

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РФ
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«ДАГЕСТАНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»
Юридический институт

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Преступность в сфере информационных технологий

**Кафедра информационного права и информатики
юридического института**

Образовательная программа:

40.03.01 Юриспруденция

Профиль подготовки:

Уголовно-правовой

Уровень высшего образования: **бакалавриат**

Форма обучения: **очная**


Статус дисциплины: **вариативная**

Махачкала
2016 год


Рабочая программа дисциплины **Преступность в сфере информационных технологий** составлена в 2016 году в соответствии с требованиями ФГОС ВПО по направлению подготовки 40.03.01 Юриспруденция (уровень бакалавриата) от 4 мая 2010г. №464.


Разработчик(и): кафедра «Информационное право и информатика»,
Абдусаламов Руслан Абдусаламович, к.п.н., доцент,
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 29 августа
2016г., протокол №1.

Зав. кафедрой  Абдусаламов Р.А.
(подпись)

на заседании Методической комиссии юридического института от «4»
08 2016г., протокол №1.

Председатель  Арсланбекова А.З.,
(подпись)

Рабочая программа дисциплины согласована с учебно-методическим
управлением «5» 08 2016г. 
(подпись)

Аннотация рабочей программы дисциплины

Дисциплина **Преступность в сфере информационных технологий** входит в вариативную часть образовательной программы бакалавриата по направлению 40.03.01 Юриспруденция.

Дисциплина реализуется в юридическом институте кафедрой информационного права и информатики.

Содержание дисциплины охватывает круг вопросов, связанных с изучением основных понятий и принципов информационных процессов, информационных технологий, информационной безопасности и методов правового регулирования информационных отношений в информационной сфере. Рассматриваются вопросы ответственности за правонарушения и преступления в сфере информационных технологий, а также механизмы защиты прав и законных интересов субъектов информационной сферы.

Дисциплина нацелена на формирование следующих компетенций выпускника: общекультурных – ОК-11, ОК-12, профессиональных - ПК-6, 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

Семес тр	Учебные занятия						СРС, в том числе экзамен	Форма промежуточной аттестации (зачет, дифференцирован ный зачет, экзамен
	в том числе							
	Контактная работа обучающихся с преподавателем							
	Всего	из них						
Лекц ии		Лабораторн ые занятия	Практиче ские занятия	КСР	консульта ции			
6	72	16		16			40	зачет

1. Цели освоения дисциплины

Целями освоения дисциплины «Преступность в сфере информационных технологий» являются:

- ознакомление студентов с современными системами информационной безопасности, методами и средствами защиты информации, организационными и правовыми мерами по информационной защите;
- ознакомление с совокупностью современных приемов поиска, исследования и фиксации информации при расследовании киберпреступлений.
- формирование и развитие у будущих юристов теоретических знаний и практических навыков, связанных с организацией информационной безопасности, планированием, подготовкой и реализацией процесса обеспечения информационной безопасности;
- 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 ООП бакалавриата

Дисциплина входит в вариативную часть информационно-правового цикла (Б.2) 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) информационными технологиями в юридической деятельности, формирующими знания о принципах и методах осуществления информационных процессов в правовой сфере, особенностях работы в глобальных компьютерных сетях.

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-11	<p>Владение основными методами, способами и средствами получения, хранения, переработки информации, имеет навыки работы с компьютером как средством управления информацией.</p>	<p>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.</p> <p>Уметь: пользоваться основными методами, способами и средствами получения, хранения, переработки информации; соблюдать основные требования компьютерной безопасности, получать, хранить, перерабатывать использовать информацию; правильно давать оценку информации.</p> <p>Владеть: навыками поиска, получения, хранения, переработки и защиты компьютерной информации, навыками сбора и обработки информации; навыками анализа информации; навыками обработки информации.</p>
ОК-12	<p>Способность работать с информацией в глобальных компьютерных сетях</p>	<p>Знать: основы работы с информацией в глобальных компьютерных сетях; информационно-правовые технологии (правовые порталы) с помощью которых осуществляется поиск информации в сети Интернет.</p> <p>Уметь: работать в глобальных компьютерных сетях; решать любые юридические задачи, связанные с добыванием в сети Интернет правовых материалов.</p> <p>Владеть: навыками обработки правовых материалов, найденных в среде правовых порталов.</p>

ПК-6	Способность правильно квалифицировать факты и обстоятельства	<p>Знать: понятие, виды и способы квалификации фактов и обстоятельств, этапы юридической квалификации, содержание источников информационной безопасности в сфере информационных технологий, с точки зрения разных авторов на проблемные вопросы</p> <p>Уметь: правильно давать юридическую оценку фактам и обстоятельствам, обоснованно применять нормы права при правовой квалификации обстоятельств.</p> <p>Владеть: юридической терминологией отраслей права, позволяющей юридически правильно квалифицировать факты и обстоятельства</p>
ПК-16	Способность давать квалифицированные юридические заключения и консультации в конкретных видах юридической деятельности	<p>Знать: понятие, виды и способы квалификации фактов и обстоятельств, правовые явления и методы их анализа</p> <p>Уметь: оценивать правовые явления и формулировать выводы и предложения на основе их анализа, давать разъяснения по правовым вопросам в рамках своей профессиональной деятельности</p> <p>Владеть навыками работы по толкованию правовых норм, навыками общения, методами аргументированного, обоснованного убеждения</p>

