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

Информационная безопасность

Образовательная программа:

40.03.01Юриспруденция

Профиль подготовки:

уголовно-правовой

Уровень высшего образования
бакалавриат

Форма обучения
очная

Статус дисциплины: **вариативная**

Махачкала
2020 год

Рабочая программа дисциплины «Информационная безопасность» составлена в 2020 г. в соответствии с требованиями ФГОС ВО по направлению Юриспруденция (уровень бакалавриат) от «01» декабря 2016 г. №1511

Разработчик(и): кафедра «Информационное право и информатика»,
Рагимханова Динара Айдабековна, к.э.н., доцент,
Магдилова Лариса Владимировна, к.э.н., доцент.

Рабочая программа дисциплины одобрена:

На заседании кафедры информационного права и информатики

от «19» 03 2020 г., протокол № 8

Зав. кафедрой _____ Абдусаламов Р.А.
(подпись)

На заседании Методической комиссии юридического института

от «25» 03 2020г., протокол № 7

Председатель _____ Арсланбекова А.З.
(подпись)

Рабочая программа дисциплины согласована с учебно-методическим управление «26» 03 2020г. _____
(подпись)

Аннотация рабочей программы дисциплины

Дисциплина «Информационная безопасность» входит в вариативную часть образовательной программы бакалавриата по направлению подготовки 40.03.01Юриспруденция.
Дисциплина реализуется в юридическом институте кафедрой информационного права и информатики.

Содержание дисциплины охватывает круг вопросов, связанных с изучением основных понятий, принципов информационной безопасности и методов правового регулирования информационных отношений в информационной сфере. Рассматриваются 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: общекультурных –ОК-3, ОК-4, профессиональных - ПК-6, ПК-15, ПК-16.

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 зачета.

Объем дисциплины 2 зачетных единиц, в том числе в академических часах по видам учебных занятий

Семестр	Учебные занятия							Форма промежуточной аттестации (зачет, дифференцированный зачет, экзамен
	в том числе							
	Контактная работа обучающихся с преподавателем						СРС, в том числе экзамен	
	Всего	из них						
		Лекции	Лабораторные занятия	Практические занятия	КСР	консультации		
6	72	14		14			44	зачет

1. Цели освоения дисциплины

Целями освоения дисциплины «Информационная безопасность» являются:

- формирование и развитие у будущих юристов теоретических знаний и практических навыков, связанных с организацией информационной безопасности, планированием, подготовкой и реализацией процесса обеспечения информационной безопасности;
- ознакомление студентов с современными системами информационной безопасности, методами и средствами защиты информации, организационными и правовыми мерами по информационной защите;
- расширение теоретической базы в сфере изучения процессов создания и развития информационного общества, правового регулирования этих процессов, формирования и развития информационного законодательства.

2.Место дисциплины в структуре ОПОП бакалавриата

Дисциплина входит в вариативную часть образовательной программы бакалавриата по направлению подготовки 40.03.01 Юриспруденция и изучается в шестом семестре.

Дисциплина логически и содержательно-методически связана с

а) теорией государства и права, формирующей знания в области механизма государства, системе права, механизма и средств правового регулирования, реализации права, особенностей правового развития России;

б) конституционным правом, определяющим особенности конституционного строя, правового положения граждан, форм государственного устройства, организации и функционирования системы органов государства и местного самоуправления в России, в частности провозглашение права граждан на свободный поиск, получение и потребление информации любым законным способом.

в) информационным правом, формирующей знания об объектах, предметах, принципах, методах, способах правового регулирования, основных информационных правах и свободах.

г) отраслями материального и процессуального права (административного, гражданского, гражданско-процессуального, уголовного, уголовно-процессуального, международного, трудового), характеризующиеся основными понятиями, категориями, институтами, правовыми статусами субъектов, особенностями правоотношений.

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

Компетенции	Формулировка компетенции из ФГОС	Планируемые результаты обучения (показатели достижения

	ВО	заданного уровня освоения компетенций)
ОК-3	Владение основными методами, способами и средствами получения, хранения, переработки информации, имеет навыки работы с компьютером как средством управления информацией.	Знать: основные методы, способы и средства получения, хранения, переработки информации; закономерности обращения информации в правовой сфере; методы и способы защиты информации; методы законного получения, хранения и переработки информации. Уметь: пользоваться основными методами, способами и средствами получения, хранения, переработки информации; соблюдать основные требования информационной безопасности, в том числе защите государственной, служебной и иных видов тайн; получать, хранить, перерабатывать использовать информацию; правильно давать оценку информации. Владеть: навыками поиска, получения, хранения, переработки и защиты информации, в том числе государственной, служебной, профессиональной и иных видов тайн; навыками защиты персональных данных; навыками сбора и обработки информации; навыками анализа информации; навыками обработки информации.
ОК-4	Способность работать с информацией в глобальных компьютерных сетях	Знать: основы работы с информацией в глобальных компьютерных сетях; информационно-правовые технологии (правовые порталы) с помощью которых осуществляется поиск информации в сети Интернет. Уметь: работать в глобальных компьютерных сетях; решать любые юридические задачи, связанные с добыванием в сети Интернет правовых материалов. Владеть: навыками обработки правовых материалов, найденных в среде правовых порталов.
ПК-6	Способность правильно квалифицировать факты и обстоятельства	Знать: понятие, виды и способы квалификации фактов и обстоятельств, этапы юридической квалификации, содержание источников информационной безопасности, с точки зрения разных авторов на проблемные вопросы Уметь: правильно давать юридическую оценку фактам и обстоятельствам, обоснованно применять нормы права при

		правовой квалификации обстоятельств. Владеть: юридической терминологией отраслей права, позволяющей юридически правильно квалифицировать факты и обстоятельства
ПК- 15	Способность толковать различные правовые акты	Знать: понятие, виды и способы толкования правовых норм Уметь: анализировать содержание правовых норм, использовать различные приемы толкования для уяснения точного смысла нормы при квалификации фактов и обстоятельств Владеть: навыками работы по толкованию правовых норм
ПК-16	Способность давать квалифицированные юридические заключения и консультации в конкретных видах юридической деятельности	Знать: понятие, виды и способы квалификации фактов и обстоятельств, правовые явления и методы их анализа Уметь: оценивать правовые явления и формулировать выводы и предложения на основе их анализа, давать разъяснения по правовым вопросам в рамках своей профессиональной деятельности Владеть навыками работы по толкованию правовых норм, навыками общения, методами аргументированного, обоснованного убеждения

