

Документ подписан простой электронной подписью Информация о владельце: ФИО: Таскаев Сергей Валерьевич Должность: Ректор Дата подписания: 02.06.2025 11:50:53 Уникальный программный ключ: 04c19ed8bfb98f3b6cb77a486b9a8788b8322323	МИНОБРАЗОВАНИЯ РОССИИ Федеральное государственное бюджетное образовательное учреждение высшего образования «Челябинский государственный университет» (ФГБОУ ВО «ЧелГУ»)	стр. 1
---	--	---------------

Рабочая программа дисциплины (модуля)* Правовые обеспечение информационной безопасности

Направление подготовки (специальность)

40.03.01 Юриспруденция

Направленность (профиль)

уголовно-правовой

Присваиваемая квалификация (степень)

Бакалавр

Форма обучения

очно-заочная

Год(ы) набора 2023

*Рабочая программа дисциплины (модуля) адаптирована для инклюзивного обучения инвалидов и лиц с ограниченными возможностями здоровья

Челябинск 2023 г.



Содержание

1. Цели освоения дисциплины
2. Место дисциплины в структуре ОПОП
3. Компетенции обучающегося, формируемые в результате освоения дисциплины (модуля)
4. Объем дисциплины (модуля)
5. Структура и содержание дисциплины (модуля)
6. Фонд оценочных средств
 - 6.1. Перечень видов оценочных средств
 - 6.2. Типовые контрольные задания и иные материалы для текущей аттестации
 - 6.3. Типовые контрольные вопросы и задания для промежуточной аттестации
 - 6.4. Критерии оценивания
7. Учебно-методическое и информационное обеспечение дисциплины (модуля)
 - 7.1. Рекомендуемая литература
 - 7.2. Перечень ресурсов информационно-телекоммуникационной сети "Интернет"
 - 7.3. Перечень информационных технологий
8. Материально-техническое обеспечение дисциплины (модуля)
9. Методические указания для обучающихся по освоению дисциплины (модуля)
10. Специальные условия освоения дисциплины обучающимися с инвалидностью и ограниченными возможностями здоровья



1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Дисциплина «Правовые основы информационной безопасности» имеет теоретико-прикладной характер и предполагает ознакомление студентов с основами законодательства Российской Федерации, действующего в сфере регулирования информационных отношений и обеспечения информационной безопасности. В рамках этой учебной дисциплины происходит ознакомление с основами государственной политики в информационной сфере, с основными понятиями информационного права и информационной безопасности, с особенностями построения информационных систем, формами и способами защиты информации коммерческих и государственных структур. Преподавание учебной дисциплины «Правовые основы информационной безопасности» носит интегративный характер, направленный на формирование у студентов системы знаний, умений и навыков, необходимых для профессиональной деятельности в соответствии с квалификационными характеристиками бакалавра юриспруденции.

Целью преподавания дисциплины «Правовые основы информационной безопасности» являются формирование у будущих юристов профессиональной компетенции (ПК-1) "Способен юридически правильно квалифицировать факты и обстоятельства". Должны быть сформированы навыки реализации компетенции ПК-1.1: Способен юридически правильно квалифицировать факты и обстоятельства. В результате изучения дисциплины «Правовые основы информационной безопасности» студенты должны знать содержание юридической квалификации фактов и обстоятельств и правила разработки документов правового характера в сфере информационной безопасности (реализация компетенции ПК-1.1), уметь юридически правильно квалифицировать факты и обстоятельства, разрабатывать документы правового характера в сфере информационной безопасности (реализация компетенции ПК-1.1), владеть навыками квалификации фактов и обстоятельств, разработки документов правового характера в сфере информационной безопасности (реализация компетенции ПК-1.1).

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП

Цикл (раздел) ОПОП: Б1.О.31

2.1 Требования к предварительной подготовке обучающегося:

Логика

Правоохранительные органы

Теория государства и права

2.2 Дисциплины и практики, для которых освоение данной дисциплины (модуля) необходимо как предшествующее:

Уголовный процесс

Административное право

Криминалистика

3. КОМПЕТЕНЦИИ ОБУЧАЮЩЕГОСЯ, ФОРМИРУЕМЫЕ В РЕЗУЛЬТАТЕ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)

ОПК-8: Способен целенаправленно и эффективно получать юридически значимую информацию из различных источников, включая правовые базы данных, решать задачи профессиональной деятельности с применением информационных технологий и с учетом требований информационной безопасности

Знать:

Для ОПК-8.1. Знает источники получения юридически значимой информации

Уметь:

Для ОПК-8.1 Уметь: получать юридически значимую информацию из различных источников

Владеть:

Для ОПК-8.2 владеть: способностью решать задачи профессиональной деятельности, применяя информационные технологии с учетом требований информационной безопасности

ОПК-9: Способен понимать принципы работы современных информационных технологий и использовать их для решения задач профессиональной деятельности

Знать:

Для ОПК-9.1 Знать: виды современных информационных технологий, основные принципы их работы

Уметь:

Для ОПК 9.1 уметь: применять основные виды современных информационных технологий, основные принципы их



работы

Владеть:

Для ОПК-9.2 Решает задачи профессиональной деятельности с использованием современных информационных технологий

Владеть: способностью решать задачи профессиональной деятельности с использованием современных информационных технологий

В результате освоения дисциплины обучающийся должен

3.1 Знать:	
3.1.1	Знает виды современных информационных технологий, основные принципы их работы
3.1.2	источники получения юридически значимой информации
3.1.3	справочно-правовые системы для решения задач профессиональной деятельности с применением информационных технологий
3.2 Уметь:	
3.2.1	Умеет применять основные виды современных информационных технологий, основные принципы их работы.
3.2.2	Умеет получать юридически значимую информацию из различных источников
3.2.3	использовать справочные правовые системы, с учетом требований информационной безопасности.
3.3 Владеть:	
3.3.1	способностью решать задачи профессиональной деятельности с использованием современных информационных технологий
3.3.2	способностью решать задачи профессиональной деятельности, применяя информационные технологии с учетом требований информационной безопасности

