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

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Расследование преступлений в сфере компьютерной информации

Кафедра информационного права и информатики
юридического института

Образовательная программа:

40.03.01Юриспруденция

Профиль подготовки:

Уголовно-правовой

Уровень высшего образования: **бакалавриат**

Форма обучения: **очная**

Статус дисциплины: **вариативная**

Махачкала
2016 год

Рабочая программа дисциплины **Расследование преступлений в сфере компьютерной информации** 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 «2» 09 2016г., протокол №1.

Председатель _____ Арсланбекова А.З..
(подпись)

Рабочая программа дисциплины согласована с учебно-методическим управлением «5» 09 2016г. _____
(подпись)

Аннотация рабочей программы дисциплины

Дисциплина Расследование преступлений в сфере компьютерной информации входит в вариативную часть образовательной программы бакалавриата по направлению 40.03.01Юриспруденция.
Дисциплина реализуется в юридическом институте кафедрой информационного права и информатики.

Содержание дисциплины охватывает круг вопросов, связанных с изучением основных понятий и принципов компьютерной безопасности. Рассматриваются способы и механизмы совершения компьютерных преступлений, следственные действия при расследовании таких преступлений и вопросы юридической ответственности за преступления в области компьютерной безопасности.

Дисциплина нацелена на формирование следующих компетенций выпускника: общекультурных –ОК-10, 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

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	16		16			40	зачет

1. Цели освоения дисциплины

Целями освоения дисциплины «Расследование преступлений в сфере компьютерной информации» являются:

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

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) 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 ВО	Планируемые результаты обучения (показатели достижения заданного уровня освоения компетенций)

ОК-10	Способность понимать сущность и значение информации в развитии современного информационного общества, сознавать опасности и угрозы, возникающие в этом процессе, соблюдать основные требования к безопасности, в том числе защиты государственной тайны.	Знать: основные закономерности создания и функционирования информационных процессов в правовой сфере; основы государственной политики в области компьютерной безопасности; методы и средства поиска, систематизации и обработки правовой информации. Уметь: применять современные информационные технологии для поиска и обработки правовой информации, оформления юридических документов и проведения статистического анализа информации. Владеть: навыками сбора, обработки и защите информации, имеющей значение для реализации правовых норм в соответствующих сферах профессиональной деятельности.
ОК-11	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 компьютерной безопасности, получать, хранить, перерабатывать использовать информацию; правильно давать оценку информации. Владеть: навыками поиска, получения, хранения, переработки и защиты компьютерной информации, навыками сбора и обработки информации; навыками анализа информации; навыками обработки информации.
ОК-12	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 компьютерной 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-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 компьютерной безопасности								
1	Криминалистическая характеристика преступлений в сфере компьютерной информации	6		2	2			4	Контрольный опрос
2	Правовое и организационное обеспечение компьютерной	6		2	2			4	Контрольный опрос, тестирование

	безопасности								
3	Способы совершения компьютерных преступлений	6		2	2			6	Контрольный опрос
4	Особенности образования следов по делам о компьютерных преступлениях	6		2	2			6	Контрольный опрос, тестирование
	Итого по модулю 1:			8	8			20	
	Модуль 2. Методика расследования компьютерных преступлений								
5	Осмотр места происшествия по делам о компьютерных преступлениях	6		2	2			4	Контрольный опрос
6	Изъятие следов компьютерных преступлений	6		2	2			4	Контрольный опрос, тестирование
7	Проведение компьютерно-технической экспертизы	6		2	2			6	Контрольный опрос
8	Ответственность за компьютерные преступления	6		2	2			6	Контрольный опрос, рефераты
	Итого по модулю 2:			8	8			20	
	Промежуточный контроль								зачет
	ИТОГО:			16	16			40	

4.3. Содержание дисциплины, структурированное по темам (разделам)

Модуль 1. Основы компьютерной безопасности

Тема 1. Криминалистическая характеристика преступлений в сфере компьютерной информации

Компьютерная информация. Понятие компьютерного преступления. Классификация компьютерных преступлений. 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.

Личностная характеристика преступника, совершающего компьютерное преступление. Непосредственный предмет преступного посягательства по делам о компьютерных преступлениях.

Тема 2. Правовое и организационное обеспечение компьютерной безопасности

Понятие правового обеспечения компьютерной безопасности. Уголовное преследование за совершение компьютерных преступлений. Понятие каналов утечки информации. Организационно-административные мероприятия. Организационно- технические мероприятия.

Тема 3. Способы совершения компьютерных преступлений

Компьютерные манипуляции. Компьютерный шпионаж и кража программ. Компьютерный саботаж. Компьютерные злоупотребления.

Перехват информации. Несанкционированный доступ к информации.

Способы нарушения конфиденциальности и целостности компьютерной информации.

Тема 4. Особенности образования следов по делам о компьютерных преступлениях

Понятие и классификация следов компьютерных преступлений. Структурные файловые следы. Внешние файловые следы. Локальные файловые следы. Сетевые файловые следы. Следы – предметы. Следы-вещества. Регистрационные файлы операционных систем. Политика учетных записей. Политика прав пользователей. Политика аудита.

Модуль 2. Методика расследования компьютерных преступлений

Тема 5. Осмотр места происшествия по делам о компьютерных преступлениях

Понятие осмотра места происшествия. Задачи следственного осмотра.

