

Документ подписан простой электронной подписью
Информация о владельце:
ФИО: Минцаев Магомед Шавалович
Должность: Ректор
Дата подписания: 2025-03-26
Уникальный программный ключ:
236bcc35c296f119d6aafdc22856b21db52dbc07971a86865a5825f9fa4304cc

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
ГРОЗНЕНСКИЙ ГОСУДАРСТВЕННЫЙ НЕФТЯНОЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ
имени академика М.Д. Миллионщикова

«УТВЕРЖДАЮ»



Первый проректор – проректор ОД

И.Г. Гайрабеков

« 05 » 2025г.

РАБОЧАЯ ПРОГРАММА

дисциплины

«Киберправо»

Направление подготовки

40.03.01 Юриспруденция

профиль

«Юриспруденция»

Квалификация

Магистр

1. Цели и задачи дисциплины

1.1 Целью изучения дисциплины является получение студентами знаний в области информационного, гражданского, уголовного законодательства, выработка навыков и умений использования полученных знаний в практической деятельности, реализации прав и законных интересов в информационной сфере, решения профессиональных задач в условиях развития информационного общества, формирование профессионального правосознания, уверенности в реализации прав и свобод, законных интересов в информационной сфере и их защите.

1.2. Задачи изучения дисциплины:

- обучение студента навыкам обоснования и принятия решений, а также совершения действий, связанных с применением норм, регулирующих киберправо;
- овладение знаниями, необходимыми для успешного использования правовых норм в профессиональной деятельности;
- формирование навыков проведения научных исследований по проблемам киберправа;
- овладение умением критически анализировать действующее законодательство; обобщать судебную практику применения законодательства в сфере высоких технологий;
- овладение методикой пополнения и закрепления знаний и умений о правовом регулировании высокотехнологичной сферы;
- приобретение углублённых знаний, касающихся правовых норм в сфере высоких технологий, необходимых для преподавания в высшей школе.

2. Место дисциплины в структуре образовательной программы:

Дисциплина «**Киберправо**» относится к обязательным дисциплинам. К началу изучения данной дисциплины студенты должны обладать соответствующими знаниями по дисциплинам «Теория государства и права», «Уголовное право», «Гражданское право», «Административное право», «Международное право» и др. Знания, умения и навыки, сформированные при изучении дисциплины «**Киберправо**», могут быть использованы при прохождении производственной практики.

3. Перечень планируемых результатов обучения по дисциплине (модулю), соотнесенных с индикаторами достижения компетенций:

Таблица 1

Код по ФГОС	Индикаторы достижения	Планируемые результаты обучения по дисциплине
Профессиональные		
ПК-2. Способен квалифицированно применять нормативные правовые акты в	ПК-2.1. Имеет представление об основных юридических понятиях и категориях, необходимых для реализации норм права в	Знать: нормы материального и процессуального права. Уметь: реализовать нормы

конкретных сферах юридической деятельности, реализовывать нормы материального и процессуального права в профессиональной деятельности	юридической деятельности ПК-2.2. Применяет нормативные правовые акты в профессиональной деятельности	материального и процессуального права в профессиональной деятельности. Владеть: навыками работы с правовыми актами, на основе их анализа принимает решения о реализации норм материального и процессуального права в профессиональной деятельности.
ПК-5. Способен защищать права и законные интересы субъектов права	ПК-5.1. Понимает механизм защиты прав и законных интересов субъектов права ПК-5.2. Применяет различные способы защиты прав и законных интересов субъектов права	Знать: законодательство в сфере информационных технологий, киберпреступности, формы и способы защиты нарушенных прав и особенности их применения Уметь: применять нормы закона в области киберправа Владеть: навыками анализа и применения нормативных правовых актов в сфере киберправа

4. Объем дисциплины и виды учебной работы

Таблица 2

Вид учебной работы	Всего часов/ зач.ед.			Семестры		
				3	4	4
	ОФО	ОЗФО	ЗФО	ОФО	ОЗФО	ЗФО
Контактная работа (всего)	34/0,94	32/0,88	12/0,33	34/0,94	32/0,88	12/0,33
В том числе:						
Лекции	17/0,47	16/0,44	6/0,16	17/0,47	16/0,44	6/0,16
Практические занятия	17/0,47	16/0,44	6/0,16	17/0,47	16/0,44	6/0,16
Самостоятельная работа (всего)	74/2,05	76/2,1	96/2,66	74/2,05	76/2,1	96/2,66
В том числе:						

Темы для самостоятельного изучения		36/1	32/0,8	36/1	36/1	32/0,8	36/1
Подготовка к реферату		19/0,52	22/0,6	36/1	19/0,52	22/0,6	36/1
Подготовка к зачету		19/0,52	22/0,6	24/0,66	19/0,52	22/0,6	24/0,66
Вид промежуточной аттестации		зачет	зачет	зачет	зачет	зачет	зачет
Общая трудоемкость дисциплины	ВСЕГО в часах	108	108	108	108	108	108
	ВСЕГО в зач. единицах	3	3		3	3	

