Министерство науки и высшего образования Российской Федерации
Федеральное государственное автономное образовательное учреждение высшего образования
«Самарский государственный экономический университет»

Институт Институт права

Кафедра Организации борьбы с экономическими преступлениями

УТВЕРЖДЕНО
Ученым советом Университета
(протокол №10 от 30 мая 2024 г.)

РАБОЧАЯ ПРОГРАММА

Наименование дисциплины	Б1.В.ДЭ.02.01 Юрисдикция государств в кибер пространстве
Основная профессиональная образовательная программа	40.04.01 Юриспруденция программа Международное публичное и частное право в системе глобальной интеграции

Квалификация (степень) выпускника магистр

Самара 2024

Содержание (рабочая программа)

Стр.

Целью изучения дисциплины является формирование результатов обучения, обеспечивающих достижение планируемых результатов освоения образовательной программы.

1. Место дисциплины в структуре ОП

Дисциплина Юрисдикция государств в кибер пространстве входит в часть, формируемая участниками образовательных отношений (дисциплина по выбору) блока Б1.Дисциплины (модули)

Предшествующие дисциплины по связям компетенций: Международные финансовые отношения, История и методология юридической науки

Последующие дисциплины по связям компетенций: Международные расчетные отношения

2. Планируемые результаты обучения по дисциплине, обеспечивающие достижение планируемых результатов обучения по программе

Изучение дисциплины Юрисдикция государств в кибер пространстве в образовательной программе направлено на формирование у обучающихся следующих компетенций:

Универсальные компетенции (УК):

УК-2 - Способен управлять проектом на всех этапах его жизненного цикла

Планируемые результаты обучения по программе	**Планируемые результаты обучения по дисциплине**		
УК-2	УК-2.1: Знать:	УК-2.2: Уметь:	УК-2.3: Владеть (иметь навыки):
	действующие правовые нормы, влияющие на имеющиеся ресурсы и создавая ограничения	определять круг задач в рамках поставленной цели и выбирать оптимальные способы их решения	навыками разработки оптимальных способов решения поставленных задач, исходя из действующих правовых норм и имеющихся ресурсов

Профессиональные компетенции (ПК):

ПК-7 - Способен принимать участие в проведении юридической экспертизы проектов нормативных правовых актов, в том числе в целях выявления в них положений, способствующих созданию условий для проявления коррупции, давать квалифицированные юридические заключения и консультации в конкретных сферах юридической деятельности

Планируемые результаты обучения по программе	**Планируемые результаты обучения по дисциплине**		
ПК-7	ПК-7.1: Знать:	ПК-7.2: Уметь:	ПК-7.3: Владеть (иметь навыки):
	понятие и виды коррупционного поведения	выявлять признаки коррупционного поведения	навыками оценки коррупционного поведения

3. Объем и виды учебной работы

Учебным планом предусматриваются следующие виды учебной работы по дисциплине:

Заочная форма обучения

Виды учебной работы	Всего час/ з.е.
	Сем 3
Контактная работа, в том числе:	8.15/0.23
Занятия семинарского типа	8/0.22
Индивидуальная контактная работа (ИКР)	0.15/0

Самостоятельная работа:	117.85/3.27
Промежуточная аттестация	18/0.5
Вид промежуточной аттестации: Зачет	Зач
Общая трудоемкость (объем части образовательной программы): Часы Зачетные единицы	144 4

4. Содержание дисциплины

4.1. Разделы, темы дисциплины и виды занятий:

Тематический план дисциплины Юрисдикция государств в кибер пространстве представлен в таблице.

Разделы, темы дисциплины и виды занятий
Заочная форма обучения

№ п/п	Наименование темы (раздела) дисциплины	Контактная работа			Самостоятельная работа	Планируемые результаты обучения в соотношении с результатами обучения по образовательной программе
		Занятия семинарского типа	ИКР	ГКР		
		Практич. занятия				
1.	Основная часть	4			50	УК-2.1, УК-2.2, УК -2.3, ПК-7.1, ПК-7.2, ПК-7.3
2.	Особенная часть	4			67,8	УК-2.1, УК-2.2, УК -2.3, ПК-7.1, ПК-7.2, ПК-7.3
	Контроль	18				
	Итого	**8**	**0.15**		**117.85**	

