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

Кафедра информационного права и информатики

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Расследование преступлений в сфере компьютерной информации

Образовательная программа:
40.03.01Юриспруденция

Профиль подготовки:
Уголовно-правовой

Уровень высшего образования
бакалавриат

Форма обучения
очная

Статус дисциплины: **вариативная по выбору**

Махачкала
2020 год

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

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

Рабочая программа дисциплины одобрена:

На заседании кафедры информационного права и информатики

от «19» 03 2020 г., протокол № 8

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

На заседании Методической комиссии юридического института

от «25» 03 2020г., протокол № 7

Председатель _____ Арсланбекова А.З.
(подпись)

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

Аннотация рабочей программы дисциплины

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

Содержание дисциплины охватывает круг вопросов, связанных с изучением основных понятий 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-3, ОК-4, 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	14		14			44	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 ОПОП бакалавриата

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

Дисциплина логически и содержательно-методически связана с

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

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

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

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

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

Компетенции	Формулировка компетенции из ФГОС ВО	Планируемые результаты обучения (показатели достижения заданного уровня освоения компетенций)

ОК-3	Владение основными методами, способами и средствами получения, хранения, переработки информации, имеет навыки работы с компьютером как средством управления информацией.	Знать: основные методы, способы и средства получения, хранения, переработки информации; закономерности обращения информации в правовой сфере; методы и способы защиты информации; методы законного получения, хранения и переработки ин-формации. Уметь: пользоваться основными методами, способами и средствами получения, хранения, переработки информации; соблюдать основные требования компьютерной без-опасности, 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-4	Способность работать с информацией в глобальных компьютерных сетях	Знать: основы работы с информацией в глобальных компьютерных сетях; информационно-правовые технологии (правовые порталы) с помощью которых осуществляется поиск информации в сети Интернет. Уметь: работать в глобальных компьютерных сетях; решать любые юридические задачи, связанные с добыванием в сети Интернет правовых материалов. Владеть: навыками обработки правовых материалов, найденных в среде правовых порталов.
ПК-6	Способность правильно квалифицировать факты и обстоятельства	Знать: понятие, виды и способы квалификации фактов и обстоятельств, этапы

		юридической квалификации, содержание источников 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**	**Виды учебной работы, включая самостоятельную работу студентов и трудоемкость (в часах)**	**Самостоятел**	**Формы текущего контроля успеваемости *(по неделям семестра)* Форма**

				Лекции	**Практические занятия**	**Лабораторные**	**Контроль самост.**		**промежуточной аттестации *(по семестрам)***
	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 безопасности	6		2	2			4	Контрольный опрос, тестирование
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		1	1			6	Контрольный опрос
6	Изъятие следов компьютерных преступлений	6		1	1			6	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:			6	6			24	
	Промежуточный контроль								зачет
	ИТОГО:			14	14			44	

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 экспертиза.

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

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

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

В ходе освоения учебного курса «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 института 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.

Основными видами самостоятельной работы студентов являются:

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

№п/п	**Вид самостоятельной работы**	**Вид контроля**	**Учебно-методическое обеспечение**
1.	Изучение рекомендованной литературы, поиск дополнительного материала	Опрос, тестирование, коллоквиум	См. разделы 6 и 7 данного документа

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

Нормативно-правовые акты

1. Конституция Российской Федерации: принята всенар. голосованием 12.12.1993 г. // Собр. законодательства Рос. Федерации. – 2014. – № 31. – Ст. 4398.
2. Арбитражный процессуальный кодекс Российской Федерации: федеральный закон от 24.07.2002 № 95-ФЗ: в ред. от 29.06.2015 №195-ФЗ // СЗ РФ. – 2002. – № 30. – Ст. 3012.; СЗ РФ. – 2015. – № 27. – Ст. 3986.
3. 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.
4. Гражданский кодекс РФ (часть 4): Федеральный закон от 18.12.2006 N 230-ФЗ //СЗ РФ. – 2006. - №52. – Ст. 5496.
5. Гражданский процессуальный кодекс Российской Федерации от 14.11.2002 № 138-ФЗ (ред. от 30.12.2015) (с изм. и доп., вступ. в силу с 01.01.2016) // Собрание законодательства РФ. – 2002. – № 46. – Ст. 4532.

