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

ОРГАНИЗАЦИОННОЕ И ПРАВОВОЕ ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Кафедра информационного права и информатики юридического института

Образовательная программа бакалавриата
09.03.03 Прикладная информатика

Направленность (профиль) подготовки
Прикладная информатика в юриспруденции

Форма обучения
очная

Статус дисциплины: **входит в часть, формируемую участниками образовательных отношений**

Махачкала, 2022

Рабочая программа дисциплины «Организационное и правовое обеспечение информационной безопасности» 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 «Информационное право и информатика», Рагимханова Камилла Тагировна, ст. преп.

Рабочая программа дисциплины одобрена:
на заседании кафедры информационного права и информатики
от «25» 02 2022 г., протокол № 7

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

на заседании Методической комиссии юридического института
от «21» 03 2022 г., протокол № 7.

Председатель _____ Арсланбекова А.З.
(подпись)

Рабочая программа дисциплины согласована с учебно-методическим управлением
«31» 03 2022 г.

Начальник УМУ _____ Гасангаджиева А.Г.
(подпись)

Аннотация рабочей программы дисциплины

Дисциплина «**Организационное и правовое обеспечение информационной безопасности»** входит в часть, формируемую участниками образовательной программы бакалавриата (модуль профессиональной направленности) 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 раскрытием положения, связанные со структурой правового обеспечения информационной безопасности и соответствующего законодательства в области информации, информационных технологий и защиты информации, персональных данных, интеллектуальной собственности, государственной тайны, электронной цифровой подписи, технического регулирования. Раскрывает вопросы юридической ответственности за правонарушения в области информационной безопасности, а также механизмы защиты прав и законных интересов субъектов информационной сферы. Значительное внимание уделено построению систем организационного обеспечения информационной безопасности.

Дисциплина нацелена на формирование следующих компетенций выпускника: профессиональных – **ПК-1, ПК-7.**

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.

Очная форма обучения

Семестр	Учебные занятия в том числе:							СРС, в том числе зачет, дифференцированный зачет, экзамен	Форма промежуточной аттестации (зачет, дифференцированный зачет, экзамен)
	всего	Контактная работа обучающихся с преподавателем							
		всего	из них						
			Лекции	Лабораторные занятия	Практические занятия	…	..		
6	72		12		22			38	Зачет

1. Цели освоения дисциплины

Целями освоения дисциплины «Организационное и правовое обеспечение информационной безопасности» являются:

- формирование и развитие у будущих юристов теоретических знаний и практических навыков применения технологий информационных систем судебной деятельности;
- 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 модуль профессиональной направленности и изучается в четвертом семестре.

Дисциплина логически и содержательно-методически связана с

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

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

в) 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 «Организационное и правовое обеспечение информационной безопасности» 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).

Код и наименование универсальной компетенции выпускника	**Код и наименование индикатора достижения универсальной компетенции выпускника**	**Планируемые результаты обучения**	**Процедура освоения**
ПК-1. Способность проводить обследование организаций, выявлять информационные потребности пользователей, формировать требования к информационной системе	ИПК- 1.1. Знает методики обследования организаций, выявления информационных потребностей пользователей	Знать: основные способы и режимы обработки экономической информации; методику обследования организаций, выявления информационных потребностей пользователей; формирования требований к информационной системе; классы ИС и особенности корпоративных ИС; типы объектов проектирования и их структуры, состав компонент технологии проектирования, классы технологий проектирования, методы и инструментальные средства проектирования; особенности жизненного цикла проекта ИС; состав проектной и регламентной документации; состав стадий и этапов проектирования ИС для предметной области; виды моделей и методов моделирования ИС и информационных технологий и средства моделирования ИС	Устный опрос
	ИПК- 1.2. Умеет анализировать предметную область, выявлять информационные потребности пользователей, формировать требования к ИС	Уметь: проводить анализ информационных потребностей пользователей и формировать требования к информационной системе; анализировать предметную область и выявлять состав подразделений, выполняемые функции и задачи; исследовать объекты проектирования как системы; проводить декомпозицию системы и выделять компоненты систем на различных уровнях изучения; классифицировать и выбирать типы моделей и методымоделирования ИС; выделять стадии цикла жизни проекта ИС и их содержание.	Письменный опрос

