МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Российский государственный гуманитарный университет»
(ФГБОУ ВО «РГГУ»)

ИНСТИТУТ УПРАВЛЕНИЯ, ЭКОНОМИКИ И ПРАВА
ЮРИДИЧЕСКИЙ ФАКУЛЬТЕТ
Кафедра предпринимательского права

ПРАВОВАЯ БЕЗОПАСНОСТЬ В ИНФОРМАЦИОННОМ ПРОСТРАНСТВЕ

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

43.04.02 - Туризм

Код и наименование направления подготовки/специальности

«Cultural Heritage Management and Sustainable Tourism»
«Сохранение культурного наследия и устойчивый туризм»

Наименование направленности (профиля)/ специализации

Уровень высшего образования: *магистратура*

Форма обучения: *очная*

РПД адаптирована для лиц
с ограниченными возможностями
здоровья и инвалидов

Москва 2023

Правовая безопасность в информационном пространстве
Рабочая программа дисциплины

Составители:
Д-р юрид.наук, профессор, декан юридического факультета С.В. Тимофеев
Канд.юрид.наук, доцент, заведующий кафедрой предпринимательского права Т.В. Белова
Канд.юрид.наук, доцент, доцент кафедры уголовного права и процесса Е.А. Редькина

УТВЕРЖДЕНО
Протокол заседания кафедры
№ 12 от16.06.2022

ОГЛАВЛЕНИЕ

1. Пояснительная записка

1.1. Цель и задачи дисциплины

Цель дисциплины – комплексное изучение правовой безопасности в информационном пространстве, в том числе особенностей регламентации различных областей деятельности и юридической защиты в киберпространстве.

Задачи дисциплины:

- получение знаний о правовой безопасности в информационном пространстве, включая особенности регламентации отдельных областей деятельности и специфики мер правовой защиты в киберпространстве.
- формирование умений и навыков, позволяющих реализовывать меры правовой защиты в информационном пространстве.

Дисциплина реализуется в формате онлайн-курса на платформе РГГУ.

1.2. Перечень планируемых результатов обучения по дисциплине

В результате освоения дисциплины обучающийся должен:

Знать: основные этапы развития информационной безопасности; систему законодательства об информационной безопасности и ответственность за его нарушение; систему мер правовой защиты в информационном пространстве в различных областях (сферах) деятельности.

Уметь: применять нормы законодательства для осуществления правовой защиты в информационном пространстве.

Владеть: знаниями законодательства в сфере информационного пространства; знаниями по соблюдению информационной безопасности; специальными навыками правовой защиты в информационном пространстве.

1.3. Место дисциплины в структуре образовательной программы

Дисциплина «Правовая безопасность в информационном пространстве» относится к факультативным дисциплинам учебного плана.

2. Структура дисциплины

Общая трудоёмкость дисциплины составляет 2 з.е., 72 академических часа.

Структура дисциплины для очной формы обучения

Объем дисциплины в форме контактной работы обучающихся с педагогическими работниками и (или) лицами, привлекаемыми к реализации образовательной программы на иных условиях, при проведении учебных занятий:

Семестр	Тип учебных занятий	Количество часов
2	Лекции	10
2	Семинары	10
	Всего:	72

Объем дисциплины (модуля) в форме самостоятельной работы обучающихся составляет 52 академических часа.

Структура дисциплины для очно-заочной формы обучения

Объем дисциплины в форме контактной работы обучающихся с педагогическими работниками и (или) лицами, привлекаемыми к реализации образовательной программы на иных условиях, при проведении учебных занятий:

Семестр	Тип учебных занятий	Количество часов
2	Лекции	8
2	Семинары	8
	Всего:	16

Объем дисциплины (модуля) в форме самостоятельной работы обучающихся составляет 56 академических часов.

Структура дисциплины для заочной формы обучения

Объем дисциплины в форме контактной работы обучающихся с педагогическими работниками и (или) лицами, привлекаемыми к реализации образовательной программы на иных условиях, при проведении учебных занятий:

Год	Тип учебных занятий	Количество часов
1	Лекции	4
1	Семинары	4
	Всего:	8

Объем дисциплины (модуля) в форме самостоятельной работы обучающихся составляет 64 академических часа.

3. Содержание дисциплины

№	Наименование раздела дисциплины	Содержание
1	Ретроспективный анализ правовых норм об информационной безопасности	Этапы развития системы информационной безопасности. Формирование международной информационной безопасности. Развитие законодательства об информационной безопасности.
2	Система законодательства об информационной безопасности	Понятие и нормативно-правовое регулирование информационной безопасности. Принципы государственной политики обеспечения информационной безопасности. Характеристика основных нормативных правовых актов об информационной безопасности. Ответственность за нарушение законодательства об информационной безопасности. Дисциплинарная ответственность. Материальная ответственность. Гражданско-правовая ответственность. Административная ответственность. Уголовная ответственность.

3	Информационная безопасность в сфере экономической деятельности	Понятие цифровой экономики. Основные направления обеспечения информационной безопасности цифровой экономики. Действия под чужим аккаунтом: понятие, квалификация. Добровольное предоставление доступа к аккаунту. Действия под чужим аккаунтом в отсутствие воли владельца. Правовое регулирование электронной коммерции. Особенности заключения договора дистанционным способом.
4	Защита объектов интеллектуальной собственности в киберпространстве	Понятие интеллектуальной собственности. Интеллектуальные права на результаты интеллектуальной деятельности и средства индивидуализации. Способы защиты интеллектуальных прав
5	Защита персональных данных в цифровой среде	Понятие и категории персональных данных. Условия обработки персональных данных, права и обязанности оператора и субъекта обработки данных. Меры защиты персональных данных. Обезличивание персональных данных. «Право на забвение».
6	Правовая защита от деструктивного контента в цифровой среде	Понятие деструктивного контента. Информация, распространение которой запрещено или ограничено. Порядок ограничения доступа к сайтам, содержащим информацию, распространение которой запрещено.

4. Образовательные технологии

Для проведения занятий по дисциплине применяются такие образовательные технологии как онлайн-лекции, представление конспектов лекций и презентационного материала. К каждой лекции прилагаются контрольные вопросы для повторения и самопроверки, список рекомендуемой литературы и глоссарий.

5. Оценка планируемых результатов обучения

5.1 Система оценивания

Форма контроля	**Макс. количество баллов**	
	За одну работу	**Всего**
Текущий контроль:		60 баллов
Анализ нормативных правовых актов и судебных актов	*2*	*16*
Решение задач	*2*	*20*
Выполнение тестов	*4*	*24*
Промежуточная аттестация – *зачет*		40 баллов
Итого за семестр		100 баллов

Полученный совокупный результат конвертируется в традиционную шкалу оценок и в шкалу оценок Европейской системы переноса и накопления кредитов (European Credit Transfer System; далее – ECTS) в соответствии с таблицей:

100-балльная шкала	Традиционная шкала		Шкала ECTS
95 – 100	отлично	зачтено	A
83 – 94			B
68 – 82	хорошо		C
56 – 67	удовлетворительно		D
50 – 55			E
20 – 49	неудовлетворительно	не зачтено	FX
0 – 19			F

5.2 Критерии выставления оценки по дисциплине

Баллы/ Шкала ECTS	**Оценка по дисциплине**	**Критерии оценки результатов обучения по дисциплине**
100-83/ A,B	отлично/ зачтено	Выставляется обучающемуся, если он глубоко и прочно усвоил теоретический и практический материал, может продемонстрировать это на занятиях и в ходе промежуточной аттестации. Обучающийся исчерпывающе и логически стройно излагает учебный материал, умеет увязывать теорию с практикой, справляется с решением задач профессиональной направленности высокого уровня сложности, правильно обосновывает принятые решения. Свободно ориентируется в учебной и профессиональной литературе. Оценка по дисциплине выставляются обучающемуся с учётом результатов текущей и промежуточной аттестации. Компетенции, закреплённые за дисциплиной, сформированы на уровне – «высокий».
82-68/ C	хорошо/ зачтено	Выставляется обучающемуся, если он знает теоретический и практический материал, грамотно и по существу излагает его на занятиях и в ходе промежуточной аттестации, не допуская существенных неточностей. Обучающийся правильно применяет теоретические положения при решении практических задач профессиональной направленности разного уровня сложности, владеет необходимыми для этого навыками и приёмами. Достаточно хорошо ориентируется в учебной и профессиональной литературе. Оценка по дисциплине выставляются обучающемуся с учётом результатов текущей и промежуточной аттестации. Компетенции, закреплённые за дисциплиной, сформированы на уровне – «хороший».
67-50/ D,E	удовлетво-рительно/ зачтено	Выставляется обучающемуся, если он знает на базовом уровне теоретический и практический материал, допускает отдельные ошибки при его изложении на занятиях и в ходе промежуточной аттестации. Обучающийся испытывает определённые затруднения в применении теоретических положений при решении практических задач профессиональной направленности стандартного уровня сложности, владеет необходимыми для этого базовыми навыками и приёмами. Демонстрирует достаточный уровень знания учебной литературы по дисциплине. Оценка по дисциплине выставляются обучающемуся с учётом результатов текущей и промежуточной аттестации. Компетенции, закреплённые за дисциплиной, сформированы на уровне – «достаточный».
49-0/ F,FX	неудовлет-ворительно/ не зачтено	Выставляется обучающемуся, если он не знает на базовом уровне теоретический и практический материал, допускает грубые ошибки при его изложении на занятиях и в ходе промежуточной аттестации.

Баллы/ Шкала ECTS	Оценка по дисциплине	Критерии оценки результатов обучения по дисциплине
		Обучающийся испытывает серьёзные затруднения в применении теоретических положений при решении практических задач профессиональной направленности стандартного уровня сложности, не владеет необходимыми для этого навыками и приёмами. Демонстрирует фрагментарные знания учебной литературы по дисциплине. Оценка по дисциплине выставляются обучающемуся с учётом результатов текущей и промежуточной аттестации. Компетенции на уровне «достаточный», закреплённые за дисциплиной, не сформированы.

5.3 Оценочные средства (материалы) для текущего контроля успеваемости, промежуточной аттестации обучающихся по дисциплине

Оценочные материалы для текущего контроля успеваемости по дисциплине

Анализ нормативных правовых актов и судебных актов

Проанализируйте Конституцию Российской Федерации, выделив конституционные гарантии права граждан на информацию, заполнив следующую таблицу:

Конституционные гарантии права граждан на информацию	
Статья, часть статьи	*Основные положения*

2. Проанализируйте Постановление Правительства Российской Федерации от 31 декабря 2020 г. № 2463 ««Об утверждении Правил продажи товаров по договору розничной купли-продажи, перечня товаров длительного пользования, на которые не распространяется требование потребителя о безвозмездном предоставлении ему товара, обладающего этими же основными потребительскими свойствами, на период ремонта или замены такого товара, и перечня непродовольственных товаров надлежащего качества, не подлежащих обмену, а также о внесении изменений в некоторые акты Правительства Российской Федерации»» и письменно выделите особенности правил продажи товаров при дистанционном способе продажи товара по договору розничной купли-продажи.

3. Проанализируйте нормы Федерального закона от 27 июня 2011 № 161-ФЗ «О национальной платежной системе» и представьте письменный краткий анализ следующих положений: особенности перевода электронных денежных средств; порядок использования электронных средств платежа и требования к приему данных на территории РФ; порядок использования электронных средств платежа при осуществлении перевода электронных денежных средств.

4. Проанализируйте Постановление Конституционного Суда Российской Федерации от 27 марта 1996 г. № 8-П «По делу о проверки конституционности статей 1 и 21 Закона Российской Федерации от 221 июля 1993 года «О государственной тайне» в связи с жалобами граждан В.М. Гурджиянца, В.Н. Синцова, В.Н. Бугрова и А.К. Никитина» и заполните следующую таблицу:

Параметр	Содержание
Повод к рассмотрению	
Основание рассмотрения	
Суть (краткое содержание) жалобы	
Постановление суда	

Примеры задач

1. Лицо является автором фотографического снимка, размещенного на его странице в одной из социальных сетей. Через некоторое время после размещения фотографии, данное лицо обнаружило, что фотография используется в качестве иллюстрации статьи на другом сайте. Разрешения на использование фотографии не представлялось. **Были ли нарушены права фотографа?**

2. Обществом на сайте в сети Интернет, посвященном вопросам архитектуры, градостроительства и охраны наследия, опубликован ряд еженедельных обзоров блогов, которые являются обзорными авторскими творческими произведениями на темы архитектуры, урбанистики и охраны наследия. Эти произведения созданы конкретными авторами, чьи имена указаны для каждой публикации. Обзоры включали в себя в виде цитат фотографии и фрагменты текста различных материалов, публикуемых в сети Интернет. Обществом в числе прочих были размещены фрагменты блога предпринимателя с 22 фотографиями, исключительные авторские права на которые принадлежат предпринимателю. Спорные фотографии, исключительные права на которые принадлежат предпринимателю, были использованы в 14 еженедельных обзорных статьях в информационных целях в порядке цитирования, в том числе фоторепортажей предпринимателя, размещенных им в своем блоге. При этом на сайте предпринимателя была размещена информация о возможности свободного использования его фотографий в некоммерческих целях с указанием автора и ссылки на сайт предпринимателя. Считая, что при размещении фотографий обществом были нарушены права и законные интересы предпринимателя, последний обратился в суд с иском о взыскании компенсации. **Должна ли быть взыскана компенсация?**

4. Интернет-магазин осуществлял продажу товаров, не имеющих возрастного ограничения. При этом, при заполнении формы заказа было необходимо указать Ф.И.О., дату рождения, пол и местожительство покупателя, а также номер его телефона. Также на сайте отсутствовал документ, содержащих политику конфиденциальности. **Будет ли в данной ситуации нарушение законодательства о персональных данных?**

5. На информационном ресурсе, расположенного в сети «Интернет», была размещена статья, в которой приводился рассказ лица, употребляющего наркотические средства на протяжении нескольких лет, с высказыванием о том, что употребление наркотиков не оказало влияние на социальную и общественную жизнь данного лица. Роскомнадзором было сформировано и направлено провайдеру хостинга и владельцу сайта уведомление на русском языке об ограничении доступа к информационному ресурсу. **Были ли допущены нарушения при направлении уведомления?**

Примеры тестов

1. Началом формирования концепции международной информационной безопасности считается:

1. 1996 год.
2. 1992 год.
3. 1998 год.