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.		
<i>Модуль 1. Основы информационной безопасности в сфере информационных технологий</i>									
1	Информационная безопасность в сфере использования информационных технологий	6		2	2			4	Контрольный опрос
2	Правовое и организационное обеспечение информационной безопасности в сфере информационных технологий	6		2	2			4	Контрольный опрос, тестирование
3	Информационное обеспечение борьбы с преступлениями в сфере использования информационных технологий	6		2	2			6	Контрольный опрос
4	Основы организации борьбы с преступлениями в глобальных компьютерных сетях.	6		2	2			6	Контрольный опрос, тестирование
	<i>итого по модулю 1:</i>			8	8			20	
<i>Модуль 2. Методы защиты информации и ответственность в сфере использования информационных технологий</i>									
5	Компьютерные	6		4	2			4	Контрольный опрос,

	преступления								реферат
6	Предупреждение преступлений в глобальных компьютерных сетях.	6		2	2			4	Контрольный опрос, тестирование
7	Ответственность за преступления в сфере информационных технологий	6		2	2			6	Контрольный опрос
	<i>Итого по модулю 2:</i>			8	8			20	
	Промежуточный контроль								зачет
	ИТОГО:			16	16			40	

4.3. Содержание дисциплины, структурированное по темам (разделам)

Модуль 1. Основы информационной безопасности в сфере информационных технологий

Тема 1. Информационная безопасность в сфере использования информационных технологий

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

Государственная политика в области информационной безопасности. Основные цели, задачи и направления реализации государственной политики в информационной сфере.

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. Правовое и организационное обеспечение информационной безопасности в сфере информационных технологий

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.

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 3. Информационное обеспечение борьбы с преступлениями в сфере использования информационных технологий

Информационное обеспечение борьбы с преступлениями, связанные с подделкой документов. Информационное обеспечение международного розыска лиц.

Использование результатов оперативно-розыскной деятельности в глобальных компьютерных сетях. Информационное сопровождение уголовно-процессуальных действий, связанных с раскрытием преступлений. Подготовка аналитической информации для определения перспективных направлений борьбы с преступностью в глобальных компьютерных сетях. Применение полученных данных в дальнейшем решении конкретных оперативно-тактических задач.

Тема 4. Основы организации борьбы с преступлениями в глобальных компьютерных сетях

Система правоохранительных органов и выбор стратегии борьбы с преступлениями в глобальных компьютерных сетях. Управление компьютерной и информационной безопасности ФСБ. Управление по борьбе с преступлениями в сфере высоких технологий (Управление «Р»). Главное управление специальных технических мероприятий МВД России (ГУСТМ). Общая стратегия борьбы с преступностью в глобальных компьютерных сетях.

Организация взаимодействия участников борьбы с преступностью в глобальных компьютерных сетях. Осуществление правоохранительных мероприятий на международном уровне. Действия различных правоохранительных органов на национальном уровне и подразделений различного уровня, входящих в одно ведомство. Осуществление уполномоченными органами совместной деятельности с иными организациями.

Модуль 2. Методы защиты информации и ответственность в сфере использования информационных технологий

Тема 5. 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 6. Предупреждение преступлений в глобальных компьютерных сетях

Аналитическая работа как средство предотвращения сетевых компьютерных преступлений. Стратегический анализ. Тактический анализ. Оперативный анализ. Технологическое обеспечение аналитической деятельности. Использование результатов аналитической работы. Основные направления профилактики сетевых компьютерных преступлений.

Тема 7. Ответственность за преступления в сфере информационных технологий

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.

Семинарские занятия.

Модуль 1. Основы информационной безопасности в сфере информационных технологий

Тема 1. Информационная безопасность в сфере использования информационных технологий

Вопросы для обсуждения:

1. Понятие и структура информационной безопасности.
2. Государственная политика в сфере использования информационных технологий.

Тема 2. Правовое и организационное обеспечение информационной безопасности в сфере информационных технологий

Вопросы для обсуждения:

1. Понятие и виды угроз информационной безопасности.
2. Основные направления организационной защиты на объекте. Структура средств организационной защиты информации.
3. Законодательство в сфере обеспечения информационной безопасности РФ.
4. Основные причины утечки информации.

Тема 3. Информационное обеспечение борьбы с преступлениями в сфере использования информационных технологий

Вопросы для обсуждения:

1. Информационное обеспечение борьбы с преступлениями, связанные с подделкой документов.
2. Информационное обеспечение международного розыска лиц.
3. Информационное сопровождение уголовно-процессуальных действий, связанных с раскрытием преступлений.

Тема 4. Основы организации борьбы с преступлениями в глобальных компьютерных сетях

Вопросы для обсуждения:

1. Понятие киберпреступности.
2. Система правоохранительных органов и выбор стратегии борьбы с преступлениями в глобальных компьютерных сетях.
3. Организация взаимодействия участников борьбы с преступностью в глобальных компьютерных сетях.

Модуль 2. Методы защиты информации и ответственность в сфере использования информационных технологий

Тема 5. Компьютерные преступления

Вопросы для обсуждения:

1. Понятие и виды компьютерных преступлений.

2. Особенности квалификации компьютерных преступлений.
3. Преступления имущественного характера, которые совершаются с применением или в отношении средств компьютерной техники.

Тема 6. Предупреждение преступлений в глобальных компьютерных сетях

Вопросы для обсуждения:

1. Технологическое обеспечение аналитической деятельности.
2. Основные направления профилактики сетевых компьютерных преступлений.

