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

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Информационная безопасность

Образовательная программа:

09.03.03 Прикладная информатика

Профиль подготовки:

Прикладная информатика в юриспруденции

Уровень высшего образования:
бакалавриат

Форма обучения:
очная

Статус дисциплины:
базовая

Махачкала
2020 год

Рабочая программа дисциплины «Информационная безопасность» составлена в 2020 г. в соответствии с требованиями ФГОС ВО по направлению 09.03.03 Прикладная информатика (уровень бакалавриата) от «19» сентября 2017 г. №922

Разработчик(и): кафедра «Информационного права и информатики»,
Рагимханова Динара Айдабековна, к.э.н., доцент
Магдилова Лариса Владимировна, к.э.н., доцент

Рабочая программа дисциплины одобрена:
на заседании кафедры от «19» 03 2020 г., протокол № 8
Зав. кафедрой ________________ Абдусаламов Р.А.
(подпись)
на заседании Методической комиссии юридического института от «25» 03 2020 г., протокол № 7.
Председатель ________________ Арсланбекова А.З.
(подпись)

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

Аннотация рабочей программы дисциплины

Дисциплина «**Информационная безопасность»** входит в базовую часть образовательной программы бакалавриата по направлению подготовки 09.03.03 Прикладная информатика.
Дисциплина реализуется в юридическом институте кафедрой информационного права и информатики.

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

Дисциплина нацелена на формирование следующих компетенций выпускника: общепрофессиональных - ОПК-3, ОПК-4.

Преподавание дисциплины предусматривает проведение следующих видов учебных занятий: лекции, практические занятия, лабораторные занятия и 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 3 зачетных единиц, в том числе в академических часах по видам учебных занятий

<table>
<tr><th rowspan="5">Семестр</th><th colspan="7">Учебные занятия</th><th rowspan="5">Форма промежуточной аттестации (зачет, дифференцированный зачет, экзамен</th></tr>
<tr><th colspan="7">в том числе</th></tr>
<tr><th colspan="6">Контактная работа обучающихся с преподавателем</th><th rowspan="3">СРС, в том числе экзамен</th></tr>
<tr><th rowspan="2">Всего</th><th colspan="5">из них</th></tr>
<tr><th>Лекции</th><th>Лабораторные занятия</th><th>Практические занятия</th><th>КСР</th><th>консультации</th></tr>
<tr><td>4</td><td>108</td><td>18</td><td></td><td>36</td><td></td><td></td><td>54</td><td>зачет</td></tr>
</table>

1. Цели освоения дисциплины

Целями освоения дисциплины «Информационная безопасность» являются:
- формирование у обучаемых знаний в области теоретических основ информационной безопасности;
- ознакомление студентов с современными системами информационной безопасности, методами и средствами защиты информации, организационными и правовыми мерами по информационной защите.

2.Место дисциплины в структуре ОПОП бакалавриата

Дисциплина входит в базовую часть по направлению 09.03.03 «Прикладная информатика» и изучается в шестом семестре.

Дисциплина логически и содержательно-методически связана с

- Информационным правом, представляющих систему знаний о признаках и юридических свойствах информации, методах и принципах правового регулирования общественных отношений в информационной сфере.
- Правовыми основами прикладной информатики, вырабатывающие основные навыки осуществления информационных процессов на основе современных программно-технических средств, с учетом безопасного удовлетворения информационных потребностей личности, общества и государства

Для изучения дисциплины «Информационная безопасность» обучающийся априори должен иметь знания об объектах, предметах, принципах, методах, способах правового регулирования, основных информационных правах и свободах, полученные в ходе изучения курса «Теории государства и права», «Конституционного права», а также знать основные направления государственной информационной политики, виды информационных процессов, иметь навыки по работе со справочно-правовыми системами, упрощающими работу с нормативно-правовой информацией, базирующиеся на дисциплинах «Информационные системы и сети» и «Информационное право».

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)
ОПК-3	Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	**Знать:** принципы, методы и средства решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности. . **Уметь:** решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности. **Владеть:** навыками подготовки обзоров, аннотаций, составления рефератов, научных докладов, публикаций, и библиографии по научно-исследовательской работе с учетом требований информационной безопасности.
ОПК- 4	Способен участвовать в разработке стандартов, норм и правил, а также технической документации, связанной с профессиональной деятельностью	**Знать:** основные стандарты оформления технической документации на различных стадиях жизненного цикла информационной системы. **Уметь:** применять стандарты оформления технической документации на различных стадиях жизненного цикла информационной системы **Владеть:** навыками поиска, получения, хранения, переработки и защиты информации, в том числе государственной, служебной, профессиональной и иных видов тайн; навыками защиты персональных данных; навыками сбора и обработки информации; навыками анализа информации; навыками обработки информации.