2. Принятие федеральной целевой программы «Электронная Россия (2002 - 2010 годы)» положило начало:

1. цифровизации.
2. персонализации.
3. информатизации.

3. Развитие безопасного информационного пространства, защита российского общества от деструктивного информационно-психологического воздействия – это:

1.национальный интерес
2. национальный приоритет.
3. направление защиты.

4. Ст. 138 УК РФ «Нарушение тайны переписки, телефонных переговоров, почтовых, телеграфных или иных сообщений» относится к:

1. преступлениям, связанным с нарушением установленных ограничений на распространение информации определенного содержания.
2. преступлениям, связанным с нарушением режима конфиденциальности информации.
3. преступлениям, связанным с нарушением права на доступ к информации.

5. Может ли владелец агрегатора довести до сведения потребителей информацию о продавце путем размещения ссылки на сайт продавца?

1. да
2. нет
3. на усмотрение агрегатора

6. Дизайн сайта будет отнесен к объектам авторского права, если:

1. он является результатом творческого труда.
2. относится к решению технических средств.
3. дизайн не является объектом авторского права.

7. Если при оформлении электронного издания, использовалось художественное оформление другой книги (без прав на него и без согласия правообладателя), то это может быть квалифицировано как:

1. нарушение изобретательских или патентных прав
2. нарушение авторских и смежных прав
3. недобросовестная конкуренция в форме введения в оборот товара с незаконным использованием результатов интеллектуальной деятельности

8. Данные голоса человека, полученные с помощью звукозаписывающих устройств – это:

1. персональные данные общего характера.
2. персональные данные, разрешенные субъектом персональных данных для распространения.
3. биометрические персональные данные.

9. Какой доступ обязан обеспечить оператор к документу, определяющему его политику в отношении обработки персональных данных, к сведениям о реализуемых требованиях к защите персональных данных?

1. ограниченный.
2. неограниченный.
3. любой.

10. Порядок ограничения доступа к сайтам, содержащим противоправный контент может быть:

1. только судебным.
2. только внесудебным.
3. как судебным так и внесудебным.

Оценочные материалы для промежуточной аттестации обучающихся по дисциплине

Итоговый тест

1. Состояние защищенности жизненно важных интересов личности, общества и государства от внутренних и внешних угроз – называется

---

2. Термин «безопасность» был введен:

1. в 1995 г.
2. в 1992 г.
3. в 2006 г.

3. Началом формирования концепции международной информационной безопасности считается:

1. 1996 год.
2. 1992 год.
3. 1998 год.

4. Закон «О государственной тайне» был принят:

1. в 1991 г.
2. в 1992 г.
3. в 1993 г.

5. На каком этапе развития информационной безопасности ее задача сводилась к защите самих сведений об определенных фактах:

1. I этапе.
2. II этапе.
3. V этапе.

6. Ограничения вывода информации за пределы России были установлены:

1. Федеральным законом «Об участии в международном информационном обмене».
2. Федеральным законом «Об информации, информатизации и защите информации».
3. Законом РФ «О государственной тайне».

7. Впервые Доктрина об информационной безопасности РФ была принята:

1. в 1998 г.
2. в 2000 г.
3. в 2006 г.

8. Создание и развитие локальных информационно-коммуникационных сетей характеризует:

1. II этап.
2. IV этап.
3. V этап.

9. Принятие федеральной целевой программы «Электронная Россия (2002 - 2010 годы)» положило начало:

1. цифровизации.
2. персонализации.
3. информатизации.

10. Действующий Федеральный закон «Об информации, информационных технологиях и о защите информации» был принят:

1. в 2004 г.
2. в 2006 г.
3. в 2008 г.

11. Согласно Стратегии национальной безопасности РФ, безопасное информационное пространство является:

1. национальным приоритетом
2. стратегическим национальным приоритетом
3. задачей национальной безопасности

12. Правовое равенство всех участников отношений, основанное на конституционном праве граждан свободно искать, получать, передавать, производить и распространять информацию любым законным способом – это принцип:

1. соблюдения баланса
2. законности
3. конструктивного взаимодействия.

13. Мониторинг информационных угроз помогает определить:

1. достаточность сил и средств
2. соблюдение баланса
3. законность

14. Достижение и поддержание информационного суверенитета в Стратегии обеспечения информационной безопасности государств – участников СНГ – это:

1. цель обеспечения информационной безопасности.

2. задача обеспечения информационной безопасности.

3. приоритет обеспечения информационной безопасности.

15. Право на информацию в Конституции РФ закреплено в:

1. ст. 29.

2. ст. 30.

3.ст. 56.

16. Основания для ограничения информационных прав и свобод граждан определены:

1. Федеральным законом «Об информации, информационных технологиях и о защите информации»

2. Конституционным Судом РФ

3. Конституцией РФ.

17. Классификация информационной продукции установлена в:

1. Федеральном законе «Об основных гарантиях прав ребенка в Российской Федерации»

2. Федеральном законе «Об информации, информационных технологиях и о защите информации»

3. Федеральном законе «О защите детей от информации, причиняющей вред их здоровью и развитию».

18. Развитие безопасного информационного пространства, защита российского общества от деструктивного информационно-психологического воздействия – это:

1.национальный интерес

2. национальный приоритет.

3. направление защиты.

19. Система официальных взглядов на обеспечение национальной безопасности Российской Федерации в информационной сфере – это:

1. Стратегия национальной безопасности

2. Доктрина информационной безопасности

3. Основы государственной политики Российской Федерации в области международной информационной безопасности.

20. Противодействию угрозе использования информационно-коммуникационных технологий в целях подрыва (ущемления) суверенитета – это:

1. задача государственной политики в области международной информационной безопасности.

2. направление государственной политики в области международной информационной безопасности.

3. цель государственной политики в области международной информационной безопасности.

21. Процесс создания оптимальных условий максимально полного удовлетворения информационно-правовых потребностей государственных и общественных структур, предприятий, организаций, учреждений и граждан на основе эффективной организации и использования информационных ресурсов с применением прогрессивных технологий – это:

1. правовая информатизация.

2. правовая цифровизация.

3. правовая автоматизация.

22. Обеспечение единства государственных стандартов в сфере информатизации – это:

1. цель государственной политики в сфере информатизации.

2. задача государственной политики в сфере информатизации.

3. направление государственной политики в сфере информатизации.

23. Неблагоприятные имущественные последствия, которые виновное лицо должно понести в целях компенсации потерь потерпевшего от его неправомерных действий лица – это:

1. материальная ответственность.

2. дисциплинарная ответственность.

3. гражданско-правовая ответственность.

24. Ст. 138 УК РФ «Нарушение тайны переписки, телефонных переговоров, почтовых, телеграфных или иных сообщений» относится к:

1. преступлениям, связанным с нарушением установленных ограничений на распространение информации определенного содержания.

2. преступлениям, связанным с нарушением режима конфиденциальности информации.

3. преступлениям, связанным с нарушением права на доступ к информации.

25. Основным видом административного наказания за нарушения требований информационной безопасности является:

1. конфискация.

2. административный штраф.

3. административное приостановление деятельности.

26. Если работником были разглашены сведения, составляющие охраняемую законом тайну, то он:

1. возмещает полный размер причиненного ущерба.

2. возмещает прямой действительный ущерб.

3. размер возмещения определяется работодателем.

27. Последствия применения мер дисциплинарной ответственности:

1. могут быть определены в локальных актах.

2. определяются в приказе (распоряжении).

3. определяются исключительно Трудовым кодексом.

28. Выговор – это вид:

1. дисциплинарного проступка.

2. дисциплинарного взыскания.

3. дисциплинарной ответственности.

29. Неисполнение или ненадлежащее исполнение работником по его вине возложенных на него трудовых обязанностей – это:

1. дисциплинарная ответственность.

2. материальная ответственность.

3. дисциплинарный проступок.

30. Федеральный закон «Об информации, информационных технологиях и о защите информации»:

1. устанавливает отсылочную норму об ответственности за нарушение закона.

2. указывает конкретные виды правонарушений.

3. не содержит нормы об ответственности за нарушение закона.

31. Хозяйственная деятельность, в которой ключевым фактором производства являются данные в цифровом виде, обработка больших объемов и использование результатов анализа которых по сравнению с традиционными формами хозяйствования позволяют существенно повысить эффективность различных видов производства, технологий, оборудования, хранения, продажи, доставки товаров и услуг – это:

1. экосистема цифровой экономики.

2. цифровая экономика.

3. цифровая технология.

32. Партнерство организаций, обеспечивающее постоянное взаимодействие принадлежащих им технологических платформ, прикладных интернет-сервисов, аналитических систем, информационных систем органов государственной власти Российской Федерации, организаций и граждан – это:

1. экосистема цифровой экономики.

2. цифровая экономика.

3. цифровая технология.

33. Автоматизированные системы управления субъектов критической информационной инфраструктуры относятся к:

1. субъектам критической информационной инфраструктуры.
2. объектам критической информационной инфраструктуры.
3. видам критической информационной инфраструктуры

34. Обеспечение правового благоприятного режима развития современных технологий относится к:

1. Информационной инфраструктуре.
2. Нормативному регулированию цифровой среды.
3. Цифровому государственному управлению.

35. Преобразование приоритетных отраслей экономики и социальной сферы, посредством внедрения цифровых технологий и платформенных решений относится к:

1. Цифровым технологиям.
2. Нормативному регулированию цифровой среды.
3. Цифровому государственному управлению.

36. ГосСОПКА создана Указом Президента РФ в:

1. 2011 году.
2. 2013 году.
3. 2015 году.

37. Приводится ли в законодательстве понятие «интернет-аккаунт»?

1. да.
2. нет.
3. приводится, но не раскрывается.

38. Добровольное предоставление доступа к аккаунту обычно рассматривается как:

1. действие в чужом интересе.
2. представительство.
3. неправомерное действие.

39. Приводится ли в законодательстве понятие «учетная запись»?

1. да.
2. нет.
3. приводится, но не раскрывается.

40. Может ли небанковская кредитная организация быть субъектом национальной платежной системы?

1. да, может
2. нет, не может
3. может в исключительных случаях

41. ГАТС было принято в:

1. 1994 г.
2. 1998 г.
3. 2000 г.

*42. Покупатель приобрел в онлайн-магазине товар, который был надлежащего качества. Товар доставлен вовремя. После передачи товара, спустя 12 дней покупатель решил отказаться от товара. Имеет ли он право на такой отказ? Обоснуйте свой ответ*_____
_____
_____

43. Может ли владелец агрегатора довести до сведения потребителей информацию о продавце путем размещения ссылки на сайт продавца?

1. да
2. нет
3. на усмотрение агрегатора

44. При предоставлении недостоверной информации о товаре агрегатор:

1. несет ответственность за убытки, причиненные покупателю.

2. несет дисциплинарную ответственность.

3. несет административную ответственность.

45. Предъявление претензии непосредственно продавцу является таким способом защиты прав как:

1. самозащита права.

2. признание права.

3. возмещение убытков.

46. Понятие электронной коммерции:

1. закреплено в законодательстве.

2. не закреплено в законодательстве.

3. в законодательстве данный термин используется, но не раскрывается.

47. Если за товар внесена оплата на банковский счет владельца агрегатора, и указанный товар не был передан в срок, то потребитель вправе:

1. предъявить требование к продавцу о возврате суммы предварительной оплаты

2. предъявить требование к владельцу агрегатора о возврате суммы предварительной оплаты.

3. обратиться в суд.

48. Обязан ли продавец доводить до покупателя информацию о форме и способах направления претензий?

1. обязан.

2. не обязан.

3. обязан по запросу покупателя.

49. Дистанционным способом могут продаваться:

1. любые товары.

2. установлено ограничение продажи отдельных видов товаров.

3. установлен перечень товаров, которые могут продаваться дистанционным способом.

50. Типовой закон об электронной торговле был принят:

1. Генеральной Ассамблеей ООН.

2. Всемирной торговой организацией (ВТО).

3. Международным институтом унификации частого права (УНИДРУА).

51. Совершенствование антимонопольного законодательства – это:

1. условие реализации национального интереса в области цифровой экономики.

2. национальный интерес в области цифровой экономики.

3. показатель реализации Стратегии развития информационного общества.

52. Создание специальных центров, занимающихся обработкой данных относится к:

1. Нормативному регулированию цифровой среды.

2. Цифровым технологиям.

3. Информационной инфраструктуре.

53. Типовой закон об электронной был разработан:

1. Комиссия Организации Объединенных Наций по праву международной торговли (ЮНСИТРАЛ).

2. Международным институтом унификации частого права (УНИДРУА)

3. Всемирной торговой организацией (ВТО).

54. Доведение по потребителя информации о сроке службы и годности товара является стадией:

1. информирования покупателя.

2. заключения договора.

3. исполнения договора.

55. Внедрение цифровых технологий и платформенных решений в сфере оказания государственных услуг – это:

1. Цифровое государственное управление.

