

Документ подписан простой электронной подписью

Информация о владельце:

ФИО: Минцаев Магомед Шавалович

Должность: Ректор

Дата подписания: 19.07.2026 10:17:18

Уникальный программный ключ:

736bce35c296f119d6aafdc22836b21db52dbc07971a86865a5825f9fa4304ce

**МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ
ФЕДЕРАЦИИ**

**ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ
УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ**

**«ГРОЗНЕНСКИЙ ГОСУДАРСТВЕННЫЙ НЕФТЯНОЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ
ИМЕНИ АКАДЕМИКА М.Д. МИЛЛИОНЩИКОВА»**

Кафедра «Юриспруденция»

УТВЕРЖДЕН

на заседании кафедры

« 04 » 05 2026 г., протокол № 9

и.о. Зав. кафедрой



М.Р. Богатырев

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ПО УЧЕБНОЙ ДИСЦИПЛИНЕ

Киберправо

Направление подготовки

40.04.01 «Юриспруденция»

Направленность (профиль)

«Юриспруденция»

Квалификация

Магистр

Составитель



М.Р. Богатырев

Грозный – 2026

**ПАСПОРТ
ФОНДА ОЦЕНОЧНЫХ СРЕДСТВ ПО УЧЕБНОЙ ДИСЦИПЛИНЕ
Киберправо**

№ п/п	Контролируемые разделы (темы) дисциплины	Код контролируемой компетенции (или ее части)	Наименование оценочного средства
1.	Введение в киберправо: предмет, метод, система и источники.	ПК-2	Тестовые задания; реферат
2.	Юрисдикция и применимое право в киберпространстве.	ПК-5	Тестовые задания; реферат
3.	Правовой режим цифровых данных и информационных объектов.	ПК-2	Тестовые задания; реферат
4.	Право интеллектуальной собственности в цифровой среде.	ПК-2	Тестовые задания; реферат
5.	Правовое регулирование интернет-коммуникаций и электронной коммерции.	ПК-5	Тестовые задания; реферат
6.	Правовые основы информационной безопасности и кибербезопасности.	ПК-5	Тестовые задания; реферат
7.	Киберпреступность и административно-правовые нарушения в цифровой среде.	ПК-5	Тестовые задания; реферат
8.	Правовое регулирование искусственного интеллекта и робототехники.	ПК-5	Тестовые задания; реферат
9.	Право в сфере биометрии и больших данных.	ПК-5	Тестовые задания; реферат

ПРИМЕРНЫЙ ПЕРЕЧЕНЬ ОЦЕНОЧНЫХ СРЕДСТВ

№ п/п	Наименование оценочного средства	Краткая характеристика оценочного средства	Представление оценочного средства в фонде
1	Тест	Средство проверки полученных знаний по пройденным темам или разделам учебной дисциплины.	Комплект тестовых заданий
2	Реферат	Продукт самостоятельной работы студента, представляющий собой публичное выступление по решению определенной учебно-практической, учебно- исследовательской или научной темы.	Темы рефератов
3	Зачет	Промежуточная форма оценки	Комплект билетов к зачету

Темы 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.

Критерии оценивания рефератов

- **0 баллов** *выставляется студенту, если подготовлен некачественный реферат: тема не раскрыта, в изложении отсутствует четкая структура, логическая последовательность, отражающая сущность раскрываемых понятий, теорий, явлений.*
- **1- балл** *выставляется студенту, если подготовлен некачественный реферат: тема раскрыта, однако в изложении отсутствует четкая структура, отражающая сущность раскрываемых понятий, теорий, явлений.*
- **2 балла** *выставляется студенту, если подготовлен качественный реферат: тема хорошо раскрыта, в изложении прослеживается четкая структура, логическая последовательность, отражающая сущность раскрываемых понятий, теорий, явлений. Однако студент недостаточно владеет подготовленным материалом.*
- **3 балла** *выставляется студенту, если подготовлен качественный реферат: тема хорошо раскрыта, в изложении прослеживается четкая структура, логическая последовательность, отражающая сущность раскрываемых понятий, теорий, явлений. Студент хорошо апеллирует терминами науки. Однако затрудняется ответить на дополнительные вопросы по теме реферата (1-2 вопроса).*
- **4 балла** *выставляется студенту, если подготовлен качественный реферат: тема хорошо раскрыта, в изложении прослеживается четкая структура логическая последовательность, отражающая сущность раскрываемых понятий, теорий, явлений. Студент свободно апеллирует терминами науки. Однако на дополнительные вопросы по теме реферата (1-2 вопроса) отвечает только с помощью преподавателя.*
- **5 баллов** *выставляется студенту, если подготовлен качественный реферат: тема хорошо раскрыта, в изложении прослеживается четкая структура логическая последовательность, отражающая сущность раскрываемых понятий, теорий, явлений. Студент свободно апеллирует терминами науки, демонстрирует авторскую позицию. Способен ответить на дополнительные вопросы по теме реферата (1-2 вопроса).*