4. Объем, структура и содержание дисциплины

4.1. Объем дисциплины составляет 3 зачетных единиц, 108 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. Основные положения теории информационной безопасности								
1	Основные понятия курса «Информационная безопасность»	6		2	6			10	Контрольный опрос
2	Правовое обеспечение информационной безопасности	6		4	6			8	Контрольный опрос, тестирование, лабораторное задание
	Итого по модулю 1:			6	12			18	36
	Модуль 2. Правовые режимы обеспечения безопасности информации ограниченного доступа								
3	Организационное обеспечение информационной безопасности	6		4	6			8	Выполнение контрольных практических заданий, лабораторное задание, тестирование. Письменный опрос по теоретическому материалу.
4	Правовые режимы конфиденциальной информации	6		2	6			10	Контрольный опрос, лабораторное задание
	Итого по модулю 2:			6	12			18	36
	Модуль 3. Механизмы обеспечения защиты информации и ответственность в информационной сфере								
5	Преступления в сфере компьютерной информации	6		4	6			8	Выполнение контрольных практических заданий, лабораторное задание, тестирование. Письменный опрос по теоретическому материалу.
6	Защита информации в информационных системах	6		2	6			10	Контрольный опрос, тестирование, лабораторное задание, рефераты с презентацией
	Итого по модулю 3:			6	12			18	36
	Промежуточный контроль								зачет

	ИТОГО:			18	36			54	

4.3. Содержание дисциплины, структурированное по темам (разделам)

Модуль 1. Основные положения теории информационной безопасности

Тема 1. **Основные понятия курса «Информационная безопасность»**

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

Понятие и структура информационной безопасности. Субъекты и объекты правоотношений в области информационной безопасности. Понятия и виды защищаемой информации по российскому законодательству. Субъекты и средства, представляющие угрозу для ИБ. Субъекты и средства, осуществляющие защиту информации.

Составляющие информационной безопасности: доступность информации, целостность информации, конфиденциальность информации.

Тема 2. Правовые основы обеспечения информационной безопасности

Принципы, задачи, функции и стандарты обеспечения информационной безопасности. Законодательство в сфере обеспечения информационной безопасности и его место в системе российского законодательства. Основы нормативно-правовой защиты информации. Основные нормативные документы РФ по защите информации. Доктрина информационной безопасности РФ.

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

Модуль 2. Правовые режимы обеспечения безопасности информации ограниченного доступа

Тема 3. Организационное обеспечение информационной безопасности

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

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

Тема 4. Правовые режимы конфиденциальной информации

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

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

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

Модуль 2. Механизмы обеспечения защиты информации и ответственность в информационной сфере

Тема 5. Преступления в сфере компьютерной информации

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

Расследование компьютерного преступления. Законодательство РФ о компьютерных преступлениях.
Случайные, преднамеренные воздействия. Хищение носителей информации, чтение информации с экрана, чтение информации из распечатки, перехват паролей, расшифровка зашифрованной информации, копирование информации с носителя, подключение специально разработанных аппаратных средств, обеспечивающих доступ к информации, перехват побочных электромагнитных излучений от аппаратуры, линий связи, сетей электропитания и т. д. Вирусы как угроза информационной безопасности Классификация компьютерных вирусов.

Тема 6. Защита информации в информационных системах

Основные принципы организации процесса защиты информации в информационных системах. Угрозы информационной безопасности. Средства защиты информации. Ответственность за правонарушения в сфере информационной безопасности.

Тематика лабораторных занятий

1. Защита данных в текстовом редакторе.
2. Защита данных в табличном процессоре.
3. Защита данных в СУБД.
   - Анализ рисков ИБ
   - Проверка компьютера на предмет наличия уязвимостей
   - Исследование угроз доступности
   - Процедура аутентификации пользователя на основе пароля
   - Программная реализация криптографических алгоритмов
   - Механизм контроля целостности данных
   - Использование антивирусных программ
   - Защита и восстановление данных на компьютере, используя систему архивации

Семинарские занятия

Тема 1. **Основные понятия курса «Информационная безопасность»**

Вопросы для обсуждения:

1. Информационной сфера и ее элементы.
2. Понятие безопасности и защиты информации.
3. Понятие и структура информационной безопасности.
4. Принципы обеспечения информационной безопасности.