2. Цифровые технологии.

3. Нормативное регулирование цифровой среды.

56. Будет ли номер заказа являться подтверждением заключения договора при онлайн-продаже товара?

1. нет, номер заказа подтверждением не является.

2. да, номер заказа является подтверждением.

57. Передача приобретенного дистанционным способом товара осуществляется:

1. только покупателю.

2. любому лицу.

3. любому лицу, который предъявил информацию и номер заказа.

58. Если товар был оплачен, то при нарушении срока доставки продавец:

1. возвращает оплату доставки.

2. уплачивает неустойку (пени).

3. расторгает договор.

59. Снижение времени реагирования по блокировке распространения фишинговых сайтов – это такое направление обеспечения информационной безопасности цифровой экономики как:

1. Цифровое государственное управление.

2. Повышение уровня защищенности информационных систем и ресурсов.

3. Создание условий для снижения количества правонарушений с использованием информационных технологий.

60. Формирование институциональной системы (среды) для развития исследовательской деятельности, разработок в сфере цифровой экономики относится к:

1. Цифровым технологиям.

2. Информационной безопасности.

3. Цифровому государственному управлению.

61. Отказ от личных неимущественных прав:

1. признается.

2.ничтожен.

3. признается в исключительных случаях.

62. Фонограмма является объектом:

1. авторского права.

2. смежного права.

3. патентного права.

63. Дизайн сайта будет отнесен к объектам авторского права, если:

1. он является результатом творческого труда.

2. относится к решению технических средств.

3. дизайн не является объектом авторского права.

64. Наложение цифрового водяного знака является:

1. криптографией.

2. цифровым отпечатком.

3. цифровой маркировкой.

65. Публикация решения суда о допущенном нарушении является способом:

1. защиты личных неимущественных прав.

2. защиты исключительных прав.

3. защиты и личных неимущественных и исключительных прав.

66. Изъятие материального носителя является способом:

1. защиты личных неимущественных прав.

2. защиты исключительных прав.

3. защиты и личных неимущественных и исключительных прав.

67. Иск может быть предъявлен, если на претензию не был получен ответ в течение:

1. 10 дней.

2. 20 дней.

3. 30 дней.

68. Может ли быть взыскана компенсация морального вреда при нарушении исключительных прав?

1. может
2. не может
3. может в исключительных случаях

69. Право требовать выплаты компенсации имеет обладатель исключительного права на момент:

1. обращения в суд.
2. нарушения права.
3. вынесения судебного решения.

70. Может ли суд по собственной инициативе изменять способ расчета суммы компенсации?

1. да, может.
2. да, может, при согласовании со сторонами.
3. нет, не может.

71. Признается ли скриншот экрана допустимым доказательством в суде?

1. да, признается.
2. признается в исключительных случаях.
3. нет, не признается.

72. Незаконное использование экземпляров произведений может быть квалифицировано как:

1. нарушение изобретательских или патентных прав
2. нарушение авторских и смежных прав
3. недобросовестная конкуренция в форме введения в оборот товара с незаконным использованием результатов интеллектуальной деятельности

73. Незаконное использование средств индивидуализации товаров (работ, услуг) уголовно-наказуемо в случае, если оно:

1. совершено неоднократно.
2. причинило значительный ущерб.
3. лицо до этого было привлечено к административной ответственности.

74. Если при оформлении электронного издания, использовалось художественное оформление другой книги (без прав на него и без согласия правообладателя), то это может быть квалифицировано как:

1. нарушение изобретательских или патентных прав
2. нарушение авторских и смежных прав
3. недобросовестная конкуренция в форме введения в оборот товара с незаконным использованием результатов интеллектуальной деятельности

*75. Как Вы считаете, будет ли неоднократностью одновременное использование двух и более чужих товарных знаков на одной единице товара? Обоснуйте свое мнение*_____
_____
_____
_____
_____

76. Будет ли считаться плагиатом издание лицом исключительно под своим именем произведения, созданного в соавторстве?

1. да, будет.
2. нет, не считается.
3. да, при условии причинения крупного ущерба.

77. Признание права является способом защиты:

1. личных неимущественных прав.

2. исключительных прав.

3. и личных неимущественных и исключительных прав.

78. Свободное использование фотографии, размещенной в социальной сети возможно при соблюдении следующих условий:

1. использование в информационных, научных, учебных или культурных целях; обязательное указание автора; указание источника заимствования; в объеме, оправданном целью цитирования.

2. использование в информационных, научных, учебных или культурных целях; обязательное указание автора; указание источника заимствования; в объеме, оправданном целью цитирования; направлением автору фотографии уведомления об ее использовании.

3. подобное использование не допускается.

79. Право следования относится к:

1. исключительным права.

2. личным неимущественным правам.

3. иным правам.

80. Интеллектуальные права на полезную модель являются:

1. патентными правами.

2. авторскими правами.

3. смежными правами.

81. Федеральный закон «О персональных данных» принят в:

1. 2004 г.

2. 2006 г.

3. 2010 г.

82. Данные голоса человека, полученные с помощью звукозаписывающих устройств – это:

1. персональные данные общего характера.

2. персональные данные, разрешенные субъектом персональных данных для распространения.

3. биометрические персональные данные.

83. Религиозные убеждения относятся к:

1. персональным данным общего характера.

2. специальным категориям персональных данных.

3. персональным данным, разрешенным субъектом персональных данных для распространения.

84. Действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных – это _____
_____

85. Моральный вред при нарушении законодательства о персональных данных:

1. возмещается в зависимости от того, возмещен ли имущественный вред.

2. не возмещается.

3. возмещается вне зависимости от того, возмещен ли имущественный вред.

86. Влечет ли нарушение законодательства о персональных данных материальную ответственность работника?

1. нет.

2. всегда влечет.

3. влечет при наличии определенных условий, установленных законодательством.

87. Может ли разглашение персональных данных другого работника стать основанием для расторжения трудового договора работодателем?

1. да.

2. нет.

3. в исключительных случаях.

88. Существует ли специальная норм об уголовной ответственности при нарушении законодательства о персональных данных?

1. да.

2. нет, к уголовной ответственности такое лицо не привлекается.

3. нет, но при нарушении работы с персональными данными, возможно привлечение к уголовной ответственности.

89. Если на сайте онлайн-магазина отсутствует документ, содержащих политику конфиденциальности, однако для покупки товара без возрастного ограничения, требуется заполнить форму с указанием персональных данных (Ф.И.О., возраст, место жительства, телефон), будет ли это нарушением законодательства о персональных данных? Свой ответ обоснуйте _____
_____
_____
_____

90. Какой доступ обязан обеспечить оператор к документу, определяющему его политику в отношении обработки персональных данных, к сведениям о реализуемых требованиях к защите персональных данных?

1. ограниченный.

2. неограниченный.

3. любой.

91. Закреплено ли понятие «деструктивный контент» в законодательстве РФ?

1. закреплено.

2. не закреплено.

3. закреплено, но не раскрывается.

92. Оскорбление, совершенное публично в сети «Интернет» является:

1. информацией, распространение которой запрещено.

2. информацией, распространение которой ограничено.

3. законодательно не регламентировано.

93. Используется ли понятие «противоправный контент» в законодательстве РФ?

1. используется.

2. не используется.

3. используется, но не раскрывается.

94. Может ли постановление судебного пристава-исполнителя об ограничении доступа к информации, распространяемой в сети «Интернет» быть основанием для включения в Единый реестр доменных имен, указателей страниц сайтов в информационно-телекоммуникационной сети "Интернет" и сетевых адресов, позволяющих идентифицировать сайты в информационно-телекоммуникационной сети "Интернет", содержащие информацию, распространение которой в Российской Федерации запрещено?

1. да.

2. нет.

3. да, при условии, что данная информация порочит честь, достоинство или деловую репутацию гражданина либо деловую репутацию юридического лица.

95. В отношении информации по организации и проведению азартных игр и лотерей с использованием сети "Интернет" уполномоченным органом по решению, являющему основанием для включения в соответствующий Реестр, является:

1. Министерство внутренних дел России.

2. Федеральная налоговая служба.

3. Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций.

96. Основанием для блокировки сайта иностранного СМИ, выполняющего функции иностранного агента и определенного в этом качестве в соответствии с законом о средствах массовой информации (либо учрежденного им российского юридического лица), является:

1. постановление по делу об административном правонарушении

2. постановление по делу об административном правонарушении нарушения порядка деятельности такого СМИ

3. вступившее в законную силу постановление по делу об административном правонарушении нарушения порядка деятельности такого СМИ.

97. Порядок ограничения доступа к сайтам, содержащим противоправный контент может быть:

1. только судебным.

2. только внесудебным.

3. как судебным так и внесудебным.

98. В отношении распространяемой посредством сети "Интернет" информации, содержащей предложения о розничной продаже дистанционным способом алкогольной продукции уполномоченным органом по решению, являющему основанием для включения в соответствующий Реестр, является:

1. Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций.

2. Министерство внутренних дел России.

3. Федеральная служба по регулированию алкогольного рынка

99. Провайдеру хостинга направляется уведомление о включении в Единый реестр доменных имен, указателей страниц сайтов в информационно-телекоммуникационной сети "Интернет" и сетевых адресов, позволяющих идентифицировать сайты в информационно-телекоммуникационной сети "Интернет", содержащие информацию, распространение которой в Российской Федерации запрещено:

1. За сутки до включения в Реестр.

2. Одновременно с включением в Реестр.

3. После включения в Реестр.

100. в отношении распространяемой посредством сети "Интернет" информации, направленной на склонение или иное вовлечение несовершеннолетних в совершение противоправных действий уполномоченным органом по решению, являющему основанием для включения в соответствующий Реестр, является:

1. Федеральное агентство по делам молодежи

2. Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций.

3. Министерство внутренних дел России.

6. Учебно-методическое и информационное обеспечение дисциплины

6.1 Список источников и литературы

Источники

Основные

1. Конституция Российской Федерации от 12 декабря 1993 // СПС «Консультант Плюс»

2. Федеральный закон от 27 июля 2006 № 152-ФЗ «О персональных данных» // СПС «Консультант Плюс».

3. Федеральный закон от 27 июля 2006 N 149-ФЗ «Об информации, информационных технологиях и о защите информации» // СПС «Консультант Плюс».

4. Гражданский кодекс Российской Федерации (часть четвертая) от 18 декабря 2006 N 230-ФЗ // СПС «Консультант Плюс».

5. Кодекс Российской Федерации об административных правонарушениях от 30 декабря 2001 № 195-ФЗ // СПС «Консультант Плюс»

6. Трудовой кодекс Российской Федерации от 30 декабря 2001 № 195-ФЗ // СПС «Консультант Плюс».

7. Уголовный кодекс Российской Федерации от 13 июня 1996 № 63-ФЗ // СПС «Консультант Плюс»

8. Гражданский кодекс Российской Федерации (часть вторая) от 26 января 1996 N 14-ФЗ // СПС «Консультант Плюс».

9. Гражданский кодекс Российской Федерации (часть первая) от 30 ноября 1994 г. N 51-ФЗ // СПС «Консультант Плюс».

10. Постановление Правительства РФ от 26 октября 2012 N 1101 «О единой автоматизированной информационной системе "Единый реестр доменных имен, указателей страниц сайтов в информационно-телекоммуникационной сети "Интернет" и сетевых адресов, позволяющих идентифицировать сайты в информационно-телекоммуникационной сети "Интернет", содержащие информацию, распространение которой в Российской Федерации запрещено» // СПС «Консультант Плюс».

Дополнительные

1. Всеобщая Декларации прав человека (1948 г.) // СПС «Консультант Плюс».

2. Международный пакт о гражданских и политических правах (1966 г.) // СПС «Консультант Плюс».

3. Основы государственной политики Российской Федерации в области международной информационной безопасности (утверждены Указом Президента РФ от 12 апреля 2021 № 213) // СПС «Консультант Плюс».

4. Федеральный закон от 27 июня 2011 № 161-ФЗ «О национальной платежной системе» // СПС «Консультант Плюс».

5. Постановление Федерального арбитражного суда Волго-Вятского округа от 27 апреля 2011 г. по делу № А82-12456/2010 // СПС «Консультант Плюс».

6. Письмо Федеральной налоговой службы от 31 марта 2016 г. № СА-4-7/5589 // СПС «Консультант Плюс»

7. Приказ Роскомнадзора от 6 июля 2010 № 420 «Об утверждении порядка направления обращений о недопустимости злоупотреблений свободой массовой информации к средствам массовой информации, распространение которых осуществляется в информационно-телекоммуникационных сетях, в том числе в сети Интернет» // СПС «Консультант Плюс».

Литература

Основная

1. Гаврилов, Л. П. Электронная коммерция : учебник и практикум для вузов / Л. П. Гаврилов. — 4-е изд. — Москва : Издательство Юрайт, 2022. — 521 с. // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/489784

2. Жарова, А. К. Правовое регулирование создания и использования информационной инфраструктуры в Российской Федерации : монография / А. К. Жарова. — Москва : Издательство Юрайт, 2022. — 301 с. // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/496939

3. Информационное право : учебник для вузов / М. А. Федотов [и др.] ; под редакцией М. А. Федотова. — Москва : Издательство Юрайт, 2022. — 497 с. // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/489946

4. Организационное и правовое обеспечение информационной безопасности : учебник и практикум для вузов / под редакцией Т. А. Поляковой, А. А. Стрельцова. — Москва : Издательство Юрайт, 2022. — 325 с. // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/498844

5. Рассолов, И. М. Информационное право : учебник и практикум для вузов / И. М. Рассолов. — 6-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2022. — 415 с. // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/488767

6. Суворова, Г. М. Информационная безопасность : учебное пособие для вузов / Г. М. Суворова. — Москва : Издательство Юрайт, 2022. — 253 с. // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/496741

7. Щербак, Н. В. Право интеллектуальной собственности: общее учение. Авторское право и смежные права : учебное пособие для вузов / Н. В. Щербак. — Москва : Издательство Юрайт, 2022. — 309 с. // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/495164

Дополнительная

1. Алисова Е.В. Актуальные проблемы защиты авторского права в сети Internet // Современные научные исследования и инновации. 2016. № 7. – URL: https://web.snauka.ru/issues/2016/07/69396.

