

Федеральное государственное образовательное бюджетное учреждение
высшего образования
**«ФИНАНСОВЫЙ УНИВЕРСИТЕТ
ПРИ ПРАВИТЕЛЬСТВЕ РОССИЙСКОЙ ФЕДЕРАЦИИ»**
(Финансовый университет)

Департамента международного и публичного права

УТВЕРЖДАЮ

Проректор по учебной и
методической работе

_____ Е.А. Каменева
«_02_»_декабря_2022 г.

А.В. Остроушко

Правовое обеспечение кибербезопасности

Рабочая программа дисциплины

для студентов, обучающихся по направлению подготовки
40.03.01 - ЮРИСПРУДЕНЦИЯ

ОП «Юриспруденция»,
профили «Экономическое право»,
«Международное экономическое право (с частичной реализацией
на английском языке)»

*Рекомендовано Ученым советом Юридического факультета
(протокол № 23 от 16 ноября 2022 г.)*

*Одобрено Советом Департамента международного и публичного права
(протокол № 4 от 26 октября 2022 г.)*

Москва 2022

УДК 001.1(073)
ББК 67.404.3
О-79

Рецензент:

Остроушко А.В.

Рабочая программа дисциплины «Правовое обеспечение кибербезопасности» предназначена для студентов, обучающихся по направлению подготовки 40.03.01 «Юриспруденция» – М.: Финансовый университет, Департамент международного и публичного права, 2022. – 32 с.

В рабочей программе дисциплины представлены: тематический план изучения дисциплины, содержание тем дисциплины, учебно-методическое обеспечение.

Учебное издание

Остроушко Александр Владимирович

Правовое обеспечение кибербезопасности

Рабочая программа дисциплины

Компьютерный набор, верстка: *Остроушко А.В.*

Формат 60х90/16. Гарнитура *Times New Roman*

Усл. п.л. ____ . Изд. № ____ - 2022. Тираж ____

©Остроушко Александр Владимирович, 2022

©Финансовый университет, 2022

СОДЕРЖАНИЕ

| | |
|--|----|
| 1. Наименование дисциплины..... | 4 |
| 2. Перечень планируемых результатов освоения образовательной программы (перечень компетенций) с указанием индикаторов их достижения и планируемых результатов обучения по дисциплине..... | 4 |
| 3. Место дисциплины в структуре образовательной программы | 6 |
| 4. Объем дисциплины в зачетных единицах и в академических часах с выделением объема аудиторной (лекции, семинары) и самостоятельной работы обучающихся..... | 6 |
| 5. Содержание дисциплины, структурированное по темам (разделам) дисциплины с указанием их объемов (в академических часах) и видов учебных занятий | 7 |
| 5.1. Содержание дисциплины..... | 7 |
| 5.2. Учебно-тематический план..... | 11 |
| 5.3. Содержание семинаров, практических занятий | 12 |
| 6. Перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине..... | 14 |
| 6.1. Перечень вопросов, отводимых на самостоятельное освоение дисциплины, формы внеаудиторной самостоятельной работы..... | 14 |
| 6.2. Перечень вопросов, заданий, тем для подготовки к текущему контролю..... | 17 |
| 7. Фонд оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине..... | 20 |
| 8. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины..... | 28 |
| 9. Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины..... | 29 |
| 10. Методические указания для обучающихся по освоению дисциплины..... | 29 |
| 11. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине, включая перечень необходимого программного обеспечения и информационных справочных систем..... | 32 |
| 12. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине..... | 32 |

1. Наименование дисциплины

Правовое обеспечение кибербезопасности

2. Перечень планируемых результатов освоения образовательной программы (перечень компетенций) с указанием индикаторов их достижения и планируемых результатов обучения по дисциплине

для студентов, обучающихся по направлению подготовки

40.03.01. «Юриспруденция», профиль «Международное экономическое право (с частичной реализацией на английском языке)»

| Код компетенции | Наименование компетенции | Индикаторы достижения компетенции | Результаты обучения (умения и знания), соотнесенные с индикаторами достижения компетенции |
|-----------------|---|--|--|
| 1 | 2 | 3 | 4 |
| ПКП-3 | Способность участвовать в проведении юридической экспертизы проектов национальных правовых актов на предмет их соответствия нормам и принципам международного права, а также антикоррупционным стандартам | 1. Демонстрирует знание норм национального законодательства о правовых экспертизах, их целях проведения и основных положениях. | Знать: основные положения нормативных правовых актов в области проведения юридической экспертизы проектов национальных нормативных правовых актов на предмет их соответствия нормам и принципам международного права, а также антикоррупционным стандартам. Уметь: ориентироваться в проблематике соответствия национальных правовых актов нормам и принципам международного права, а также антикоррупционным стандартам; владеть категориальным аппаратом; соотносить юридические факты с законодательством; систематизировать необходимый материал с целью проведения экспертизы; |
| | | 2. Обосновывает решения в части поставленной задачи, в целях практической реализации в области международной экономической деятельности. | Знать: основные направления реализации международной экономической деятельности; методы, способы и средства практической реализации в области международной экономической деятельности; особенности применения актов информационного законодательства; возможности использования официальных Интернет-ресурсов Уметь: соотносить юридические факты с законодательством; систематизировать необходимый материал и анализировать практику правоприменения; на основании анализа осуществлять выбор оптимального варианта обоснования решения в части поставленной задачи с учетом фактических обстоятельств |

| | | | |
|-------|--|--|---|
| | | 3. Проводит юридическую экспертизу проектов национальных нормативных правовых актов на предмет их соответствия нормам и принципам международного права, а также антикоррупционным стандартам | Знать: основные нормативные акты о противодействии коррупции; сущность и характеристики коррупционных проявлений в различных сферах общественной жизни; способы противодействия различным проявлениям коррупции Уметь: проводить юридическую экспертизу проектов национальных нормативных правовых актов на предмет их соответствия нормам и принципам международного права, а также антикоррупционным стандартам |
| ПКП-4 | Способность давать консультации и квалифицированные юридические заключения по международным экономическим вопросам | 1. Проводит юридическое консультирование по международным экономическим вопросам | Знать: основные нормативные акты о противодействии коррупции; сущность и характеристики коррупционного поведения, причины его появления и формы его проявления в различных сферах общественной жизни; существующие в обществе способы формирования нетерпимости к коррупционному поведению; способы противодействия различным проявлениям коррупционного поведения Уметь: проводить юридическое консультирование по международным экономическим вопросам |
| | | 2. Оценивает содержание нормативных правовых актов и актов правоприменения на предмет соответствия действующему законодательству в области международных экономических отношений. | Знать: принципы и методы анализа содержания нормативных правовых актов на предмет их соответствия действующему законодательству с использованием справочных правовых систем; Уметь: обрабатывать правовую информацию и аналитические материалы и проводить оценку содержания нормативных правовых актов и актов правоприменения на предмет соответствия действующему законодательству |
| | | 3. Дает квалифицированные юридические заключения по международным экономическим вопросам | Знать: основные положения нормативных правовых актов и позиции высших судебных инстанций в области регулирования международных экономических вопросов Уметь: давать квалифицированные юридические заключения по международным экономическим вопросам |