Тема 2. Правовые основы обеспечения информационной безопасности

Вопросы для обсуждения:

1. Доктрина информационной безопасности РФ об основных угрозах в информационной сфере и их источниках.
2. Угрозы нарушения конфиденциальности, целостности, доступности информации.
3. Ответственность за правонарушения в информационной сфере.

Тема 3. Организационное обеспечение информационной безопасности

Вопросы для обсуждения:

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

Модуль 2. Механизмы обеспечения защиты информации и ответственность в информационной сфере

Тема 4. Правовые режимы конфиденциальной информации

Вопросы для обсуждения:

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

Тема 5. Преступления в сфере компьютерной информации

Вопросы для обсуждения:
1. Понятие и виды компьютерных преступлений.
2. Особенности квалификации компьютерных преступлений.
3. Преступления имущественного характера, которые совершаются с применением или в отношении средств компьютерной техники.

Тема 6. Защита информации в информационных системах

Вопросы для обсуждения:
1. Понятие и виды угроз в информационных системах.
2. Средства и методы защиты информации в информационных системах.

5. Образовательные технологии

В соответствии с требованиями Федерального государственного образовательного стандарта высшего образования 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 интерактивных формах, определяется главной целью программы, особенностью контингента обучающихся и содержанием конкретных дисциплин, и в целом в учебном процессе они должны составлять не менее 20% аудиторных занятий.

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

В ходе освоения учебного курса «Информационная безопасность» при проведении аудиторных занятий используются следующие образовательные технологии: лекции, семинарские занятия с использованием активных и интерактивных форм проведения занятий, моделирование и разбор деловых ситуаций, использование тестовых заданий и задач на практических занятиях.

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

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

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

Промежуточные аттестации проводятся в форме контрольной работы и модульного тестирования.

6. Учебно-методическое обеспечение самостоятельной работы студентов.

Самостоятельные формы учебной работы студента юридического института имеют своей целью приобретение им системы знаний по дисциплине «Информационная безопасность». Используя лекционный материал, доступный учебник или учебное пособие, дополнительную литературу, проявляя творческий подход, студент готовится к практическим и лабораторным 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.

Нелишне иметь в виду и то, что каждый учебник или учебное пособие имеет свою логику построения, которая, естественно, не совпадает с логикой данной программы учебного курса. Одни авторы более широко, а другие более узко рассматривают ту или иную проблему. Учебник или учебное пособие целесообразно изучать последовательно, главу за главой, как это сделано в них. При этом, обращаясь к программе учебного курса, следует постоянно отмечать, какие ее вопросы (пусть в иной логической последовательности) рассмотрены в данной главе учебника, учебного пособия, а какие опущены. По завершении работы над учебником у Вас должна быть ясность в том, какие темы, вопросы программы учебного курса Вы уже изучили, а какие предстоит изучить по другим источникам.

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 (до 3000 слов), посвященное какой-либо значимой проблеме информационного права. 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 обеспечения судебной деятельности, в том числе обработанные результаты социологического опроса по заранее составленной анкете, видео-интервью, презентация по проблеме и др.

Основными видами самостоятельной работы студентов являются:

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

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

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

Нормативно-правовые акты

1. Конституция Российской Федерации: 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 A (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 информации, информационных технологиях и о защите информации: Федеральный закон от 27 июля 2006 г. № 149 – ФЗ // СЗ РФ. – 2006. - №31 (1ч.). – Ст. 3448.
23. 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.
24. 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.
25. 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.
26. Об обеспечении доступа к информации о деятельности судов в Российской Федерации: Федеральный закон от 22.12.2008 № 262 – ФЗ (ред. от 28.06.2010) //Парламентская газета. — 2008. — № 90.
27. Об электронной подписи: Федеральный закон от 6 апреля 2011 г. № 10 // Собрание законодательства РФ, 11.04.2011, N 15, ст. 2036.
28. 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.