4. Объем, структура и содержание дисциплины

4.1. Объем дисциплины составляет 2 зачетных единиц, 72 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	Практические занятия	Лабораторные занятия	Контроль самост. раб.		
	Модуль 1. Основы информационной безопасности								
1	Основные понятия курса «Информационная безопасность»	6		2	2			6	Контрольный опрос
2	Информационная безопасность в системе национальной	6		2	2			6	Контрольный опрос

	безопасности РФ								
3	Правовые основы обеспечения информационной безопасности	6		2	2			4	Контрольный опрос
4	Организационное обеспечение информационной безопасности	6		2	2			4	Контрольный опрос, тестирование
	Итого по модулю 1:			8	8			20	
	Модуль 2. Методы защиты информации и ответственность в информационной сфере								
5	Правовые режимы конфиденциальной информации	6		2	2			6	Контрольный опрос
6	Компьютерные преступления	6		2	2			6	Контрольный опрос, тестирование
7	Ответственность за правонарушения в информационной сфере	6		2	2			6	Контрольный опрос, рефераты
	Итого по модулю 2:			6	6			24	
	Промежуточный контроль								зачет
	ИТОГО:			14	14			44	

4.3. Содержание дисциплины, структурированное по темам (разделам)

Модуль 1. Основы информационной безопасности

Тема 1. Основные понятия курса «Информационная безопасность».

Понятие и признаки информации. Классификация информации по роли, в которой она выступает в правовой системе, по доступу к ней, по порядку предоставления и распространения.

Структура информационной сферы и характеристика ее элементов. Конституционные гарантии прав на информацию и механизм их реализации.

Понятие и структура информационной безопасности. Субъекты и объекты правоотношений в области информационной безопасности. Понятия и виды защищаемой информации по российскому законодательству.

Принципы обеспечения информационной безопасности. Защита интересов личности, общества, государства от угроз воздействия недоброкачественной информации, от нарушения порядка распространения информации. Защита информации, информационных ресурсов и информационных систем от угроз несанкционированного и неправомерного воздействия посторонних лиц. Защита прав и свобод в информационной сфере в условиях информатизации.

Тема 2. Информационная безопасность в системе национальной безопасности РФ

Национальная безопасность РФ. Обеспечение национальной безопасности. Национальные интересы личности. Национальные интересы общества. Национальные интересы государства.

Система органов управления в информационной сфере. Система обеспечения информационной безопасности РФ. Функции системы обеспечения информационной безопасности РФ. Полномочия Президента РФ, Парламента РФ, высших органов судебной власти РФ, Совета безопасности РФ, Прокуратуры РФ, Уполномоченного по правам человека РФ в информационной сфере. Полномочия Правительства РФ и основных федеральных органов исполнительной власти в информационной сфере.

Тема 3. Правовые основы обеспечения информационной безопасности.

Принципы, задачи, функции и стандарты обеспечения информационной безопасности. Законодательство в сфере обеспечения информационной безопасности и его место в системе российского законодательства.

Угрозы нарушения конфиденциальности, целостности, доступности информации. Основные причины утечки информации.

Тема 4. Организационное обеспечение информационной безопасности

Виды угроз информационной безопасности. Цели и задачи организационной защиты информации. Виды угроз информационной безопасности. Модели нарушителей. Основные направления организационной защиты на объекте. Структура средств организационной защиты информации.

Роль персонала в обеспечении информационной безопасности объекта. Требования к сотрудникам организации, допущенным к секретной (конфиденциальной) информации. Основные критерии приема на работу, связанную с сохранением тайны.

Модуль 2. Методы защиты информации и ответственность в информационной сфере

Тема 5. Правовой режим конфиденциальной информации.

Понятие правового режима, правового режима информации. Основные признаки правового режима информации.

Конфиденциальность информации. Тайна. Государственная тайна как особый вид защищаемой информации и ее характерные признаки. Принципы, механизмы и процедура отнесения сведений к государственной тайне, их засекречивания и рассекречивания. Органы защиты государственной тайны и их компетенция. Порядок допуска и доступа к государственной тайне. Перечень и содержание организационных мер, направленных на защиту государственной тайны.

Персональные данные, служебная тайна, коммерческая тайна, банковская тайна, тайна следствия и судопроизводства, профессиональная тайна. Основные требования, предъявляемые к организации защиты конфиденциальной информации.

Тема 6. Компьютерные преступления

Преступления в сфере компьютерной информации. Неправомерный доступ к компьютерной информации. Создание, использование и распространение вредоносных программ для ЭВМ. Нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети. Признаки и элементы состава преступления.

Информационная война. Информационное оружие. Особенности ведения информационной войны. Основные отличия информационного оружия от обычных средств вооружения. Цели использования информационного оружия. Методы организации защиты от информационного оружия.

Расследование компьютерного преступления. Законодательство РФ о компьютерных преступлениях.

Тема 7. Ответственность за правонарушения в информационной сфере.

Понятие и характеристика информационного правонарушения и преступления.

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.

Семинарские занятия.

Модуль 1. Основы информационного права

Тема 1. Основные понятия курса «Информационная безопасность».

Вопросы для обсуждения:

1. Понятие и признаки информации.
2. Информационной сфера и ее элементы.
3. Понятие и структура информационной безопасности.

Тема 2. Информационная безопасность в системе национальной безопасности РФ

Вопросы для обсуждения:

1. Понятие национальной безопасности.
2. Принципы обеспечения информационной безопасности.
3. Национальные интересы в информационной сфере.

Тема 3. Правовые основы обеспечения информационной безопасности.

Вопросы для обсуждения:

1. Доктрина информационной безопасности РФ об основных угрозах в информационной сфере и их источниках.
2. Угрозы нарушения конфиденциальности, целостности, доступности информации.
3. Основные причины утечки информации.
4. Правовые средства обеспечения безопасности информации.

Тема 4. Организационное обеспечение информационной безопасности

Вопросы для обсуждения:

1. Концептуальные положения организационного обеспечения информационной безопасности.
2. Угрозы информационной безопасности на объекте.
3. Организация службы безопасности объекта.

Модуль 2. Методы защиты информации и ответственность в информационной сфере

Тема 5. Правовой режим конфиденциальной информации.

Вопросы для обсуждения:

1. Правовой режим информации: понятие, признаки, содержание.
2. Виды информации ограниченного доступа.
3. Требования, предъявляемые к организации защиты конфиденциальной информации.

Тема 6. Компьютерные преступления

Вопросы для обсуждения:

1. Понятие и виды компьютерных преступлений.
2. Лица, совершающие компьютерные преступления.
3. Особенности квалификации компьютерных преступлений.

