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

Преступления в сфере информационных технологий

Кафедра информационного права и информатики юридического института

Образовательная программа
09.03.03 Прикладная информатика

Профили подготовки
Прикладная информатика в юриспруденции

Уровень высшего образования
бакалавриат

Форма обучения
очная

Статус дисциплины: **входит в часть, формируемую участниками образовательных отношений (дисциплины по выбору)**

Махачкала 2022 год

Рабочая программа дисциплины «Преступления в сфере информационных технологий» составлена в 2022 году в соответствии с требованиями ФГОС ВО-бакалавриат по направлению подготовки 09.03.03 Прикладная информатика от 19.09.2017 N917

Разработчик(и): кафедра информационного права и информатики,
Рагимханова Камилла Тагировна, ст. преп.

Рабочая программа дисциплины одобрена:
на заседании кафедры информационного права и информатики
от «__» _____2022 г., протокол № __

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

на заседании Методической комиссии юридического института
от «___» _____2022 г., протокол №___.

Председатель _____ Арсланбекова А.З.
(подпись)

Рабочая программа дисциплины согласована с учебно-методическим управлением «____» _____2022 г.

Начальник УМУ _____ Гасангаджиева А.Г.
(подпись)

Аннотация рабочей программы дисциплины

Дисциплина «**Преступления в сфере информационных технологий**» входит в часть, формируемую участниками образовательных отношений (дисциплины по выбору) 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 уголовно-правовой и криминалистической характеристикой преступлений в сфере информационных технологий, анализируются особенности расследования данных составов, актуальные задачи в области профилактики противоправных действий в данной сфере общественных отношений.
Дисциплина нацелена на формирование следующих компетенций выпускника: универсальных – УК-1; общепрофессиональных- ОПК-1; профессиональных- ПК-6, ПК-7, ПК-11, ПК-12.

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 3 зачетных единиц, в том числе в академических часах по видам учебных занятий
Очная форма обучения

Семестр	Учебные занятия								Форма промежуточной аттестации (зачет, дифференцированный зачет, экзамен)
	в том числе:								
	всего	Контактная работа обучающихся с преподавателем						СРС, в том числе зачет, дифференцированный зачет, экзамен	
		всего	из них						
			Лекции	Лабораторные занятия	Практические занятия	…	..		
8	108		16		16			76	Зачет

1. Цели освоения дисциплины

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

- формирование и развитие у будущих юристов теоретических знаний и практических навыков в раскрытии преступлений в сфере информационных технологий;
- ознакомление студентов 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 вариативную часть в блок дисциплин по выбору и изучается в восьмом семестре.

Дисциплина входит в часть, формируемую участниками образовательных отношений в блок дисциплин по выбору изучается в восьмом семестре.

Дисциплина логически 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) уголовным правом, определяющим совокупность юридических норм, которые определяют преступность и наказуемость деяний. Уголовное право вооружает специалистов-юристов знаниями, умениями и навыками применения норм уголовного права в реальной действительности.

в) информатикой, вырабатывающей основные навыки осуществления информационных процессов на основе современных программно-технических средств, с учетом безопасного удовлетворения информационных потребностей личности, общества и государства;

г) информационным правом, представляющих систему знаний о признаках и юридических свойствах информации, методах и принципах правового регулирования общественных отношений в информационной сфере.

Для изучения дисциплины «Преступления в сфере информационных технологий» обучающийся априори должен иметь знания о понятии и значении квалификации преступлений, полученные в ходе изучения курса «Теории государства и права», «Уголовное право», а также знать основные направления государственной информационной политики, виды информационных процессов, базирующиеся на дисциплинах «Информационные системы и сети» и «Информационное право».

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

Код и наименование универсальной	Код и наименование индикатора достижения универсальной	Планируемые результаты обучения	Процедура освоение

компетенции выпускника	компетенции выпускника		
УК-1. Способен осуществлять поиск, критический анализ и синтез информации, применять системный подход для решения поставленных задач	УК-1.1. Знает принципы сбора, отбора и обобщения информации, методики системного подхода для решения профессиональных задач.	Знает принципы сбора, отбора и обобщения информации, методики системного подхода для решения профессиональных задач.	Устный опрос
	УК-1.2. Умеет анализировать и систематизировать разнородные данные, оценивать эффективность процедур анализа проблем и принятия решений в профессиональной деятельности	Умеет анализировать и систематизировать разнородные данные, оценивать эффективность процедур анализа проблем и принятия решений в профессиональной деятельности.	Письменное задание
	УК-1.3. Владеет навыками научного поиска и практической работы с информационными источниками; методами принятия решений.	Владеет навыками научного поиска и практической работы с информационными источниками; методами принятия решений.	Контрольный опрос
ОПК-1. Способен применять естественнонаучные и общеинженерные знания, методы математического анализа и моделирования, теоретического и экспериментального исследования в профессиональной деятельности.	ОПК-1.1. Знает основы математики, физики, вычислительной техники и программирования.	. Знает основы математики, физики, вычислительной техники и программирования.	Устный опрос
	ОПК-1.2. Умеет решать стандартные профессиональные задачи с применением естественнонаучных и общеинженерных знаний, методов математического анализа и моделирования.	Умеет решать стандартные профессиональные задачи с применением естественнонаучных и общеинженерных знаний, методов математического анализа и моделирования.	Письменное задание
	ОПК-1.3. Владеет навыками теоретического и экспериментального исследования объектов профессиональной деятельности.	Владеет навыками теоретического и экспериментального исследования объектов профессиональной деятельности.	Контрольный опрос
ПК-6. Способность программировать приложения и создавать программные прототипы решения прикладных задач.	Знать: проблемы и процессы анализа предметной области программных решений современные подходы анализа предметной области программных решений. Уметь: разрабатывать программные приложения для предметной области. Владеть: практическими навыками использования языков программирования	Знать: проблемы и процессы анализа предметной области программных решений современные подходы анализа предметной области программных решений. Уметь: разрабатывать программные приложения для предметной области. Владеть: практическими навыками использования языков программирования	Контрольный опрос