Тема 7. Ответственность за преступления в сфере информационных технологий

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 профессионального образования по направлению подготовки 030900 (40.03.01) - «юриспруденция» (квалификация «бакалавр») реализация компетентного 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 компетентного 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 «Преступность в сфере информационных технологий» 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 факультета имеют своей целью приобретение им системы знаний по дисциплине «Преступность в сфере информационных технологий». 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 тезисов	См. разделы 6 и 7 данного документа

6.	Подготовка к зачету	Промежуточная аттестация в форме зачета	См. раздел 7 данного документа
----	---------------------	---	--------------------------------

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-11	<p>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;</p> <p>Уметь: организовать умственную деятельность; анализировать возможные пути достижения поставленных целей; работать с компьютером как средством управления информацией</p> <p>Владеть: законами и требованиями логики; методами правового регулирования информационных отношений, возникающих при осуществлении основных информационных процессов в сфере информационных технологий.</p>	Устный опрос, разбор практических ситуаций
ОК-12	Знать: основные виды	Устный опрос, разбор

	<p>информационных правоотношений в Интернете; особенности способов правового регулирования интернет-отношений, структуру информационного законодательства, регулирующего интернет-отношения.</p> <p>Уметь: правильно применять нормы информационного права при регулировании публично-правовых и частных правовых отношений в Интернете.</p> <p>Владеть: навыками сбора и обработки информации, имеющей значение для реализации правовых норм в сфере информационных технологий, в частности в виртуальной среде Интернета.</p>	<p>практических ситуаций, тестирование</p>
ПК-6	<p>Знать: понятие, виды и способы квалификации фактов и обстоятельств, этапы юридической квалификации, содержание источников компьютерного права, точки зрения разных авторов на проблемные вопросы</p> <p>Уметь: правильно давать юридическую оценку фактам и обстоятельствам, обоснованно применять нормы права при правовой квалификации обстоятельств.</p> <p>Владеть: юридической терминологией отраслей права, позволяющей юридически правильно квалифицировать факты и обстоятельства.</p>	<p>Устный опрос, разбор практических ситуаций, тестирование</p>
ПК-16	<p>Знать: понятие, виды и</p>	<p>Устный опрос, письменный</p>

	<p>способы квалификации фактов и обстоятельств, правовые явления и методы их анализа.</p> <p>Уметь: оценивать правовые явления и формулировать выводы и предложения на основе их анализа, давать разъяснения по правовым вопросам в рамках своей профессиональной деятельности.</p> <p>Владеть навыками работы по толкованию правовых норм, навыками общения, методами аргументированного, обоснованного убеждения.</p>	опрос, разбор практических ситуаций, тестирование
--	---	---

7.2. Описание показателей и критериев оценивания компетенций, описание шкал оценивания.

Схема оценки уровня формирования компетенции «ОК-11 Владение основными методами, способами и средствами получения, хранения, переработки информации, имеет навыки работы с компьютером как средством управления информацией»

Уровень	Показатели (что обучающийся должен продемонстрировать)	Оценочная шкала		
		Удовлетворительно	Хорошо	Отлично
Пороговый	Понимает социальную значимость основных методов, способов и средств получения, хранения, переработки информации в условиях развития информационного общества и его правовых основ. Определяет особенности навыков работы с компьютером как средством управления	Называет особенности основных методов, способов и средств получения, хранения, переработки информации; дает определение понятий «метод», «способ», «средство», «информация», «информационные технологии», «обобщение информации», «анализ	Толкует смысл понятий «метод», «способ», «средство», «информация», «компьютерные технологии», «обобщение информации», «анализ информации», «восприятие информации». Умеет использовать навыки работы с	Распознает требования, которые предъявляются к компьютерной информации, к ее обобщению, анализу как основному ресурсу информационного общества и элемента информационной инфраструктуры. Владеет навыками правового

	информацией в условиях правовой информатизации и развитии информационного общества.	информации», «восприятие информации»; «методы правового регулирования информационных правоотношений»; «принципы компьютерной безопасности».	компьютером как средством управления информацией для решения практических задач, анализа судебной практики по компьютерным преступлениям	регулирования информационных правоотношений при осуществлении информационных процессов в информационной сфере.
--	---	---	--	--

Схема оценки уровня формирования компетенции «ОК-12Способность работать с информацией в глобальных компьютерных сетях»

Уровень	Показатели (что обучающийся должен продемонстрировать)	Оценочная шкала		
		Удовлетворительно	Хорошо	Отлично
Пороговый	Понимает социальную значимость работы с информацией в глобальных компьютерных сетях и необходимости правового регулирования информационных отношений нормами действующего законодательства.	Называет особенности работы с информацией в глобальных компьютерных сетях в современных условиях развития глобального информационного общества и методы защиты информации.	Дает правовую оценку работы с информацией в глобальных компьютерных сетях и определяет объекты правоотношений в Интернете; оценивает сложность и многообразие информации, ее обобщения, анализа и восприятия; оценивает сложность и многообразие основных методов, способов и средств получения, хранения, переработки информации, а также средства защиты информации.	Выделяет и описывает работу с информацией в глобальных компьютерных сетях; анализирует правовую информацию; обобщает правовую информацию; классифицирует полученную информацию по определенным категориям для ее использования в профессиональной деятельности; анализирует вопросы навыка работы с компьютером как средством управления информацией критически

				оценивает проделанную работу; делает выводы и формулирует новые цели и задачи.
--	--	--	--	--

Схема оценки уровня формирования компетенции «ПК-6Способность правильно квалифицировать факты и обстоятельства»