4. ОБЪЕМ ДИСЦИПЛИНЫ (МОДУЛЯ)

Общая трудоемкость			3 ЗЕТ
Часов по учебному плану	:	108	Виды контроля в семестрах: зачеты 7
в том числе	:		
аудиторные занятия	:	10	
самостоятельная работа	:	96,25	
контактная работа:	:	11,75	
ИКР:	:	1,75	

5. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

Код занятия	Наименование разделов и тем /вид занятия/	Семестр / Курс	Часов	Литература
	Раздел 1. Тема 1. Информация как объект правового регулирования.			
1.1	Тема 1. Информация как объект правового регулирования. /Лек/	7	1	Л1.1 Л1.1 Л1.1Л3.1 Л3.2 Э1
	Раздел 2. Тема 2. Правые вопросы обеспечение информационной безопасности.			
2.1	/Лек/	7	1	Л1.1 Л1.1 Л1.1Л3.2 Э1
2.2	/Пр/	7	2	Л1.2 Л1.1Л1.1 Э1
	Раздел 3. Тема 3. Правовое регулирование отношений по защите государственной тайны.			
3.1	/Лек/	7	1	Л1.1 Л1.1 Л1.1Л3.2



	Раздел 4. Тема 3. Правовое регулирование отношений по защите государственной тайны.			
4.1	Понятие правового режима государственной тайны. Государственная тайна как особый вид защищаемой информации и ее характерные признаки. Сведения, составляющие государственную тайну. Принципы, механизмы и процедура отнесения сведений к государственной тайне, их засекречивания и рассекречивания. Порядок распоряжения сведениями, составляющими государственную тайну. Органы защиты государственной тайны и их компетенция. Порядок допуска и доступа к государственной тайне. Перечень и содержание организационных мер, направленных на защиту государственной тайны. Юридическая ответственность за нарушение правового режима защиты государственной тайны. /Пр/	7	2	Л1.1 Л1.1 Л1.1Л3.2 Э1
4.2	/ИКР/	7	1,75	
	Раздел 5. Тема 5. Правовое регулирование отношений в области обработки персональных данных.			
5.1	/Лек/	7	1	Л3.1 Л1.1 Л1.1 Л1.1Л1.2Л3.2
	Раздел 6. Тема 5. Правовое регулирование отношений в области обработки персональных данных.			
6.1	Понятие персональных данных, их категории. Понятие правового режима защиты персональных данных. Принципы обработки персональных данных. Порядок и условия обработки персональных данных (автоматизированная и неавтоматизированная обработка персональных данных). Права субъектов персональных данных. Обязанности оператора при обработке персональных данных. Контроль и надзор за соблюдением законодательства при обработке персональных данных. Регуляторы в области защиты персональных данных и их функции. Юридическая ответственность за нарушение законодательства персональных данных. /Пр/	7	2	Л1.1 Л1.1 Л1.1Л3.1 Л1.2Л3.2 Э1
	Раздел 7. Самостоятельная работа			
7.1	Тема 1. Информация как объект правового регулирования. Тема 2. Правые вопросы обеспечения информационной безопасности. Тема 3. Правовое регулирование отношений по защите государственной тайны. Тема 4. Правовое регулирование отношений, связанных с режимом коммерческой тайны. Тема 5. Правовое регулирование отношений в области обработки персональных данных. Тема 6. Правовое регулирование электронного документооборота. Тема 7. Правовое регулирование отношений в области связи и массовых коммуникаций. Тема 8. Правовое регулирование отношений в области библиотечного и архивного дела. Тема 9. Правовое регулирование отношений в сфере организации и деятельности средств массовой информации. /Ср/	7	96,25	Л3.1 Л1.1 Л1.1Л1.2 Л1.1Л3.2 Э1

6. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

6.1. Перечень видов оценочных средств

тест
устный опрос

6.2. Типовые контрольные задания и иные материалы для текущей аттестации

Тесты для контроля знаний студентов

Правильные ответы помечены *.

1. В соответствии с Конституцией Российской Федерации информация и связь относятся:



- а) к исключительному ведению Российской Федерации*;
б) к совместному ведению Российской Федерации и субъектов Российской Федерации;
в) к ведению субъектов Российской Федерации.
2. Согласно легальному определению информация - это:
а) сведения о каких-либо событиях, явлениях, процессах, передаваемые от человека к человеку;
б) сведения (сообщения, данные) независимо от формы их представления*;
в) сообщение, переданное или полученное пользователем информационно-телекоммуникационной сети.
3. Лицо, самостоятельно создавшее информацию, либо получившее право разрешать или ограничивать доступ к информации, является:
а) создателем информации;
б) хранителем информации;
в) обладателем информации*.
4. Не подлежат размещению в сети «Интернет»:
а) фамилии, имена и отчества председателя суда, заместителей председателя суда, судей, руководителя аппарата суда;
б) тексты судебных актов, вынесенные по делам, затрагивающим безопасность государства*;
в) информация о внепроцессуальных обращениях, поступивших судьям по делам, находящимся в их производстве.
5. Объективная сторона информационной безопасности- это:
а) психологическое отношение граждан к вопросу правового регулирования отношений в сфере информационной безопасности;
б) система норм права об информационной безопасности*;
в) система охранительных действий субъектов информационного права в отношении объекта охраны.
6. Под киберпреступлением понимается:
а) самостоятельный вид виновно совершенного общественно опасного деяния, запрещенного нормами Уголовного кодекса Российской Федерации;
б) любое преступление, совершенное в сфере информационной безопасности;
в) совершение действий в системе Интернет, при которых компьютер является орудием либо предметом посяательства в кибернетическом пространстве*.
7. Понятие «информационная безопасность» закреплено:
а) в Законе Российской Федерации от 27 декабря 1991г. №1224-11 «О средствах массовой информации»;
б) в Федеральном законе от 27.07.2006 №149-ФЗ «Об информации, информационных технологиях и о защите информации»;
в) в Доктрине информационной безопасности*.
8. К числу носителей сведений, составляющих государственную тайну, не относится:
а) руководитель органа государственной власти*;
б) служебные документы;
в) техническое устройство.
9. Система защиты государственной тайны представляет собой:
а) совокупность органов защиты государственной тайны и используемых ими средств и методов защиты*;
б) процедуры оформления права граждан на доступ к сведениям, составляющим государственную тайну, а предприятий, учреждений и организаций - на проведение работ с использованием таких сведений;
в) порядок и способы отнесения сведений к государственной тайне и их засекречивание.
10. Под засекречиванием сведений понимается:
а) взаимная передача сведений, составляющих государственную тайну, органами государственной власти, предприятиями, учреждениями и организациями;
б) передача сведений, составляющих государственную тайну, другим государствам или международным организациям;
в) ведение ограничений на распространение сведений, составляющих государственную тайну, и на доступ к их носителям*.
11. Материальный ущерб, наносимый собственнику информации в связи с ее засекречиванием, возмещается



государством в размерах, определяемых:

- а) административным актом органа государственной власти, в распоряжение которого переходит эта информация;
- б) в договоре между органом государственной власти, в распоряжение которого переходит эта информация, и ее собственником*;
- в) в соответствии с заявлением собственника информации.

12. К сведениям, составляющим государственную тайну, без проведения проверочных мероприятий допускаются:

- а) представители истца и ответчика в суде;
- б) действующие судьи*;
- в) члены Правительства РФ.

13. Коммерческая тайна представляет собой:

- а) защищаемые юридическим лицом сведения любого характера (производственные, технические, экономические), имеющие коммерческую ценность в силу неизвестности их третьим лицам;
- б) режим конфиденциальности информации, позволяющий ее обладателю при существующих или возможных обстоятельствах увеличить доходы, избежать неоправданных расходов, сохранить положение на рынке товаров, работ, услуг или получить иную коммерческую выгоду*;
- в) сведения, для которых установлен специальный режим сбора, хранения, обработки, распространения и использования, доступ к которым ограничен в соответствии с федеральным законом.

14. Могут быть отнесены к информации, составляющей коммерческую тайну:

- а) сведения о составе имущества государственного или муниципального предприятия, государственного учреждения;
- б) сведения о численности и составе работников, о системе оплаты труда;
- в) сведения, позволяющие юридическому лицу увеличить доходы и избежать неоправданных расходов*.

15. Обладателем секрета производства является:

- а) лицо, которое использует ноу-хау в целях извлечения прибыли;
- б) лицо, которое владеет информацией, составляющей коммерческую тайну, на законном основании*;
- в) любое юридическое лицо или индивидуальный предприниматель.

16. По лицензионному договору:

- а) одна сторона обязуется оформить в интересах другой стороны исключительное право на секрет производства;
- б) одна сторона передает или обязуется передать принадлежащее ей исключительное право на секрет производства в полном объеме другой стороне;
- в) одна сторона - обладатель исключительного права на секрет производства предоставляет или обязуется предоставить другой стороне право использования соответствующего секрета производства в установленных договором пределах*.

17. Материальный ущерб, наносимый собственнику информации в связи с ее засекречиванием, возмещается государством в размерах, определяемых:

- а) административным актом органа государственной власти, в распоряжение которого переходит эта информация;
- б) в договоре между органом государственной власти, в распоряжение которого переходит эта информация, и ее собственником*;
- в) в соответствии с заявлением собственника информации.

18. Информация, относящаяся к прямо или косвенно определенному или определяемому лицу является:

- а) персональными данными субъекта*;
- б) коммерческой тайной;
- в) служебной тайной.

19. Правами в информационной сфере пользуются:

- а) только физические лица;
- б) физические лица и юридические лица;
- в) физические лица, юридические лица, органы государственной власти, должностные лица, общественные организации*.

20. Не относятся к числу специальных категорий персональных данных:

- а) сведения, которые характеризуют физиологические особенности человека*;
- б) сведения, касающиеся расовой и национальной принадлежности;



в) сведения о состоянии здоровья и интимной жизни человека.

21. К числу прав субъекта персональных данных относятся:

- а) право на выбор вида обработки персональных данных автоматизированная, неавтоматизированная);
- б) право на доступ к своим персональным данным*;
- в) право контролировать деятельность оператора персональных данных.

22. Информация в электронной форме, которая присоединена к другой информации в электронной форме или иным образом связана с такой информацией и которая используется для определения лица, подписывающего информацию – это:

- а) ключ электронной подписи;
- б) сертификат ключа проверки электронной подписи;
- в) электронная подпись*.

23. Информация, переданная или полученная пользователем информационно-телекоммуникационной сети, называется:

- а) электронным сообщением*;
- б) базой данных;
- в) электронной цифровой подписью.

24. Удостоверяющий центр - это:

- а) государственный орган, осуществляющий функции по созданию и выдаче сертификатов ключей проверки электронных подписей, а также иные функции, предусмотренные законодательством Российской Федерации;
- б) любое юридическое или физическое лицо, осуществляющие функции по созданию и выдаче сертификатов ключей проверки электронных подписей, а также иные функции, предусмотренные законодательством Российской Федерации;
- в) юридическое лицо или индивидуальный предприниматель, осуществляющие функции по созданию и выдаче сертификатов ключей проверки электронных подписей, а также иные функции, предусмотренные законодательством Российской Федерации*.