29. 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.
30. 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.
31. Республиканская целевая программа «Развитие электронного правительства Республики Дагестан до 2017 года»: Постановление Правительства Республики Дагестан от 12.09.2013 года №432.
32. 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.
33. Уголовно–процессуальный кодекс Российской Федерации //Российская газета. — 2001. — № 249.
34. 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. Угрозы информационной безопасности РФ.
2. Информационно-психологическое оружие.
3. Информационно-психологическая война.
4. Защита информационных ресурсов от несанкционированного доступа.
5. Информационный терроризм.
6. Международное сотрудничество РФ в области защиты информации.
7. Государственная тайна.
8. Служебная тайна.
9. Коммерческая тайна.
10. Персональные данные.
11. Личная тайна.
12. Семейная тайна.
13. Тайна ЗАГСа.
14. Врачебная (медицинская) тайна.
18. Тайна вероисповедания.
19. Тайна исповеди.
20. Адвокатская тайна.
21. Тайна следствия.
22. Судебная тайна.
23. Тайна нотариата.
24. Налоговая тайна.
25. Банковская тайна.
26. Журналистская тайна (тайна СМИ).
27. Авторское право.

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
ОПК-3	**Знать:** принципы, методы и средства решения стандартных задач	Устный опрос, письменный опрос, реферат

	профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности. . **Уметь:** решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности. **Владеть:** навыками подготовки обзоров, аннотаций, составления рефератов, научных докладов, публикаций, и библиографии по научно- исследовательской работе с учетом требований информационной безопасности.	
ОПК4	**Знать:** основные стандарты оформления технической документации на различных стадиях жизненного цикла информационной системы. **Уметь:** применять стандарты оформления технической документации на различных стадиях жизненного цикла информационной системы **Владеть:** навыками поиска, получения, хранения, переработки и защиты информации, в том числе государственной, служебной, профессиональной и иных видов тайн; навыками защиты персональных данных; навыками сбора и обработки информации; навыками анализа информации; навыками обработки информации.	Устный опрос, разбор практических ситуаций

7.2 Типовые контрольные задания

Примерные тестовые задания для проведения текущего и промежуточного контроля

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

2. 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

3. 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
4. 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
5. 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
6. 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
7. 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
8. 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
9. 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.)
10. 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
11. 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
12. 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.)
13. 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
14. Основными мотивами при совершении компьютерных преступлений являются
- корыстные, политические, исследовательский интерес, хулиганство и озорство, месть

- корыстные, политические

- хулиганство и озорство

-месть

15. Основными опасными субъектами неправомерного доступа к компьютерной информации являются
- все верны

- хакеры-исследователи, хакеры взломщики, хакеры-вандалы

- крэкеры, компьютерные пираты, кибертеррористы

- вирмейкеры, кардеры, фрикеры

16. 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
17. 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
18. 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
19. 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
20. 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
21. 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
22. 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
23. Кардеры – люди
- специализирующиеся на изучении особенностей кредитных карт и банкоматов
- специализирующиеся на изучении особенностей незаконного подключения к линиям связи
- которые занимаются написанием компьютерных вирусов
24. 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
25. По типу возникновения угрозы безопасности информации принято делить на
- случайные и умышленные
- активные и пассивные
- регламентированные и нерегламентированные
- уголовные и административные
26. 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

27. 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
28. 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)

Вопросы к зачету

1. Понятие безопасности и защиты информации.

2. Понятие политики безопасности информационных систем. Назначение политики безопасности.
3. Основные типы политики безопасности доступа к данным.
4. Законодательный уровень обеспечения информационной безопасности. Основные законодательные акты РФ в области защиты информации.
5. Функции и назначение стандартов информационной безопасности.
6. Основные положения «Доктрины информационной безопасности РФ».
7. Административный уровень защиты информации. Задачи различных уровней управления в решении задачи обеспечения информационной безопасности.
8. Процедурный уровень обеспечения безопасности. Авторизация пользователей в информационной системе.
9. Идентификация и аутентификация при входе в информационную систему. Использование парольных схем. Недостатки парольных схем.
10. Биометрические средства идентификации и аутентификации пользователей.
11. Понятие электронной цифровой подписи. Процедуры формирования цифровой подписи.
12. Законодательный уровень применения цифровой подписи.
13. Информационная сфера и ее элементы.
14. Понятие безопасности и информационной безопасности.
15. Основные составляющие информационной безопасности.
16. Субъекты и объекты правоотношений в области информационной безопасности.
17. Концептуальные положения организационного обеспечения информационной безопасности.
18. Понятие и виды угроз безопасности.
19. Угрозы информационной безопасности на объекте.
20. Организация службы безопасности объекта
21. Правовой режим информации: понятие, признаки, содержание.
22. Виды информации ограниченного доступа.
23. Требования, предъявляемые к организации защиты конфиденциальной информации.
24. Виды компьютерных преступлений.
25. Особенности квалификации компьютерных преступлений.
26. Преступления имущественного характера, которые совершаются с применением или в отношении средств компьютерной техники.
27. Компьютерные вирусы
28. Угрозы нарушения конфиденциальности, целостности, доступности информации.
29. Основные причины утечки информации.