Подготовительный этап осмотра места происшествия. Рабочий этап осмотра места происшествия. Криминалистическое исследование компьютерных систем и их сетей. Криминалистическое исследование операционных систем.

Тема 6. Изъятие следов компьютерных преступлений

Понятие изъятия следов компьютерных преступлений. Фиксация следовой информации по делам о преступлениях. Резервное копирование файлов серверов. Документы со следами действий операционных систем. Документы со следами действий аппаратуры. Составление протокола изъятия следов.

Тема 7. Проведение компьютерно-технической экспертизы

Понятие компьютерно-технической экспертизы. Аппаратно-компьютерная экспертиза. Программно-компьютерная экспертиза. Информационно-компьютерная экспертиза. Компьютерно-сетевая экспертиза. Комплексные экспертизы.

Тема 8. Ответственность за компьютерные преступления

Уголовная ответственность за преступления в сфере компьютерной информации. Признаки и элементы состава преступления.

Ответственность за неправомерный доступ к компьютерной информации. Ответственность за создание, использование и распространение вредоносных программ для ЭВМ. Ответственность за нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети.

Международный опыт борьбы с преступлениями в сфере компьютерной информации.

Семинарские занятия.

Модуль 1. Основы компьютерной безопасности

Тема 1. **Криминалистическая характеристика преступлений в сфере компьютерной информации**

Вопросы для обсуждения:

1. Понятие и признаки компьютерной информации.
2. Понятие компьютерного преступления.
3. Личностная характеристика преступника, совершившего компьютерные преступления.
4. Непосредственный объект компьютерного преступления.

Тема 2. **Правовое и организационное обеспечение компьютерной безопасности**

Вопросы для обсуждения:

1. Основные направления обеспечения компьютерной безопасности.
2. Понятие правового обеспечения компьютерной безопасности.
3. Организационно-административные мероприятия.
4. Организационно-технические мероприятия.

Тема 3. **Способы совершения компьютерных преступлений**

Вопросы для обсуждения:

1. Понятие способа совершения компьютерного преступления.
2. Классификация способов совершения компьютерных преступлений.

Тема 4. Особенности образования следов по делам о компьютерных преступлениях

Вопросы для обсуждения:

1. Понятие и классификация следов компьютерных преступлений.
2. Регистрационные файлы операционных систем.

Модуль 2. Методика расследования компьютерных преступлений

Тема 5. Осмотр места происшествия по делам о компьютерных преступлениях

Вопросы для обсуждения:

1. Особенности подготовительного этапа осмотра места происшествия.
2. Особенности криминалистического исследования компьютерных систем и их сетей на месте происшествия
3. Криминалистическое исследование операционных систем.

Тема 6. Изъятие следов компьютерных преступлений

Вопросы для обсуждения:

1. Сущность изъятия следов компьютерной информации.
2. Фиксация следовой информации по делам о компьютерных преступлениях.
3. Составление протокола изъятия следов компьютерных преступлений.

Тема 7. **Проведение компьютерно-технической экспертизы**

Вопросы для обсуждения:

1. Понятие и классификация компьютерно-технической экспертизы.
2. Компьютерно-сетевая экспертиза.
3. Комплексная компьютерно-техническая и технико-криминалистическая экспретиза.

Тема 8. **Ответственность за компьютерные преступления**

Вопросы для обсуждения:

1. Ответственность за неправомерный доступ к компьютерной информации.
2. Ответственность за создание, использование и распространение вредоносных программ для ЭВМ.
3. Ответственность за нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети.
4. Международный опыт борьбы с преступлениями в сфере компьютерной 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 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 «Расследование преступлений в сфере компьютерной информации» 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 «Расследование преступлений в сфере компьютерной информации». 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

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-10	Знать: социальную значимость информации в развитии современного информационного общества, роль соблюдения основных требований компьютерной безопасности информации, опасности и угрозы, возникающие в этом процессе; виды, уровни, методы и средства компьютерной безопасности; Уметь: анализировать организационные методы защиты информации.	Устный опрос, письменный опрос, реферат
ОК-11	Знать: основные методы, способы и средства получения, хранения, переработки информации; роль обобщения,	Устный опрос, разбор практических ситуаций

	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.	
ОК-12	Знать: основные виды информационных правоотношений в Интернете; особенности способов правового регулирования 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.	Устный опрос, разбор практических ситуаций, тестирование
ПК-6	Знать: понятие, виды и способы квалификации фактов и обстоятельств, этапы юридической квалификации, содержание источников компьютерного права, точки зрения разных авторов на проблемные вопросы	Устный опрос, разбор практических ситуаций, тестирование

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

Схема оценки уровня формирования компетенции «ОК-10Способность понимать сущность и значение информации в развитии современного информационного общества, сознавать опасности и угрозы, возникающие в этом процессе, соблюдать основные требования информационной безопасности, в том числе защиты государственной тайны»**.**

Уровень	Показатели (что обучающийся должен продемонстрировать)	Оценочная шкала		
		Удовлетворительно	Хорошо	Отлично
Пороговый	Знает социальную значимость информации в развитии современного информационного общества. Умеет определять особенности опасности и	Знает особенности и социальную значимость информации в развитии современного информационного общества; Умеет давать	Толкует смысл понятий «компьютерная информация», «компьютерное преступлени	Распознает требования, которые предъявляются к компьютерной безопасности,; определяет

