

Документ подписан простой электронной подписью
Информация о владельце:
ФИО: Чумакова Лидия Петровна
Должность: Директор НЮИ(ф)ТГУ
Дата подписания: 31.07.2024 15:55:04
Уникальный программный ключ:
b0ab169ee4b8a4189968d4a664a074d7ef8855f4

Министерство науки и высшего образования Российской Федерации
НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ
ТОМСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ (НИ ТГУ)
Новосибирский юридический институт (филиал) ТГУ

УТВЕРЖДАЮ:
Директор НЮИ (ф) ТГУ

Л.П. Чумакова
« 17 » июня 2024 г.

Рабочая программа дисциплины

ПРАВОВОЕ ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

по направлению подготовки

40.04.01 Юриспруденция

Магистерская программа
«Частное право в эпоху цифровизации»

Форма обучения

Очная

Квалификация

Магистр

Год приема

2024

Код дисциплины в учебном плане: Б1.В.07

СОГЛАСОВАНО:

Руководитель ОПОП

 И.В. Фролов

Председатель МК

 И.В. Фролов

Новосибирск – 2024

1. Цель и планируемые результаты освоения дисциплины (модуля)

Целью освоения дисциплины является формирование следующих компетенций:

УК-4	Способен применять современные коммуникативные технологии, в том числе на иностранном языке, для академического и профессионального взаимодействия
ПК-2	Способен разрешать правовые споры и регламентировать отношения в сфере частного права
ПК-3	Способен подготавливать аналитические заключения в частноправовой сфере правового регулирования
ПК-7	Способен проводить поиск научно-практических проблем и осуществлять научные исследования в сфере гражданского права и частноправового регулирования общественных отношений

Результатами освоения дисциплины являются следующие индикаторы достижения компетенций:

ИУК-4.1	Обосновывает выбор актуальных коммуникативных технологий (информационные технологии, модерирование, медиация и др.) для обеспечения академического и профессионального взаимодействия
ИПК-2.4	Оказывает услуги по разрешению споров гражданско-правового характера
ИПК-3.1	Владеет навыками по сбору информации и составлению аналитических заключений в сфере частного права
ИПК-3.2	Умеет систематизировать и классифицировать информацию в сфере частноправовых отношений
ИПК-3.3	Проводит обобщение и оценку правовых действий юридических служб организаций в сфере хозяйственной деятельности
ИПК-7.1	Обладает навыками поиска и выявления проблем теории и практики частноправового регулирования

2. Задачи освоения дисциплины

- Обладать навыками по выбору актуальных коммуникативных технологий (информационные технологии, модерирование, медиация и др.) для обеспечения академического и профессионального взаимодействия и построения систем безопасности
- Обладать навыками по предоставлению услуги по разрешению споров гражданско-правового характера в сфере информационной безопасности
- Владеть навыками по сбору информации и составлению аналитических заключений в сфере частного права
- Уметь систематизировать и классифицировать информацию в сфере частноправовых отношений и обеспечивать безопасность её хранения
- Проводить обобщение и оценку правовых действий юридических служб организаций в сфере хозяйственной деятельности и безопасности
- Обладать навыками поиска и выявления проблем теории и практики частноправового регулирования в сфере информационной безопасности

3. Место дисциплины (модуля) в структуре образовательной программы

Дисциплина относится к части образовательной программы, формируемой участниками образовательных отношений, является обязательной для изучения.

4. Семестр(ы) освоения и форма(ы) промежуточной аттестации по дисциплине

Семестр 2, зачет.

5. Входные требования для освоения дисциплины

Для успешного освоения дисциплины требуются компетенции, сформированные в ходе освоения образовательных программ предшествующего уровня образования (бакалавриат), а именно при изучении таких дисциплин как конституционное право, теория государства и права, информационные технологии в юридической деятельности, гражданское право, гражданский процесс, арбитражный процесс.

6. Язык реализации

Русский

7. Объем дисциплины (модуля)

Общая трудоемкость дисциплины составляет 3 з.е., 108 часов, из которых:

– лекции: 4 ч.;

– семинарские занятия: 0 ч.

– практические занятия: 22 ч.;

– лабораторные работы: 0 ч.

в том числе практическая подготовка: 0 ч.

Объем самостоятельной работы студента определен учебным планом.