30. Режим, правовой режим, правовой режим информации: определение.
31. Понятие правового режима информации и его основные признаки.
32. Понятие правового режима информации и его типовые элементы.
33. Характеристика видов правового режима информации с точки зрения его обязательности и объекта.
34. Общий правовой режим информации.
35. Специальные правовые режимы информации.
36. Тайна как специальный правовой режим.
37. Конфиденциальность как специальный правовой режим.
38. Государственная тайна и ее защита.
39. Защита персональных данных.
40. Защита коммерческой тайны.
41. Профессиональная тайна.
42. Служебная тайна.
43. Виды информационного законодательства, применяемые для регулирования отношений в Интернет.
44. Угроза безопасности, обеспечение безопасности: понятие.
45. Информационная безопасность: понятие, первоочередные меры по обеспечению, общие методы.
46. Информационная безопасность и информационные войны: понятие.
47. Информационная безопасность и информационное оружие: понятие.
48. Правонарушение и информационное правонарушение: определение, признаки, юридическая ответственность и основание привлечения к ответственности.

49. Состав информационного правонарушения.
50. Уголовная ответственность за информационное преступление.
51. Административная и гражданско-правовая ответственность в информационной сфере.

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

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

Текущий контроль по дисциплине включает:

- участие на практических занятиях -30 баллов,
- выполнение домашних заданий – 10 баллов,
- выполнение аудиторных контрольных работ - 20 баллов.

Промежуточный контроль по дисциплине включает:

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

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

Основная литература

1. Мельников В. П., Клейменов С.А., Петраков А.М. Информационная безопасность и защита информации : учеб. пособие для студентов вузов. - 2е изд.,стер. - Москва : Academia, 2011.
2. Информационная безопасность : учеб. пособие / С. В. Петров. - Новосибирск: М. : АРТА, 2012.
3. Казанцев С.Я и др. Правовое обеспечение информационной безопасности : учеб. пособие для студентов вузов. - 3-е изд.,стер. -Москва : Academia, 2008.
4. Городов О.А. Информационное право [Электронный ресурс]: учебник для бакалавров. – М.: Издательство Проспект, 2016. – 303 с. – URL: http://нэб.рф/catalog/000199_000009_008578609/ - ЭБС «НЭБ».
5. Ковалева Н.Н. Информационное право России (2-е издание) [Электронный ресурс]: учебное пособие/ Ковалева Н.Н.— М.: Дашков и К, Ай Пи Эр Медиа, 2016.— 352 с.— URL: http://www.iprbookshop.ru/57155.html.— ЭБС «IPRbooks».
6. Организационное и правовое обеспечение информационной безопасности: учебник и практикум для бакалавриата и магистратуры / Т. А. Полякова, А. А. Стрельцов, С. Г. Чубукова, В. А. Ниесов ; под ред. Т. А. Поляковой, А. А. Стрельцова. — М. : Издательство Юрайт, 2017. — 325 с. — (Серия : Бакалавр и магистр. Академический курс).

в) дополнительная литература:

1. Бачило, И. Л. Информационное право: учебник для академического бакалавриата / И. Л. Бачило. — 5-е изд., перераб. и доп. — М.: Издательство Юрайт, 2017. — 419 с.
2. Ефимова Л.Л. Информационное право. Учебное пособие. Москва, 2011.
3. Килясханов И.Ш. Информационное право в терминах и понятиях: учебное пособие для студентов вузов, обучающихся по специальности 030501 «Юриспруденция»/ Килясханов И.Ш., Саранчук Ю.М.— М.: ЮНИТИ-ДАНА, 2015.— 135 с.
4. Кириленко В.П., Алексеев Г.В. Международное право и информационная безопасность государств. Монография – Санкт-Петербург, 2016.
5. 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.
6. Лапина М.А., Ревин А.Г., Лапин В.И., Килясханов И.Ш. Информационное право. Учебное пособие. –Москва, 2012.
7. Ловцов Д.А. Системология правового регулирования информационных отношений в инфосфере: монография/ Ловцов Д.А.— М.: Российский государственный университет правосудия, 2016.
8. 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 c.

