МИНОБРНАУКИ РОССИИ
федеральное государственное бюджетное образовательное учреждение
высшего образования
«ИРКУТСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»
ФГБОУ ВО «ИГУ»
Кафедра политологии, истории и регионоведения

УТВЕРЖДАЮ
Декан исторического факультета
_____ Е. А. Матвеева
«17» апреля 2024 г.

Рабочая программа дисциплины (модуля)

Б1.В.ДВ.02.02 Политика обеспечения информационной безопасности в зарубежных государствах

Направление подготовки: 41.03.04 Политология

Направленность (профиль) подготовки: Политология

Квалификация выпускника – БАКАЛАВР

Форма обучения: очная
программа реализуется с использованием электронного обучения, дистанционных образовательных технологий (частично)

Согласовано с УМК
исторического факультета
Протокол № 5 от «16» апреля 2024 г.

Председатель _____Е. А. Матвеева

Рекомендовано
кафедрой политологии, истории и регионоведения ИГУ
Протокол № 6 от «01» апреля 2024 г.

Зав. кафедрой _____ Ю.А. Зуляр

Иркутск 2024 г.

Содержание

I. ЦЕЛИ И ЗАДАЧИ ДИСЦИПЛИНЫ (МОДУЛЯ):

Цели:

Основной целью освоения дисциплины Б1.В.ДВ.02.02 «Политика обеспечения информационной безопасности в зарубежных государствах» является ознакомление студентов бакалавров, обучающихся по направлению 41.03.04 «Политология», с политологическими подходами и современными тенденциями в оценке значения проблемы информационной безопасности в зарубежных государствах в XXI веке. Курс позволяет определить место информационной безопасности в системе национальной безопасности зарубежных государств, а также особенности и основные тенденции трансформации их национальной безопасности в связи с всеобщей информатизацией, революцией в военном деле и формированием информационного общества, а также влиянием этих тенденций на внешнюю политику зарубежных государств. В результате усвоения дисциплины у студентов должны сформироваться знания об основных категориях и понятиях международной информационной безопасности в зарубежных государствах, а также о современных методах и методиках исследования политических явлений и процессов.

Задачи:

Основными задачами учебной дисциплины Б1.В.ДВ.02.02 «Политика обеспечения информационной безопасности в зарубежных государствах» является знакомство студентов с объектом и предметом, категориальным аппаратом, основными теоретическими и практическими проблемами национальной политики зарубежных государств в области обеспечения международной информационной безопасности, а также формирование анализа политической информации, выявления основных тенденций развития мировых политических процессов в сфере обеспечения информационной безопасности в зарубежных государствах.

Более конкретно, задачами дисциплины являются:

- определение места и роли обеспечения информационной безопасности в общей системе национальной безопасности зарубежных государств;
- изучение основных понятий и категорий информационной безопасности;
– анализ основных тенденций и трендов политического процесса в сфере национальной информационной безопасности зарубежных государств;
– анализ современных вызовов и угроз национальным интересам зарубежных государств в сфере информатизации и развитию цифрового общества;
- определение места и роли зарубежных государств в мировом политическом процессе по вопросу обеспечения информационной безопасности.

II. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП ВО

2.1. Дисциплина Б1.В.ДВ.02.02 «Политика обеспечения информационной безопасности в зарубежных государствах» относится к части элективных дисциплин. Дисциплина изучается в 7 семестре на 4 курсе.

2.2. Для изучения данной учебной дисциплины (модуля) необходимы знания, умения и навыки, формируемые предшествующими дисциплинами: Б1.В.03 «Политика обеспечения информационной безопасности», Б1.В.04 «Мировая политика и международные отношения», Б1.О.12 «Информационно-аналитическая деятельность во внутренней и внешней политике», Б1.О.22 «Введение в политическую теорию», Б1.О.05 «Иностранный язык», Б1.О.13 «Процесс принятия политических решений», Б1.О.14 «Политический анализ и прогнозирование», Б1.О.20 «Сравнительная политология», Б1.О.22 «Введение в политическую теорию», Б1.В.02 «Политическая конфликтология»,

Б1.В.13 «Политическая история зарубежных стран», Б1.О.17 «Информационно-коммуникационные технологии».

2.3. Перечень последующих учебных дисциплин, для которых необходимы знания, умения и навыки, формируемые данной учебной дисциплиной: *подготовка ВКР*

III. ТРЕБОВАНИЯ К РЕЗУЛЬТАТАМ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Процесс освоения дисциплины направлен на формирование компетенций (элементов следующих компетенций) в соответствии с ФГОС ВО и ОП ВО по данному направлению подготовки (специальности) 41.03.04 Политология:

Перечень планируемых результатов обучения по дисциплине (модулю), соотнесенных с индикаторами достижения компетенций

Компетенция	Индикаторы компетенций	Результаты обучения
ПК-5 Владеет методами разрешения политических конфликтов, организации политической социализации молодежи, политической мобилизации масс, с использованием технологий и каналов массовой коммуникации и средств массовой информации	ИДК ПК 5.1 Собирает, обрабатывает, анализирует, интерпретирует документальные, печатные, телевизионные и ИНТЕРНЕТ-источники с целью формирования взгляда на существующую в регионе социально-политическую ситуацию	Знать: сущность, значение, основные положения и перспективы развития международных процессов в сфере обеспечения информационной безопасности Уметь: объяснять содержание направлений обеспечения информационной безопасности, обосновывать содержание национальных интересов Российской Федерации в информационной сфере на международном уровне; выявлять правовые средства, используемые для обеспечения информационной безопасности на мировой арене. Владеть: методами и навыками анализа документов по вопросам обеспечения международной информационной безопасности, основных источников права в области обеспечения информационной безопасности.
	ИДК ПК 5.2 Определяет стадии реально существующих политических конфликтов в онлайн и киберпространстве, в том числе прямо или косвенно связанных с национальными проблемами, предлагает пути их разрешения	Знать: систему обеспечения информационной безопасности; Уметь: анализировать условия и средства обеспечения информационной безопасности; Владеть: методами и навыками и реализации государственной международной политики в сфере обеспечения информационной безопасности.

IV. СОДЕРЖАНИЕ И СТРУКТУРА ДИСЦИПЛИНЫ

Объем дисциплины составляет 4 зачетных единицы, 144 часа
Из них реализуется с использованием электронного обучения и дистанционных образовательных технологий 28 часов
Из них 0 часов – практическая подготовка (указать при наличии)
Форма промежуточной аттестации: зачет

4.1 Содержание дисциплины, структурированное по темам, с указанием видов учебных занятий и отведенного на них количества академических часов

№ п/п	Раздел дисциплины/темы	Семестр	Всего часов	Из них практическая подготовка обучающихся	Виды учебной работы, включая самостоятельную работу обучающихся и трудоемкость (в часах)				Формы текущего контроля успеваемости; Форма промежуточной аттестации *(по семестрам)*
					Контактная работа преподавателя с обучающимися			Самостоятельная работа (в том числе внеаудиторная СР/КСР)	
					Лекции	Семинарские (практические занятия)	Из них практическая	Консультации/КО	
1	**Современное информационное общество**	7						2	

№ п/п	Раздел дисциплины/темы	Семестр	Всего часов	Из них практическая подготовка обучающихся	Виды учебной работы, включая самостоятельную работу обучающихся и трудоемкость (в часах)				Формы текущего контроля успеваемости; Форма промежуточной аттестации *(по семестрам)*
						Контактная работа преподавателя с обучающимися		Самостоятельная работа (в том числе внеаудиторная СР/КСР)	
1.1	Понятие информационного общества. Основные вехи формирования информационного общества.	7			1	2		7	Выступление на семинарском занятии, сообщение с презентацией, участие в дискуссии, контрольная работа, зачет
1.2	Основные характеристики современного информационного общества	7			1	2		7	Выступление на семинарском занятии, сообщение с презентацией, участие в дискуссии, контрольная работа, зачет
2	**Международная информационная безопасность: общие характеристики**	7					0,5	2	
2.1	Понятие международной информационной безопасности	7			1	2		7	Выступление на семинарском занятии, сообщение с презентацией, участие в дискуссии, контрольная работа, зачет
2.2	Вызовы и угрозы международной информационной безопасности	7			2	2		7	Выступление на семинарском занятии, сообщение с презентацией, участие в дискуссии, контрольная работа, зачет
2.3	Информационные войны и информационные конфликты	7			2	4		7	Выступление на семинарском занятии, сообщение с презентацией, участие в дискуссии, контрольная работа, зачет
2.4	Информационный терроризм и информационная преступность	7			1	2		7	Выступление на семинарском занятии, сообщение с презентацией, участие в дискуссии, контрольная работа, зачет
3	**Подходы к обеспечению информационной**	7						2	