КОНТРОЛЬНО-ИЗМЕРИТЕЛЬНЫЕ МАТЕРИАЛЫ ПО ДИСЦИПЛИНЕ
«Киберправо»

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.

**Тестовые задания к текущему контролю по дисциплине
«Киберправо»**

Первая текущая аттестация:

Вариант 1

1. Какой ФЗ в РФ устанавливает правовой режим для сделок с цифровыми финансовыми активами?

- А) Федеральный закон «Об информации, информационных технологиях и о защите информации» №149-ФЗ;
- В) Федеральный закон «О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации» №259-ФЗ;
- С) Федеральный закон «О персональных данных» №152-ФЗ;

2. Какую ответственность влечет за собой неправомерный доступ к компьютерной информации, если это повлекло ее уничтожение, блокирование или модификацию?

- А) Только административную ответственность по КоАП РФ
- В) Только дисциплинарную ответственность по Трудовому Кодексу
- С) Уголовную ответственность по УК РФ

3. Какое определение соответствует термину «электронная подпись» согласно Федеральному закону № 63-ФЗ?

- А) Информация в электронной форме, присоединенная к другой информации и используемая для определения лица, подписавшего информацию
- В) Отсканированное изображение собственноручной подписи, вставленное в текст документа
- С) Код подтверждения, отправляемый на номер мобильного телефона при входе в личный кабинет

4. Какой федеральный орган исполнительной власти в РФ осуществляет функции по контролю и надзору в сфере обработки персональных данных?

- А) Министерство цифрового развития, связи и массовых коммуникаций РФ
- В) Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор)
- С) Федеральная служба безопасности РФ (ФСБ)

5. Сколько статей в Уголовном кодексе РФ включены в главу о преступлениях в сфере компьютерной информации?

- А) Три
- В) Пять
- С) Семь

6. К объектам авторских прав, охраняемым Гражданским кодексом РФ, относятся программы для ЭВМ и базы данных?

- А) Нет, они охраняются как изобретения патентным правом
- В) Искключительно в течение 7 дней
- В) Да, они охраняются как литературные произведения
- С) Только в случае их государственной регистрации в Роспатенте

7. На какой максимальный срок может быть ограничен доступ к информационному ресурсу, распространяющему запрещенную информацию, по решению Роскомнадзора во внесудебном порядке (по ст. 15.1 ФЗ № 149-ФЗ)?

- А) До 24 часов для принятия оперативных мер
- В) До истечения срока делегирования доменного имени
- С) Такое решение вообще не может приниматься — только по решению суда

8. Какой знак используется правообладателем для оповещения об авторском праве на программу для ЭВМ?

- A) ®
- B) ©
- C) ™

9. Что из перечисленного является «фишингом» как видом киберпреступления?

- A) Распространение спам-рассылок рекламного характера
- B) Создание поддельных веб-сайтов или сообщений для получения конфиденциальных данных пользователей (логинов, паролей, данных банковских карт)
- C) Целенаправленная DDoS-атака на сервер компании с целью вымогательства

10. Что из перечисленного относится к основным аспектам (свойствам) информационной безопасности?

- A) Дискретность и секретность
- B) Конфиденциальность, целостность и доступность
- C) Устойчивость, открытость и надежность

Вариант 2

1. Кто из перечисленных лиц может быть признан автором служебного произведения — программы для ЭВМ, созданной в вузе по договору с коммерческим заказчиком?

- А) Только штатные преподаватели вуза, участвовавшие в разработке
- В) Только заказчик, оплативший разработку
- С) Штатные преподаватели, аспиранты и студенты, если их творческий труд был использован для создания программы

2. Что из перечисленного является основным риском для заказчика при использовании в разрабатываемом программном обеспечении Open Source кода (например, библиотек, распространяемых под лицензией GPL)?