Тема 8. Ответственность за правонарушения в информационной сфере.

Вопросы для обсуждения:

1. Понятие и характеристика правонарушений в сфере компьютерной информации.
2. Криминалистическая характеристика преступлений в сфере компьютерной информации.
3. Ответственность за правонарушения в сфере информации.

5. **Образовательные технологии**

В соответствии с требованиями Федерального государственного образовательного стандарта высшего образования по направлению подготовки 40.03.01 - «юриспруденция» (квалификация «бакалавр») реализация компетентностного подхода должна предусматривать широкое использование в учебном процессе активных и интерактивных форм проведения занятий (компьютерных симуляций, деловых игр, разбор конкретных ситуаций) в сочетании с внеаудиторной работой с целью формирования и развития профессиональных навыков обучающихся.

Удельный вес занятий, проводимых в интерактивных формах, определяется главной целью программы, особенностью контингента обучающихся и содержанием конкретных дисциплин, и в целом в учебном процессе они должны составлять не менее 20% аудиторных занятий.

Для реализации компетентностного подхода все проводимые занятия, в том числе самостоятельная работа студентов, предусматривают сочетание передовых методических приемов с новыми образовательными информационными технологиями и достижениями науки и техники. Используются современные формы и методы обучения (тренинги, исследовательские методы, проблемное и проектное обучение), направленные на развитие творческих способностей и самостоятельности студентов, привитие им интереса к исследовательской работе, формирование убеждения о необходимости при решении любых прикладных задач использовать инновационные информационные технологии.

В ходе освоения учебного курса «Информационная безопасность» при проведении аудиторных занятий используются следующие образовательные технологии: лекции, семинарские занятия с использованием активных и интерактивных форм проведения занятий, моделирование и разбор деловых

ситуаций, использование тестовых заданий и задач на практических занятиях.

Лекционные занятия проводятся в аудиториях с применением мультимедийных технологий и предусматривают развитие полученных теоретических знаний с использованием рекомендованной учебной литературы и других источников информации, в том числе информационных ресурсов глобальной сети Интернет.

На семинарских занятиях и в часы консультаций преподаватель дает оценку правильности выбора конкретными студентами средств и технологий разрешения поставленных задач и проблем, привлекая к дискуссии других студентов.

При организации самостоятельной работы занятий используются следующие образовательные технологии: индивидуальное и групповое консультирование, разбор конкретных ситуаций; тестирование; подготовка докладов, рефератов; привлечение студентов к научно-исследовательской деятельности.В ходе самостоятельной работы, при подготовке к плановым занятиям, контрольной работе, зачету студенты анализируют поставленные преподавателем задачи и проблемы и с использованием инструментальных средств офисных технологий, учебно-методической литературы, правовых баз СПС, содержащих специализированные подборки по правовым вопросам, сведений, найденных в глобальной сети Интернет, находят пути их разрешения.

Промежуточные аттестации проводятся в форме контрольной работы и модульного тестирования.

6. Учебно-методическое обеспечение самостоятельной работы студентов.

Самостоятельные формы учебной работы студента юридического института имеют своей целью приобретение им системы знаний по дисциплине «Информационная безопасность». Используя лекционный материал, доступный учебник или учебное пособие, дополнительную литературу, проявляя творческий подход, студент готовится к практическим занятиям, рассматривая их как пополнение, углубление, систематизация своих теоретических знаний.

Самостоятельная работа студента начинается с внимательного ознакомления с каждой темой курса, с изучением вопросов. Они ориентируют студента, показывают, что он должен знать по данной теме. Вопросы темы как бы накладываются на соответствующую главу избранного учебника или учебного пособия. В итоге должно быть ясным, какие вопросы темы программы учебного курса раскрыты в данном учебном материале, а какие вообще опущены.

Проработка лекционного курса является одной из важных активных форм самостоятельной работы. Лекция преподавателя не является озвученным учебником, а представляет плод его индивидуального

творчества. В своих лекциях преподаватель стремится преодолеть многие недостатки, присущие опубликованным учебникам, учебным пособиям, лекционным курсам. В лекциях находят освещение сложные вопросы, которые вызывают затруднения у студентов.

Студенту важно понять, что лекция есть своеобразная творческая форма самостоятельной работы. Надо пытаться стать активным соучастником лекции: думать, сравнивать известное с вновь получаемыми знаниями, войти в логику изложения материала лектором, по возможности вступать с ним в мысленную полемику, следить за ходом его мыслей, за его аргументацией, находить в ней кажущиеся вам слабости.

Одним из видов самостоятельной работы студентов является написание творческой работы по заданной либо согласованной с преподавателем теме. Творческая работа (реферат) представляет собой оригинальное произведение объемом до 10 страниц текста, посвященное какой-либо значимой проблеме информационной безопасности личности, общества и государства. Работа не должна носить описательный характер, большое место в ней должно быть уделено аргументированному представлению своей точки зрения студентами, критической оценке рассматриваемого материала.

При оценивании результатов освоения дисциплины (текущей и промежуточной аттестации) применяется балльно-рейтинговая система, внедренная в Дагестанском государственном университете. В качестве оценочных средств на протяжении семестра используется тестирование, контрольные работы студентов, творческая работа, итоговое испытание.

Тестовые задания могут формулироваться в форме тестов с одним правильным ответом, тестов с несколькими правильными ответами, тестов, направленных на сопоставление понятий или расположения в определенной последовательности, а также тестов с открытым ответом.

Творческая работа оформляется в виде набора материалов по актуальным проблемам информационного права, в том числе обработанные результаты социологического опроса по заранее составленной анкете, видео-интервью, презентация по проблеме и др.

Основными видами самостоятельной работы студентов являются:

1) изучение рекомендованной литературы, поиск дополнительного материала;
2) работа над темами для самостоятельного изучения;
3) подготовка докладов, рефератов, презентаций;
4) тестирование;
5) участие студентов в научно-исследовательской деятельности;
6) подготовка к зачету.