	ИПК- 1.3 Владеет навыками работы с технологиями и программным инструментарием формирования требований к информационной системе	Владеть: навыками работы с технологиями и программным инструментарием формирования требований к информационной системе; навыками осуществления декомпозиции сложных экономических и организационных систем на макро и микро уровне, на уровне процессов управления и функционирования системы, а также на уровне происходящих в системе процессов.	Контрольная работа
ПК-7. Способность принимать участие в организации ИТ-инфраструктуры и управлении информационной безопасностью.	ИПК- 7.1. Знает инструменты и методы оценки качества и эффективности ИС; основы информационной безопасности организации.	Знать: архитектуру, устройство и функционирование вычислительных систем; инструменты и методы оптимизации ИС; методы информационной безопасности.	Устный опрос
	ИПК- 7.2. Умеет анализировать ИТ-инфраструктуру и информационную безопасность организации	Уметь: обеспечивать информационную безопасность ИТ-инфраструктуры организаций различных видов деятельности; разрабатывать метрики работы ИС; анализировать исходные данные	Письменный опрос
	ИПК- 7.3. Владеет навыками организации ИТ-инфраструктуры, характеризующейся высокой степенью информационной безопасности	Владеть: навыками оценки параметров работы ИС; определения базовых элементов ИТ-инфраструктуры; определения параметров, которые должны быть улучшены; осуществления оптимизации ИС для достижения высокой степенью информационной безопасности	Контрольная работа

4. Объем, структура и содержание дисциплины

4.1. Объем дисциплины составляет 2 зачетные единицы, 72 академические часа.

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	Прак.занятия	Лаб. Занятия	КСР		
1	2	3	4	5	6	7	8	9	10
	Модуль 1. Российское законодательство в области информационной безопасности и защиты информации								
1	Введение в дисциплину. Понятие и структура правовой информации	6		2	2			3	Устный и письменный опрос
2	Структура и общая характеристика законодательства в области информационной безопасности	6		2	2			3	Устный и письменный опрос
3	Правовой режим защиты государственной тайны	6		2	2			3	Устный и письменный опрос
4	Правовой режим защиты информации конфиденциального характера	6			2			3	Устный и письменный опрос
5	Правовая защита персональных данных	6			2			3	Устный и письменный опрос
6	Государственное регулирование деятельности в области защиты информации	6			2			3	Устный и письменный опрос
	Итого по модулю 1:			6	12			18	36
	Модуль 2. Организационное обеспечение информационной безопасности								
1	Понятие организационной защиты информации	6		2	2			4	Устный и письменный опрос
2	Организация режима секретности	6		2	2			4	Устный и письменный опрос
3	Допуск к государственной тайне	6			2			4	Устный и письменный опрос
4	Организация охраны объектов	6		2	2			4	Устный и письменный опрос

5	Организация режимных мероприятий	6			2			4	Устный и письменный опрос
	Итого по модулю 3:			6	10			20	36
	ИТОГО:			12	22			38	Зачет

4.3. Содержание дисциплины, структурированное по темам (разделам)

Модуль 1. Российское законодательство в области информационной безопасности и защиты информации

Тема 1. Введение в дисциплину. Понятие и структура правовой информации.

Введение. Государственное устройство и нормотворчество Российской Федерации. Нормативные правовые акты: официальное опубликование и вступление НПА в силу; официальные источники правовой информации; Федеральный регистр нормативных актов субъектов РФ; поиск правовой информации.

Тема 2. Структура и общая характеристика законодательства в области информационной безопасности.

Структура информационной сферы и характеристика ее элементов. Информация как объект правоотношений. Категории информации по условиям доступа к ней и распространения. Конституционные гарантии прав граждан в информационной сфере и механизм их реализации. Субъекты и объекты правоотношений в области информационной безопасности. Система нормативных правовых актов, регулирующие обеспечение информационной безопасности в Российской Федерации. Понятие и виды информации ограниченного доступа по законодательству РФ. Доктрина информационной безопасности России.

Тема 3. Правовой режим защиты государственной тайны.

Понятие правового режима защиты государственной тайны. Система нормативных правовых актов, регламентирующих обеспечение сохранности сведений, составляющих государственную тайну в Российской Федерации. Государственная тайна как особый вид защищаемой информации и ее характерные признаки. Принципы и механизмы отнесения сведений к государственной тайне, их засекречивания и рассекречивания.

Тема 4. Правовой режим защиты информации конфиденциального характера.

Понятие информации конфиденциального характера по российскому законодательству. Основные виды конфиденциальной информации: персональные данные, служебная тайна, коммерческая тайна, банковская тайна, профессиональная тайна, тайна следствия и судопроизводства.

Правовой режим конфиденциальной информации: содержание и особенности. Основные требования, предъявляемые к организации защиты конфиденциальной информации.

Тема 5. Правовая защита персональных данных.

Правовые основы защиты информации персонального характера. Закон РФ «О персональных данных», подзаконные нормативно-правовые документы о порядке правовой защиты персональных данных. Государственный надзор и контроль обработки персональных данных.

Тема 6. Государственное регулирование деятельности в области защиты ин формации.