8. Содержание дисциплины (модуля), структурированное по темам

Тема 1. Введение в информационную безопасность и её правовое обеспечение

Информационная безопасность. Основные понятия. Модели информационной безопасности. Виды защищаемой информации. Основные нормативно-правовые акты в области информационной безопасности. Правовые особенности обеспечения безопасности конфиденциальной информации и государственной тайны.

Тема 2. Организационное обеспечение информационной безопасности и технические методы её защиты

Основные стандарты в области обеспечения информационной безопасности. Политика безопасности. Экономическая безопасность предприятия. Инженерная защита объектов. Защита информации от утечки по техническим каналам. Программно-аппаратные средства и методы обеспечения информационной безопасности. Основные виды сетевых и компьютерных угроз. Средства и методы защиты от сетевых компьютерных угроз.

Тема 3. Криптографические методы защиты информации

Симметричные и асимметричные системы шифрования. Цифровые подписи (Электронные подписи). Инфраструктура открытых ключей. Криптографические протоколы.

Тема 4. Применение информационных технологий для изучения вопросов организационно-правового обеспечения информационной безопасности

Использование баз данных для нахождения и изучения нормативных документов в области информационной безопасности. Использование криптографических средств защиты информации. Создание зашифрованных файлов и криптоконтейнеров и их расшифрование.

Тема 5. Реализация работы инфраструктуры открытых ключей

Создание удостоверяющего центра, генерация открытых и секретных ключей, создание сертификатов открытых ключей, создание электронной подписи, проверка электронной подписи. Средства стеганографии для защиты информации. Использование средств стеганографии для защиты файлов.

Тема 6. Настройка безопасного сетевого соединения

Создание защищенного канала связи средствами виртуальной частной сети. Антивирусные средства защиты информации. Изучение настроек средств антивирусной защиты информации.

9. Текущий контроль по дисциплине

Текущий контроль по дисциплине проводится путем контроля посещаемости, выполнения практических заданий, выполнения заданий в программе PowerPoint.

10. Порядок проведения и критерии оценивания промежуточной аттестации

Зачет по дисциплине, проводится во втором семестре. Форма зачета – устный ответ по билетам. Билет содержит два теоретических вопроса.

Первые теоретические вопросы билета, проверяющие ИПК-3.2; ИПК-3.3; ИПК-7.1 включаются в билет из предложенного списка и предполагают ответ в развернутой форме с учетом знаний о защите информации в рамках занятий по курсам информатики и гражданского права.

Вторые теоретические вопросы билета, проверяющие ИУК-4.1; ИПК-2.4; ИПК-3.1 включаются в билет из предложенного списка и предполагают ответ в развернутой форме с учетом по систематизации и классификации методов защиты информации с учетом современных технологий и различных моделей процессуального регулирования данных правоотношений, в том числе с использованием цифровых технологий.

Примерный перечень теоретических вопросов к зачету

1. Введение в информационную безопасность и её правовое обеспечение.
2. Информационная безопасность.
3. Основные понятия.
4. Модели информационной безопасности.
5. Виды защищаемой информации.
6. Основные нормативно-правовые акты в области информационной безопасности.
7. Правовые особенности обеспечения безопасности конфиденциальной информации.
8. Правовые особенности обеспечения государственной тайны.
9. Организационное обеспечение информационной безопасности и технические методы её защиты.
10. Основные стандарты в области обеспечения информационной безопасности.
11. Политика безопасности.
12. Экономическая безопасность предприятия.
13. Формирование правовой системы экономической безопасности предприятия.
14. Инженерная защита объектов.
15. Защита информации от утечки по техническим каналам.
16. Программно-аппаратные средства и методы обеспечения информационной безопасности.
17. Основные виды сетевых и компьютерных угроз.
18. Средства и методы защиты от сетевых компьютерных угроз.