2. Ванюшина Е. А. Технические средства защиты авторских прав в сети Интернет / Е. А. Ванюшина // Молодой ученый. – 2021. – № 53 (395). Режим доступа: URL: https://moluch.ru/archive/395/87447/

3. Воробьева А.А., Пантюхин И.С. История развития программно–аппаратных средств защиты информации.– СПб: Университет ИТМО, 2017 – 62 с. – Режим доступа: https://books.ifmo.ru/file/pdf/2188.pdf.

4. Вострецова Е.В. Основы информационной безопасности: учебное пособие. – Екатеринбург: Издательство Уральского университета, 2019. – Режим доступа: https://elar.urfu.ru/bitstream/10995/73899/3/978-5-7996-2677-8_2019.pdf

5. Ганжа К.П. Правовое регулирование электронной коммерции в России // Электронный научно-практический журнал «Современные научные исследования и инновации» // Режим доступа: https://web.snauka.ru/issues/2013/10/27833

6. Жигулин Г.П. Организационное и правовое обеспечение информационной безопасности. – СПб: СПбНИУТМО, 2014. – Режим доступа: https://books.ifmo.ru/file/pdf/1484.pdf

7. Зенков, А. В. Информационная безопасность и защита информации : учебное пособие для вузов / А. В. Зенков. — Москва : Издательство Юрайт, 2022. — 104 с. // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/497002

8. Маркетинговое исследование Интернет-торговля в России 2021 // Режим доступа: https://datainsight.ru/eCommerce_2021.

9. Международная информационная безопасность: Теория и практика: В трех томах. Том 2: Сборник документов (на русском языке) / Под общ. ред. А.В. Крутских. 2-е изд., доп. М.: Издательство «Аспект Пресс», 2021. – С. 225 (История переговорного процесса по международной информационной безопасности в ООН // Международная информационная безопасность: подходы России). – Режим доступа: https://mgimo.ru/upload/2022/03/mezhdunarodnaya-informatsionnaya-bezopasnost-podkhody-rossii.pdf

10. Смоляков П.Н. Ответственность за нарушение законодательства о персональных данных // СПС Консультант Плюс. 2022.

11. Холодкова К.С. Анализ рынка электронной коммерции в России // Современные научные исследования и инновации. 2013. № 10. – Режим доступа: http://web.snauka.ru/issues/2013/10/26760

12. Проект Федерального закона «Об электронной торговле» (режим доступа: https://sozd.duma.gov.ru/bill/11081-3)

6.2 Перечень ресурсов информационно-телекоммуникационной сети «Интернет».

ELibrary.ru Научная электронная библиотека www.elibrary.ru

6.3 Профессиональные базы данных и информационно-справочные системы

Информационные справочные системы:
1. Консультант Плюс
2. Гарант

7. Материально-техническое обеспечение дисциплины

Для обеспечения дисциплины используется материально-техническая база образовательного учреждения: учебные аудитории, оснащённые компьютером, проектором и аудиосистемой для демонстрации учебных материалов.

Состав программного обеспечения:
1. Windows
2. Microsoft Office
3. Kaspersky Endpoint Security

8. Обеспечение образовательного процесса для лиц с ограниченными возможностями здоровья и инвалидов

В ходе реализации дисциплины используются следующие дополнительные методы обучения, текущего контроля успеваемости и промежуточной аттестации обучающихся в зависимости от их индивидуальных особенностей:

- для слепых и слабовидящих: лекции оформляются в виде электронного документа, доступного с помощью компьютера со специализированным программным обеспечением; письменные задания выполняются на компьютере со специализированным программным обеспечением или могут быть заменены устным ответом; обеспечивается индивидуальное равномерное освещение не менее 300 люкс; для выполнения задания при необходимости предоставляется увеличивающее устройство; возможно также использование собственных увеличивающих устройств; письменные задания оформляются увеличенным шрифтом; экзамен и зачёт проводятся в устной форме или выполняются в письменной форме на компьютере.
- для глухих и слабослышащих: лекции оформляются в виде электронного документа, либо предоставляется звукоусиливающая аппаратура индивидуального пользования; письменные задания выполняются на компьютере в письменной форме; экзамен и зачёт проводятся в письменной форме на компьютере; возможно проведение в форме тестирования.
- для лиц с нарушениями опорно-двигательного аппарата: лекции оформляются в виде электронного документа, доступного с помощью компьютера со специализированным программным обеспечением; письменные задания выполняются на компьютере со специализированным программным обеспечением; экзамен и зачёт проводятся в устной форме или выполняются в письменной форме на компьютере.

При необходимости предусматривается увеличение времени для подготовки ответа.

Процедура проведения промежуточной аттестации для обучающихся устанавливается с учётом их индивидуальных психофизических особенностей. Промежуточная аттестация может проводиться в несколько этапов.

При проведении процедуры оценивания результатов обучения предусматривается использование технических средств, необходимых в связи с индивидуальными особенностями обучающихся. Эти средства могут быть предоставлены университетом, или могут использоваться собственные технические средства.

Проведение процедуры оценивания результатов обучения допускается с использованием дистанционных образовательных технологий.

Обеспечивается доступ к информационным и библиографическим ресурсам в сети Интернет для каждого обучающегося в формах, адаптированных к ограничениям их здоровья и восприятия информации:

- для слепых и слабовидящих: в печатной форме увеличенным шрифтом, в форме электронного документа, в форме аудиофайла.
- для глухих и слабослышащих: в печатной форме, в форме электронного документа.
- для обучающихся с нарушениями опорно-двигательного аппарата: в печатной форме, в форме электронного документа, в форме аудиофайла.

Учебные аудитории для всех видов контактной и самостоятельной работы, научная библиотека и иные помещения для обучения оснащены специальным оборудованием и учебными местами с техническими средствами обучения:

- для слепых и слабовидящих: устройством для сканирования и чтения с камерой SARA CE; дисплеем Брайля PAC Mate 20; принтером Брайля EmBraille ViewPlus;
- для глухих и слабослышащих: автоматизированным рабочим местом для людей с нарушением слуха и слабослышащих; акустический усилитель и колонки;
- для обучающихся с нарушениями опорно-двигательного аппарата: передвижными, регулируемыми эргономическими партами СИ-1; компьютерной техникой со специальным программным обеспечением.

9. Методические материалы

9.1 Планы семинарских занятий

№	Наименование раздела дисциплины	Содержание
1	Ретроспективный анализ правовых норм об информационной безопасности	**Контрольные вопросы:** 1. Раскройте основные этапы развития информационной безопасности. 2. Охарактеризуйте развитие законодательства об информационной безопасности в России. 3. Какое значение судебных актов в развитии законодательства об информационной безопасности в России. **Практические задания** (сравнительный анализ нормативных правовых актов, анализ актов судебной власти) **Тестирование по теме**
2	Система законодательства об информационной безопасности	**Контрольные вопросы** 1. Дайте понятие информационной безопасности. 2. Раскройте основные принципы государственной политики об информационной безопасности. 3. Охарактеризуйте систему законодательства РФ об информационной безопасности. 4. Роль и значение Конституции Российской Федерации в обеспечении информационной безопасности. 5. Система федеральных законодательных актов об информационной безопасности. 6. Охарактеризуйте основные подзаконные акты об информационной безопасности. 7. Раскройте виды юридической ответственности за нарушение норм законодательства об информационной безопасности.

		Практические задания (анализ нормативных правовых актов) **Тестирование по теме**
3	Информационная безопасность в сфере экономической деятельности	**Контрольные вопросы** 1. Понятие цифровой экономики и ее стратегический характер. 2. Структура национальной программы «Цифровая экономика». 3. Основные направления обеспечения информационной безопасности цифровой экономики. 4. Понятие интернет-аккаунта. 5. Квалификация действий под чужим аккаунтом при добровольном предоставлении доступа к аккаунту. 6. Использование третьим лицом аккаунта против воли владельца. 7. Понятие и значение электронной коммерции. 8. Стадии договора о покупке товара дистанционным способом. 9. Защита нарушенных прав при электронной коммерции. **Практические задания** (анализ нормативных правовых актов) **Тестирование по теме**
4	Защита объектов интеллектуальной собственности в киберпространстве	**Контрольные вопросы** 1. Понятие интеллектуальной собственности и его объекты. 2. Особенности ответственности информационного посредника. 3. Правовые способы защиты интеллектуальных прав. 4. Технические средства и способы защиты авторских прав в сети Интернет. 5. Защита личных неимущественных прав. 6. Защита исключительных прав. 7. Административная ответственность за нарушение интеллектуальных прав. 8. Уголовная ответственность за нарушение интеллектуальных прав. Практическое задание (решение задач) Тестирование по теме
5	Защита персональных данных в цифровой среде	**Контрольные вопросы** 1. Понятие и категории персональных данных. 2. Обязанности оператора персональных данных субъекта. 3. Правовые способы защиты персональных данных. **Практическое задание** (решение задач) **Тестирование по теме**
6	Правовая защита от деструктивного контента в цифровой среде	**Контрольные вопросы** 1. Понятие деструктивного контента.

		2. Информация, распространение которой на территории РФ запрещено. 3. Правовые меры ограничения доступа к сайтам, содержащим противоправный контент. **Практическое задание** (решение задач) **Тестирование по теме**

9.2 Глоссарий по дисциплине

Автор – гражданин, творческим трудом которого создан результат интеллектуальной деятельности.

Авторские права – интеллектуальные права на произведения науки, литературы и искусства.

Административное правонарушение – противоправное виновное действие (бездействие) физического или юридического лица, за которое Кодексом РФ об административных правонарушениях или законами субъектов РФ об административных правонарушениях установлена административная ответственность.

Владелец агрегатора информации о товарах (услугах) – организация независимо от организационно-правовой формы либо индивидуальный предприниматель, которые являются владельцами программы для электронных вычислительных машин и (или) владельцами сайта и (или) страницы сайта в информационно-телекоммуникационной сети "Интернет" и которые предоставляют потребителю в отношении определенного товара (услуги) возможность одновременно ознакомиться с предложением продавца (исполнителя) о заключении договора купли-продажи товара (договора возмездного оказания услуг), заключить с продавцом (исполнителем) договор купли-продажи (договор возмездного оказания услуг), а также произвести предварительную оплату указанного товара (услуги) путем наличных расчетов либо перевода денежных средств владельцу агрегатора в рамках применяемых форм безналичных расчетов.

Владелец сайта в сети "Интернет" – лицо, самостоятельно и по своему усмотрению определяющее порядок использования сайта в сети "Интернет", в том числе порядок размещения информации на таком сайте.

Государственная тайна – защищаемые государством сведения в области его военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб безопасности Российской Федерации.

Дисциплинарный проступок – неисполнение или ненадлежащее исполнение работником по его вине возложенных на него трудовых обязанностей.

Идентификация – совокупность мероприятий по установлению сведений о лице и их проверке, осуществляемых в соответствии с федеральными законами и принимаемыми в соответствии с ними нормативными правовыми актами, и сопоставлению данных сведений с уникальным обозначением (уникальными обозначениями) сведений о лице, необходимым для определения такого лица.

Интеллектуальная собственность – результаты интеллектуальной деятельности и приравненные к ним средствами индивидуализации юридических лиц, товаров, работ, услуг и предприятий, которым предоставляется правовая охрана.

Интернет-аккаунт – учетная запись определенного пользователя, расположенная в информационной системе, которая идентифицирует данного пользователя, а также содержит в себе определенные (дополнительные по отношению к идентификационным) данные.

Информационная безопасность – состояние защищенности личности, общества и государства от внутренних и внешних информационных угроз, при котором обеспечиваются реализация конституционных прав и свобод человека и гражданина, достойные качество и

уровень жизни граждан, суверенитет, территориальная целостность и устойчивое социально-экономическое развитие Российской Федерации, оборона и безопасность государства.

Информационно-коммуникационная сеть – технологическая система, предназначенная для передачи по линиям связи информации, доступ к которой осуществляется с использованием средств вычислительной техники.

Информационные технологии – процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов.

Информационный посредник – лицо, осуществляющее передачу материала в информационно- телекоммуникационной сети, в том числе в сети "Интернет", лицо, предоставляющее возможность размещения материала или информации, необходимой для его получения с использованием информационно-телекоммуникационной сети, лицо, предоставляющее возможность доступа к материалу в этой сети.

Информация – сведения (сообщения, данные) независимо от формы их представления.

Исполнитель – организация независимо от ее организационно-правовой формы, а также индивидуальный предприниматель, выполняющие работы или оказывающие услуги потребителям по возмездному договору.

Конфиденциальность информации – обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя.

Критическая информационная инфраструктура – объекты критической информационной инфраструктуры, а также сети электросвязи, используемые для организации взаимодействия таких объектов.

Моральный вред – физические и нравственные страдания, причиненные гражданину действиями, нарушающими его личные неимущественные права либо посягающими на принадлежащие гражданину нематериальные блага.

Обезличивание персональных данных – действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных.

Обработка персональных данных – любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных.

Объект авторских прав – произведения науки, литературы и искусства независимо от достоинств и назначения произведения, а также от способа его выражения.