	для создания программные прототипов решения прикладных задач	для создания программные прототипов решения прикладных задач	
ПК-7. Способность принимать участие в организации ИТ инфраструктуры и управлении информационной безопасностью.	Знать: методы информационной безопасности. Уметь: обеспечивать информационную безопасность ИТ-инфраструктуры правовых подсистем. Владеть: навыками организации ИТ-инфраструктуры, характеризующейся высокой степенью информационной безопасности.	Знать: методы информационной безопасности. Уметь: обеспечивать информационную безопасность ИТ-инфраструктуры правовых подсистем. Владеть: навыками организации ИТ-инфраструктуры, характеризующейся высокой степенью информационной безопасности.	Устный опрос
ПК-11. Способность применять системный подход и математические методы в формализации решения прикладных задач	Знать: принципы системного подхода и математические методы в формализации решения прикладных задач, в обосновании правильности выбранной модели информационных процессов и систем; Уметь: применять системный подход и математические методы в формализации решения прикладных задач; Владеть: методами построения математической модели профессиональных задач и содержательной интерпретации полученных результатов, навыками разработки информационно-логической, функциональной и объектноориентированной модели информационной системы, модели данных информационных систем.	Знать: принципы системного подхода и математические методы в формализации решения прикладных задач, в обосновании правильности выбранной модели информационных процессов и систем; Уметь: применять системный подход и математические методы в формализации решения прикладных задач; Владеть: методами построения математической модели профессиональных задач и содержательной интерпретации полученных результатов, навыками разработки информационно-логической, функциональной и объектноориентированной модели информационной системы, модели данных информационных систем.	
ПК-12. Способность готовить обзоры научной литературы и электронных информационно-образовательных ресурсов для	Знать: принципы сбора, анализа научно-технической информации, отечественного и зарубежного опыта по тематике исследования; основные электронные информационнообразовательные ресурсы;	Знать: принципы сбора, анализа научно-технической информации, отечественного и зарубежного опыта по тематике исследования; основные электронные информационнообразовательные ресурсы;	

профессиональной деятельности	Уметь: готовить обзоры научной литературы и электронных информационно-образовательных ресурсов для профессиональной деятельности; Владеть: навыками подготовки обзоров научной литературы и электронных информационнообразовательных ресурсов для профессиональной деятельности.	Уметь: готовить обзоры научной литературы и электронных информационно-образовательных ресурсов для профессиональной деятельности; Владеть: навыками подготовки обзоров научной литературы и электронных информационнообразовательных ресурсов для профессиональной деятельности.	

4. Объем, структура и содержание дисциплины

4.1. Объем дисциплины составляет 3 зачетных единиц, 108 академических часов.

4.2. Структура дисциплины.

4.2.1. Структура дисциплины в очной форме

№ 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.		
	Модуль1.Общая характеристика преступлений в сфере информационных технологий и компьютерной информации								
1	Понятие и признаки преступления	8		2	2			14	Контрольный опрос
2	Уголовно-правовая характеристика преступлений в сфере информационных технологий	8		2	2			14	Контрольный опрос, тестирование
	Итого по модулю 1:			4	4			28	36
	Модуль 2. Анализ составов преступлений в сфере информационных технологий								
3	Компьютерные преступления в сфере информационных технологий.	8		4	4			28	Контрольный опрос
	Итого по модулю 2:			4	4			28	36
	Модуль 3. Вопросы квалификации преступлений в сфере компьютерной								

	информации								
4	Соотношение составов преступлений в сфере компьютерной информации со смежными и иными составами преступлений	8		8	8			20	Выполнение контрольных практических заданий, тестирование. Письменный опрос по теоретическому материалу.
	Итого по модулю 3:			8	8			20	36
	Промежуточный контроль								зачет
	ИТОГО:			16	16			76	

4.3. Содержание дисциплины, структурированное по темам (разделам)

Модуль 1. Общая характеристика преступлений в сфере информационных технологий и компьютерной информации

Тема 1. Понятие и признаки преступления

Развитие понятия преступления в теории права и уголовном законодательстве. Материально-формальное определение преступления по действующему уголовному законодательству.