5. Содержание дисциплины

5.1. Разделы дисциплины и виды занятий

Таблица 3

№ п/п	Наименование раздела дисциплины	Часы лекционных занятий			Часы практических занятий		
		ОФО	ОЗФО	ЗФО	ОФО	ОЗФО	ЗФО
1.	Введение в киберправо: предмет, метод, система и источники.	2	2	-	2	2	-
2.	Юрисдикция и применимое право в киберпространстве.	2	2	2	2	2	2
3.	Правовой режим цифровых данных и информационных объектов.	2	2	-	2	2	-
4.	Право интеллектуальной собственности в цифровой среде.	2	2	-	2	2	-
5.	Правовое регулирование интернет-коммуникаций и электронной коммерции.	2	2	-	2	2	-
6.	Правовые основы информационной безопасности и кибербезопасности.	2	2	2	2	2	2
7.	Киберпреступность и административно-правовые нарушения в цифровой среде.	2	2	-	2	2	-
8.	Правовое регулирование искусственного интеллекта и робототехники.	2	2	2	2	2	2

9.	Право в сфере биометрии и больших данных.	1	-	-	1	-	-
		17	16	6	17	16	6

5.2. Лекционные занятия

Таблица 4

№ п/п	Наименование раздела дисциплины	Содержание раздела
1.	Введение в киберправо: предмет, метод, система и источники	1.Предмет и метод дисциплины киберправо. 2.Особенности регулирования цифровой среды. 3.Обзор международных актов и роль судебной практики.
2.	Юрисдикция и применимое право в киберпространстве.	1.Проблемы виртуального пространства. 2. Конфликт законов. 3.Роль соглашений пользователей. 4.Правовые позиции российской судов и зарубежная практика.
3.	Правовой режим цифровых данных и информационных объектов.	1.Понятие информации. 2. Базы данных и их правовая охрана. 3. Правовая база токенов, криптоактивов. 4. Понятие и виды цифровых прав.
4.	Право интеллектуальной собственности в цифровой среде	1.Авторское право в интернете. 2. Особенности защиты программ для ЭВМ. 3.Проблемы «цифрового пиратства» и механизмы противодействия» 4. Доменные имена и конфликты с товарными знаками.
5.	Правовое регулирование интернет-коммуникаций и электронной коммерции.	1.Правовой статус интернет-сайтов и мобильных приложений. 2.Договоры в электронной форме. 3.Публичная оферта в интернете. 4.Особенности оказания цифровых услуг и продажи цифрового контента.
6.	Правовые основы информационной безопасности и кибербезопасности.	1.Понятия и соотношение: информационная безопасность, кибербезопасность, безопасность критической информационной инфраструктуры. 2. Обязанности операторов КИИ (187-ФЗ). 3.Правовой статус и деятельность CERT-команд. 4.Уведомления об утечках данных.
7.	Киберпреступность и административно-правовые нарушения в цифровой среде.	1.Составы преступлений в сфере компьютерной информации (гл. 28 УК РФ: неправомерный доступ, создание и распространение вредоносных программ). 2.Смежные составы: мошенничество с использованием ИТ (ст. 159.6 УК РФ), кибербуллинг, кибершпионаж. 3.Административная ответственность (гл. 13

		КоАП РФ).
8.	Правовое регулирование искусственного интеллекта и робототехники.	1. Проблемы правосубъектности ИИ. 2. Ответственность за вред, причиненный системами ИИ и автономными роботами. 3. Авторское право на произведения, созданные ИИ. 4. Этические принципы и подходы к регулированию (законодательные инициативы в ЕС, США, Китае).
9.	Право в сфере биометрии и больших данных.	1. Правовые основы обработки биометрических данных. 2. Проблемы прогнозной аналитики, профилирования и манипулирования поведением. 3. Баланс между безопасностью, коммерческим интересом и приватностью. 4. Правовые пределы использования систем распознавания лиц.

5.3 Лабораторный минимум не предусмотрен

5.4. Практические занятия

Таблица 5

№ п/п	Наименование раздела дисциплины	Содержание раздела
1.	Введение в киберправо: предмет, метод, система и источники	Сравнительный анализ определений ключевых понятий («информация», «информационная система», «киберпространство») в разных законах (149-ФЗ, 152-ФЗ, УК РФ) и доктрине. Выявление противоречий и пробелов.
2.	Юрисдикция и применимое право в киберпространстве.	Анализ юрисдикционной оговорки и применимого права в ToS крупных международных компаний (Google, Meta, Apple, AliExpress). Оценка её справедливости и исполнимости в российских реалиях.
3.	Правовой режим цифровых данных и информационных объектов.	Группе дается описание «стартапа»: компания создает платформу для торговли цифровыми коллекционными карточками (NFT) на основе спортивных видеозаписей. Необходимо провести правовой анализ: какие объекты права здесь есть (базы данных, изображения, токены), кто и какие права на них имеет, каковы риски.
4.	Право интеллектуальной собственности в цифровой среде.	На основе смоделированной ситуации (размещение на YouTube видео, нарушающего авторские права) составить грамотное уведомление для администрации сервиса в соответствии со ст. 15.7 149-ФЗ (аналог DMCA).
5.	Правовое регулирование интернет-коммуникаций и электронной коммерции.	Аудит условного сайта интернет-магазина на предмет наличия и корректности всех обязательных документов и информации: оферта, политика обработки персональных данных (согласно 152-ФЗ), информация об ОГРН, порядке