25. Тайна взы представляет собой:

- а) деятельность по приему, обработке, хранению, передаче, доставке сообщений электросвязи или почтовых отправлений;
- б) нечто скрываемое от других, известное не всем; секрет;
- в) определенный режим доступа к информации, не подлежащей разглашению без согласия пользователя услуг, который реализуется путём принятия специальных мер организационного, правового, технического характера*.

26. В соответствии с Федеральным законом « О почтовой связи» в Российской Федерации действуют:

- а) почтовая связь общего пользования, осуществляемая государственными унитарными предприятиями, государственными учреждениями почтовой связи, а также иными операторами почтовой связи;
- б) почтовая связь общего пользования; специальная связь федерального органа исполнительной власти; федеральная фельдъегерская связь; фельдъегерско-почтовая связь*;
- в) специальная связь федерального органа исполнительной власти, осуществляющего управление деятельностью в области связи; федеральная фельдъегерская связь; фельдъегерско-почтовая связь федерального органа исполнительной власти в области обороны.

27. Деятельность юридических лиц и индивидуальных предпринимателей по возмездному оказанию услуг связи:

- а) не подлежит лицензированию;
- б) осуществляется только на основании лицензии на осуществление деятельности в области оказания услуг связи*;
- в) подлежит лицензированию только в предусмотренных законом случаях.

28. Не может выступать учредителем средства массовой информации:

- а) государственный орган;
- б) гражданин другого государства *;
- в) гражданин Российской Федерации, признанный судом дееспособным.

29. Средство массовой информации - это:

- а) результат интеллектуальной деятельности;
- б) печатные, аудио-, аудиовизуальные и иные сообщения и материалы;
- в) форма периодического распространения массовой информации*.



30. Деятельность средства массовой информации не может быть прекращена или приостановлена:

- а) по решению учредителя;
- б) судом в порядке гражданского судопроизводства по иску регистрирующего органа;
- в) судом по требованию органа, осуществляющего цензуру*.

Вопросы для устного опроса (собеседования):

Тема 1. Информация как объект правового регулирования.

Понятие, структура и признаки информационного общества. Информация как объект правового регулирования. Содержание и значение информационной политики. Тенденции развития информационного общества. Информационно правовое отношение, его элементы. Законодательство Российской Федерации в сфере информационной безопасности.

Тема 2. Правовые вопросы обеспечения информационной безопасности.

Общие вопросы информационных прав и свобод человека и гражданина. Сущность конституционного права на информацию и его гарантии. Особенности обеспечения информационной безопасности в различных сферах жизни общества. Правонарушение в информационной сфере, состав правонарушения. Гражданская, административная, уголовная, дисциплинарная и иные виды ответственности за правонарушения в информационной сфере.

Тема 3. Правовое регулирование отношений по защите государственной тайны.

Понятие правового режима государственной тайны. Государственная тайна как особый вид защищаемой информации и ее характерные признаки. Сведения, составляющие государственную тайну. Принципы, механизмы и процедура отнесения сведений к государственной тайне, их засекречивания и рассекречивания. Порядок распоряжения сведениями, составляющими государственную тайну. Органы защиты государственной тайны и их компетенция. Порядок допуска и доступа к государственной тайне. Перечень и содержание организационных мер, направленных на защиту государственной тайны. Юридическая ответственность за нарушение правового режима защиты государственной тайны.

Тема 4. Правовое регулирование отношений, связанных с режимом коммерческой тайны.

Понятие правового режима защиты коммерческой тайны. Информация, составляющая коммерческую тайну (секреты производства). Нормативное регулирование, порядок и процедура отнесения информации к информации, составляющей коммерческую тайну (секреты производства). Охрана конфиденциальности в рамках трудовых отношений. Исключительное право на секреты производства. Распоряжение исключительным правом путем его отчуждения по договору другому лицу или заключения лицензионного договора. Ограничение исключительного права обладателя секрета производства. Юридическая ответственность за нарушение исключительного права на секрет производства.

Тема 5. Правовое регулирование отношений в области обработки персональных данных.

Понятие персональных данных, их категории. Понятие правового режима защиты персональных данных. Принципы обработки персональных данных. Порядок и условия обработки персональных данных (автоматизированная и неавтоматизированная обработка персональных данных). Права субъектов персональных данных. Обязанности оператора при обработке персональных данных. Контроль и надзор за соблюдением законодательства при обработке персональных данных. Регуляторы в области защиты персональных данных и их функции. Юридическая ответственность за нарушение законодательства персональных данных.

Тема 6. Правовое регулирование электронного документооборота.

Общая характеристика законодательства в сфере электронного документооборота. Понятие электронного документа и электронной подписи. Принципы использования электронной подписи. Правовой режим электронной подписи. Виды электронных подписей. Простая и усиленная электронная подпись. Порядок использования простой и усиленной электронных подписей. Соотношение электронных документов с документами на бумажном носителе. Подтверждение принадлежности ключа электронной подписи ее владельцу. Правовой статус удостоверяющего центра. Признание электронных подписей, созданных в соответствии с нормами иностранного права и международными стандартами. Электронная подпись юридического лица или государственного органа. Особенности использования электронной подписи при оказании государственных и муниципальных услуг. Полномочия федеральных органов исполнительной власти в сфере использования электронной подписи.

Тема 7. Правовое регулирование отношений в области связи и массовых коммуникаций.

