

Скоков
Роман
Юрьевич 2026.02.27
Ректор " 15:49:20
ВИЭПП" +03'00'

Приложение 2 к рабочей программе дисциплины
«Право цифровых платформ»

ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
ВЫСШЕГО ОБРАЗОВАНИЯ
«ВОЛЖСКИЙ ИНСТИТУТ ЭКОНОМИКИ, ПЕДАГОГИКИ И ПРАВА»

Факультет информационной безопасности и права

Фонд оценочных средств
по дисциплине
«Право цифровых платформ»

Направление подготовки:
09.03.03 Прикладная информатика

Направленность (профиль) образовательной программы:
Прикладная информатика в юриспруденции

Уровень высшего образования:
бакалавриат

Квалификация выпускника:
«бакалавр»

Волжский, 2026 г.

Содержание

1	Перечень компетенций с указанием этапов их формирования в процессе освоения образовательной программы, описание показателей, критериев оценивания компетенций на различных этапах их формирования, описание шкал оценивания.....	3
2	Методические материалы и типовые контрольные задания, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций в процессе освоения образовательной программы.....	6
2.1	Типовые контрольные задания, используемые для проведения входного контроля	6
2.2	Типовые контрольные задания, используемые для промежуточной аттестации по дисциплине.....	7
2.2.1	Примерный перечень вопросов к зачету	7
2.2.2	Примерное задание на зачет Дайте полный и развернутый ответ на следующие вопросы:	8
2.3	Методические материалы и типовые контрольные задания, используемые для текущего контроля по дисциплине.....	8
2.3.1	Методические материалы, используемые для текущего контроля знаний по дисциплине.....	8
2.3.2	Вопросы, выносимые на самостоятельное изучение	9
2.3.3	Задания для самостоятельной работы	9
2.3.4	Тесты по дисциплине	10
2.3.5	Типовые задания.....	11
2.3.6	Задания для контрольной работы	12
2.3.7	Методика проведения лекции-дискуссии	13
2.3.8	Методика проведения интерактивного решения задач	13
3	Методические материалы, определяющие процедуры оценивания знаний, умений, навыков по дисциплине.....	14

1 Перечень компетенций с указанием этапов их формирования в процессе освоения образовательной программы, описание показателей, критериев оценивания компетенций на различных этапах их формирования, описание шкал оценивания

Перечень компетенций	Показатели оценивания компетенций	Критерии оценивания компетенций	Этапы формирования компетенций	Шкала оценивания
ПК-6. Способен квалифицированно проводить юридическую экспертизу программного обеспечения в профессиональной деятельности, обеспечивать эксплуатацию комплекса средств автоматизации технологических решений	- знает нормативно-правовые основы регулирования программного обеспечения; требования к юридической экспертизе ПО; - умеет анализировать документацию на программное обеспечение на соответствие законодательству; выявлять правовые дефекты в алгоритмах; - владеет навыками проведения правовой экспертизы исходного кода и документации.	- имеет базовые знания нормативно-правовых основ регулирования ПО; - умеет на основе типовых примеров анализировать документацию на соответствие законодательству; - владеет навыками проведения правовой экспертизы под руководством преподавателя.	Начальный	удовлетворительно (60 – 74 баллов)
	- знает нормативно-правовые основы регулирования программного обеспечения; требования к юридической экспертизе ПО; - умеет анализировать документацию на программное обеспечение на соответствие законодательству; выявлять правовые дефекты в алгоритмах; - владеет навыками проведения правовой экспертизы исходного кода и документации.	- знает стандарты и регламенты эксплуатации средств автоматизации; - умеет самостоятельно анализировать документацию и выявлять правовые дефекты; - владеет навыками самостоятельного проведения правовой экспертизы ПО.	Основной	хорошо (75 – 89 баллов)
	- знает нормативно-правовые основы регулирования программного	- знает правовые риски внедрения технологических решений; - умеет	Завершающий	отлично (90 – 100 баллов)