№ п/п	Раздел дисциплины/темы	Семестр	Всего часов	Из них практическая подготовка обучающихся	Виды учебной работы, включая самостоятельную работу обучающихся и трудоемкость (в часах)				Формы текущего контроля успеваемости; Форма промежуточной аттестации *(по семестрам)*
						Контактная работа преподавателя с обучающимися		Самостоятельная работа (в том числе внеаудиторная СР/КСР)	
	безопасности в зарубежных государствах						0,5		
3.1	Политика обеспечения информационной безопасности в США	7			2	4		7	Выступление на семинарском занятии, сообщение с презентацией, участие в дискуссии, контрольная работа, зачет
3.2	Политика обеспечения информационной безопасности в КНР	7			2	4		7	Выступление на семинарском занятии, сообщение с презентацией, участие в дискуссии, контрольная работа, зачет
3.3	Политика обеспечения информационной безопасности в США в странах Европейского Союза	7			2	4		7	Выступление на семинарском занятии, сообщение с презентацией, участие в дискуссии, контрольная работа, зачет
3.4	Политика обеспечения информационной безопасности в странах Ближнего Востока	7			2	4		7	Выступление на семинарском занятии, сообщение с презентацией, участие в дискуссии, контрольная работа, зачет
3.5	Политика обеспечения информационной безопасности в США в странах Азиатско-Тихоокеанского региона	7			2	4		7	Выступление на семинарском занятии, сообщение с презентацией, участие в дискуссии, контрольная работа, зачет
	Зачет						8		
Итого часов			144		**18**	**34**	**1/8**	**77/6**	

4.2 План внеаудиторной самостоятельной работы обучающихся по дисциплине

Семестр	Название раздела, темы	Самостоятельная работа обучающихся			Оценочное средство	Учебно-методическое обеспечение самостоятельной работы
		Вид самостоятельной работы	Сроки выполнения	Затраты времени (час.)		
7	Понятие информационного общества. Основные вехи формирования информационного общества. Основные характеристики современного информационного общества	Изучение учебной, научной литературы с привлечением электронных средств официальной, статистической и научной информации Подготовка к выступлениям на семинаре Подготовка презентации	сентябрь	7/7	Выступление на семинарском занятии, сообщение с презентацией, участие в дискуссии, контрольная работа	Инновационные направления современных международных отношений : учеб. пособие для студ. гуманитар. вузов и фак. / ред.: А. В. Крутских, А. В. Бирюков. - М. : Аспект Пресс, 2010. - 295 с. ; 22 см. - Библиогр. в конце глав. - ISBN 978-5-7567-0562-1 : 340.33 р., 270.00 р. Экземпляры всего: 11; Информационные вызовы национальной и международной безопасности : монография / И. Ю. Алексеева, И. В. Авчаров, А. В. Бедрицкий и др.]; под общ. ред. А. В. Федорова и В. Н. Цыгичко; ПИР-центр. - М. : ПИР-Центр полит. исслед., 2001. - 327 с.; 20 см. - (Библиотека ПИР-Центра).; ISBN 5-94013-006-2. Режим доступа: http://www.pircenter.org/media/content/files/9/13464042510.pdf; Базы данных, информационно-справочные и поисковые системы Интернета.

Семестр	Название раздела, темы	Самостоятельная работа обучающихся			Оценочное средство	Учебно-методическое обеспечение самостоятельной работы
		Вид самостоятельной работы	Сроки выполнения	Затраты времени (час.)		
7	Понятие международной информационной безопасности	Изучение учебной, научной литературы с привлечением электронных средств официальной, статистической и научной информации Подготовка к выступлениям на семинаре Подготовка презентации	октябрь	7	Выступление на семинарском занятии, сообщение с презентацией, участие в дискуссии, контрольная работа	Федоров А. В. Информационная безопасность в мировом политическом процессе : учеб. пособие / А. В. Федоров ; Московский гос. ин-т междунар. отношений (ун-т) МИД РФ. - М. : Изд-во МГИМО (Университет), 2006. - 219 с. ; 20 см. - ISBN 5-9228-0263-1 : 258.72 р. Экземпляры всего: 1; Угрозы информационной безопасности в кризисах и конфликтах XXI века : монография / под ред. А. В. Загорского, Н. П. Ромашкиной. - М. : ИМЭМО РАН, 2015. - 151 с. Режим доступа: https://www.imemo.ru/files/File/ru/publ/2015/2015_027.pdf; Проблемы информационной безопасности в международных военно-политических отношениях: монография / под ред. А. В. Загорского, Н. П. Ромашкиной. М. : ИМЭМО РАН, 2016, 183 с. Режим доступа: https://www.imemo.ru/files/File/ru/publ/2016/2016_037.pdf; Базы данных, информационно-справочные и поисковые системы Интернета.

Семестр	Название раздела, темы	Самостоятельная работа обучающихся			Оценочное средство	Учебно-методическое обеспечение самостоятельной работы
		Вид самостоятельной работы	Сроки выполнения	Затраты времени (час.)		
7	Вызовы и угрозы международной информационной безопасности	Изучение учебной, научной литературы с привлечением электронных средств официальной, статистической и научной информации Подготовка к выступлениям на семинаре Подготовка презентации	октябрь	7	Выступление на семинарском занятии, сообщение с презентацией, участие в дискуссии, контрольная работа	Угрозы информационной безопасности в кризисах и конфликтах XXI века : монография / под ред. А. В. Загорского, Н. П. Ромашкиной. - М. : ИМЭМО РАН, 2015. - 151 с. Режим доступа: https://www.imemo.ru/files/File/ru/publ/2015/2015_027.pdf; Проблемы информационной безопасности в международных военно-политических отношениях: монография / под ред. А. В. Загорского, Н. П. Ромашкиной. М. : ИМЭМО РАН, 2016, 183 с. Режим доступа: https://www.imemo.ru/files/File/ru/publ/2016/2016_037.pdf; Базы данных, информационно-справочные и поисковые системы Интернета.

Семестр	Название раздела, темы	Самостоятельная работа обучающихся			Оценочное средство	Учебно-методическое обеспечение самостоятельной работы
		Вид самостоятельной работы	Сроки выполнения	Затраты времени (час.)		
7	Информационные войны и информационные конфликты	Изучение учебной, научной литературы с привлечением электронных средств официальной, статистической и научной информации Подготовка к выступлениям на семинаре Подготовка презентации	октябрь	7	Выступление на семинарском занятии, сообщение с презентацией, участие в дискуссии, контрольная работа	Угрозы информационной безопасности в кризисах и конфликтах XXI века : монография / под ред. А. В. Загорского, Н. П. Ромашкиной. - М. : ИМЭМО РАН, 2015. - 151 с. Режим доступа: https://www.imemo.ru/files/File/ru/publ/2015/2015_027.pdf; Проблемы информационной безопасности в международных военно-политических отношениях: монография / под ред. А. В. Загорского, Н. П. Ромашкиной. М. : ИМЭМО РАН, 2016, 183 с. Режим доступа: https://www.imemo.ru/files/File/ru/publ/2016/2016_037.pdf; Базы данных, информационно-справочные и поисковые системы Интернета.

Семестр	Название раздела, темы	Самостоятельная работа обучающихся			Оценочное средство	Учебно-методическое обеспечение самостоятельной работы
		Вид самостоятельной работы	Сроки выполнения	Затраты времени (час.)		
	Информационный терроризм и информационная преступность	Изучение учебной, научной литературы с привлечением электронных средств официальной, статистической и научной информации Подготовка к выступлениям на семинаре Подготовка презентации	ноябрь	7	Выступление на семинарском занятии, сообщение с презентацией, участие в дискуссии, контрольная работа	Угрозы информационной безопасности в кризисах и конфликтах XXI века : монография / под ред. А. В. Загорского, Н. П. Ромашкиной. - М. : ИМЭМО РАН, 2015. - 151 с. Режим доступа: https://www.imemo.ru/files/File/ru/publ/2015/2015_027.pdf; Проблемы информационной безопасности в международных военно-политических отношениях: монография / под ред. А. В. Загорского, Н. П. Ромашкиной. М. : ИМЭМО РАН, 2016, 183 с. Режим доступа: https://www.imemo.ru/files/File/ru/publ/2016/2016_037.pdf; Базы данных, информационно-справочные и поисковые системы Интернета.
	Политика обеспечения информационной безопасности в США	Изучение учебной, научной литературы с привлечением электронных средств официальной, статистической и научной информации Подготовка к выступлениям на семинаре Подготовка презентации	ноябрь	7	Выступление на семинарском занятии, сообщение с презентацией, участие в дискуссии, контрольная работа	Весь список литературы. Базы данных, информационно-справочные и поисковые системы Интернета.

Семестр	Название раздела, темы	Самостоятельная работа обучающихся			Оценочное средство	Учебно-методическое обеспечение самостоятельной работы
		Вид самостоятельной работы	Сроки выполнения	Затраты времени (час.)		
	Политика обеспечения информационной безопасности в КНР	Изучение учебной, научной литературы с привлечением электронных средств официальной, статистической и научной информации Подготовка к выступлениям на семинаре Подготовка презентации	ноябрь	7	Выступление на семинарском занятии, сообщение с презентацией, участие в дискуссии, контрольная работа	Весь список литературы. Базы данных, информационно-справочные и поисковые системы Интернета.
	Политика обеспечения информационной безопасности в США в странах Европейского Союза	Изучение учебной, научной литературы с привлечением электронных средств официальной, статистической и научной информации Подготовка к выступлениям на семинаре Подготовка презентации	декабрь	7	Выступление на семинарском занятии, сообщение с презентацией, участие в дискуссии, контрольная работа	Весь список литературы. Базы данных, информационно-справочные и поисковые системы Интернета.
	Политика обеспечения информационной безопасности в странах Ближнего Востока	Изучение учебной, научной литературы с привлечением электронных средств официальной, статистической и научной информации Подготовка к выступлениям на семинаре Подготовка презентации	декабрь	7	Выступление на семинарском занятии, сообщение с презентацией, участие в дискуссии, контрольная работа	Весь список литературы. Базы данных, информационно-справочные и поисковые системы Интернета.