		возврата и т.д.
6.	Правовые основы информационной безопасности и кибербезопасности.	Анализ типового акта проверки на предмет соблюдения требований к защите персональных данных или безопасности КИИ. Составление ответа на предписание.
7.	Киберпреступность и административно-правовые нарушения в цифровой среде.	Написание мотивированного заявления о преступлении в сфере компьютерной информации с описанием технических деталей на доступном для следователя языке.
8.	Правовое регулирование искусственного интеллекта и робототехники.	Ролевая игра по делу о ДТП с беспилотным автомобилем или о врачебной ошибке системы диагностики. Обсуждение в формате дебатов: кто должен нести ответственность (разработчик, владелец, оператор)?
9.	Право в сфере биометрии и больших данных.	Дано ТЗ на внедрение системы распознавания лиц в университете/торговом центре/«умном городе». Задание: составить список правовых вопросов к заказчику (основание обработки, согласие, размещение уведомлений, сроки хранения) и проект информационного уведомления для физических лиц.

6. Самостоятельная работа студентов по дисциплине

Самостоятельная работа студентов, направленная на углубление и закрепление знаний, заключается в:

- работе студентов с лекционным материалом, поиск и анализ литературы и электронных источников информации по заданной теме;
- изучение тем, вынесенных на самостоятельную проработку;
- изучение теоретического материала к практическим занятиям;
- написание реферата;
- подготовке к зачету.

6.1 Темы для самостоятельного изучения

1. Сравнительный анализ моделей регулирования персональных данных.
2. Правовые и этические проблемы «права на забвение» в интернете.
3. Ответственность информационных посредников: от хостинга до социальных сетей.
4. Правовая природа смарт-контрактов: можно ли считать их договором в традиционном смысле?
5. Кибербуллинг и киберсталкинг: пробелы в уголовном и административном законодательстве РФ.
6. Цифровое наследование: судьба аккаунтов в социальных сетях, игровых

ценностей и криптоактивов.

7. Грань между коммерческой тайной, добросовестной практикой и нарушением прав потребителей.

8. Законность заключения договоров с «белыми» хакерами, разграничение с преступной деятельностью, вопросы ответственности за превышение полномочий.

9. Современные вызовы экстерриториальности права: как государства пытаются регулировать глобальные IT-платформы.

10. Правовой статус и ответственность создателей и пользователей открытого программного обеспечения.

11. Киберправо для будущего: первичный анализ правовых проблем, связанных с развитием квантовых вычислений и нейроинтерфейсов.

6.2 Темы для рефератов

1. Правовые модели регулирования персональных данных.
2. Ответственность владельцев онлайн-платформ за контент пользователей.
3. Правовой статус смарт-контрактов и токенов: поиск адекватных конструкций в традиционном гражданском праве.
4. Юридическая сила смарт-контрактов: договор или программный код?
5. Киберпреступность: проблемы квалификации и доказывания в условиях анонимности и трансграничности.
6. Искусственный интеллект как субъект и объект права: проблемы гражданской и уголовной ответственности.
7. «Право на забвение» в цифровую эпоху: баланс между приватностью личности и свободой информации.
8. Трансграничная передача персональных данных.
9. Правовые аспекты использования биометрических данных: между удобством, безопасностью и тотальным контролем.
10. Правовые основы и пределы мониторинга сотрудников в цифровой среде
11. Правовое регулирование краудфандинга и краудинвестинга: риски для создателей и инвесторов в цифровую эпоху.
12. Особенности правовой защиты несовершеннолетних в интернете: от персональных данных до кибербуллинга.
13. Правовой режим цифровых финансовых активов в Российской Федерации.
14. Ответственность провайдеров хостинга за контент третьих лиц: сравнительный анализ подходов.

15. Судебная практика по диффамации в сети Интернет.
16. Крайняя необходимость в киберпространстве.
17. Киберсталкинг и кибербуллинг: квалификация.
18. Юридическая природа внутриигрового имущества.
19. Цифровой профиль гражданина.
20. Кибершпионаж как преступление против основ конституционного строя.
21. Правовое значение времени и даты в блокчейн-транзакциях: проблема «хронологической атаки».
22. Правовая защита интерфейса сайта и мобильного приложения.
23. Ханойская конвенция ООН против киберпреступности.
24. Технология дипфейк как новый инструмент киберпреступности: поиск эффективных правовых средств защиты.
25. Правовой статус виртуального имущества в онлайн-играх: скины, аккаунты, внутриигровая валюта.