19. Юридические средства и методы защиты от сетевых компьютерных угроз.
 20. Судебная защита от сетевых компьютерных угроз.
 21. Криптографические методы защиты информации.
 22. Симметричные и ассиметричные системы шифрования.
 23. Цифровые подписи (Электронные подписи).
 24. Инфраструктура открытых ключей.
 25. Криптографические протоколы.
 26. Применение информационных технологий для изучения вопросов организационно-правового обеспечения информационной безопасности.
 27. Использование баз данных для нахождения и изучения нормативных документов в области информационной безопасности.
 28. Использование криптографических средств защиты информации.
 29. Ответственность за нарушение криптографических средств защиты информации.
 30. Создание зашифрованных файлов и криптоконтейнеров и их расшифрование.
 31. Реализация работы инфраструктуры открытых ключей.
 32. Создание удостоверяющего центра.
 33. Генерация открытых и секретных ключей.
 34. Создание сертификатов открытых ключей.
 35. Создание электронной подписи.
 36. Правила проверки электронной подписи.
 37. Средства стеганографии для защиты информации.
 38. Использование средств стеганографии для защиты файлов.
 39. Настройка безопасного сетевого соединения.
 40. Создание защищенного канала связи средствами виртуальной частной сети.
- Антивирусные средства защиты информации.
41. Изучение настроек средств антивирусной защиты информации.
 42. Какие виды сигнализаций устанавливаются для обеспечения инженерной защиты?
 43. Что такое технические каналы утечки информации?
 44. Перечислите основные виды технических каналов утечки информации?
 45. Перечислите методы защиты информации от утечки по визуальному каналу.
 46. Перечислите методы защиты информации от утечки по воздушному каналу.
 47. Перечислите методы защиты информации от утечки по вибрационному каналу.
 48. Перечислите методы защиты информации от утечки по индукционному каналу.
 49. Перечислите средства и методы защиты информации от утечки в телефонных линиях.
 50. Перечислите основные мероприятия по обеспечению защиты информации от утечки по техническим каналам.

Обучающийся допускается к промежуточной аттестации в случае выполнения им учебного плана по дисциплине: 80% всех заданий текущего контроля. При невыполнении, в т.ч. неправильном выполнении заданий текущего контроля обучающийся дополнительно выполняет такие задания в форме, предложенной преподавателем.

При проведении промежуточной аттестации могут быть использованы технические средства обучения.

Ответ обучающегося на зачете оценивается одной из следующих оценок: «зачтено» и «не зачтено», которые выставляются по следующим критериям.

Оценки «зачтено» заслуживает обучающийся, обнаруживший всестороннее, систематическое и глубокое знание учебного и нормативного материала, умеющий свободно выполнять задания, предусмотренные программой, усвоивший основную литературу и знакомый с дополнительной литературой, рекомендованной кафедрой.

Также оценка «зачтено» выставляется обучающимся, обнаружившим полное знание учебного материала, успешно выполняющим предусмотренные в программе задания, усвоившим основную литературу, рекомендованную кафедрой, демонстрирующие систематический характер знаний по дисциплине и способные к их самостоятельному пополнению и обновлению в ходе дальнейшей учебной работы и профессиональной деятельности.

Наконец, оценкой «зачтено» оцениваются ответы обучающихся, показавших знание основного учебного материала в объеме, необходимом для дальнейшей учебы и в предстоящей работе по профессии, справляющихся с выполнением заданий, предусмотренных программой, но допустившим погрешности в ответе на зачете и при выполнении заданий, не носящие принципиального характера, когда установлено, что обучающийся обладает необходимыми знаниями для последующего устранения указанных погрешностей под руководством преподавателя.

Оценка «не зачтено» выставляется обучающимся, обнаружившим пробелы в знаниях основного учебного материала, допускающим принципиальные ошибки в выполнении предусмотренных программой заданий. Такой оценки заслуживают ответы обучающихся, носящие несистематизированный, отрывочный, поверхностный характер, когда обучающийся не понимает существа излагаемых им вопросов.

11. Учебно-методическое обеспечение

- а) Электронный учебный курс по дисциплине в электронном университете «Moodle»
- б) Оценочные материалы текущего контроля и промежуточной аттестации по дисциплине.
- в) План практических занятий по дисциплине.
- г) Методические указания по организации самостоятельной работы студентов.

12. Перечень учебной литературы и ресурсов сети Интернет

а) основная литература:

–Жарова А. К. Правовое регулирование создания и использования информационной инфраструктуры в Российской Федерации : монография / А. К. Жарова. – Москва : Издательство Юрайт, 2022. – 301 с. – (Актуальные монографии). – ISBN 978-5-534-14919-7. – URL : <https://urait.ru/bcode/496939>.