6. Доктрина информационной безопасности Российской Федерации: Указ Президента РФ от 05.12.2016 N 646 "Об утверждении Доктрины информационной безопасности Российской Федерации". //Собрание законодательства РФ, 12.12.2016, N 50, ст. 7074
7. Кодекс Российской Федерации об административных правонарушениях// Российская газета. — 2001. — № 256.
8. 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.
9. О безопасности: Федеральный закон от 28 декабря 2010 г. N 390-ФЗ//Собрание законодательства Российской Федерации, 2011, N 1, ст. 2.
10. О государственной тайне: Федеральный закон от 21 июля 1993г. № 5485 – 1 – ФЗ // СЗ РФ. – 1993. - №41. – Ст. 4673.
11. О коммерческой тайне: Федеральный закон от 29 июля 2004 г. N 98-ФЗ // СЗ РФ. 2004. N 32. Ст. 3283.
12. О персональных данных: Федеральный закон от 27 июля 2006 г. № 152 – ФЗ // СЗ РФ. – 2006. - №31 (1ч.). – Ст. 3451.
13. О порядке освещения деятельности органов государственной власти в государственных средствах массовой информации: Федеральный закон от 13.01.1995 N 7-ФЗ (ред. от 12.05.2009) (принят ГД ФС РФ 15.12.1994) // "Собрание законодательства РФ", 16.01.1995, N 3, ст. 170.
14. О порядке рассмотрения обращений граждан Российской Федерации: Федеральный закон от 02.05.2006 № 59 – ФЗ (ред. от 29.06.2010) //Парламентская газета. — 2006. — № 70–71.
15. 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.
16. 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.
17. О рекламе: Федеральный закон от 13 марта 2006 г.№ 38 – ФЗ //СЗ РФ . - 2006. - №12. - ст. 1232.
18. О рекламе: Федеральный Закон РФ от 13.03.2006 № 38 - ФЗ (ред. от 08.03.2015) //Собрание Законодательства РФ. - 2006. - №12. - ст. 1232.
19. 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.
20. О средствах массовой информации: Закон РФ от 27.12.1991 №2124-1. // Ведомости РФ СНД и ВС РФ, 13.02.1992, № 7, ст. 300.
21. Об информации, информационных технологиях и о защите информации: Федеральный закон от 27 июля 2006 г. № 149 – ФЗ // СЗ РФ. – 2006. - №31 (1ч.). – Ст. 3448.

22. Об обеспечении доступа к информации о деятельности государственных органов и органов местного самоуправления: Федеральный закон от 09.02.2009 № 8-ФЗ «» // Собрание законодательства Российской Федерации, 16.02.2009, № 7, ст. 776.
23. 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.
24. Об электронной подписи: Федеральный закон от 6 апреля 2011 г. № 10 // Собрание законодательства РФ, 11.04.2011, N 15, ст. 2036.
25. 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.
26. 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.
27. 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.
28. Уголовно–процессуальный кодекс Российской Федерации //Российская газета. — 2001. — № 249.
29. Уголовный кодекс РФ //СЗ РФ. – 1996. - №25. – Ст. 2954.

Задачи для самостоятельной работы

1. Районный суд признал запрещенной «Инструкцию по даче взятки гаишнику», размещенную в сети Интернет. Аргументы суда: 1) дача взятки является уголовно наказуемым деянием; 2) п. 6 ст. 10 Федерального закона «Об информации, информационных технологиях и о защите информации»; 3) распространение таких сведений «подрывает конституционный строй и авторитет Российской Федерации, а также основы нравственности граждан России, способствует развитию коррупции, чем нарушает права и законные интересы неопределенного круга лиц, получающих доступ к незаконной информации, в связи с чем, подлежит ограничению». *Можно ли согласиться с таким решением и такой аргументацией? Ознакомьтесь с мнением юриста об этой ситуации:* https://goo.gl/wjh5px.
2. В соответствии с абз. 3 пункта 82 Стратегии национальной безопасности Российской Федерации, утв. Указом Президента РФ от 31.12.2015 № 683 укреплению национальной безопасности в области культуры способствуют принятие мер по защите российского 45 общества от внешней идейно-ценностной экспансии и деструктивного информационно-психологического воздействия. С учетом этого *проанализируйте федеральные законы «О рекламе», «О защите детей от информации, причиняющей вред их здоровью и развитию», «О СМИ» и выпишите нормы, которые способствуют выполнению данного*

положения Стратегии. Если такие нормы вам обнаружить не удалось, предложите собственные варианты юридического закрепления соответствующих защитных мер.