	обеспечения; требования к юридической экспертизе ПО; - умеет анализировать документацию на программное обеспечение на соответствие законодательству; выявлять правовые дефекты в алгоритмах; - владеет навыками проведения правовой экспертизы исходного кода и документации.	готовить заключения по результатам юридической экспертизы ПО; - владеет опытом проведения правовой экспертизы и оценки рисков в ИТ-проектах.		
ПК-7. Способен принимать решения в точном соответствии с законодательством РФ и совершать юридические действия в организации ИТ инфраструктуры и управлении информационной безопасностью	- знает законодательство РФ в сфере информационной безопасности; основы организации ИТ-инфраструктуры с точки зрения права; - умеет принимать управленческие решения на основе анализа правового поля; совершать юридические действия при настройке и защите ИТ-инфраструктуры; - владеет навыками правового моделирования ИТ-процессов.	- имеет базовые знания законодательства РФ в сфере ИБ; - умеет на основе типовых примеров принимать управленческие решения; - владеет навыками совершения юридически значимых действий под руководством.	Начальный	удовлетворительно (60 – 74 баллов)
	- знает законодательство РФ в сфере информационной безопасности; основы организации ИТ-инфраструктуры с точки зрения права; - умеет принимать управленческие решения на основе анализа правового поля; совершать юридические действия при настройке и защите ИТ-инфраструктуры; - владеет навыками правового моделирования ИТ-процессов.	- знает порядок совершения юридически значимых действий в цифровой среде; - умеет самостоятельно принимать решения и взаимодействовать с регуляторами; - владеет навыками разработки локальных нормативных актов по ИБ.	Основной	хорошо (75 – 89 баллов)
	- знает законодательство РФ в сфере информационной безопасности; основы организации ИТ-инфраструктуры с точки зрения права; - умеет принимать управленческие решения на основе	- знает ответственность за нарушения в сфере ИТ и ИБ; - умеет обеспечивать правовое сопровождение эксплуатации автоматизированных систем; -	Завершающий	отлично (90 – 100 баллов)

	анализа правового поля; совершать юридические действия при настройке и защите ИТ-инфраструктуры; - владеет навыками правового моделирования ИТ-процессов.	владеет опытом защиты прав при инцидентах информационной безопасности.		
--	--	---	--	--

2 Методические материалы и типовые контрольные задания, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций в процессе освоения образовательной программы

2.1 Типовые контрольные задания, используемые для проведения входного контроля

1. Что является основным источником права в сфере информационных технологий в РФ? а) Обычай делового оборота. б) Гражданский кодекс РФ и федеральные законы. в) Судебный прецедент. г) Корпоративные стандарты.

2. Какой закон регулирует защиту персональных данных в РФ? а) ФЗ «Об информации». б) ФЗ «О персональных данных». в) ФЗ «О связи». г) ФЗ «О коммерческой тайне».

3. Что такое интеллектуальная собственность в контексте ПО? а) Право собственности на компьютер. б) Исключительное право на программу для ЭВМ. в) Право на доступ в Интернет. г) Право на использование социальных сетей.

4. Какая форма договора наиболее характерна для цифровых платформ? а) Письменная форма с нотариальным заверением. б) Публичная оферта (клик-рапп). в) Устная договоренность. г) Трудовой договор.

5. Что такое конфиденциальная информация? а) Информация, доступная всем пользователям сети. б) Информация, доступ к которой ограничен ее обладателем. в) Информация из открытых источников. г) Рекламная информация.

6. Какой орган осуществляет надзор в сфере связи и информационных технологий? а) МВД России. б) Роскомнадзор. в) ФНС России. г) Роспотребнадзор.

7. Что такое электронная подпись? а) Сканированная подпись на бумаге. б) Аналог собственноручной подписи в электронном виде. в) Пароль от электронной почты. г) Логин в системе.

8. Какая ответственность предусмотрена за нарушение авторских прав на ПО? а) Только дисциплинарная. б) Гражданская, административная и уголовная. в) Только моральная. г) Ответственность не предусмотрена.