6.3 Учебно-методическое обеспечение самостоятельной работы

Современные профессиональные базы данных:

1. <http://elibrary.ru/> - Научная электронная библиотека
2. <http://www.biblioclub.ru/> - Евразийский открытый институт
3. <http://www.net.nns.ru> - /Национальная электронная библиотека
4. <http://www.rsl.ru/> - Российская государственная библиотека
5. <http://www.runivers.ru> - Электронная библиотека Руниверс 35
6. www.garant.ru – Справочная правовая система «Гарант»
7. www.consultant.ru – Справочная правовая система «Консультант Плюс»
8. www.supcourt.ru – Верховный суд Российской Федерации

7. Оценочные средства

7.1. Вопросы к зачету

1. Определение киберправа как комплексной отрасли.
2. Основные группы источников киберправа.
3. Проблема определения юрисдикции в киберпространстве.
4. Трансграничные киберспоры.
5. Правовая природа информации как объекта правоотношений.
6. Цифровое право и примеры его реализации.

7. Правовая специфика регулирования отношений в сети Интернет по сравнению с традиционными правоотношениями.

8. Правовой статус токенов в соответствии с действующим российским законодательством.

9. Правовые способы защиты прав на товарный знак.

10. Особенности охраны авторских прав на произведения, созданные с использованием искусственного интеллекта.

11. База данных как объект авторского права или смежных прав.

12. Свободные лицензии.

13. Существенные условия и порядок заключения договора в электронной форме.

14. Публичная оферта в сети Интернет и требования к ее содержанию.

15. Специфика защита прав потребителей при дистанционном способе продажи товаров.

16. Правовой режим электронной подписи. Разница между простой и усиленной квалифицированной электронной подписью.

17. Атака как форс-мажорное обстоятельство, освобождающее от ответственности за неисполнение обязательств.

18. Принципы обработки персональных данных в сети Интернет.

19. Права субъекта персональных данных и механизмы их реализации.

20. Особый порядок обработки биометрических персональных данных.

21. Правовые последствия утечки персональных данных для оператора.

22. Безопасность критической информационной инфраструктуры.

23. «Права на забвение» в российском законодательстве, механизм его реализации.

24. Пределы использования систем видеоаналитики с распознаванием лиц в публичных пространствах.

25. Уголовно-правовая характеристика преступлений в сфере компьютерной информации.

26. Мошеннические действия, совершенные с использованием информационно-телекоммуникационных технологий.

27. Особенности сбора и процессуального закрепления электронных доказательств.

28. Составы административных правонарушений в информационной сфере.

29. Проблема атрибуции кибератаки и как она влияет на привлечение к ответственности.
30. Основные подходы к проблеме правосубъектности искусственного интеллекта.
31. Ответственность за вред, причиненный действиями (решениями) автономной системы с элементами ИИ.
32. «Цифровой суверенитет» государства, правовые инструменты его обеспечения.
33. Основные модели государственного регулирования интернет-пространства.
34. Правовые основы оказания государственных и муниципальных услуг в электронной форме.

Образец билета к зачету.

**Грозненский государственный нефтяной технический университет им.акад. М.Д.
Миллионщикова
Институт ""
Группа "" Семестр "3"
Дисциплина "Киберправо"
Билет № 1**

1. Цифровое право и примеры его реализации.
2. Принципы обработки персональных данных в сети Интернет.

Подпись преподавателя _____ Подпись заведующего кафедрой _____

7.2. Текущий контроль

Задача 1. Юрисдикция и трансграничный спор

Ситуация: Российская онлайн-школа, разместившая свои курсы на платформе Teachable (зарегистрирована в США), обнаружила, что её авторский контент массово копируется и продаётся через сайт, хостинг которого находится в Нидерландах, а владелец предположительно является резидентом Беларуси. Ученики школы — граждане России и Казахстана.

Задание для студента: Составьте план действий для защиты прав школы. Определите, правоприменимые нормы какой страны (РФ, США, Нидерландов) будут наиболее благоприятны для подачи иска о нарушении авторских прав? Какова вероятность привлечения информационного посредника (хостера) к ответственности по российскому праву?

Задача 2. Утечка персональных данных и взаимодействие с регулятором

Ситуация: Небольшой интернет-магазин детских товаров стал жертвой хакерской атаки. Утечке подверглась база данных, содержащая ФИО, адреса электронной почты, номера телефонов и адреса доставки 50 000 клиентов. Пароли были зашифрованы. Атака обнаружена сегодня.

Задание для студента: Вы — юрист компании. Каковы ваши первые конкретные действия в соответствии с 152-ФЗ? В какой срок и в каком формате необходимо уведомить Роскомнадзор? Нужно ли уведомлять самих субъектов ПДн? Составьте черновик обязательного уведомления для регулятора.

Задача 3. Ответственность платформы

Ситуация: На маркетплейсе пользователь разместил объявление о продаже устройства для радиозахвата GSM-сигналов, оборот которого в РФ ограничен. После получения жалобы от правообладателя патента маркетплейс удалил объявление через 5 дней. Правообладатель требует возместить убытки, ссылаясь на ст. 1253.1 ГК РФ.