- А) Невозможность защитить программу авторским правом
- В) Обязанность раскрыть исходный код всего производного программного продукта (эффект «вирусной лицензии»)
- С) Запрет на коммерческое использование программы

3. Какое понятие в международном киберправе означает метод скрытой передачи информации, при котором сам факт передачи маскируется внутри другого, безобидного файла (изображения, аудио, видео)?

- А) криптоанализ
- В) стеганография
- С) фишинг

4. Какой федеральный закон РФ регулирует вопросы безопасности критической информационной инфраструктуры (КИИ)?

- А) Федеральный закон № 149-ФЗ «Об информации...»
- В) Федеральный закон № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации»
- С) Федеральный закон № 152-ФЗ «О персональных данных»

5. Какой метод борьбы с компьютерными вирусами относится к интеллектуальным (основан на системах логического вывода для выявления вредоносного поведения по коду программы)?

- А) Сигнатурный метод (поиск по известным сигнатурам вирусов)
- В) Эвристический (интеллектуальный) анализ поведения программы
- С) Аппаратная блокировка портов ввода-вывода

6. Кто является уполномоченным органом в РФ, на который возложено руководство работами в области криптографической защиты информации?

- А) Федеральная служба безопасности (ФСБ)
- В) Министерство цифрового развития, связи и массовых коммуникаций
- С) Федеральная служба по техническому и экспортному контролю (ФСТЭК)

7. Что из перечисленного относится к кибертерроризму как к виду киберпреступности?

- А) Кража банковских данных с использованием фишинговой рассылки
- В) Политически мотивированные атаки на критическую информационную инфраструктуру, создающие угрозу гибели людей или тяжких последствий
- С) Распространение ложной информации о компании с целью подрыва ее репутации

8. Согласно российскому законодательству, какие права имеют граждане на доступ к государственным информационным ресурсам?

- А) Равные права, и они не обязаны обосновывать перед владельцем ресурса необходимость получения запрашиваемой информации
- В) Разные права в зависимости от социального статуса
- С) Равные права, но обязаны обосновать необходимость получения информации

9. Что из перечисленного НЕ является объектом авторских прав согласно российскому законодательству о программах для ЭВМ и базах данных?

- А) Программа для ЭВМ как результат творческой деятельности автора
- В) База данных, являющаяся результатом творческой деятельности
- С) Идеи и принципы, лежащие в основе программы или базы данных

10. Может ли быть выдан патент на секретное изобретение в сфере компьютерных технологий в Российской Федерации?

- А) Да, но заявка рассматривается специальным уполномоченным органом (например, ФСБ), а сведения об изобретении не публикуются
- В) Нет, изобретения, содержащие государственную тайну, не патентуются
- С) Да, на общих основаниях с полной публикацией сведений в открытых реестрах

**Вторая текущая аттестация:
Вариант 1**

1. Российский интернет-магазин подвергся хакерской атаке, в результате которой цены на товары были изменены злоумышленниками. Около 100 пользователей успели разместить заказы по ценам, установленным хакерами, и получили подтверждение на электронную почту. На следующий день магазин аннулировал заказы. Пользователи обратились в суд. Каковы правовые последствия данной ситуации?

- А) Пользователи вправе требовать исполнения договора, поскольку хакерская атака не освобождает магазин от ответственности за обеспечение безопасности сайта
- В) Магазин вправе аннулировать заказы, так как договор считается незаключенным из-за отсутствия согласования цены (цена была установлена неуполномоченным лицом)
- С) Пользователи не могут требовать исполнения договора, так как заказы были сделаны в ночное время

2. Кто из перечисленных лиц может быть признан автором программного решения с элементами машинного обучения, разработанного вузом по договору с коммерческим заказчиком?

- А) Только штатные преподаватели вуза, участвовавшие в разработке
- В) Только заказчик, оплативший разработку
- С) Штатные преподаватели, аспиранты и студенты, если их творческий труд был использован для создания программы

3. Что такое «доксинг» как вид киберпреступления?

- А) Сбор персональной информации о человеке и ее публикация без согласия, часто с целью преследования или шантажа
- В) Атака на сервер с целью вывода его из строя
- С) Распространение фишинговых ссылок через мессенджеры

4. Какой федеральный орган исполнительной власти в РФ осуществляет руководство работами в области криптографической защиты информации?