Семестр	Название раздела, темы	Самостоятельная работа обучающихся			Оценочное средство	Учебно-методическое обеспечение самостоятельной работы
		Вид самостоятельной работы	Сроки выполнения	Затраты времени (час.)		
	Политика обеспечения информационной безопасности в США в странах Азиатско-Тихоокеанского региона	Изучение учебной, научной литературы с привлечением электронных средств официальной, статистической и научной информации Подготовка к выступлениям на семинаре Подготовка презентации	декабрь	7	Выступление на семинарском занятии, сообщение с презентацией, участие в дискуссии, контрольная работа	Весь список литературы. Базы данных, информационно-справочные и поисковые системы Интернета.
	По всем темам курса	Подготовка к зачету. Подготовиться к устному ответу	декабрь		Зачет в виде устного опроса	Весь список литературы. Базы данных, информационно-справочные и поисковые системы Интернета.
Общая трудоемкость самостоятельной работы по дисциплине (час)				**77**		
Из них объем самостоятельной работы **с использованием электронного обучения и дистанционных образовательных технологий (час)**				**14**		

4.3 Содержание учебного материала

№	Наименование раздела / тема	Содержание дисциплины
РАЗДЕЛ 1. Современное информационное общество		
1.1	**Понятие информационного общества. Основные вехи формирования информационного общества.**	Понятие «информация» и «информационное общество». Теоретические концепции информационного общества. Концепции информационного общества в трудах российских ученых. Этапы развития информационного общества.
1.2	**Основные характеристики современного информационного общества**	Развитие интернета как ключевой инфраструктуры информационного общества. Основные характеристики интернета. Международное управление интернетом: позиции США и России по вопросам международного управления интернетом. Современные тенденции развития глобального информационного общества. Цифровая дипломатия и социальные сети. Промышленная революция 4.0. Развитие «Интернета вещей» и социальных сетевых сервисов. «Большие данные» (big data). Блокчейн – новая эпоха интернета. Искусственный интеллект – новые вызовы. Электронные деньги и онлайн-банкинг. Политико-экономические аспекты развития глобального информационного общества. Развитие информационного общества в России. Основополагающие документы России в области развития информационного общества и информационной безопасности.
РАЗДЕЛ 2. Международная информационная безопасность: общие характеристики		
2.1	**Понятие международной информационной безопасности**	Понятие международной информационной безопасности. Подходы к определению понятия. Информационная безопасность и кибербезопасность: сравнительный анализ исследовательских дискурсов и политической практики. Российский подход к определению международной информационной безопасности. Американский подход к определению международной информационной безопасности. Информационно-психологические и информационно-технические аспекты информационной безопасности. Подход, зафиксированный в официальных документах ООН и других международных организаций.
2.2	**Вызовы и угрозы международной информационной безопасности**	Перечень угроз информационной безопасности в международной повестке. Принципы классификации и источники угроз МИБ. Триада угроз международной информационной безопасности: преступная, террористическая, военно-политическая. Субъекты, действующие в информационном пространстве: государства; хакеры и хакерские группы; организованные преступные группировки; террористы. Международная безопасность и государственный суверенитет в эпоху цифровых технологий. Субъекты информационного воздействия – государства и негосударственные акторы.
2.3	**Информационные войны и информационные конфликты**	Понятия «информационная война», «информационное противоборство», «информационное оружие»: существующие подходы к определению. Характеристика понятия «информационное оружие». Типизация информационного оружия. Теория и практика информационных войн в контексте цифровых информационно-коммуникационных технологий. Зарубежные аналитики и официальные документы США об информационной войне в цифровую эпоху. Особенности кибервойн в зарубежной теории и практике. Использование информационно-коммуникационных технологий в военном деле. Концепции информационных операций Вооруженных сил США. Радиоэлектронная борьба как фактор информационных операций. Радиоэлектронная борьба в истории российской армии. Концепция деятельности Вооруженных Сил Российской Федерации в информационном пространстве. Теории и практики гибридных войн и «цветных революций» в контексте применения информационно-коммуникационных технологий. Гибридная война: миф или реальность — теория или практика. Пропаганда угрозы гибридной войны как политический механизм попыток усилить НАТО.
2.4	**Информационный терроризм и**	Использование информационных технологий в противоправных целях. Международный классификатор правонарушений в сфере компьютерной

	информационная преступность	Информации. Использование интернета в преступных целях. Коммерческий потенциал информационной преступности. Кибертерроризм — актуальная проблема современных международных отношений. Информационный терроризм и трансформация международного терроризма. Международно-политическое измерение проблем информационного терроризма и информационной преступности.
РАЗДЕЛ 3. Подходы к обеспечению информационной безопасности в зарубежных государствах		
3.1	**Политика обеспечения информационной безопасности в США**	Подходы США к обеспечению кибербезопасности и их эволюция. Национальная киберстратегия США. Основополагающие документы США в области обеспечения кибербезопасности. Политико-правовые аспекты обеспечения кибербезопасности в США. Военно-политические институты, ответственные за обеспечение кибербезопасности США. Киберкомандование США. Спецслужбы США. Сотрудничество правительства с частным сектором по вопросу обеспечения кибербезопасности. Инциденты кибербезопасности. Инициативы США по обеспечению информационной безопасности на международной арене и в рамках ООН. Международная информационная безопасность и «силовой» сценарий взаимодействия США с Россией. НАТО: киберпространство — пятая сфера военной деятельности. Центры передового опыта киберНАТО.
3.2	**Политика обеспечения информационной безопасности в КНР**	Подходы Китая к обеспечению информационной безопасности и их эволюция. Роль Коммунистической партии Китая в обеспечении национальной информационной безопасности. Цивилизационный опыт Китая и китайская философия: уроки для современности. Основополагающие документы КНР в области обеспечения информационной безопасности. Политико-правовые аспекты обеспечения информационной безопасности в Китае. Военно-политические институты, ответственные за обеспечение информационной безопасности КНР. Сотрудничество правительства с частным сектором по вопросу обеспечения кибербезопасности. Инциденты кибербезопасности. в КНР. Инициативы КНР по обеспечению информационной безопасности на международной арене. Сотрудничество КНР с Россией по вопросу обеспечения информационной безопасности на двусторонней основе и в рамках международных организаций: ООН, ШОС, БРИКС.
3.3	**Политика обеспечения информационной безопасности в США в странах Европейского Союза**	Стратегия кибербезопасности Европейского Союза. Директивы и документы Европейского союза в области обеспечения кибербезопасности. Политико-правовые аспекты обеспечения кибербезопасности в Европейском Союзе. Европейское агентство по сетевой и информационной безопасности. Политика ЕС по противодействию гибридным угрозам и в сфере кибердипломатии. Координация действий ЕС с киберпланами НАТО.
3.4	**Политика обеспечения информационной безопасности в странах Ближнего Востока**	Обзор стратегий государств Ближнего Востока в сфере обеспечения кибербезопасности. Сотрудничество стран Ближнего Востока в сфере противодействия киберугрозам. Угрозы, с которыми сталкиваются страны Ближнего Востока.
3.5	**Политика обеспечения информационной безопасности в странах Азиатско-Тихоокеанского региона**	Обзор стратегий государств Азиатско-Тихоокеанского региона в сфере обеспечения кибербезопасности. Сотрудничество стран Азиатско-Тихоокеанского региона в сфере противодействия киберугрозам. Угрозы, с которыми сталкиваются страны Азиатско-Тихоокеанского региона.

4.3.1. Перечень семинарских, практических занятий и лабораторных работ

	№ раздела и темы дисциплины	Наименование семинаров, практических и лабораторных работ	Трудоемкость (часы)		Оценочные средства	Формируемая компетенция
			Всего часов	Из них практическая подготовка		
1	2	3	4	5	6	7
1.	**1.1 – 1.2**	1.1 Понятие информационного общества. Основные вехи формирования информационного общества.	2		Выступление на семинарском занятии, сообщение с презентацией, участие в дискуссии, контрольная работа	ПК-5
2.		1.2 Основные характеристики современного информационного общества	2		Выступление на семинарском занятии, сообщение с презентацией, участие в дискуссии, контрольная работа	ПК-5
4.	**2.1 – 2.4**	2.1 Понятие международной информационной безопасности	2		Выступление на семинарском занятии, сообщение с презентацией, участие в дискуссии, контрольная работа	ПК-5
5.		2.2 Вызовы и угрозы международной информационной безопасности	4		Выступление на семинарском занятии, сообщение с презентацией, участие в дискуссии, контрольная работа	ПК-5
6.		2.3 Информационные войны и информационные конфликты	2		Выступление на семинарском занятии, сообщение с презентацией, участие в дискуссии, контрольная работа	ПК-5
7.		2.4 Информационный терроризм и информационная преступность	2		Выступление на семинарском занятии, сообщение с презентацией, участие в дискуссии, контрольная работа	ПК-5
9.	**3.1 – 3.5**	Политика обеспечения информационной безопасности в США	4		Выступление на семинарском занятии, сообщение с презентацией, участие в дискуссии, контрольная работа	ПК-5
10.		Политика обеспечения информационной безопасности в КНР	4		Выступление на семинарском занятии, сообщение с	ПК-5