3. Какие действия входят в понятие «защита информации»? Дайте ответ с учетом положений статьи 23 Федерального закона «Об организованных торгах», статьи 101 Федерального закона «О таможенном регулировании в Российской Федерации», статьи 27 Федерального закона «О национальной платежной системе».
4. Кинофильмы, документальные фильмы, учебные фильмы, мультфильмы, книги, интерактивные книги, электронные книги, компьютерные программы, компьютерные игры, андроид-приложения, реклама, объявления, смс-рассылки, цирковые представления, аттракционы в парках развлечений, газеты, журналы, листовки, квитанции, протоколы, видео на Ютюб, сайты, публикации ВКонтакте. *Какие из перечисленных объектов подлежат возрастной маркировке в соответствии с законодательством о защите детей от информации, причиняющей вред здоровью и развитию?*
5. Осужденному П., переведенному в одиночную камеру, было отказано в получении от родственников смартфона, с пояснением, что ограничение необходимо в целях обеспечения информационной безопасности в процессе отбывания наказания. П. не согласился с таким решением и пояснил, что в соответствии со статьей 94 УИК РФ даже в одиночной камере он имеет право смотреть кинофильмы и видеофильмы не реже одного раза в неделю. На смартфоне хранятся 46 его любимые фильмы, и он хотел бы, чтобы устройство выдавалось ему не реже одного раза в неделю на 2 часа. Сим-карты в смартфоне нет, поэтому для звонков и выхода в Интернет использовать устройство невозможно. *Дайте юридическую оценку действий администрации исправительного учреждения. Можно ли признать состоятельными доводы П.?*
6. Известный блогер распространил в Интернете информацию о похищении девушки неизвестными лицами на черном БМВ. В заметке он указал место и время совершения преступления, точный адрес, фамилию и имя потерпевшей, подробно описал автомобиль преступников. Проверкой этого сообщения сотрудниками правоохранительных органов было установлено, что распространенная информация не соответствует действительности. Дайте юридическую оценку действиям блогера.
7. Житель дома номер 8 по ул. Кирова города N расклеил на подъездах своего дома объявление следующего содержания: «Председатель нашей управляющей компании Иванов И. И. — жулик и вор! Собрание по поводу избрания новой управляющей компании состоится…». Иванов И. И. обратился к юристу за консультацией. Какие рекомендации можно дать гражданину Иванову?
8. К. со своего личного аккаунта ВКонтакте оставила под фотографией своего бывшего сожителя У. следующий публичный комментарий: «Девушки! Он подлец, негодяй и скотина! Бегите от него, пока не

поздно!». У. сохранил данный комментарий и обратился в суд с иском к К., в котором потребовал, чтобы она в соответствии со ст. 152 ГК РФ публично опровергла порочащие его честь и достоинство сведения. В качестве доказательств У. предоставил в суд положительную характеристику на него, составленную участковым инспектором полиции по месту жительства, положительную характеристику с места работы, а также пригласил девять свидетелей-соседей, которые подтвердили, что У. замечательный человек и никакой не подлец, негодяй и скотина. К. в судебное заседание не явилась, отзыв не представила, хотя была извещена надлежащим образом. Какое решение должен вынести суд?

Примерная тематика рефератов (творческих работ)

1. Понятие и виды вредной информации.
2. Правовые проблемы борьбы со «спамом»
3. Классификация вредоносных программ и защита от их воздействия.
4. Информационная война.
5. Информационное оружие.
6. Кибертерроризм как новая угроза информационной безопасности.
7. Виды угроз компьютерной безопасности.
8. Электронные деньги: проблемы правового регулирования
9. Правовое регулирование информационных технологий в области электронной коммерции
10. Правовое регулирование информационных технологий в области рекламы и маркетинга в Интернет
11. Правовое регулирование информационных технологий в области электронных банковских услуг
12. Правовое регулирование информационных технологий в области электронного документооборота
13. Стандартизация, сертификация и лицензирование в информационной сфере.
14. Информационные риски.

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

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

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

Компетенция	Знания, умения, навыки	Процедура освоения
ОК-3	Знать: основные методы, способы и средства	Устный

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

	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 Типовые контрольные задания

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

4. 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

5. 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

6. 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

7. 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

8. 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

9. 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

10. 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

11. 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.)

12. 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

13. 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

14. 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.)