для студентов, обучающихся по направлениям подготовки
40.03.01. «Юриспруденция», профиль «Экономическое право»

| Код компетенции | Наименование компетенции | Индикаторы достижения компетенции | Результаты обучения (умения и знания), соотнесенные с индикаторами достижения компетенции |
|-----------------|---|---|---|
| 1 | 2 | 3 | 4 |
| ПКП-1 | Способность использовать фундаментальные знания в области частного и публичного права в современных условиях и оказывать помощь в реализации правовых норм субъектам гражданского права | 1. Демонстрирует знания нормативно правовых актов, а также прогнозирует результат экономической деятельности для решения практических задач | Знать: основные положения нормативных правовых актов в области обеспечения кибербезопасности; позиции высших судебных инстанций; Уметь: ориентироваться в проблематике обеспечения кибербезопасности и на данной основе прогнозировать результат экономической деятельности ; |
| | | 2. Использует фундаментальные знания в области частного и публичного права в современных условиях | Знать: фундаментальные частного и публичного права в современных условиях применительно к проблематике кибербезопасности Уметь: соотносить юридические факты с законодательством; систематизировать необходимый материал и анализировать практику правоприменения в информационно правовой сфере; осуществлять выбор оптимального варианта правомерного поведения в информационных правоотношениях с учетом фактических обстоятельств дела |
| | | 3. Оказывает помощь в реализации правовых норм субъектам гражданского оборота | Знать: основные положения нормативных правовых актов в области обеспечения кибербезопасности, угрозы кибербезопасности и правовые меры обеспечения информационной безопасности; Уметь: оказывать помощь в реализации правовых норм для обеспечения кибербезопасности субъектам гражданского оборота |
| ПКП-2 | Способность действовать с учетом кризисных ситуаций в экономике, вызываемых рисками правового и экономического | 1. Действует с учетом кризисных ситуаций в экономике, вызываемых рисками правового и экономического характера | Знать: кризисных ситуаций в экономике, вызываемых рисками нарушения кибербезопасности; Уметь: анализировать кризисные ситуации в экономике, вызываемых рисками нарушения кибербезопасности; противодействовать различным проявлениям информационных угроз |

| | | | |
|--|---|--|---|
| | характера, анализировать проблемные ситуации на рынке товаров, работ, услуг, а также выявлять правонарушения при осуществлении предпринимательской деятельности давать юридически обоснованные предложения по их преодолению и устранению | 2. Выявляет правонарушения при осуществлении предпринимательской деятельности | Знать: основные направления обеспечения кибербезопасности; требования нормативных правовых актов к субъектам предпринимательской деятельности по обеспечению кибербезопасности; Уметь: выявлять правонарушения в ходе обеспечения кибербезопасности при осуществлении предпринимательской деятельности |
| | | 3. Дает юридически обоснованные предложения по преодолению и устранению правонарушений при осуществлении предпринимательской деятельности. | Знать: основные направления правового обеспечения кибербезопасности; Уметь: вырабатывать обоснованные предложения по преодолению и устранению правонарушений при обеспечении кибербезопасности при осуществлении предпринимательской деятельности. |

3. Место дисциплины в структуре образовательной программы

Дисциплина «Правовое обеспечение кибербезопасности» входит в модуль «Международно-правовое регулирование цифровой экономики» (для проф. «Международное экономическое право (с частичной реализацией на английском языке)») и модуль «Право цифровой экономики» (для проф. «Экономическое право») цикла профиля (элективный) части, формируемой участниками образовательных отношений по направлению подготовки 40.03.01 «Юриспруденция».

4. Объем дисциплины в зачетных единицах и в академических часах с выделением объема аудиторной (лекции, семинары) и самостоятельной работы обучающихся

для очной / очно-заочной форм обучения

| Вид учебной работы по дисциплине | Всего (в з/е и часах) | Семестр 7/8 (в часах) |
|---|--------------------------|---------------------------|
| Общая трудоемкость дисциплины | 3 з.е. и 108 | 108 |
| Контактная работа - Аудиторные занятия | 34/16 | 34/16 |
| <i>Лекции</i> | 16/8 | 16/8 |
| <i>Семинары, практические занятия</i> | 18/8 | 18/8 |
| Самостоятельная работа | 74/92 | 74/92 |
| Вид текущего контроля | Контрольная работа | Контрольная работа |
| Вид промежуточной аттестации | Зачет | Зачет |

5. Содержание дисциплины, структурированное по темам (разделам) дисциплины с указанием их объемов (в академических часах) и видов учебных занятий

5.1. Содержание дисциплины

Тема 1. Понятие кибербезопасности, место кибербезопасности в системе информационной безопасности РФ

Национальная безопасность. Информационная безопасность. Соотношение кибербезопасности и информационной безопасности.

Дискуссионные вопросы определения кибербезопасности.

Необходимость правового регулирования кибербезопасности. Методы обеспечения кибербезопасности. Цель обеспечения кибербезопасности. Принципы обеспечения кибербезопасности.

Понятия информационного пространства и киберпространства. Национальная киберинфраструктура: система передачи данных, в том числе телекоммуникационной сети Интернет, и услугах, направленных на расширение использования киберпространства; система основных услуг, включающая национальную систему распределения доменных имен, национальную систему идентификации аутентификации (цифрового профиля); услуги и приложения в области информационных технологий, включая онлайн-сервисы; электронное правительство, электронная коммерция, сайты сети «Интернет» с общественно значимой информацией, онлайн-форумы, социальные сети, блоги; искусственный интеллект; инфраструктура информационных технологий умного города, система виртуальной реальности, облачные вычисления, система больших данных, системы мгновенной передачи данных и иные интеллектуальные системы.

Тема 2. Основные направления правового регулирования информационных отношений в Российской Федерации

Понятие и виды источников информационного права. Структура, состав и особенности информационного законодательства. Конституционные основы информационного законодательства.

Базовый закон информационной сферы. Базовые законодательные акты, нормативные правовые акты Президента Российской Федерации и Правительства Российской Федерации, федеральных органов исполнительной власти, регулирующие отношения в информационной сфере.

Понятие, содержание, структура информационных правоотношений.

Классификация информационных правоотношений. Объекты и субъекты информационных правоотношений.

Тема 3. Основные виды киберугроз и проблема защиты конечных пользователей

Киберпреступность.

Компьютерные атаки и инциденты (кибератаки)

Кибертерроризм.

Вредоносное программное обеспечение: вирусы, троянские программы, шпионское ПО, программы-вымогатели, рекламное ПО в Интернет, ботнеты.

Булинг.

Фишинг.

DDos – атаки.

Защита пользователей

Тема 4. Международно-правовое регулирование кибербезопасности

Международный стандарт ISO/IEC 27032:2012 «Информационные технологии. Методы обеспечения безопасности. Руководящие указания по обеспечению кибербезопасности» (ISO/ IEC 27032 Information technology. Security techniques. Guidelines for cybersecurity)

Будапештская Конвенция Совета Европы по киберпреступлениям ETS 185 от 23 ноября 2001 г. Общие правила ЕС по защите данных (GDPR) от 14 апреля 2016 года. Регламент 2019/881 Об Агентстве ЕС по кибербезопасности (ENISA) и сертификации по кибербезопасности информационных и коммуникационных технологий (Cybersecurity Act) 2019 г.

Проект Конвенции Организации Объединенных Наций о противодействии использованию информационно-коммуникационных технологий в преступных целях (подготовлен РФ).

Международные стандарты NIST, IEC 62443.

Тема 5. Правовое обеспечение кибербезопасности в РФ

Стратегия развития информационного общества в Российской Федерации об обеспечении кибербезопасности. Проблемы разработки Стратегии кибербезопасности Российской Федерации. Доктрина информационной безопасности. Указ Президента от 01 мая 2022 года №250 «О дополнительных мерах по обеспечению информационной безопасности Российской Федерации» и нормативные правовые акты, принятые для его реализации.

Государственные (национальные) стандарты РФ и руководящие документы по кибербезопасности. Правовое обеспечение безопасности критической информационной инфраструктуры Российской Федерации. Создание ГосСОПКА (государственной системы обнаружения, предупреждения и ликвидации

последствий компьютерных атак на информационные ресурсы Российской Федерации).

Критерии и методы оценки эффективности систем и средств обеспечения информационной безопасности и кибербезопасности. Оценка защищенности государственных информационных ресурсов и систем.

Создание механизма мониторинга киберугроз и реагирования на них. Повышение информированности общества в сфере кибербезопасности.

Тема 6. Правовое обеспечение кибербезопасности критической информационной инфраструктуры

Органы ответственные за обеспечение кибербезопасности критической информационной инфраструктуры. Полномочия ФСТЭК, ФСБ и иных государственных органов в сфере обеспечения кибербезопасности.