					презентацией, участие в дискуссии, контрольная работа	
11.		Политика обеспечения информационной безопасности в США в странах Европейского Союза	4		Выступление на семинарском занятии, сообщение с презентацией, участие в дискуссии, контрольная работа	ПК-5
12.		Политика обеспечения информационной безопасности в странах Ближнего Востока	4		Выступление на семинарском занятии, сообщение с презентацией, участие в дискуссии, контрольная работа	ПК-5
13.		Политика обеспечения информационной безопасности в США в странах Азиатско-Тихоокеанского региона	4		Выступление на семинарском занятии, сообщение с презентацией, участие в дискуссии, контрольная работа	ПК-5

4.3.2. Перечень тем (вопросов), выносимых на самостоятельное изучение студентами в рамках самостоятельной работы (СРС)

№ п/п	Тема	Задание	Формируемая компетенция	ИДК
1	Понятие информационного общества. Основные вехи формирования информационного общества. Основные характеристики современного информационного общества	Подготовка доклада с презентацией.	ПК-5	ПК 5.1 ПК 5.2
2	Понятие международной информационной безопасности	Подготовка доклада с презентацией.	ПК-5	ИДК $_{ПК\ 5.1}$ ИДК $_{ПК\ 5.2}$
3	Вызовы и угрозы международной информационной безопасности	Подготовка доклада с презентацией.	ПК-5	ИДК $_{ПК\ 5.1}$ ИДК $_{ПК\ 5.2}$
4	Информационные войны и информационные конфликты	Подготовка доклада с презентацией.	ПК-5	ИДК $_{ПК\ 5.1}$ ИДК $_{ПК\ 5.2}$
5	Информационный терроризм и информационная преступность	Подготовка доклада с презентацией.	ПК-5	ИДК $_{ПК\ 5.1}$ ИДК $_{ПК\ 5.2}$
6	Политика обеспечения информационной безопасности в США	Подготовка доклада с презентацией.	ПК-5	ИДК $_{ПК\ 5.1}$ ИДК $_{ПК\ 5.2}$
7	Политика обеспечения информационной безопасности в КНР	Подготовка доклада с презентацией.	ПК-5	ИДК $_{ПК\ 5.1}$ ИДК $_{ПК\ 5.2}$
8	Политика обеспечения информационной безопасности в США в странах Европейского Союза	Подготовка доклада с презентацией.	ПК-5	ИДК $_{ПК\ 5.1}$ ИДК $_{ПК\ 5.2}$
9	Политика обеспечения информационной безопасности в странах Ближнего Востока	Подготовка доклада с презентацией.	ПК-5	ИДК $_{ПК\ 5.1}$ ИДК $_{ПК\ 5.2}$
10	Политика обеспечения информационной безопасности в США в странах Азиатско-Тихоокеанского региона	Подготовка доклада с презентацией.	ПК-5	ИДК $_{ПК\ 5.1}$ ИДК $_{ПК\ 5.2}$

4.4. Методические указания по организации самостоятельной работы студентов

В ходе изучения дисциплины «Политика обеспечения информационной безопасности в зарубежных государствах» предусмотрена подготовка к семинарским занятиям, в том числе составление конспекта по теме семинара;

Работа с книгой

При работе с книгой необходимо подобрать литературу, научиться правильно ее читать, вести записи. Для подбора литературы в библиотеке используются алфавитный и систематический каталоги.

Важно помнить, что рациональные навыки работы с книгой – это всегда большая экономия времени и сил.

Правильный подбор учебников рекомендуется преподавателем, читающим лекционный курс. Необходимая литература может быть также указана в методических разработках по данному курсу.

Изучая материал по учебнику, следует переходить к следующему вопросу только после правильного уяснения предыдущего, описывая на бумаге все выкладки и вычисления (в том числе те, которые в учебнике опущены или на лекции даны для самостоятельного вывода).

При изучении любой дисциплины большую и важную роль играет самостоятельная индивидуальная работа.

Особое внимание следует обратить на определение основных понятий курса. Студент должен подробно разбирать примеры, которые поясняют такие определения, и уметь строить аналогичные примеры самостоятельно. Нужно добиваться точного представления о том, что изучаешь. Полезно составлять опорные конспекты. При изучении материала по учебнику полезно в тетради (на специально отведенных полях) дополнять конспект лекций. Там же следует отмечать вопросы, выделенные студентом для консультации с преподавателем.

Выводы, полученные в результате изучения, рекомендуется в конспекте выделять, чтобы они при перечитывании записей лучше запоминались.

Опыт показывает, что многим студентам помогает составление листа опорных сигналов, содержащего важнейшие и наиболее часто употребляемые формулы и понятия. Такой лист помогает запомнить формулы, основные положения лекции, а также может служить постоянным справочником для студента.

Различают два вида чтения; первичное и вторичное. *Первичное* – эти внимательное, неторопливое чтение, при котором можно остановиться на трудных местах. После него не должно остаться ни одного непонятного олова. Содержание не всегда может быть понятно после первичного чтения.

Задача *вторичного* чтения полное усвоение смысла целого (по счету это чтение может быть и не вторым, а третьим или четвертым).

Правила самостоятельной работы с литературой

Как уже отмечалось, самостоятельная работа с учебниками и книгами (а также самостоятельное теоретическое исследование проблем, обозначенных преподавателем на лекциях) – это важнейшее условие формирования у себя научного способа познания. Основные советы здесь можно свести к следующим:

• Составить перечень книг, с которыми Вам следует познакомиться; «не старайтесь запомнить все, что вам в ближайшее время не понадобится, – советует студенту и молодому ученому Г. Селье, – запомните только, где это можно отыскать».

• Сам такой перечень должен быть систематизированным (что необходимо для семинаров, что для экзаменов, что пригодится для написания курсовых и дипломных работ, а что Вас интересует за рамками официальной учебной деятельности, то есть что может расширить Вашу общую культуру).

• Обязательно выписывать все выходные данные по каждой книге (при написании курсовых и дипломных работ это позволит очень сэкономить время).
• Разобраться для себя, какие книги (или какие главы книг) следует прочитать более внимательно, а какие – просто просмотреть.

• При составлении перечней литературы следует посоветоваться с преподавателями и научными руководителями (или даже с более подготовленными и эрудированными сокурсниками), которые помогут Вам лучше сориентироваться, на что стоит обратить большее внимание, а на что вообще не стоит тратить время...

•Естественно, все прочитанные книги, учебники и статьи следует конспектировать, но это не означает, что надо конспектировать «все подряд»: можно выписывать кратко основные идеи автора и иногда приводить наиболее яркие и показательные цитаты (с указанием страниц).

• Если книга – Ваша собственная, то допускается делать на полях книги краткие пометки или же в конце книги, на пустых страницах просто сделать свой «предметный указатель», где отмечаются наиболее интересные для Вас мысли и обязательно указываются страницы в тексте автора (это очень хороший совет, позволяющий экономить время и быстро находить «избранные» места в самых разных книгах).

• Если Вы раньше мало работали с научной литературой, то следует выработать в себе способность «воспринимать» сложные тексты; для этого лучший прием – научиться «читать медленно», когда Вам понятно каждое прочитанное слово (а если слово незнакомое, то либо с помощью словаря, либо с помощью преподавателя обязательно его узнать), и это может занять немалое время (у кого-то – до нескольких недель и даже месяцев); опыт показывает, что после этого студент каким-то «чудом» начинает буквально заглатывать книги и чуть ли не видеть «сквозь обложку», стоящая это работа или нет...

• «Либо читайте, либо перелистывайте материал, но не пытайтесь читать быстро... Если текст меня интересует, то чтение, размышление и даже фантазирование по этому поводу сливаются в единый процесс, в то время как вынужденное скорочтение не только не способствует качеству чтения, но и не приносит чувства удовлетворения, которое мы получаем, размышляя о прочитанном», – советует Г. Селье.

• Есть еще один эффективный способ оптимизировать знакомство с научной литературой – следует увлечься какой-то идеей и все книги просматривать с точки зрения данной идеи. В этом случае студент (или молодой ученый) будет как бы искать аргументы «за» или «против» интересующей его идеи, и одновременно он будет как бы общаться с авторами этих книг по поводу своих идей и размышлений... Проблема лишь в том, как найти «свою» идею...

Чтение научного текста является частью познавательной деятельности. Ее цель – извлечение из текста необходимой информации. От того на сколько осознанна читающим собственная внутренняя установка при обращении к печатному слову (найти нужные сведения, усвоить информацию полностью или частично, критически проанализировать материал и т.п.) во многом зависит эффективность осуществляемого действия.

Выделяют четыре основные установки в чтении научного текста:

1. информационно-поисковый (задача – найти, выделить искомую информацию)

2. усваивающая (усилия читателя направлены на то, чтобы как можно полнее осознать и запомнить как сами сведения излагаемые автором, так и всю логику его рассуждений)

3. аналитико-критическая (читатель стремится критически осмыслить материал, проанализировав его, определив свое отношение к нему)

4. творческая (создает у читателя готовность в том или ином виде – как отправной пункт для своих рассуждений, как образ для действия по аналогии и т.п. – использовать суждения автора, ход его мыслей, результат наблюдения, разработанную методику, дополнить их, подвергнуть новой проверке).