Понятие связи, ее структура, принципы функционирования. Государственное регулирование деятельности в области



связи. Лицензирование деятельности в области оказания услуг связи. Услуги связи. Защита прав пользователей услугами связи. Управление сетями связи в чрезвычайных ситуациях и в условиях чрезвычайного положения. Право и Интернет как социальные явления. Киберпреступления: понятие, основные черты, формы проявления. Ответственность за нарушение законодательства Российской Федерации в области связи.

Тема 8. Правовое регулирование отношений в области библиотечного и архивного дела.

Понятие библиотечного дела. Правовое регулирование отношений в области библиотечного дела. Субъекты и объекты правоотношений в области библиотечного дела. Права и обязанности граждан в области библиотечного дела. Обязанности и права библиотек. Особенности функционирования электронных библиотек. Правовое регулирование общественных отношений в области формирования обязательного экземпляра документов. Понятие и виды обязательных экземпляров документов. Правовое регулирование общественных отношений в области архивного дела и архивов. Понятие архивного дела в Российской Федерации. Основные объекты информационных правоотношений в области архивного дела. Архивный фонд. Управление архивным делом в Российской Федерации.

Тема 9. Правовое регулирование отношений в сфере организации и деятельности средств массовой информации.

Понятие и распространение массовой информации. Правовой статус средств массовой информации. Общие принципы работы средств массовой информации. Правовые формы организации деятельности средств массовой информации. Правовой статус редакции. Отношения средств массовой информации с гражданами и организациями. Распространение массовой информации средствами массовой информации. Обязательные сообщения. Профессиональный статус журналиста. Специальная редакционная ответственность средств массовой информации.

6.3. Типовые контрольные вопросы и задания для промежуточной аттестации

Вопросы к зачету

1. Вопросы к зачету

Информационное общество: понятие, структура, признаки.

Понятие информационной сферы общества.

Информация и ее виды.

Сущность конституционного права на информацию и его гарантии.

Правовые режимы информации.

Понятие и виды информационных правоотношений.

Субъекты, объекты, содержание информационных правоотношений.

Законодательство Российской Федерации в области информационной безопасности.

Понятие информационной безопасности.

Особенности обеспечения информационной безопасности в различных сферах общественной жизни.

Понятие правонарушений в информационной сфере.

Ответственность за правонарушения в информационной сфере.

Понятие государственной тайны. Сведения, составляющие государственную тайну.

Отнесение сведений к государственной тайне, их засекречивание и рассекречивание.

Порядок распоряжения сведениями, составляющими государственную тайну.

Защита сведений, составляющих государственную тайну.

Юридическая ответственность за нарушение режима государственной тайны.

Понятие коммерческой тайны. Информация, составляющая коммерческую тайну (секреты производства).

Отнесение информации к информации, составляющей коммерческую тайну (секрет производства).

Содержание и реализация исключительного права на секрет производства.

Ответственность за нарушение исключительного права на секрет производства.

Понятие и виды персональных данных.

Принципы обработки персональных данных.

Порядок и условия обработки персональных данных.

Права и обязанности субъекта персональных данных.

Права и обязанности оператора при обработке персональных данных.

Контроль и надзор за обработкой персональных данных.

Ответственность за нарушение положений законодательства о персональных данных.

Понятие электронного документа и электронного документооборота.

Правовое регулирование и юридические риски электронного документооборота.

Общая характеристика законодательства в сфере электронного документооборота.

Понятие и виды электронной подписи.

Правовой статус удостоверяющего центра.

Полномочия федеральных органов исполнительной власти в сфере использования электронной подписи.

Правовое регулирование отношений в области формирования обязательного экземпляра документов.

Правовое регулирование общественных отношений в сфере формирования, хранения, учета и использования



архивов и архивных фондов.

Понятие связи, ее структура, принципы функционирования.

Общая характеристика отношений в сфере связи и массовых коммуникаций.

Государственное регулирование деятельности в области связи.

Право и Интернет как социальные явления.

Особенности регулирования интернет-отношений.

Правовое регулирование деятельности в киберпространстве.

Киберпреступления: понятие, основные черты, формы проявления.

Понятие и распространение массовой информации.

Понятие и правовой статус средства массовой информации.

Правовые формы организации деятельности средств массовой информации.

Общие принципы работы средств массовой информации.

Правовые формы организации деятельности средств массовой информации.

Специальная редакционная ответственность средств массовой информации.

Особенности владения навыками сбора обработки информации, имеющей значение для реализации правовых норм в соответствующих сферах профессиональной деятельности.

Проявление навыков работы с информацией в глобальных компьютерных сетях.

Квалифицирующие факты и обстоятельства киберпреступлений.

Виды правонарушений в информационной сфере и особенности предупреждения правонарушений.

6.4. Критерии оценивания

1. Критерии оценивания тестирования:

- Оценка "отлично" - 86-100 % выполненных заданий (max – 100);
- Оценка "хорошо" - 71-85 % выполненных заданий;
- Оценка "удовлетворительно" - 56-70 % выполненных заданий;
- Оценка "неудовлетворительно" - менее 55 % выполненных заданий.

2. Общий порядок проведения экзамена и критерии оценивания промежуточной аттестации:

Порядок проведения промежуточной аттестации.

Порядок проведения промежуточной аттестации устанавливается действующими нормативными документами ФГБОУ ВО «ЧелГУ» (Положением о текущем контроле и промежуточной аттестации обучающихся в федеральном государственном бюджетном образовательном учреждении высшего образования «Челябинский государственный университет» по программам высшего образования).

Промежуточная аттестация обучающихся осуществляется при условии положительного результата по итогам контроля знаний. Формой контроля знаний является зачет, предполагающий ответ на теоретический вопрос. На зачете оцениваются теоретические знания обучающегося и приобретенные навыки их практического применения. Зачет проводится в соответствии с графиком учебного процесса и расписанием сессии.