–Организационное и правовое обеспечение информационной безопасности : учебник и практикум для вузов / под ред. Т. А. Поляковой, А. А. Стрельцова. – Москва : Издательство Юрайт, 2022. – 325 с. – (Высшее образование). – ISBN 978-5-534-03600-8. – Текст : электронный // Образовательная платформа Юрайт. – URL: <https://urait.ru/bcode/498844>.

–Основы информационной безопасности : учебник / В. Ю. Рогозин, И. Б. Галушкин, В. Новиков, С. Б. Вепрев ; Академия Следственного комитета Российской Федерации. – Москва : Юнити-Дана : Закон и право, 2018. – 287 с. : ил. – Режим доступа : по подписке. – URL: <https://biblioclub.ru/index.php?page=book&id=562348>. – Библиогр. в кн. – ISBN 978-5-238-02857-6. – Текст : электронный.

б) дополнительная литература:

–Бартош А. А. Основы международной безопасности. Организации обеспечения международной безопасности : учебное пособие для вузов / А. А. Бартош. – 2-е изд., перераб. и доп. – Москва : Издательство Юрайт, 2022. – 320 с. – (Высшее образование). – ISBN 978-5-534-11783-7. – URL : <https://urait.ru/bcode/493387>.

–Басалова Г. В. Основы криптографии : курс лекций / Г. В. Басалова ; Национальный Открытый Университет "ИНТУИТ". – Москва : Интернет-Университет Информационных Технологий (ИНТУИТ), 2011. – 253 с. – Режим доступа: по подписке. – URL: <https://biblioclub.ru/index.php?page=book&id=233689>. – Текст : электронный.

–Белоус А. И. Кибероружие и кибербезопасность. О сложных вещах простыми словами : монография / А. И. Белоус, В. А. Солодуха. – Москва ; Вологда : Инфра-Инженерия, 2020. – 692 с. – ISBN 978-5-9729-0486-0. – Текст : электронный. – URL: <https://znanium.com/catalog/product/1167736>. – Режим доступа : по подписке.

–Загинайлов Ю. Н. Теория информационной безопасности и методология защиты информации : учебное пособие / Ю. Н. Загинайлов. – Москва ; Берлин : Директ-Медиа, 2015. – 255 с. : ил. – Режим доступа: по подписке. – URL: <https://biblioclub.ru/index.php?page=book&id=276557>. – Библиогр. в кн. – ISBN 978-5-4475-3946-7. – DOI 10.23681/276557. – Текст : электронный.

–Информационное право : учебник для вузов / Н. Н. Ковалева [и др.] ; под ред. Н. Н. Ковалевой. – Москва : Издательство Юрайт, 2022. – 353 с. – (Высшее образование). – ISBN 978-5-534-13786-6. – URL : <https://urait.ru/bcode/496717>.

–Информационные технологии в юридической деятельности : учебное пособие / С. Я. Казанцев, Н. М. Дубинина, А. И. Уринцов и др. ; под ред. А. И. Уринцова. – 2-е изд., перераб. и доп. – Москва : Юнити-Дана, 2020. – 353 с. : схем., табл, ил. – Режим доступа: по подписке. – URL: <https://biblioclub.ru/index.php?page=book&id=683023>. – Библиогр.: с. 341. – ISBN 978-5-238-03242-9. – Текст : электронный.

–Корабельников С. М. Преступления в сфере информационной безопасности : учебное пособие для вузов / С. М. Корабельников. – Москва : Издательство Юрайт, 2022. – 111 с. – (Высшее образование). – ISBN 978-5-534-12769-0. – URL : <https://urait.ru/bcode/496492>.

–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. – (Высшее образование). – ISBN 978-5-534-14327-0. – URL : <https://urait.ru/bcode/488767>.

–Суворова Г. М. Информационная безопасность : учебное пособие для вузов / Г. М. Суворова. – Москва : Издательство Юрайт, 2022. – 253 с. – (Высшее образование). – ISBN 978-5-534-13960-0. – URL : <https://urait.ru/bcode/496741>.

–Чернова Е. В. Информационная безопасность человека : учебное пособие для вузов / Е. В. Чернова. – 2-е изд., испр. и доп. – Москва : Издательство Юрайт, 2022. – 243 с. – (Высшее образование). – ISBN 978-5-534-12774-4. – URL : <https://urait.ru/bcode/495922>.