15. 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

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

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

18. 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

19. 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

20. 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

21. 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

22. 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

23. 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

24. 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

25. Кардеры – люди

- специализирующиеся на изучении особенностей кредитных карт и банкоматов
- специализирующиеся на изучении особенностей незаконного подключения к линиям связи
- которые занимаются написанием компьютерных вирусов

26. 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

27. По типу возникновения угрозы безопасности информации принято делить на

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

28. Правонарушителей в области компьютерной преступности по социальному статусу и уровню образования можно разделить на следующие группы

- ученики школ; студенты; сотрудники высших учебных заведений;
- кассиры банков; программисты

- лица, состоящие с потерпевшим в трудовых или иных деловых отношениях; лица, не связанные деловыми отношениями с потерпевшим

-хакеры-исследователи, хакеры взломщики, хакеры-вандалы все верны

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)

30. 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

31. 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
32. 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
33. 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

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

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

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

Текущий контроль по дисциплине включает:

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

Промежуточный контроль по дисциплине включает:

- письменная контрольная работа - 30 баллов,
- тестирование - 10 баллов.

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

а) основная литература:

1. Бачило И.Л. Информационное право: учеб. для магистров / Бачило, Иллария Лаврентьевна; Ин-т гос. и права РАН, Акад. правовой ун-т (Ин-т). - 3-е изд., перераб. и доп. - М. : Юрайт, 2013. - 564 с.
2. Бачило И.Л. Информационное право: учебник / Бачило, ИлларияЛаврентьевна ; Ин-т гос. и права Рос. акад. наук, Академический

правовой ун-т (ин-т). - 2-е изд., перераб. и доп. - М. : Юрайт, 2011. - 522 с. - (Магистр).
3. Мельников В.П., Клеймёнов С.А., Петраков А.М. Информационная безопасность и защита информации: учебник - Москва : Academia, 5-е издание, 2011
4. Организационное и правовое обеспечение информационной безопасности: учебник и практикум / под ред. Поляковой Т.А., Стрельцова А.А. – М.: Юрайт, 2017. – 325 с.
5. Городов О.А. Информационное право [Электронный ресур с]: учебник для бакалавров. – М.: Издательство Проспект, 2016. – 303 с. – URL: http://нэб.рф/catalog/000199_000009_008578609/ - ЭБС «НЭБ».
6. Кузнецов П.У. Информационное право [Электронный ресурс]: учебник для бакалавров.. – М.: Издательство Юстиция, 2017. – 335 с. – URL: http://нэб.рф/catalog/000199_000009_009476417/ - ЭБС «НЭБ».
7. Информационное право: учеб. пособие / Р. А. Абдусаламов; Минобрнауки России, Дагест. гос. ун-т. - Махачкала : Изд-во ДГУ, 2015. - 211 с.
8. Информационное право: учеб.-метод. комплекс / [М.А.Эмиров, Л.В.Корж]; М-во образования и науки Рос. Федерации; Федерал. агентство по образованию; Дагест. гос. ун-т. - Махачкала : ИПЦ ДГУ, 2007. - 146 с.
9. Рассолов И.М. Информационное право: учеб. для магистров / Рассолов, Илья Михайлович. - 2-е изд., испр. и доп. - М. :Юрайт, 2012. - 444 с. - (Магистр).
10. Рассолов И.М. Информационное право: учеб. для магистров / Рассолов, Илья Михайлович. - 2-е изд., испр. и доп. - М. : Юрайт, 2013. - 444 с.

б) дополнительная литература:

1. Безугленко О.С. Законодательство в области правовой защиты детей от вредной информации: сравнительно-правовой анализ. // Информационное право, № 1(32), 2013.
2. Безугленко О.С. Сравнительная характеристика регионального и федерального законодательства в области правовой защиты детей от вредной информации. // Информационное право, № 2(33), 2013.
3. Булгакова Е.В., Архиереев Н.Л. Методика формирования компетенций юриста в области организационно-правового обеспечения информационной безопасности. // Информационное право, № 3(34), 2013.
4. Булгакова Л.И. Правовой режим аудиторской тайны. "Журнал российского права", 2008, № 5.
5. Бусленко Н.И. Медиаправо России: Документы, комментарии, вопросы и ответы. Феникс, 2005. 285 с.
6. Волчинская Е.К. О проблемах формирования правовой системы ограничения доступа к информации. // Информационное право, № 4(35), 2013.
7. Волчинская Е.К.К юбилею Закона Российской Федерации «О государственной тайне». // Информационное право, № 2(33), 2013.
8. Жарова А.К. Право и информационные конфликты в информационно-телекоммуникационной сфере. – Москва, 2016.

