

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

10.04.01 Информационная безопасность

Код и наименование направления подготовки/специальности

Организация и технологии защиты государственной тайны

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 от 16.06.2022

ОГЛАВЛЕНИЕ

1. Пояснительная записка	4
1.1. Цель и задачи дисциплины	4
1.2. Перечень планируемых результатов обучения по дисциплине	4
1.3. Место дисциплины в структуре образовательной программы	4
2. Структура дисциплины.....	4
3. Содержание дисциплины.....	5
4. Образовательные технологии	5
5. Оценка планируемых результатов обучения.....	6
5.1 Система оценивания	6
5.2 Критерии выставления оценки по дисциплине.....	6
5.3 Оценочные средства (материалы) для текущего контроля успеваемости, промежуточной аттестации обучающихся по дисциплине	7
6. Учебно-методическое и информационное обеспечение дисциплины.....	20
6.1 Список источников и литературы	20
6.2 Перечень ресурсов информационно-телекоммуникационной сети «Интернет».	22
6.3 Профессиональные базы данных и информационно-справочные системы.....	22
7. Материально-техническое обеспечение дисциплины	22
8. Обеспечение образовательного процесса для лиц с ограниченными возможностями здоровья и инвалидов.....	22
9. Методические материалы.....	23
9.1 Планы семинарских занятий.....	23
9.2 Иные материалы:.....	25
<i>Глоссарий по дисциплине</i>	Ошибка! Закладка не определена.
Приложение 1. Аннотация рабочей программы дисциплины	29

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 23.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.

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 – <i>зачет</i>		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	<p>Выставляется обучающемуся, если он глубоко и прочно усвоил теоретический и практический материал, может продемонстрировать это на занятиях и в ходе промежуточной аттестации.</p> <p>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.</p> <p>Свободно ориентируется в учебной и профессиональной литературе.</p> <p>Оценка по дисциплине выставляется обучающемуся с учётом результатов текущей и промежуточной аттестации.</p> <p>Компетенции, закреплённые за дисциплиной, сформированы на уровне – «высокий».</p>

Баллы/ Шкала ECTS	Оценка по дисциплине	Критерии оценки результатов обучения по дисциплине
82-68/ С	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 выставляется 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 выставляется 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. 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 выставляется 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	
<i>Статья, часть статьи</i>	<i>Основные положения</i>

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 проверке 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 место жительства покупателя, а также номер его телефона. Также на сайте отсутствовал документ, содержащий 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 частного 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 частного 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 немущественных 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 неоднократно одновременно 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 норма 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, содержащий 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, являющемуся 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, являющемуся 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 КонсультантПлюс. 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. MicrosoftOffice
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 EmBrailleViewPlus;

- 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, регулируемые 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	<p>Контрольные вопросы:</p> <ol style="list-style-type: none"> 1. Раскройте основные этапы развития информационной безопасности. 2. Охарактеризуйте развитие законодательства об информационной безопасности в России.

		<p>3. Какое значение судебных актов в развитии законодательства об информационной безопасности в России.</p> <p>Практические задания (сравнительный анализ нормативных правовых актов, анализ актов судебной власти)</p> <p>Тестирование по теме</p>
2	Система законодательства об информационной безопасности	<p>Контрольные вопросы</p> <ol style="list-style-type: none"> 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. <p>Практические задания (анализ нормативных правовых актов)</p> <p>Тестирование по теме</p>
3	Информационная безопасность в сфере экономической деятельности	<p>Контрольные вопросы</p> <ol style="list-style-type: none"> 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. <p>Практические задания (анализ нормативных правовых актов)</p> <p>Тестирование по теме</p>
4	Защита объектов интеллектуальной собственности в киберпространстве	<p>Контрольные вопросы</p> <ol style="list-style-type: none"> 1. Понятие интеллектуальной собственности и его объекты. 2. Особенности ответственности информационного

		<p>посредника.</p> <p>3. Правовые способы защиты интеллектуальных прав.</p> <p>4. Технические средства и способы защиты авторских прав в сети Интернет.</p> <p>5. Защита личных неимущественных прав.</p> <p>6. Защита исключительных прав.</p> <p>7. Административная ответственность за нарушение интеллектуальных прав.</p> <p>8. Уголовная ответственность за нарушение интеллектуальных прав.</p> <p>Практическое задание (решение задач)</p> <p>Тестирование по теме</p>
5	Защита персональных данных в цифровой среде	<p>Контрольные вопросы</p> <p>1. Понятие и категории персональных данных.</p> <p>2. Обязанности оператора персональных данных субъекта.</p> <p>3. Правовые способы защиты персональных данных.</p> <p>Практическое задание (решение задач)</p> <p>Тестирование по теме</p>
6	Правовая защита от деструктивного контента в цифровой среде	<p>Контрольные вопросы</p> <p>1. Понятие деструктивного контента.</p> <p>2. Информация, распространение которой на территории РФ запрещено.</p> <p>3. Правовые меры ограничения доступа к сайтам, содержащим противоправный контент.</p> <p>Практическое задание (решение задач)</p> <p>Тестирование по теме</p>

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 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, удостоверить 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.

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.