Задание для студента: Дайте правовую оценку. Будет ли нести ответственность маркетплейс как информационный посредник? Проанализируйте условия освобождения от ответственности по ст. 1253.1 ГК РФ. Учитывайте характер товара и сроки реакции.

Задача 4. Квалификация киберинцидента

Ситуация: Бывший IT-сотрудник компании «ГазНефтьСервис», используя сохранившийся у него логин и пароль коллеги, вошёл во внутреннюю систему и скопировал на внешний носитель архив технической документации, содержащий коммерческую тайну. Сделать это ему удалось, так как пароль коллеги был простым, а система не требовала двухфакторной аутентификации.

Задание для студента: Квалифицируйте действия бывшего сотрудника по УК РФ. Есть ли состав преступления по ст. 272 УК РФ (неправомерный доступ)? Можно ли говорить о халатности со стороны компании или самого коллеги, чей аккаунт был использован?

Задача 5. Смарт-контракт и «цифровые права»

Ситуация: В рамках пилотного проекта, два юридических лица заключили сделку купли-продажи партии товара через блокчейн-платформу, используя смарт-контракт. Условия: оплата автоматически переводится продавцу при подтверждении датчиком факта прибытия груза на склад покупателя. Датчик дал сбой, подтвердив прибытие, хотя груз был в пути. Деньги переведены, продавец их вывел.

Задание для студента: Проанализируйте правовую природу отношений. Можно ли оспорить исполнение смарт-контракта по правилам ГК РФ о недействительности сделок (заблуждение, обман) или на основании его ненадлежащего исполнения? Кто и как может нести риск технического сбоя?

Задача 6. Правовые риски использования ИИ в HR

Ситуация: Крупный банк внедрил систему AI-скоринга для первичного отбора резюме. Система была обучена на данных по успешным сотрудникам за последние 10 лет. В результате она стала систематически отсеивать резюме женщин в возрасте 25-35 лет (статистически чаще уходивших в декрет в обучающей выборке) и выпускников определённых региональных ВУЗов. Один из кандидатов, получивший автоматический отказ, требует разъяснений.

Задание для студента: Составьте юридическое заключение о правовых рисках использования такой системы. Укажите, какие нормы трудового права, закона о персональных данных и о запрете дискриминации могут быть нарушены. Какие меры (технические и организационные) должна принять компания для их минимизации?

Задача 7. Спор о доменном имени и товарном знаке

Ситуация: Компания «Зелёный мир», производитель экотоваров (зарегистрировала товарный знак «ECO LIFE»), обнаружила сайт ecolife.su, на котором продаются товары конкурентов. Владелец домена — индивидуальный предприниматель Иванов, который утверждает, что «есо» и «life» — общеупотребительные слова, а домен он зарегистрировал раньше, чем компания получила свидетельство на товарный знак.

Задание для студента: Подготовьте правовую аргументацию для подачи заявления в арбитражный центр для доменных споров. Оцените шансы на принудительный перевод домена. Какие дополнительные доказательства необходимо собрать?

Задача 8. Атака как форс-мажор

Ситуация: Интернет-магазин не смог выполнить тысячи заказов в день распродажи, потому что его сайт был выведен из строя масштабной атакой. В договоре с потребителями есть пункт об ответственности за задержку. Магазин ссылается на форс-мажор (п. 3 ст. 401 ГК РФ). Потребители требуют неустойку.

Задание для студента: Дайте правовую оценку. Можно ли считать атаку непреодолимой силой для целей освобождения от ответственности? Какие условия должен доказать магазин (например, наличие надлежащих мер защиты)? Каковы могут быть аргументы потребителей?

Задача 9. Краудфандинг и ответственность создателя

Ситуация: Разработчик собрал на краудфандинг-платформе 5 млн рублей на создание «умной» кружки с подогревом. Спустя 2 года после запланированного срока доставки заказчики получили неработающие прототипы. Создатель заявляет, что все деньги ушли на НИОКР и производство, он действовал добросовестно, но технологические трудности не позволили выполнить обещания.

Задание для студента: определите правовую природу отношений между создателем и заказчиками (дарение, предварительный договор купли-продажи, иное). Какие способы защиты есть у заказчиков? Можно ли привлечь создателя к гражданско-правовой или уголовной ответственности? Проанализируйте оферту платформы.

Задача 10. Права на объекты культуры

Ситуация: Цифровой художник создал токен, используя в качестве основного визуального элемента отсканированное и цифровое обработанное изображение знаменитой советской картины из собрания государственного музея. Музей, обладающий неимущественными правами на произведение (право на защиту репутации автора, право доступа), требует прекратить продажи, утверждая, что это искажает восприятие оригинала и нарушает его права.

Задание для студента: Проанализируйте конфликт. Какие права художника и какие права музея/наследников автора картины здесь задействованы? Применимо ли здесь исключение о свободе панорамы? Является ли токен новым произведением (производным объектом) или просто копией?

7.3. Описание показателей и критериев оценивания компетенций на различных этапах и формирования, описание шкалы оценивания.