С наличием различных установок обращения к научному тексту связано существование и нескольких видов чтения:

1. библиографическое – просматривание карточек каталога, рекомендательных списков, сводных списков журналов и статей за год и т.п.;

2. просмотровое – используется для поиска материалов, содержащих нужную информацию, обычно к нему прибегают сразу после работы со списками литературы и каталогами, в результате такого просмотра читатель устанавливает, какие из источников будут использованы в дальнейшей работе;

3. ознакомительное – подразумевает сплошное, достаточно подробное прочтение отобранных статей, глав, отдельных страниц, цель – познакомиться с характером информации, узнать, какие вопросы вынесены автором на рассмотрение, провести сортировку материала;

4. изучающее – предполагает доскональное освоение материала; в ходе такого чтения проявляется доверие читателя к автору, готовность принять изложенную информацию, реализуется установка на предельно полное понимание материала;

5. аналитико-критическое и творческое чтение – два вида чтения близкие между собой тем, что участвуют в решении исследовательских задач. Первый из них предполагает направленный критический анализ, как самой информации, так и способов ее получения и подачи автором; второе – поиск тех суждений, фактов, по которым или в связи с которыми, читатель считает нужным высказать собственные мысли.

Из всех рассмотренных видов чтения основным для студентов является изучающее – именно оно позволяет в работе с учебной литературой накапливать знания в различных областях. Вот почему именно этот вид чтения в рамках учебной деятельности должен быть освоен в первую очередь. Кроме того, при овладении данным видом чтения формируются основные приемы, повышающие эффективность работы с научным текстом.

Основные виды систематизированной записи прочитанного:

1. Аннотирование – предельно краткое связное описание просмотренной или прочитанной книги (статьи), ее содержания, источников, характера и назначения;

2. Планирование – краткая логическая организация текста, раскрывающая содержание и структуру изучаемого материала;

3. Тезирование – лаконичное воспроизведение основных утверждений автора без привлечения фактического материала;

4. Цитирование – дословное выписывание из текста выдержек, извлечений, наиболее существенно отражающих ту или иную мысль автора;

5. Конспектирование – краткое и последовательное изложение содержания прочитанного.

Конспект – сложный способ изложения содержания книги или статьи в логической последовательности. Конспект аккумулирует в себе предыдущие виды записи, позволяет всесторонне охватить содержание книги, статьи. Поэтому умение составлять план, тезисы, делать выписки и другие записи определяет и технологию составления конспекта.

Методические рекомендации по составлению конспекта:

1. Внимательно прочитайте текст. Уточните в справочной литературе непонятные слова. При записи не забудьте вынести справочные данные на поля конспекта;

2. Выделите главное, составьте план;

3. Кратко сформулируйте основные положения текста, отметьте аргументацию автора;

4. Законспектируйте материал, четко следуя пунктам плана. При конспектировании старайтесь выразить мысль своими словами. Записи следует вести четко, ясно.

5. Грамотно записывайте цитаты. Цитируя, учитывайте лаконичность, значимость мысли.

В тексте конспекта желательно приводить не только тезисные положения, но и их доказательства. При оформлении конспекта необходимо стремиться к емкости каждого

предложения. Мысли автора книги следует излагать кратко, заботясь о стиле и выразительности написанного. Число дополнительных элементов конспекта должно быть логически обоснованным, записи должны распределяться в определенной последовательности, отвечающей логической структуре произведения. Для уточнения и дополнения необходимо оставлять поля.

Доклад – публичное сообщение, представляющее собой развёрнутое изложение определённой темы.

Этапы подготовки доклада:

1. Определение цели доклада;
2. Подбор необходимого материала;
3. Составление плана доклада;
4. Общее знакомство с литературой и выделение основных источников;
5. Уточнение плана, отбор материала к пунктам;
6. Оформление доклада согласно требованиям;
7. Запоминание текста доклада, подготовка тезисов выступления;
8. Выступление с докладом;
9. Обсуждение доклада;
10. Оценка доклада.

Вступление: название доклада; основная идея; оценка предмета изложения; краткое перечисление рассматриваемых вопросов; форму изложения; акцентирование оригинальности подхода.

Основная часть: суть темы, обычно строится по принципу отчёта.

Заключение: четкое обобщение и краткие выводы по излагаемой теме.

Оформление презентации. Для всех слайдов необходимо использовать один и тот же шаблон оформления, кегль – для заголовков - не меньше 24 пунктов, для информации - не менее 18. В презентациях не принято ставить переносы в словах. Наилучшими являются контрастные цвета фона и текста (белый фон – черный текст). Лучше не смешивать разные типы шрифтов в одной презентации. Неконтрастные слайды будут смотреться тусклыми и невыразительными, особенно в светлых аудиториях. Для лучшей ориентации в презентации по ходу выступления лучше пронумеровать слайды. На слайдах должны быть поля, не менее 1 см с каждой стороны. Для акцентирования внимания можно воспользоваться лазерной указкой. Если Вы предпочитаете воспользоваться помощью оператора, а не листать слайды самостоятельно, очень полезно предусмотреть ссылки на слайды в тексте доклада. Заключительный слайд презентации, содержащий текст «Спасибо за внимание» или «Конец», неприемлем для презентации, сопровождающей публичное выступление, поскольку завершение показа слайдов не является завершением выступления. Такие слайды, так же как и слайд «Вопросы?», дублируют устное сообщение. Оптимальный вариант – повторение первого слайда в конце презентации, поскольку это дает возможность еще раз напомнить слушателям тему выступления и имя докладчика и либо перейти к вопросам, либо завершить выступление. После подготовки презентации необходима репетиция выступления.

4.5. Примерная тематика курсовых работ (проектов) (*при наличии*) курсовые работы не предусмотрены учебным планом

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

а) основная литература

1. Инновационные направления современных международных отношений : учеб. пособие для студ. гуманитар. вузов и фак. / ред.: А. В. Крутских, А. В. Бирюков. -

М. : Аспект Пресс, 2010. - 295 с. ; 22 см. - Библиогр. в конце глав. - ISBN 978-5-7567-0562-1 : 340.33 р., 270.00 р. Экземпляры всего: 11+
2. Современные глобальные проблемы : учеб. пособие / Московский гос. ин-т междунар. отношений, Рос. акад. наук, Ин-т мировой экон. и междунар. отношений ; ред.: В. Г. Барановский, А. Д. Богатуров. - М. : Аспект Пресс, 2010. - 350 с. ; 21 см. - Библиогр. в конце глав. - ISBN 978-5-7567-0595-9 : 270.00 р., 270.00 р. Экземпляры всего: 30+
3. Современная мировая политика. Прикладной анализ : учеб. пособие для студ. вузов, обуч. по напр. подгот. "Междунар. отношения" и "Зарубежное регионоведение" / ред. А. Д. Богатуров. - 2-е изд., испр. и доп. - М. : Аспект Пресс, 2010. - 591 с. : табл. ; 22 см. - Библиогр.: с. 589-590. - ISBN 978-5-7567-0580-5 : 435.55 р., 435.55 р., 578.90 р. Экземпляры всего: 6.+
4. Международная информационная безопасность: теория и практика : учеб. для вузов, по направл. подгот. (спец.) "Междунар. отношения", "Зарубеж. регионоведение", "Политология" : в 3 т. / А. В. Крутских [и др.] ; Моск. гос. ин-т междунар. отношений (ун-т) МИД России. – 2-е изд., доп. –Москва : Аспект Пресс, 2021. – ISBN 978-5-7567-1097-7.
Т. 1 / ред. А. В. Крутских. - 2021. - 381 с. : ил., табл. - ISBN 978-5-7567-1098-4 : 1040.00 р. – Текст : непосредственный. Экземпляры всего: 6

б) дополнительная литература

1. Петренко С. А. Киберустойчивость индустрии 4.0 : науч. изд. / С. А. Петренко ; Моск. физ.-техн. ин-т (нац. исслед. ун-т). - СПб. : Изд. дом "Афина", 2020. - 255 с. : ил., табл. ; 29 см. - Библиогр.: с. 238-255. - ISBN 978-5-6045272-0-7 : 400.00 р. Экземпляры всего: 2
2. Нартов Н. А. Геополитика : учебник / Н. А. Нартов, В. Н. Нартов ; ред. В. И. Староверов. - 5-е изд., перераб. и доп. - М. : Юнити-Дана, 2013. - 639 с. ; 21 см. - Библиогр.: с. 635. - ISBN 978-5-238-01816-4 : 495.00 р., 473.85 р. Экземпляры всего: 11
3. Информационное общество : информ. войны; информ. управление; информ. безопасность / С-Пб гос.ун-т,Ин-т проблем управления РАН ; Под. ред. М. А.Вуса. - СПб. : Изд-во С.-Петербург.ун-та, 1999. - 211 с. ; 22см. - ISBN 5288026149 : 25.00 р. Экземпляры всего: 2

в) периодические издания

1. Журнал «Международные процессы»
2. Журнал «Россия в глобальной политике»
3. Журнал «Международная жизнь»
4. Журнал «Сравнительная политика»
5. Журнал «Стратегическая стабильность»