Уровень	Показатели (что обучающийся должен продемонстрировать)	Оценочная шкала		
		Удовлетворительно	Хорошо	Отлично
Пороговый	<p>Знает понятие, виды и способы квалификации фактов и обстоятельств, этапы юридической квалификации, содержание источников компьютерного права, точки зрения разных авторов на проблемные вопросы</p> <p>Умет правильно давать юридическую оценку фактам и обстоятельствам, обоснованно применять нормы права при правовой квалификации обстоятельств.</p> <p>Владеет: юридической терминологией отраслей права, позволяющей юридически правильно квалифицировать факты и обстоятельства;</p>	<p>Знает основные положения обеспечения компьютерной безопасности, понимает сущность основных понятий и категорий, выбранных им.</p>	<p>Умеет оперировать юридическими понятиями и категориями компьютерной безопасности. Обладает навыками анализа юридических фактов и возникших в связи с ними правоотношений</p>	<p>Знать: понятие, виды и способы квалификации фактов и обстоятельств, угрозы компьютерной безопасности личности, общества и государства, точки зрения разных авторов на проблемные вопросы</p> <p>Умеет принимать решения и совершать юридические действия в точном соответствии с законом; правильно давать юридическую оценку фактам и обстоятельствам.</p> <p>Владеет навыками анализа, толкования и правильного</p>

				применения правовых норм и юридической терминологий
--	--	--	--	--

Схема оценки уровня формирования компетенции «ПК-16 Способность давать квалифицированные юридические заключения и консультации в конкретных видах юридической деятельности»

Уровень	Показатели (что обучающийся должен продемонстрировать)	Оценочная шкала		
		Удовлетворительно	Хорошо	Отлично
Пороговый	Знает понятие, виды и способы квалификации фактов и обстоятельств, правовые явления и методы их анализа Умет оценивать правовые явления и формулировать выводы и предложения на основе их анализа, давать разъяснения по правовым вопросам в рамках своей профессиональной деятельности Владеет навыками работы по толкованию правовых норм, навыками общения, методами аргументированного, обоснованного убеждения	Демонстрирует слабое умение анализировать содержание правовых норм, формулировать выводы и предложения; владения навыками работы по толкованию правовых норм	Имеет представление о видах способах квалификации фактов и обстоятельств. Умет оценивать правовые явления и формулировать выводы и предложения. Обладает навыками работы по толкованию правовых норм, навыками общения.	Знает понятие, виды и способы квалификации фактов и обстоятельств, правовые явления и методы их анализа Умет оценивать правовые явления и формулировать выводы и предложения на основе их анализа, давать разъяснения по правовым вопросам в рамках своей профессиональной деятельности Владеет навыками работы по толкованию правовых норм, навыками общения, методами аргументированного, обоснованного убеждения

Если хотя бы одна из компетенций не сформирована, то положительная оценки по дисциплине быть не может.

7.3 Типовые контрольные задания

Примерная тематика рефератов

1. Персональные данные и тайна частной жизни: общее и отличия.
2. Правовое регулирование электронной подписи
3. Правовое регулирование в сфере массовой информации
4. Правовое регулирование банковской тайны
5. Правовое регулирование государственной тайны
6. Правовое регулирование коммерческой тайны
7. Правовое регулирование рекламной деятельности
8. Правовые основы защиты персональных данных
9. Уголовная ответственность за правонарушения в информационной сфере
10. Административная ответственность за правонарушения в информационной сфере
11. Гражданско-правовая ответственность за правонарушения в информационной сфере.
12. Правовые проблемы борьбы со «спамом»
13. Электронные деньги: проблемы правового регулирования
14. Правовое регулирование информационных технологий в области электронной коммерции
15. Правовое регулирование информационных технологий в области рекламы и маркетинга в Интернет
16. Правовое регулирование информационных технологий в области электронных банковских услуг
17. Правовое регулирование информационных технологий в области электронного документооборота
18. Стандартизация, сертификация и лицензирование в информационной сфере

Примерные тесты

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. 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

5. При правовом регулировании отношений в Интернет важно соблюдение баланса

) между свободой слова и интересами несовершеннолетних; свободой доступа к информации и информационной безопасностью; свободой производства информации и ограничения производства и распространения опасной информации

) между свободой слова и интересами несовершеннолетних; между свободой слова и цензурой; свободой 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

6. 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 - Business to Administration

7. 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

8. 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»

9. 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

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

-) общими и специальными
-) регулятивными и охранительными
-) абсолютными и относительными
-) императивными и диспозитивными

19. 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

11. 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

12. 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

13. 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

14. 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

15. С точки зрения уголовно-правовой охраны под компьютерными преступлениями следует понимать

) предусмотренные уголовным законом общественно опасные действия, в которых машинная информация является объектом преступного посягательства

) нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети, повлекшее уничтожение, блокирование или модификацию охраняемой законом информации ЭВМ (т.е. машинной информации)

) предусмотренные уголовным законом общественно опасные действия, совершенные с использованием средств электронно-вычислительной (компьютерной) техники

16. С точки зрения криминалистических аспектов под компьютерными преступлениями следует понимать

) предусмотренные уголовным законом общественно опасные действия, совершенные с использованием средств электронно-вычислительной (компьютерной) техники

) предусмотренные уголовным законом общественно опасные действия, в которых машинная информация является объектом преступного посягательства

) нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети, повлекшее уничтожение, блокирование или модификацию охраняемой законом информации ЭВМ (т.е. машинной информации)

Примерные вопросы к зачету

1. Информационная сфера и ее элементы.
2. Информационные технологии.