Таблица 6

Планируемые результаты освоения компетенции	Критерии оценивания результатов обучения				Наименование оценочного средства
	Менее 41 баллов (неудовлетворительно)	41-60 баллов (удовлетворительно)	61-80 баллов (хорошо)	81-100 баллов (отлично)	
ПК-2. Способен квалифицированно применять нормативные правовые акты в конкретных сферах юридической деятельности, реализовывать нормы материального и процессуального права в профессиональной деятельности					
Знать: нормы материального и процессуального права.	Фрагментарные знания	Неполные знания	Сформированные, но содержащие отдельные пробелы знания	Сформированные систематические знания	опрос, практические задания, темы рефератов, темы докладов, тестовые задания.
Уметь: реализовать нормы материального и процессуального права в профессиональной деятельности.	Частичные умения	Неполные умения	Умения полные, допускаются небольшие ошибки	Сформированные знания	опрос, практические задания, темы рефератов, темы докладов, тестовые задания.
Владеть: навыками работы с правовыми актами, на основе их анализа принимает решения о реализации норм материального и процессуального права в профессиональной деятельности.	Частичное владение навыками	Несистематическое применение навыков	В систематическом применении навыков допускаются пробелы	Успешное и систематическое применение навыков	опрос, практические задания, темы рефератов, темы докладов, тестовые задания.
ПК-5. Способен защищать права и законные интересы субъектов права					

Знать: законодательство в сфере информационных технологий, киберпреступности, формы и способы защиты нарушенных прав и особенности их применения.	Фрагментарные знания	Неполные знания	Сформированные, но содержащие отдельные пробелы знания	Сформированные, систематические знания	опрос, практические задания, темы рефератов, темы
Уметь: применять нормы закона в области информационной безопасности.	Частичные умения	Неполные умения	Умения полные, допускаются небольшие ошибки	Сформированные умения	опрос, практические задания, темы рефератов, темы докладов, тестовые задания.
Владеть: навыками анализа и применения нормативных правовых актов в сфере информационной безопасности.	Частичное владение навыками	Несистематическое применение навыков	В систематическом применении навыков допускаются пробелы	Успешное и систематическое применение навыков	опрос, практические задания, темы рефератов, темы докладов, тестовые задания.

8. Особенности реализации дисциплины для инвалидов и лиц с ограниченными возможностями здоровья

Для осуществления процедур текущего контроля успеваемости и промежуточной аттестации обучающихся созданы фонды оценочных средств, адаптированные для инвалидов и лиц с ограниченными возможностями здоровья и позволяющие оценить достижение ими запланированных в основной образовательной программе результатов обучения и уровень сформированности всех компетенций, заявленных в образовательной программе. Форма проведения текущей аттестации для студентов-инвалидов устанавливается с учетом индивидуальных психофизических особенностей (устно, письменно на бумаге, письменно на компьютере, в форме тестирования и т.п.). При тестировании для слабовидящих студентов используются фонды оценочных средств с укрупненным шрифтом. На экзамен приглашается сопровождающий, который обеспечивает техническое сопровождение студенту. При необходимости студенту-инвалиду предоставляется дополнительное время для подготовки ответа на экзамене (или зачете). Обучающиеся с ограниченными возможностями здоровья, и обучающиеся инвалиды обеспечиваются печатными и электронными образовательными ресурсами (программы, учебные пособия для самостоятельной работы и т.д.) в формах, адаптированных к ограничениям их здоровья и восприятия информации:

1) для инвалидов и лиц с ограниченными возможностями здоровья по зрению:

- для слепых: задания для выполнения на семинарах и практических занятиях оформляются рельефно-точечным шрифтом Брайля или в виде электронного документа, доступного с помощью компьютера со специализированным программным обеспечением для слепых, либо зачитываются ассистентом; письменные задания выполняются на бумаге рельефно-точечным шрифтом Брайля или на компьютере со специализированным программным обеспечением для слепых либо надиктовываются ассистенту; обучающимся для выполнения задания при необходимости предоставляется комплект письменных принадлежностей и бумага для письма рельефно-точечным шрифтом Брайля, компьютер со специализированным программным обеспечением для слепых;

- для слабовидящих: обеспечивается индивидуальное равномерное освещение не менее 300 люкс; обучающимся для выполнения задания при необходимости предоставляется увеличивающее устройство; возможно также использование собственных увеличивающих устройств; задания для выполнения заданий оформляются увеличенным шрифтом;

2) для инвалидов и лиц с ограниченными возможностями здоровья по слуху:

- для глухих и слабослышащих: обеспечивается наличие звукоусиливающей аппаратуры коллективного пользования, при необходимости обучающимся предоставляется

звукоусиливающая аппаратура индивидуального пользования; предоставляются услуги сурдопереводчика;

- для слепоглухих допускается присутствие ассистента, оказывающего услуги тифлсурдопереводчика (помимо требований, выполняемых соответственно для слепых и глухих);

3) для лиц с тяжелыми нарушениями речи, глухих, слабослышащих лекции и семинары, проводимые в устной форме, проводятся в письменной форме;

4) для инвалидов и лиц с ограниченными возможностями здоровья, имеющих нарушения опорно-двигательного аппарата:

- для лиц с нарушениями опорно-двигательного аппарата, нарушениями двигательных функций верхних конечностей или отсутствием верхних конечностей: письменные задания выполняются на компьютере со специализированным программным обеспечением или надиктовываются ассистенту; выполнение заданий (тестов, контрольных работ), проводимые в письменной форме, проводятся в устной форме путем опроса, беседы с обучающимся.