4.2 Содержание разделов и тем

4.2.1 Контактная работа

Тематика занятий семинарского типа

№п/п	Наименование темы (раздела) дисциплины	Вид занятия семинарского типа**	Тематика занятия семинарского типа
1.	Основная часть	практическое занятие	Правовой статус киберпространства.
		практическое занятие	Территориальный суверенитет и делимитация юрисдикций в киберпространстве
2.	Особенная часть	практическое занятие	Международно-правовая ответственность государств в киберпространстве
		практическое занятие	Кибератака как современная форма совершения акта агрессии

** семинары, практические занятия, практикумы, лабораторные работы, коллоквиумы и иные аналогичные занятия

Иная контактная работа

При проведении учебных занятий СГЭУ обеспечивает развитие у обучающихся навыков командной работы, межличностной коммуникации, принятия решений, лидерских качеств

(включая при необходимости проведение интерактивных лекций, групповых дискуссий, ролевых игр, тренингов, анализ ситуаций и имитационных моделей, преподавание дисциплин (модулей) в форме курсов, составленных на основе результатов научных исследований, проводимых организацией, в том числе с учетом региональных особенностей профессиональной деятельности выпускников и потребностей работодателей).

Формы и методы проведения иной контактной работы приведены в Методических указаниях по основной профессиональной образовательной программе.

4.2.2 Самостоятельная работа

№п/п	Наименование темы (раздела) дисциплины	Вид самостоятельной работы ***
1.	Основная часть	- подготовка доклада - подготовка электронной презентации - тестирование
2.	Особенная часть	- подготовка доклада - подготовка электронной презентации - тестирование

*** самостоятельная работа в семестре, написание курсовых работ, докладов, выполнение контрольных работ

5. Материально-техническое и учебно-методическое обеспечение дисциплины

5.1 Литература:

Основная литература

1. 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, 2023. — 320 с. — (Высшее образование). — ISBN 978-5-534-11783-7. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/515578

Петрова, Г. В. Международное частное право в 2 т. Том 1 : учебник для вузов / Г. В. Петрова. — Москва : Издательство Юрайт, 2023. — 396 с. — (Высшее образование). — ISBN 978-5-534-01932-2. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/512722

Петрова, Г. В. Международное частное право в 2 т. Том 2 : учебник для вузов / Г. В. Петрова. — Москва : Издательство Юрайт, 2023. — 376 с. — (Высшее образование). — ISBN 978-5-534-01938-4. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/512728

Дополнительная литература

1. Кардашова, И. Б. Основы теории национальной безопасности : учебник для вузов / И. Б. Кардашова. — 3-е изд. — Москва : Издательство Юрайт, 2023. — 334 с. — (Высшее образование). — ISBN 978-5-534-15789-5. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/509729

Кефели, И. Ф. Теория мировой политики : учебное пособие для вузов / И. Ф. Кефели, И. Г. Бутырская ; под редакцией И. Ф. Кефели. — 2-е изд., испр. и доп. — Москва : Издательство Юрайт, 2023. — 142 с. — (Высшее образование). — ISBN 978-5-534-06404-9. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/512607

Зенков, А. В. Информационная безопасность и защита информации : учебное пособие для вузов / А. В. Зенков. — 2-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2023. — 107 с. — (Высшее образование). — ISBN 978-5-534-16388-9. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/530927

Литература для самостоятельного изучения

1. Информационная безопасность и защита информации [Текст] : учебное пособие / Ю. Ю. Громов [и др.]. - Старый Оскол : ТНТ, 2013. - 384 с.

2. Калуцкий, И.В. Программно-аппаратные средства защиты информационных систем [Текст] : учебное пособие / И.В. Калуцкий, А.Г. Спеваков ; Юго-Зап. гос. унт. - Курск : ЮЗГУ, 2014. - 179 с.

3. Технологии защиты информации в компьютерных сетях. Межсетевые экраны и интернет-маршрутизаторы [Текст] : учебное пособие / Елена Анатольевна Богданова [и др.]. - М. : Национальный Открытый Университет "ИНТУИТ", 2013. - 743 с.

4. Технические средства и методы защиты информации [Текст] : учебное пособие / Роман Валерьевич Мещеряков [и др.] ; под ред. А. П. Зайцева и А. А. Шелупанова. - М. : Горячая линия-Телеком, 2012. - 616 с.