Объекты критической информационной инфраструктуры – информационные системы, информационно-телекоммуникационные сети, автоматизированные системы управления субъектов критической информационной инфраструктуры.

Персональные данные – любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных).

Потребитель – гражданин, имеющий намерение заказать или приобрести либо заказывающий, приобретающий или использующий товары (работы, услуги) исключительно для личных, семейных, домашних и иных нужд, не связанных с осуществлением предпринимательской деятельности.

Правовая информатизация – процесс создания оптимальных условий максимально полного удовлетворения информационно-правовых потребностей государственных и общественных структур, предприятий, организаций, учреждений и граждан на основе эффективной организации и использования информационных ресурсов с применением прогрессивных технологий.

Представительство – совершение сделки одним лицом (представителем) от имени другого лица (представляемого) в силу полномочия, основанного на доверенности, указании закона либо акте уполномоченного на то государственного органа или органа местного самоуправления, создающей, изменяющей или и прекращающей гражданские права и обязанности представляемого.

Преступление – виновно совершенное общественно опасное деяние, запрещенное Уголовным кодексом РФ под угрозой наказания.

Провайдер хостинга – лицо, оказывающее услуги по предоставлению вычислительной мощности для размещения информации в информационной системе, постоянно подключенной к сети "Интернет".

Продавец – организация независимо от ее организационно-правовой формы, а также индивидуальный предприниматель, реализующие товары потребителям по договору купли-продажи.

Распространение информации – действия, направленные на получение информации неопределенным кругом лиц или передачу информации неопределенному кругу лиц.

Сайт в сети "Интернет" – совокупность программ для электронных вычислительных машин и иной информации, содержащейся в информационной системе, доступ к которой обеспечивается посредством информационно-телекоммуникационной сети "Интернет" по доменным именам и (или) по сетевым адресам, позволяющим идентифицировать сайты в сети "Интернет".

Скриншот – распечатки материалов, размещенных в информационно-телекоммуникационной сети.

Страница сайта в сети "Интернет" (интернет-страница) – часть сайта в сети "Интернет", доступ к которой осуществляется по указателю, состоящему из доменного имени и символов

Технические средства защиты авторских прав – любые технологии, технические устройства или их компоненты, контролирующие доступ к произведению, предотвращающие либо ограничивающие осуществление действий, которые не разрешены автором или иным правообладателем в отношении произведения.

Уничтожение персональных данных – действия, в результате которых становится невозможным восстановить содержание персональных данных в информационной системе персональных данных и (или) в результате которых уничтожаются материальные носители персональных данных.

Цифровая экономика – хозяйственная деятельность, в которой ключевым фактором производства являются данные в цифровом виде, обработка больших объемов и использование результатов анализа которых по сравнению с традиционными формами хозяйствования позволяют существенно повысить эффективность различных видов производства, технологий, оборудования, хранения, продажи, доставки товаров и услуг.

Экосистема цифровой экономики – партнерство организаций, обеспечивающее постоянное взаимодействие принадлежащих им технологических платформ, прикладных интернет-сервисов, аналитических систем, информационных систем органов государственной власти Российской Федерации, организаций и граждан.

Электронная коммерция – система экономических отношений, которые осуществляются с использованием Интернета; совершение транзакций (сделок) через сеть Интернет.

Электронная подпись – информация в электронной форме, которая присоединена к другой информации в электронной форме (подписываемой информации) или иным образом связана с такой информацией и которая используется для определения лица, подписывающего информацию.

Электронное средство платежа – средство и (или) способ, позволяющие клиенту оператора по переводу денежных средств составлять, удостоверять и передавать распоряжения в целях осуществления перевода денежных средств в рамках применяемых форм безналичных

расчетов с использованием информационно-коммуникационных технологий, электронных носителей информации, в том числе платежных карт, а также иных технических устройств.

Приложение 1. Аннотация
рабочей программы дисциплины

АННОТАЦИЯ РАБОЧЕЙ ПРОГРАММЫ ДИСЦИПЛИНЫ

Цель дисциплины – комплексное изучение правовой безопасности в информационном пространстве, в том числе особенностей регламентации различных областей деятельности и юридической защиты в киберпространстве.

Задачи дисциплины:

- получение знаний о правовой безопасности в информационном пространстве, включая особенности регламентации отдельных областей деятельности и специфики мер правовой защиты в киберпространстве.
- формирование умений и навыков, позволяющих реализовывать меры правовой защиты в информационном пространстве.

В результате освоения дисциплины обучающийся должен:

Знать: основные этапы развития информационной безопасности; систему законодательства об информационной безопасности и ответственность за его нарушение; систему мер правовой защиты в информационном пространстве в различных областях (сферах) деятельности.

Уметь: применять нормы законодательства для осуществления правовой защиты в информационном пространстве.

Владеть: знаниями законодательства в сфере информационного пространства; знаниями по соблюдению информационной безопасности; специальными навыками правовой защиты в информационном пространстве.

Federal State Budgetary Educational Institution
higher education
"Russian State Humanitarian University"
(FSBEI HE "RGGU")

INSTITUTE OF MANAGEMENT, ECONOMICS AND LAW
FACULTY OF LAW
Department of Business Law

LEGAL SECURITY IN THE INFORMATION SPACE

DISCIPLINE WORK PROGRAM

43.04.02 - Tourism

Code and name of the area of training/specialty

"Cultural Heritage Management and Sustainable Tourism"
"Cultural Heritage Conservation and Sustainable Tourism"

Name of focus (profile)/specialization

Level of higher education: *master's degree*

Form of study: *full-time*

RPD adapted for persons
disabled
health and disabled

Moscow 2023

Legal security in the information space
Work program of the discipline

Compiled by:
Doctor of Legal Sciences , Professor, Dean of the Faculty of Law S.V. Timofeev
Candidate of Legal Sciences , Associate Professor, Head of the Department of Business Law T.V. Belova
Candidate of Legal Sciences , Associate Professor, Associate Professor of the Department of Criminal Law and Procedure E.A. Redkina

APPROVED
Minutes of the department meeting
No. 12 from 06/16/2022

TABLE OF CONTENTS

10. Explanatory note

1.2. Purpose and objectives of the discipline

The purpose of the discipline is a comprehensive study of legal security in the information space, including the features of regulation of various areas of activity and legal protection in cyberspace.

Objectives of the discipline:

- gaining knowledge about legal security in the information space, including the specifics of regulation of certain areas of activity and the specifics of legal protection measures in cyberspace.
- formation of skills and abilities that allow implementing legal protection measures in the information space.

The discipline is implemented in the format of an online course on the Russian State University for the Humanities platform.

1.2. List of planned learning outcomes in the discipline

As a result of mastering the discipline, the student must:

Know : the main stages of information security development; the system of legislation on information security and liability for its violation; a system of legal protection measures in the information space in various areas (fields) of activity.

Be able to : apply legal norms to implement legal protection in the information space.

Possess : knowledge of legislation in the field of information space; knowledge of information security compliance; special skills of legal defense in the information space.

1.3. Place of discipline in the structure of the educational program

The discipline "Legal Security in the Information Space" is one of the optional disciplines of the curriculum.

11. Discipline structure

The total labor intensity of the discipline is 2 credits , 72 academic hours.

Discipline structure for full-time education

The scope of the discipline in the form of contact work between students and teaching staff and (or) persons involved in the implementation of the educational program on other terms during training sessions:

Semester	Type of training sessions	Number of hours
2	Lectures	10
2	Seminars	10
	Total:	72

The volume of the discipline (module) in the form of independent work of students is 52 academic hours.

Discipline structure for full-time and part-time courses

The scope of the discipline in the form of contact work between students and teaching staff and (or) persons involved in the implementation of the educational program on other terms during training sessions:

Semester	Type of training sessions	Number of hours
2	Lectures	8
2	Seminars	8
	Total:	16

The volume of the discipline (module) in the form of independent work of students is 56 academic hours.

Discipline structure for distance learning

The scope of the discipline in the form of contact work between students and teaching staff and (or) persons involved in the implementation of the educational program on other terms during training sessions:

Year	Type of training sessions	Number of hours
1	Lectures	4
1	Seminars	4
	Total:	8

The volume of the discipline (module) in the form of independent work of students is 64 academic hours.

12. Contents of the discipline

No.	Name of the discipline section	Content
1	Retrospective analysis of legal norms on information security	Stages of development of an information security system. Formation of international information security. Development of legislation on information security.
2	Information security legislation system	Concept and legal regulation of information security. Principles of state policy for ensuring information security. Characteristics of the main regulatory legal acts on information security. Responsibility for violation of information security legislation. Disciplinary responsibility. Material liability. Civil liability. Administrative responsibility. Criminal liability.
3	Information security in the field of economic activity	The concept of digital economy. Main directions of ensuring information security of the digital economy. Actions under someone else's account: concept, qualifications. Voluntary provision of account access. Actions under someone else's account in the absence of the owner's will. Legal regulation of electronic commerce. Features of concluding a contract remotely.

4	Protection of intellectual property in cyberspace	The concept of intellectual property. Intellectual rights to the results of intellectual activity and means of individualization. Methods of protecting intellectual rights
5	Protection of personal data in the digital environment	Concept and categories of personal data. In terms of personal data processing, rights and obligations of the operator and subject of data processing. Personal data protection measures. Depersonalization of personal data. "The right to be forgotten."
6	Legal protection from destructive content in the digital environment	The concept of destructive content. Information the distribution of which is prohibited or restricted. The procedure for restricting access to sites containing information the distribution of which is prohibited.

13. Educational technology

To conduct classes in the discipline, educational technologies such as online lectures, presentation of lecture notes and presentation material are used. Each lecture is accompanied by test questions for repetition and self-test, a list of recommended literature and a glossary.

14. Assessment of planned learning outcomes

14.1 Grading system

form of control	**Max. number of points**	
	For one job	**Total**
Current control:		60 points
Analysis of regulatory legal acts and judicial acts	*2*	*16*
Problem solving	*2*	*20*
Running tests	*4*	*24*
Interim certification - *test*		40 points
Total for the semester		100 points

The resulting aggregate result is converted into the traditional grading scale and into the grading scale of the European Credit Transfer and Accumulation System (European Credit Transfer System ; hereinafter referred to as ECTS) in accordance with the table:

100 point scale	Traditional scale		ECTS scale
9 5 – 100	Great	passed	A
83 – 9 4			B
68 – 8 2	Fine		C
5 6 – 6 7	satisfactorily		D
50 - _ 5 5			E
20 – 49	unsatisfactory	not accepted	FX
0 – 19			F

14.2 Criteria for grading the discipline

Points/ ECTS scale	**Discipline grade**	**Criteria for assessing learning outcomes in the discipline**
100-83/ A,B	Great/ passed	It is awarded to the student if he has deeply and firmly mastered the theoretical and practical material and can demonstrate this in classes and during intermediate certification. The student presents educational material comprehensively and logically, knows how to link theory with practice, copes with solving professional problems of a high level of complexity, and correctly substantiates the decisions made. Fluently navigates educational and professional literature. The grade for the discipline is given to the student taking into account the results of the current and intermediate certification. The competencies assigned to the discipline are formed at the "high" level.
82-68/ C	Fine/ passed	It is awarded to the student if he knows the theoretical and practical material, presents it competently and essentially in classes and during intermediate certification, without allowing significant inaccuracies. The student correctly applies theoretical principles when solving practical professional problems of varying levels of complexity, and has the necessary skills and techniques for this. He is well versed in educational and professional literature. The grade for the discipline is given to the student taking into account the results of the current and intermediate certification. The competencies assigned to the discipline are formed at the " good ***" level*** .
67-50/ D,E	satisfactory / passed	It is awarded to the student if he knows theoretical and practical material at a basic level and makes some mistakes when presenting it in class and during intermediate certification. The student experiences certain difficulties in applying theoretical principles when solving practical problems of a professional nature of a standard level of complexity, but possesses the necessary basic skills and techniques. Demonstrates a sufficient level of knowledge of educational literature in the discipline. The grade for the discipline is given to the student taking into account the results of the current and intermediate certification. The competencies assigned to the discipline are formed at the "sufficient ***" level*** .
49-0/ F,FX	unsatisfactor y / not accepted	It is given to a student if he does not know theoretical and practical material at a basic level, or makes gross mistakes when presenting it in classes and during intermediate certification. The student experiences serious difficulties in applying theoretical principles when solving practical professional problems of a standard level of complexity, and does not possess the necessary skills and techniques for this. Demonstrates fragmentary knowledge of educational literature in the discipline. The grade for the discipline is given to the student taking into account the results of the current and intermediate certification. Competencies at the "sufficient ***" level*** assigned to the discipline have not been formed.

14.3 Assessment tools (materials) for ongoing monitoring of progress, intermediate certification of students in the discipline

Assessment materials for ongoing monitoring of progress in the discipline

Analysis of regulatory legal acts and judicial acts

Analyze the Constitution of the Russian Federation, highlighting the constitutional guarantees of the right of citizens to information, filling out the following table:

Constitutional guarantees of the right of citizens to information	
Article, part of an article	*Basic provisions*

2. Analyze the Decree of the Government of the Russian Federation of December 31, 2020 No. 2463 " On approval of the Rules for the sale of goods under a retail purchase and sale agreement, a list of durable goods that are not subject to the consumer's requirement for the free provision of goods that have the same basic consumer properties, for the period of repair or replacement of such a product, and a list of non-food products of adequate quality that are not subject to exchange, as well as on amendments to certain acts of the Government of the Russian Federation" "and highlight in writing the features of the rules for the sale of goods in the remote method of selling goods under a retail agreement purchase and sale.