Признаки преступления. Содержание и сущность признака общественной опасности. Уголовная противоправность, значение этого признака для установления режима законности. Виновность. Наказуемость. Единство признаков преступления.

Преступление и другие правонарушения. Характер общественной опасности и вид противоправности как критерии отграничения преступлений от других правонарушений. Основные теоретические взгляды по вопросу отграничения преступлений от других видов правонарушений. Отличие преступлений от проступков.

Категории преступлений. Степень общественной опасности как критерий классификации преступлений. Виды преступлений: 1) преступления небольшой тяжести; 2) преступления средней тяжести; 3) тяжкие преступления; 4) особо тяжкие преступления.

Тема 2. Уголовно-правовая характеристика преступлений в сфере информационных технологий

Понятие и признаки преступлений в сфере информационных технологий. Причины и условия компьютерной преступности. Обстоятельства, способствующие совершению компьютерных преступлений. Факторы компьютерной преступности, относящиеся к информации, информационной среде и ее инфраструктуре.

Факторы, относящиеся к особенностям компьютерной преступности. Факторы компьютерной преступности, относящиеся к личности, обществу и государству. Криминологическая характеристика преступности в сфере информационных технологий в России.

Модуль 2. Анализ составов преступлений в сфере информационных технологий

Тема3.Компьютерные преступления в сфере информационных технологий.

Объективная сторона состава преступления, предусмотренного ст. 272 УК РФ. Объект преступления. Доступ к информации. Уничтожение информации. Удаление информации. Модификация. Блокирование информации. Субъективная сторона преступления. Субъект преступления. Квалифицирующие признаки преступления. Крупный ущерб. Корыстная заинтересованность. Наступление тяжких последствий.

Объективная сторона состава преступления, предусмотренного ст. 273 УК РФ. Объект преступления. Компьютерная программа. Создание вредоносных программы или файла. Распространение программы или файла. Нейтрализация средств защиты информации. Субъективная сторона. Субъекты преступления. Квалифицирующие признаки преступления.

Объективная сторона состава преступления, предусмотренного ст. 274 УК РФ. Объект преступления. Средства хранения, обработки или передачи информации. Информационно-телекоммуникационная сеть. Оконечное оборудование.

Объективная сторона состава преступления, предусмотренного ст. 274.1 УК РФ. Объект преступления. Критическая информационная инфраструктура. Предмет преступления. Субъективная сторона. Субъекты преступления. Квалифицирующие признаки преступления.

Нарушение правил централизованного управления техническими средствами противодействия угрозам устойчивости, безопасности и целостности функционирования на территории Российской Федерации информационно-телекоммуникационной сети "Интернет" и сети связи общего пользования. Должностное лицо.

Модуль 3. Вопросы квалификации преступлений в сфере информационных технологий

Тема 4. Соотношение составов преступлений в сфере компьютерной информации со смежными и иными составами преступлений.

Преступления в сфере компьютерной информации (ст.ст. 272, 273 УК РФ) и преступления против половой неприкосновенности и половой свободы личности (ст.ст. 132, 135 УК РФ).

Преступления в сфере компьютерной информации (ст.ст. 272, 273 УК РФ) и нарушение тайны переписки, телефонных переговоров, почтовых, телеграфных или иных сообщений (ст. 138 УК РФ).

Неправомерный доступ к компьютерной информации (ст. 272 УК РФ) и нарушение авторских и смежных прав (ст. 146 УК РФ).

Преступления в сфере компьютерной информации (ст.ст. 272, 273 УК РФ) и преступления против собственности (ст.ст. 158, 159.6 УК РФ).

Неправомерный доступ к компьютерной информации (ст. 272 УК РФ) и причинение имущественного ущерба путем обмана или злоупотребления доверием без признаков хищения (ст. 165 УК РФ).

Неправомерный доступ к компьютерной информации (ст. 272 УК РФ) и незаконные получение и разглашение сведений, составляющих коммерческую, налоговую или банковскую тайну (ст. 183 УК РФ)

Семинарские занятия.

Модуль 1. Общая характеристика преступлений в сфере информационных технологий и компьютерной информации

Тема 1. Понятие и признаки преступления.

Вопросы для обсуждения

1. Определение понятия преступления.
2. Характеристика признаков преступления: общественная опасность, противоправность, виновность и наказуемость. Проблема материального либо формального определения понятия преступления.
3. Отличие преступления от иных правонарушений и его соотношение с ними (с дисциплинарными проступками, гражданско-правовыми деликтами и административными правонарушениями).
4. Классификация преступлений и ее значение. Группировка преступлений в Особенной части УК РФ по особенностям родового объекта преступления; разновидности преступлений по степени тяжести и общественной опасности, по формам вины и другим критериям. Категории преступлений и значение их определения в уголовном кодексе.