- А) Федеральная служба по техническому и экспортному контролю (ФСТЭК)
- В) Федеральная служба безопасности (ФСБ)
- С) Министерство цифрового развития, связи и массовых коммуникаций (Минцифра)

5. Что такое «интеллектуальные методы» борьбы с компьютерными вирусами?

- А) Поиск по известным сигнатурам вирусов, внесенным в антивирусные базы
- В) Методы, основанные на системах логического вывода для определения алгоритма программы по ее коду и выявления программ, осуществляющих несанкционированный доступ
- С) Аппаратная блокировка портов ввода-вывода

6. Что из перечисленного относится к классической «триаде информационной безопасности»?

- А) Дискретность, секретность и открытость
- В) Конфиденциальность, целостность и доступность
- С) Устойчивость, надежность и актуальность

7. Что представляет собой стеганография в контексте киберправа?

- А) Метод шифрования информации с использованием асимметричного ключа
- В) Маскировку самого факта скрытой передачи сообщений по незащищенным каналам связи, при которой информация прячется внутри безобидного файла (изображения, аудио, видео)
- С) Способ кодирования информации с использованием специальных символов

8. Что означает понятие «трансграничная передача персональных данных»?

- А) Передача персональных данных внутри одного федерального округа РФ
- В) Передача персональных данных на территорию иностранного государства органу власти иностранного государства, иностранному физическому лицу или иностранному юридическому лицу
- С) Передача персональных данных между коммерческими организациями в рамках одного холдинга

9. Какой федеральный закон РФ устанавливает правовой режим для сбора и обработки персональных данных?

- А) Федеральный закон «Об информации, информационных технологиях и о защите информации» № 149-ФЗ
- В) Федеральный закон «О персональных данных» № 152-ФЗ
- С) Федеральный закон «О цифровых финансовых активах» № 259-ФЗ

10. Какие меры безопасности являются критически важными при работе с облачными хранилищами юридических документов?

- А) Отказ от использования облачных хранилищ для любых юридических документов
- В) Регулярное создание резервных копий данных
- С) Отправка всех данных на общедоступные серверы

Вариант 2

- 1. Какое понятие в международном киберправе означает метод скрытой передачи информации, при котором сам факт передачи маскируется внутри другого, безобидного файла (изображения, аудио, видео)?**
 - А) Криптоанализ
 - В) Стеганография
 - С) Фишинг
- 2. Что представляет собой «кликбейт» с точки зрения правового регулирования цифрового контента?**
 - А) Программа для взлома учётных записей пользователей
 - В) Текст или изображение, вызывающие у пользователей желание перейти по предлагаемой гиперссылке (независимо от целей)
 - С) Ссылка на очень полезную и актуальную информацию, распространяемая в спам-рассылках
- 3. Согласно российскому законодательству, могут ли идеи и принципы, лежащие в основе программы для ЭВМ, охраняться авторским правом?**
 - А) Да, охраняются в полном объеме наравне с исходным кодом
 - В) Нет, авторское право не распространяется на идеи и принципы, лежащие в основе программы или базы данных
 - С) Да, но только при условии государственной регистрации
- 4. Какой федеральный орган исполнительной власти в РФ осуществляет координацию работ в области технической защиты информации?**
 - А) Федеральная служба безопасности (ФСБ)
 - В) Министерство цифрового развития, связи и массовых коммуникаций
 - С) Федеральная служба по техническому и экспортному контролю (ФСТЭК)
- 5. В чем заключается основная причина уязвимости информационных систем, связанная с человеческим фактором?**
 - А) Недостаточная производительность серверного оборудования
 - В) Ошибки, невнимательность или недостаточная квалификация пользователей и администраторов
 - С) Отсутствие лицензионного антивирусного программного обеспечения
- 6. Что означает понятие «трансграничная передача персональных данных»?**
 - А) Передача персональных данных внутри одного федерального округа РФ
 - В) Передача персональных данных на территорию иностранного государства органу власти иностранного государства, иностранному физическому лицу или иностранному юридическому лицу
 - С) Передача персональных данных между коммерческими организациями в рамках одного холдинга
- 7. Какой международный документ считается первым универсальным международным договором в сфере киберпреступности, инициированным при участии России и подписанным в 2025 году?**
 - А) Будапештская конвенция о киберпреступности
 - В) Ханойская конвенция ООН против киберпреступности
 - С) Шанхайская конвенция о борьбе с терроризмом
- 8. Пользователь получил электронное письмо, предлагающее для получения информации перейти по ссылке. Ссылка визуально выглядит как адрес известного банка, но при наведении мыши в браузере отображается другой адрес. О каком явлении идет речь?**