5.2. Перечень лицензионного программного обеспечения

1. Astra Linux Special Edition «Смоленск», «Орел»; РедОС
2. МойОфис Стандартный 2, МойОфис Образование, Р7-Офис Профессиональный

5.3 Современные профессиональные базы данных, к которым обеспечивается доступ обучающихся

1. Профессиональная база данных «Информационные системы Министерства экономического развития Российской Федерации в сети Интернет» (Портал «Официальная Россия» - http://www.gov.ru/)
2. Государственная система правовой информации «Официальный интернет-портал правовой информации» (http://pravo.gov.ru/)
3. Профессиональная база данных «Финансово-экономические показатели Российской Федерации» (Официальный сайт Министерства финансов РФ - https://www.minfin.ru/ru/)
4. Профессиональная база данных «Официальная статистика» (Официальный сайт Федеральной службы государственной статистики - http://www.gks.ru/

5.4. Информационно-справочные системы, к которым обеспечивается доступ обучающихся

1. Справочно-правовая система «Консультант Плюс»
2. Справочно-правовая система «ГАРАНТ-Максимум»

5.5. Специальные помещения

Учебные аудитории для проведения занятий лекционного типа	Комплекты ученической мебели Мультимедийный проектор Доска Экран
Учебные аудитории для проведения практических занятий (занятий семинарского типа)	Комплекты ученической мебели Мультимедийный проектор Доска Экран Компьютеры с выходом в сеть «Интернет» и ЭИОС СГЭУ
Учебные аудитории для групповых и индивидуальных консультаций	Комплекты ученической мебели Мультимедийный проектор Доска Экран Компьютеры с выходом в сеть «Интернет» и ЭИОС СГЭУ
Учебные аудитории для текущего контроля и промежуточной аттестации	Комплекты ученической мебели Мультимедийный проектор Доска Экран Компьютеры с выходом в сеть «Интернет» и ЭИОС СГЭУ
Помещения для самостоятельной работы	Комплекты ученической мебели Мультимедийный проектор Доска Экран Компьютеры с выходом в сеть «Интернет» и ЭИОС СГЭУ
Помещения для хранения и	Комплекты специализированной мебели для

профилактического обслуживания оборудования	хранения оборудования

5.6 Лаборатории и лабораторное оборудование

6. Фонд оценочных средств по дисциплине Юрисдикция государств в кибер пространстве:

6.1. Контрольные мероприятия по дисциплине

Вид контроля	**Форма контроля**	**Отметить нужное знаком « + »**
Текущий контроль	Оценка докладов	+
	Устный/письменный опрос	+
	Тестирование	+
	Практические задачи	+
	Оценка контрольных работ (для заочной формы обучения)	+
Промежуточный контроль	Зачет	+

Порядок проведения мероприятий текущего и промежуточного контроля определяется Методическими указаниями по основной профессиональной образовательной программе высшего образования; Положением о балльно-рейтинговой системе оценки успеваемости обучающихся по основным образовательным программам высшего образования – программам бакалавриата, программам специалитета, программам магистратуры в федеральном государственном автономном образовательном учреждении высшего образования «Самарский государственный экономический университет».

6.2. Планируемые результаты обучения по дисциплине, обеспечивающие достижение планируемых результатов обучения по программе

Универсальные компетенции (УК):

УК-2 - Способен управлять проектом на всех этапах его жизненного цикла

Планируемые результаты обучения по программе	**Планируемые результаты обучения по дисциплине**		
	УК-2.1: Знать:	УК-2.2: Уметь:	УК-2.3: Владеть (иметь навыки):
	действующие правовые нормы, влияющие на имеющиеся ресурсы и создавая ограничения	определять круг задач в рамках поставленной цели и выбирать оптимальные способы их решения	навыками разработки оптимальных способов решения поставленных задач, исходя из действующих правовых норм и имеющихся ресурсов
Пороговый	действующие правовые нормы	определять круг задач в рамках поставленной цели	навыками разработки оптимальных способов решения поставленных задач
Стандартный (в дополнение к пороговому)	действующие правовые нормы, влияющие на имеющиеся ресурсы и создавая ограничения	определять круг задач в рамках поставленной цели и выбирать оптимальные способы их решения	навыками разработки оптимальных способов решения поставленных задач, исходя из действующих правовых

			норм и имеющихся ресурсов
Повышенный (в дополнение к пороговому, стандартному)	действующие правовые нормы, влияющие на имеющиеся ресурсы и создавая ограничения, способен их анализировать	определять круг задач в рамках поставленной цели и выбирать оптимальные способы их решения, учитывая особенности проблемы	навыками разработки оптимальных способов решения поставленных задач, исходя из действующих правовых норм и имеющихся ресурсов, учитывая особенности поставленной проблемы

Профессиональные компетенции (ПК):