9. Учебно-методическое и информационное обеспечение дисциплины

Основная литература:

1. Спешаков, Александр Геннадьевич. Информационная безопасность: учебное пособие: [для студентов, обучающихся по специальностям 100301 «Информационная безопасность», 400301 «Юриспруденция», 380301 «Экономика»] / А.Г. Спешаков, М.О. Таныгин, В.С. Панищев; Юго-Зап. Гос. Ун-т.- Курск: ЮЗГУ, 2017. – 196 с.

2. Киберправо: учебное пособие/ А. Н. Леонтьев; ВолгГТУ. – Волгоград, 2021. – 80 с. ISBN 978-5-9948-4110-5

3. Бегишев И.Р., Латыпова Э.Ю., Кирпичников Д.В. Искусственный интеллект как правовая категория: доктринальный подход к разработке дефиниции // Актуальные проблемы экономики и права. 2020. Т. 14. № 1.

Дополнительная литература:

4. Борисов С. Преступления в сфере компьютерной информации: монография - Москва: Лаборатория книги, 2010.

5. Милашевская Е. С. Уголовная ответственность за преступления в сфере компьютерной информации: монография - Москва: Лаборатория книги, 2012.

10 Методические указания для обучающихся по освоению дисциплины (Приложение).

11. Материально-техническое обеспечение дисциплины

Помещения для всех видов работ, предусмотренных учебным планом, укомплектованы необходимой специализированной учебной мебелью и техническими средствами обучения:

- столы, стулья;
- персональный компьютер / ноутбук (переносной);
- проектор;
- экран / интерактивная доска.

Составитель:

к. ю. н., зав. кафедры «Юриспруденция»



М.Р. Богатырев

Согласовано:

и.о. Зав. выпускающей кафедрой

«Юриспруденция»



М.Р. Богатырев

Директор ДУМР



М.А. Магомаева

Методические указания по освоению дисциплины «Киберправо»

1. Методические указания для обучающихся по планированию и организации времени, необходимого для освоения дисциплины.

Изучение рекомендуется начать с ознакомления с рабочей программой дисциплины, ее структурой и содержанием разделов (модулей), фондом оценочных средств, ознакомиться с учебно-методическим и информационным обеспечением дисциплины.

Дисциплина «Киберправо» состоит из 9 связанных между собою тем, обеспечивающих последовательное изучение материала.

Обучение по дисциплине «Киберправо» осуществляется в следующих формах:

1. Аудиторные занятия (лекции, практические занятия).
2. Самостоятельная работа студента (подготовка к лекциям, практическим занятиям, тестам/рефератам/докладам/, и иным формам письменных работ, выполнение анализа кейсов, индивидуальная консультация с преподавателем).

Описание последовательности действий обучающегося:

При изучении курса следует внимательно слушать и конспектировать материал, излагаемый на аудиторных занятиях. Для его понимания и качественного усвоения рекомендуется следующая последовательность действий:

1. После окончания учебных занятий для закрепления материала просмотреть и обдумать текст лекции, прослушанной сегодня, разобрать рассмотренные примеры (10 – 15 минут).
2. При подготовке к лекции следующего дня повторить текст предыдущей лекции, подумать о том, какая может быть следующая тема (10 - 15 минут).
3. В течение недели выбрать время для работы с литературой в библиотеке (по 1 часу).
4. При подготовке к практическому/ семинарскому занятию повторить основные понятия по теме, изучить примеры. Решая конкретную ситуацию, - предварительно понять, какой теоретический материал нужно использовать. Наметить план решения, попробовать на его основе решить 1 - 2 практические ситуации (лаб. работы).

2. Методические указания по работе обучающихся во время проведения лекций.

Лекции дают обучающимся систематизированные знания по дисциплине, концентрируют их внимание на наиболее сложных и важных вопросах. Лекции обычно излагаются в традиционном или в проблемном стиле. Для студентов в большинстве случаев в проблемном стиле. Проблемный стиль позволяет стимулировать активную познавательную деятельность обучающихся и их интерес к дисциплине, формировать творческое мышление,

активизировать внимание обучающихся путем постановки проблемных вопросов, поощрять дискуссию.

Во время лекционных занятий рекомендуется вести конспектирование учебного материала, обращать внимание на формулировки и категории, раскрывающие суть того или иного явления, или процессов, выводы и практические рекомендации.

Конспект лекции лучше подразделять на пункты, соблюдая красную строку. Этому в большой степени будут способствовать вопросы плана лекции, предложенные преподавателям. Следует обращать внимание на акценты, выводы, которые делает преподаватель, отмечая наиболее важные моменты в лекционном материале замечаниями «важно», «хорошо запомнить» и т.п. Можно делать это и с помощью разноцветных маркеров или ручек, подчеркивая термины и определения.