9. Казанцев С.Я и др. Правовое обеспечение информационной безопасности : учеб. пособие для студентов вузов. - 3-е изд.,стер. -Москва : Academia, 2008.
10. Кириленко В.П., Алексеев Г.В. Международное право и информационная безопасность государств. Монография – Санкт-Петербург, 2016.
11. Кротов А.В. Защита права на неприкосновенность частной жизни при реализации информационных прав посредством телефонной связи. // Информационное право, № 2(33), 2013.
12. Крылов Г.О., Кубанков А.Н. Учебный план магистерской программы «Правовое обеспечение информационной безопасности» . // Информационное право, № 3(34), 2013.
13. Кузнецов П.У. Научно-образовательные проблемы информационного права. // Информационное право, № 3(34), 2013.
14. Лапина М.А. Информационное право: учебное пособие для студентов вузов, обучающихся по специальности 021100 «Юриспруденция»/ Лапина М.А., Ревин А.Г., Лапин В.И.— М.: ЮНИТИ-ДАНА, 2017.— 335 с.
15. Лапина М.А., Николаенко Б.С. Информационная функция государства в сети «Интернет» . // Информационное право, № 4(35), 2013.
16. Ловцов Д.А. Обеспечение информационной безопасности в российских телематических сетях. // Информационное право, № 4(31), 2012.
17. Морозов А.В. Информационное право и информационная безопасность. Часть 1: учебник для магистров и аспирантов/ Морозов А.В., Филатова Л.В., Полякова Т.А.— Москва, Саратов: Всероссийский государственный университет юстиции (РПА Минюста России), Ай Пи Эр Медиа, 2016.— 436 с.
18. Морозов А.В. Информационное право и информационная безопасность. Часть 2: учебник для магистров и аспирантов/ Морозов А.В., Филатова Л.В., Полякова Т.А. — Москва, Саратов: Всероссийский государственный университет юстиции (РПА Минюста России), Ай Пи Эр Медиа, 2016.— 604 с.
19. Морозов А.В. Правовые вопросы доступа к информации: учебное пособие/ Морозов А.В., Филатова Л.В.— М.: Всероссийский государственный университет юстиции (РПА Минюста России), 2015.— 84 с.
20. Организационное и правовое обеспечение информационной безопасности : учебник и практикум для бакалавриата и магистратуры / Т. А. Полякова, А. А. Стрельцов, С. Г. Чубукова, В. А. Ниесов ; под ред. Т. А. Поляковой, А. А. Стрельцова. — М. : Издательство Юрайт, 2018. — 325 с. — (Серия : Бакалавр и магистр. Академический курс).
21. Полякова Т.А., Химченко А.И Особенности подготовки кадров в области организационно-правового обеспечения информационной безопасности. // Информационное право, № 3(34), 2013.
22. Потрашкова О.А. Коммерческая тайна: проблемы правовой защиты. // Информационное право, № 1(32), 2013.
23. Просвирнин Ю.Г. Информационное право: Учеб.пособие. Воронеж: Изд-во Воронеж.гос. ун-та, 2003. 628 с.

24. Рагимханова Д.А., Аливердиева М.А. Особенности правового режима информации ограниченного доступа. - Научные труды РАЮН, Вып. 14 в 2 т. Т.1 – Москва, 2014г. - С. 974-977.
25. Рагимханова Д.А., Аливердиева М.А. Правовой режим общедоступной информации. - Вестник Дагестанского государственного университета. 2013. № 2. - ИПЦ ДГУ, Махачкала. -С. 57-61
26. Рассолов И.М. Информационное право : учеб.для магистров / Рассолов, Илья Михайлович. - 2-е изд., испр. и доп. - М. : Юрайт, 2012. - 444 с. - (Магистр).
27. Рассолов И.М. Информационное право : учеб.для магистров / Рассолов, Илья Михайлович. - 2-е изд., испр. и доп. - М. : Юрайт, 2013. - 444 с.
28. Смирнов А.А. Обеспечение информационной безопасности в условиях виртуализации общества. Опыт Европейского Союза [Электронный ресурс]: монография/ Смирнов А.А.— М.: ЮНИТИ-ДАНА, 2015.— 159 с.— URL: http://www.iprbookshop.ru/52524.html.— ЭБС «IPRbooks».
29. Сурин В.В. Информационная безопасность уголовно-исполнительной системы: подходы к определению понятия. // Информационное право, № 1(32), 2013.
30. Сычев Ю.Н. Стандарты информационной безопасности. Защита и обработка конфиденциальных документов [Электронный ресурс]: учебное пособие/ Сычев Ю.Н.— Саратов: Вузовское образование, 2018.— 195 с.— URL: http://www.iprbookshop.ru/72345.html.— ЭБС «IPRbooks».
31. Чеботарева А.А. Информационное право. Учебное пособие / Москва, 2014.
32. Шаньгин В. Ф. Информационная безопасность и защита информации. - М. : Проспект, 2014.
33. Шибаев Д.В. Информационное право: практикум по курсу/ Шибаев Д.В.— Саратов: Ай Пи Эр Медиа, 2017.— 277 с.