Понятие лицензирования по российскому законодательству. Виды деятельности, подлежащие лицензированию. Правовая регламентация лицензионной деятельности в области обеспечения информационной безопасности. Объекты лицензирования и участники лицензионных отношений в сфере защиты информации. Органы лицензирования и их полномочия. Организация лицензирования в сфере обеспечения информационной безопасности. Контроль за соблюдением лицензиатами условий ведения деятельности. Правовые основы сертификации в области защиты информации.

Модуль 2. Организационное обеспечение информационной безопасности

Тема 7. Понятие организационной защиты информации.

Введение в организационное обеспечение информационной безопасности. Список рекомендованной литературы. Сущность организационных методов защиты информации. Соотношение организационных мер защиты информации с мерами правового и технического характера. Основные термины, связанные с организацией защиты информации.

Тема 8. Организация режима секретности.

Организационные меры, направленные на защиту государственной тайны. Режим секретности как основной порядок деятельности в сфере защиты государственной тайны. Особенности системы организационной защиты государственной тайны. Распределение между уровнями государственного управления полномочий, управленческих функций и задач по защите государственной тайны. Организация деятельности режимно-секретных органов. Установление и изменение степени секретности сведений, отнесенных к государственной тайне. Понятие «рассекречивание сведений». Основания для рассекречивания сведений. 16

Тема 9. Допуск к государственной тайне.

Порядок допуска и доступа к государственной тайне. Основные принципы допускной работы. Номенклатура должностей работни ков, подлежащих оформлению на допуск и порядок ее составления и утверждения. Документальное оформление для отправки на согласование. Процедура оформления и переоформления допусков и ее документирование, подлежащее согласованию с органами государственной безопасности. Организация доступа к сведениям, составляющим государственную тайну.

Тема 10. Организация охраны объектов.

Понятие «охрана». Цели и задачи охраны. Объекты охраны: территория, здания, помещения, персонал, информационные ресурсы, материальные и финансовые ценности. Особенности их охраны. Виды, способы и особенности охраны различных объектов. Понятие о рубежах охраны. Многорубежная система охраны. Факторы выбора методов и средств охраны. Организация охраны объектов защиты в процессе их транспортировки.

Тема 11. Организация режимных мероприятий.

Понятие «режим», цели и задачи режимных мероприятий. Виды режима. Организация пропускного режима. Основные положения инструкции об организации пропускного режима и работе бюро пропусков. Виды пропускных документов. Порядок организации работы бюро пропусков. Контрольно-пропускные пункты, их оборудование и организация работы. Понятие «внутриобъектовый режим» и его общие требования. Противопожарный режим и его обеспечение.

Семинарские занятия.

Модуль 1. Российское законодательство в области информационной безопасности и защиты информации

Тема 1. **Российское законодательство в области информационной безопасности и защиты информации (12 ч.)**

1. Понятие и структура правовой информации.
2. Структура и общая характеристика законодательства в области информации.
3. Правовой режим защиты государственной тайны.
4. Правовой режим защиты информации конфиденциального характера.
5. Правовая защита персональных данных.
6. Государственное регулирование деятельности в области защиты ин формации.

Модуль 2. Организационное обеспечение информационной безопасности

Тема 3. Организационное обеспечение информационной безопасности (10 ч.)

1. Понятие организационной защиты информации.
2. Организация режима секретности.
3. Допуск к государственной тайне.
4. Организация охраны объектов.
5. Организация режимных мероприятий.
6. Текущая работа с персоналом, обладающим конфиденциальной информацией.

5. **Образовательные технологии**

В соответствии с требованиями Федерального государственного образовательного стандарта высшего образования по направлению подготовки 090303 - «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 «Организационное и правовое обеспечение информационной безопасности» 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 «Организационное и правовое обеспечение информационной безопасности». 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. Фонд оценочных знаний по дисциплине «Организационное и правовое обеспечение информационной безопасности» сформирован в виде учебного пособия по подготовке к тестированию, размещенному на сайте кафедры «Информационное право и информатика» юридического факультета ДГУ. Также используется тренинго-тестирующая система ОАО «Консультант-Плюс».

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,	См. разделы 6 и 7 данного документа