	угрозы, возникающие в этом процессе. Владеет методами и средствами соблюдения основных требований компьютерной безопасности.	определения понятиям «компьютерная информация», «компьютерная безопасность», «компьютерные преступления»	е»; определяет особенности опасности и угрозы информации	четкие критерии защиты информации

Схема оценки уровня формирования компетенции «ОК-11Владение 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 информацией в условиях	Называет особенности основных методов, способов и средств получения, хранения, переработки информации; дает определение понятий «метод», «способ», «средство», «информация», «информационные системы», «обобщение информации», «анализ информации», «восприятие	Толкует смысл понятий «метод», «способ», «средство», «информация», «компьютерные системы», «обобщение информации», «анализ информации», «восприятие информации». Умеет использовать навыки работы с компьютером как	Распознает требования, которые предъявляются к компьютерной информации, к ее обобщению, анализу как основному ресурсу информационного общества и элемента информационной инфраструктуры. Владеет навыками правового регулирования информационных

	правовой информатизации и развитии информационного общества.	информации»; «методы правового регулирования информационных правоотношений»; «принципы компьютерной безопасности».	средством управления информацией для решения практических задач, анализа судебной практики по компьютерным преступлениям.	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	Выделяет и описывает работу с информацией в глобальных компьютерных сетях; анализирует правовую информацию; обобщает правовую информацию; классифицирует полученную информацию по определенным категориям для ее использовани

			многообразие основных методов, способов и средств получения, хранения, переработки информации, а также средства защиты информации.	я 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	Знает понятие, виды и способы квалификации фактов и обстоятельств, этапы юридической квалификации, содержание источников компьютерного права, точки зрения разных авторов на проблемные	Знает основные положения обеспечения компьютерной безопасности, понимает сущность основных понятий и категорий, выбранных им.	Умеет оперировать юридическими понятиями и категориями компьютерной безопасности. Обладает навыками анализа юридических фактов и возникших в	Знать: понятие, виды и способы квалификации фактов и обстоятельств, угрозы компьютерной безопасности личности, общества и государства, точки зрения

	вопросы Умет правильно давать юридическую оценку фактам и обстоятельствам, обоснованно применять нормы права при правовой квалификации обстоятельств. Владеет: юридической терминологией отраслей права, позволяющей юридически правильно квалифицировать факты и обстоятельства;		связи с ними правоотношений	разных авторов на проблемные вопросы Умеет принимать решения и совершать юридические действия в точном соответствии с законом; правильно давать юридическую оценку фактам и обстоятельствам. Владеет навыками анализа, толкования и правильного 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	Демонстрирует слабое	Имеет представление	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	умение анализировать содержание правовых норм, формулировать выводы и предложения; владения навыками работы по толкованию правовых норм	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.	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. Уголовно-правовая характеристика посягательств на авторские и смежные права в компьютерных сетях

2. Способы совершения посягательств на авторские и смежные права в компьютерных сетях.
3. Криминологическая характеристика посягательств на авторские и смежные права в компьютерных сетях.
4. Особенности расследования посягательств на авторские и смежные права в компьютерных сетях
5. Понятие и виды вредной информации.
6. Правовые проблемы борьбы со «спамом»
7. Классификация вредоносных программ и защита от их воздействия.
8. Информационная война.
9. Информационное оружие.
10. Кибертерроризм как новая угроза информационной безопасности.
11. Виды угроз компьютерной безопасности.
12. Электронные деньги: проблемы правового регулирования
13. Правовое регулирование информационных технологий в области электронной коммерции
14. Правовое регулирование информационных технологий в области рекламы и маркетинга в Интернет
15. Правовое регулирование информационных технологий в области электронных банковских услуг
16. Правовое регулирование информационных технологий в области электронного документооборота
17. Стандартизация, сертификация и лицензирование в информационной сфере.
18. Информационные риски.
19. Хищения с использованием банковских платёжных карт.
20. История использования компьютеров для совершения хищений
21. Компьютерное вымогательство

Примерные тесты

1. 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)

2. Все способы совершения компьютерных преступлений классифицируются в следующие общие группы:

- изъятие средств компьютерной техники (СКТ); перехват информации; несанкционированный доступ к СКТ; манипуляция данными и управляющими командами; комплексные методы
- перехват информации; несанкционированный доступ к СКТ; манипуляция данными и управляющими командами; комплексные методы
- правовые; организационно-технические; программные

3. Основные группы мер предупреждения компьютерных преступлений:

- правовые; организационно-технические; программные
- организационно-технические; криминалистические
- правовые; программные; криминалистические

4. По типу возникновения угрозы безопасности информации принято делить на

- случайные и умышленные
- активные и пассивные
- регламентированные и нерегламентированные
- уголовные и административные

5. Основная угроза безопасности информации – раскрытие конфиденциальной информации выражается в

- несанкционированном доступе к БД, прослушивании каналов и т.п., т.е. это получение информации, являющейся достоянием некоторого лица другими лицами, в результате чего владельцам информации наносится существенный ущерб
- внесении несанкционированных изменений в БД, в результате чего ее потребитель вынужден либо отказаться от нее, либо предпринять дополнительные усилия для выявления изменений и восстановления истинных сведений
- получении одним из абонентов сведений, доступ к которым ему запрещен
- непризнании получателем или отправителем информации фактов ее получения или отправки