в) ресурсы сети Интернет:

Название ресурса	Электронный адрес	Содержание ресурса
ОФИЦИАЛЬНЫЕ РЕСУРСЫ		
Официальный интернет-портал правовой информации	http://pravo.gov.ru/	<i>Конституция РФ. Официальные информационные источники органов государственной власти Российской Федерации, официальные нормативные акты и документы</i>
Официальный интернет-портал правовой информации Новосибирской области	https://nsopravo.ru/	<i>Список опубликованных правовых актов и официальной информации Новосибирской области</i>
Правительство Новосибирской области / Нормативные правовые акты	https://www.nso.ru/npa	<i>Список опубликованных правовых актов Новосибирской области</i>
Государственная автоматизированная система	https://sudrf.ru/	<i>Судебные акты и информация о судебной системе Российской Федерации</i>

Название ресурса	Электронный адрес	Содержание ресурса
Российской Федерации «Правосудие»		
Судебные и нормативные акты РФ (СудАкт)	https://sudact.ru/	<i>Судебные акты судов Российской Федерации, нормативно-правовая информация</i>
Верховный Суд Российской Федерации / Информация по судебным делам	https://www.vsrfr.ru/lk/practice/cases	<i>Судебные акты по всем инстанциям Верховного Суда Российской Федерации</i>
ЭЛЕКТРОННЫЕ ИЗДАНИЯ		
Научная электронная библиотека eLIBRARY.RU	https://www.elibrary.ru/defaultx.asp? крупнейший российский информационно-аналитический портал в области науки, содержащий рефераты и полные тексты научных публикаций	
Научная электронная библиотека «КиберЛенинка»	https://cyberleninka.ru/ Бесплатный оперативный доступ к полным текстам научных публикаций в электронном виде	

13. Перечень информационных технологий

- а) лицензионное и свободно распространяемое программное обеспечение:
- Microsoft Office Standart 2013 Russian: пакет программ. Включает приложения: MS Office Word, MS Office Excel, MS Office PowerPoint, MS Office On-eNote, MS Office 2010 Publisher;
 - публично доступные облачные технологии (Google Docs, Яндекс диск и т.п.).
- б) информационные справочные системы:
- Национальная библиографическая база данных научного цитирования eLibrary;
 - Библиотечный информационный комплекс (электронно-библиотечная система «Университетская библиотека online»;
 - Электронная библиотека диссертаций Российской государственной библиотеки;
 - Информационно-правовая база данных «Гарант»;
 - Информационно-правовая база данных «КонсультантПлюс»;
 - Adobe Connect.
 - Электронный каталог Научной библиотеки ТГУ – <http://chamo.lib.tsu.ru/search/query?locale=ru&theme=system>;
 - Электронная библиотека (репозиторий) ТГУ – <http://vital.lib.tsu.ru/vital/access/manager/Index>;
 - ЭБС Лань – <http://e.lanbook.com/>;
 - ЭБС Консультант студента – <http://www.studentlibrary.ru/> ;
 - Образовательная платформа Юрайт – <https://urait.ru/> ;
 - ЭБС ZNANIUM.com – <https://znanium.com/>;
 - ЭБС IPRbooks – <http://www.iprbookshop.ru/>.
- в) профессиональные базы данных :
- Университетская информационная система РОССИЯ – <https://uisrussia.msu.ru/>
 - Единая межведомственная информационно-статистическая система (ЕМИСС) – <https://www.fedstat.ru/>
- г) онлайн-платформы:
- Zoom Video Communications (<https://zoom.us/signin>);
 - электронный университет «Moodle».

14. Материально-техническое обеспечение

Аудитории для проведения занятий лекционного типа.

Аудитории для проведения практических занятий и занятий семинарского типа, индивидуальных и групповых консультаций, текущего контроля и промежуточной аттестации.

Помещения для самостоятельной работы, оснащенные компьютерной техникой и доступом к сети Интернет, в электронную информационно-образовательную среду и к информационным справочным системам.

15. Информация о разработчиках

Карпов Владимир Борисович, старший преподаватель кафедры общественных наук НЮИ (ф)ТГУ.

Фролов Игорь Валентинович, доктор юридических наук, профессор, и.о. зав. кафедрой трудового, земельного и финансового права НЮИ (ф)ТГУ.