Тема 2. Уголовно-правовая характеристика преступлений в сфере информационных технологий

Вопросы для обсуждения:

1. Понятие и виды компьютерных преступлений.
2. Факторы компьютерных преступлений.
3. Криминологическая характеристика преступности в сфере информационных технологий в России.

Модуль 2. Анализ составов преступлений в сфере информационных технологий

Тема 3. Компьютерные преступления в сфере информационных технологий.

Вопросы для обсуждения:

1. Неправомерный доступ к охраняемой законом компьютерной информации.
2. Создание, использование и распространение вредоносных компьютерных программ.
3. Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей.
4. Нарушение правил централизованного управления техническими средствами противодействия угрозам устойчивости, безопасности и целостности функционирования на территории Российской Федерации информационно-телекоммуникационной сети "Интернет" и сети связи общего пользования.

Модуль 3. Вопросы квалификации преступлений в сфере информационных технологий

Тема 4. Соотношение составов преступлений в сфере компьютерной информации со смежными и иными составами преступлений.

Вопросы для обсуждения:

1. Преступления в сфере компьютерной информации (ст.ст. 272, 273 УК РФ) и преступления против половой неприкосновенности и половой свободы личности (ст.ст. 132, 135 УК РФ).
2. Преступления в сфере компьютерной информации (ст.ст. 272, 273 УК РФ) и нарушение тайны переписки, телефонных переговоров, почтовых, телеграфных или иных сообщений (ст. 138 УК РФ).
3. Неправомерный доступ к компьютерной информации (ст. 272 УК РФ) и нарушение авторских и смежных прав (ст. 146 УК РФ).
4. Преступления в сфере компьютерной информации (ст.ст. 272, 273 УК РФ) и преступления против собственности (ст.ст. 158, 159.6 УК РФ).
5. Неправомерный доступ к компьютерной информации (ст. 272 УК РФ) и причинение имущественного ущерба путем обмана или злоупотребления доверием без признаков хищения (ст. 165 УК РФ).
6. Неправомерный доступ к компьютерной информации (ст. 272 УК РФ) и незаконные получение и разглашение сведений, составляющих коммерческую, налоговую или банковскую тайну (ст. 183 УК РФ).

5. **Образовательные технологии**

В соответствии с требованиями Федерального государственного образовательного стандарта высшего образования по направлению подготовки 09.03.03 Прикладная информатика (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 «Преступления в сфере информационных технологий» при проведении аудиторных занятий используются следующие образовательные технологии: лекции, семинарские занятия с использованием активных и интерактивных форм проведения занятий, моделирование и разбор деловых ситуаций, использование тестовых заданий и задач на практических занятиях.

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

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

При организации самостоятельной работы занятий используются следующие образовательные технологии: индивидуальное и групповое консультирование, разбор конкретных ситуаций; тестирование; подготовка докладов, рефератов; 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 факультета имеют своей целью приобретение им системы знаний по дисциплине «Преступления в сфере информационных технологий». Используя лекционный материал, доступный учебник или учебное пособие, дополнительную литературу, проявляя творческий подход, студент готовится к практическим занятиям, рассматривая их как пополнение, углубление, систематизация своих теоретических знаний.

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

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-атериалов, 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

а) нормативно-правовые акты:

1. Конституция Российской Федерации. – М.: Юрид. лит., 1994.
2. Всеобщая декларация прав человека (принята на третьей сессии Генеральной Ассамблеи ООН резолюцией 217 А (III) от 10 декабря 1948 г.) // Российская газета. 10 декабря 1998г.
3. Международный пакт о гражданских и политических правах (Нью-Йорк, 19 декабря 1966г.) // Сборник действующих договоров, соглашений и конвенций, заключенных с иностранными государствами, М., 1978 г., вып. XXXII, с. 44.
4. Протокол N1 к Конвенции о защите прав человека и основных свобод ETS N 009 (Париж, 20 марта 1952г.) // Собрание законодательства Российской Федерации, 18 мая 1998г., N 0, ст. 2143.
5. Хартия Глобального информационного общества (Окинава) // Дипломатический вестник. - 2000. - №8.
6. О безопасности: Закон РФ от 5.03.92г. №2446-1 – 1 – ФЗ //Ведомости Съезда народных депутатов РФ и Верховного Совета РФ. – 1992. – №15. – Ст. 769.
7. О государственной тайне: Федеральный закон от 21 июля 1993г. № 5485 – 1 – ФЗ // СЗ РФ. – 1993. - №41. – Ст. 4673.