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

1. eLIBRARY.RU[Электронный ресурс]: электронная библиотека / Науч. электрон. б-ка. — Москва, 1999 – . Режим доступа: http://elibrary.ru/defaultx.asp. – Яз. рус., англ.
2. Moodle[Электронный ресурс]: система виртуального обучением: [база данных] / Даг. гос. ун-т. – Махачкала, г. – Доступ из сети ДГУ или, после регистрации из сети ун-та, из любой точки, имеющей доступ в интернет. – URL: http://edu.dgu.ru/course/
3. Образовательный блог по Информационному праву (Ragimhanova.blogspot.ru)/
4. Государственная автоматизированная система «Правосудие» - http://www.sudrf.ru/index.php?id=300
5. Научная библиотека Дагестанского государственного университета - http://www.elib.dgu.ru/

6. Официальный сайт открытого правительства РФ - http://openstandard.ru/
7. Официальный сайт ФГБОУ ВО «Дагестанский государственный университет» - http://cathedra.icc.dgu.ru/?id=71
8. Официальный сайт Федеральной службы безопасности РФ - http://www.fsb.ru/
9. Официальный сайт Следственного комитета РФ - http:// www.sledcom.ru
10. Официальный сайт Федеральной службы судебных приставов России http:// www.fssprus.ru
11. Портал государственных программ РФ - http://programs.gov.ru/Portal/programs/list
12. Портал государственных услуг РФ - http://www.gosuslugi.ru/pgu/stateStructure.html
13. Портал открытых данных РФ - http://data.gov.ru/taxonomy/term/71/datasets
14. Собрание законодательства РФ на портале Государственной системы правовой информации - http://pravo.gov.ru/proxy/ips/?editions
15. Судебная практика – www.sud-praktika.narod.ru

Базы данных, информационно-справочные и поисковые системы

1. Справочная правовая система «КонсультантПлюс» www.consultant.ru
2. Справочная правовая система Гарант –http://www.garant.ru/
3. Электронная Библиотека Диссертаций Российской государственной библиотеки ЭБД РГБ. Включает полнотекстовые базы данных диссертаций. http://diss.rsl.ru
4. Научная электронная библиотека диссертаций и авторефератов. http://www.dissercat.com/
5. Электронная библиотека образовательных и научных изданий Iqlib. www.iqlib.ru
6. Интернет-библиотека СМИ Public.ru www.public.ru
7. Информационные ресурсы научной библиотеки Даггосуниверситета (доступ через платформу Научной электронной библиотеки elibrary.ru)/ http://elib.dgu.ru
8. Электронные каталоги Научной библиотеки Даггосуниверситетаhttp://elib.dgu.ru/?q=node/256
9. Сайт образовательных ресурсов Даггосуниверситета http://edu.icc.dgu.ru
10. Юридический Вестник ДГУ.http://www.jurvestnik.dgu.ru

1. Шибаев Д.В. Правовой режим врачебной тайны как информационно-правового объекта. //Право. Журнал Высшей школы экономики. 2015. № 3. С. 66-77.
2. Шутова А.А. Особенности квалификации деяния при наличии конкуренции норм уголовного и административного законодательства (на примере информационных противоправных деяний). //Юридическая наука и практика: Вестник Нижегородской академии МВД России. 2016. № 2 (34). С. 360-364.
3. Шутова А.А. Сравнительно-правовое исследование отдельных норм уголовного и административного законодательства,

предусматривающих ответственность за информационные противоправные деяния. //Вестник Нижегородской правовой академии. 2016. № 10 (10). С. 71-74.

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 «Расследование преступлений в сфере компьютерной информации» 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 «Расследование преступлений в сфере компьютерной информации» 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 дисциплины «Расследование преступлений в сфере компьютерной информации» 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 «Расследование преступлений в сфере компьютерной информации».

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.

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.