- А) Сниффинг (перехват трафика)
- В) Фишинг (поддельный сайт с целью хищения данных)
- С) Доксинг (сбор и публикация персональной информации)

9. Что из перечисленного НЕ относится к объектам авторских прав согласно российскому законодательству о программах для ЭВМ и базах данных?

- А) Программа для ЭВМ как результат творческой деятельности автора
- В) База данных, являющаяся результатом творческой деятельности
- С) Языки программирования и алгоритмы

10. Вопрос по кейсу: Компания разработала программное обеспечение с использованием библиотек с открытым исходным кодом, распространяемых под лицензией GPL (General Public License). Какие обязательства возникают у компании при коммерческом распространении этого ПО?

- А) Нет никаких обязательств, лицензия GPL не налагает ограничений на коммерческое использование
- В) Обязанность раскрыть исходный код всего производного программного продукта (эффект «вирусной лицензии»)
- С) Запрет на коммерческое использование программы в любой форме

Критерии оценки выполнения тестовых заданий:

- 0 баллов – задание не выполнено (не найдено правильное решение).
- 5 баллов - задание выполнено на 50%
- 10 баллов – задание выполнено на 100% (найдено правильное решение).

Баллы за тесты выводятся по следующему критерию - в каждом варианте тестов - 10 вопросов - 1 балл за каждый верный ответ.

Ключи к тестовым заданиям

№	Первая текущая аттестация		Вторая текущая аттестация	
	Вариант №1	Вариант №2	Вариант №1	Вариант №2
1	В	С	А	В
2	С	В	С	В
3	А	В	А	В
4	В	В	В	С
5	В	В	В	В
6	В	А	В	В
7	А	В	В	В
8	В	А	В	В
9	В	С	В	С
10	В	А	В	В

Комплект билетов 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 _____

Грозненский государственный нефтяной технический университет им.акад. М.Д. Миллионщикова

Институт ""

Группа "" Семестр "3"

Дисциплина "Киберправо"

Билет № 2

1. Основные подходы к проблеме правосубъектности искусственного интеллекта.
2. Безопасность критической информационной инфраструктуры.

Подпись преподавателя _____ Подпись заведующего кафедрой _____

Грозненский государственный нефтяной технический университет им.акад. М.Д. Миллионщикова

Институт ""

Группа "" Семестр "3"

Дисциплина "Киберправо"

Билет № 3

1. Правовая специфика регулирования отношений в сети Интернет по сравнению с традиционными правоотношениями.
2. Трансграничные киберспоры.

Подпись преподавателя _____ Подпись заведующего кафедрой _____

Грозненский государственный нефтяной технический университет им.акад. М.Д. Миллионщикова

Институт ""

Группа "" Семестр "3"

Дисциплина "Киберправо"

Билет № 4

1. Атака как форс-мажорное обстоятельство, освобождающее от ответственности за неисполнение обязательств.
2. Определение киберправа как комплексной отрасли.

Подпись преподавателя _____ Подпись заведующего кафедрой _____

Грозненский государственный нефтяной технический университет им.акад. М.Д. Миллионщикова
Институт ""
Группа "" Семестр "3"
Дисциплина "Киберправо"
Билет № 5

1. Основные модели государственного регулирования интернет-пространства.
2. Свободные лицензии.

Подпись преподавателя _____ Подпись заведующего кафедрой _____

Грозненский государственный нефтяной технический университет им.акад. М.Д. Миллионщикова
Институт ""
Группа "" Семестр "3"
Дисциплина "Киберправо"
Билет № 6

1. Проблема атрибуции кибератаки и как она влияет на привлечение к ответственности.
2. Правовая специфика регулирования отношений в сети Интернет по сравнению с традиционными правоотношениями.