Приказ ФСТЭК России от 25 декабря 2017 г. № 239 «Об утверждении Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации». ФСБ РФ рекомендации №149/2/7-200 от 24 декабря 2016 г. «Методические рекомендации по созданию ведомственных и корпоративных центров государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации».

Категорирование объектов. Внедрение и поддержка технических средств и решений для осуществления деятельности по мониторингу информационной безопасности средств и систем мониторинга.

Осуществление взаимодействия при осуществлении информационного обмена в области обнаружения, предупреждения и ликвидации последствий компьютерных атак.

Тема 7. Правовое обеспечение кибербезопасности конечных пользователей в информационно-телекоммуникационной сети «Интернет»

Особенности правового регулирования общественных отношений в сети «Интернет». Требования к информационным ресурсам в сети «Интернет».

Распространение информации в сети «Интернет». Правовое регулирование социальных сетей.

Защита персональных данных в сети «Интернет»

Деятельности иностранных лиц в информационно-телекоммуникационной сети «Интернет».

Актуальные вопросы ограничения доступа к сайтам в сети «Интернет» с информацией, распространяемой с нарушением законодательства РФ.

Тема 8. Юридическая ответственность за правонарушения в сфере кибербезопасности

Понятие киберпреступления и правонарушения в сфере кибербезопасности.

Уголовная ответственность за киберпреступления: создание, распространение и использование программ для неправомерного воздействия; неправомерный доступ к информации с последовавшим причинением вреда; нарушение правил эксплуатации средств хранения, обработки, передачи информации; распространение заведомо недостоверной информации; несанкционированный доступ к персональным данным; преступления, связанные с экстремистской и террористической деятельностью.

Административная ответственность за противоправные деяния в киберпространстве.

5.2 Учебно-тематический план

для очной / очно-заочной форм обучения

| № п/ п | Наименование темы (раздела) дисциплины | | Трудоемкость в часах | | | | Формы текущего контроля успеваемости |
|--------------|--|-------|---|--------|--|-------------------------------|--|
| | | Всего | Аудиторная работа- Контактная работа | | | Самостояте льная работа | |
| | | | Общая | Лекции | Практич еские и семинар ские занятия | | |
| 1. | Понятие кибербезопасности, место кибербезопасности в системе информационной безопасности РФ | 17/17 | 6/2 | 2/1 | 4/1 | 11/15 | Доклады, опрос, дискуссия |
| 2. | Основные направления правового регулирования информационных отношений в Российской Федерации | 13/13 | 4/2 | 2/1 | 2/1 | 9/11 | Доклады, тестирование, опрос, дискуссия |
| 3. | Основные виды киберугроз и проблема защиты конечных пользователей | 13/13 | 4/2 | 2/1 | 2/1 | 9/11 | Доклады, тестирование, решение практических ситуационных задач, опрос, дискуссия |

| | | | | | | | |
|------------------------------|--|----------------|--------------|--------------|--------------|--------------|--|
| 4. | Международно-правовое регулирование кибербезопасности | 13/13 | 4/2 | 2/1 | 2/1 | 9/11 | Доклады, опрос, решение практических ситуационных задач, дискуссия |
| 5. | Правовое обеспечение кибербезопасности в РФ | 13/13 | 4/2 | 2/1 | 2/1 | 9/11 | Доклады, решение практических ситуационных задач, дискуссия |
| 6. | Правовое обеспечение кибербезопасности критической информационной инфраструктуры | 13/13 | 4/2 | 2/1 | 2/1 | 9/11 | Доклады, решение практических ситуационных задач, дискуссия |
| 7. | Правовое обеспечение кибербезопасности конечных пользователей в информационно-телекоммуникационной сети «Интернет» | 13/13 | 4/2 | 2/1 | 2/1 | 9/11 | Доклады, опрос, дискуссия |
| 8. | Юридическая ответственность за правонарушения в сфере кибербезопасности | 13/13 | 4/2 | 2/1 | 2/1 | 9/11 | Доклады, опрос, дискуссия |
| В целом по дисциплине | | 108/108 | 34/16 | 16/8 | 18/8 | 74/92 | Контрольная работа |
| Итого в % | | | 31/15 | 47/50 | 53/50 | 69/85 | |

5.3. Содержание семинаров, практических занятий

| Название тем дисциплины | Перечень вопросов для обсуждения на семинарских, практических занятиях, рекомендуемые источники из разделов 8, 9 | Формы проведения занятий |
|---|---|----------------------------|
| Тема 1. Понятие кибербезопасности, место кибербезопасности в системе | 1. Понятия Национальная безопасность и Информационная безопасность. 2. Определения киберпространства и кибербезопасности. 3. Необходимость правового регулирования кибербезопасности. | опрос, групповая дискуссия |

| | | |
|---|---|---|
| информационной безопасности РФ | 4. Методы обеспечения кибербезопасности. 5. Принципы обеспечения кибербезопасности. 6. Национальная киберинфраструктура. Рекомендуемые источники: раздел 8: 1, 6, 7, 8, 11, 12 раздел 9: 2, 3, 4, | |
| Тема 2. Основные направления правового регулирования информационных отношений в Российской Федерации | 1. Понятие и виды источников информационного права. 2. Структура, состав и особенности информационного законодательства. 3. Конституционные основы информационного законодательства. 4. Базовый закон информационной сферы. 5. Объекты и субъекты информационных правоотношений. 6. Права и обязанности обладателя информации. 7. Государство как субъект информационных отношений. Рекомендуемые источники: раздел 8: 1, 2, 11, 14 раздел 9: 1, 2, 3, 4, | опрос, тестирование, групповая дискуссия, презентация докладов |
| Тема 3. Основные виды киберугроз и проблема защиты конечных пользователей | 1. Субъекты кибербезопасности. 2. Киберпреступность. 3. Компьютерные атаки и инциденты. 4. Защита конечных пользователей. Рекомендуемые источники: раздел 8: 7, 12, 13, 14 раздел 9: 4, 5, 6 | опрос, групповая дискуссия, решение практических ситуационных задач, презентация докладов – |
| Тема 4. Международно-правовое регулирование кибербезопасности | 1. Международные стандарты кибербезопасности. 2. Конвенция о киберпреступности. 3. Cybersecurity Act. 4. Проблемы международно-правового обеспечения кибербезопасности. Рекомендуемые источники: раздел 8: 1, 12, 14, 15 раздел 9: 2, 3, 4, 5 | опрос, решение практико-ориентированных задач, групповая дискуссия, презентация докладов – |
| Тема 5. Правовое обеспечение кибербезопасности в РФ | 1. Нормативно правовая база Российской Федерации об обеспечении кибербезопасности. 2. Проблемы разработки Стратегии кибербезопасности Российской Федерации. 3. Государственные (национальные) стандарты РФ и руководящие документы по кибербезопасности. 4. Критерии и методы оценки эффективности систем и средств обеспечения информационной безопасности и кибербезопасности. 5. Мониторинг киберугроз и система реагирования на них | решение практико-ориентированных задач, групповая дискуссия, презентация докладов – |

| | | |
|---|--|--|
| | Рекомендуемые источники: раздел 8: 1, 2, 3, 4, 6, 11, 12, 13 раздел 9: 1, 2, 3, 4, 6 | |
| Тема 6. Правовое обеспечение кибербезопасности критической информационной инфраструктуры | 1. Понятие критической информационной инфраструктуры. 2. Принципы, задачи, функции и стандарты обеспечения безопасности критической информационной инфраструктуры. 3. ГосСОПКА. 4. Полномочия ФСТЭК, ФСБ и иных государственных органов в сфере обеспечения кибербезопасности. Рекомендуемые источники: раздел 8: 1, 4, 5, 7, 8, 11, 12, раздел 9: 2, 3, 6 | опрос, групповая дискуссия, тестирование, презентация докладов – |
| Тема 7. Правовое обеспечение кибербезопасности конечных пользователей в информационно-телекоммуникационной сети «Интернет» | 1. Особенности правового регулирования общественных отношений в сети «Интернет». 2. Актуальные вопросы ограничения доступа к сайтам в сети «Интернет» с информацией, распространяемой с нарушением законодательства РФ. 3. Правовой статус организатора распространения информации в сети "Интернет". 4. Регулирование социальных сетей 5. Особенности распространения информации в сети интернет. 6. Особенности распространения информации иностранными субъектами. Рекомендуемые источники: раздел 8: 1, 2, 3, 10, 11, 12, 13, 14 раздел 9: 1, 2, 3, 4 | Опрос, ситуационные и практические задачи, дискуссия |
| Тема 8. Юридическая ответственность за правонарушения в сфере кибербезопасности | 1. Понятия киберпреступности, киберпреступления и административного правонарушения в сфере кибербезопасности. 2. Уголовная ответственность за киберпреступления. 3. Административная ответственность за правонарушения в сфере кибербезопасности. Рекомендуемые источники: раздел 8: 1, 9, 10, 11, 12, 13, 15 раздел 9: 1, 2, 3, 4, 5 | опрос, групповая дискуссия, анализ нормативно-правовых документов и судебной практики. |

6. Перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине

6.1. Перечень вопросов, отводимых на самостоятельное освоение дисциплины, формы внеаудиторной самостоятельной работы

| Название тем дисциплины | Перечень вопросов, отводимых на самостоятельное освоение | Формы внеаудиторной самостоятельной работы |
|---|--|---|
| Тема 1. Понятие кибербезопасности место кибербезопасности в системе информационной безопасности РФ | 1. Общеметодологические проблемы обеспечения информационной безопасности и кибербезопасности. 2. Стратегия развития информационного общества в Российской Федерации. 3. Проблемы формирования понятийного (терминологического) аппарата в области кибербезопасности. 4. Проблемы развития информационной сферы как системообразующего фактора жизни общества. | Подготовка ответов на вопросы по теме занятия из рабочей программы дисциплины, работа со справочно-правовыми системами, подбор материала к групповой дискуссии, изучение рекомендованных к занятию нормативных правовых актов, литературных источников. |
| Тема 2. Основные направления правового регулирования информационных отношений в Российской Федерации | 1. Информационное право как наука, учебная дисциплина, система правового регулирования общественных отношений в информационном обществе. 2. Система информационного права. 3. Законодательные акты, нормативные правовые акты Президента Российской Федерации и Правительства Российской Федерации, федеральных органов исполнительной власти, регулирующие отношения в информационной сфере. 4. Правовой статус государственных организаций и учреждений в области обеспечения кибербезопасности. | Подготовка ответов на вопросы по теме занятия из рабочей программы дисциплины, изучение рекомендованных к занятию нормативных правовых актов и литературных источников, подготовка к решению практических и ситуационных задач. |
| Тема 3. Основные виды киберугроз и проблема защиты конечных пользователей | 1. Проблемы выявления, идентификации, классификации, оценки угроз информационной безопасности. 2. Проблемы создания, совершенствования и обеспечения функционирования государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации. 3. Научно-технические проблемы развития современных информационных технологий, индустрии средств информатизации, телекоммуникации и связи. 4. Проблемы защиты личности в ходе трансграничного использования информационных технологий. | Подготовка ответов на вопросы по теме занятия из рабочей программы дисциплины, изучение рекомендованных к занятию нормативных правовых актов, судебной практики и литературных источников, подготовка к решению практических и ситуационных задач. |
| Тема 4. Международно-правовое регулирование кибербезопасности | 1. Кибербезопасность как компонент международных отношений. 2. Правовые гарантии свободы коммуникации. 3. Закона о кибербезопасности Европейского союза (ЕС). 4. Международные стандарты кибербезопасности | Подготовка ответов на вопросы по теме занятия из рабочей программы дисциплины, изучение рекомендованных к занятию нормативных правовых актов, судебной практики и литературных источников, подготовка к |

| | | |
|---|--|--|
| | 5. Проблемы обеспечения снижения риска использования информационных и коммуникационных технологий для осуществления враждебных действий и актов агрессии, направленных на дискредитацию суверенитета, нарушение территориальной целостности государств и представляющих угрозу международному миру, безопасности и стратегической стабильности. | решению практических и ситуационных задач. |
| Тема 5. Правовое обеспечение кибербезопасности в РФ | <ol style="list-style-type: none"> 1. Проблемы противодействия угрозам и вызовам информационной безопасности личности, общества, государства и международного сообщества. 2. Проблемы развития системы обеспечения кибербезопасности Российской Федерации. 3. Проблемы влияния информационной сферы на конкурентоспособность России на современном этапе. 4. Проблемы оценки информационной безопасности личности, общества и государства. 5. Проблемы развития нормативного правового и нормативного технического обеспечения кибербезопасности. | Подготовка ответов на вопросы по теме занятия из рабочей программы дисциплины, изучение рекомендованных к занятию нормативных правовых актов, судебной практики и литературных источников, подбор материала к групповой дискуссии, подготовка к решению практических и ситуационных задач. |
| Тема 6. Правовое обеспечение кибербезопасности критической информационной инфраструктуры | <ol style="list-style-type: none"> 1. Критическая информационная инфраструктура России. 2. Проблемы нормативного правового обеспечения устойчивости функционирования и безопасности использования информационных систем и телекоммуникационных сетей, в том числе в составе глобальной информационной инфраструктуры. 3. Проблемы противодействия использованию информационных технологий в террористических целях для оказания деструктивного воздействия на элементы критической информационной инфраструктуры. | Подготовка ответов на вопросы по теме занятия из рабочей программы дисциплины, работа со справочно-правовыми системами, изучение рекомендованных к занятию нормативных правовых актов, судебной практики, литературных источников. |
| Тема 7. Правовое обеспечение кибербезопасности конечных пользователей в информационно-телекоммуникационной сети «Интернет» | <ol style="list-style-type: none"> 1. Особенности правового регулирования общественных отношений в сети «Интернет». 2. Государственный сегмент сети «Интернет». 3. Требования к информационным ресурсам в сети «Интернет». 4. Противодействие киберугрозам в социальных сетях | Подготовка ответов на вопросы по теме занятия из рабочей программы дисциплины, изучение рекомендованных к занятию нормативных правовых актов, судебной практики и литературных источников, подбор материала к групповой дискуссии. |

| | | |
|--|---|--|
| Тема 8. Юридическая ответственность за правонарушения в сфере кибербезопасности | 1. Субъекты юридической ответственности за нарушения в информационном пространстве. 2. Уголовная ответственность за киберпреступления. 3. Иные виды юридической ответственности за нарушения в информационном пространстве. | Подготовка ответов на вопросы по теме занятия из рабочей программы дисциплины, работа со справочно-правовыми системами, изучение рекомендованных к занятию нормативных правовых актов, судебной практики, литературных источников. |
|--|---|--|

6.2. Перечень вопросов, заданий, тем для подготовки к текущему контролю

Перечень примерных тем Контрольной работы:

1. Основные угрозы кибербезопасности, влияющие на темпы роста информационного общества в Российской Федерации.
2. Соотношение кибербезопасности и информационной безопасности.
3. Дискуссионные вопросы определения кибербезопасности.
4. Понятия информационного пространства и киберпространства.
5. Структура, состав и особенности информационного законодательства.
6. Конституционные основы информационного законодательства.
7. Базовый закон информационной сферы.
8. Объекты и субъекты правоотношений в сфере кибербезопасности.
9. Киберпреступность: понятие и виды.
10. Компьютерные атаки и инциденты (кибератаки)
11. Кибертерроризм.
12. Вредоносное программное обеспечение: понятие и виды.
13. Проблемы КиберБулинга.
14. Фишинг и противодействие ему.
15. DDos – атаки: понятие и противодействие.
16. Международный стандарт ISO/IEC 27032:2012: Основные положения.
17. Будапештская Конвенция Совета Европы по киберпреступлениям ETS 185 от 23 ноября 2001 г.
18. Регламент 2019/881 Об Агентстве ЕС по кибербезопасности (ENISA) и сертификации по кибербезопасности информационных и коммуникационных технологий (Cybersecurity Act) 2019 г.
19. Стратегия развития информационного общества в Российской Федерации об обеспечении кибербезопасности.
20. Проблемы разработки Стратегии кибербезопасности Российской Федерации.