г) базы данных, информационно-справочные и поисковые системы

1. Российский совет по международным делам. URL: https://russiancouncil.ru/
2. Международный дискуссионный клуб «Валдай». URL: https://ru.valdaiclub.com/
3. Независимое военное обозрение. URL: URL:https://nvo.ng.ru/
4. Россия в глобальной политике. URL: https://globalaffairs.ru/
5. Международная жизнь. URL: https://interaffairs.ru/
6. Cyberleninka. URL: https://cyberleninka.ru/
7. Российская национальная библиотека http://nlr.ru/
8. Научная библиотека Иркутского государственного университета http://library.isu.ru/ru

9. Иркутская областная государственная универсальная научная библиотека им. И. И. Молчанова-Сибирского http://www.irklib.ru/
10. Научная электронная библиотека eLibrary.ru
11. ЭЧЗ «БиблиоТех»
12. ЭБС «Издательство Лань»
13. ЭБС «Руконт»
14. ЭБС «Айбукс»
15. ЭБС «ЮРАЙТ»

Перечень ресурсов прилагается **по состоянию на март 2024 г.**

ЭЛЕКТРОННО-БИБЛИОТЕЧНЫЕ СИСТЕМЫ	
ЭБС «Издательство Лань»	
Информационное письмо № 1258 от 30.11.2022 г. Исполнитель: ООО «Издательство Лань»	Реквизиты (номер, дата заключения, срок действия): ООО «Издательство Лань». Информационное письмо № 1258 от 30.11.2022 г. Срок действия: бессрочный 2.Адрес доступа: http://e.lanbook.com/ 3. Цена контракта: бесплатный доступ 4.Количество пользователей: круглосуточный доступ неограниченному числу пользователей из любой точки сети Интернет 5.Характеристика: Доступ к 752научным журналам, с общим количеством статей более 355 000. Классическая литература по следующим отраслям знаний: «География» - 408 книг, «Искусствоведение» - 188 книг, «Право и Юридические науки» - 693 книга, «Психология. Педагогика» - 161 книг, «Социально-гуманитарные науки» - 2212 книг, «Экономика. Менеджмент» - 116 книг, Языкознание и литературоведение – 2028 книг, «Художественная литература» - 27479 книг.
Контракт № 271/23 от 01.11.2023г. Исполнитель: ООО ЭБС« Лань»	1.Реквизиты (номер, дата заключения, срок действия) ООО «ЭБС Лань». Контракт № 271/23 от 01.11.2023г.; Срок действия по 13.11.2024 г. 2.Адрес доступа: www.e.lanbook.com Цена контракта: 488 5438,46 руб. 4. Акт № ТЭ11-00017 от 14.11.2023 г. 5. Характеристика коллекции «Языкознание и литературоведение» издательство ВКН (222 назв.), «Химия» (52), «Биология» (35) - изд-ва «Лаборатория знаний», Политематическая – 98 электронных книг издательств: Физматлит, ДМК-Пресс, Генезис, Дашков и К, Флинта и др. 6. Количество пользователей: круглосуточный доступ неограниченному числу авторизованных пользователей из любой точки сети Интернет
Контракт № 256/23 от 18.10.2023г. Исполнитель: ООО «Издательство Лань»	1.Реквизиты (номер, дата заключения, срок действия) ООО «Издательство Лань». Контракт № 256/23 от 18.10.2023г.; Срок действия по 13.11.2024 г. 2.Адрес доступа: www.e.lanbook.com 3.Цена контракта: 700 000,00 руб. 4. Акт № ТЛ11-9 от 14.11.2023 г. 5. Характеристика: единая профессиональная база знаний для классических вузов 5334 назв. 6. Количество пользователей: круглосуточный доступ неограниченному числу авторизованных пользователей из любой точки сети Интернет
ЭБС ЭЧЗ «Библиотех» работает на платформе **Book on Lime** с 01.10.2023г.	

Государственный контракт № 019 от 22.02.2011 г. Лицензионное соглашение № 31 от 22.02.2011 г. Исполнитель: ООО» Библиотех»	1.Реквизиты (номер, дата заключения, срок действия): ООО «Библиотех» Государственный контракт № 019 от 22.02.2011 г. Срок действия: бессрочный Лицензионное соглашение 31 от 22.02.2011 г. 2.Адрес доступа: https://isu.bookonlime.ru/ 3. Цена контракта:390000 руб. 4.Количество пользователей: круглосуточный доступ неограниченному числу пользователей из любой почки сети Интернет 5.Характеристика: программный модуль для реализации работы ЭБС. Наполнение «ЭЧЗ Библиотех» - приобретаемыми электронными версиями книг (ЭВК) и трудами ученых ИГУ. 2198 назв. на 01.07.2023 г.
ЭБС «Национальный цифровой ресурс «Руконт»	
Контракт № 249/23 от 13.10.2023г. Исполнитель: ООО ЦКБ «Бибком»	1.Реквизиты (номер, дата заключения, срок действия) ЦКБ «Бибком». Контракт № 249/23 от 13.10.2023; Акт от 14.11.2023 г. Срок действия по 13.11.2024. 2.Адрес доступа: http://rucont.ru/ 3.Цена контракта: 225 114,82 руб. 4.Количество пользователей: круглосуточный доступ неограниченному числу авторизованных пользователей из любой точки сети Интернет 5.Характеристика: Коллекция Политематическая – 136 назв.
ЭБС «Айбукс.ру/ibooks.ru»	
Контракт № 246/23 от 12.10.2023 г. Исполнитель: ООО «Айбукс»	1.Реквизиты (номер, дата заключения, срок действия) ООО «Айбукс» Контракт № 246/23 от 12.10.2023 г.; Акт №81 от 14.11.2023 г. Срок действия по 13.11.2024г. 2.Адрес доступа: http://ibooks.ru 3.Цена контракта: 285 127,00 руб. 4.Количество пользователей: круглосуточный доступ неограниченному числу авторизованных пользователей из любой точки сети Интернет 5.Характеристика: электронные версии печатных изданий по различным дисциплинам учебного процесса - 198 назв.
Электронно-библиотечная система «ЭБС Юрайт»	
Контракт № 212/23 от 18.08.2023 Исполнитель: ООО «ЭБС Юрайт»	1.Реквизиты (номер, дата заключения, срок действия) ООО «Электронное издательство Юрайт». Контракт № 212/23 от 18.08.2023; Срок действия по 17.10. 2024. 2.Адрес доступа: https://urait.ru/ 3. Акт об оказании услуг от 18.10.2023. 4.Цена контракта: 722 650,00 руб. 5.Количество пользователей: круглосуточный доступ из любой точки сети Интернет, количество единовременных доступов согласно приложению к Контракту. 6.Характеристика: электронные версии печатных изданий по различным отраслям знаний, свыше 10,9 тыс. назв.
БД литературных произведений «Литрес»	
Контракт (Лицензионный договор) № 317/23 от 08.12.2023 Исполнитель: ООО «ИТ»	1.Реквизиты (номер, дата заключения, срок действия) ООО «ИТ». Контракт № 317/23 от 08.12.2023; Срок действия по 08.12.2024. 2.Адрес доступа: https://litres.ru/ 3. Акт об оказании услуг от 08.12.2023. 4.Лицензионное вознаграждение: 97 218,00 руб. 5.Количество пользователей: круглосуточный доступ из любой точки сети Интернет, количество единовременных доступов согласно приложению к Контракту. 6.Характеристика: электронные версии печатных изданий по различным отраслям знаний доступ к более 120 000 назв.

ПРОФЕССИОНАЛЬНЫЕ БАЗЫ ДАННЫХ, ИНФОРМАЦИОННЫЕ СПРАВОЧНЫЕ И ПОИСКОВЫЕ СИСТЕМЫ	
EBSCO. Полнотекстовая коллекция книг eBook Academic Collection	
В рамках централизованной подписки 2023 года Исполнитель: Российский фонд фундаментальных исследований (РФФИ) – оператор национальной и централизованной подписки на научные информационные ресурсы.	1.Реквизиты (номер, дата заключения, срок действия) в рамках централизованной подписки 2022 года. Окончание доступа – 31.12.2030. 2. Адрес доступа: https://search.ebscohost.com 3. Цена контракта: на безвозмездной основе. 4. Количество пользователей: без ограничений, с компьютеров сети ИГУ. 5. Характеристика: полнотекстовая междисциплинарная коллекция, которая включает более 210 000 электронных книг от ведущих научных и университетских издательств, в том числе Cambridge University Press, De Gruyter, Elsevier, Harvard University Press, Oxford University Press, State University of New York Press, Taylor & Francis, University of California Press – и охватывает широкий и спектр тем: бизнес, всемирная история, инженерия, литературоведение, медицина, образование, политология, религия, социальные науки, технологии, философия, экономика, языкознание и др. Глубина доступа: 1913–2022 гг.
Springer Nature	
В рамках централизованной подписки 2023 года Исполнитель: Российский фонд фундаментальных исследований (РФФИ) – оператор национальной и централизованной подписки на научные информационные ресурсы	1.Реквизиты (номер, дата заключения, срок действия) в рамках централизованной подписки 2023 года. Окончание доступа – 31.12.2030. 2. Адрес доступа: https://link.springer.com/, https://www.nature.com/siteindex. 3. Цена контракта: на безвозмездной основе. 4. Количество пользователей: без ограничений, с компьютеров сети ИГУ. 5. Характеристика: база данных Spriner Nature 2023 eBook Collections, коллекция журналов Social Sciences Package, коллекция журналов Life Sciences Package, коллекция журналов Physical Sciences & Engineering , полнотекстовая коллекция журналов Springer Journal (1997 г. - 2017 г.)
База данных Wiley Journals Database	
В рамках централизованной подписки 2024 года Исполнитель: Российский фонд фундаментальных исследований (РФФИ) – оператор национальной и централизованной подписки на научные информационные ресурсы.	1. Реквизиты (номер, дата заключения, срок действия) в рамках централизованной подписки 2020 года Окончание доступа – 30.06.2024. 2. Адрес доступа: http://onlinelibrary.wiley.com/ 3. Цена контракта: на безвозмездной основе. 4. Количество пользователей: без ограничений, с компьютеров сети ИГУ. 5. Характеристика: полнотекстовые коллекции, которые включают в себя как текущие, так и архивные выпуски из более чем 1700 журналов издательства, охватывающие такие области как гуманитарные, естественные, общественные и технические науки, а также сельское хозяйство, медицину и здравоохранение**.**
ЭКБСОН	
Соглашение № 84 ЭКБСОН от 15.10.2015 о сотрудничестве в области развития Информационной системы доступа к электронным каталогам библиотек сферы образования и науки в рамках единого Интернет-ресурса. Исполнитель: Федеральное государственное бюджетное учреждение «Государственная публичная научно-техническая библиотека	1.Реквизиты (номер, дата заключения, срок действия) Соглашение № 84 ЭКБСОН от 15.10.2015 о сотрудничестве в области развития Информационной системы доступа к электронным каталогам библиотек сферы образования и науки в рамках единого Интернет-ресурса. 2.Адрес доступа: http://www.vlibrary.ru 3.Цена контракта: на безвозмездной основе. 4.Количество пользователей: без ограничений, с компьютеров сети ИГУ