6. Основная угроза безопасности информации – компрометация информации выражается в

- внесении несанкционированных изменений в БД, в результате чего ее потребитель вынужден либо отказаться от нее, либо предпринять дополнительные усилия для выявления изменений и восстановления истинных сведений
- несанкционированном доступе к БД, прослушивании каналов и т.п., т.е. это получение информации, являющейся достоянием некоторого лица другими лицами, в результате чего владельцам информации наносится существенный ущерб
- получении одним из абонентов сведений, доступ к которым ему запрещен

- непризнании получателем или отправителем информации фактов ее получения или отправки

7. Основная угроза безопасности информации – несанкционированный обмен информацией между абонентами выражается в
- получении одним из абонентов сведений, доступ к которым ему запрещен
- внесении несанкционированных изменений в БД, в результате чего ее потребитель вынужден либо отказаться от нее, либо предпринять дополнительные усилия для выявления изменений и восстановления истинных сведений
- несанкционированном доступе к БД, прослушивании каналов и т.п., т.е. это получение информации, являющейся достоянием некоторого лица другими лицами, в результате чего владельцам информации наносится существенный ущерб

8. Основная угроза безопасности – информации отказ от информации выражается в
- непризнании получателем или отправителем информации фактов ее получения или отправки
- получении одним из абонентов сведений, доступ к которым ему запрещен
- внесении несанкционированных изменений в БД, в результате чего ее потребитель вынужден либо отказаться от нее, либо предпринять дополнительные усилия для выявления изменений и восстановления истинных сведений
- несанкционированном доступе к БД, прослушивании каналов и т.п., т.е. это получение информации, являющейся достоянием некоторого лица другими лицами, в результате чего владельцам информации наносится существенный ущерб

9. Основная угроза безопасности информации – отказ в обслуживании выражается в
- неправильной работе самой ИС, является весьма существенной и распространенной угрозой
- непризнании получателем или отправителем информации фактов ее получения или отправки
- получении одним из абонентов сведений, доступ к которым ему запрещен
- внесении несанкционированных изменений в БД, в результате чего ее потребитель вынужден либо отказаться от нее, либо предпринять дополнительные усилия для выявления изменений и восстановления истинных сведений

10. Препятствие – это метод защиты информации путем
- физического преграждения пути злоумышленнику к защищаемой информации (к аппаратуре, носителям информации и т.п.)

- побуждения пользователей ИС не разрушать установленные порядки за счет соблюдения сложившихся моральных и этических норм, как регламентированных, так и неписаных
- регулирования использования всех ресурсов ИС и выполнения таких функций как идентификация объекта, опознание объекта по предъявленному им идентификатору, проверку полномочий; разрешение и создание условий работы в пределах установленного регламента, регистрацию обращений к защищаемым ресурсам, регулирование при попытках несанкционированных действий
- вынуждения пользователей и персонала ИС соблюдать правила обработки, передачи и использования защищаемой информации под угрозой материальной, административной или уголовной ответственности

11. Управление доступом – это метод защиты информации путем
- регулирования использования всех ресурсов ИС и выполнения таких функций как идентификация объекта, опознание объекта по предъявленному им идентификатору, проверку полномочий; разрешение и создание условий работы в пределах установленного регламента, регистрацию обращений к защищаемым ресурсам, регулирование при попытках несанкционированных действий
- побуждения пользователей ИС не разрушать установленные порядки за счет соблюдения сложившихся моральных и этических норм, как регламентированных, так и неписаных
- вынуждения пользователей и персонала ИС соблюдать правила обработки, передачи и использования защищаемой информации под угрозой материальной, административной или уголовной ответственности

12. Маскировка – это метод защиты информации путем
- ее криптографического закрытия
- регулирования использования всех ресурсов ИС и выполнения таких функций как идентификация объекта, опознание объекта по предъявленному им идентификатору, проверку полномочий; разрешение и создание условий работы в пределах установленного регламента, регистрацию обращений к защищаемым ресурсам, регулирование при попытках несанкционированных действий
- вынуждения пользователей и персонала ИС соблюдать правила обработки, передачи и использования защищаемой информации под угрозой материальной, административной или уголовной ответственности
- физического преграждения пути злоумышленнику к защищаемой информации (к аппаратуре, носителям информации и т.п.)

13. Регламентация – это метод защиты информации путем
- создания такие условия автоматизированной обработки, хранения и передачи защищаемой информации, при которых возможности несанкционированного доступа к ней сводились бы к минимуму

- побуждения пользователей ИС не разрушать установленные порядки за счет соблюдения сложившихся моральных и этических норм, как регламентированных, так и неписаных
- регулирования использования всех ресурсов ИС и выполнения таких функций как идентификация объекта, опознание объекта по предъявленному им идентификатору, проверку полномочий; разрешение и создание условий работы в пределах установленного регламента, регистрацию обращений к защищаемым ресурсам, регулирование при попытках несанкционированных действий

