catalog/000199_000009_008578609/ - ЭБС «НЭБ».
3. Информационное право: учеб. пособие / Р. А. Абдусаламов; Минобрнауки России, Дагест. гос. ун-т. - Махачкала: Изд-во ДГУ, 2015. - 211 с.
4. Ковалева Н.Н. Информационное право России (2-е издание) [Электронный ресурс]: учебное пособие/ Ковалева Н.Н.— М.: Дашков и К,

Ай Пи Эр Медиа, 2016.— 352 c.— URL: http://www.iprbookshop.ru/57155.html.— ЭБС «IPRbooks».
5. Кузнецов П.У. Информационное право [Электронный ресурс]: учебник для бакалавров.. – М.: Издательство Юстиция, 2017. – 335 с. – URL: http://нэб.рф/catalog/000199_000009_009476417/ - ЭБС «НЭБ».
6. Организационное и правовое обеспечение информационной безопасности: учебник и практикум для бакалавриата и магистратуры / Т. А. Полякова, А. А. Стрельцов, С. Г. Чубукова, В. А. Ниесов ; под ред. Т. А. Поляковой, А. А. Стрельцова. — М. : Издательство Юрайт, 2017. — 325 с. — (Серия : Бакалавр и магистр. Академический курс).
7. Рассолов И. М. Информационное право: учебник и практикум для академического бакалавриата / И. М. Рассолов. — 4-е изд., перераб. и доп. — М.: Издательство Юрайт, 2017. — 346 с. — Серия: Бакалавр. Академический курс.

Дополнительная литература

1. Бабаян Р.А. Институт неприкосновенности частной жизни и национальная безопасность в эпоху информационных технологий. //Юридическое образование и наука. 2016. № 4. С. 150-154.
2. Бастрыкин А.И. Преступления против несовершеннолетних в интернет-пространстве: к вопросу о виктимологической профилактике и уголовно-правовой оценке. //Всероссийский криминологический журнал. 2017. Т. 11. № 1. С. 5-12.
3. Бачило И.Л. Информационное право. Учебник для магистров / Москва, 2015. Сер. 64 Авторский учебник (3-е изд., пер. и доп)
4. Безугленко О.С. Сравнительная характеристика регионального и федерального законодательства в области правовой защиты детей от вредной информации. // Информационное право, № 2(33), 2013.
5. Булгакова Л.И. Правовой режим аудиторской тайны. "Журнал российского права", 2008, № 5.
6. Бусленко Н.И. Медиаправо России: Документы, комментарии, вопросы и ответы. Феникс, 2005. 285 с.
7. Войниканис Е., Якушев М. Информация. Собственность. Интернет: традиция и новеллы в современном праве. М.: ВолтерсКлувер, 2004.
8. Войниканис Е.А. Право интеллектуальной собственности в цифровую эпоху: парадигма баланса и гибкости. Москва, 2016.
9. Волчинская Е.К. О проблемах формирования правовой системы ограничения доступа к информации. // Информационное право, № 4(35), 2013.
10. Волчинская Е.К.К юбилею Закона Российской Федерации «О государственной тайне». // Информационное право, № 2(33), 2013.
11. Гаврилин Ю.В. Преступления в сфере компьютерной информации. Квалификация и доказывание: Учеб.пособие. М.: Книжный мир, 2003. 245 с.

12. Городов О.А. Основы информационного права России: Учебное пособие. М.: Юридический центр Пресс, 2003. 305 с.;
13. Дайсон Э. Жизнь в эпоху Интернета. М.: Бизнес и компьютер, 1998.
14. Ефремова М. А. Мошенничество с использованием электронной информации. // Информационное право, № 4(35), 2013.
15. Жарова А.К. Право и информационные конфликты в информационно-телекоммуникационной сфере. Москва, 2016.
16. Журавлев М.С. Персональные данные в трудовых отношениях: допустимые пределы вмешательства в частную жизнь работника. // Информационное право, № 4(35), 2013.
17. Загородников С.Н., Шмелев. А.А. Основы Информационного права: Учеб.пособие. Ростов н/Д: Феникс, 2005.
18. Зверева Е. Имущественные и исключительные права на информационные продукты, их реализация и защита. "Право и экономика", 2004, N 12.
19. Зверева Е.А. Информация как объект неимущественных гражданских прав. "Право и экономика", № 9, 2003.
20. Иванова А.Ю. Проблемы ведения регистра муниципальных нормативных актов в едином информационном пространстве. // Информационное право, № 4(31), 2012.
21. Ильюшенко В.Н. Методологические, организационные и правовые основы информационной безопасности. В 3 ч. Томск: Изд-во Ин-та оптики атмосферы, 2005. 474 с.
22. Информационная безопасность России в условиях глобального информационного общества. М., 2001.
23. Информационное право. Информационная безопасность и защита информации: Сб. норматив.-правовых актов. Пермь: Перм. гос. ин-т искусства и культуры; Западно-Урал. ин-т экономики и права, 2004. 325 с.
24. Информационные ресурсы развития Российской Федерации. Правовые проблемы: Монография. СПб.: Наука, 2003. 403 с.
25. Казанцев С.Я., Згадзай О.Э., Оболенский Р.М. Правовое обеспечение информационной безопасности: Учеб.пособие для студентов вузов, обучающихся по спец. 075200 "Компьютерная безопасность", 075500 "Комплексное обеспечение информационной безопасности и автоматизированных систем". М.: Академия, 2005. 239 с.
26. Караваев А.О., Забайкалов А.П. О некоторых аспектах ответственности провайдера за нарушение авторских прав в сети интернет. //NB: Административное право и практика администрирования. 2016. № 5. С. 17-25.
27. Кириленко В.П., Алексеев Г.В. Международное право и информационная безопасность государств. монография / Санкт-Петербург, 2016.
28. Кодинец А.А. Теоретические аспекты деликтной ответственности за правонарушения в информационной сфере. //Известия Гомельского государственного университета им. Ф. Скорины. 2015. № 5 (92). С. 81-86.
29. Кузнецов П.У. Информационное право. Москва, 2017.