9. Что такое коммерческая тайна в ИТ-компании? а) Режим конфиденциальности информации, позволяющей получить прибыль. б) Открытый исходный код. в) Публикация отчетностей. г) Рекламная кампания.

10. Какой срок действия исключительного права на программу для ЭВМ? а) 5 лет. б) 10 лет. в) В течение всей жизни автора и 70 лет после его смерти. г) Бессрочно.

11. Что регулирует ФЗ «Об информации, информационных технологиях и о защите информации»? а) Только работу государственных сайтов. б) Отношения, возникающие при формировании и использовании информационных ресурсов. в) Только вопросы авторского права. г) Только вопросы связи.

12. Что такое доменное имя? а) Адрес сайта в сети Интернет. б) Название компьютера. в) Пароль доступа. г) Название программного обеспечения.

13. Какая лицензия позволяет свободное использование ПО с открытым кодом? а) Proprietary License. б) Open Source License (GPL, MIT). в) Trial License. г) NDA.

14. Что является объектом авторского права в сфере ИТ? а) Идеи и методы. б) Программа для ЭВМ, база данных. в) Аппаратное обеспечение. г) Каналы связи.

15. Что такое киберпреступление? а) Преступление, совершенное с использованием ИТ. б) Поломка компьютера. в) Потеря пароля. г) Вирусная атака без умысла.

16. Какой документ регулирует правила использования сайта пользователем? а) Трудовой договор. б) Пользовательское соглашение. в) Устав предприятия. г) Должностная инструкция.

17. Что такое обезличивание персональных данных? а) Удаление данных. б) Действия, в результате которых становится невозможным определение принадлежности данных. в) Копирование данных. г) Шифрование данных.

18. Кто является оператором персональных данных? а) Любой пользователь интернета. б) Лицо, организующее обработку персональных данных. в) Провайдер услуг связи. г) Владелец компьютера.

19. Что такое смарт-контракт? а) Договор, исполняемый автоматически при наступлении условий. б) Умный договор с юристом. в) Договор в бумажном виде. г) Договор аренды сервера.

20. Какая ответственность наступает за утечку персональных данных? а) Только предупреждение. б) Административная, гражданская, уголовная. в) Никакая. г) Только дисциплинарная.

2.2 Типовые контрольные задания, используемые для промежуточной аттестации по дисциплине

2.2.1 Примерный перечень вопросов к зачету

Теоретические вопросы

1. Понятие цифровой платформы в законодательстве РФ и доктрине.
2. Классификация платформ: агрегаторы, маркетплейсы, социальные сети, финтех-платформы.
3. Правовой статус владельца платформы, пользователей и контрагентов.
4. Регулирование деятельности агрегаторов информации (ФЗ «Об информации»).
5. Антимонопольное регулирование платформенной экономики.
6. Ответственность платформы за контент и действия пользователей.
7. Зарубежный опыт регулирования (DSA, DMA).
8. Правовая природа пользовательских соглашений (License Agreement, EULA, Terms of Service).
9. Требования к форме и содержанию оферты в сети Интернет.
10. Акцепт оферты конклюдентными действиями.
11. Особенности заключения сделок через цифровые платформы.
12. Смарт-контракты и их юридическая сила в РФ.
13. Защита прав потребителей в цифровой среде.
14. Споры по договорам присоединения.
15. Механизмы разрешения споров онлайн (ODR).
16. Цели и задачи юридической экспертизы ПО.
17. Объекты экспертизы: исходный код, документация, интерфейсы, алгоритмы.
18. Методология проведения экспертизы на соответствие законодательству.
19. Выявление правовых рисков в алгоритмах ИИ.
20. Оформление заключения эксперта по ПО. Практические вопросы
21. Проанализируйте пользовательское соглашение популярной цифровой платформы на предмет соответствия ГК РФ.
22. Разработайте план юридической экспертизы модуля программного обеспечения.
23. Определите правовые риски при внедрении системы обработки персональных данных в облаке.
24. Составьте проект ответа на претензию пользователя платформы о блокировке аккаунта.
25. Оцените законность сбора данных пользователей мобильным приложением.
26. Разработайте политику конфиденциальности для интернет-магазина.
27. Проанализируйте кейс ответственности агрегатора за действия продавца.