России»	5.Характеристика: единая информационная система доступа к электронным каталогам библиотечной системы образования и науки в рамках единого интернет-ресурса на основе унифицированного каталога библиотечных ресурсов.
Государственная информационная система «Национальная электронная библиотека» (НЭБ)	
Договор № 101/НЭБ/0760 от 14.09.2015 о предоставлении доступа к Национальной электронной библиотеке. Исполнитель: федеральное государственное бюджетное учреждение «Российская государственная библиотека»	1.Реквизиты (номер, дата заключения, срок действия) Договор № 101/НЭБ/0760 от 14.09.2015 о предоставлении доступа к Национальной электронной библиотеке. 2.Адрес доступа: http://нэб.рф 3.Цена контракта: на безвозмездной основе. 4.Количество пользователей: без ограничений, с компьютеров сети ИГУ 5.Характеристика: доступ к совокупности распределенных фондов полнотекстовых электронных версий печатных, электронных и мультимедийных ресурсов НЭБ, а также к единому сводному каталогу фонда НЭБ.
УИС РОССИЯ	
Письмо от директора НБ ИГУ № 26/06 от 19.12.2006 Исполнитель: Научно-исследовательского вычислительного центра МГУ имени М.В. Ломоносова	1. Реквизиты (номер, дата заключения, срок действия) письмо от директора НБ ИГУ № 26/06 от 19.12.2006 (доступ предоставляется по обращению руководителя организации), срок действия – без ограничений. 2. Адрес доступа: http://uisrussia.msu.ru/ 3. Цена контракта: на безвозмездной основе 4. Количество пользователей: без ограничений, с компьютеров сети ИГУ. 5. Характеристика: тематическая электронная библиотека и база для исследований и учебных курсов в области экономики, управления, социологии, лингвистики, философии, филологии, международных отношений и других гуманитарных наук.
ПОЛПРЕД	
Информационное письмо от 16.02.2015 (сообщение о доступе с 24.08.2009). Исполнитель: ООО "ПОЛПРЕД Справочники"	1. Реквизиты (номер, дата заключения, срок действия) информационное письмо от 16.02.2015 г. (сообщение о доступе с 24.08.2009). 2. Адрес доступа: http://polpred.com 3. Цена контракта: на безвозмездной основе 4. Количество пользователей: без ограничений, с компьютеров сети ИГУ 5. Характеристика: база данных представляет результаты мониторинга СМИ на темы промышленной политики РФ и зарубежья
Справочно-правовая система «Консультант Плюс»	
Договор о сотрудничестве от 15.10.2018 Исполнитель: ООО «Информационный Центр ЮНОНА»	1. Реквизиты (номер, дата заключения, срок действия) Договор о сотрудничестве от 15.10.2018. Срок действия - до расторжения сторонами. 2. Адрес доступа: в локальной сети НБ ИГУ. 3. Цена контракта: на безвозмездной основе. 4. Количество пользователей: без ограничений. 5.Характеристика: правовая БД - законодательство РФ, международное право, юридическая литература.
Справочно-правовая система «ГАРАНТ»	
Договор № Б/12 об информационно-правовом сотрудничестве между ООО «Гарант-Сервис Иркутск» и Федеральное государственное бюджетное управление высшего профессионального образования «иркутский государственный университет» (ФГБОУ ВПО «ИГУ») от 16.11.2012; регистрационный лист № 38-70035-003593 от 21.11.2012	1. Реквизиты (номер, дата заключения, срок действия) Договор № Б/12 об информационно-правовом сотрудничестве между ООО «Гарант-Сервис Иркутск» и Федеральное государственное бюджетное управление высшего профессионального образования «Иркутский государственный университет» (ФГБОУ ВПО «ИГУ») от 16.11.2012; Регистрационный лист № 38-70035-003593 от 21.11.2012. Срок действия - до расторжения сторонами. 2. Адрес доступа: в локальной сети НБ ИГУ

Исполнитель: ООО «Гарант-Сервис Иркутск»	3. Цена контракта: на безвозмездной основе 4. Количество пользователей: без ограничений 5. Характеристика: правовая БД – законодательство РФ, международное право, юридическая литература.
Межрегиональная аналитическая роспись статей «МАРС»	
Договор № С/111-1 о сотрудничестве в области развития библиотечно-информационных ресурсов и сервисов от 01.09.2011 с автоматической пролонгацией на следующий календарный год (число пролонгаций не ограничено). Исполнитель: некоммерческое партнерство Ассоциация региональных библиотечных консорциумов (АРБИКОН)	1. Реквизиты (номер, дата заключения, срок действия) Договор № С/111-1 о сотрудничестве в области развития библиотечно-информационных ресурсов и сервисов от 01.09.2011 с автоматической пролонгацией на следующий календарный год (число пролонгаций не ограничено). 2. Адрес доступа: http://arbicon.ru 3. Цена контракта: на безвозмездной основе. 4. Количество пользователей: без ограничений, с компьютеров сети ИГУ 5. Характеристика: база включает 2.5 млн. записей из более 7,5 тыс. российских журналов.
Электронные ресурсы Научной библиотеки Иркутского университета	
Система баз данных электронного каталога	1. Реквизиты (номер, дата заключения, срок действия) 2. Адрес доступа: в локальной сети ИГУ, http://ellib.library.isu.ru 3. Количество пользователей: без ограничений 4. Характеристика: включает более 500 тыс. записей в базах данных. Электронный каталог книг, продолжающихся изданий; БД редких книг и рукописей; БД «Коллекция Н. С. Романова»; БД «Библиотека Н. О. Шаракшиновой»; БД «Иностранная литература»; БД «Американистика»; БД «Коллекция «Оксфорд»; БД «Электронные издания»; БД «Авторефераты диссертаций»; ЭК периодических изданий; БД «Книги библиотеки Иркутского МИОНа»
Библиографические базы данных	1. Реквизиты (номер, дата заключения, срок действия) 2. Адрес доступа: в локальной сети ИГУ 3. Количество пользователей: без ограничений. 4. Характеристика: «Статьи. Социально-гуманитарные науки»; «Статьи. Точные и естественные науки»; «Научная Сибирика» (ГПНТБ); «Научные журналы JDP»
Полнотекстовые базы данных	1. Реквизиты (номер, дата заключения, срок действия) 2. Адрес доступа: в локальной сети ИГУ, http://ellib.library.isu.ru 3. Количество пользователей: без ограничений, с компьютеров локальной сети ИГУ и в локальной сети университета 4. Характеристика: **«Труды ученых ИГУ»** - библиографические описания и полные тексты: 1990-2021 гг. – монографий, учебников, учебных пособий, статей из периодических и продолжающихся изданий, научных сборников ученых ИГУ; с 2015 г. – в т.ч. преподавателей Педагогического института **«Труды ученых ИГУ. 1918-1990 гг.»** - библиографические описания и полные тексты: 1921-1942 гг. – статей из «Сборников (Трудов)… ИГУ»; 1948-1970 – статей из «Трудов…», издаваемых по сериям: «Геологическая», «Биологическая», «Языкознание», «Филологическая», «Литературоведение и критика», «Историческая»,

	«Химическая», «Юридическая» и др.; 1924-1970 гг. – из «Известий БГНИИ»; с 1918-1929 гг. – отдельные издания, статьи из периодических изданий профессоров ИГУ. **«Издания ВСОРГО»** - библиографические и полные тексты «Записок», «Трудов», «Известий» и других изданий ВСОРГО в целом, а также статей, опубликованных в этих изданиях, монографий, «Отчетов» с 1856 по 1930 гг. **«Дореволюционные периодические издания»** - библиографические описания и полные тексты отдельных номеров газет: «Иркутские губернские ведомости» (1857-1916 гг.), «Восточное обозрение» (1882-1906 гг.), «Сибирь» (1873-1887 гг.), «Сибирь» (1890-1913 гг.), «Восточная заря» (1909-1910 гг.), «Иркутская жизнь» (1913-1917 гг.), «Сибирская врачебная газета» (1909-1914 гг.), «Иркутская газета» (1913 г.), «Иркутский вестник» (1912 г.). **Газета «Власть труда»** - библиографические описания и полные тексты отдельных номеров газеты с 1918 по 1930 гг., впоследствии переименованной в «Восточно-Сибирскую правду».