№п/п	**Вид самостоятельной работы**	**Вид контроля**	**Учебно-методическое обеспечение**

1.	Изучение рекомендованной литературы, поиск дополнительного материала	Опрос, тестирование, коллоквиум	См. разделы 6 и 7 данного документа
2.	Работа над темами для самостоятельного изучения	Опрос, тестирование, коллоквиум	См. разделы 6 и 7 данного документа
3.	Подготовка докладов, рефератов и презентаций	Прием доклада, реферата, презентации, и оценка качества их исполнения	См. разделы 6 и 7 данного документа
4.	Тестирование	Использование тренинго-тестирующей системы «Консультант-Плюс» для оценки знаний	См. разделы 6 и 7 данного документа
5.	Участие студентов в научно-исследовательской деятельности	Прием материалов социологических опросов, интервью, видео-материалов, научных статей и тезизов	См. разделы 6 и 7 данного документа
6.	Подготовка к зачету	Промежуточная аттестация в форме зачета	См. раздел 7 данного документа

Нормативно-правовые акты

1. Конституция Российской Федерации. – М.: Юрид. лит., 1994.
2. Всеобщая декларация прав человека (принята на третьей сессии Генеральной Ассамблеи ООН резолюцией 217 А (III) от 10 декабря 1948 г.) // Российская газета. 10 декабря 1998г.
3. Международный пакт о гражданских и политических правах (Нью-Йорк, 19 декабря 1966г.) //Сборник действующих договоров, соглашений

и конвенций, заключенных с иностранными государствами, М., 1978 г., вып. XXXII, с. 44.
4. Протокол N1 к Конвенции о защите прав человека и основных свобод ETS N 009 (Париж, 20 марта 1952г.) // Собрание законодательства Российской Федерации, 18 мая 1998г., N 0, ст. 2143.
5. Хартия Глобального информационного общества (Окинава) // Дипломатический вестник. - 2000. - №8.
6. О безопасности: Федеральный закон от 8 декабря 2010 года N 390-ФЗ.
7. О безопасности критической информационной инфраструктуры Российской Федерации: Федеральный закон от 26.07.2017 N 187-ФЗ
8. О государственной тайне: Федеральный закон от 21 июля 1993г. № 5485 – 1 – ФЗ // СЗ РФ. – 1993. - №41. – Ст. 4673.
9. О коммерческой тайне: Федеральный закон от 29 июля 2004 г. N 98-ФЗ // СЗ РФ. 2004. N 32. Ст. 3283.
10. О персональных данных: Федеральный закон от 27 июля 2006 г. № 152 – ФЗ // СЗ РФ. – 2006. - №31 (1ч.). – Ст. 3451.
11. О ратификации Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных: Федеральный закон от 19 декабря 2005 г. N 160-ФЗ // СЗ РФ. 2005. N 52. Ч. I. Ст. 5573.
12. Об информации, информационных технологиях и о защите информации: Федеральный закон от 27 июля 2006 г. № 149 – ФЗ // СЗ РФ. – 2006. - №31 (1ч.). – Ст. 3448.
13. Об электронной подписи: Федеральный закон от 6 апреля 2011 г. № 10 // Собрание законодательства РФ, 11.04.2011, N 15, ст. 2036.
14. Об обеспечении доступа к информации о деятельности судов в Российской Федерации: Федеральный закон от 22 декабря 2008 г. № 262 // Собрание законодательства РФ, 29.12.2008, N 52 (ч. 1), ст. 6217.
15. Об обеспечении доступа к информации о деятельности государственных органов и органов местного самоуправления: Федеральный закон от 9 февраля 2009 г. N 8 // Собрание законодательства РФ, 16.02.2009, N 7, ст. 776.
16. Об организации предоставления государственных и муниципальных услуг: Федеральный закон от 27 июля 2010 г. N 210 // Собрание законодательства РФ, 02.08.2010, N 31, ст. 4179.
17. Стратегия развития информационного общества в Российской Федерации: Утверждена Президентом Российской Федерации В.Путиным 7 февраля 2008 г., № ПР-212. //Российская газета, 16.02.2008, N 34.
18. Доктрина информационной безопасности Российской Федерации: Указ Президента РФ от 05.12.2016 N 646 "Об утверждении Доктрины информационной безопасности Российской Федерации". //Собрание законодательства РФ, 12.12.2016, N 50, ст. 7074
19. Об утверждении Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных: Постановление Правительства Российской Федерации от 17 ноября 2007 года № 781// СЗ РФ. – 2007.

20. Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации: Постановление Правительства Российской Федерации от 15 сентября 2008 г. № 687// СЗ РФ. – 2008.
21. Концепция региональной информатизации до 2010 года: Распоряжение Правительства Российской Федерации от 17 июля 2006 г. N 1024-р. //Собрание законодательства РФ, 24.07.2006, N 30, ст. 3419.
22. Концепция формирования в Российской Федерации электронного правительства до 2010 года: Распоряжение Правительства Российской Федерации от 6 мая 2008 г. N 632-р. //Собрание законодательства РФ, 19.05.2008, N 20, ст. 2372.
23. О государственной программе Российской Федерации «Информационное общество (2011 - 2020 годы): Распоряжение Правительства РФ от 20.10.2010 N 1815-р (ред. от 20.07.2013) //Собрание законодательства РФ, 15.11.2010, N 46, ст. 6026.
24. О правительственной комиссии Республики Дагестан по внедрению информационных технологий: Постановление Правительства Республики Дагестан от 19 июля 2010 г. N 258. //Собрание законодательства Республики Дагестан, 30.07.2010, N 14, ст. 717.
25. О республиканском реестре государственных и муниципальных услуг (функций): Постановление Правительства Республики Дагестан от 30 июня 2010 г. N 234. //Собрание законодательства Республики Дагестан, 30.06.2010, N 12 ст. 611.
26. Об информационной системе поддержки оказания органами исполнительной власти Республики Дагестан и органами местного самоуправления государственных услуг с использованием электронных средств коммуникаций по принципу «одного окна»: Постановление Правительства Республики Дагестан от 20 июля 2009 г. N 242. //Собрание законодательства Республики Дагестан, 31.07.2009, N 14, ст. 712.
27. Республиканская целевая программа «Развитие электронного правительства Республики Дагестан до 2017 года»: Постановление Правительства Республики Дагестан от 12.09.2013 года №432.

Задачи для самостоятельной работы

1. Обвиняемый Огурцов, в отношении которого была применена мера пресечения в виде подписки о невыезде, проходящий по громкому политическому делу, дал интервью зарубежной телекомпании, предоставив для публикации текст, полностью совпадающий с текстом протокола его допроса следователем. Имело ли место в данном случае разглашение данных предварительного расследования?