28. Определите порядок уведомления регулятора об инциденте ИБ.
29. Составьте чек-лист для правового аудита ИТ-инфраструктуры.
30. Разработайте алгоритм действий юриста при утечке данных.
31. Оцените правовые последствия использования open-source библиотек в коммерческом ПО.
32. Проанализируйте договор лицензирования программного обеспечения.
33. Определите jurisdiction применимого права в трансграничной цифровой сделке.
34. Разработайте инструкцию для сотрудников по соблюдению режима коммерческой тайны.
35. Оцените риски использования биометрических данных на платформе.
36. Составьте проект оферты для цифрового сервиса.
37. Проанализируйте судебную практику по спорам с цифровыми платформами.
38. Определите требования к хранению логинов и паролей с точки зрения закона.
39. Разработайте регламент обработки запросов субъектов персональных данных.
40. Оцените соответствие платформы требованиям ФЗ-152 и ФЗ-187.

2.2.2 Примерное задание на зачет Дайте полный и развернутый ответ на следующие вопросы:

1. Проведите правовую экспертизу типового пользовательского соглашения цифровой платформы (на примере выбранного сервиса). Выявите пункты, potentially нарушающие права потребителей.
2. Разработайте алгоритм действий организации при выявлении уязвимости в ИТ-инфраструктуре с точки зрения законодательства РФ об информационной безопасности.

2.3 Методические материалы и типовые контрольные задания, используемые для текущего контроля по дисциплине

2.3.1 Методические материалы, используемые для текущего контроля знаний по дисциплине

Наименование оценочного средства	Краткая характеристика оценочного средства	Представление оценочного средства в фонде
Контрольный опрос	Контрольный опрос – это метод оценки уровня освоения компетенций, основанный на непосредственном (беседа, интервью) или опосредованном (анкета) взаимодействии преподавателя и студента. Источником контроля знаний в данном случае служит словесное или письменное суждение студента	Примерный перечень вопросов к зачету и экзамену Вопросы, выносимые на самостоятельное изучение Задания для самостоятельной работы
Собеседование	Собеседование – это один из методов контрольного опроса, представляющий собой относительно свободный диалог между преподавателем и студентом на заданную тему	Примерный перечень вопросов к зачету и экзамену Вопросы, выносимые на самостоятельное изучение Задания для самостоятельной работы
Тестовые задания	Тестирование удовлетворяющая критериям исследования эмпирико-аналитическая процедура оценки уровня освоения компетенций студентами	Тесты по дисциплине

Самостоятельное решение задач	Метод, при котором обучающиеся приобретают навыки творческого мышления, самостоятельного решения проблем теории и практики.	Типовые задания
Лекция-дискуссия	Оценочное средство, позволяющее включить обучающимся в процесс обсуждения спорного вопроса, проблемы и оценить их умение аргументировать собственную точку зрения	Методика проведения лекции-дискуссии
Интерактивное решение задач	Метод модерации, при котором при решении задач принимают участие все обучающиеся под руководством преподавателя-модератора	Методика проведения интерактивного решения задач Типовые задания

2.3.2 Вопросы, выносимые на самостоятельное изучение

1. Понятие и виды цифровых платформ: Что такое цифровая платформа? Какие виды платформ существуют в РФ?
2. Правовой статус агрегатора: Какие обязанности возлагаются на владельца агрегатора информации?
3. Пользовательские соглашения: Какова юридическая сила клика по кнопке «Я согласен»?
4. Смарт-контракты: Признаются ли смарт-контракты судом в РФ?
5. Ответственность за контент: Когда платформа отвечает за комментарии пользователей?
6. Юридическая экспертиза ПО: Зачем нужна правовая проверка кода?
7. Алгоритмы и право: Как регулировать решения, принятые искусственным интеллектом?
8. Информационная безопасность: Какие законы регулируют защиту ИТ-инфраструктуры?
9. Персональные данные в облаках: Можно ли хранить ПДн на зарубежных серверах?
10. Инциденты ИБ: Какие действия обязательны при утечке данных?