3. Analyze the provisions of the Federal Law of June 27, 2011 No. 161-FZ "On the National Payment System" and provide a written brief analysis of the following provisions: features of the transfer of electronic funds; the procedure for using electronic means of payment and requirements for receiving data on the territory of the Russian Federation; the procedure for using electronic means of payment when transferring electronic funds.

4. Analyze the Resolution of the Constitutional Court of the Russian Federation of March 27, 1996 No. 8-P "In the case of verifying the constitutionality of Articles 1 and 21 of the Law of the Russian Federation of July 221, 1993 "On State Secrets" in connection with complaints from citizens V.M. Gurdzhiyants , V.N. Sintsova, V.N. Bugrova and A.K. Nikitin" and fill out the following table:

Parameter	Content
Reason for consideration	
Reason for consideration	
Essence (summary) of the complaint	
Court statement	

Sample problems

1. The person is the author of the photograph posted on his page on one of the social networks. Some time after posting the photograph, the individual discovered that the photograph was being used to illustrate an article on another website. No permission was given to use the photograph. **Were the photographer's rights violated?**

2. The Society has published a number of weekly blog reviews on the Internet website dedicated to issues of architecture, urban planning and heritage protection, which are overviews of the author's creative works on the topics of architecture, urban planning and heritage protection. These works are created by specific authors, whose names are indicated for each publication. The reviews included photographs and text fragments of various materials published on the Internet in the form of quotes. The company, among others, posted fragments of the entrepreneur's blog with 22 photographs, the exclusive copyright of which belongs to the entrepreneur. The controversial photographs, the exclusive rights to which belong to the entrepreneur, were used in 14 weekly review articles for informational purposes in the order of citation, including photo reports of the entrepreneur posted on his blog. At the same time, information was posted on the entrepreneur's website about the possibility of free use of his photographs for non-commercial purposes, indicating the author and a link to the entrepreneur's website. Considering that the company violated the rights and legitimate interests of the entrepreneur when posting photographs, the latter filed a lawsuit for compensation. **Should compensation be collected?**

4. The online store sold goods that did not have an age limit. At the same time, when filling out the order form, it was necessary to indicate the buyer's full name, date of birth, gender and place of residence, as well as his telephone number. There was also no document containing a privacy policy on the site. **Will there be a violation of personal data legislation in this situation?**

5. An article was posted on an information resource located on the Internet, which presented the story of a person who has been using drugs for several years, with the statement that drug use did not have an impact on the social and public life of this person. Roskomnadzor generated and sent a notification in Russian to the hosting provider and the site owner about restricting access to the information resource. **Were there any violations in sending the notification?**

Test examples

1. The beginning of the formation of the concept of international information security is considered to be:

1. 1996
2. 1992
3. 1998

2. The adoption of the federal target program "Electronic Russia (2002 - 2010)" marked the beginning of:

1. digitalization .
2. personalization.
3. informatization.

3. Development of a safe information space, protection of Russian society from destructive information and psychological influences is:

1.national interest
2. national priority.
3. direction of protection.

4. Art. 138 of the Criminal Code of the Russian Federation "Violation of the secrecy of correspondence, telephone conversations, postal, telegraph or other messages" refers to:

1. crimes related to violation of established restrictions on the dissemination of information of certain content.
2. crimes related to violation of confidentiality of information.
3. crimes related to violation of the right to access information.

5. Can the owner of the aggregator bring information about the seller to the attention of consumers by posting a link to the seller's website?

1. yes
2. no
3. at the discretion of the aggregator

6. The design of the site will be classified as objects of copyright if:

1. it is the result of creative work.
2. refers to the solution of technical means.
3. design is not subject to copyright.

7. If, when designing an electronic publication, the artistic design of another book was used (without rights to it and without the consent of the copyright holder), then this can be qualified as:

1. violation of inventive or patent rights
2. violation of copyright and related rights
3. unfair competition in the form of introducing goods into circulation with illegal use of the results of intellectual activity

8. Human voice data obtained using sound recording devices is:

1. general personal data.
2. personal data authorized by the subject of personal data for distribution.
3. biometric personal data.

9. What access is the operator obliged to provide to the document defining its policy regarding the processing of personal data, to information about the implemented requirements for the protection of personal data?

1. limited.
2. unlimited.
3. any.

10. The procedure for restricting access to sites containing illegal content may be:

1. only judicial.
2. only extrajudicial.
3. both judicial and extrajudicial.

Evaluation materials for intermediate certification of students in the discipline

Final test

1. The state of protection of the vital interests of the individual, society and state from internal and external threats is called _____

_

2. The term " security " was introduced:

1. in 1995
2. in 1992
3. in 2006

3. The beginning of the formation of the concept of international information security is considered to be:

1. 1996
2. 1992
3. 1998

4. The Law "On State Secrets" was adopted:

1. in 1991
2. in 1992
3. in 1993

5. At what stage of the development of information security its task was reduced to protecting the information itself about certain facts:

1. Stage I.
2. Stage II .
3. V stage.

6. Restrictions on the transfer of information outside of Russia were established:

1. Federal Law "On participation in international information exchange".
2. Federal Law "On Information, Informatization and Information Protection".
3. Law of the Russian Federation "On State Secrets".

7. For the first time, the Doctrine on Information Security of the Russian Federation was adopted:

1. in 1998
2. in 2000
3. in 2006

8. The creation and development of local information and communication networks is characterized by:

1. Stage II .
2. IV stage.
3. V stage.

9. The adoption of the federal target program "Electronic Russia (2002 - 2010)" marked the beginning of:

1. digitalization .
2. personalization.
3. informatization.

10. The current Federal Law "On Information, Information Technologies and Information Protection" was adopted:

1. in 2004
2. in 2006
3. in 2008

11. According to the National Security Strategy of the Russian Federation, a safe information space is:

1. national priority
2. strategic national priority
3. national security task

12. Legal equality of all participants in relations, based on the constitutional right of citizens to freely seek, receive, transmit, produce and disseminate information in any legal way - this is the principle:

1. maintaining balance
2. legality
3. constructive interaction.

13. Monitoring information threats helps determine:

1. sufficiency of forces and means
2. maintaining balance
3. legality

14. Achieving and maintaining information sovereignty in the Strategy for ensuring information security of the CIS member states is:

1. the purpose of ensuring information security.
2. the task of ensuring information security.
3. priority of ensuring information security.

15. The right to information in the Constitution of the Russian Federation is enshrined in:

1st Art. 29.
2. Art. thirty.
3.st. 56.

16. The grounds for restricting the information rights and freedoms of citizens are determined:

1. Federal Law "On Information, Information Technologies and Information Protection"
2. Constitutional Court of the Russian Federation
3. The Constitution of the Russian Federation.

17. The classification of information products is established in:

1. Federal Law "On Basic Guarantees of the Rights of the Child in the Russian Federation"
2. Federal Law "On Information, Information Technologies and Information Protection"
3. Federal Law "On the protection of children from information harmful to their health and development."

18. Development of a safe information space, protection of Russian society from destructive information and psychological influences is:

1.national interest
2. national priority.
3. direction of protection.

19. The system of official views on ensuring the national security of the Russian Federation in the information sphere is:

1. National Security Strategy
2. Information security doctrine
3. Fundamentals of the state policy of the Russian Federation in the field of international information security.

20. Countering the threat of using information and communication technologies for the purpose of undermining (infringing) sovereignty is:

1. the task of state policy in the field of international information security.
2. direction of state policy in the field of international information security.
3. the goal of state policy in the field of international information security.

21. The process of creating optimal conditions for the fullest possible satisfaction of the information and legal needs of government and public structures, enterprises, organizations, institutions

and citizens based on the effective organization and use of information resources using advanced technologies is:

1. legal informatization.
2. legal digitalization .
3. legal automation.

22. Ensuring the unity of state standards in the field of informatization is:

1. the goal of state policy in the field of informatization.
2. the task of state policy in the field of informatization.
3. direction of state policy in the field of informatization.

23. The adverse property consequences that the guilty person must suffer in order to compensate for the losses of the victim from his unlawful actions are:

1. financial responsibility.
2. disciplinary liability.
3. civil liability.

24. Art. 138 of the Criminal Code of the Russian Federation "Violation of the secrecy of correspondence, telephone conversations, postal, telegraph or other messages" refers to:

1. crimes related to violation of established restrictions on the dissemination of information of certain content.
2. crimes related to violation of confidentiality of information.
3. crimes related to violation of the right to access information.

25. The main type of administrative punishment for violations of information security requirements is:

1. confiscation.
2. administrative fine.
3. administrative suspension of activities.

26. If an employee disclosed information constituting a secret protected by law, then he:

1. compensates for the full amount of damage caused.
2. compensates for direct actual damage.
3. The amount of compensation is determined by the employer.

27. Consequences of applying disciplinary measures:

1. can be defined in local acts.
2. are determined in the order (instruction).
3. are determined exclusively by the Labor Code.

28. A reprimand is a type of:

1. disciplinary offense.
2. disciplinary action.
3. disciplinary liability.

29. Failure to perform or improper performance by an employee through his fault of the labor duties assigned to him is:

1. disciplinary liability.
2. financial responsibility.
3. disciplinary offense.

30. Federal Law "On Information, Information Technologies and Information Protection":

1. establishes a reference rule on liability for violation of the law.
2. indicates specific types of offenses.
3. does not contain provisions on liability for violation of the law.

31. Economic activity in which the key factor of production is digital data, the processing of large volumes and the use of analysis results of which, in comparison with traditional forms of management, can significantly increase the efficiency of various types of production, technologies, equipment, storage, sales, delivery of goods and services - This:

1. ecosystem of the digital economy.
2. digital economy.

3. digital technology.

32. Partnership of organizations that ensures constant interaction of their technological platforms, applied Internet services, analytical systems, information systems of government bodies of the Russian Federation, organizations and citizens is:

1. ecosystem of the digital economy.
2. digital economy.
3. digital technology.

33. Automated management systems of subjects of critical information infrastructure refer to:

1. subjects of critical information infrastructure.
2. objects of critical information infrastructure.
3. types of critical information infrastructure

34. Ensuring a favorable legal regime for the development of modern technologies relates to:

1. Information infrastructure.
2. Regulatory regulation of the digital environment.
3. Digital public administration.

35. Transformation of priority sectors of the economy and social sphere through the introduction of digital technologies and platform solutions refers to:

1. Digital technologies.
2. Regulatory regulation of the digital environment.
3. Digital public administration.

36. GosSOPKA was created by Decree of the President of the Russian Federation in:

1. 2011.
2. 2013.
3. 2015.

37. Is the concept of "Internet account" defined in the legislation?

1. yes.
2. no.
3. is given but not disclosed.

38. Voluntary provision of account access is generally regarded as:

1. action in someone else's interest.
2. representation.
3. illegal action.

39. Is the concept of "account" defined in the legislation?

1. yes.
2. no.
3. is given but not disclosed.

40. Can a non-bank credit organization be a subject of the national payment system?

1. yes, it can
2. no, it can't
3. may in exceptional cases

41. The GATS was adopted in:

1. 1994
2. 1998
3. 2000

42. The buyer purchased a product from an online store that was of adequate quality. The product was delivered on time. After handing over the goods, 12 days later the buyer decided to refuse the goods. Does he have the right to such a refusal? Justify your answer

_____
_____
_____
_____

43. Can the owner of an aggregator bring information about the seller to the attention of consumers by posting a link to the seller's website?

1. yes
2. no
3. at the discretion of the aggregator

44. When providing false information about a product, the aggregator :

1. is responsible for losses caused to the buyer.
2. bears disciplinary liability.
3. bears administrative responsibility.

45. Filing a claim directly with the seller is such a way to protect rights as:

1. self-defense rights.
2. recognition of rights.
3. compensation for losses.

46. Concept of e-commerce:

1. enshrined in legislation.
2. not enshrined in legislation.
3. in legislation this term is used, but not disclosed.

47. If payment for the goods is made to the bank account of the owner of the aggregator , and the specified goods were not transferred on time, then the consumer has the right:

1. submit a demand to the seller for the return of the prepayment amount
2. present a demand to the owner of the aggregator for the return of the prepayment amount.
3. go to court.

48. Is the seller obliged to provide the buyer with information about the form and methods of filing claims?

1. obliged.
2. not obliged.
3. obliged upon buyer's request.

49. The following can be sold remotely:

1. any goods.
2. restrictions have been established on the sale of certain types of goods.
3. a list of goods that can be sold remotely has been established.

50. The Model Law on Electronic Commerce was adopted:

1. UN General Assembly.
2. World Trade Organization (WTO).
3. International Institute for the Unification of Private Law (UNIDROIT).

51. Improving antimonopoly legislation is:

1. a condition for the implementation of national interest in the field of digital economy.
2. national interest in the digital economy.
3. indicator of the implementation of the Information Society Development Strategy.

52. The creation of special centers involved in data processing applies to:

1. Regulatory regulation of the digital environment.
2. Digital technologies.
3. Information infrastructure.

53. The Model Electronic Law was developed by:

1. United Nations Commission on International Trade Law (UNCITRAL).
2. International Institute for the Unification of Private Law (UNIDROIT)
3. World Trade Organization (WTO).

54. Providing information to the consumer about the service life and shelf life of the product is the stage:

1. informing the buyer.
2. conclusion of an agreement.
3. execution of the contract.

55. The introduction of digital technologies and platform solutions in the provision of public services is:

1. Digital public administration.
2. Digital technologies.
3. Regulatory regulation of the digital environment.

56. Will the order number serve as confirmation of the conclusion of the contract when selling goods online?

1. No, the order number is not confirmation.
2. Yes, the order number is confirmation.

57. Transfer of goods purchased remotely is carried out:

1. only to the buyer.
2. to any person.
3. to any person who has provided information and order number.