21. Государственные (национальные) стандарты РФ и руководящие документы по кибербезопасности.

22. Государственная система обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации.

23. Повышение информированности общества в сфере кибербезопасности.

24. Органы, ответственные за обеспечение кибербезопасности критической информационной инфраструктуры.

25. Приказ ФСТЭК России от 25 декабря 2017 г. № 239 : основные требования.

26. Особенности правового регулирования общественных отношений в сети «Интернет».

27. Требования к безопасности информационных ресурсов в сети «Интернет».

28. Правовое регулирование социальных сетей.

29. Защита персональных данных в сети «Интернет»

30. Деятельности иностранных лиц в информационно-телекоммуникационной сети «Интернет».

31. Актуальные вопросы ограничения доступа к сайтам в сети «Интернет» с информацией, распространяемой с нарушением законодательства РФ.

32. Понятие киберпреступления и правонарушения в сфере кибербезопасности.

33. Уголовная ответственность за киберпреступления.

34. Административная ответственность за нарушения в области обеспечения кибербезопасности.

Перечень примерных тем для докладов

35. Основные требования, по обеспечению кибербезопасности, предъявляемые государственным информационным ресурсам.

36. Основные препятствия, влияющие на темпы роста информационного общества в Российской Федерации.

37. Динамика разработки правовых актов информационного законодательства и ее обусловленность.

38. Проблематика международного правового противодействия киберугрозам.

39. Сравнительный анализ законодательства по обеспечению кибербезопасности Евросоюза и США.

40. Нормативное регулирование обеспечения кибербезопасности в Сбербанке.

41. Органы публичной власти как субъекты правоотношений по обеспечению кибербезопасности

42. Конфликты в информационной сфере (споры, конфликты, войны) и формы их разрешения.

43. Кредитные организации как субъекты правоотношений по обеспечению кибербезопасности.

44. Государственные информационные ресурсы во всемирной сети: проблемы обеспечения безопасности.

45. Распространение ненадлежащей информации в сети «Интернет»: применение мер ответственности.

46. Проблемы обеспечения безопасности электронных средств массовой информации.

47. Влияние процесса обеспечения кибербезопасности на ограничение свободы СМИ.

48. Цифровая экономика: проблемы и риски.

49. Защита интеллектуальной собственности в сети «Интернет».

50. Принципы, задачи, функции и стандарты обеспечения информационной безопасности в публичном управлении.

51. Доктрина информационной безопасности: обзор основных особенностей.

52. Стратегия построения Информационного общества: проблемы реализации.

53. Обеспечение безопасности детей в сети «Интернет»

54. Анализ правоприменительной практики ограничения доступа к сайтам в сети «Интернет»

55. Глобальное сетевое управление посредством сети «Интернет».

56. Гармонизация национальных и международных стандартов кибербезопасности.

57. Обеспечение безопасности объектов критической информационной инфраструктуры.

58. Защита пользователей сети «Интернет» от киберугроз.

59. Международное сотрудничество в сфере обеспечения кибербезопасности.

Примеры типовых ситуационных заданий

1. Владелец и создатель информационного ресурса в сети «Интернет» на автомобильную тему на своем сайте разместил ссылку на сбор средств для закупки машин повышенной проходимости для незаконных вооруженных формирований.

Законны ли такие действия?

2. В ходе категорирования объекта критической информационной инфраструктуры была допущена ошибка и определена категория ниже требуемой.

Является ли данное деяние правонарушением? Если – да, то кто и какому виду ответственности будет привлечен? Какие возможны риски в случае, если по ошибке будет определена категория выше требуемой?

3. В ходе проверки было установлено, что информационная система федерального органа исполнительной власти использует ресурсы европейского провайдера хостинга.

Является ли выявленный факт нарушением кибербезопасности?

Критерии балльной оценки различных форм текущего контроля успеваемости содержатся в соответствующих методических рекомендациях Департамента международного и публичного права (<http://www.fa.ru/org/dep/dmpp/Pages/Home.aspx>).

7. Фонд оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине

Перечень компетенций, формируемых в процессе освоения дисциплины

Перечень компетенций, формируемых в процессе освоения дисциплины, содержится в разделе 2. «Перечень планируемых результатов освоения образовательной программы (перечень компетенций) с указанием индикаторов их достижения и планируемых результатов обучения по дисциплине».

Перечень примерных контрольных заданий или иных материалов, необходимых для оценки индикаторов достижения компетенций, умений и знаний

для студентов, обучающихся по направлению подготовки

40.03.01. «Юриспруденция» профиль Международное экономическое право (с ч. р. на англ. яз.)

| Наименование компетенции | Наименование индикаторов достижения компетенции | Результаты обучения (умения и знания), соотнесенные с индикаторами достижения компетенции | Типовые контрольные задания |
|--------------------------|---|---|-----------------------------|
| | | | |

| | | | |
|---|---|--|---|
| ПКП-3 Способность участвовать в проведении юридической экспертизы проектов национальных нормативных правовых актов на предмет их соответствия нормам и принципам международного права, а также антикоррупционным стандартам | Индикатор 1. Демонстрирует знание норм национального законодательства о правовых экспертизах, их целях проведения и основных положениях. | Знать: основные положения нормативных правовых актов в области проведения юридической экспертизы проектов национальных нормативных правовых актов на предмет их соответствия нормам и принципам международного права, а также антикоррупционным стандартам. Уметь: ориентироваться в проблематике соответствия национальных правовых актов нормам и принципам международного права, а также антикоррупционным стандартам; владеть категориальным аппаратом; соотносить юридические факты с законодательством; систематизировать необходимый материал с целью проведения экспертизы; | Администрация г. К. в целях обеспечения кибербезопасности своих ресурсов в сети «Интернет» потребовало от разработчиков сайтов руководствоваться Регламентом 2019/881 ЕС при разработке программного обеспечения. Оцените законность решения, принятого администрацией г. К. |
| | Индикатор 2. Обосновывает решения в части поставленной задачи, в целях практической реализации в области международной экономической деятельности. | Знать: основные направления реализации международной экономической деятельности; методы, способы и средства практической реализации в области международной экономической деятельности; особенности применения актов информационного законодательства; возможности использования официальных Интернет-ресурсов Уметь: соотносить юридические факты с законодательством; систематизировать необходимый материал и анализировать практику правоприменения; на основании анализа осуществлять выбор оптимального варианта обоснования решения в части поставленной задачи с учетом фактических обстоятельств | Используя нормы действующего национального и международного законодательства разработайте перечень обязательной к распространению информации, которая должна быть размещена на официальном сайте предприятия осуществляющего международную экономическую деятельность. |
| | Индикатор 3. Проводит юридическую экспертизу проектов национальных нормативных правовых актов на предмет их соответствия нормам и принципам международного права, а также | Знать: основные нормативные акты о противодействии коррупции; сущность и характеристики коррупционных проявлений в различных сферах общественной жизни; способы противодействия различным проявлениям коррупции Уметь: проводить юридическую экспертизу проектов национальных | В сети «Интернет» созданы ресурсы, на которых публикуется информация о фактах взяточничества в различных государственных организациях. Являются ли данные публикации основанием для возбуждения уголовных дел против указанных в |

| | | | |
|--|---|--|--|
| | антикоррупционным стандартам | нормативных правовых актов на предмет их соответствия нормам и принципам международного права, а также антикоррупционным стандартам | публикациях лиц? Как может быть использована данная информация? |
| ПКП-4 Способность давать консультации и квалифицированные юридические заключения по международным экономическим вопросам | Индикатор 1. Проводит юридическое консультирование по международным экономическим вопросам | Знать: основные нормативные акты по международным экономическим вопросам Уметь: проводить юридическое консультирование по международным экономическим вопросам | Обоснуйте почему в РФ не применяется Европейская Конвенция о киберпреступности |
| | Индикатор 2. Оценивает содержание нормативных правовых актов и актов правоприменения на предмет соответствия действующему законодательству в области международных экономических отношений. | Знать: принципы и методы анализа содержания нормативных правовых актов на предмет их соответствия действующему законодательству с использованием справочных правовых систем; Уметь: обрабатывать правовую информацию и аналитические материалы и проводить оценку содержания нормативных правовых актов и актов правоприменения на предмет соответствия действующему законодательству | На предприятии химической промышленности, принадлежащему иностранному гражданину, но расположенному на территории РФ, по указанию владельца не были выполнены требования Приказа ФСТЭК России от 25 декабря 2017 г. № 239. Каким образом обязать владельца, находящегося за рубежом исполнить требования российского законодательства. |
| | Индикатор 3. Дает квалифицированные юридические заключения по международным экономическим вопросам | Знать: основные положения нормативных правовых актов и позиции высших судебных инстанций в области регулирования международных экономических вопросов Уметь: давать квалифицированные юридические заключения по международным экономическим вопросам | Каким образом обязать иностранное юридическое лицо прекратить распространение недостоверной информации, порочащей деловую репутацию российского контрагента. |