2. Федорова заподозрила мужа в измене и решила получить у оператора сотовой связи распечатку сведений о его телефонных переговорах за последний месяц. С этой целью она обратилась к своей подруге адвокату и получила от нее стандартный адвокатский запрос на имя оператора, в котором говорилось, что Федоров якобы является клиентом данного адвоката

и в целях его защиты адвокату необходимо получить детализацию звонков за месяц. Федорова отправилась в офис оператора сотовой связи, предъявила свой паспорт, свидетельство о браке и попросила детализацию звонков. Ей было отказано. Затем она достала адвокатский запрос и предъявила его начальнику офиса, который взял паспорт Федоровой, свидетельство о браке, запрос и отправился к юристу. Проконсультируйте начальника офиса. Какие действия ему следует предпринять?

3. В целях понуждения должников к погашению задолженности Водоканал поручил расклеить на подъездах многоквартирных домов пофамильные списки жильцов, имеющих задолженность более, чем за шесть месяцев. Что и было сделано. Спустя некоторое время инициативная группа горожан обратилась по этому поводу с коллективной жалобой в прокуратуру. Какое решение следует принять по жалобе?

4. В 2011 году в поле зрения ФСБ попал предприниматель, пытавшийся продать иностранцам документы с грифом «совершенно секретно». Деятельность коммерсанта была пресечена, сам он задержан, возбуждено уголовное дело. Но Министерство обороны дало заключение, что сведения, содержащиеся в планируемых к реализации документах, утратили актуальность и государственной тайны не составляют, просто не были вовремя рассекречены. В результате уголовное дело на основании полученного заключения было прекращено. Однако следователь остался при своем мнении. Он считал, что предприниматель действовал с умыслом, так как считал, что продает совершенно секретные документы. *Как вы считаете, имелись ли в данной ситуации законные основания для прекращения уголовного преследования?*

5. Арефьева обратилась в суд с иском к банку об отзыве ее персональных данных из бюро кредитных историй. В исковом заявлении ссылалась на Закон о персональных данных и утверждала, что все ее персональные данные могут быть в любое время исключены из общедоступных источников. Представитель ответчика возражал, пояснил суду, что особенности обработки данных могут устанавливаться законом, определяющим цель сбора и обработки данных, к числу таких норм относится закон о кредитных историях. Возможность отзыва кредитной истории законом о кредитных историях не предусматривается. Просил суд в иске отказать. Решите дело.

Примерная тематика рефератов (творческих работ)

1. Понятие, структура и признаки информации с ограниченным доступом.
2. Понятие и виды вредной информации.
3. Персональные данные и тайна частной жизни: общее и отличия.
4. Правовое регулирование электронной подписи
5. Правовое регулирование в сфере массовой информации
6. Правовое регулирование банковской тайны
7. Правовое регулирование государственной тайны

8. Правовое регулирование коммерческой тайны
9. Правовое регулирование рекламной деятельности
10. Правовые основы защиты персональных данных
11. Уголовная ответственность за правонарушения в информационной сфере
12. Административная ответственность за правонарушения в информационной сфере
13. Гражданско-правовая ответственность за правонарушения в информационной сфере.
14. Правовые проблемы борьбы со «спамом»
15. Электронные деньги: проблемы правового регулирования
16. Правовое регулирование информационных технологий в области электронной коммерции
17. Правовое регулирование информационных технологий в области рекламы и маркетинга в Интернет
18. Правовое регулирование информационных технологий в области электронных банковских услуг
19. Правовое регулирование информационных технологий в области электронного документооборота
20. Стандартизация, сертификация и лицензирование в информационной сфере

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: основные методы, способы и средства получения, хранения, переработки информации; роль обобщения, анализа, восприятия информации; как отделить правильную информацию от неправильной (от дезинформации), как разумно обобщить, устранить излишние детали; что грамотная постановка цели неизбежно приведет необходимому результату; Уметь: организовать умственную деятельность; анализировать возможные пути достижения поставленных целей; работать с компьютером как средством управления информацией Владеть: законами и требованиями логики; методами правового регулирования информационных отношений, возникающих при осуществлении основных информационных процессов в информационной сфере.	Устный опрос, разбор практических ситуаций
ОК-4	Знать: основные виды информационных правоотношений в Интернете; особенности способов правового регулирования	Устный опрос, разбор

	интернет-отношений, структуру информационного законодательства, регулирующего интернет-отношения. Уметь: правильно применять нормы информационного права при регулировании публично-правовых и частно-правовых отношений в Интернете. Владеть: навыками сбора и обработки информации, имеющей значение для реализации правовых норм в информационной сфере, в частности в виртуальной среде Интернета.	практических ситуаций, тестирование
ПК-6	Знать: понятие, виды и способы квалификации фактов и обстоятельств, этапы юридической квалификации, содержание источников информационнй безопасности, точки зрения разных авторов на проблемные вопросы Уметь: правильно давать юридическую оценку фактам и обстоятельствам, обоснованно применять нормы права при правовой квалификации обстоятельств. Владеть: юридической терминологией отраслей права, позволяющей юридически правильно квалифицировать факты и обстоятельства.	Устный опрос, разбор практических ситуаций, тестирование
ПК-15	Знать: понятие, виды и способы толкования правовых норм. Уметь: анализировать содержание правовых норм, использовать различные приемы толкования для уяснения точного смысла нормы при квалификации фактов и обстоятельств. Владеть: навыками работы по толкованию правовых норм.	Устный опрос, разбор практических ситуаций, тестирование
ПК-16	Знать: понятие, виды и способы квалификации фактов и обстоятельств, правовые явления и методы их анализа. Уметь: оценивать правовые явления и формулировать выводы и предложения на основе их анализа, давать разъяснения по правовым вопросам в рамках своей профессиональной деятельности. Владеть навыками работы по толкованию правовых норм, навыками общения, методами аргументированного, обоснованного убеждения.	Устный опрос, письменный опрос, разбор практических ситуаций, тестирование

7.2 Типовые контрольные задания

Примерные тестовые задания для проведения текущего и промежуточного контроля

1. Информационная сфера (среда) – это

) сфера деятельности, связанная с созданием, распространением, преобразованием и потреблением информации

) сфера деятельности, связанная с правовым регулированием информационных отношений, возникающих в обществе

) процесс сбора, обработки, накопления, хранения, поиска, получения, распространения и потребления информации

2. Информационная сфера как сфера правового регулирования представляет собой

) совокупность субъектов права, объектов права, социальных отношений, регулируемых правом или подлежащих правовому регулированию