58. If the goods have been paid for, then if the delivery time is missed, the seller:

1. Refunds shipping fees.
2. pays a penalty (penalty).
3. terminates the contract.

59. Reducing the response time to block the spread of phishing sites is an area of ensuring information security of the digital economy such as:

1. Digital public administration.
2. Increasing the level of security of information systems and resources.
3. Creating conditions to reduce the number of offenses using information technology.

60. The formation of an institutional system (environment) for the development of research activities and developments in the field of the digital economy refers to:

1. Digital technologies.
2. Information security.
3. Digital public administration.

61. Waiver of personal non-property rights:

1. is recognized.
2.insignificant.
3. recognized in exceptional cases.

62. A phonogram is an object:

1. copyright.
2. related rights.
3. patent law.

63. Website design will be classified as objects of copyright if:

1. it is the result of creative work.
2. refers to the solution of technical means.
3. design is not subject to copyright.

64. Digital watermarking is:

1. cryptography.
2. digital fingerprint.
3. digital marking.

65. Publication of a court decision on a violation is a way:

1. protection of personal non-property rights.
2. protection of exclusive rights.
3. protection of personal non-property and exclusive rights.

66. Seizure of a material carrier is a method:

1. protection of personal non-property rights.
2. protection of exclusive rights.
3. protection of personal non-property and exclusive rights.

67. A claim may be brought if a response to the claim is not received within:

1. 10 days.
2. 20 days.
3. 30 days.

68. Can compensation for moral damage be recovered in case of violation of exclusive rights?

1. can
2. can't
3. may in exceptional cases

69. The owner of the exclusive right at the time of:

1. going to court.
2. violations of rights.
3. making a court decision.

70. Can the court, on its own initiative, change the method of calculating the amount of compensation?

1. yes, it can.
2. yes, maybe, upon agreement with the parties.
3. no, he can't.

71. Is a screenshot considered admissible evidence in court?

1. yes, he admits it.
2. recognized in exceptional cases.
3. no, it is not recognized.

72. Illegal use of copies of works can be classified as:

1. violation of inventive or patent rights
2. violation of copyright and related rights
3. unfair competition in the form of introducing goods into circulation with illegal use of the results of intellectual activity

73. Illegal use of means of individualization of goods (works, services) is criminally punishable if it:

1. committed repeatedly.
2. caused significant damage.
3. the person has previously been brought to administrative responsibility.

74. If, when designing an electronic publication, the artistic design of another book was used (without rights to it and without the consent of the copyright holder), then this can be qualified as:

1. violation of inventive or patent rights
2. violation of copyright and related rights
3. unfair competition in the form of introducing goods into circulation with illegal use of the results of intellectual activity

75. In your opinion, will the simultaneous use of two or more foreign trademarks on one item of goods be considered repeated? Justify your opinion

_____
_____
_____
_____
_____

76. Will the publication by a person solely under his own name of a work created in co-authorship be considered plagiarism?

1. yes, it will.
2. no, it doesn't count.
3. yes, provided that major damage is caused.

77. Recognition of rights is a way of protecting:

1. personal non-property rights.
2. exclusive rights.
3. and personal non-property and exclusive rights.

78. Free use of photographs posted on a social network is possible subject to the following conditions:

1. use for informational, scientific, educational or cultural purposes; mandatory indication of the author; indication of the source of borrowing; to the extent justified by the purpose of quoting.

2. use for informational, scientific, educational or cultural purposes; mandatory indication of the author; indication of the source of borrowing; to the extent justified by the purpose of quoting; sending the author of the photograph a notification about its use.

3. Such use is not permitted.

79. The right of succession applies to:

1. exclusive rights.

2. personal non-property rights.

3. other rights.

80. Intellectual rights to a utility model are:

1. patent rights.

2. copyright.

3. related rights.

81. The Federal Law "On Personal Data" was adopted in:

1. 2004

2. 2006

3. 2010

82. Human voice data obtained using sound recording devices are:

1. general personal data.

2. personal data authorized by the subject of personal data for distribution.

3. biometric personal data.

83. Religious beliefs refer to:

1. personal data of a general nature.

2. special categories of personal data.

3. personal data authorized by the subject of personal data for distribution.

84. Actions as a result of which it becomes impossible, without the use of additional information, to determine the ownership of personal data to a specific subject of personal data - this is _____

_____

85. Moral damage in case of violation of the legislation on personal data:

1. is compensated depending on whether the property damage is compensated.

2. not refundable.

3. is compensated regardless of whether property damage is compensated.

86. Does violation of the legislation on personal data entail financial liability for the employee?

1. no.

2. always attracts.

3. entails in the presence of certain conditions established by law.

87. Can disclosure of personal data of another employee become grounds for termination of an employment contract by the employer?

1. yes.

2. no.

3. in exceptional cases.

88. Is there a special rule on criminal liability for violation of legislation on personal data?

1. yes.

2. no, such a person will not be held criminally liable.

3. no, but if the work with personal data is violated, criminal prosecution is possible.

89. If there is no document containing a privacy policy on the website of an online store, but to purchase a product without an age limit, you need to fill out a form indicating personal data (full name, age, place of residence, telephone number), will this be a violation legislation on personal data? Justify your answer

_____
_____
_____
_____
_____

90. What access is the operator required to provide to the document defining its policy regarding the processing of personal data, to information about the implemented requirements for the protection of personal data?

1. limited.
2. unlimited.
3. any.

91. Is the concept of "destructive content" enshrined in the legislation of the Russian Federation?

1. secured.
2. not secured.
3. secured, but does not open.

92. An insult committed publicly on the Internet is:

1. information the distribution of which is prohibited.
2. information whose distribution is limited.
3. not regulated by law.

93. Is the concept of "illegal content" used in the legislation of the Russian Federation?

1. used.
2. not used.
3. used but not disclosed.

94. Can a bailiff's decision to restrict access to information distributed on the Internet be the basis for inclusion in the Unified Register of domain names, indexes of site pages on the Internet information and telecommunications network and network addresses that allow identifying sites on information and telecommunications network "Internet" containing information the distribution of which is prohibited in the Russian Federation?

1. yes.
2. no.
3. yes, provided that this information discredits the honor, dignity or business reputation of a citizen or the business reputation of a legal entity.

95. With regard to information on the organization and conduct of gambling and lotteries using the Internet, the authorized body for the decision that is the basis for inclusion in the relevant Register is:

1. Ministry of Internal Affairs of Russia.
2. Federal Tax Service.
3. Federal Service for Supervision of Communications, Information Technologies and Mass Communications.

96. The basis for blocking the website of a foreign media outlet performing the functions of a foreign agent and designated as such in accordance with the law on mass media (or a Russian legal entity established by it) is:

1. resolution in a case of an administrative offense
2. resolution in a case of an administrative offense of violation of the procedure for the activities of such a media outlet
3. a decision that has entered into legal force in the case of an administrative offense of violation of the procedure for the activities of such a media outlet.

97. The procedure for restricting access to sites containing illegal content may be:

1. only judicial.
2. only extrajudicial.
3. both judicial and extrajudicial.

98. With regard to information distributed via the Internet containing proposals for remote retail sale of alcoholic beverages, the authorized body by decision, which is the basis for inclusion in the relevant Register, is:

1. Federal Service for Supervision of Communications, Information Technologies and Mass Communications.

2. Ministry of Internal Affairs of Russia.

3. Federal Service for Regulation of the Alcohol Market

99. The hosting provider is sent a notification about the inclusion in the Unified Register of domain names, site page indexes on the Internet information and telecommunications network and network addresses that allow identifying sites on the Internet information and telecommunications network containing information the distribution of which is prohibited in the Russian Federation :

1. One day before inclusion in the Register.

2. Simultaneously with inclusion in the Register.

3. After inclusion in the Register.

100. in relation to information disseminated via the Internet aimed at inducing or otherwise involving minors in committing illegal actions, the authorized body by decision, which is the basis for inclusion in the relevant Register, is:

1. Federal Agency for Youth Affairs

2. Federal Service for Supervision of Communications, Information Technologies and Mass Communications.

3. Ministry of Internal Affairs of Russia.

15. Educational, methodological and information support of the discipline

15.1 List of sources and literature

Sources

Basic

1. Constitution of the Russian Federation of December 12, 1993 // ATP "Consultant Plus"

2. Federal Law of July 27, 2006 No. 152-FZ "On Personal Data" // SPS "Consultant Plus".

3. Federal Law of July 27, 2006 N 149-FZ "On information, information technologies and information protection" // SPS "Consultant Plus".

4. Civil Code of the Russian Federation (part four) dated December 18, 2006 N 230-FZ // SPS "Consultant Plus".

5. Code of the Russian Federation on Administrative Offenses of December 30, 2001 No. 195-FZ // SPS "Consultant Plus"

6. Labor Code of the Russian Federation of December 30, 2001 No. 195-FZ // SPS "Consultant Plus".

7 . Criminal Code of the Russian Federation of June 13, 1996 No. 63-FZ // SPS "Consultant Plus"

8. Civil Code of the Russian Federation (part two) dated January 26, 1996 N 14-FZ // SPS "Consultant Plus".

9. Civil Code of the Russian Federation (part one) dated November 30, 1994 N 51-FZ // SPS "Consultant Plus".

10. Decree of the Government of the Russian Federation of October 26, 2012 N 1101 "On a unified automated information system "Unified register of domain names, indexes of site pages on the Internet information and telecommunications network and network addresses that allow identifying sites on the Internet information and telecommunications network" containing information the distribution of which is prohibited in the Russian Federation" // SPS "Consultant Plus".

Additional

1. Universal Declaration of Human Rights (1948) // SPS "Consultant Plus".

2. International Covenant on Civil and Political Rights (1966) // SPS "Consultant Plus".

3. Fundamentals of the state policy of the Russian Federation in the field of international information security (approved by Decree of the President of the Russian Federation of April 12, 2021 No. 213) // SPS "Consultant Plus".

4. Federal Law of June 27, 2011 No. 161-FZ "On the National Payment System" // SPS "Consultant Plus".

5. Resolution of the Federal Arbitration Court of the Volga-Vyatka District dated April 27, 2011 in case No. A82-12456/2010 // ATP "Consultant Plus".

6. Letter of the Federal Tax Service dated March 31, 2016 No. SA-4-7/5589 // SPS "Consultant Plus"

7. Order of Roskomnadzor dated July 6, 2010 No. 420 "On approval of the procedure for sending appeals about the inadmissibility of abuse of freedom of the media to the media, the distribution of which is carried out in information and telecommunication networks, including the Internet" // SPS "Consultant Plus " .

Literature

Main

1. Gavrilov, L. P. Electronic commerce: textbook and workshop for universities / L. P. Gavrilov. — 4th ed. - Moscow: Yurayt Publishing House , 2022. - 521 p. // Educational platform Urayt [website]. — URL: https://urait.ru/bcode/489784

2. Zharova, A. K. Legal regulation of the creation and use of information infrastructure in the Russian Federation: monograph / A. K. Zharova. - Moscow: Yurayt Publishing House , 2022. - 301 p. // Educational platform Urayt [website]. — URL: https://urait.ru/bcode/496939

3. Information law: textbook for universities / M. A. Fedotov [et al.]; edited by M. A. Fedotov. - Moscow: Yurayt Publishing House , 2022. - 497 p. // Educational platform Urayt [website]. — URL: https://urait.ru/bcode/489946

4. Organizational and legal support of information security: textbook and workshop for universities / edited by T. A. Polyakova, A. A. Streltsov . - Moscow: Yurayt Publishing House , 2022. - 325 p. // Educational platform Urayt [website]. — URL: https://urait.ru/bcode/498844

5. Rassolov, I. M. Information law: textbook and workshop for universities / I. M. Rassolov. — 6th ed., revised . and additional - Moscow: Yurayt Publishing House , 2022. - 415 p. // Educational platform Urayt [website]. — URL: https://urait.ru/bcode/488767

6. Suvorova, G. M. Information security: a textbook for universities / G. M. Suvorova. - Moscow: Yurayt Publishing House , 2022. - 253 p. // Educational platform Urayt [website]. — URL: https://urait.ru/bcode/496741

7. Shcherbak, N. V. Intellectual property rights: general teaching. Copyright and related rights: textbook for universities / N. V. Shcherbak. - Moscow: Yurayt Publishing House , 2022. - 309 p. // Educational platform Urayt [website]. — URL: https://urait.ru/bcode/495164

Additional

13. Alisova E.V. Current problems of copyright protection on the Internet // Modern scientific research and innovation. 2016. No. 7. – URL: https://web.snauka.ru/issues/2016/07/69396 .

14. Vanyushina E. A. Technical means of protecting copyright on the Internet / E. A. Vanyushina // Young scientist. – 2021. – No. 53 (395). Access mode: URL: https://moluch.ru/archive/395/87447/

15. Vorobyova A.A., Pantyukhin I.S. History of the development of software and hardware for information security . – St. Petersburg: ITMO University, 2017 – 62 p. – Access mode: https://books.ifmo.ru/file/pdf/2188.pdf .