ПК-7 - Способен принимать участие в проведении юридической экспертизы проектов нормативных правовых актов, в том числе в целях выявления в них положений, способствующих созданию условий для проявления коррупции, давать квалифицированные юридические заключения и консультации в конкретных сферах юридической деятельности

Планируемые результаты обучения по программе	**Планируемые результаты обучения по дисциплине**		
	ПК-7.1: Знать:	ПК-7.2: Уметь:	ПК-7.3: Владеть (иметь навыки):
	понятие и виды коррупционного поведения	выявлять признаки коррупционного поведения	навыками оценки коррупционного поведения
Пороговый	систему юридических документов	анализировать систему юридических документов	приемами систематизации юридических документов
Стандартный (в дополнение к пороговому)	систему юридических документов; приемы подготовки юридических документов;	анализировать систему юридических документов; - самостоятельно разрабатывать юридические документы;	приемами систематизации юридических документов; - навыками самостоятельной подготовки юридических документов;
Повышенный (в дополнение к пороговому, стандартному)	систему юридических документов; приемы подготовки юридических документов; требования к документообороту в профессиональной деятельности	анализировать систему юридических документов; - самостоятельно разрабатывать юридические документы; - оценивать процессы документооборота в профессиональной деятельности	приемами систематизации юридических документов; - навыками самостоятельной подготовки юридических документов; - самостоятельной организации документооборота в профессиональной деятельности

6.3. Паспорт оценочных материалов

№ п/п	**Наименование темы (раздела) дисциплины**	**Контролируемые планируемые результаты обучения в соотношении с результатами обучения по**	**Вид контроля/используемые оценочные средства**	
			Текущий	**Промежуточный**

		программе		
1.	Общая часть	УК-2.1, УК-2.2, УК- 2.3, ПК-7.1, ПК-7.2, ПК-7.3	Оценка докладов Проведение устных (письменных) Опросов Эссе Коллоквиум	Оценка докладов Проведение устных (письменных) Опросов Эссе Коллоквиум
2.	Особенная часть	УК-2.1, УК-2.2, УК- 2.3, ПК-7.1, ПК-7.2, ПК-7.3	Оценка докладов Проведение устных (письменных) Опросов Эссе Коллоквиум	Оценка докладов Проведение устных (письменных) Опросов Эссе Коллоквиум

6.4.Оценочные материалы для текущего контроля

https://lms2.sseu.ru/course/index.php?categoryid=1930

Примерная тематика докладов

Раздел дисциплины	**Темы**
Общая часть	1.Политика адмимнистрации Б. Обамы в области обеспечения информационной безопасности. 2.Европейская политика информационной безопасности. 3.Взаимодействие государств в области информационной безопасности в Азиатско-Тихоокеанском регионе. 4. Информационная преступность: Уголовноправовые и криминалистические аспекты. 5. Правовые проблемы оборота «больших данных» в условиях цифровой экономики. 6. Защита прав человека в Интернете.
Особенная часть	7. Кибербезопасность и кибервойна. 8. Правовой статус киберпространства. 9. Национальное информационное законодательство как отражение вызовов времени. 10. Судебная власть в условиях новой информационной реальности. 11. Неприкосновенность частной жизни и информационные технологии. 12. Практика Европейского Суда по правам человека по делам, затрагивающим использование новых технологий.

Вопросы для устного/письменного опроса

Раздел дисциплины	**Вопросы**

Задания для тестирования по дисциплине для оценки сформированности компетенций (min 20, max 50 + ссылку на ЭИОС с тестами)

Как называется умышленно искаженная информация?