3. Понятие безопасности и информационной безопасности.
4. Основные составляющие информационной безопасности.
5. Субъекты и объекты правоотношений в области информационной безопасности.
6. Понятие государственной информационной политики.
7. Основные положения государственной политики обеспечения информационной безопасности РФ.
8. Система обеспечения информационной безопасности РФ и ее основные функции.
9. Понятие и виды угроз безопасности.
10. Угрозы информационной безопасности на объекте.
11. Понятие и виды компьютерных преступлений.
12. Особенности квалификации компьютерных преступлений.
13. Преступления имущественного характера, которые совершаются с применением или в отношении средств компьютерной техники.
14. Доктрина информационной безопасности РФ об основных угрозах в информационной сфере и их источниках.
15. Угрозы нарушения конфиденциальности, целостности, доступности информации.
16. Основные причины утечки информации.
17. Виды информационного законодательства, применяемые для регулирования отношений в Интернет.
18. Угроза безопасности, обеспечение безопасности: понятие.
19. Понятие и признаки компьютерной информации.
20. Понятие компьютерного преступления.
21. Личностная характеристика преступника, совершившего компьютерные преступления.
22. Международный опыт борьбы с преступлениями в сфере компьютерной информации
23. Информационная безопасность и информационные войны: понятие.
24. История информационных войн.
25. Информационная безопасность и информационное оружие: понятие.
26. Правонарушение и информационное правонарушение: определение, признаки, юридическая ответственность и основание привлечения к ответственности.
27. Состав информационного правонарушения.
28. Уголовная ответственность за информационное преступление.
29. Административная и гражданско-правовая ответственность в информационной сфере.

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

Общий результат выводится как интегральная оценка, складывающаяся из текущего контроля - 60% и промежуточного контроля - 40%.

Текущий контроль по дисциплине включает:

- участие на практических занятиях - 20 баллов,
- выполнение домашних заданий - 20 баллов,
- выполнение аудиторных контрольных работ - 20 баллов.

Промежуточный контроль по дисциплине включает:

- устный опрос - 10 баллов,
- письменная контрольная работа - 15 баллов,
- тестирование - 15 баллов.

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

а) 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 государственной тайне: Федеральный закон от 21 июля 1993г. № 5485 – 1 – ФЗ // СЗ РФ. – 1993. - №41. – Ст. 4673.
7. О коммерческой тайне: Федеральный закон от 29 июля 2004 г. N 98-ФЗ // СЗ РФ. 2004. N 32. Ст. 3283.
8. О персональных данных: Федеральный закон от 27 июля 2006 г. № 152 – ФЗ // СЗ РФ. – 2006. - №31 (1ч.). – Ст. 3451.
9. 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.
10. Об информации, информационных технологиях и о защите информации: Федеральный закон от 27 июля 2006 г. № 149 – ФЗ // СЗ РФ. – 2006. - №31 (1ч.). – Ст. 3448.
11. Об электронной подписи: Федеральный закон от 6 апреля 2011 г. № 10 // Собрание законодательства РФ, 11.04.2011, N 15, ст. 2036.

12. 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.
13. 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.
14. 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.
15. 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.
16. 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.
17. 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.
18. 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.
19. 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.
20. 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.
21. 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.
22. 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.
23. 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.

24. Республиканская целевая программа «Развитие электронного правительства Республики Дагестан до 2017 года»: Постановление Правительства Республики Дагестан от 12.09.2013 года №432.

б) основная литература:

1. Белов Е.Б., Лось В.П., Мещеряков Р.В., Шелупанов А.А. Основы информационной безопасности. Учебное пособие для вузов. Гриф МО РФ. - М.: Горячая линия - Телеком, 2006.
2. Галатенко В.А. Основы информационной безопасности: Курс лекций.- М.: Интернет- Университет Информационных технологий, 2006.
3. ГОСТ Р 50922-2006. Защита информации. Основные термины и определения. - М.: Стандартинформ, 2008. - 12 с.
4. ГОСТ Р 51275-2006. Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения. - М.: Стандартинформ, 2007. - 11 с.
5. ГОСТ Р ИСО/МЭК 15408-1-2002. Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. - М.: Госстандарт России, 2002. - 40 с.
6. Девянин П.Н., Михальский О.О. , Правиков Д.И. , Щербаков А.Ю. Теоретические основы компьютерной безопасности: учебное пособие для вузов. - М.: Радио и связь, 2000.
7. Казанцев С.Я и др. Правовое обеспечение информационной безопасности : учеб. пособие для студентов вузов. - 3-е изд.,стер. -Москва : Academia, 2008.
8. Конеев И.Р., Беляев А.В. Информационная безопасность предприятия. - СПб.: БХВ-Петербург, 2003. - 752 с.
9. Мельников В. П., Клейменов С.А., Петраков А.М. Информационная безопасность и защита информации : учеб. пособие для студентов вузов. - 2е изд.,стер. - Москва : Academia, 2007.
10. Рассолов И.М. Информационное право : учеб.для магистров / Рассолов, Илья Михайлович. - 2-е изд., испр. и доп. - М. : Юрайт, 2012. - 444 с. - (Магистр).
11. Рассолов И.М. Информационное право : учеб.для магистров / Рассолов, Илья Михайлович. - 2-е изд., испр. и доп. - М. : Юрайт, 2013. - 444 с.
12. Расторгуев С. П. Основы информационной безопасности : учеб. пособие для студ. вузов. -М.: Академия, 2007.
13. Романец Ю.В., Тимофеев П.А., Шаньгин В.Ф. Защита информации в компьютерных системах и сетях. - М.: Радио и связь, 1999. -328 с. 17.
14. Тихонов В.А., Райх В.В. Информационная безопасность: концептуальные, правовые, организационные и технические аспекты: Учебное пособие. - М.: Гелиос АРВ, 2006.
15. Шаньгин В.Ф. Информационная безопасность компьютерных систем и сетей: Учебное пособие. - М.: ИД «ФОРУМ»: ИНФРА-М, 2008.