30. Морозов А.В., Филатова Л.В. Правовые вопросы доступа к информации. Учебное пособие / Москва, 2015.
31. Николаев В.В. Ограничение доступа к интернет-ресурсу как мера государственного принуждения. //Финансовое право и управление. 2015. № 2. С. 240-245.
32. Рассолов И.М. Информационное право. Учебник для магистров / Москва, 2015. Сер. 58 Бакалавр. Академический курс (2-е изд., испр. и доп)
33. Рассолов И.М. Право и кибернетическое пространство. Монография / Москва, 2016. (2-е издание).
34. Шибаев Д.В. Правовой режим врачебной тайны как информационно-правового объекта. //Право. Журнал Высшей школы экономики. 2015. № 3. С. 66-77.

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

1. Рагимханова Д.А. Электронный курс лекций по Информационному праву. Moodle [Электронный ресурс]: система виртуального обучением: [база данных] / Даг. гос. ун-т. – Махачкала, 2018 г. – Доступ из сети ДГУ или после регистрации из сети ун-та, из любой точки, имеющей доступ в интернет. – URL: http://moodle.dgu.ru
2. Рагимханова Д.А. Электронный курс лекций по Информационным технологиям в юридической деятельности. Moodle [Электронный ресурс]: система виртуального обучением: [база данных] / Даг. гос. ун-т. – Махачкала, 2018 г. – Доступ из сети ДГУ или после регистрации из сети ун-та, из любой точки, имеющей доступ в интернет. – URL: http://moodle.dgu.ru/.
3. eLIBRARY.RU[Электронный ресурс]: электронная библиотека / Науч. электрон. б-ка. — Москва, 1999 – Режим доступа: http://elibrary.ru/defaultx.asp – Яз. рус., англ.
4. Образовательный блог по Информационным технологиям в юридической деятельности [Электронный ресурс]: (ragimhanova.blogspot.ru)
5. Образовательный блог по направлению магистратуры «Актуальные проблемы информационного права» [Электронный ресурс]: (ragimhanovamag.blogspot.ru)
6. Федеральный портал «Российское образование» http://www.edu.ru/
7. Федеральное хранилище «Единая коллекция цифровых образовательных ресурсов» http://school-collection.edu.ru/
8. Российский портал «Открытое образование» http://www.openet.edu.ru
9. Сайт образовательных ресурсов Даггосуниверситета http://edu.dgu.ru
10. Информационные ресурсы научной библиотеки Даггосуниверситета http://elib.dgu.ru.
11. Открытая электронная библиотека http: www.diss.rsl.ru.
12. СПС «Гарант» http: www.garant.ru.
13. СПС «Консультант плюс» http: www.tls-cons.ru.

14. СПС «Право» http: www.pravo.ru.
15. Государственная автоматизированная система «Правосудие» - http://www.sudrf.ru/index.php?id=300
16. Научная библиотека Дагестанского государственного университета - http://www.elib.dgu.ru/
17. Официальный сайт открытого правительства РФ - http://openstandard.ru/rating_2015.html
18. Портал государственных программ РФ - http://programs.gov.ru/Portal/programs/list
19. Портал государственных услуг РФ - http://www.gosuslugi.ru/
20. Портал открытых данных РФ - http://data.gov.ru/
21. Собрание законодательства РФ на портале Государственной системы правовой информации - http://pravo.gov.ru/proxy/ips/?editions
22. Судебная практика – www.sud-praktika.narod.ru
23. Правительство РФ правительство.рф
24. Сервер органов государственной власти РФ www.gov.ru

10. Методические указания для обучающихся по освоению дисциплины

Настоящая программа по дисциплине «Организационно-правовое обеспечение информационной безопасности» предназначена для подготовки магистров по направлению 40.04.01 «Юриспруденция» в соответствии с требованиями, отраженными в Федеральных государственных образовательных стандартах высшего образования.