3. Критерии оценки знаний студентов при проведении опроса – специальная беседа преподавателя со студентом на темы, связанные с изучаемой дисциплиной, рассчитанная на вынесение объема знаний студента по определенному разделу, теме, проблеме.

Критериями устного ответа выступают следующие качества знаний:

полнота – количество знаний об изучаемом объекте, входящих в программу;

глубина – совокупность осознанных знаний об объекте;

конкретность – умение раскрыть конкретные проявления обобщенных знаний (доказать на примерах основные положения);

системность – представление знаний об объекте в системе, с выделением структурных её элементов, расположенных в логической последовательности;

развёрнутость – способность развернуть знания в ряд последовательных шагов;

осознанность – понимание связей между знаниями, умение выделить существенные и несущественные связи, познание способов и принципов получения знаний.

7. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

7.1. Рекомендуемая литература

7.1.1. Основная литература

	Авторы,	Заглавие	Издательство,	Ресурс
--	---------	----------	---------------	--------



	Авторы,	Заглавие	Издательство,	Ресурс
Л1.1	Шаньгин В.Ф.	Комплексная защита информации в корпоративных системах: учебное пособие (https://znanium.com/catalog/document?id=389857)	Москва : Издательский Дом "ФОРУМ", 2022	ЭБС

7.1.2. Дополнительная литература

	Авторы,	Заглавие	Издательство,	Ресурс
Л2.1		Защита персональных данных в информационных системах: лабораторный практикум: практикум (https://biblioclub.ru/index.php?page=book&id=494823)	Ставрополь : Северо- Кавказский Федеральный университет (СКФУ), 2018	ЭБС
Л2.2	Ярочкин В.И.	Информационная безопасность: учебник (https://www.studentlibrary.ru/book/ISBN9785829130312.html)	Москва : Академический Проект, 2020	ЭБС

7.1.3. Методические разработки

	Авторы,	Заглавие	Издательство,	Ресурс
Л3.1	Брауде-Золотарёв М. Ю., Сербина Е. С., Негородов В. С., Волошкин И. Г.	Персональные данные в государственных информационных ресурсах: монография (https://biblioclub.ru/index.php?page=book&id=443169)	Москва : Дело, 2016	ЭБС
Л3.2	Клименко И.С.	Информационная безопасность и защита информации: модели и методы управления: монография (https://znanium.com/catalog/document?id=397337)	Москва : ООО "Научно- издательский центр ИНФРА- М", 2022	ЭБС
Л3.3	Мельников В. П., под ред., Куприянов А. И.	Информационная безопасность: учебник (https://book.ru/book/944143)	Москва : КноРус, 2022	ЭБС

7.2. Перечень ресурсов информационно-телекоммуникационной сети "Интернет"

Э1	https://e.lanbook.com https://biblio-online.ru https://elibrary.ru/defaultx.asp http://www.supcourt.ru http://ks.rfnet.ru http://www.fsb.ru http://www.advpalata.ru http://www.mvd.ru http://www.minjust.ru http://genproc.gov.ru
----	--

7.3 Перечень информационных технологий

7.3.1 Программное обеспечение

MS Office365

LMS Moodle

Adobe Reader

7.3.2 Профессиональные базы данных и информационно-справочные системы

1. Научная электронная библиотека eLIBRARY.RU (<https://elibrary.ru/defaultx.asp?>) eLIBRARY.RU : научная электронная библиотека : сайт. – Москва, 2000 – . – URL: <https://elibrary.ru>. – Режим доступа: для зарегистрир. пользователей. – Текст : электронный.

2. Справочно-правовая система «КонсультантПлюс» (<http://www.consultant.ru/>) КонсультантПлюс : справочно-правовая система : база данных / Региональный центр правовой информации Информправо. – Москва, 1992 – . – Режим доступа: из читальных залов библиотеки. – Текст : электронный.



3. Справочно-правовая система «Гарант» (<http://www.garant.ru/>) ГАРАНТ.РУ : информационно-правовой портал / ООО «НПО ГАРАНТ-СЕРВИС». – Москва, 1990 – . – Режим доступа: из читальных залов библиотеки 1-го корпуса (читальный зал № 3 – ауд. 205, медиацентр – ауд. 206, библиотека юридической литературы – ауд. 215). – Текст : электронный.

4. Национальная электронная библиотека (НЭБ) (<https://rusneb.ru/>) Национальная электронная библиотека (НЭБ) : объединенный электронный каталог фондов российских библиотек : сайт. – URL: <http://нэб.рф>. – Режим доступа: из читальных залов библиотеки ЧелГУ. – Текст : электронный.

8. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

Для реализации дисциплины используются учебные аудитории для проведения занятий лекционного типа, занятий семинарского типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации, а также помещения для самостоятельной работы.

Учебные аудитории укомплектованы специализированной мебелью и техническими средствами обучения: доска, парты, мультимедийное и аудио оборудование.

Для проведения занятий лекционного типа предлагаются наборы демонстрационного оборудования и учебно-наглядных пособий: цифровые образовательные ресурсы, мультимедийный проектор, переносное и /или стационарное мультимедийное оборудование (ноутбук, проектор, колонки).

Для проведения семинарских занятий используются аудитории, оснащенные обычной доской, партами, переносным мультимедийным оборудованием (ноутбук, проектор, колонки).

Помещения для самостоятельной работы обучающихся оснащены компьютерной техникой с подключением к сети "Интернет" и обеспечением доступа в электронную информационно-образовательную среду университета.

9. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ (МОДУЛЯ)

Изучение учебной дисциплины «Правовые основы информационной безопасности» требует от студента серьезного и добросовестного отношения к овладению специальными знаниями, необходимыми для становления качественно нового уровня юридического образования и практики.