16. Шаньгин В. Ф. Информационная безопасность и защита информации. - М. : Проспект, 2014.
17. Ярочкин В.И. Информационная безопасность.- М.: Академический проект, 2003. Бачило И.Л. Информационное право : учебник / Бачило, Илларию 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).

в) дополнительная литература:

1. Бакаев А.В. Основы информационного права: Учеб.пособие. Ростов-на-Дону: Рост.гос. строит. ун-т, 2005. 82 с.
2. Батурин Ю.М. Проблемы компьютерного права. М., 1991.
3. Безугленко О.С. Законодательство в области правовой защиты детей от вредной информации: сравнительно-правовой анализ. // Информационное право, № 1(32), 2013.
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 Е.В., Архиреев Н.Л. Методика формирования компетенций юриста в области организационно-правового обеспечения информационной безопасности. // Информационное право, № 3(34), 2013.
6. Булгакова Л.И. Правовой режим аудиторской тайны. "Журнал российского права", 2008, № 5.
7. Бусленко Н.И. Медиаправо России: Документы, комментарии, вопросы и ответы. Феникс, 2005. 285 с.
8. Войниканис Е., Якушев М. Информация. Собственность. Интернет: традиция и новеллы в современном праве. М.: ВолтерсКлувер, 2004.
9. Волчинская Е., Терещенко Л., Якушев М. Интернет и гласность. М.: Галерея, 1999.
10. Волчинская Е.К. О проблемах формирования правовой системы ограничения доступа к информации. // Информационное право, № 4(35), 2013.
11. Волчинская Е.К. К юбилею Закона Российской Федерации «О государственной тайне». // Информационное право, № 2(33), 2013.
12. Вопросы совершенствования законодательства в сфере информационной безопасности. М., Изд-во Государственной Думы Федерального Собрания Российской Федерации. М., 2007. С.80.
13. Гаврилин Ю.В. Преступления в сфере компьютерной информации. Квалификация и доказывание: Учеб.пособие. М.: Книжный мир, 2003. 245 с.
14. Городов О.А. Основы информационного права России: Учебное пособие. М.: Юридический центр Пресс, 2003. 305 с.;
15. Дайсон Э. Жизнь в эпоху Интернета. М.: Бизнес и компьютер, 1998.

16. Данилов Н.А. Цифровое равенство: опыт Австрии и Дании. // Информационное право, № 4(31), 2012.
17. Ермакова В.В., Кротов И.Е. Информационные таможенные технологии для бизнеса в России. // Информационное право, № 1(32), 2013.
18. Ефремова М. А. Мошенничество с использованием электронной информации. // Информационное право, № 4(35), 2013.
19. Жарова А.К. О конфликте интересов субъектов в информационных отношениях // Государство и право. 2011. № 4. С. 42-49.
20. Журавлев М.С. Персональные данные в трудовых отношениях: допустимые пределы вмешательства в частную жизнь работника. // Информационное право, № 4(35), 2013.
21. Загородников С.Н., Шмелев. А.А. Основы Информационного права: Учеб.пособие. Ростов н/Д: Феникс, 2005.
22. Зверева Е. Имущественные и исключительные права на информационные продукты, их реализация и защита. "Право и экономика", 2004, N 12.
23. Зверева Е.А. Информация как объект неимущественных гражданских прав. "Право и экономика", № 9, 2003.
24. Иванова А.Ю. Проблемы ведения регистра муниципальных нормативных актов в едином информационном пространстве. // Информационное право, № 4(31), 2012.
25. Ильюшенко В.Н. Методологические, организационные и правовые основы информационной безопасности. В 3 ч. Томск: Изд-во Ин-та оптики атмосферы, 2005. 474 с.
26. Информационная безопасность России в условиях глобального информационного общества. М., 2001.
27. 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.
28. Информационные ресурсы развития Российской Федерации. Правовые проблемы: Монография. СПб.: Наука, 2003. 403 с.
29. 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.
30. Калятин В.О. Право в сфере Интернета. М.: Инфра-М, 2004. 480 с.
31. Кемрадж А.С., Головеров Д.В. Правовые аспекты использования интернет-технологий. М.: Книжный мир, 2002. 410 с.
32. Киреева Н.В. О программе развития информационных технологий в Роспатенте и ФИПС до 2020 г.. // Информационное право, № 1(32), 2013.
33. Ковалева Н.Н. Информационное право России: Учеб.пособие. М.: Дашков и Ко, 2007. 359 с.