+ Дезинформация

- Информативный поток

- Достоверная информация

- Перестает быть информацией
2.Как называется информация, к которой ограничен доступ?
+ Конфиденциальная
- Противозаконная
- Открытая
- Недоступная
3.Какими путями может быть получена информация?
+ проведением, покупкой и противоправным добыванием информации научных исследований
- захватом и взломом ПК информации научных исследований
- добыванием информации из внешних источников и скремблированием информации научных исследовании
- захватом и взломом защитной системы для информации научных исследований
4.Основной документ, на основе которого проводится политика информационной безопасности?
+ программа информационной безопасности
- регламент информационной безопасности
- политическая информационная безопасность
- Протекторат
5.В зависимости от формы представления информация может быть разделена на?
+ Речевую, документированную и телекоммуникационную
- Мысль, слово и речь
- цифровая, звуковая и тайная
- цифровая, звуковая
6.К каким процессам относят процессы сбора, обработки, накопления, хранения, поиска и распространения информации
+ Информационным процессам
- Мыслительным процессам
- Машинным процессам
- Микропроцессам
7.Что называют защитой информации?
+ Все ответы верны
- Называют деятельность по предотвращению утечки защищаемой информации
- Называют деятельность по предотвращению несанкционированных воздействий на защищаемую информацию
- Называют деятельность по предотвращению непреднамеренных воздействий на защищаемую информацию
8.Под непреднамеренным воздействием на защищаемую информацию понимают?
+ Воздействие на нее из-за ошибок пользователя, сбоя технических или программных средств и воздействие природных явлений
- Процесс ее преобразования, при котором содержание информации изменяется на ложную
- Возможности ее преобразования, при котором содержание информации изменяется на ложную информацию
- Не ограничения доступа в отдельные отрасли экономики или на конкретные производства
9.Функция защиты информационной системы, гарантирующая то, что доступ к информации, хранящейся в системе может быть осуществлен только тем лицам, которые на это имеют право
- управление доступом
+ конфиденциальность
- аутентичность
- целостность

- доступность
10.Основные предметные направления Защиты Информации?
+ охрана государственной, коммерческой, служебной, банковской тайн, персональных данных и интеллектуальной собственности
- Охрана золотого фонда страны
- Определение ценности информации
- Усовершенствование скорости передачи информации
11.Государственная тайна это
+ защищаемые государством сведения в области его военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб безопасности страны
- ограничения доступа в отдельные отрасли экономики или на конкретные производства
- защищаемые банками и иными кредитными организациями сведения о банковских операциях
- защищаемая по закону информация, доверенная или ставшая известной лицу (держателю) исключительно в силу исполнения им своих профессиональных обязанностей
12.Меры по защите информации от неавторизованного доступа, разрушения, модификации, раскрытия и задержек в доступе
+ Информационная безопасность
- Защитные технологии
- Заземление
- Конфиденциальность
13.Можно выделить следующие направления мер информационной безопасности
- Правовые
- Организационные
+ Все ответы верны
- Технические
14.Что можно отнести к правовым мерам ИБ?
+ Разработку норм, устанавливающих ответственность за компьютерные преступления, защиту авторских прав программистов, совершенствование уголовного и гражданского законодательства, а также судопроизводства
- охрану вычислительного центра, тщательный подбор персонала, исключение случаев ведения особо важных работ только одним человеком, наличие плана восстановления работоспособности центра итд
- Защиту от несанкционированного доступа к системе, резервирование особо важных компьютерных подсистем, организацию вычислительных сетей с возможностью перераспределения ресурсов в случае нарушения работоспособности отдельных звеньев, установку оборудования обнаружения и тушения пожара, оборудования обнаружения воды, принятие конструкционных мер защиты от хищений, саботажа, диверсий, взрывов, установку резервных систем электропитания, оснащение помещений замками, установку сигнализации и многое другое
- охрану вычислительного центра, установку сигнализации и многое другое
15.Что можно отнести к организационным мерам ИБ?
- Разработку норм, устанавливающих ответственность за компьютерные преступления, защиту авторских прав программистов, совершенствование уголовного и гражданского законодательства, а также судопроизводства.
+ Охрану вычислительного центра, тщательный подбор персонала, исключение случаев ведения особо важных работ только одним человеком, наличие плана восстановления работоспособности центра и т.д.
- Защиту от несанкционированного доступа к системе, резервирование особо важных компьютерных подсистем.
- Охрану работоспособности отдельных звеньев и организацию