8. О коммерческой тайне: Федеральный закон от 29 июля 2004 г. N 98-ФЗ // СЗ РФ. 2004. N 32. Ст. 3283.
9. О персональных данных: Федеральный закон от 27 июля 2006 г. № 152 – ФЗ // СЗ РФ. – 2006. - №31 (1ч.). – Ст. 3451.
10. 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.
11. Об информации, информационных технологиях и о защите информации: Федеральный закон от 27 июля 2006 г. № 149 – ФЗ // СЗ РФ. – 2006. - №31 (1ч.). – Ст. 3448.
12. Об электронной подписи: Федеральный закон от 6 апреля 2011 г. № 10 // Собрание законодательства РФ, 11.04.2011, N 15, ст. 2036.
13. 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.
14. 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.
15. Об организации предоставления государственных и муниципальных услуг: Федеральный закон от 27 июля 2010 г. N 210 // Собрание законодательства РФ, 02.08.2010, N 31, ст. 4179.
16. 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.
17. 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.
18. 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.
19. Концепция региональной информатизации до 2010 года: Распоряжение Правительства Российской Федерации от 17 июля 2006 г. N 1024-р. //Собрание законодательства РФ, 24.07.2006, N 30, ст. 3419.
20. Концепция формирования в Российской Федерации электронного правительства до 2010 года: Распоряжение Правительства Российской Федерации от 6 мая 2008 г. N 632-р. //Собрание законодательства РФ, 19.05.2008, N 20, ст. 2372.
21. О государственной программе Российской Федерации «Информационное общество (2011 - 2020 годы): Распоряжение Правительства РФ от 20.10.2010 N 1815-р (ред. от 20.07.2013) //Собрание законодательства РФ, 15.11.2010, N 46, ст. 6026.

22. 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.
23. 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.
24. Об информационной системе поддержки оказания органами исполнительной власти Республики Дагестан и органами местного самоуправления государственных услуг с использованием электронных средств коммуникаций по принципу «одного окна»: Постановление Правительства Республики Дагестан от 20 июля 2009 г. N 242. //Собрание законодательства Республики Дагестан, 31.07.2009, N 14, ст. 712.
25. Республиканская целевая программа «Развитие электронного правительства Республики Дагестан до 2017 года»: Постановление Правительства Республики Дагестан от 12.09.2013 года №432.

7. Фонд оценочных средств для проведения текущего контроля успеваемости, промежуточной аттестации по итогам освоения дисциплины.7.1 **Типовые контрольные задания**

Примерная тематика рефератов

1. Понятие и сущность информации. Классификация информации. Юридические свойства и признаки информации.

2. Понятие и сущность преступлений в сфере информационных технологий.

3. Понятие, объекты и субъекты компьютерных преступлений.

4. Особенности квалификации преступлений в сфере информационных технологий.

5. Теоретические основы классификации преступлений в сфере информационных технологий. Обзор отечественного и международного опыта.

6. Виды компьютерных преступлений. Ответственность за правонарушения в информационной сфере.

7. Преступления в сфере телекоммуникаций.

8. Национальное законодательство о компьютерных правонарушениях и защите информации.

9. Особенности криминального использования компьютерной техники в экономической сфере и материальном производстве (подлог документированной информации фискальных систем; преступления в сфере безналичных расчетов; преступления в сети Интернет; применение полиграфических компьютерных технологий).

10. Неправомерный доступ к компьютерной информации.

11. Создание, использование и распространение вредоносных программ для ЭВМ. 12. Нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети.

13. Контроль над компьютерной преступностью в России.

14. Уголовно-правовой контроль над компьютерной преступностью в России.

15. Особенности оперативно-розыскной деятельности при расследовании преступлений в сфере информационных технологий.

16. Методика расследования преступлений в сфере информационных технологий. 17. Особенности тактики расследования преступлений в сфере информационных технологий.

18. Назначение компьютерно-технических экспертиз при расследовании преступлений в сфере информационных технологий. Опросы, выносимые на их разрешение.

19. Организационно-технические меры предупреждения компьютерных преступлений.

20. Правовые меры предупреждения компьютерных преступлений.

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

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

Текущий контроль по дисциплине включает:

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

Промежуточный контроль по дисциплине включает:

- письменная контрольная работа - 30 баллов,

- тестирование – 10 баллов.

Примерные тесты

1. Европейская Конвенция по борьбе с киберпреступностью принята Советом Европы:
а) 23 ноября 2001 г.;
б) 22 ноября 2010 г.;
в) 13 июля 2015 г.
2. Информация по ряду преступлений в сфере высоких технологий выступает в качестве:
а) предмета преступления;
б) состояния «плазменной среды»;
в) объекта преступления.
3. Первый законодательный акт, направленный на правовую охрану программ
для ЭВМ и баз данных, в России был принят:
а) 17 октября 1998 г.;
б) 23 сентября 1992 г.;
в) 22 июня 2001 г.
4. Причины преступности, как правило, классифицируются на:
а) частные и личностные;
б) судебно-медицинские и судебно-психиатрические;
в) экономические, социальные, политические и нравственно-психологические.
5. Международные преступления – это:
а) международные преступные деяния, совершаемые транснациональными преступными формированиями;
б) международные преступные деяния, посягающие на интересы отдельных политических и экономических организаций (ООН, БРИГС и т.д.);
в) преступные деяния, затрагивающие интересы всего мирового сообщества и
подлежащие юрисдикции Международного уголовного суда.
6. Преступления международного характера – это:
а) преступные деяния, касающиеся ряда отдельных государств и в рамках принципа двойной подсудности, подпадающие под регулятивное действие института выдачи (экстрадиции);
б) преступление, совершенное иностранным лицом или лицом без гражданства;
в) международное преступление, совершенное гражданином Российской Федерации.
7. Периодом зарождения компьютерной преступности в мире можносчитать:
а) 30-е годы прошлого века;
б) 50- е годы прошлого века;
в) 70-е годы прошлого века.