Блок вопросов для закрепления практических навыков

1. Анализ оферты: Как найти незаконные пункты в договоре присоединения?
2. Аудит ПО: Какие документы проверять при экспертизе программы?
3. Compliance: Как проверить соответствие платформы ФЗ-152?
4. Договоры в ИТ: Чем отличается лицензионный договор от договора отчуждения?
5. Защита прав: Как пользователю вернуть деньги за цифровой товар?
6. Регуляторы: Куда жаловаться на действия цифровой платформы?
7. Риски ИИ: Как оценить правовые риски алгоритма кредитного скоринга?
8. Локальные акты: Какие документы нужны для защиты коммерческой тайны в ИТ-фирме?
9. Экспертиза: Как составить заключение юриста по коду?
10. Кейсы: Разбор реальных судебных споров с Яндекс, Ozon, VK.

2.3.3 Задания для самостоятельной работы

1. Подготовьте сравнительную таблицу правовых статусов различных видов цифровых платформ (маркетплейс, соцсеть, агрегатор).

2. Проведите анализ пользовательского соглашения одного из популярных сервисов (на выбор) на соответствие ГК РФ.
3. Составьте проект политики обработки персональных данных для веб-сайта.
4. Разработайте чек-лист для проведения юридической экспертизы программного модуля.
5. Подготовьте реферат на тему «Ответственность платформ за контент пользователей в РФ и ЕС».

2.3.4 Тесты по дисциплине

1. Что является основным признаком цифровой платформы? а) Наличие физического офиса. б) Посредничество между группами пользователей. в) Производство товаров. г) Государственная собственность.
2. Какой закон регулирует деятельность агрегаторов информации? а) ФЗ «О защите прав потребителей». б) ФЗ «Об информации, информационных технологиях и о защите информации». в) ФЗ «О рекламе». г) УК РФ.
3. Что такое акцепт оферты в интернете? а) Подписание бумаги. б) Совершение конклюдентных действий (клик, оплата). в) Устное согласие. г) Отправка письма.
4. Кто несет ответственность за незаконный контент, размещенный пользователем? а) Только пользователь. б) Платформа, если не удалила после уведомления. в) Провайдер хостинга. г) Никто.
5. Что такое EULA? а) Лицензионное соглашение с конечным пользователем. б) Трудовой договор. в) Договор аренды. г) Налоговая декларация.
6. Какой срок хранения персональных данных допускается без цели обработки? а) Бессрочно. б) Не дольше чем требуют цели обработки. в) 5 лет. г) 1 год.
7. Что является объектом юридической экспертизы ПО? а) Компьютерное железо. б) Исходный код и документация. в) Офисное помещение. г) Сотрудники компании.
8. Какая ответственность грозит за утечку персональных данных? а) Только штраф. б) Штраф, компенсация морального вреда, уголовная ответственность. в) Предупреждение. г) Блокировка сайта навсегда.
9. Что такое категорирование объектов КИИ? а) Присвоение категории значимости объекту критической информационной инфраструктуры. б) Разделение сотрудников по зарплате. в) Классификация компьютеров по цвету. г) Учет программного обеспечения.
10. Обязательно ли уведомлять Роскомнадзор об обработке ПДн? а) Да, всегда. б) Нет, есть исключения. в) Только госорганы. г) Только банки.
11. Что такое Smart Contract? а) Договор с умным юристом. б) Компьютерный алгоритм, исполняющий условия сделки. в) Договор в рамке. г) Устная договоренность.
12. Какой закон регулирует безопасность значимых объектов КИИ? а) ФЗ-152. б) ФЗ-187. в) ФЗ-149. г) ГК РФ.
13. Что такое Open Source? а) Закрытое ПО. б) ПО с открытым исходным кодом. в) Бесплатное ПО без прав. г) Вирусное ПО.
14. Можно ли передавать ПДн третьим лицам без согласия субъекта? а) Да, всегда. б) Только в случаях, предусмотренных законом. в) Нет, никогда. г) Только за деньги.
15. Что такое Digital Rights? а) Цифровые права на объекты имущества. б) Права на покупку компьютера. в) Права программиста. г) Права доступа в интернет.
16. Кто является субъектом персональных данных? а) Оператор. б) Физическое лицо, к которому относятся данные. в) Регулятор. г) Владелец сайта.
17. Что такое фишинг с точки зрения права? а) Рыбалка. б) Мошенничество в сети. в) Поиск информации. г) Тестирование безопасности.