*для студентов, обучающихся по направлениям подготовки
40.03.01. «Юриспруденция» профиль Экономическое право*

| Наименование компетенции | Наименование индикаторов достижения компетенции | Результаты обучения (умения и знания), соотнесенные с индикаторами достижения компетенции | Типовые контрольные задания |
|--------------------------|---|---|-----------------------------|
|--------------------------|---|---|-----------------------------|

| | | | |
|---|---|---|--|
| ПКП-1 Способность использовать фундаментальные знания в области частного и публичного права в современных условиях и оказывать помощь в реализации правовых норм субъектам гражданского права | Индикатор 1. Демонстрирует знания нормативно правовых актов, а также прогнозирует результат экономической деятельности для решения практических задач | Знать: основные положения нормативных правовых актов в области обеспечения кибербезопасности; позиции высших судебных инстанций; Уметь: ориентироваться в проблематике обеспечения кибербезопасности и на данной основе прогнозировать результат экономической деятельности; | Возможно ли разместить в сети «Интернет» схему водоснабжения города Смоленска? |
| | Индикатор 2. Использует фундаментальные знания в области частного и публичного права в современных условиях | Знать: фундаментальные частного и публичного права в современных условиях применительно к проблематике кибербезопасности Уметь: соотносить юридические факты с законодательством; систематизировать необходимый материал и анализировать практику правоприменения в информационно правовой сфере; осуществлять выбор оптимального варианта правомерного поведения в информационных правоотношениях с учетом фактических обстоятельств дела | Охарактеризуйте взаимосвязь процессов обеспечения национальной безопасности с обеспечением информационной безопасности и кибербезопасности |
| | Индикатор 3. Оказывает помощь в реализации правовых норм субъектам гражданского оборота | Знать: основные положения нормативных правовых актов в области обеспечения кибербезопасности, угрозы кибербезопасности и правовые меры обеспечения информационной безопасности; Уметь: оказывать помощь в реализации правовых норм для обеспечения кибербезопасности субъектам гражданского оборота | Укажите, с какими государственными органами должен взаимодействовать юрист организации, выполняющий указание руководителя по разработке положения о кибербезопасности предприятия |
| ПКП-2 Способность действовать с учетом кризисных ситуаций в экономике, вызываемых рисками правового и экономического характера, анализировать проблемные ситуации на рынке товаров, работ, услуг, а также выявлять правонарушения при | Индикатор 1. Действует с учетом кризисных ситуаций в экономике, вызываемых рисками правового и экономического характера | Знать: кризисных ситуаций в экономике, вызываемых рисками нарушения кибербезопасности; Уметь: анализировать кризисные ситуации в экономике, вызываемых рисками нарушения кибербезопасности; противодействовать различным проявлениям информационных угроз | Каким образом осуществить взаимодействие в случае обнаружения факта компьютерной атаки на ресурсы субъекта хозяйственной деятельности и как минимизировать причиненный ущерб? |
| | Индикатор 2. Выявляет правонарушения при осуществлении предпринимательской деятельности | Знать: основные направления обеспечения кибербезопасности; требования нормативных правовых актов к субъектам предпринимательской деятельности по обеспечению кибербезопасности; Уметь: выявлять правонарушения в ходе обеспечения кибербезопасности при осуществлении предпринимательской деятельности | Правомерно ли требование, что индивидуальный предприниматель должен: - иметь круглосуточный выход в сеть «Интернет»; - создать официальный электронный адрес и официальный сайт; - обеспечивать кибербезопасность своих |

| | | | |
|--|--|---|--|
| осуществлении предпринимательской деятельности давать юридически обоснованные предложения по их преодолению и устранению | Индикатор 3. Дает юридически обоснованные предложения по преодолению и устранению правонарушений при осуществлении предпринимательской деятельности. | Знать: основные направления правового обеспечения кибербезопасности; Уметь: вырабатывать обоснованные предложения по преодолению и устранению правонарушений при обеспечении кибербезопасности при осуществлении предпринимательской деятельности. | информационных ресурсов. В ходе проверки было установлено, что информационная система российского банка «РоСаБанк» располагается на ресурсах израильского провайдера хостинга. Является ли выявленный факт правонарушением? |
|--|--|---|--|

Примерный перечень вопросов к зачету

1. Понятия Национальная безопасность и Информационная безопасность.
2. Определения киберпространства и кибербезопасности.
3. Необходимость правового регулирования кибербезопасности.
4. Методы обеспечения кибербезопасности.
5. Принципы обеспечения кибербезопасности.
6. Национальная киберинфраструктура.
7. Стратегия развития информационного общества в Российской Федерации.
8. Проблемы формирования понятийного (терминологического) аппарата в области кибербезопасности.
9. Проблемы развития информационной сферы как системообразующего фактора жизни общества.
10. Понятие и виды источников информационного права.
11. Структура, состав и особенности информационного законодательства.
12. Конституционные основы информационного законодательства.
13. Базовый закон информационной сферы.
14. Объекты и субъекты информационных правоотношений.
15. Права и обязанности обладателя информации.
16. Государство как субъект информационных отношений.
17. Правовой статус государственных организаций и учреждений в области обеспечения кибербезопасности.

18. Субъекты кибербезопасности.
19. Киберпреступность.
20. Компьютерные атаки и инциденты.
21. Защита конечных пользователей.
22. Проблемы выявления, идентификации, классификации, оценки угроз информационной безопасности.
23. Научно-технические проблемы развития современных информационных технологий, индустрии средств информатизации, телекоммуникации и связи.
24. Проблемы защиты личности в ходе трансграничного использования информационных технологий.
25. Международные стандарты кибербезопасности.
26. Конвенция о киберпреступности.
27. Cybersecurity Act.
28. Проблемы международно-правового обеспечения кибербезопасности.
29. Кибербезопасность как компонент международных отношений.
30. Правовые гарантии свободы коммуникации.
31. Нормативно правовая база Российской Федерации об обеспечении кибербезопасности.
32. Проблемы разработки Стратегии кибербезопасности Российской Федерации.
33. Государственные (национальные) стандарты РФ и руководящие документы по кибербезопасности.
34. Критерии и методы оценки эффективности систем и средств обеспечения информационной безопасности и кибербезопасности.
35. Мониторинг киберугроз и система реагирования на них
36. Проблемы влияния информационной сферы на конкурентоспособность России на современном этапе.
37. Проблемы оценки информационной безопасности личности, общества и государства.
38. Проблемы развития нормативного правового и нормативного

технического обеспечения кибербезопасности.

39. Понятие критической информационной инфраструктуры.

40. Принципы, задачи, функции и стандарты обеспечения безопасности критической информационной инфраструктуры.

41. ГосСОПКА.

42. Полномочия ФСТЭК, ФСБ и иных государственных органов в сфере обеспечения кибербезопасности.

43. Проблемы нормативного правового обеспечения устойчивости функционирования и безопасности использования информационных систем и телекоммуникационных сетей, в том числе в составе глобальной информационной инфраструктуры.