16. Vostretsova E.V. Fundamentals of information security: textbook. – Ekaterinburg: Ural University Publishing House, 2019. – Access mode: https://elar.urfu.ru/bitstream/10995/73899/3/978-5-7996-2677-8_2019.pdf

17. Ganzha K.P. Legal regulation of e-commerce in Russia // Electronic scientific and practical journal "Modern scientific research and innovation" // Access mode: https://web.snauka.ru/issues/2013/10/27833

18. Zhigulin G.P. Organizational and legal support of information security. – St. Petersburg: SPbNIUTMO , 2014. – Access mode: https://books.ifmo.ru/file/pdf/1484.pdf

19. Zenkov , A.V. Information security and information protection: a textbook for universities / A.V. Zenkov . - Moscow: Yurayt Publishing House , 2022. - 104 p. // Educational platform Urayt [website]. — URL: https://urait.ru/bcode/497002

20. Marketing research Internet commerce in Russia 2021 // Access mode: https://datainsight.ru/eCommerce_2021 .

21. International information security: Theory and practice: In three volumes. Volume 2: Collection of documents (in Russian) / Ed. ed. A.V. Krutskikh . 2nd ed., add. M.: Aspect Press Publishing House, 2021. – P. 225 (History of the negotiation process on international information security at the UN // International information security: Russian approaches). – Access mode: https://mgimo.ru/upload/2022/03/mezhdunarodnaya-informatsionnaya-bezopasnost-podkhody-rossii.pdf

22. Smolyakov P.N. Responsibility for violation of legislation on personal data // SPS Consultant Plus. 2022.

23. Kholodkova K.S. Analysis of the e-commerce market in Russia // Modern scientific research and innovation. 2013. No. 10. – Access mode: http://web.snauka.ru/issues/2013/10/26760

24. Draft Federal Law "On Electronic Commerce" (access mode: https://sozd.duma.gov.ru/bill/11081-3)

15.2 List of resources of the information and telecommunications network "Internet".

ELibrary.ru Scientific electronic library www . library . ru

15.3 Professional databases and information and reference systems

Information help systems:

3. Consultant Plus
4. Guarantee

16. Material and technical support of the discipline

To ensure discipline, the material and technical base of the educational institution is used: classrooms equipped with a computer, projector and audio system for demonstrating educational materials.

Software composition:

4. Windows
5. Microsoft Office
6. Kaspersky Endpoint Security

17. Ensuring the educational process for persons with disabilities and people with disabilities

During the implementation of the discipline, the following additional methods of teaching, ongoing monitoring of progress and intermediate certification of students are used, depending on their individual characteristics:

- for the blind and visually impaired: lectures are presented in the form of an electronic document, accessible using a computer with specialized software; written tasks are performed on a computer with specialized software or can be replaced by an oral response; individual uniform lighting of at least 300 lux is provided; To complete the task, if necessary, a magnifying device is provided; It is also possible to use your own magnifying devices; written assignments are presented in larger font; The exam and test are conducted orally or performed in writing on a computer.
- for the deaf and hard of hearing: lectures are issued in the form of an electronic document, or sound amplification equipment for individual use is provided; written assignments are completed on a computer in written form; the exam and test are carried out in writing on a computer; may be carried out in the form of testing.
- for persons with musculoskeletal disorders: lectures are presented in the form of an electronic document accessible using a computer with specialized software; written tasks are completed on a computer with specialized software; The exam and test are conducted orally or performed in writing on a computer.

If necessary, an increase in time for preparing a response is provided.

The procedure for conducting intermediate certification for students is established taking into account their individual psychophysical characteristics. Interim certification can be carried out in several stages.

When carrying out the procedure for assessing learning outcomes, the use of technical means necessary in connection with the individual characteristics of students is provided. These facilities may be provided by the university , or their own technical facilities may be used.

The procedure for assessing learning outcomes is permitted using distance learning technologies.

Access to information and bibliographic resources on the Internet is provided for each student in forms adapted to the limitations of their health and perception of information:

- for the blind and visually impaired: in printed form in enlarged font, in the form of an electronic document, in the form of an audio file.
- for the deaf and hard of hearing: in printed form, in the form of an electronic document.
- for students with musculoskeletal disorders: in printed form, in the form of an electronic document, in the form of an audio file.

Classrooms for all types of contact and independent work, a scientific library and other training premises are equipped with special equipment and training places with technical teaching aids:

- for the blind and visually impaired: a scanning and reading device with a SARA CE camera; Braille display PAC Mate 20; Braille printer EmBraille View Plus ;
- for the deaf and hard of hearing: automated workstation for people with hearing loss and hard of hearing; acoustic amplifier and speakers;
- for students with musculoskeletal disorders: mobile, adjustable ergonomic desks SI-1; computer equipment with special software.

18. Methodological materials

18.1 Seminar lesson plans

No.	Name of the discipline section	Content
1	Retrospective analysis of legal norms on information security	**Control questions:** 1. Reveal the main stages of information security development. 2. Describe the development of information security legislation in Russia. 3. What is the significance of judicial acts in the development of information security legislation in Russia.

		Practical tasks (comparative analysis of normative legal acts, analysis of acts of the judiciary) **Testing on the topic**
2	Information security legislation system	**Control questions** 1. Give the concept of information security. 2. Reveal the basic principles of state policy on information security. 3. Describe the system of legislation of the Russian Federation on information security. 4. The role and significance of the Constitution of the Russian Federation in ensuring information security. 5. System of federal legislative acts on information security. 6. Describe the main by-laws on information security. 7. Disclose the types of legal liability for violation of information security legislation. **Practical tasks** (analysis of regulatory legal acts) **Testing on the topic**
3	Information security in the field of economic activity	**Control questions** 1. The concept of the digital economy and its strategic nature. 2. Structure of the national program "Digital Economy". 3. Main directions of ensuring information security of the digital economy. 4. The concept of an Internet account. 5. Qualification of actions under someone else's account when voluntarily providing access to the account. 6. Use of an account by a third party against the will of the owner. 7. The concept and meaning of e-commerce. 8. Stages of an agreement for the purchase of goods remotely. 9. Protection of violated rights in electronic commerce. **Practical tasks** (analysis of regulatory legal acts) **Testing on the topic**
4	Protection of intellectual property in cyberspace	**Control questions** 1. The concept of intellectual property and its objects. 2. Features of the responsibility of an information intermediary. 3. Legal methods of protecting intellectual rights. 4. Technical means and methods of protecting copyright on the Internet. 5. Protection of personal non-property rights. 6. Protection of exclusive rights. 7. Administrative liability for violation of intellectual rights. 8. Criminal liability for violation of intellectual rights. Practical task (problem solving) Testing on the topic
5	Protection of personal data in the digital environment	**Control questions** 1. Concept and categories of personal data.

		2. Obligations of the operator of the subject's personal data. 3. Legal ways to protect personal data. **Practical task** (problem solving) **Testing on the topic**
6	Legal protection from destructive content in the digital environment	**Control questions** 1. The concept of destructive content. 2. Information the distribution of which is prohibited on the territory of the Russian Federation. 3. Legal measures to restrict access to sites containing illegal content. **Practical task** (problem solving) **Testing on the topic**

18.2Glossary by discipline

The author is a citizen whose creative work created the result of intellectual activity.

Copyrights are intellectual rights to works of science, literature and art.

An administrative offense is an unlawful guilty action (inaction) of an individual or legal entity for which administrative liability is established by the Code of the Russian Federation on Administrative Offenses or the laws of the constituent entities of the Russian Federation on administrative offenses.

The owner of an aggregator of information about goods (services) is an organization, regardless of its legal form, or an individual entrepreneur who is the owner of a program for electronic computers and (or) the owner of a website and (or) a website page on the Internet information and telecommunications network and who provide the consumer with respect to a certain product (service) with the opportunity to simultaneously familiarize himself with the seller's (performer's) offer to conclude a purchase and sale agreement for goods (an agreement for the provision of paid services), to conclude a purchase and sale agreement (an agreement for the provision of paid services) with the seller (performer), and also make an advance payment for the specified product (service) by cash payments or transfer of funds to the owner of the aggregator within the framework of the applicable forms of non-cash payments.

The owner of a site on the Internet is a person who independently and at his own discretion determines the procedure for using a site on the Internet, including the procedure for posting information on such a site.

State secret is information protected by the state in the field of its military, foreign policy, economic, intelligence, counterintelligence and operational investigative activities, the dissemination of which could harm the security of the Russian Federation.

A disciplinary offense is the failure or improper performance by an employee of his assigned job duties through his fault.

Identification is a set of measures to establish information about a person and verify them, carried out in accordance with federal laws and regulations adopted in accordance with them, and to compare this information with a unique designation (unique designations) of information about a person necessary to identify such a person.

Intellectual property is the results of intellectual activity and equivalent means of individualization of legal entities, goods, works, services and enterprises that are provided with legal protection.

Internet account is an account of a specific user located in an information system that identifies this user and also contains certain (additional to identification) data .

Information security is a state of protection of the individual, society and the state from internal and external information threats, which ensures the implementation of the constitutional rights and freedoms of man and citizen, a decent quality and standard of living for citizens, sovereignty, territorial

integrity and sustainable socio-economic development of the Russian Federation, defense and state security.

An information and communication network is a technological system designed to transmit information over communication lines, accessed using computer technology.

Information technologies – processes, methods of searching, collecting, storing, processing, providing, distributing information and methods for implementing such processes and methods.

Information intermediary - a person who transmits material on an information and telecommunication network, including on the Internet, a person who provides the opportunity to post material or information necessary to receive it using an information and telecommunication network, a person who provides access to the material on this network.

Information – information (messages, data) regardless of the form of their presentation.

Contractor is an organization, regardless of its legal form, as well as an individual entrepreneur performing work or providing services to consumers under a paid contract.

Confidentiality of information is a mandatory requirement for a person who has gained access to certain information not to transfer such information to third parties without the consent of its owner.

Critical information infrastructure – objects of critical information infrastructure, as well as telecommunication networks used to organize the interaction of such objects.

Moral harm is physical and moral suffering caused to a citizen by actions that violate his personal non-property rights or encroach on the intangible benefits belonging to the citizen.

Depersonalization of personal data is actions as a result of which it becomes impossible to determine the ownership of personal data by a specific subject of personal data without the use of additional information.

Processing of personal data – any action (operation) or set of actions (operations) performed using automation tools or without the use of such means with personal data, including collection, recording, systematization, accumulation, storage, clarification (updating, changing), extraction, use, transfer (distribution, provision, access), depersonalization, blocking, deletion, destruction of personal data.

The object of copyright is works of science, literature and art, regardless of the merits and purpose of the work, as well as the method of its expression.

Objects of critical information infrastructure - information systems, information and telecommunication networks, automated control systems of subjects of critical information infrastructure.

Personal data – any information relating to a directly or indirectly identified or identifiable individual (subject of personal data).

Consumer is a citizen who intends to order or purchase, or who orders, purchases or uses goods (work, services) exclusively for personal, family, household and other needs not related to business activities.

Legal informatization is the process of creating optimal conditions for the fullest possible satisfaction of the information and legal needs of state and public structures, enterprises, organizations, institutions and citizens based on the effective organization and use of information resources using advanced technologies.

Representation is the execution of a transaction by one person (representative) on behalf of another person (represented) by virtue of authority based on a power of attorney, an indication of the law or an act of an authorized state body or local government body, creating, changing or terminating the civil rights and obligations of the represented .

A crime is a socially dangerous act committed guilty of guilt, prohibited by the Criminal Code of the Russian Federation under threat of punishment.

Hosting provider is a person who provides services for the provision of computing power for placing information in an information system permanently connected to the Internet.

Seller is an organization, regardless of its legal form, as well as an individual entrepreneur who sells goods to consumers under a sales contract.

Dissemination of information – actions aimed at obtaining information by an indefinite number of persons or transmitting information to an indefinite number of persons.

Website on the Internet - a set of programs for electronic computers and other information contained in an information system, access to which is provided through the Internet information and telecommunications network using domain names and (or) network addresses that allow identifying sites on the network "Internet".

Screenshot – printouts of materials posted on the information and telecommunications network.

A site page on the Internet (Internet page) is a part of a site on the Internet, accessed by an index consisting of a domain name and symbols

Technical means of copyright protection are any technologies, technical devices or their components that control access to a work, prevent or limit the implementation of actions that are not authorized by the author or other copyright holder in relation to the work.

Destruction of personal data – actions as a result of which it becomes impossible to restore the content of personal data in the personal data information system and (or) as a result of which material media of personal data are destroyed.

Digital economy is an economic activity in which the key production factor is data in digital form, the processing of large volumes and the use of analysis results of which, in comparison with traditional forms of management, can significantly increase the efficiency of various types of production, technologies, equipment, storage, sales, delivery of goods and services.

The ecosystem of the digital economy is a partnership of organizations that ensures the constant interaction of their technological platforms, applied Internet services, analytical systems, information systems of government authorities of the Russian Federation, organizations and citizens.

E-commerce is a system of economic relations that are carried out using the Internet; making transactions (deals) via the Internet.

Electronic signature is information in electronic form that is attached to or otherwise associated with other information in electronic form (signed information) and that is used to identify the person signing the information.

Electronic means of payment - a means and (or) method that allows a client of a money transfer operator to draw up, certify and transmit orders for the purpose of transferring funds within the framework of applicable forms of non-cash payments using information and communication technologies, electronic media, including payment cards, as well as other technical devices.

Annex 1 . Abstract of
the discipline's work program

ABSTRACT OF THE DISCIPLINE WORK PROGRAM

The purpose of the discipline is a comprehensive study of legal security in the information space, including the features of regulation of various areas of activity and legal protection in cyberspace.

Objectives of the discipline:

- gaining knowledge about legal security in the information space, including the specifics of regulation of certain areas of activity and the specifics of legal protection measures in cyberspace.
- formation of skills and abilities that allow implementing legal protection measures in the information space.

As a result of mastering the discipline, the student must:

Know : the main stages of information security development; the system of legislation on information security and liability for its violation; a system of legal protection measures in the information space in various areas (fields) of activity.

Be able to : apply legal norms to implement legal protection in the information space.

Possess : knowledge of legislation in the field of information space; knowledge of information security compliance; special skills of legal defense in the information space.