14. Принуждение – это метод защиты информации путем
- вынуждения пользователей и персонала ИС соблюдать правила обработки, передачи и использования защищаемой информации под угрозой материальной, административной или уголовной ответственности
- побуждения пользователей ИС не разрушать установленные порядки за счет соблюдения сложившихся моральных и этических норм, как регламентированных, так и неписаных
- регулирования использования всех ресурсов ИС и выполнения таких функций как идентификация объекта, опознание объекта по предъявленному им идентификатору, проверку полномочий;
- разрешение и создание условий работы в пределах установленного регламента, регистрацию обращений к защищаемым ресурсам, регулирование при попытках несанкционированных действий

15. Побуждение – это метод защиты информации путем
- побуждения пользователей ИС не разрушать установленные порядки за счет соблюдения сложившихся моральных и этических норм, как регламентированных, так и неписаных
- регулирования использования всех ресурсов ИС и выполнения таких функций как идентификация объекта, опознание объекта по предъявленному им идентификатору, проверку полномочий; разрешение и создание условий работы в пределах установленного регламента, регистрацию обращений к защищаемым ресурсам, регулирование при попытках несанкционированных действий
- вынуждения пользователей и персонала ИС соблюдать правила обработки, передачи и использования защищаемой информации под угрозой материальной, административной или уголовной ответственности
- физического преграждения пути злоумышленнику к защищаемой информации (к аппаратуре, носителям информации и т.п.)

16. В главе 28 "Преступления в сфере компьютерной информации" УК РФ определяются следующие общественно-опасные деяния в отношении средств компьютерной техники:

- неправомерный доступ к охраняемой законом компьютерной информации; создание вредоносных программ для ЭВМ; нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети
- финансовое мошенничество; кража конфиденциальной информации; мошенничество, касающееся средств связи; несанкционированный доступ; диверсия; проникновение в систему
- несанкционированный доступ к информации; применение не сертифицированных программ и баз данных; создание вирусных программ

17. Основными мотивами при совершении компьютерных преступлений являются.
- корыстные, политические, исследовательский интерес, хулиганство и озорство, месть
- корыстные, политические
- хулиганство и озорство
- месть

18. Основными опасными субъектами неправомерного доступа к компьютерной информации являются
- все верны
- хакеры-исследователи, хакеры взломщики, хакеры-вандалы
- крэкеры, компьютерные пираты, кибертеррористы
- вирмейкеры, кардеры, фрикеры

19. Хакеры-исследователи – люди
- образованные и талантливые, основным занятием которых является анализ разнообразного программного обеспечения на уязвимости, которыми может воспользоваться потенциальный взломщик или которые могут улучшить работу компьютерной системы, сети, увеличивая ее эффективность
- осуществляющие по различным целям взлом, проникновение, при котором никакая информация не была уничтожена на каких-либо носителях, система продолжала работать без снижения своей эффективности, после проникновения хакер сообщил соответствующим лицам, ответственным за безопасность данной системы о проникновении, способе проникновения и подробно описал процедуру вторжения
- специализирующиеся на изучении особенностей кредитных карт и банкоматов

20. Хакеры-взломщики – люди
- осуществляющие по различным целям взлом, проникновение, при котором никакая информация не была уничтожена на каких-либо носителях, система продолжала работать без снижения своей эффективности, после проникновения хакер сообщил соответствующим лицам, ответственным за

безопасность данной системы о проникновении, способе проникновения и подробно описал процедуру вторжения
- по каким-то причинам планирующие и осуществляющие вторжение в компьютерные системы с сознательной целью причинения ущерба этим системам
- которые целенаправленно занимаются коммерческим взломом компьютерных систем и сетей в корыстных целях

21. Хакеры-вандалы – люди
- по каким-то причинам планирующие и осуществляющие вторжение в компьютерные системы с сознательной целью причинения ущерба этим системам
- которые целенаправленно занимаются коммерческим взломом компьютерных систем и сетей в корыстных целях
- которые специализируются на взломе программного обеспечения для последующей продажи

22. Крэкеры – люди
- которые целенаправленно занимаются коммерческим взломом компьютерных систем и сетей в корыстных целях
- чаще всего группы, которые специализируются на взломе программного обеспечения для последующей продажи
- которые целенаправленно стараются причинить вред государству или какой-то группе людей, по идеологическим соображениям, по возможности, максимизируя причиненный ущерб

23. Компьютерные пираты – люди
- чаще всего группы, которые специализируются на взломе программного обеспечения для последующей продажи
- которые целенаправленно занимаются коммерческим взломом компьютерных систем и сетей в корыстных целях
- по каким-то причинам планирующие и осуществляющие вторжение в компьютерные системы с сознательной целью причинения ущерба этим системам

24. Кибертеррористы – люди
- которые целенаправленно стараются причинить вред государству или какой-то группе людей, по идеологическим соображениям, по возможности, максимизируя причиненный ущерб
- по каким-то причинам планирующие и осуществляющие вторжение в компьютерные системы с сознательной целью причинения ущерба этим системам
- чаще всего группы, которые специализируются на взломе программного обеспечения для последующей продажи

- которые целенаправленно занимаются коммерческим взломом компьютерных систем и сетей в корыстных целях

25. Вирмейкеры – люди
- которые занимаются написанием компьютерных вирусов
- которые целенаправленно стараются причинить вред государству или какой-то группе людей, по идеологическим соображениям, по возможности, максимизируя причиненный ущерб
- чаще всего группы, которые специализируются на взломе программного обеспечения для последующей продажи