44. Проблемы противодействия использованию информационных технологий в террористических целях для оказания деструктивного воздействия на элементы критической информационной инфраструктуры.

45. Особенности правового регулирования общественных отношений в сети «Интернет».

46. Актуальные вопросы ограничения доступа к сайтам в сети «Интернет» с информацией, распространяемой с нарушением законодательства РФ.

47. Правовой статус организатора распространения информации в сети "Интернет".

48. Регулирование социальных сетей

49. Особенности распространения информации в сети "Интернет".

50. Особенности распространения информации иностранными субъектами.

51. Понятия киберпреступности, киберпреступления и административного правонарушения в сфере кибербезопасности.

52. Уголовная ответственность за киберпреступления.

53. Административная ответственность за правонарушения в сфере кибербезопасности.

Соответствующие приказы, распоряжения ректората о контроле уровня освоения дисциплин и сформированности компетенций студентов

Приказ от 23.03.2017 № 0557/о «Об утверждении Положения о проведении текущего контроля успеваемости и промежуточной аттестации обучающихся по программам бакалавриата и магистратуры в Финансовом университете».

8. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины

Нормативные акты

1. Конституция Российской Федерации. Принята всенародным голосованием 12.12.1993 (в действ. ред.).
2. Федеральный закон "Об информации, информационных технологиях и о защите информации" от 27.07.2006 № 149-ФЗ (в действ. ред.).
3. Федеральный закона "О персональных данных" от 27.07.2006 № 152-ФЗ (в действ. ред.).
4. Федеральный закон от 26.07.2017 N 187-ФЗ "О безопасности критической информационной инфраструктуры Российской Федерации" (в действ. ред.).
5. Приказ ФСТЭК России от 25.12.2017 N 239 "Об утверждении Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации" (в действ. ред.).
6. Федеральный закон от 28.12.2010 N 390-ФЗ "О безопасности» (в действ. ред.).
7. Указ Президента РФ от 05.12.2016 N 646 "Об утверждении Доктрины информационной безопасности Российской Федерации"
8. Указ Президента РФ от 09.05.2017 N 203 "О Стратегии развития информационного общества в Российской Федерации на 2017 - 2030 годы" (в действ. ред.).
9. УК РФ (в действ. ред.).
10. КоАП РФ (в действ. ред.).

Основная литература:

11. Информационное право : учебник для вузов / М. А. Федотов [и др.] ; под редакцией М. А. Федотова. — Москва: Юрайт, 2021. — 497 с. — (Высшее образование).— Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/469790> (дата обращения: 17.10.2022). — Текст : электронный

12. Степанов, О. А. Противодействие кибертерроризму в цифровую эпоху : монография / О. А. Степанов. — Москва : Юрайт, 2022. — 103 с. — (Актуальные монографии). — ISBN 978-5-534-12775-1. Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/496448> (дата обращения: 17.10.2022). — Текст : электронный

13. Организационное и правовое обеспечение информационной безопасности : учебник и практикум для вузов / под редакцией Т. А. Поляковой, А. А. Стрельцова. — Москва: Юрайт, 2022. — 325 с. — (Высшее образование). — Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/498844> (дата обращения: 17.10.2022). — Текст : электронный

Дополнительная литература:

14. Актуальные проблемы информационного права : учебник / РАН, Ин-т государства и права ; под ред. И. Л. Бачило, М. А. Лапиной. - Москва: Юстиция, 2016. - 534 с. — Текст : непосредственный. Актуальные проблемы информационного права : учебник / под ред. И. Л. Бачило, М. А. Лапиной. — Москва : Юстиция, 2020. — 592 с. — (магистратура, аспирантура). — ЭБС BOOK.ru. - URL: <https://book.ru/book/935207> (дата обращения: 17.10.2022)

15. Жарова, А. К. Правовое регулирование создания и использования информационной инфраструктуры в Российской Федерации : монография / А. К. Жарова. — Москва : Юрайт, 2022. — 301 с. — (Актуальные монографии). — Текст : электронный—Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/496939> (дата обращения: 17.10.2022).

9. Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины:

1. Официальный интернет-портал правовой информации. Государственная система правовой информации: <http://www.pravo.gov.ru>

2. Официальный сайт Совета Безопасности РФ
<http://www.scrf.gov.ru/security/information/>

3. Электронная библиотека Финансового университета (ЭБ) <http://elib.fa.ru/>

4. Электронно-библиотечная система BOOK.RU <http://www.book.ru>

5. Электронно-библиотечная система «Университетская библиотека ОНЛАЙН» <http://biblioclub.ru/>

6. Электронно-библиотечная система Znanium <http://www.znaniy.com>

7. Электронно-библиотечная система издательства «ЮРАЙТ» <https://urait.ru/>

8. Электронно-библиотечная система издательства Проспект
<http://ebs.prospekt.org/books>

9. Электронно-библиотечная система издательства «Лань»
<https://e.lanbook.com/>
10. Электронная библиотека Издательского дома «Гребенников»
<https://grebennikon.ru/>
11. Деловая онлайн-библиотека Alpina Digital <https://finunivers.alpinadigital.ru/>
12. Научная электронная библиотека eLibrary.ru <http://elibrary.ru>
13. Национальная электронная библиотека <http://нэб.пф/>
14. Справочно-правовая система "КонсультантПлюс".
<http://www.library.fa.ru/resource.asp?id=351>
15. Справочно-правовая система по законодательству Российской Федерации "ГАРАНТ" <http://www.library.fa.ru/resource.asp?id=350>

10. Методические указания для обучающихся по освоению дисциплины

| | |
|---|---|
| Об утверждении Методических рекомендаций по планированию и организации внеаудиторной самостоятельной работы студентов по образовательным программам бакалавриата и магистратуры в Финансовом университете | http://www.fa.ru/univer/DocLib/%D0%9E%D1%80%D0%B3%D0%B0%D0%BD%D0%B8%D0%B7%D0%B0%D1%86%D0%B8%D1%8F%20%D1%83%D1%87%D0%B5%D0%B1%D0%BD%D0%BE%D0%B3%D0%BE%20%D0%BF%D1%80%D0%BE%D1%86%D0%B5%D1%81%D1%81%D0%B0%D0%9D%D0%BE%D1%80%D0%BC%D0%B0%D1%82%D0%B8%D0%B2%D0%BD%D1%8B%D0%B5%20%D0%B4%D0%BE%D0%BA%D1%83%D0%BC%D0%B5%D0%BD%D1%82%D1%8B%20%D0%BF%D0%BE%20%D1%81%D0%B0%D0%BC%D0%BE%D1%81%D1%82%D0%BE%D1%8F%D1%82%D0%B5%D0%BB%D1%8C%D0%BD%D0%BE%D0%B9%20%D1%80%D0%B0%D0%B1%D0%BE%D1%82%D0%B5/%D0%9F%D1%80%D0%B8%D0%BA%D0%B0%D0%B7%20%E2%84%96%201040_%D0%BE%20%D0%BE%D1%82%2011.05.2021.PDF |
| Об утверждении Положения о проведении текущего контроля успеваемости и промежуточной аттестации обучающихся по программам бакалавриата и магистратуры в | http://www.fa.ru/univer/DocLib/%D0%9E%D1%80%D0%B3%D0%B0%D0%BD%D0%B8%D0%B7%D0%B0%D1%86%D0%B8%D1%8F%20%D1%83%D1%87%D0%B5%D0%B1%D0%BD%D0%BE%D0%B3%D0%BE%20%D0%BF%D1%80%D0%BE%D1%86%D0%B5%D1%81%D1%81%D0%B0%D0%B1%D1%89%D0%B8%D0%B5%20%D0%BD%D0%BE%D1%80%D0%BC%D0%B0%D1%82%D0%B8%D0%B2%D0%BD%D1%8B%D0%B5%20%D0%B4%D0%BE%D0%BA%D1%83%D0%BC%D0%B5%D0%BD%D1%82%D1%8B%20%D0%BF%D0%BE%20%D1%83%D1%87%D0%B5%D0%B1%D0%BD%D0%BE%D0%B9%20%D1%80%D0%B0%D0%B1%D0%BE%D1%82%D0%B5/%D0%9F%D1%80%D0%B8%D0%BA%D0%B0%D0%B7%20%E2%84%96%201040_%D0%BE%20%D0%BE%D1%82%2011.05.2021.PDF |

| | |
|----------------------------|--|
| Финансовом университете | D1%80%D0%B8%D0%BA%D0%B0%D0%B7%20%E2%84%960557_%D0%BE%20%D0%BE%D1%82%2023.03.2017.pdf |
|----------------------------|--|