		научных статей и тезизов	
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. «Цифровое неравенство» и его влияние на другие формы неравенства.
2. Блокирование информационного сотрудничества как форма информационной борьбы.
3. Государственная информационная политика - составная часть процесса трансформации общественных отношений.
4. Институт тайны как универсальный способ правовой защиты информации ограниченного доступа.
5. Интеллектуальный шпионаж. Особенности, виды, меры борьбы.
6. Интернет и Интерпол.
7. Информационная сфера как сфера правового регулирования.
8. Информационное право и его эволюция.
9. Информационно-поисковые языки. Языки предметного типа.
10. Информационные барьеры.
11. Информационные отношения.
12. Информационные правоотношения. Субъекты и объекты правоотношений.
13. Информационные преступления как угроза экономической безопасности.
14. Информационные ресурсы: понятие, особенности правовой охраны.
15. Информация как объект гражданских правоотношений.
16. Информация как объект информационных правоотношений.
17. Информация как объект преступных посягательств.
18. Информация с ограниченным доступом: понятие и виды.
19. История возникновения и создания автоматизированных информационных систем.
20. Классификация социальной информации по сфере применения, по режиму доступа, по функциональному назначению.
21. Коммерческая (профессиональная, служебная) информация, ее правовая защита. Ответственность за неправомерное использование такой информации.
22. Концепция электронного правительства.
23. Криминализация нарушений авторского и смежного права в Интернете. Примеры.
24. Криминальная деятельность в области информационных отношений.
25. Методы ведения электронной (информационной) разведки в мирное время. Примеры.
26. Механизмы управления в информационном обществе.

27. Модели формирования глобального информационного общества.
28. Негативные последствия информатизации общества.
29. Нормативные правовые акты, определяющие основное содержание и развитие системы обеспечения свободы массовой информации, а также регулирующие библиотечное и архивное дело в Российской Федерации.
30. Носители правовой информации.
31. Окинавская Хартия глобального информационного общества.
32. Основные задачи в области обеспечения информационной безопасности.
33. Основные направления использования информационных систем в юридической деятельности.
34. Основные ограничения права на доступ к информации. Информация без права ограничения доступа.
35. Основные проблемы, цели и перспективы информатизации РФ.
36. Основные требования, предъявляемые к современным информационным системам.
37. Особенности информационных войн современности и их примеры.
38. Особенности правоотношений, возникающих при производстве, распространении и потреблении массовой информации.
39. Особенности правоотношений, возникающих при производстве, распространении и потреблении библиотечной информации.
40. Особенности правоотношений, возникающих при производстве, распространении и потреблении архивной информации.
41. Особенности сети Интернет как средства распространения информации.
42. Особенности следственных действий при выявлении информационных преступлений.
43. Особенности субъективной стороны информационных преступлений.
44. Ответственность СМИ за злоупотребление правом свободы массовой информации.
45. Перемещение информационного взаимодействия государственной власти с гражданами в сетевой среде.
46. Порядок регистрации доменных имен Интернет.
47. Право в Интернете - проблемы, подходы, решения, нормы. Современное состояние проблемы «право в Интернете».
48. Право собственности на средства обработки информации. Нормы, определяющие право собственности на информацию, информационные ресурсы и средства обработки информации.
49. Правовые аспекты борьбы со спамом в Интернете. Примеры разновидностей спама.
50. Правовые особенности построения Интернет-2. Подходы к решению.
51. Правовые ресурсы сети Интернет.

52. Проблемы авторского права на информационные ресурсы и на информационные технологии в виртуальной среде Интернет.

53. Распространение информации о нарковеществах в Интернете - вид правонарушения.

54. Роль «электронного правительства» в борьбе с коррупцией.

55. Роль «электронного правительства» в повышении общей информационной культуры населения.

56. Сговор при ограничении доступа к открытой информации. Примеры нарушений.

57. Стимулы и факторы, способствующие созданию «электронного правительства».

58. Уголовная ответственность за нарушение имущественных и смежных прав в Интернете. Примеры.

59. Федеральная целевая программа «Электронная Россия».

60. Эволюция моделей «электронной власти» (от компьютерного офиса до «электронного правительства»).

61. Электронно-цифровая подпись и ее юридическое значение в информационном праве.

62. Электронный адрес (e-mail, URL) как источник официальной правовой информации. Примеры.

63. Юридический статус электронной переписки. Примеры нарушений.

Примерные тесты

Примерные тестовые задания для проведения текущего и промежуточного контроля

1. Разделение информации на категории свободного и ограниченного доступа,
причем информации ограниченного доступа подразделяются на:
а) отнесенные к государственной тайне;
б) отнесенные к служебной тайне (информации для служебного пользования),
персональные данные (и другие виды тайн);
в) отнесенные к информации о прогнозах погоды;
г) все верны ответы.
2. Государственная тайна — это:
а) защищаемые государственные сведения в области военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которой может нанести ущерб безопасности Российской Федерации;
б) защищаемые государственные сведения только в области военной и внешнеполитической деятельности, распространение которой может нанести ущерб безопасности Российской Федерации;
в) защищаемые государственные сведения только в области экономической и