вычислительных сетей с возможностью перераспределения ресурсов.
- Принятие конструкционных мер защиты от хищений, саботажа, диверсий, взрывов, установку резервных систем электропитания, оснащение помещений замками, установку сигнализации и многое другое.
16.Что можно отнести к техническим мерам ИБ?
- Разработку норм, устанавливающих ответственность за компьютерные преступления, защиту авторских прав программистов, совершенствование уголовного и гражданского законодательства, а также судопроизводства
- Охрану вычислительного центра, тщательный подбор персонала, исключение случаев ведения особо важных работ только одним человеком, наличие плана восстановления работоспособности центра и т.д.
+ Защиту от несанкционированного доступа к системе, резервирование особо важных компьютерных подсистем, организацию вычислительных сетей с возможностью перераспределения ресурсов в случае нарушения работоспособности отдельных звеньев и многое другое
- Простые и доступные меры защиты от хищений, саботажа, диверсий, взрывов
- В административных местах установку резервных систем электропитания, оснащение помещений замками, установку сигнализации и многое другое.
17.Обеспечение достоверности и полноты информации и методов ее обработки.
- Конфиденциальность
+ Целостность
- Доступность
- Целесообразность
18.Обеспечение доступа к информации только авторизованным пользователям?
+ Конфиденциальность
- Целостность
- Доступность
- Целесообразность
19.Целью информационной безопасности является?
+ все перечисленное
- обезопасить ценности системы
- защитить и гарантировать точность и целостность информации
- минимизировать разрушения
20.Укажите направления мер информационной безопасности.
+правовые, организационные, технические
-правовые, аппаратные, программные
-личные, организационные
-технические
21.Что такое Информационная безопасность?
+ меры по защите информации от неавторизованного доступа
-меры по защите ПК
-безопасность личной информации
-все перечисленное
22. Основные принципы вхождения государств в информационное общество провозглашены в:
а) Федеральном законе «Об информации, информационных технологиях и защите информации»;
+б) Окинавской хартии глобального информационного общества;
в) Государственной программе Кировской области «Информационное общество»;
г) Доктрине информационной безопасности Российской Федерации.
23. Целями перехода России к информационному обществу являются:
+а) преодоление информационного неравенства и равноправное вхождение в глобальное информационное общество;

б) мировое информационное господство;
в) развитие гражданского общества и демократических традиций;
+г) обеспечение прав человека на свободный доступ к информации и защиту персональных данных.
24.Задачами государственной информационной политики являются:
а) совершенствование правовой системы;
+б) формирование единого информационного пространства России;
+в) обеспечение информационной безопасности личности, общества и государства;
.+г) вхождение России в мировое информационное пространство
25. Для удостоверения интернет-страниц для последующего предоставления документов в суд следует обратиться:
а) к системному администратору;
+б) к провайдеру или оператору информационной системы;
в) к нотариусу;
г) в канцелярию суда
26. Понятие информационной системы закреплено в:
а) Конституции РФ;
+б) Федеральном законе Российской Федерации от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;
в) Доктрине информационной безопасности РФ, утвержденная Указом Президента РФ 9 сентября 2000 года.

Практические задачи (min 20, max 50 + ссылку на ЭИОС с электронным изданием, если имеется)

Раздел дисциплины	Задачи

Тематика контрольных работ

Раздел дисциплины	Темы

6.5. Оценочные материалы для промежуточной аттестации

Фонд вопросов для проведения промежуточного контроля в форме зачета

Раздел дисциплины	Вопросы
Общая часть	1.Государственный суверенитет Российской Федерации в информационно-телекоммуникационной сети «Интернет». 2.Территориальный аспект юрисдикции и суверенитета государства в киберпространстве. 3. Территориальный суверенитет и делимитация юрисдикций в киберпространстве. 4. Международно-правовая ответственность государств в киберпространстве. 5. Международное сотрудничество государств в сфере информационной безопасности и правовые подходы к его регулированию. 6. К вопросу о международно-правовой концепции угроз международной информационной безопасности. 7.Деятельность ООН в области информации и международные аспекты информационной безопасности России. 8.Современные аспекты кибербезопасности в мире в контексте глобальных угроз. 9.Международное сотрудничество государств в сфере информационной

	безопасности и правовые подходы к его урегулированию. 10.Виртуальная реальность: концепция угроз информационной безопасности США и ее международная составляющая
Особенная часть	11.Управление процессами обеспечения кибербезопасности как фактор международной стабильности. 12.Угрозы международной информационной безопасности: формирование концептуальных подходов. 13.Глобальные военно-политические проблемы международной информационной безопасности: тенденции, угрозы, перспективы. 14.Международно-правовая регламентация киберпреступности. 15. Кибератака как современная форма совершения акта агрессии. 16.Современные аспекты кибербезопасности в мире в контексте глобальных угроз. 17.Киберсредства ведения войны: проблемы международно-правового регулирования. 18.Перспективные тенденции формирования международного режима по обеспечению информационной безопасности. 19.Новый приоритет для российской публичной дипломатии: предотвращение кибератак на объекты критической инфраструктуры. 20.Правовые аспекты обеспечения кибербезопасности критической инфраструктуры Российской Федерации.

6.6. Шкалы и критерии оценивания по формам текущего контроля и промежуточной аттестации

Шкала и критерии оценивания

Оценка	**Критерии оценивания для мероприятий контроля с применением 2-х балльной системы**
«зачтено»	УК-2, ПК-7
«не зачтено»	Результаты обучения не сформированы на пороговом уровне