26. Кардеры – люди
- специализирующиеся на изучении особенностей кредитных карт и банкоматов
- специализирующиеся на изучении особенностей незаконного подключения к линиям связи
- которые занимаются написанием компьютерных вирусов

27. Фрикеры – люди
- специализирующиеся на изучении особенностей незаконного подключения к линиям связи
- специализирующиеся на изучении особенностей кредитных карт и банкоматов
- которые целенаправленно занимаются коммерческим взломом компьютерных систем и сетей в корыстных целях

28. По типу возникновения угрозы безопасности информации принято делить на
- случайные и умышленные
- активные и пассивные
- регламентированные и нерегламентированные

29. 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

30. 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. Понятие и признаки компьютерной информации.
2. Понятие компьютерного преступления.
3. Личностная характеристика преступника, совершившего компьютерные преступления.
4. Основные опасные субъекты неправомерного доступа к компьютерной информации.
5. Непосредственный объект компьютерного преступления.
6. Основные направления обеспечения компьютерной безопасности.
7. Понятие правового обеспечения компьютерной безопасности.
8. Организационно-административные мероприятия.
9. Организационно-технические мероприятия.
10. Понятие способа совершения компьютерного преступления.
11. Классификация способов совершения компьютерных преступлений.
12. Понятие и классификация следов компьютерных преступлений.
13. Регистрационные файлы операционных систем.
14. Особенности подготовительного этапа осмотра места происшествия.
15. Особенности криминалистического исследования компьютерных систем и их сетей на месте происшествия
16. Криминалистическое исследование операционных систем.
17. Сущность изъятия следов компьютерной информации.
18. Фиксация следовой информации по делам о компьютерных преступлениях.
19. Составление протокола изъятия следов компьютерных преступлений.
20. Понятие и классификация компьютерно-технической экспертизы.
21. Компьютерно-сетевая экспертиза.
22. Комплексная компьютерно-техническая и технико-криминалистическая экспретиза.
23. Угрозы безопасности информации.
24. Средства защиты компьютерной информации.

25. Методы защиты компьютерной информации.
26. Основные мотивы при совершении компьютерных преступлений.

27. Ответственность за неправомерный доступ к компьютерной информации.
28. Ответственность за создание, использование и распространение вредоносных программ для ЭВМ.
29. Ответственность за нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети.
30. Международный опыт борьбы с преступлениями в сфере компьютерной информации

7.4. 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 -20 баллов,
- выполнение домашних заданий - 20баллов,
- 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. Преступления в сфере компьютерной информации: квалификация и доказывание: Учеб. пособие / Под ред. Ю.В. Гаврилина. М., 2003. 75 с.
11. Проблемы предупреждения преступности в сфере высоких технологий: Сб. науч. ст. / Отв. ред. А.Н. Тарбагаев. Красноярск РУМЦ ЮО, 2004. - 95с.
12. Рассолов И.М. Информационное право : учеб.для магистров / Рассолов, Илья Михайлович. - 2-е изд., испр. и доп. - М. : Юрайт, 2012. - 444 с. - (Магистр).
13. Рассолов И.М. Информационное право : учеб.для магистров / Рассолов, Илья Михайлович. - 2-е изд., испр. и доп. - М. : Юрайт, 2013. - 444 с.
14. Расторгуев С. П. Основы информационной безопасности : учеб. пособие для студ. вузов. -М.: Академия, 2007.
15. Романец Ю.В., Тимофеев П.А., Шаньгин В.Ф. Защита информации в компьютерных системах и сетях. - М.: Радио и связь, 1999. -328 с. 17.
16. Тихонов В.А., Райх В.В. Информационная безопасность: концептуальные, правовые, организационные и технические аспекты: Учебное пособие. - М.: Гелиос АРВ, 2006.
17. Шаньгин В. Ф. Информационная безопасность и защита информации. - М. : Проспект, 2014.
18. Шаньгин В.Ф. Информационная безопасность компьютерных систем и сетей: Учебное пособие. - М.: ИД «ФОРУМ»: ИНФРА-М, 2008.
19. 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).

в) дополнительная литература:

1. Батурин Ю.М. Проблемы компьютерного права. М., 1991.
2. Безугленко О.С. Законодательство в области правовой защиты детей от вредной информации: сравнительно-правовой анализ. // Информационное право, № 1(32), 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., Терещенко Л., Якушев М. Интернет и гласность. М.: Галерия, 1999.