разведывательной деятельности, распространение которой может нанести ущерб безопасности Российской Федерации.
3. К информации ограниченного доступа относятся:
а) государственная тайна;
б) конфиденциальная информация;
в) персональные данные;
г) все ответы верны.
4. Государственная тайна — это:
а) информация, сведения, несанкционированный доступ к которым может причинить вред интересам страны, государства;
б) информация, сведения, несанкционированный доступ к которым может причинить вред интересам только жителям страны, но всего государства;
в) информация, сведения, несанкционированный доступ к которым может причинить вред интересам только руководству страны, государства.
5. Как называется закон, регулирующий деятельность государственной тайны на
территории РФ?
а) «О коммерческой тайне»;
б) «О государственной тайне»;
в) «О служебной тайне»;
г) «О врачебной тайне».
6. Назовите признаки государственной тайны?
а) это очень важные сведения; их разглашение может причинить ущерб государственным интересам; перечень сведений, которые могут быть отнесены к государственной тайне, закрепляется федеральным законом;
б) это очень важные сведения и их разглашение может причинить ущерб государственным интересам;
в) это очень важные сведения и перечень сведений, которые могут быть отнесены к государственной тайне, закрепляется федеральным законом.
7. К носителям сведений, составляющих государственную тайну относятся:
а) материальные объекты, в том числе физические поля, в которых сведения, составляющие государственную тайну, находят свое отражение в виде символов, образов, сигналов, технических решений и процессов;
б) материальные объекты, за исключением физических полей, в которых сведения, составляющие государственную тайну, находят свое отражение в виде символов, образов, сигналов, технических решений и процессов;
в) нет верного ответа.
8. Гриф секретности — это:
а) реквизиты, свидетельствующие о степени секретности сведений, содержащихся в их носителе, проставляемые на самом носителе кроме сопроводительной документации на него;
б) реквизиты, свидетельствующие о степени секретности сведений, содержащихся в их носителе, проставляемые на самом носителе и (или) в сопроводительной документации на него.
в) оба варианта верны.

9. Степень секретности — это:
а) категория, характеризующая важность такой информации, возможный ущерб в случае ее разглашения, степень ограничения доступа к ней и уровень ее охраны государством;
б) категория, характеризующая важность такой информации, возможный ущерб в случае ее разглашения, но не степень ограничения доступа к ней и уровень ее охраны государством;
в) нет верного ответа.
10. Устанавливаются степени секретности сведений, составляющих государственную тайну:
а) три;
б) две;
в) четыре.
11. Субъектами отнесения сведений к государственной тайне являются:
а) Палаты Федерального Собрания;
б) Президент Российской Федерации;
в) Правительство Российской Федерации;
г) Органы государственной власти Российской Федерации, органы государственной власти субъектов Российской Федерации и органы местного самоуправления во взаимодействии с органами защиты государственной тайны, расположенными в пределах соответствующих территорий;
д) верны все варианты.
12. Не подлежат отнесению к государственной тайне и засекречиванию сведения:
а) о чрезвычайных происшествиях и катастрофах, угрожающих безопасности и здоровью граждан и их последствиях, а также о стихийных бедствиях, их официальных прогнозах и последствиях;
б) состоянии экологии, здравоохранения, санитарии, демографии, образования, культуры, сельского хозяйства, а также о состоянии преступности;
в) размерах золотого запаса и государственных валютных резервах Российской Федерации;
г) верны все варианты.
13. Срок засекречивания сведений, составляющих государственную тайну, не должен превышать:
а) 30 лет;
б) 40 лет;
в) 50 лет;
г) 60 лет.
14. Персональные данные - это:
а) конкретная информация, относящаяся к определенному или определяемому
на основании такой информации физическому лицу (субъекту персональных данных);

б) любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных);
в) любая информация, относящаяся к определенному или определяемому на основании такой информации юридическому лицу (субъекту персональных данных).
15. Субъект персональных данных обладает правами:
а) на доступ к своим персональным данным;
б) возражение против принятия решений исключительно на основании автоматизированной обработки персоналом данных, порождающих юридические последствия в отношении субъекта или иным образом затрагивающих его права и законные интересы;
в) обжалование действий или бездействий;
г) верны все варианты
16. ИСПДн согласно 5 пункту Постановления №1119 подразделяются на следующие группы (категории):
а) Специальные ИСПДн;
б) Биометрические ИСПДн;
в) Общедоступные ИСПДн;
г) Иные ИСПДн;
д) верны все варианты.
17. По форме отношений между организацией и субъектами, обработка подразделяется на следующие виды:
а) обработка ПДн сотрудников (субъектов, с которыми организация связана трудовыми отношениями);
б) обработка ПДн субъектов, не являющихся сотрудниками организации;
в) верны оба варианта.