) процесс сбора, обработки, накопления, хранения, поиска, получения, распространения и потребления информации
) социальные (общественные) отношения, возникающие при выполнении информационных процессов и подлежащих правовому регулированию
3. Структура информационного законодательства включает
) информационно-правовые нормы международного законодательства; информационно-правовые нормы Конституции РФ; нормативно-правовые акты отрасли информационного законодательства
) международные акты информационного законодательства; информационно-правовые нормы Конституции РФ; отрасли законодательства, акты которых целиком посвящены вопросам информационного законодательства
) информационно-правовые нормы Конституции РФ; отрасли законодательства, акты которых целиком посвящены вопросам информационного законодательства; отрасли законодательства, акты которых включают отдельные информационно-правовые нормы информационных ресурсов и предоставлении информации из них пользователю
4. Под объектами информационных правоотношений понимают
) блага, существующие в формах информации, документированной информации и информационных систем, по поводу которых возникает и осуществляется деятельность участников этих правоотношений
) блага, возникающие при осуществлении поиска, получения и потребления информации, информационных ресурсов, информационных продуктов, информационных услуг
) блага, возникающие при создании и применении информационных систем, их сетей, средств обеспечения;
) блага, возникающие при создании средств и механизмов информационной безопасности
5. 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
6. Правовой режим объекта правоотношения может быть
) общим (или первичным) и специальным (или вторичным)
) императивным и диспозитивным
) открытым и ограниченным

) публичноправовым и частноправовым
7. 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
8. 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
9. 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
10. 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
11. 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

12. 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»

13. 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

14. Информационные правонарушения обладают следующими признаками, имеющими существенное значение для этого класса правонарушений

) общими и специальными

) регулятивными и охранительными

) абсолютными и относительными

) императивными и диспозитивными

15. 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
16. 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
17. 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
18. 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
19. 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 зачету

1. Понятие и признаки информации.
2. Информационная сфера и ее элементы.
3. Понятие безопасности и информационной безопасности.
4. Основные составляющие информационной безопасности.
5. Субъекты и объекты правоотношений в области информационной безопасности.
6. Понятие национальной безопасности.
7. Интересы личности в области информационной безопасности.
8. Интересы общества в области информационной безопасности.
9. Интересы государства в области информационной безопасности.
10. Понятие государственной информационной политики.
11. Основные положения государственной политики обеспечения информационной безопасности РФ.
12. Система обеспечения информационной безопасности РФ и ее основные функции.
13. Концептуальные положения организационного обеспечения информационной безопасности.
14. Понятие и виды угроз безопасности.
15. Угрозы информационной безопасности на объекте.
16. Организация службы безопасности объекта
17. Правовой режим информации: понятие, признаки, содержание.
18. Виды информации ограниченного доступа.
19. Требования, предъявляемые к организации защиты конфиденциальной информации.
20. Виды компьютерных преступлений.
21. Особенности квалификации компьютерных преступлений.
22. Преступления имущественного характера, которые совершаются с применением или в отношении средств компьютерной техники.
23. Доктрина информационной безопасности РФ об основных угрозах в информационной сфере и их источниках.
24. Право и законодательство в сфере обеспечения информационной безопасности и их место в системе российского права и законодательства России.
25. Угрозы нарушения конфиденциальности, целостности, доступности информации.
26. Основные причины утечки информации.
27. Режим, правовой режим, правовой режим информации: определение.
28. Понятие правового режима информации и его основные признаки.

29. Понятие правового режима информации и его типовые элементы.
30. Характеристика видов правового режима информации с точки зрения его обязательности и объекта.
31. Общий правовой режим информации.
32. Специальные правовые режимы информации.
33. Тайна как специальный правовой режим.
34. Конфиденциальность как специальный правовой режим.
35. Государственная тайна и ее защита.
36. Защита персональных данных.
37. Защита коммерческой тайны.
38. Профессиональная тайна.
39. Служебная тайна.
40. Виды информационного законодательства, применяемые для регулирования отношений в Интернет.
41. Угроза безопасности, обеспечение безопасности: понятие.
42. Характеристика национальных интересов в Концепции национальной безопасности РФ.
43. Информационная безопасность: понятие, первоочередные меры по обеспечению, общие методы.
44. Информационная безопасность и информационные войны: понятие.
45. История информационных войн.
46. Информационная безопасность и информационное оружие: понятие.
47. Правонарушение и информационное правонарушение: определение, признаки, юридическая ответственность и основание привлечения к ответственности.
48. Состав информационного правонарушения.
49. Уголовная ответственность за информационное преступление.
50. Административная и гражданско-правовая ответственность в информационной сфере.

7.3. 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 - 60% и промежуточного контроля - 40%.

Текущий контроль по дисциплине включает:

- - участие на практических занятиях -40 баллов,
- выполнение домашних заданий - 10баллов,
- выполнение аудиторных контрольных работ - 10 баллов.

Промежуточный контроль по дисциплине включает:

- письменная контрольная работа (или коллоквиум) - 30 баллов,
- тестирование - 10 баллов.

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

а) основная литература:

1. Бачило И.Л. Информационное право: учеб. для магистров / Бачило, Иллария Лаврентьевна; Ин-т гос. и права РАН, Акад. правовой ун-т (Ин-т). - 3-е изд., перераб. и доп. - М. : Юрайт, 2013. - 564 с.
2. Бачило И.Л. Информационное право: учебник / Бачило, ИлларияЛаврентьевна ; Ин-т гос. и права Рос. акад. наук, Академический правовой ун-т (ин-т). - 2-е изд., перераб. и доп. - М. : Юрайт, 2011. - 522 с. - (Магистр).
3. Мельников В.П., Клеймёнов С.А., Петраков А.М. Информационная безопасность и защита информации: учебник - Москва : Academia, 5-е издание, 2011
4. Организационное и правовое обеспечение информационной безопасности: учебник и практикум / под ред. Поляковой Т.А., Стрельцова А.А. – М.: Юрайт, 2017. – 325 с.
5. Городов О.А. Информационное право [Электронный ресур с]: учебник для бакалавров. – М.: Издательство Проспект, 2016. – 303 с. – URL: http://нэб.рф/catalog/000199_000009_008578609/ - ЭБС «НЭБ».
6. 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».
7. Информационное право: учеб. пособие / Р. А. Абдусаламов; Минобрнауки России, Дагест. гос. ун-т. - Махачкала : Изд-во ДГУ, 2015. - 211 с.
8. Информационное право: учеб.-метод. комплекс / [М.А.Эмиров, Л.В.Корж]; М-во образования и науки Рос. Федерации; Федерал. агентство по образованию; Дагест. гос. ун-т. - Махачкала : ИПЦ ДГУ, 2007. - 146 с.
9. Рассолов И.М. Информационное право: учеб. для магистров / Рассолов, Илья Михайлович. - 2-е изд., испр. и доп. - М. :Юрайт, 2012. - 444 с. - (Магистр).
10. Рассолов И.М. Информационное право: учеб. для магистров / Рассолов, Илья Михайлович. - 2-е изд., испр. и доп. - М. : Юрайт, 2013. - 444 с.