34. Ковалева Н.Н. Органы публичной власти как субъекты управления в информационной сфере. // Информационное право, № 2(33), 2013.
35. Козориз Н.Л. Информационная безопасность в системе противодействия опасности. // Информационное право, № 1(32), 2013.
36. Козориз Н.Л. О предмете правового регулирования информационной безопасности. // Информационное право, № 4(35), 2013.
37. Козырева Т.В. Доступ к информации о деятельности судов. // Информационное право, № 4(31), 2012.
38. Колобов О.А., Ясенев В.Н. Информационная безопасность и антитеррористическая деятельность современного государства: проблемы правового регулирования и варианты их решения: Учеб.пособие. Нижний Новгород, 2001. 374 с.
39. Коломиец А.В. Тайна. Коммерческая.Служебная.Государственная: Сборник нормативных правовых актов РФ. М.: Статус, 2001. 656 с.
40. Комзюк Л.Т. Правовые проблемы создания общественного телевидения Украины в контексте зарубежного опыта. // Информационное право, № 1(32), 2013.
41. Копылов В.А. Информационное право. М.,1997.
42. Копьёв А.В. Проблемы защиты права на доменное имя. // Информационное право, № 1(32), 2013.
43. Королев А.Н., Плешакова О.В. Комментарий к Федеральному закону "Об информации, информационных технологиях и о защите информации" (постатейный). М., ЗАО Юстицинформ, 2007.
44. Костылев А.К. Информационное право: Учеб.пособие. Тюмень: Изд-во Тюменского гос. ун-та, 2005. 214 с.
45. Кротов А.В. Защита права на неприкосновенность частной жизни при реализации информационных прав посредством телефонной связи. // Информационное право, № 2(33), 2013.
46. Крылов Г.О., Кубанков А.Н. Учебный план магистерской программы «Правовое обеспечение информационной безопасности» . // Информационное право, № 3(34), 2013.
47. Кузнецов В.К. Информационное право: Учеб.-метод. комплекс для дистанц. обучения по спец. 021100 "Юриспруденция". Новосибирск: СибАГС, 2003. 168 с.
48. Кузнецов П.У. Научно-образовательные проблемы информационного права. // Информационное право, № 3(34), 2013.
49. Лапина М.А., Николаенко Б.С. Информационная функция государства в сети «Интернет» . // Информационное право, № 4(35), 2013.
50. Лапина М.А., Ревин А.Г., Лапин В.И. Информационное право: Учеб.пособие для студентов вузов. М.: Юнити: Закон и право, 2004. 335 с.
51. Лебедева Н.Н. Право. Личность. Интернет. М.: ВолтерсКлувер, 2004. 232 с.
52. Ловцов Д.А. Обеспечение информационной безопасности в российских телематических сетях. // Информационное право, № 4(31), 2012.

53. Логинов Е.Л. Отмывание денег через интернет-технологии: Методы использования электронных финансовых технологий для легализации криминальных доходов и уклонения от уплаты налогов: Учеб.пособие. М.: ЮНИТИ-ДАНА, 2005. 207 с.
54. Лопатин В.Н. Интеллектуальная собственность в информационном праве. // Информационное право, № 2(33), 2013.
55. Магдилов М.М., Магдилова Л.В. Практика обеспечения информационных прав и свобод в Республике Дагестан. // Информационное право, № 4(35), 2013.
56. Мазуров В.А. Тайна: государственная, коммерческая, банковская, частной жизни: Уголовно-правовая защита: Учеб.пособие / Науч. ред. С.В. Землюков. Издательство "Дашков", 2003. 156 с.
57. Международное информационное право. Метод.материалы к междисциплинарному спецкурсу / Фонд защиты гласности; авт.-сост. Т.М. Смыслова. М.: СТЭНСИ, 2002. 190 с.
58. Монахов В.Н. Свобода массовой информации в Интернете. Правовые условия реализации. М.: Галерея, 2005. 412 с.
59. Наумов В.Б. Право и Интернет: очерки теории и практики. М.: Изд-во "Книжный дом "Университет", 2002.
60. Новое в законодательстве о защите информации: Сб. документов (Новое в российском законодательстве). ДеЛи, 2005. 48 с.
61. О проблемах законодательного регулирования деятельности в сфере информационных технологий и связи: Материалы парламент.слушаний (1 марта 2005 г.); материалы "правительств. часа" (20 апреля 2005 г.); материалы семинара-совещания (7 июня 2005 г.) / Федерал. Собрание РФ.; Гос. Дума. М.: Гос. Дума, 2006. 27 с.
62. Пальцева Е.С. Информационная прозрачность правосудия: пределы и ограничения. // Информационное право, № 4(35), 2013.
63. Паршуков М.И. Понятийный аппарат информационного права в законодательстве, науке и образовательной деятельности. // Информационное право, № 3(34), 2013.
64. Петровский С.В. Интернет-услуги в правовом поле России. М., Агентство «Издательский сервис», 2003.
65. Пилипенко Ю.С. Особенности профессиональных тайн. "Законодательство и экономика", 2008, № 3.
66. Подзорова А.А. Информационное право: Учеб.пособие. Липецк: Липец.эколого-гуманитар. ин-т, 2005. 43 с.
67. Полякова Т.А., Химченко А.И Особенности подготовки кадров в области организационно-правового обеспечения информационной безопасности. // Информационное право, № 3(34), 2013.
68. Потрашкова О.А. Коммерческая тайна: проблемы правовой защиты. // Информационное право, № 1(32), 2013.
69. Просвирнин Ю.Г. Информационное право: Учеб.пособие. Воронеж: Изд-во Воронеж.гос. ун-та, 2003. 628 с.