Примерные вопросы к зачету

1. Государство: понятие, признаки, функции
2. Формы государства
3. Правовое государство
4. Сущность права: признаки, структура, функции
5. Источники права
6. Норма права и система права
7. Понятие, предмет и объект гражданского права
8. Принципы гражданского права
9. Источники гражданского права
10. Объекты гражданского права
11. Субъекты гражданского права
12. Структура информационной сферы, характеристика ее элементов.
13. Информация как объект правоотношений, категории информации.
14. Система правовой защиты информации.
15. Понятие и виды защищаемой информации.

16. Особенности государственной тайны как защищаемой информации.
17. Система защиты государственной тайны.
18. Засекречивание информации, отнесенной к государственной тайне.
19. Защита сведений отнесенных к государственной тайне.
20. Понятие информации конфиденциального характера.
21. Основные виды конфиденциальной информации, в соответствии с требованиями российской нормативно-правовой базы.
22. Правовой режим конфиденциальной информации.
23. Основные требования, предъявляемые к организации защиты конфиденциальной ин формации.
24. Понятие и характеристика служебной тайны.
25. Нормативно - правовые основы защиты служебной тайны.
26. Порядок обращения с документами, содержащими служебную информацию ограниченного распространения.
27. Правовые основы защиты коммерческой тайны.
28. Виды информации, составляющей коммерческую тайну.
29. Права и обязанности обладателя коммерческой тайны.
30. Основные угрозы коммерческой тайны.
31. Правовая защита коммерческой тайны.
32. Правовые основы защиты банковской тайны.
33. Раскрытие информации, относящейся к банковской тайне.
34. Нарушение банковской тайны и ответственность за подобные нарушения.
35. Нотариальная тайна и ее особенности. Тайна завещания.
36. Врачебная тайна и ее особенности.
37. Адвокатская тайна и ее особенности.
38. Тайна страхования и ее особенности.
39. Тайна связи и ее особенности. Тайна переписки, почтовых, телеграфных и иных сообщений.
40. Тайна усыновления (удочерения). Тайна исповеди.
41. Формирование российского законодательства в области защиты персональных данных. 31. Основные понятия и содержание закона РФ «О персональных данных».
42. Подзаконные нормативно-правовые документы о порядке правовой защиты персональных данных.
43. Государственный надзор и контроль обработки персональных данных, ответственность за нарушения российского законодательства в данной области.
44. Правовые основы лицензирования в области защиты информации.
45. Правовые основы сертификации в области защиты информации.
46. Особенности правонарушений в информационной сфере.
47. Преступления в сфере компьютерной информации: виды, состав.
48. Основы расследования преступлений в сфере компьютерной информации.
49. Правовая защита информационных систем.

50. Правовая защита результатов интеллектуальной деятельности.
51. Соотношение организационных мер защиты информации с мерами правового и технического характера.
52. Основные термины, связанные с организацией защиты информации.
53. Организационные меры, направленные на защиту государственной тайны.
54. Режим секретности как основной порядок деятельности в сфере защиты государственной тайны.
55. Особенности системы организационной защиты государственной тайны.
56. Распределение между уровнями государственного управления полномочий, управленческих функций и задач по защите государственной тайны.
57. Организация деятельности режимно-секретных органов.
58. Установление и изменение степени секретности сведений, отнесенных к государственной тайне.
59. Понятие «рассекречивание сведений». Основания для рассекречивания сведений.
60. Порядок допуска и доступа к государственной тайне. Основные принципы допускной работы.
61. Номенклатура должностей работников, подлежащих оформлению на допуск и порядок ее составления и утверждения.
62. Документальное оформление для отправки на согласование.
63. Процедура оформления и переоформления допусков и ее документирование, подлежащее согласованию с органами государственной безопасности.
64. Организация доступа к сведениям, составляющим государственную тайну.
65. Понятие «охрана». Цели и задачи охраны.
66. Объекты охраны: территория, здания, помещения, персонал, информационные ресурсы, материальные и финансовые ценности. Особенности их охраны.
67. Виды, способы и особенности охраны различных объектов.
68. Понятие о рубежах охраны. Многорубежная система охраны.
69. Факторы выбора методов и средств охраны.
70. Организация охраны объектов защиты в процессе их транспортировки.
71. Понятие «режим», цели и задачи режимных мероприятий. Виды режима.
72. Организация пропускного режима. Основные положения инструкции об организации пропускного режима и работе бюро пропусков.
73. Виды пропускных документов.
74. Порядок организации работы бюро пропусков.
75. Контрольно-пропускные пункты, их оборудование и организация

работы.

76. Понятие «внутриобъектовый режим» и его общие требования.

77. Противопожарный режим и его обеспечение.

78. Подбор и расстановка кадров.

79. Направления и методы работы с персоналом, обладающим конфиденциальной информацией. Организация обучения персонала.

80. Основные формы обучения и методы контроля знаний.

81. Мотивация персонала к выполнению требований по защите информации.