Целесообразно разработать собственную систему сокращений, аббревиатур и символов. Однако при дальнейшей работе с конспектом символы лучше заменить обычными словами для быстрого зрительного восприятия текста.

Работая над конспектом лекций, необходимо использовать не только основную литературу, но и ту литературу, которую дополнительно рекомендовал преподаватель. Именно такая серьезная, кропотливая работа с лекционным материалом позволит глубоко овладеть теоретическим материалом.

Тематика лекций дается в рабочей программе дисциплины.

3. Методические указания обучающимся по подготовке к практическим занятиям.

На практических занятиях приветствуется активное участие в обсуждении конкретных ситуаций, способность на основе полученных знаний находить наиболее эффективные решения поставленных проблем, уметь находить полезный дополнительный материал по тематике семинарских занятий.

Студенту рекомендуется следующая схема подготовки к семинарскому занятию:

1. Ознакомление с планом практических занятий, который отражает содержание предложенной темы;
2. Проработать конспект лекций;
3. Прочитать основную и дополнительную литературу.

В процессе подготовки к практическим занятиям, необходимо обратить особое внимание на самостоятельное изучение рекомендованной литературы. При всей полноте конспектирования лекции в ней невозможно изложить весь материал из-за лимита аудиторных часов. Поэтому самостоятельная работа с учебниками, учебными пособиями, научной, справочной литературой, материалами периодических изданий и Интернета является наиболее эффективным методом получения дополнительных знаний, позволяет значительно

активизировать процесс овладения информацией, способствует более глубокому усвоению изучаемого материала, формирует у студентов отношение к конкретной проблеме. Все новые понятия по изучаемой теме необходимо выучить наизусть и внести в глоссарий, который целесообразно вести с самого начала изучения курса;

4. Ответить на вопросы плана практических занятиях;
5. Выполнить домашнее задание;
6. Проработать тестовые задания и задачи;
7. При затруднениях сформулировать вопросы к преподавателю.

Результат такой работы должен проявиться в способности студента свободно ответить на теоретические вопросы, выступать и участвовать в коллективном обсуждении вопросов изучаемой темы, правильно выполнять задания на практических занятиях, которые даются в фонде оценочных средств дисциплины.

4. Методические указания обучающимся по организации самостоятельной работы.

Цель организации самостоятельной работы по дисциплине «Киберправо» — это углубление и расширение знаний в области фундаментальных исследований; формирование навыка и интереса к самостоятельной познавательной деятельности.

Самостоятельная работа обучающихся является важнейшим видом освоения содержания дисциплины, подготовки к практическим занятиям и к контрольной работе. Сюда же относятся и самостоятельное углубленное изучение тем дисциплины. Самостоятельная работа представляет собой постоянно действующую систему, основу образовательного процесса и носит исследовательский характер, что послужит в будущем основанием для написания выпускной квалификационной работы, практического применения полученных знаний.

Организация самостоятельной работы обучающихся ориентируется на активные методы овладения знаниями, развитие творческих способностей, переход от поточного к индивидуализированному обучению, с учетом потребностей и возможностей личности.

Правильная организация самостоятельных учебных занятий, их систематичность, целесообразное планирование рабочего времени позволяет студентам развивать умения и навыки в усвоении и систематизации приобретаемых знаний, обеспечивать высокий уровень успеваемости в период обучения, получить навыки повышения профессионального уровня.

Подготовка к практическим занятиям включает, кроме проработки конспекта и презентации лекции, поиск литературы (по рекомендованным спискам и самостоятельно), подготовку заготовок для выступлений по вопросам, выносимым для обсуждения по конкретной теме. Такие заготовки могут включать цитаты, факты, сопоставление различных позиций, собственные мысли. Если проблема заинтересовала обучающегося, он может подготовить реферат и выступить с ним на практическом занятии. При подготовке к

контрольной работе обучающийся должен повторять пройденный материал в строгом соответствии с учебной программой, используя конспект лекций и литературу, рекомендованную преподавателем. При необходимости можно обратиться за консультацией и методической помощью к преподавателю.

Самостоятельная работа реализуется:

- непосредственно в процессе аудиторных занятий - на лекциях, практических занятиях;
- в контакте с преподавателем вне рамок расписания - на консультациях по учебным вопросам, в ходе творческих контактов, при ликвидации задолженностей, при выполнении индивидуальных заданий и т.д.
- в библиотеке, дома, на кафедре при выполнении обучающимся учебных и практических задач.

Виды СРС и критерии оценок

(по балльно-рейтинговой системе ГГНТУ)

1. Реферат
2. Доклад
3. Участие в мероприятиях

Темы для самостоятельной работы прописаны в рабочей программе дисциплины. Эффективным средством осуществления обучающимся самостоятельной работы является электронная информационно-образовательная среда университета, которая обеспечивает доступ к учебным планам, рабочим программам дисциплин (модулей), практик, к изданиям электронных библиотечных систем.