б) дополнительная литература:

1. Безугленко О.С. Законодательство в области правовой защиты детей от вредной информации: сравнительно-правовой анализ. // Информационное право, № 1(32), 2013.
2. Безугленко О.С. Сравнительная характеристика регионального и федерального законодательства в области правовой защиты детей от вредной информации. // Информационное право, № 2(33), 2013.
3. Булгакова Е.В., Архиереев Н.Л. Методика формирования компетенций юриста в области организационно-правового обеспечения информационной безопасности. // Информационное право, № 3(34), 2013.

4. Булгакова Л.И. Правовой режим аудиторской тайны. "Журнал российского права", 2008, № 5.
5. Бусленко Н.И. Медиаправо России: Документы, комментарии, вопросы и ответы. Феникс, 2005. 285 с.
6. Волчинская Е.К. О проблемах формирования правовой системы ограничения доступа к информации. // Информационное право, № 4(35), 2013.
7. Волчинская Е.К.К юбилею Закона Российской Федерации «О государственной тайне». // Информационное право, № 2(33), 2013.
8. Жарова А.К. Право и информационные конфликты в информационно-телекоммуникационной сфере. – Москва, 2016.
9. Казанцев С.Я и др. Правовое обеспечение информационной безопасности : учеб. пособие для студентов вузов. - 3-е изд.,стер. -Москва : Academia, 2008.
10. Кириленко В.П., Алексеев Г.В. Международное право и информационная безопасность государств. Монография – Санкт-Петербург, 2016.
11. Кротов А.В. Защита права на неприкосновенность частной жизни при реализации информационных прав посредством телефонной связи. // Информационное право, № 2(33), 2013.
12. Крылов Г.О., Кубанков А.Н. Учебный план магистерской программы «Правовое обеспечение информационной безопасности» . // Информационное право, № 3(34), 2013.
13. Кузнецов П.У. Научно-образовательные проблемы информационного права. // Информационное право, № 3(34), 2013.
14. Лапина М.А. Информационное право: учебное пособие для студентов вузов, обучающихся по специальности 021100 «Юриспруденция»/ Лапина М.А., Ревин А.Г., Лапин В.И.— М.: ЮНИТИ-ДАНА, 2017.— 335 с.
15. Лапина М.А., Николаенко Б.С. Информационная функция государства в сети «Интернет» . // Информационное право, № 4(35), 2013.
16. Ловцов Д.А. Обеспечение информационной безопасности в российских телематических сетях. // Информационное право, № 4(31), 2012.
17. Морозов А.В. Информационное право и информационная безопасность. Часть 1: учебник для магистров и аспирантов/ Морозов А.В., Филатова Л.В., Полякова Т.А.— Москва, Саратов: Всероссийский государственный университет юстиции (РПА Минюста России), Ай Пи Эр Медиа, 2016.— 436 с.
18. Морозов А.В. Информационное право и информационная безопасность. Часть 2: учебник для магистров и аспирантов/ Морозов А.В., Филатова Л.В., Полякова Т.А. — Москва, Саратов: Всероссийский государственный университет юстиции (РПА Минюста России), Ай Пи Эр Медиа, 2016.— 604 с.
19. Морозов А.В. Правовые вопросы доступа к информации: учебное пособие/ Морозов А.В., Филатова Л.В.— М.: Всероссийский государственный университет юстиции (РПА Минюста России), 2015.— 84 с.

20. Организационное и правовое обеспечение информационной безопасности : учебник и практикум для бакалавриата и магистратуры / Т. А. Полякова, А. А. Стрельцов, С. Г. Чубукова, В. А. Ниесов ; под ред. Т. А. Поляковой, А. А. Стрельцова. — М. : Издательство Юрайт, 2018. — 325 с. — (Серия : Бакалавр и магистр. Академический курс).
21. Полякова Т.А., Химченко А.И Особенности подготовки кадров в области организационно-правового обеспечения информационной безопасности. // Информационное право, № 3(34), 2013.
22. Потрашкова О.А. Коммерческая тайна: проблемы правовой защиты. // Информационное право, № 1(32), 2013.
23. Просвирнин Ю.Г. Информационное право: Учеб.пособие. Воронеж: Изд-во Воронеж.гос. ун-та, 2003. 628 с.
24. Рагимханова Д.А., Аливердиева М.А. Особенности правового режима информации ограниченного доступа. - Научные труды РАЮН, Вып. 14 в 2 т. Т.1 – Москва, 2014г. - С. 974-977.
25. Рагимханова Д.А., Аливердиева М.А. Правовой режим общедоступной информации. - Вестник Дагестанского государственного университета. 2013. № 2. - ИПЦ ДГУ, Махачкала. -С. 57-61
26. Рассолов И.М. Информационное право : учеб.для магистров / Рассолов, Илья Михайлович. - 2-е изд., испр. и доп. - М. : Юрайт, 2012. - 444 с. - (Магистр).
27. Рассолов И.М. Информационное право : учеб.для магистров / Рассолов, Илья Михайлович. - 2-е изд., испр. и доп. - М. : Юрайт, 2013. - 444 с.
28. Смирнов А.А. Обеспечение информационной безопасности в условиях виртуализации общества. Опыт Европейского Союза [Электронный ресурс]: монография/ Смирнов А.А.— М.: ЮНИТИ-ДАНА, 2015.— 159 с.— URL: http://www.iprbookshop.ru/52524.html.— ЭБС «IPRbooks».
29. Сурин В.В. Информационная безопасность уголовно-исполнительной системы: подходы к определению понятия. // Информационное право, № 1(32), 2013.
30. Сычев Ю.Н. Стандарты информационной безопасности. Защита и обработка конфиденциальных документов [Электронный ресурс]: учебное пособие/ Сычев Ю.Н.— Саратов: Вузовское образование, 2018.— 195 с.— URL: http://www.iprbookshop.ru/72345.html.— ЭБС «IPRbooks».
31. Чеботарева А.А. Информационное право. Учебное пособие / Москва, 2014.
32. Шаньгин В. Ф. Информационная безопасность и защита информации. - М. : Проспект, 2014.
33. Шибаев Д.В. Информационное право: практикум по курсу/ Шибаев Д.В.— Саратов: Ай Пи Эр Медиа, 2017.— 277 с.
34. Шибаев Д.В. Правовое регулирование электронного документооборота: учебное пособие/ Шибаев Д.В.— Саратов: Вузовское образование, 2016.— 70 с.
35. Ярочкин В.И. Информационная безопасность.- М.: Академический проект, 2003. Бачило И.Л. Информационное право : учебник / Бачило,

Иллария Лаврентьевна ; Ин-т гос. и права Рос.акад. наук, Академический правовой ун-т (ин-т). - 2-е изд., перераб. и доп. - М. : Юрайт, 2011. - 522 с. - (Магистр).