Подпись преподавателя _____ Подпись заведующего кафедрой _____

Грозненский государственный нефтяной технический университет им.акад. М.Д. Миллионщикова
Институт ""
Группа "" Семестр "3"
Дисциплина "Киберправо"
Билет № 7

1. Мошеннические действия, совершенные с использованием информационно-телекоммуникационных технологий.
2. Проблема определения юрисдикции в киберпространстве.

Подпись преподавателя _____ Подпись заведующего кафедрой _____

Грозненский государственный нефтяной технический университет им.акад. М.Д. Миллионщикова
Институт ""
Группа "" Семестр "3"
Дисциплина "Киберправо"
Билет № 8

1. Публичная оферта в сети Интернет и требования к ее содержанию.
2. Трансграничные киберспоры.

Подпись преподавателя _____ Подпись заведующего кафедрой _____

Грозненский государственный нефтяной технический университет им.акад. М.Д. Миллионщикова
Институт ""

Группа "" Семестр "3"
Дисциплина "Киберправо"
Билет № 9

1. Ответственность за вред, причиненный действиями (решениями) автономной системы с элементами ИИ.
2. Публичная оферта в сети Интернет и требования к ее содержанию.

Подпись преподавателя _____ Подпись заведующего кафедрой _____

Грозненский государственный нефтяной технический университет им.акад. М.Д. Миллионщикова
Институт ""
Группа "" Семестр "3"
Дисциплина "Киберправо"
Билет № 10

1. Основные подходы к проблеме правосубъектности искусственного интеллекта.
2. Правовые последствия утечки персональных данных для оператора.

Подпись преподавателя _____ Подпись заведующего кафедрой _____

Грозненский государственный нефтяной технический университет им.акад. М.Д. Миллионщикова
Институт ""
Группа "" Семестр "3"
Дисциплина "Киберправо"
Билет № 11

1. Цифровое право и примеры его реализации.
2. Правовой режим электронной подписи. Разница между простой и усиленной квалифицированной электронной подписью.

Подпись преподавателя _____ Подпись заведующего кафедрой _____

Грозненский государственный нефтяной технический университет им.акад. М.Д. Миллионщикова
Институт ""
Группа "" Семестр "3"
Дисциплина "Киберправо"
Билет № 12

1. Публичная оферта в сети Интернет и требования к ее содержанию.
2. Проблема определения юрисдикции в киберпространстве.

Подпись преподавателя _____ Подпись заведующего кафедрой _____

Грозненский государственный нефтяной технический университет им.акад. М.Д. Миллионщикова
Институт ""
Группа "" Семестр "3"
Дисциплина "Киберправо"

Билет № 13

1. Правовая специфика регулирования отношений в сети Интернет по сравнению с традиционными правоотношениями.
2. Принципы обработки персональных данных в сети Интернет.

Подпись преподавателя _____ Подпись заведующего кафедрой _____

Грозненский государственный нефтяной технический университет им.акад. М.Д. Миллионщикова
Институт ""
Группа "" Семестр "3"
Дисциплина "Киберправо"
Билет № 14

1. Правовые способы защиты прав на товарный знак.
2. Основные группы источников киберправа.

Подпись преподавателя _____ Подпись заведующего кафедрой _____

Грозненский государственный нефтяной технический университет им.акад. М.Д. Миллионщикова
Институт ""
Группа "" Семестр "3"
Дисциплина "Киберправо"
Билет № 15

1. Существенные условия и порядок заключения договора в электронной форме.
2. Ответственность за вред, причиненный действиями (решениями) автономной системы с элементами ИИ.

Подпись преподавателя _____ Подпись заведующего кафедрой _____

Грозненский государственный нефтяной технический университет им.акад. М.Д. Миллионщикова
Институт ""
Группа "" Семестр "3"
Дисциплина "Киберправо"
Билет № 16

1. Публичная оферта в сети Интернет и требования к ее содержанию.
2. Правовые последствия утечки персональных данных для оператора.

Подпись преподавателя _____ Подпись заведующего кафедрой _____

Грозненский государственный нефтяной технический университет им.акад. М.Д. Миллионщикова
Институт ""
Группа "" Семестр "3"
Дисциплина "Киберправо"
Билет № 17

1. Особый порядок обработки биометрических персональных данных.
2. Атака как форс-мажорное обстоятельство, освобождающее от ответственности за неисполнение обязательств.