8. Киберпреступность - это:
а) преступление, совершенное с помощью компьютерной системы (сети);
б) преступление, совершенное в рамках компьютерной системы (сети);
в) любое преступление, которое может быть совершено в электронной среде.
9. Объектом компьютерных преступлений являются:
а) информационная безопасность и системы обработки информации с использованием ЭВМ;
б) информация и компьютерные сети;
в) информационные каналы связи между ЭВМ.
10. Предупреждение компьютерной преступности направлено на:
а) устранение фактора, способствовавшее совершению конкретного компьютерного преступления;
б) устранение или нейтрализацию причин и условий, способствующих совершению компьютерных преступлений;
в) создание условий для ликвидации компьютерной преступности.
11. Субъекты компьютерных преступлений могут быть квалифицированы как:
а) хакеры, шпионы, вандалы, террористы, корыстные преступники;
б) хакеры, хулиганы, разбойники;
в) хакеры, домушники, технари, лица, испытывающие компьютерные фобии.
12. Динамика компьютерных преступлений:
а) относительно стабильна;
б) характеризуется ростом;
в) имеет тенденцию к снижению.
13. К компьютерным преступлениям, в частности, относятся:
а) нарушение авторских и смежных прав, изобретательских и патентных прав;
б) самовольные установка или эксплуатация узла проводного вещания;
в) неправомерный доступ к компьютерной информации.
14. К административному проступку относится:
а) незаконная деятельность в области защиты информации;
б) создание, использование и распространение вредоносных программ для ЭВМ;
в) нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети.
15. Латентную преступность в сфере информационных технологий можно представить в виде:
а) не полно раскрытых и полно раскрытых преступлений;
б) ложной и истинной латентности;
в) естественной и искусственной латентности преступлений.
16. Как классифицируются компьютерные преступления по законодательству Российской Федерации:
а) преступления в сфере оборота компьютерной информации и телекоммуникаций;

б) преступления в сфере оборота компьютерной информации, в сфере телекоммуникаций; в сфере информационного оборудования; в сфере защиты охраняемой законом информации;
в) преступления в сфере оборота компьютерной информации и в сфере защиты
охраняемой законом информации.
17. Меры контроля над компьютерной преступностью классифицируются:
а) правовые и научно-технические;
б) правовые, научно-технические и организационные;
в) правовые, организационно-тактические и программно-технические.
18. Основной целью государственной политики по выявлению и пресечению компьютерных преступлений является:
а) создание эффективной национальной системы борьбы с правонарушениями
в сфере информационных технологий;
б) создание эффективной национальной системы профилактики и предупреждения компьютерных преступлений;
в) создание эффективной национальной системы контроля за компьютерными
преступлениями.
19. Снижение уровня латентности компьютерных преступлений предполагает:
а) расширение штатов сотрудников правоохранительных органов, ведущих борьбу с компьютерными преступлениями;
б) повышение финансирования соответствующих управлений (отделов) правоохранительных органов;
в) обеспечение неотвратимости ответственности лиц, совершивших компьютерные преступления.
20. Правовые методы борьбы с компьютерными преступлениями включает:
а) совершенствование уголовного законодательства в этой части;
б) совершенствование административного и уголовного законодательства об ответственности за компьютерные правонарушения;
в) совершенствование международного сотрудничества по борьбе с компьютерными преступлениями.

Примерные вопросы к зачету

1. Определение понятия преступления.
2. Характеристика признаков преступления: общественная опасность, противоправность, виновность и наказуемость. Проблема материального либо формального определения понятия преступления.
3. Отличие преступления от иных правонарушений и его соотношение с ними (с дисциплинарными проступками, гражданско-правовыми деликтами и административными правонарушениями).