82. Основные формы воздействия на персонал как методы мотивации: вознаграждение, управление карьерой, профессиональная этика.

83. Организация контроля соблюдения персоналом требований режима защиты информации. Методы проверки персонала.

84. Организация служебного расследования по фактам разглашения персоналом конфиденциальной информации.

85. Организационные меры по защите информации при увольнении сотрудника.

86. Основные требования, предъявляемые к подготовке и проведению конфиденциальных переговоров.

87. Основные этапы проведения конфиденциальных переговоров.

88. Подготовка помещения для проведения конфиденциальных переговоров.

89. Подготовка программы проведения конфиденциальных переговоров.

90. Порядок проведения конфиденциальных переговоров.

91. Требования режима защиты информации при приеме в организации посетителей. Поря док доступа посетителей и командированных лиц к конфиденциальной информации. По рядок пребывания посетителей на территории и в помещениях организации.

92. Требования к программе приема иностранных представителей.

93. Требования к помещениям, в которых проводится прием иностранных представителей.

94. Обеспечение защиты информации при выезде за рубеж командируемых лиц.

95. Основные виды и формы рекламы. Общие требования режима защиты информации в процессе рекламной деятельности.

96. Основные методы защиты информации в рекламной деятельности. Понятие «публикация в открытой печати». Общие требования режима защиты конфиденциальной информации при опубликовании материалов в открытой печати.

97. Особенности защиты информации при опубликовании материалов, определяемые характером деятельности организации, целями публикации, содержанием и характером публикации.

98. Концепция безопасности предприятия (организации) и ее содержание. Политика информационной безопасности.

99. Подразделения, обеспечивающие ИБ предприятия: основные функции, содержание деятельности, структура, обязанности сотрудников.

100. Основные документы службы информационной безопасности.

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 - 70% и промежуточного контроля - 30%.

Текущий контроль по дисциплине включает:

- участие на практических занятиях– 30 баллов,
- выполнение домашних заданий–10баллов,
- проектная деятельность – 20 баллов,
- тестирование - 10 баллов.

Промежуточный контроль по дисциплине включает:

- письменная контрольная работа (или коллоквиум) - 30 баллов.

8. Учебно-методическое обеспечение самостоятельной работы студентов.

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. Организационное и правовое обеспечение информационной безопасности: учебник и практикум для вузов / под редакцией Т. А. Поляковой, А. А. Стрельцова. — Москва: Издательство Юрайт, 2022. — 325 с. — (Высшее образование). — ISBN 978-5-534-03600-8. — URL : https://urait.ru/bcode/498844
2. *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
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/488767

в) дополнительная литература

1. *Бартош, А. А.* Основы международной безопасности. Организации обеспечения международной безопасности : учебное пособие для вузов / А. А. Бартош. — 2-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2022. — 320 с. — (Высшее образование). — ISBN 978-5-534-11783-7. — URL : https://urait.ru/bcode/493387
2. *Васильева, И. Н.* Криптографические методы защиты информации : учебник и практикум для вузов / И. Н. Васильева. — Москва : Издательство Юрайт, 2022. — 349 с. — (Высшее образование). — ISBN 978-5-534-02883-6. — URL : https://urait.ru/bcode/489919
3. *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/490277
4. *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
5. 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
6. 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
7. Информационные технологии в юридической деятельности : учебник и практикум для вузов / В. Д. Элькин [и др.] ; под редакцией В. Д. Элькина. — 2-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2022. — 472 с. — (Высшее образование). — ISBN 978-5-534-12733-1. — URL : https://urait.ru/bcode/488701
8. *Казарин, О. В.* Надежность и безопасность программного обеспечения : учебное пособие для вузов / О. В. Казарин, И. Б. Шубинский. — Москва : Издательство Юрайт, 2022. — 342 с. — (Высшее образование). — ISBN 978-5-534-05142-1. — URL : https://urait.ru/bcode/493262
9. *Кузнецова, Е. И.* Экономическая безопасность : учебник и практикум для вузов / Е. И. Кузнецова. — 2-е изд. — Москва : Издательство Юрайт, 2022. — 336 с. — (Высшее образование). — ISBN 978-5-534-14514-4. — URL : https://urait.ru/bcode/490856
10. *Лось, А. Б.* Криптографические методы защиты информации для изучающих компьютерную безопасность : учебник для вузов / А. Б. Лось, А. Ю. Нестеренко, М. И. Рожков. — 2-е изд., испр. — Москва : Издательство Юрайт, 2022. — 473 с. — (Высшее образование). — ISBN 978-5-534-12474-3. — URL :