7. Волчинская Е.К. О проблемах формирования правовой системы ограничения доступа к информации. // Информационное право, № 4(35), 2013.
8. Волчинская Е.К.К юбилею Закона Российской Федерации «О государственной тайне». // Информационное право, № 2(33), 2013.
9. Гаврилин Ю.В. Преступления в сфере компьютерной информации. Квалификация и доказывание: Учеб.пособие. М.: Книжный мир, 2003. 245 с.
10. Денисов Ю.Д. Противодействие экстремизму в сети Интернет // Законность. 2009. № 6.
11. Евдокимов К.Н. К вопросу о совершенствовании объективной стороны состава преступления при создании, использовании и распространении вредоносных компьютерных программ (ст. 273 УК РФ) // Российский следователь. 2013. № 7. С. 18 - 24.
12. Евдокимов К.Н. К вопросу о субъективной стороне состава преступления при создании, использовании и распространении вредоносных компьютерных программ (ст. 273 УК РФ) // Российский следователь. 2013. № 8. С. 22 - 26.
13. Евдокимов К.Н. К вопросу об объекте состава преступления при создании, использовании и распространении вредоносных программ для ЭВМ (ст. 273 УК РФ) // Российский следователь. 2012. № 12. С. 24 - 27.
14. Ермакова В.В., Кротов И.Е. Информационные таможенные технологии для бизнеса в России. // Информационное право, № 1(32), 2013.
15. Ефремова М. А. Мошенничество с использованием электронной информации. // Информационное право, № 4(35), 2013.
16. Жарова А.К. О конфликте интересов субъектов в информационных отношениях // Государство и право. 2011. № 4. С. 42-49.
17. Журавлев М.С. Персональные данные в трудовых отношениях: допустимые пределы вмешательства в частную жизнь работника. // Информационное право, № 4(35), 2013.
18. Иванова А.Ю. Проблемы ведения регистра муниципальных нормативных актов в едином информационном пространстве. // Информационное право, № 4(31), 2012.
19. Ильюшенко В.Н. Методологические, организационные и правовые основы информационной безопасности. В 3 ч. Томск: Изд-во Ин-та оптики атмосферы, 2005. 474 с.
20. Информационная безопасность России в условиях глобального информационного общества. М., 2001.
21. Калятин В.О. Право в сфере Интернета. М.: Инфра-М, 2004. 480 с.
22. Касьяненко М.А. Правовые проблемы при использовании Интернета в транснациональном терроризме // Информационное право. 2012. № 1. С. 21 - 25.
23. Киреева Н.В. О программе развития информационных технологий в Роспатенте и ФИПС до 2020 г.. // Информационное право, № 1(32), 2013.

24. Ковалева Н.Н. Информационное право России: Учеб.пособие. М.: Дашков и Ко, 2007. 359 с.
25. Козориз Н.Л. Информационная безопасность в системе противодействия опасности. // Информационное право, № 1(32), 2013.
26. Козориз Н.Л. О предмете правового регулирования информационной безопасности. // Информационное право, № 4(35), 2013.
27. Козырева Т.В. Доступ к информации о деятельности судов. // Информационное право, № 4(31), 2012.
28. 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.
29. Коломиец А.В. Тайна. Коммерческая.Служебная.Государственная: Сборник нормативных правовых актов РФ. М.: Статус, 2001. 656 с.
30. Комаров А.А. Об уточнении понятия «компьютерное мошенничество» в свете законодательных инициатив Верховного Суда РФ // Юрист. 2013. № 17. С. 33 - 36.
31. Комзюк Л.Т. Правовые проблемы создания общественного телевидения Украины в контексте зарубежного опыта. // Информационное право, № 1(32), 2013.
32. Копьёв А.В. Проблемы защиты права на доменное имя. // Информационное право, № 1(32), 2013.
33. Костылев А.К. Информационное право: Учеб.пособие. Тюмень: Изд-во Тюменского гос. ун-та, 2005. 214 с.
34. Кротов А.В. Защита права на неприкосновенность частной жизни при реализации информационных прав посредством телефонной связи. // Информационное право, № 2(33), 2013.
35. Крылов Г.О., Кубанков А.Н. Учебный план магистерской программы «Правовое обеспечение информационной безопасности» . // Информационное право, № 3(34), 2013.
36. Кузнецов В.К. Информационное право: Учеб.-метод. комплекс для дистанц. обучения по спец. 021100 "Юриспруденция". Новосибирск: СибАГС, 2003. 168 с.
37. Кузнецов П.У. Научно-образовательные проблемы информационного права. // Информационное право, № 3(34), 2013.
38. Лапина М.А., Николаенко Б.С. Информационная функция государства в сети «Интернет» . // Информационное право, № 4(35), 2013.
39. Лапина М.А., Ревин А.Г., Лапин В.И. Информационное право: Учеб.пособие для студентов вузов. М.: Юнити: Закон и право, 2004. 335 с.
40. Лебедева Н.Н. Право. Личность. Интернет. М.: ВолтерсКлувер, 2004. 232 с.
41. Ловцов Д.А. Обеспечение информационной безопасности в российских телематических сетях. // Информационное право, № 4(31), 2012.

42. 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.
43. Лопатин В.Н. Интеллектуальная собственность в информационном праве. // Информационное право, № 2(33), 2013.
44. Лямин Л.В. Управление противодействием компьютерным мошенничествам // Управление в кредитной организации. 2011. № 1. С. 87 - 97.
45. Магдилов М.М., Магдилова Л.В. Практика обеспечения информационных прав и свобод в Республике Дагестан. // Информационное право, № 4(35), 2013.
46. Мазуров В.А. Тайна: государственная, коммерческая, банковская, частной жизни: Уголовно-правовая защита: Учеб.пособие / Науч. ред. С.В. Землюков. Издательство "Дашков", 2003. 156 с.
47. Международное информационное право. Метод.материалы к междисциплинарному спецкурсу / Фонд защиты гласности; авт.-сост. Т.М. Смыслова. М.: СТЭНСИ, 2002. 190 с.
48. Монахов В.Н. Свобода массовой информации в Интернете. Правовые условия реализации. М.: Галерия, 2005. 412 с.
49. Наумов В.Б. Право и Интернет: очерки теории и практики. М.: Изд-во "Книжный дом "Университет", 2002.
50. Незнамов А.В. Территориальная подсудность дел о признании экстремистскими информационных материалов, размещенных в сети Интернет // Арбитражный и гражданский процесс. 2010. № 5. С. 12 - 16.
51. Новое в законодательстве о защите информации: Сб. документов (Новое в российском законодательстве). ДеЛи, 2005. 48 с.
52. 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.
53. Пальцева Е.С. Информационная прозрачность правосудия: пределы и ограничения. // Информационное право, № 4(35), 2013.
54. Паненков А.А. Предложения по оптимизации борьбы с использованием сети Интернет в террористических целях // Правовые вопросы связи. 2011. № 2. С. 15 - 21.
55. Паршуков М.И. Понятийный аппарат информационного права в законодательстве, науке и образовательной деятельности. // Информационное право, № 3(34), 2013.
56. Подзорова А.А. Информационное право: Учеб.пособие. Липецк: Липец.эколого-гуманитар. ин-т, 2005. 43 с.
57. Полякова Т.А., Химченко А.И Особенности подготовки кадров в области организационно-правового обеспечения информационной безопасности. // Информационное право, № 3(34), 2013.