4. Классификация преступлений и ее значение. Группировка преступлений в Особенной части УК РФ по особенностям родового объекта преступления; разновидности преступлений по степени тяжести и общественной опасности, по формам вины и другим критериям. Категории преступлений и значение их определения в уголовном кодексе.
5. Понятие и виды компьютерных преступлений.
6. Факторы компьютерных преступлений.
7. Криминологическая характеристика преступности в сфере информационных технологий в России.
8. Охарактеризуйте преступные деяния, предусмотренные главой 28 УК РФ «Преступления в сфере компьютерной информации».
9. Меры контроля над компьютерной преступностью в России
10. Меры уголовно-правового контроля над компьютерной преступностью в законодательстве России
11. Организационно-технические меры предупреждения компьютерных преступлений.
12. Направления в предупреждении компьютерных преступлений
13. Правовые меры предупреждения компьютерных преступлений?
14. Проведите анализ состава преступления, предусмотренного ст. 272 УК РФ – «Неправомерный доступ к компьютерной информации».
15. Проведите анализ состава преступления, предусмотренного ст. 273 УК РФ – Создание, использование и распространение вредоносных программ для ЭВМ».
16. Проведите анализ состава преступления, предусмотренного ст. 274 УКРФ – «Нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети».
17. Проведите анализ состава преступления, предусмотренного ст. 274.1 УК РФ – «Неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации».
18. Проведите анализ состава преступления, предусмотренного ст. 274.2 УК РФ – «Нарушение правил централизованного управления техническими средствами противодействия угрозам устойчивости, безопасности и целостности функционирования на территории Российской Федерации информационно-телекоммуникационной сети "Интернет" и сети связи общего пользования».
19. Преступления в сфере компьютерной информации (ст.ст. 272, 273 УК РФ) и преступления против половой неприкосновенности и половой свободы личности (ст.ст. 132, 135 УК РФ).
20. Преступления в сфере компьютерной информации (ст.ст. 272, 273 УК РФ) и нарушение тайны переписки, телефонных переговоров, почтовых, телеграфных или иных сообщений (ст. 138 УК РФ).
21. Неправомерный доступ к компьютерной информации (ст. 272 УК РФ) и нарушение авторских и смежных прав (ст. 146 УК РФ).

22. Преступления в сфере компьютерной информации (ст.ст. 272, 273 УК РФ) и преступления против собственности (ст.ст. 158, 159.6 УК РФ).
23. Неправомерный доступ к компьютерной информации (ст. 272 УК РФ) и причинение имущественного ущерба путем обмана или злоупотребления доверием без признаков хищения (ст. 165 УК РФ).
24. Неправомерный доступ к компьютерной информации (ст. 272 УК РФ) и незаконные получение и разглашение сведений, составляющих коммерческую, налоговую или банковскую тайну (ст. 183 УК РФ).

8. Учебно-методическое обеспечение дисциплины.

а) адрес сайта курса

1. http://distant.dgu.ru/viewTeacher/TeacherMain
2. https://ragimhanovakt.blogspot.com/p/blog-page_20.html
3. http://cathedra.dgu.ru/EducationalProcess_Umk.aspx?Value=11&id=71

б) основная литература

1. Информационное право : учебник для вузов / М. А. Федотов [и др.] ; под редакцией М. А. Федотова. — Москва : Издательство Юрайт, 2022. — 497 с. — (Высшее образование). — ISBN 978-5-534-10593-3. — URL : https://urait.ru/bcode/489946
2. Информационное право : учебник для вузов / Н. Н. Ковалева [и др.] ; под редакцией Н. Н. Ковалевой. — Москва : Издательство Юрайт, 2022. — 353 с. — (Высшее образование). — ISBN 978-5-534-13786-6. — URL : https://urait.ru/bcode/496717
3. Рассолов, И. М. Информационное право : учебник и практикум для вузов / И. М. Рассолов. — 6-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2022. — 415 с. — (Высшее образование). — ISBN 978-5-534-14327-0. — URL : https://urait.ru/bcode/488767Калятин, В. О. Право интеллектуальной собственности. Правовоерегулирование баз данных : учебное пособие для вузов / В. О. Калятин. — Москва:ИздательствоЮрайт,2021.—186с.—(Высшееобразование).— ISBN978-5-534-06200-7.—URL:https://urait.ru/bcode/473448

4. Информационные технологии в юридической деятельности : учебник для вузов / П. У. Кузнецов [и др.] ; под общей редакцией П. У. Кузнецова. — 3-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2022. — 325 с. — (Высшее образование). — ISBN 978-5-534-02598-9. — URL : https://urait.ru/bcode/488769

в) дополнительная литература

1. Корабельников, С. М. Преступления в сфере информационной безопасности : учебное пособие для вузов / С. М. Корабельников. — Москва : Издательство Юрайт, 2022. — 111 с. — (Высшее образование). — ISBN 978-5-534-12769-0. — URL : https://urait.ru/bcode/496492

2. Внуков, А. А. Защита информации : учебное пособие для вузов / А. А. Внуков. — 3-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2022. — 161 с. — (Высшее образование). — ISBN 978-5-534-07248-8. — URL : https://urait.ru/bcode/490277Правовоеобеспечениепрофессиональнойдеятельностинатранспортедляколледжей:учебникдлясреднегопрофессиональногообразования / А. И. Землин [и др.] ; ответственный редактор А. И. Землин. — Москва:ИздательствоЮрайт,2021.—254с.— (Профессиональноеобразование).—ISBN978-5-534-14241-9.— URL:https://urait.ru/bcode/468100

3. Казарин, О. В. Программно-аппаратные средства защиты информации. Защита программного обеспечения : учебник и практикум для вузов / О. В. Казарин, А. С. Забабурин. — Москва : Издательство Юрайт, 2022. — 312 с. — (Высшее образование). — ISBN 978-5-9916-9043-0. — URL : https://urait.ru/bcode/491249