18. Какой орган выдает лицензии на деятельность в сфере ИБ? а) МВД. б) ФСТЭК России (для отдельных видов работ). в) Минздрав. г) Росреестр.

19. Что такое токенизация активов? а) Выпуск цифровых прав на активы. б) Разделение компьютера на части. в) Удаление данных. г) Шифрование диска.

20. Какой срок исковой давности по спорам в цифровой среде? а) 1 год. б) 3 года (общий). в) 10 лет. г) 6 месяцев.

2.3.5 Типовые задания

Типовые задачи

Задача 1: Правовой аудит пользовательского соглашения

Описание задачи: Вам поручено провести правовой анализ пользовательского соглашения популярного маркетплейса. Руководство компании хочет убедиться в соответствии документа законодательству РФ перед запуском новой версии.

Задание:

1. Анализ структуры: Изучите структуру соглашения, выделите существенные условия.

2. Проверка на соответствие ГК РФ: Найдите пункты, которые могут быть признаны недействительными (например, чрезмерное ограничение ответственности платформы).

3. Защита прав потребителей: Оцените положения о возврате товара, обработке жалоб, персональных данных.

4. Рекомендации: Составьте список рекомендаций по изменению текста соглашения для минимизации правовых рисков.

5. Отчет: Подготовьте краткое заключение для руководства. Критерии оценки:

6. Полнота выявленных правовых рисков.

7. Аргументированность рекомендаций со ссылками на законы.

8. Качество оформления заключения.

9. Учет специфики цифровой среды.

10. Практическая применимость рекомендаций.

Задача 2: Организация защиты информации в ИТ-инфраструктуре

Описание задачи: Компания внедряет новую CRM-систему, содержащую персональные данные клиентов. Необходимо разработать комплекс организационных мер защиты с точки зрения законодательства.

Задание:

1. Анализ данных: Определите категории обрабатываемых персональных данных.

2. Модели угроз: Опишите потенциальные угрозы безопасности данных.

3. Нормативная база: Подберите необходимые нормативные акты (ФЗ-152, приказы ФСТЭК).

4. Документация: Разработайте перечень локальных нормативных актов (политика обработки ПДн, инструкции).

5. Инциденты: Опишите процедуру действий при утечке данных. Критерии оценки:

6. Соответствие требованиям регуляторов (ФСТЭК, РКН).

7. Полнота разработанной документации.

8. Реалистичность плана действий при инцидентах.

9. Учет технических и организационных мер.

10. Качество проработки модели угроз.

Дополнительные замечания:

1. При выполнении задач студенты должны использовать актуальные версии законодательства РФ.
2. Задачи могут быть адаптированы под конкретные кейсы цифровых платформ.
3. При выполнении задач рекомендуется использовать примеры из судебной практики.

2.3.6 Задания для контрольной работы

2.3.6.1 Задание к теоретической части контрольной работы

Задание 1: Правовое регулирование цифровых платформ

Описание: Подготовьте развернутый ответ на вопрос о правовом статусе владельца цифровой платформы в РФ.