Данная учебная дисциплина содержит систематизированную систему знаний об одной из важнейших институтов информационного права – организационно-правовое обеспечение информационной безопасности.

«Организационно-правовое обеспечение информационной безопасности» является учебной дисциплиной, изучение которой наряду с другими юридическими дисциплинами имеет важное значение для подготовки юристов.

Изучение данной дисциплины требует систематической целенаправленной работы, для успешной организации которой необходимо:

1. Регулярно посещать лекции и конспектировать их, поскольку в современных условиях именно лекции являются одним из основных источников получения новой информации по изучению данного курса. Для более успешного освоения учебного материала следует использовать «систему опережающего чтения». Имея на руках рекомендованную литературу, студенты могут знакомиться с содержанием соответствующей темы по учебнику и другим источникам до лекции. Это позволит заложить базу для более глубокого восприятия лекционного материала. Основные положения темы необходимо зафиксировать в рабочей тетради. В процессе лекции студенты, уже ознакомившись с содержанием рекомендованных по теме источников, дополняют свои конспекты положениями и выводами, на которые обращает внимание лектор.

2. При подготовке к семинарскому занятию студенты должны внимательно ознакомиться с планом занятия по соответствующей теме курса, перечитать свой конспект и изучить рекомендованную дополнительную литературу. После этого, следует попытаться воспроизвести свой возможный ответ на все вопросы, сформулированные в плане семинарского занятия. Оценить степень собственной подготовленности к занятию помогут вопросы для самоконтроля, которые сформулированы по каждой теме после списка дополнительной литературы. Если в процессе подготовки к семинарскому занятию остаются какие-либо вопросы, на которые не найдены ответы ни в учебной литературе, ни в конспекте лекции, следует зафиксировать их в рабочей тетради и непременно поставить перед преподавателем на семинарском занятии.

Выступление студентов на семинаре не должно сводиться к воспроизведению лекционного материала. Оно должно удовлетворять следующим требованиям: в нем излагается теория рассматриваемого вопроса, анализ соответствующих принципов, закономерностей, понятий и категорий; выдвинутые теоретические положения подкрепляются фактами, примерами из политико-правовой жизни, практики современного государства и права, а также достижениями современной юридической науки и иных отраслей знаний. Выступающий должен продемонстрировать знание дополнительной литературы, которая рекомендована к соответствующей теме. В процессе устного выступления допускается обращение к конспекту, но следует избегать сплошного чтения.

3. Большую помощь студентам в освоении учебного курса может оказать подготовка доклада по отдельным проблемам курса. Соответствующая тематика содержится в планах семинарских занятий. Приступая к данному виду учебной работы, студенты должны согласовать с преподавателем тему доклада и получить необходимую консультацию и методические рекомендации. При подготовке доклада следует придерживаться методических рекомендаций, советов и предложений преподавателя, с тем, чтобы работа оказалась теоретически обоснованной и практически полезной. Подготовленный доклад, после его рецензирования преподавателем, может быть использован для выступления на семинаре, на заседании научного кружка, а также при подготовке к экзамену.

Следуя изложенным методическим советам и рекомендациям, каждый студент сможет овладеть тем объемом знаний, который предусмотрен учебной программой, успешно сдать экзамен, а впоследствии использовать полученные знания в своей практической деятельности.

Студенту желательно освоить порядок работы с нормативно-правовыми базами. Необходим учет (отслеживание) студентом изменений в законодательстве, а также корректировка использования в освоении дисциплины учебной литературы и судебной практики в соответствии с изменениями в законодательстве.

В силу особенностей индивидуального режима подготовки каждого студента, представляется, что такое планирование должно осуществляться

студентом самостоятельно, с учетом индивидуальных рекомендаций и советов преподавателей дисциплины в соответствии с вопросами и обращениями студентов при встречающихся сложностях в подготовке и освоении дисциплины.

В соответствии с настоящей рабочей программой дисциплины на лекционных занятиях планируется охватить все основные темы дисциплины. Вместе с тем, по понятным причинам одним наиболее важным и актуальным темам будет уделено больше внимания, другим меньше. В связи с этим, темы в меньшей степени охваченные материалами лекций, студентам необходимо изучать самостоятельно. По отдельным возникающим вопросам обучения представляется полезным обращаться за советом к преподавателям.

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

При изучении данного курса студенты должны обращаться к информационно-правовой справочной системе Гарант, Консультант плюс, образовательному блогу ragimhanovamag.blogspot.com, Официальным сайтам Министерства связи и телекоммуникации, Государственные услуги, Государственные программы, Порталу открытых данных.

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

Лекционный зал, оборудованный проекционным оборудованием и выходом в Интернет, компьютерный класс в стандартной комплектации для практических; доступ к сети Интернет (во время самостоятельной подготовки и на практических занятиях), учебники и практикумы.