4. Панарина, М. М. Корпоративная безопасность: система управления рисками и комплаенс в компании : учебное пособие для вузов / М. М. Панарина. — Москва : Издательство Юрайт, 2022. — 158 с. — (Высшее образование). — ISBN 978-5-534-15342-2. — URL : https://urait.ru/bcode/497632

5. Белкин, А. Р. Теория доказывания в уголовном судопроизводстве в 2 ч. Часть 1 : учебное пособие для вузов / А. Р. Белкин. — 2-е изд., испр. и доп. — Москва : Издательство Юрайт, 2022. — 184 с. — (Высшее образование). — ISBN 978-5-534-07405-5. — URL : https://urait.ru/bcode/492441

6. Белкин, А. Р. Теория доказывания в уголовном судопроизводстве в 2 ч. Часть 2 : учебное пособие для вузов / А. Р. Белкин. — 2-е изд., испр. и доп. — Москва : Издательство Юрайт, 2022. — 294 с. — (Высшее образование). — ISBN 978-5-534-07407-9. — URL : https://urait.ru/bcode/492502

7. Автоматизированные дактилоскопические системы органов внутренних дел, используемые в раскрытии и расследовании преступлений : учебное пособие для вузов / А. А. Сафонов [и др.] ; под общей редакцией А. А. Сафонова. — Москва : Издательство Юрайт, 2022. — 124 с. — (Высшее образование). — ISBN 978-5-534-15042-1. — URL : https://urait.ru/bcode/486435

8. Цифровая криминалистика : учебник для вузов / В. Б. Вехов [и др.] ; под редакцией В. Б. Вехова, С. В. Зуева. — Москва : Издательство Юрайт, 2022. — 417 с. — (Высшее образование). — ISBN 978-5-534-14600-4. — URL : https://urait.ru/bcode/497080

9. Илякова, И. Е. Коммерческая тайна : учебное пособие для вузов / И. Е. Илякова. — Москва : Издательство Юрайт, 2022. — 139 с. — (Высшее

образование). — ISBN 978-5-534-14712-4. — URL : https://urait.ru/bcode/497149

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

1. Федеральный портал «Российское образование» http://www.edu.ru/
2. Федеральное хранилище «Единая коллекция цифровых образовательных ресурсов» http://school-collection.edu.ru/
3. Российский портал «Открытое образование» http://www.openet.edu.ru
4. Сайт образовательных ресурсов Даггосуниверситета http://edu.dgu.ru
5. Информационные ресурсы научной библиотеки Даггосуниверситета http://elib.dgu.ru.
6. Открытая электронная библиотека http: www.diss.rsl.ru.
7. СПС «Гарант» http: www.garant.ru.
8. СПС «Консультант плюс» http: www.tls-cons.ru.
9. СПС «Право» http: www.pravo.ru.
10. Государственная автоматизированная система «Правосудие» - http://www.sudrf.ru/index.php?id=300
11. Научная библиотека Дагестанского государственного университета - http://www.elib.dgu.ru/
12. Официальный сайт открытого правительства РФ - http://openstandard.ru/rating_2015.html
13. Портал государственных программ РФ - http://programs.gov.ru/Portal/programs/list
14. Портал государственных услуг РФ - http://www.gosuslugi.ru/
15. Портал открытых данных РФ - http://data.gov.ru/
16. Собрание законодательства РФ на портале Государственной системы правовой информации - http://pravo.gov.ru/proxy/ips/?editions
17. Судебная практика – www.sud-praktika.narod.ru
18. Правительство РФ правительство.рф
19. Сервер органов государственной власти РФ www.gov.ru
20. 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 «Преступления в сфере информационных технологий» предполагает изложение теоретического курса на лекционных занятиях и приобретение практических навыков в процессе решения поставленных задач, возникающих при регулировании информационно-правовых отношений. Конспекты лекций служат основой для подготовки к семинарским занятиям. Самостоятельная работа студентов состоит в повторении по конспекту начитанного лекционного материала и получение дополнительных сведений по тем же учебным вопросам из рекомендованной и дополнительной литературы, выполнение тестовых заданий по пройденным темам на семинарских занятиях, а также подготовке и защите реферата по выбранной теме исследования.

При изучении курса «Преступления в сфере информационных технологий» рекомендуется обращаться не только к учебникам, но и к рекомендованной дополнительной литературе.

Курс состоит из четырех 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 «Преступления в сфере информационных технологий» 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 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 зачету.

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 «Преступления в сфере информационных технологий»

11. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине, включая перечень программного обеспечения и информационных справочных систем

При изучении данного курса студенты должны обращаться к информационно-правовой справочной системе Гарант, Консультант плюс, образовательному блогу ragimhanova.blogspot.com, Официальным сайтам Министерства связи и телекоммуникации, Государственные услуги, Государственные программы, Порталу открытых данных.

12. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине

Лекционный зал, оборудованный проекционным оборудованием и выходом в Интернет, компьютерный класс в стандартной комплектации для практических; доступ к сети Интернет (во время самостоятельной подготовки и на практических занятиях), учебники и практикумы.