70. 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.
71. Рагимханова Д.А., Аливердиева М.А. Правовой режим общедоступной информации. - Вестник Дагестанского государственного университета. 2013. № 2. - ИПЦ ДГУ, Махачкала. -С. 57-61
72. Рассолов И.М. Право и Интернет. Теоретические проблемы. М.: Издательство "Норма", 2003.
73. Рублевская М.В. Правовые проблемы деятельности межгосударственных телеканалов на постсоветском пространстве. // Информационное право, № 4(31), 2012.
74. Северин Р.В. Сущность убытков в информационной сфере предприятия. // Информационное право, № 1(32), 2013.
75. Семилетов С.И. Законодательная база строительства электронного государства в РФ // Информационное общество и социальное государство. - М.: ИГП РАН. - 2011. - С. 170-188
76. Серго А. Интернет и право. М.: Бестселлер, 2003. 269 с.
77. Скромников К.С. Компьютерное право РФ: Учебник. МНЭПУ, 2000. 224 с.
78. Соколова С.Н., Сенив Ю.М. Информационное право и государственное регулирование информационной безопасности. // Информационное право, № 2(33), 2013.
79. Страунинг Э.Л. Пробелы в правовом регулировании рекламной деятельности в свете нового Закона "О рекламе". "Юридический мир", 2008, N 7.
80. Стрельцов А.А. Развитие правового обеспечения информационной безопасности: Монография / Под ред. А.А. Стрельцова. М.: Престиж, 2005. 196 с.
81. Сурин В.В. Информационная безопасность уголовно-исполнительной системы: подходы к определению понятия. // Информационное право, № 1(32), 2013.
82. Талапина Э.В. Право на информацию в практике Конституционного Суда Российской Федерации // Труды Института государства и права Российской академии наук. 2011. № 6. С.66-81.
83. Тедеев А.А. Информационное право: Учебник. М.: Эксмо; EksmoEducation, 2005. 463 с.; Тедеев А.А. Информационное право (право Интернета): Учеб.пособие. М.: Эксмо, 2005. 301 с.
84. Терещенко Л.К. Глава «Информационные услуги» в монографии Публичные услуги и право. Изд-во Норма. М., 2007.
85. Терещенко Л.К. Информация и собственность. Защита прав создателей и пользователей программ для ЭВМ и баз данных. М.: РПА МЮ РФ, 1996.
86. Терещенко Л.К. К вопросу о правовом режиме информации. "Информационное право", 2008, N 1.

87. Терещенко Л.К. Правовой режим информации. М., Юриспруденция, 2007.
88. Ткачев А.В. Правовой статус компьютерных документов: основные характеристики. М.: Городец, 2000. 95 с.
89. Травкин Ю.В. Персональные данные. М.: Амалдоникс, 2007. С.432.
90. Фатьянов А.А. Правовое обеспечение безопасности информации в РФ: Учеб.пособие. М.: Юристь, 2001. 412 с.
91. Федотов М.А. Право массовой информации в Российской Федерации. М.: Международные отношения, 2002. 624 с.
92. Фисун А.П., Касилов А.Н., Глоба Ю.А. Право и информационная безопасность: Учеб.пособие. М.: Приор-издат, 2005. 267 с.
93. Цымбалюк В.С. Кодификация информационного законодательства: теоретико-правовые основы. // Информационное право, № 1(32), 2013.
94. Цымбалюк В.С. О систематизации институтов информационного права при кодификации информационного законодательства в СНГ. // Информационное право, № 4(35), 2013.
95. Чамуров В.И. Электронные документы в сети интернет как доказательства в российском судопроизводстве. // Информационное право, № 4(35), 2013.
96. Чаннов С.Е. Информационное право России: Учеб.для ссузов. М.: Приор-издат, 2007. 224 с.
97. Чикурова Е.В. Правовой режим единого государственного реестра прав на недвижимость. // Информационное право, № 4(31), 2012.
98. Чубукова С.Г., Элькин В.Д. Основы правовой информатики (юридические и математические вопросы информатики): Учеб.пособие. Контракт, 2004. 252 с.
99. Шамраев А.В. Правовое регулирование информационных технологий (анализ проблем и основные документы). Версия 1.0. М.: Статут, 2006. 1013 с.
100. Ястребов Д.А. Информационное право: Учеб.-метод. материалы. М.: Изд-во "Прима-Пресс", 2004. 19 с.

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

1. Государственная автоматизированная система «Правосудие» - <http://www.sudrf.ru/index.php?id=300>
2. Министерство связи и телекоммуникаций Республики Дагестан - <http://minsvyaz.e-dag.ru/feed>
3. Научная библиотека Дагестанского государственного университета - <http://www.elib.dgu.ru/>
4. Официальный сайт открытого правительства РФ - http://openstandard.ru/rating_2015.html
5. Официальный сайт ФГБОУ ВПО «Дагестанский государственный университет» - <http://cathedra.icc.dgu.ru/?id=71>

6. Портал государственных программ РФ - <http://programs.gov.ru/Portal/programs/list> -
7. Портал государственных услуг РФ - <http://www.gosuslugi.ru/pgu/stateStructure.html> -
8. Портал открытых данных РФ - <http://data.gov.ru/taxonomy/term/71/datasets>
9. Собрание законодательства РФ на портале Государственной системы правовой информации - <http://pravo.gov.ru/proxy/ips/?editions>
10. 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 Даггосуниверситета <http://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 «Преступность в сфере информационных технологий» 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 «Преступность в сфере информационных технологий» 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, 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.