Подпись преподавателя _____ Подпись заведующего кафедрой _____

Грозненский государственный нефтяной технический университет им.акад. М.Д. Миллионщикова
Институт ""
Группа "" Семестр "3"
Дисциплина "Киберправо"
Билет № 18

1. Принципы обработки персональных данных в сети Интернет.
2. Правовые последствия утечки персональных данных для оператора.

Подпись преподавателя _____ Подпись заведующего кафедрой _____

Грозненский государственный нефтяной технический университет им.акад. М.Д. Миллионщикова
Институт ""
Группа "" Семестр "3"
Дисциплина "Киберправо"
Билет № 19

1. Составы административных правонарушений в информационной сфере.
2. Проблема атрибуции кибератаки и как она влияет на привлечение к ответственности.

Подпись преподавателя _____ Подпись заведующего кафедрой _____

Грозненский государственный нефтяной технический университет им.акад. М.Д. Миллионщикова
Институт ""
Группа "" Семестр "3"
Дисциплина "Киберправо"
Билет № 20

1. Принципы обработки персональных данных в сети Интернет.
2. Основные модели государственного регулирования интернет-пространства.

Подпись преподавателя _____ Подпись заведующего кафедрой _____

Грозненский государственный нефтяной технический университет им.акад. М.Д. Миллионщикова
Институт ""
Группа "" Семестр "3"
Дисциплина "Киберправо"
Билет № 21

1. Основные модели государственного регулирования интернет-пространства.

Подпись преподавателя _____ Подпись заведующего кафедрой _____

Грозненский государственный нефтяной технический университет им.акад. М.Д. Миллионщикова
Институт ""
Группа "" Семестр "3"
Дисциплина "Киберправо"
Билет № 22

1. Права субъекта персональных данных и механизмы их реализации.
2. Специфика защита прав потребителей при дистанционном способе продажи товаров.

Подпись преподавателя _____ Подпись заведующего кафедрой _____

Грозненский государственный нефтяной технический университет им.акад. М.Д. Миллионщикова
Институт ""
Группа "" Семестр "3"
Дисциплина "Киберправо"
Билет № 23

1. Атака как форс-мажорное обстоятельство, освобождающее от ответственности за неисполнение обязательств.
2. Особенности охраны авторских прав на произведения, созданные с использованием искусственного интеллекта.

Подпись преподавателя _____ Подпись заведующего кафедрой _____

Грозненский государственный нефтяной технический университет им.акад. М.Д. Миллионщикова
Институт ""
Группа "" Семестр "3"
Дисциплина "Киберправо"
Билет № 24

1. «Права на забвение» в российском законодательстве, механизм его реализации.
2. Правовая специфика регулирования отношений в сети Интернет по сравнению с традиционными правоотношениями.

Подпись преподавателя _____ Подпись заведующего кафедрой _____

Грозненский государственный нефтяной технический университет им.акад. М.Д. Миллионщикова
Институт ""
Группа "" Семестр "3"
Дисциплина "Киберправо"
Билет № 25

1. Проблема атрибуции кибератаки и как она влияет на привлечение к ответственности.
2. Правовые способы защиты прав на товарный знак.

Подпись преподавателя _____ Подпись заведующего кафедрой _____

Критерии оценивания:

Уровень знаний определяется оценками «отлично», «хорошо», «удовлетворительно», «неудовлетворительно».

Оценка **«отлично»** - студент показывает полные и глубокие знания программного материала, логично и аргументировано отвечает на поставленный вопрос, а также дополнительные вопросы, показывает высокий уровень теоретических знаний.

Оценка **«хорошо»** - студент показывает глубокие знания программного материала, грамотно его излагает, достаточно полно отвечает на поставленный вопрос и дополнительные вопросы, умело формулирует выводы. В тоже время при ответе допускает несущественные погрешности.

Оценка **«удовлетворительно»** - студент показывает достаточные, но не глубокие знания программного материала; при ответе не допускает грубых ошибок или противоречий, однако в формулировании ответа отсутствует должная связь между анализом, аргументацией и выводами. Для получения правильного ответа требуется уточняющие вопросы.

Оценка **«неудовлетворительно»** - студент показывает недостаточные знания программного материала, не способен аргументировано и последовательно его излагать, допускается грубые ошибки в ответах, неправильно отвечает на поставленный вопрос или затрудняется с ответом.