Сложности, которые возникают в ходе аудиторной и внеаудиторной работы, объясняются большим объемом подлежащего освоению учебного материала и необходимостью тщательной самостоятельной подготовки.

Эффективному освоению материала учебной дисциплины способствует внимательная проработка лекционного материала, позволяющая сформировать целостное представление относительно основных закономерностей административной деятельности органов внутренних дел.

Лекционный курс охватывает наиболее значимые вопросы каждой темы изучения. Уяснение лекционного материала контролируется устным опросом и тестированием. Изучение проблем каждого раздела дисциплины продолжается в ходе подготовки и участия в практических занятиях.

Форма проведения практического занятия объявляется студентам заранее.

Большую часть времени обучающиеся самостоятельно работают с учебно-методическими материалами. Студенты имеют возможность консультироваться с преподавателем по всем вопросам, возникающим в ходе самостоятельной работы посредством электронной почты, социальных сетей и т.п.

Доступ обучающегося к учебным ресурсам в режиме отложенного времени, самостоятельной работы осуществляется через сеть Интернет в удобном для него месте, времени и темпе.

Виды самостоятельной работы:

- конспектирование подзаконных нормативно-правовых источников;
- проработка учебного материала (по конспектам лекций, учебной и научной литературе) и подготовка докладов для практических занятий;
- работа с юридическими источниками и законодательной базой;
- написание творческих работ (эссе);
- работа с тестами и вопросами для самопроверки.

Результаты самостоятельной работы контролируются преподавателем и учитываются при текущей аттестации студента. При этом проводятся: тестирование, экспресс-опрос на практических занятиях, заслушивание докладов, проверка письменных работ и т.д.

Несомненно, умение анализировать юридические источники, работать с литературой, навыки поиска, обработки и оформления необходимой информации, способность обосновывать собственную позицию помогут студенту в дальнейшей самостоятельной учебной и научной работе.

При обучении лиц с ограниченными возможностями здоровья электронное обучение, дистанционные образовательные технологии предусматривают возможность приема-передачи информации в доступных для них формах.



Реализация дисциплины с применением электронного обучения, дистанционных образовательных технологий (далее – ЭО, ДОТ) осуществляется на основании «Положения о реализации основных и дополнительных образовательных программ с применением электронного обучения и дистанционных образовательных технологий в федеральном государственном бюджетном образовательном учреждении высшего образования «Челябинский государственный университет», «Положения о порядке зачета обучающимися по основным профессиональным образовательным программам высшего образования в ФГБОУ ВО «ЧелГУ» результатов освоения в организациях, осуществляющих образовательную деятельность, учебных предметов, курсов, дисциплин (модулей), практик, дополнительных образовательных программ» посредством электронной информационно-образовательной среды ФГБОУ ВО «ЧелГУ». В исключительных случаях (форс-мажор и т.п.) при реализации образовательной деятельности с применением ЭО, ДОТ могут применять компоненты, не входящие в перечень электронной информационно-образовательной среды.

В случае применения при обучении дисциплины электронного обучения, дистанционных образовательных технологий общение обучающихся и преподавателя осуществляется в режиме реального времени (онлайн-лекции (вебинары), чаты, видео-конференции и др.) или отложенного времени (система дистанционного обучения Moodle, MSOffice365, форумы, электронная почта и др.).

Большую часть времени обучающиеся самостоятельно работают с учебно-методическими материалами. Студенты имеют возможность консультироваться с преподавателем по всем вопросам, возникающим в ходе самостоятельной работы посредством электронной почты, социальных сетей и т.п.

Доступ обучающегося к учебным ресурсам в режиме отложенного времени, самостоятельной работы осуществляется через сеть Интернет в удобном для него месте, времени и темпе».

При обучении лиц с ограниченными возможностями здоровья электронное обучение, дистанционные образовательные технологии предусматривают возможность приема-передачи информации в доступных для них формах.

Реализация дисциплины с применением электронного обучения, дистанционных образовательных технологий (далее – ЭО, ДОТ) осуществляется на основании «Положения о реализации основных и дополнительных образовательных программ с применением электронного обучения и дистанционных образовательных технологий в федеральном государственном бюджетном образовательном учреждении высшего образования «Челябинский государственный университет», «Положения о порядке зачета обучающимися по основным профессиональным образовательным программам высшего образования в ФГБОУ ВО «ЧелГУ» результатов освоения в организациях, осуществляющих образовательную деятельность, учебных предметов, курсов, дисциплин (модулей), практик, дополнительных образовательных программ» посредством электронной информационно-образовательной среды ФГБОУ ВО «ЧелГУ». В исключительных случаях (форс-мажор и т.п.) при реализации образовательной деятельности с применением ЭО, ДОТ могут применять компоненты, не входящие в перечень электронной информационно-образовательной среды.

10. СПЕЦИАЛЬНЫЕ УСЛОВИЯ ОСВОЕНИЯ ДИСЦИПЛИНЫ ОБУЧАЮЩИМИСЯ С ИНВАЛИДНОСТЬЮ И ОГРАНИЧЕННЫМИ ВОЗМОЖНОСТЯМИ ЗДОРОВЬЯ

Освоение дисциплины инвалидами и лицами с ограниченными возможностями здоровья осуществляется с использованием специальных технических средств и голо информационных технологий, предоставляемых Ресурсным учебно-методическим центром по обучению инвалидов и лиц с ограниченными возможностями здоровья ЧелГУ по запросу обучающегося.

1. Мобильные специальные технические средства для лиц с нарушениями зрения: портативный компьютер с вводом/выводом шрифтом Брайля с синтезатором речи «EiBraille-W14J G2»; ноутбуки с программной экранного доступа NVDA; электронные увеличители для удаленного просмотра; видеоувеличители портативные; тифлоплеер; цифровые диктофоны.