https://urait.ru/bcode/489242
11. *Нетёсова, О. Ю.* Информационные системы и технологии в экономике: учебное пособие для вузов / О. Ю. Нетёсова. — 3-е изд., испр. и доп. — Москва: Издательство Юрайт, 2022. — 178 с. — (Высшее образование). — ISBN 978-5-534-08223-4. — URL : https://urait.ru/bcode/491479
12. *Фомичёв, В. М.* Криптографические методы защиты информации в 2 ч. Часть 1. Математические аспекты : учебник для вузов / В. М. Фомичёв, Д. А. Мельников ; под редакцией В. М. Фомичёва. — Москва : Издательство Юрайт, 2022. — 209 с. — (Высшее образование). — ISBN 978-5-9916-7088-3. — URL : https://urait.ru/bcode/489745
13. *Фомичёв, В. М.* Криптографические методы защиты информации в 2 ч. Часть 2. Системные и прикладные аспекты : учебник для вузов / В. М. Фомичёв, Д. А. Мельников ; под редакцией В. М. Фомичёва. — Москва : Издательство Юрайт, 2022. — 245 с. — (Высшее образование). — ISBN 978-5-9916-7090-6. — URL : https://urait.ru/bcode/490421

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

1. eLIBRARY.RU[Электронный ресурс]: электронная библиотека / Науч. электрон. б-ка. — Москва, 1999 – Режим доступа: http://elibrary.ru/defaultx.asp. – Яз. рус., англ.
2. Образовательный блог по Информационному праву [Электронный ресурс]: (magdilovaip.blogspot.ru)
3. Образовательный блог по Информационным технологиям в юридической деятельности [Электронный ресурс]: (magdilovaitud.blogspot.ru)
4. Федеральный портал «Российское образование» http://www.edu.ru/
5. Федеральное хранилище «Единая коллекция цифровых образовательных ресурсов» http://school-collection.edu.ru/
6. Сайт образовательных ресурсов Даггосуниверситетаhttp://edu.dgu.ru
7. Информационные ресурсы научной библиотеки Даггосуниверситетаhttp://elib.dgu.ru.
8. Открытая электронная библиотека http: www.diss.rsl.ru.
9. СПС «Гарант» https://www.garant.ru/
10. СПС «Консультант плюс» http://www.consultant.ru/
11. Официальный интернет-портал правовой информации http://pravo.gov.ru/
12. ИПС «Законодательство России» http://pravo.gov.ru/ips/
13. Государственная автоматизированная система «Правосудие» - http://www.sudrf.ru/index.php?id=300
14. Научная библиотека Дагестанского государственного университета - http://www.elib.dgu.ru/

15. Портал государственных программ РФ - http://programs.gov.ru/Portal/programs/list
16. Портал государственных услуг РФ - http://www.gosuslugi.ru/
17. Портал открытых данных РФ - http://data.gov.ru/
18. Собрание законодательства РФ на портале Государственной системы правовой информации - http://pravo.gov.ru/proxy/ips/?editions
19. Судебная практика – www.sud-praktika.narod.ru
20. Правительство РФ правительство.рф
21. Сервер органов государственной власти РФ www.gov.ru
22. Юридический Вестник ДГУ.http://www.jurvestnik.dgu.ru
23. Российский портал «Открытое образование» http://www.openedu.ru
24. Образовательная платформа Юрайт. https://urait.ru/
25. Каталог LegalTech-проектов https://platforma-online.ru/legaltech-catalog/
26. Конструктор правовых документов Гарант LegalTechhttp://lt.garant.ru/kpd
27. Роботизированная юридическая фирма нового поколения https://pravo.digital/
28. IT-Юрист защита интернет-проектов и интеллектуальной собственности https://it-consult.pro/
29. Caselook - Поиск и анализ судебной практики https://caselook.ru/
30. Система Юрист – справочная система практических разъяснений от судей https://www.1jur.ru/
31. Первый юридический конструктор чат-ботовhttps://form.one/legal/ru/
32. PracticalLaw - Юридическое ноу-хау по иностранному праву и практике его применениюhttps://www.thomsonreuters.ru/ru/products-services/legal/practical-law.html
33. XSUD — Программа учета судебных дел https://xsudsoft.ru/
34. Картотека арбитражных дел https://kad.arbitr.ru/
35. Мой Арбитр https://my.arbitr.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 «Организационное и правовое обеспечение информационной безопасности» 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 «Организационное и правовое обеспечение информационной безопасности» рекомендуется обращаться не только к учебникам, но и к рекомендованной дополнительной литературе.

Курс состоит из одиннадцати взаимосвязанных тем.

Учебный план предполагает также семинарские занятия, цель которых подробное изучение теоретического материала, анализ законодательства, регулирующего интеллектуальные права, 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 «Организационное и правовое обеспечение информационной безопасности» 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 этого курса 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 «Организационное и правовое обеспечение информационной безопасности».

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.