1. Дискуссия

Процесс дискуссии можно разделить на три последовательных этапа:

1) В ходе первой стадии обозначается проблема и вырабатывается определенная установка на ее решение. При этом перед студентом стоит задача уяснить проблему и цель дискуссии. К дискуссии необходимо привлекать всех студентов учебной группы. Кроме того, каждый студент должен внимательно выслушивать выступающего, не перебивать, аргументировано подтверждать свою позицию, не повторять сказанного ранее, не допускать личной конфронтации, сохранять беспристрастность, не оценивать выступающих, не выслушав до конца и не поняв позицию.

2) Вторая стадия – стадия оценки – обычно предполагает ситуацию сопоставления, конфронтации и даже конфликта идей, который в случае неумелого руководства дискуссией может перерасти в конфликт личностей. На этой стадии перед преподавателем ставятся следующие задачи:

- начать обмен мнениями;
- собрать максимум мнений, идей, предложений. Выступая со своим мнением, студент может сразу внести свои предложения, а может сначала просто выступить, а позже сформулировать свои предложения.
- не отклоняться от темы;
- оперативно проводить анализ высказанных идей, мнений, позиций, предложений перед тем, как переходить к следующему витку дискуссии.

3) Третья стадия – стадия консолидации – предполагает выработку определенных единых или компромиссных мнений, позиций, решений. На этом этапе осуществляется контролирующая функция. Студенты анализируют и оценивают проведенную дискуссию, подводят итоги, результаты.

Подготовка к дискуссии включает в себя изучение материала, полученного на лекции и дополнительного материала, рекомендованного преподавателем.

2. Проведение занятий с разбором конкретных ситуаций (кейсов), решение практических и ситуационных задач

Case study (кейс-метод, разбор конкретных ситуаций) – это метод активного проблемно-ситуационного анализа, основанный на обучении путем решения конкретных задач-ситуаций (решение кейсов). Представляется, что его использование в семейном праве, с одной стороны, дидактически оправданно, с другой стороны, способствует выработке необходимых компетенций практического характера, учит студентов работать с актами законодательства, применять полученные знания для конкретной жизненной ситуации.

Необходимо подготовить карточки с кейсами, раздать их студентам предварительно разделив их на малые группы. Студенты должны быть заранее предупреждены о такой форме проведения занятия.

При этом кейсы могут основываться как на вымышленных примерах, так и на реальных случаях из практики. Решение кейса должно опираться на правовые нормы действующего законодательства. Кейс не должен быть, с одной стороны, слишком простым, с другой, составленным слишком сложно, требующим для решения значительного количества времени. Целесообразно не только сформулировать ситуацию практического характера, а также поставить перед студентами конкретные вопросы.

Вариант решения обсуждается студентами в группах, по их результатам готовится коллективное заключение, которое озвучивается командами либо сдается преподавателю в краткой письменной форме.

Целесообразно вынести варианты решения, предложенные малыми группами, на обсуждение всего коллектива, дать студентам возможность корректировки ответа с учетом дискуссии в группе.

При решении задач и кейсов, во-первых, следует проанализировать ситуацию, изложенную в задаче, во-вторых, определить, с помощью каких нормативных актов она должна быть решена, в-третьих, обратиться к ним, проанализировать соответствующие положения, в-четвертых, сделать вывод о том, как с их помощью должна быть разрешена ситуация, изложенная в задаче.

3. Методика выполнения Контрольной работы

Контрольная работа представляет собой работу творческого характера, в ходе которой студенту предлагается ответить на теоретический вопрос. Цель выполнения контрольной работы - овладение студентами навыками решения типовых ситуационных задач, формирование учебно-исследовательских навыков, закрепление умений самостоятельно работать с различными источниками информации.

Для выполнения Контрольной работы студенту, во-первых, необходимо определиться с проблемным вопросом в рамках тем дисциплины. Во-вторых, самостоятельно выбрать тематику Контрольной работы из предлагаемого преподавателем перечня. Студент может предложить и свою проблему для решения, но в данном случае тематика Контрольной работы должна быть обязательно согласована с преподавателем. В-третьих, самостоятельно путем анализа изученных научных материалов и нормативных источников, решить выбранную проблему. В-четвертых, правильно с соблюдением требований ГОСТов и юридической техники оформить решение.

Работа выполняется на компьютере (гарнитура Times New Roman, кегль 14) через 1,5 интервала с полями: размер полей – 2,5 см, отступ первой строки абзаца – 1,25. Сноски – постраничные. Должна быть нумерация страниц. Таблицы и рисунки встраиваются в текст работы. На первом листе сверху по центру указывается наименование вуза, название департамента, наименование дисциплины, вариант Контрольной работы, ФИО студента. Листы работы скрепляются скоросшивателем. Объем работы – не более 6 страниц.

При выполнении Контрольной работы рекомендуется руководствоваться Положением о реферате, эссе, контрольной работе, домашнем творческом задании студента по дисциплине (модулю), утвержденным приказом от 01.04.2014 № 611/о.

При оценке Контрольной работы учитывается полнота и глубина раскрытия темы, степень самостоятельности в изложении проблемных вопросов, умение делать выводы, культура оформления контрольной работы (структура, правильное оформление сносок и списка литературы, выверенность текста от опечаток и ошибок и т.д.).

4. Подготовка к зачету

Общие правила проведения экзамена в Финансовом университете определены Положением «О проведении текущего контроля успеваемости и промежуточной аттестации обучающихся Финуниверситета», утвержденным приказом от 23.03.2017 0557/о.

По итогам изучения дисциплины сдается зачет. Зачет проходит в устной форме на последнем семинаре. Студенты набравшие в течение семестра 35 и более баллов, могут получить зачет автоматом».

Оценка на зачете носит дифференцированный характер, выставляется в баллах. Студент отвечает на вопросы преподавателя.

Во время зачета недопустимо совещаться с одногруппниками и использовать шпаргалки и иные средства получения информации, поскольку в этом случае студент удаляется из аудитории с выставлением в ведомость оценки «не зачтено».

Важно помнить, что хорошая, ответственная подготовка, четкое следование настоящим методическим рекомендациям – залог успешной сдачи зачета и получение знаний, которые запомнятся на долгие годы и которым обязательно найдется применение в будущей профессиональной деятельности.

Рекомендации по освоению дисциплины приведены в «Методические рекомендации по планированию и организации внеаудиторной самостоятельной работы по образовательным программам бакалавриата и магистратуры в Финансовом университете» (Приказ ректора № 1040_о от 11.05.2021) и в данной рабочей программе дисциплины.

11. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине, включая перечень необходимого программного обеспечения и информационных справочных систем

11.1 Комплект лицензионного программного обеспечения:

1. Windows, Microsoft Office
2. Антивирус Kaspersky

11.2 Современные профессиональные базы данных и информационные справочные системы:

1. Официальный интернет-портал правовой информации
<http://www.pravo.gov.ru>
2. Справочная правовая система «Консультант Плюс»: <http://www.consultant.ru/>
3. Справочная правовая система «Гарант»: <http://www.garant.ru/>

4. Система комплексного раскрытия информации «СКРИН» -
<http://www.skrin.ru/>

**12. Описание материально-технической базы, необходимой для
осуществления образовательного процесса по дисциплине**

Материально-техническая база, которой располагает Финансовый университет:
аудиторный фонд, компьютерные классы, библиотека Финансового университета
и др.; ПК, Интернет, справочники.