Задание:

1. Определение статуса: Кто считается владельцем платформы по закону?
2. Обязанности: Какие обязанности возлагаются на владельца (модерация, хранение данных, взаимодействие с госорганами)?
3. Ответственность: Какие виды ответственности предусмотрены за нарушения?
4. Сравнение: Сравните регулирование в РФ и ЕС (DSA).
5. Выводы: Сформулируйте тенденции развития законодательства. Критерии оценки:
6. Глубина знания нормативной базы.
7. Умение сравнивать правовые системы.
8. Логичность изложения.
9. Наличие ссылок на конкретные статьи законов.
10. Актуальность информации.

Задание 2: Юридическая экспертиза алгоритмов Описание: Опишите методику проведения юридической экспертизы алгоритма принятия решений (например, кредитный скоринг). Задание:

1. Объекты проверки: Что именно проверяет юрист в алгоритме?
 2. Критерии законности: Какие законы могут быть нарушены алгоритмом (дискриминация, ПДн)?
 3. Документирование: Как фиксировать результаты экспертизы?
 4. Риски: Какие правовые риски несет компания при использовании «черного ящика»?
 5. Рекомендации: Как минимизировать риски автоматизированных решений?
- Критерии оценки:

6. Понимание специфики экспертизы ПО.
7. Знание требований к автоматизированной обработке данных.
8. Качество предложенной методики.
9. Учет этических и правовых аспектов ИИ.
10. Практическая ценность рекомендаций.

2.3.6.2 Задание к практической части контрольной работы

Задача 1: Составление оферты для цифрового сервиса Описание: Вам необходимо разработать проект публичной оферты для нового онлайн-сервиса по подписке на программное обеспечение (SaaS).

Задание:

1. Структура документа: Определите основные разделы оферты.
2. Существенные условия: Пропишите предмет договора, цену, порядок оплаты.
3. Ответственность сторон: Установите пределы ответственности сервиса и пользователя.
4. Персональные данные: Включите раздел о согласии на обработку ПДн.

5. Применимое право: Укажите юрисдикцию и порядок разрешения споров.

Задача 2: Анализ инцидента информационной безопасности

Описание: Произошла утечка базы данных клиентов компании. Необходимо разработать план действий юриста.

Задание:

1. Фиксация факта: Какие документы нужно составить немедленно?
2. Уведомление: Кого и в какие сроки нужно уведомить (РКН, субъекты данных)?
3. Расследование: Как собрать доказательства для внутреннего расследования?
4. Минимизация ущерба: Какие меры принять для защиты репутации и снижения штрафов?
5. Отчетность: Как отчитаться перед регулятором?

2.3.7 Методика проведения лекции-дискуссии

Цель: достижение определенного мнения по обсуждаемой проблеме путем осознания участниками своих мнений, суждений, оценок по теме дискуссии ; уточнения взаимных позиций в споре ; выработки уважительного отношения к другому мнению .

Задачи:

- ☐ развитие умений анализировать проблему или проблемную ситуацию в сфере цифрового права;
- ☐ поиск и разработка перспективных идей правового регулирования платформ;
- ☐ развитие способности продуцировать множество решений правовых коллизий;
- ☐ нахождение оптимального решения среди нескольких альтернатив . Методика проведения:
- ☐ назначение секретаря лекции-дискуссии , его инструктаж по выполняемым функциям;
- ☐ объявление критерий оценки;
- ☐ свободный обмен мнениями в промежутках между логически оформленными разделами сообщения учебного материала ;
- ☐ подведение итогов дискуссии и оценка участников дискуссии по материалам, подготовленным секретарем, переход к информационной лекции. Критерии оценки: секретарь лекции-дискуссии – 0,5 – 1,5 баллов; участие в дискуссии – 0,5 – 1 баллов.

2.3.8 Методика проведения интерактивного решения задач

Цель: проверка навыков решения профессиональных задач и развитие мыслительных операций обучающихся, направленных на достижение результатов при решении профессиональных задач в сфере права цифровых платформ.