58. Потрашкова О.А. Коммерческая тайна: проблемы правовой защиты. // Информационное право, № 1(32), 2013.
59. Просвирнин Ю.Г. Информационное право: Учеб.пособие. Воронеж: Изд-во Воронеж.гос. ун-та, 2003. 628 с.
60. 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.
61. Рагимханова Д.А., Аливердиева М.А. Правовой режим общедоступной информации. - Вестник Дагестанского государственного университета. 2013. № 2. - ИПЦ ДГУ, Махачкала. -С. 57-61
62. Рассолов И.М. Право и Интернет. Теоретические проблемы. М.: Издательство "Норма", 2003.
63. Рублевская М.В. Правовые проблемы деятельности межгосударственных телеканалов на постсоветском пространстве. // Информационное право, № 4(31), 2012.
64. Северин Р.В. Сущность убытков в информационной сфере предприятия. // Информационное право, № 1(32), 2013.
65. Семилетов С.И. Законодательная база строительства электронного государства в РФ // Информационное общество и социальное государство. - М.: ИГП РАН. - 2011. - С. 170-188
66. Серго А. Интернет и право. М.: Бестселлер, 2003. 269 с.
67. Скромников К.С. Компьютерное право РФ: Учебник. МНЭПУ, 2000. 224 с.
68. Соколова С.Н., Сенив Ю.М. Информационное право и государственное регулирование информационной безопасности. // Информационное право, № 2(33), 2013.
69. Страунинг Э.Л. Пробелы в правовом регулировании рекламной деятельности в свете нового Закона "О рекламе". "Юридический мир", 2008, N 7.
70. Стрельцов А.А. Развитие правового обеспечения информационной безопасности: Монография / Под ред. А.А. Стрельцова. М.: Престиж, 2005. 196 с.
71. Сурин В.В. Информационная безопасность уголовно-исполнительной системы: подходы к определению понятия. // Информационное право, № 1(32), 2013.
72. Суслопаров А.В., Тарбагаев А.Н. Ответственность за нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно- телекоммуникационных сетей: уголовно-правовой и административный аспекты // Правовая политика и правовая жизнь. 2012. №2
73. 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.
74. Терещенко Л.К. Глава «Информационные услуги» в монографии Публичные услуги и право. Изд-во Норма. М., 2007.

75. Терещенко Л.К. Информация и собственность. Защита прав создателей и пользователей программ для ЭВМ и баз данных. М.: РПА МЮ РФ, 1996.
76. Терещенко Л.К. К вопросу о правовом режиме информации. "Информационное право", 2008, N 1.
77. Терещенко Л.К. Правовой режим информации. М., Юриспруденция, 2007.
78. Ткачев А.В. Правовой статус компьютерных документов: основные характеристики. М.: Городец, 2000. 95 с.
79. Фисун А.П., Касилов А.Н., Глоба Ю.А. Право и информационная безопасность: Учеб.пособие. М.: Приор-издат, 2005. 267 с.
80. Хилюта В.В. Уголовная ответственность за хищения с использованием компьютерной техники // Журнал российского права. 2014. № 3. С. 111 - 118.
81. Цымбалюк В.С. Кодификация информационного законодательства: теоретико-правовые основы. // Информационное право, № 1(32), 2013.
82. Цымбалюк В.С. О систематизации институтов информационного права при кодификации информационного законодательства в СНГ. // Информационное право, № 4(35), 2013.
83. Чамуров В.И. Электронные документы в сети интернет как доказательства в российском судопроизводстве. // Информационное право, № 4(35), 2013.
84. Чаннов С.Е. Информационное право России: Учеб.для ссузов. М.: Приор-издат, 2007. 224 с.
85. Чикурова Е.В. Правовой режим единого государственного реестра прав на недвижимость. // Информационное право, № 4(31), 2012.
86. Ягудин А. Н. Уголовная ответственность за нарушение правил эксплуатации средств хранения, обработки и передачи компьютерной информации и информационно-телекоммуникационных сетей. Автореферат дисс… канд. юрид. наук. М., 2013. 28 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 авторефератовhttp://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 Даггосуниверситетаhttp://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 курса «Расследование преступлений в сфере компьютерной информации» 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 восьми 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.