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

1. eLIBRARY.RU[Электронный ресурс]: электронная библиотека / Науч. электрон. б-ка. — Москва, 1999 – . Режим доступа: http://elibrary.ru/defaultx.asp. – Яз. рус., англ.
2. Moodle[Электронный ресурс]: система виртуального обучением: [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://edu.dgu.ru/course/
3. Образовательный блог по Информационному праву (Ragimhanova.blogspot.ru)/
4. Государственная автоматизированная система «Правосудие» - http://www.sudrf.ru/index.php?id=300
5. Научная библиотека Дагестанского государственного университета - http://www.elib.dgu.ru/
6. Официальный сайт открытого правительства РФ - http://openstandard.ru/
7. Официальный сайт ФГБОУ ВО «Дагестанский государственный университет» - http://cathedra.icc.dgu.ru/?id=71
8. Официальный сайт Федеральной службы безопасности РФ - http://www.fsb.ru/
9. Официальный сайт Следственного комитета РФ - http:// www.sledcom.ru
10. Официальный сайт Федеральной службы судебных приставов России http:// www.fssprus.ru
11. Портал государственных программ РФ - http://programs.gov.ru/Portal/programs/list
12. Портал государственных услуг РФ - http://www.gosuslugi.ru/pgu/stateStructure.html
13. Портал открытых данных РФ - http://data.gov.ru/taxonomy/term/71/datasets
14. Собрание законодательства РФ на портале Государственной системы правовой информации - http://pravo.gov.ru/proxy/ips/?editions
15. Судебная практика – www.sud-praktika.narod.ru

Базы данных, информационно-справочные и поисковые системы

1. Справочная правовая система «КонсультантПлюс» www.consultant.ru
2. Справочная правовая система Гарант –http://www.garant.ru/
3. Электронная Библиотека Диссертаций Российской государственной библиотеки ЭБД РГБ. Включает полнотекстовые базы данных диссертаций. http://diss.rsl.ru
4. Научная электронная библиотека диссертаций и авторефератов.

http://www.dissercat.com/
5. Электронная библиотека образовательных и научных изданий Iqlib. www.iqlib.ru
6. Интернет-библиотека СМИ Public.ru www.public.ru
7. Информационные ресурсы научной библиотеки Даггосуниверситета (доступ через платформу Научной электронной библиотеки elibrary.ru)/ http://elib.dgu.ru
8. Электронные каталоги Научной библиотеки Даггосуниверситетаhttp://elib.dgu.ru/?q=node/256
9. Сайт образовательных ресурсов Даггосуниверситета http://edu.icc.dgu.ru
10. Юридический Вестник ДГУ.http://www.jurvestnik.dgu.ru

10. Методические указания для обучающихся по освоению дисциплины.

Одной из ведущих тенденций в реформировании отечественного университетского образования, и в связи с переходом на 2-х ступенчатую систему подготовки кадров высшего образования является видение современного выпускника творческой личностью, способного самостоятельно осваивать интенсивно меняющееся социально-духовное поле культуры. Данная тенденция предполагает поиск такой модели профессиональной подготовки, в которой образовательный процесс обеспечивал бы сопряженность содержания обучения с организованной (контролируемой) самостоятельной работой студентов в развитии их индивидуальных способностей и учетом интересов профессионального самоопределения, самореализации.

Изучение базового курса «Информационная безопасность» предполагает изложение теоретического курса на лекционных занятиях и приобретение практических навыков в процессе решения поставленных задач, возникающих при регулировании информационно-правовых отношений. Конспекты лекций служат основой для подготовки к семинарским занятиям. Самостоятельная работа студентов состоит в повторении по конспекту начитанного лекционного материала и получение дополнительных сведений по тем же учебным вопросам из рекомендованной и дополнительной литературы, выполнение тестовых заданий по пройденным темам на семинарских занятиях, а также подготовке и защите реферата по выбранной теме исследования.

В теоретической части курса уделяется большое внимание рассмотрению объекта, субъектов, предмета, принципов, методов и средств обеспечения информационной безопасности, особенностям правового режима информации ограниченного доступа, основным каналам утечки информации, ответственности за правонарушения в информационной сфере.

При изучении курса «Информационная безопасность» рекомендуется обращаться не только к учебникам, но и к рекомендованной дополнительной литературе.

Курс состоит из семи взаимосвязанных тем.

Учебный план предполагает также семинарские занятия, цель которых подробное изучение теоретического материала, анализ законодательства, регулирующего обеспечение безопасности в информационной сфере, приобретение навыков формально-юридического мышления при решении задач.

Основными формами работы студентов являются выступления с краткими сообщениями по темам; подготовка письменных рефератов на основе глубокого и подробного изучения отдельных вопросов темы; подготовка презентаций. Эти формы работы способствуют выработке у студентов навыков и опыта самостоятельной научной работы. Способ проведения занятий может варьироваться в зависимости от темы. Семинар может проводиться по докладной системе, в виде "круглых столов", диспутов или в иной форме по усмотрению преподавателя.

На занятиях может применяться такая форма работы как решение задач. Это поможет студентам научиться применять изученные нормы права, лучше уяснить смысл законодательства, регулирующего обеспечение информационной безопасности.

Самостоятельная работа студентов по курсу «Информационная безопасность» направлена на более глубокое усвоение изучаемого курса, формирование навыков исследовательской работы, ориентирование студентов на умение применять теоретические знания на практике. Задания для самостоятельной работы составляются по разделам и темам, по которым не предусмотрены аудиторные занятия либо требуется дополнительно проработать и проанализировать рассматриваемый преподавателем материал.

Изучение информационной безопасности 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 зачет, а впоследствии использовать полученные знания в своей практической деятельности.

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 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 по дисциплине «Информационная безопасность».

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 ragimhanova.blogspot.com, Официальному сайту Федеральной службы безопасности РФ.

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.