2. Мобильные специальные технические средства для лиц с нарушениями слуха: система свободного звукового поля со встроенной совместимостью с FM-устройствами; радиоклассы «Сонет-PCM» с передатчиком, заушным индуктором и индукционной петлей; система информационная для слабослышащих переносная «Исток» А2 со встроенным плеером – звуковым информатором; документ-камера; программируемые слуховые аппараты индивидуального пользования.

3. Ассистивные информационные технологии: программное обеспечение экранного доступа с синтезом речи NVDA; программы экранного увеличения; программы речевого синтеза для компьютеров и ноутбуков; программы речевого синтеза для мобильных устройств; экранная клавиатура; экранная лупа.

При необходимости для обучающихся с нарушениями зрения на рабочих местах для проведения практических или лабораторных занятий устанавливается специальное программное обеспечение (программа речевой навигации NVDA, речевые синтезаторы, экранные лупы).

В учебные аудитории обеспечивается беспрепятственный доступ для обучающихся инвалидов и обучающихся с ограниченными возможностями здоровья. В каждой аудитории, где обучаются инвалиды и лица с ограниченными



возможностями здоровья, предусматривается соответствующее количество мест для обучающихся с учетом нарушений их здоровья.

Для освоения дисциплины инвалидам и лицам с ограниченными возможностями здоровья предоставляется доступ к печатным источникам, имеющимся в научной библиотеке ЧелГУ, с помощью специальных технических средств; доступ к электронным источникам, представленным в форме электронного документа в фонде научной библиотеки ЧелГУ или электронно-библиотечных системах, с помощью специальных технических и программных средств (рабочее место для незрячего пользователя с программным обеспечением экранного доступа с синтезом речи NVDA, рабочее место с компьютерным роллером и клавиатурой Clevy с большими кнопками и с разделяющей клавиши накладкой).

Учебно-методические материалы для обучающихся из числа инвалидов и лиц с ограниченными возможностями здоровья предоставляются в формах, адаптированных к ограничениям их здоровья и восприятия информации:

Для лиц с нарушениями зрения:

- в печатной форме увеличенным шрифтом,
- в форме электронного документа,
- в форме аудиофайла,
- в печатной форме шрифтом Брайля.

Для лиц с нарушениями слуха:

- в печатной форме,
- в форме электронного документа.

Для лиц с нарушениями опорно-двигательного аппарата:

- в печатной форме,
- в форме электронного документа,
- в форме аудиофайла.

Данный перечень может быть конкретизирован в зависимости от контингента обучающихся.

Для инвалидов и лиц с ограниченными возможностями здоровья освоение дисциплины может быть частично или полностью осуществлено с использованием дистанционных образовательных технологий (Moodle, Adobe Connect Pro и пр.).

В освоении дисциплины инвалидами и лицами с ограниченными возможностями здоровья используется индивидуальная работа. Под индивидуальной работой подразумевается две формы взаимодействия с преподавателем: индивидуальная учебная работа (консультации), т.е. дополнительное разъяснение учебного материала и углубленное изучение материала с теми обучающимися, которые в этом заинтересованы, и индивидуальная воспитательная работа. Индивидуальные консультации направлены на индивидуализацию обучения и установлению воспитательного контакта между преподавателем и обучающимся инвалидом или обучающимся с ограниченными возможностями здоровья.

При проведении процедуры оценивания результатов обучения инвалидов и лиц с ограниченными возможностями здоровья по дисциплине обеспечивается выполнение следующих дополнительных требований в зависимости от индивидуальных особенностей, обучающихся:

- а) инструкция по порядку проведения процедуры оценивания предоставляется в доступной форме (устно, в письменной форме, в письменной форме шрифтом Брайля, устно с использованием услуг сурдопереводчика);
- б) доступная форма предоставления заданий оценочных средств (в печатной форме, в печатной форме увеличенным шрифтом, в печатной форме шрифтом Брайля, в форме электронного документа, задания зачитываются ассистентом, задания предоставляются с использованием сурдоперевода);
- в) доступная форма предоставления ответов на задания (письменно на бумаге, набор ответов на компьютере, письменно шрифтом Брайля, с использованием услуг ассистента, устно).

При проведении процедуры оценивания результатов обучения инвалидов и лиц с ограниченными возможностями здоровья предусматривается использование технических средств, необходимых им в связи с их индивидуальными особенностями. Эти средства могут быть предоставлены ЧелГУ или могут использоваться собственные технические средства. При необходимости инвалидам и лицам с ограниченными возможностями здоровья предоставляется дополнительное время для подготовки ответа на задания, процедура оценивания результатов обучения по дисциплине может проводиться в несколько этапов.

Проведение процедуры оценивания результатов обучения инвалидов и лиц с ограниченными возможностями здоровья допускается с использованием дистанционных образовательных технологий.

**2023-2024_УР_40_03_01_УРР_оз_2023_(ДЛЯ ИП)_plx_Правовые обеспечение
информационной безопасности**

Проректор по учебной работе утверждено 24.04.2023 В.Е. Федоров

Ученым советом института права

Протокол заседания № 13 от 17.04.2023

Председатель Ученого совета
института права

согласовано

А.А. Великий

**Заседанием кафедры прокурорского надзора и организации правоохранительной
деятельности**

Протокол заседания № 9 от 14.04.2023

Заведующий кафедрой

согласовано

А.В. Майоров

Автор (составитель)

Макашова Т.П.

**Структура рабочей программы соответствует приказу ректора ФГБОУ ВО
«ЧелГУ» от «13» апреля 2021 г. № 247-1**