9. 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 c.
10. 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 c.
11. 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).
12. Рассолов, И. М. Информационное право: учебник и практикум для академического бакалавриата / И. М. Рассолов. — 5-е изд., перераб. и доп. — М.: Издательство Юрайт, 2017. — 347 с.
13. Рогозин В.Ю. Информационное право: учебное пособие для студентов вузов, обучающихся по направлению подготовки «Юриспруденция»/ Рогозин В.Ю., Вепрев С.Б., Остроушко А.В.— М.: ЮНИТИ-ДАНА, 2017.
14. Смирнов А.А. Обеспечение информационной безопасности в условиях виртуализации общества. Опыт Европейского Союза [Электронный ресурс]: монография/ Смирнов А.А.— М.: ЮНИТИ-ДАНА, 2015.— 159 c.— URL: http://www.iprbookshop.ru/52524.html.— ЭБС «IPRbooks».
15. Смоленский М.Б. Информационное право: учебник/ Смоленский М.Б., Алексеева М.В.— Ростов-на-Дону: Феникс, 2015.— 223 c.
16. Смоленский М.Б., Алексеева М.В. Информационное право. Учебник / М.Б. Смоленский, М.В. Алексеева. Ростов-на-Дону, 2015. Сер. Высшее образование

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

1. Рагимханова Д.А. Электронный курс лекций по Информационной безопасности. Moodle [Электронный ресурс]: система виртуального обучением: [база данных] / Даг. гос. ун-т. – Махачкала, 2018 г. – Доступ из сети ДГУ или после регистрации из сети ун-та, из любой точки, имеющей доступ в интернет. – URL: http://moodle.dgu.ru/.
2. Рагимханова Д.А.. Электронный курс лекций по Информационному праву. Moodle [Электронный ресурс]: система виртуального обучением: [база данных] / Даг. гос. ун-т. – Махачкала, 2018 г. – Доступ из сети ДГУ или после регистрации из сети ун-та, из любой точки, имеющей доступ в интернет. – URL: http://moodle.dgu.ru/.
3. eLIBRARY.RU[Электронный ресурс]: электронная библиотека / Науч. электрон. б-ка. — Москва, 1999 – Режим доступа: http://elibrary.ru/defaultx.asp . – Яз. рус., англ.
4. Образовательный блог по Информационным технологиям в юридической деятельности [Электронный ресурс]: (ragimhanova.blogspot.ru)
5. Образовательный блог по направлению магистратуры «Актуальные проблемы информационного права» [Электронный ресурс]: (ragimhanovamag.blogspot.ru)
6. Федеральный портал «Российское образование» http://www.edu.ru/
7. Федеральное хранилище «Единая коллекция цифровых образовательных ресурсов» http://school-collection.edu.ru/
8. Российский портал «Открытое образование» http://www.openet.edu.ru
9. Сайт образовательных ресурсов Даггосуниверситета http://edu.dgu.ru
10. Информационные ресурсы научной библиотеки Даггосуниверситета http://elib.dgu.ru.
11. Открытая электронная библиотека http: www.diss.rsl.ru.
12. СПС «Гарант» http: www.garant.ru.
13. СПС «Консультант плюс» http: www.tls-cons.ru.
14. СПС «Право» http: www.pravo.ru.
15. Государственная автоматизированная система «Правосудие» - http://www.sudrf.ru/index.php?id=300
16. Научная библиотека Дагестанского государственного университета - http://www.elib.dgu.ru/
17. Официальный сайт открытого правительства РФ - http://openstandard.ru/ rating_2015.html

18. Портал государственных программ РФ - http://programs.gov.ru/Portal/programs/list
19. Портал государственных услуг РФ - http://www.gosuslugi.ru/
20. Портал открытых данных РФ - http://data.gov.ru/
21. Собрание законодательства РФ на портале Государственной системы правовой информации - http://pravo.gov.ru/proxy/ips/?editions
22. Судебная практика – www.sud-praktika.narod.ru
23. Правительство РФ правительство.рф
24. Сервер органов государственной власти РФ www.gov.ru
25. 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 «Информационная безопасность» предполагает изложение теоретического курса на лекционных занятиях и приобретение практических навыков в процессе решения поставленных задач, возникающих при регулировании информационно-правовых отношений и выполнению лабораторных работ. 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 шести 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 и лабораторному 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 и лабораторных 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 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.