Задачи:

1. проверка навыков применения обучающимися ранее усвоенных знаний при решении профессиональных задач;
2. формирование навыков совместной деятельности подчиненных (обучающихся) и руководителя (преподавателя);
3. овладение обучающимися знаниями и общими принципами решения проблемных профессиональных задач;
4. развитие навыков активной интеллектуальной деятельности;
5. развитие коммуникативных навыков (навыков общения).
6. развитие навыков обучающихся по выработке собственной позиции по ходу решения профессиональных задач. Методика проведения интерактивного решения задач: Первый этап «подготовка проекта решения задач». Преподавателем разрабатывается проект хода решения задачи с началом или фрагментами решения. Второй этап «организационный»:

7. объявление темы и цели решения задачи;
 8. назначение секретаря и его инструктаж по выполняемым функциям;
 9. объявление критерий оценки; Третий этап «интеллектуальный»:
 10. объявление условий решения задач;
 11. индивидуальное решение задачи обучающимися, исходя из собственного мнения;
 12. высказывание обучающимися мнений по ходу решения задач;
 13. обсуждение результатов и методики индивидуального решения задач обучающимися и принятие плана верного хода решения; Третий этап «подведение итогов решения задачи»:
 14. формулирование вывода решения задачи обучающимися;
 15. подведение итога интерактивного решения задачи преподавателем;
 16. оценка преподавателем обучающихся по материалам, подготовленным секретарем.
- Критерии оценки: секретарь – 1 балл; участие в решении задач – 1 – 3 балла.

3 Методические материалы, определяющие процедуры оценивания знаний, умений, навыков по дисциплине

Балльно-рейтинговая система оценки успеваемости по дисциплине

В целях оперативного контроля уровня усвоения материала учебной дисциплины и стимулирования активной учебной деятельности студентов (очной формы обучения) используется балльно-рейтинговая система оценки успеваемости. В соответствии с этой системой оценки студенту в ходе изучения дисциплины предоставляется возможность набрать не менее 60 баллов за текущую работу в семестре и до 40 баллов на зачете (итоговый контроль). Результирующая оценка по дисциплине складывается из суммы баллов текущего и итогового контроля. К зачету допускаются студенты, посетившие все лекции и семинары, прошедшие промежуточную аттестацию, с рейтингом не менее 30 баллов. Баллы за текущую работу в семестре по дисциплине складываются из следующих видов деятельности студента.

Балльно-рейтинговая система по дисциплине «Право цифровых платформ»

Виды контроля	Максимальная сумма баллов на выполнение одного вида задания	Всего возможных за семестр работ	Итого максимальная сумма баллов
Присутствие на лекционных и практических (семинарских) занятиях	0,25	12	3
Работа на практических (семинарских) занятиях	2,0	8	16
Интерактивные занятия	2,5	4	10
СРС, в т.ч.:			31
написание конспектов	0,5	4	2
защита рефератов	1,0	3	3
выступление с докладом	1,0	2	2
самостоятельное решение задач	2,0	4	8
написание эссе	1,0	4	4
контроль СРС (контрольные опросы, тестирование, решение кейсов и др. виды	1,0	12	12

контроля)			
Итого за семестр	-	-	60
Зачет	40,0	1	40
Итого по дисциплине	-	-	100

Текущий контроль по лекционному материалу проводит лектор. Текущий контроль по семинарским занятиям проводит преподаватель, проводивший эти занятия. Балльно-рейтинговая система предусматривает поощрение студентов за работу в семестре проставлением «премиальных» баллов.

Нормы выставления дополнительных баллов по дисциплине «Право цифровых платформ»

Виды работ	Максимальная сумма баллов
Решение дополнительных задач	5
Участие в олимпиадах, конкурсах, конференциях в рамках предмета дисциплины	5
Итого	10

Шкала итоговой оценки

Количество баллов	Оценка
61 – 100	«зачтено»
0 – 60	«не зачтено»