VI. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

6.1. Учебно-лабораторное оборудование:

Специальные помещения: Аудитория для проведения занятий лекционного и семинарского типа *Адрес:* Иркутск, ул. Чкалова, 2, **ауд. 222**	Аудитория оборудована специализированной мебелью на 30 посадочных мест. Оборудована *техническими средствами обучения*, служащими для представления учебной информации большой аудитории: экран Cactus, доска меловая, проектор Miracle, системный блок AMD A8-9600, MSI A320M PRO-E, монитор Philips 23.6" 243V5QSBA/00(01), клавиатура, мышь, колонки SVEN312.

6.2. Программное обеспечение:

Наименование программного продукта	Кол-во	Обоснование для пользования ПО(Лицензия, Договор, счёт, акт или иное)	Дата выдачи лицензии	Срок действия права пользования
«Антиплагиат.ВУЗ» ,25 тыс. проверок	1	№ 04-068-2023 от 13.11.2023	01.01.2024	1 год
«Система онлайн-прокторинга Экзамус 2.0»	1	№ 0144/24 от 16.02.2024	01.05.2024	1 год
Интернет- сервис для проведения вебинаров и видеоконференций Пруффми, тарифный план «Бета»	10	№ 261/23 от 01.11.2023	01.11.2023	1 год
Программно-аппаратный комплекс Jalinga Studio	1	№ К-3329_022022-2	01.06.2022	бессрочно
Linux	Условия правообла	Условия использования по ссылке:	Условия правооблада	бессрочно

	дателя	https://ru.wikipedia.org/wiki/GNU	теля	
Moodle 3.2.1	Условия правообладателя	Условия использования по ссылке: https://ru.wikipedia.org/wiki/Moodle	Условия правообладателя	бессрочно
Kaspersky Endpoint Security для бизнеса - Стандартный Russian Edition (ежегодно обновляемое ПО)	50	№ 04-072-2023 от 13.11.2023	28.11.2023	2 года
Media player home classic	Условия правообладателя	Лицензия GNU GPL - ware free Условия использования по ссылке: https://ru.wikipedia.org/wiki/Media_Player_Classic.	Условия правообладателя	бессрочно
Microsoft Office Enterprise 2007 Russian Academic OPEN No Level	16	Номер Лицензии Microsoft 43364238	17.01.2008	бессрочно
WinPro10 Rus Upgrd OLP NL Acdmc	23	Сублицензионный договор № 502 от 03.03.2017 Счет № ФРЗ- 0003367 от 03.03.2017 Акт № 4496 от 03.03.2017 Лицензия № 68203568	13.03.2017	бессрочно
WinRAR	2	Государственный контракт № 04-175-12 от 26.11.2012	25.12.2012	бессрочно
7zip (ежегодно обновляемое ПО)	Условия правообладателя	Условия использования по ссылке: https://www.7-zip.org/license.txt	Условия правообладателя	бессрочно

Acrobat Reader DC (ежегодно обновляемое ПО)	Условия правообладателя	Условия использования по ссылке: https://acrobat.adobe.com/ru/ru/acrobat/pdf-reader/volume-distribution.html	Условия правообладателя	бессрочно
Foxit PDF Reader 8.0 (ежегодно обновляемое ПО)	Условия правообладателя	Условия использования по ссылке: https://www.foxitsoftware.com/products/pdf-reader/eula.html	Условия правообладателя	бессрочно
Google Chrome (ежегодно обновляемое ПО)	Условия правообладателя	Условия использования по ссылке: https://www.google.ru/chrome/browser/privacy/eula_text.html	Условия правообладателя	бессрочно
Mozilla Firefox (ежегодно обновляемое ПО)	Условия правообладателя	Условия использования по ссылке: https://www.mozilla.org/ru/about/legal/terms/firefox/	Условия правообладателя	бессрочно
Opera 45 (ежегодно обновляемое ПО)	Условия правообладателя	Условия использования по ссылке: http://www.opera.com/ru/terms	Условия правообладателя	бессрочно
R	Условия правообладателя	Условия использования по ссылке: https://ru.wikipedia.org/wiki/R_	Условия правообладателя	бессрочно

6.3. Технические и электронные средства обучения:

Набор демонстрационного оборудования и учебно-наглядных пособий, обеспечивающие тематические иллюстрации, соответствующие рабочей программе дисциплины (презентации).

С помощью ЭИОС ФГБОУ ВО «ИГУ» Educa у студентов есть возможность дистанционного получения материалов. В разделе дисциплины есть постоянный доступ к материалам лекций, презентациям, вопросам и темам семинарских занятий.

VII.ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ

При проведении занятий используются активные и интерактивные формы обучения: разбор конкретных ситуаций, деловые и ролевые игры, элементы психологического тренинга, метод кейсов, мозговой штурм, дискуссия, моделирование профессиональных

ситуаций. В сочетании с внеаудиторной работой это способствует формированию и развитию профессиональных навыков обучающихся.

Для закрепления знаний студентов по всем разделам курса «» проводятся практические занятия.

В учебном процессе широко используются активные и интерактивные формы проведения занятий, таких как:

1) ролевые игры – каждый участник имеет или определенное задание, или определенную роль, которую он должен исполнить в соответствии с заданием, например, при рассмотрении подходов сторонников разных школ в науке о международных отношениях по отношению к проблемам безопасности, международного сотрудничества, работы международных институтов и т.п.

2) групповые дискуссии – связаны с отработкой проведения совещаний или приобретением навыков групповой работы.

3) инновационные игры — формируют инновационное мышление участников, выдвигают инновационные идеи в традиционной системе действий, отрабатывают модели реальной, желаемой, идеальной ситуаций, включают тренинги по самоорганизации, так же способствуют развитию познавательных процессов.

4) элементы тренинговых упражнений направленные на разрешение межличностных конфликтов, повышения уверенности в себе, коммуникативные тренинги.

Наименование тем занятий с использованием активных и интерактивных форм обучения:

	Тема занятия	Вид занятия	Форма / Методы интерактивного обучения	Кол-во часов
1	Современное информационное общество	Лекция	Лекция-визуализация	2
2	Международная информационная безопасность: общие характеристики	Лекция	Лекция-визуализация	2
3	Подходы к обеспечению информационной безопасности в зарубежных государствах	Лекция	Лекция-визуализация	2
Итого часов				6

VIII.ОЦЕНОЧНЫЕ МАТЕРИАЛЫ ДЛЯ ТЕКУЩЕГО КОНТРОЛЯ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

(Материал находится на Образовательном портале ИГУ по адресу https://educa.isu.ru/course/view.php?id=52191)

8.1 Оценочные материалы (ОМ):

8.1.1 Оценочные материалы для входного контроля: входной контроль отсутствует

8.1.2 Оценочные материалы текущего контроля:

Баллы за текущую работу студента по дисциплине начисляются преподавателем в ходе образовательного процесса в постоянном режиме с фиксацией в ведомости. Кроме того, фиксируется посещаемость.

Согласно Положению «О балльно-рейтинговой системе оценки успеваемости студентов Иркутского государственного университета», усвоение студентом каждой изучаемой в семестре дисциплины максимально оценивается 100 баллами. Указанное максимальное количество баллов (Sитог), которое студент может набрать за семестр по каждой дисциплине, складывается из суммы баллов за текущую работу в семестре (Sтек) и баллов, полученных на экзаменационной сессии (Sсес).

При этом максимальное количество баллов за текущую работу в семестре (Sтек) ограничивается 60-ю баллами, а на оценку зачета/экзамена (Sсес) максимально предусматривается 30 баллов.

№ п\п	***Виды учебной деятельности***	***Баллы***	***Максимум за семестр***
	Выступление на практическом занятии	0-5-10	20
	Сообщения на практическом занятии	0-8-15-20	20
	Участие в дискуссии (вопросы)	0-2-4-6	20
	Участие в дискуссии (дополнения)	0-2-4-6	20
	Итоговая контрольня работа	0-3-6-10	10
	Контрольная экзаменационная работа	0-10-15-20	20
	Бонусные поощрительные баллы	0	10
	Всего за семестр		60-100

8.2. Материалы для проведения текущего контроля знаний студентов:

План практических занятий

Раздел 1. СОВРЕМЕННОЕ ИНФОРМАЦИОННОЕ ОБЩЕСТВО
Семинар 1.

1. Раскройте понятия «информация» и «информационное общество».
2. Какие существуют теоретические концепции информационного общества?
3. Назовите основные этапы развития информационного общества.

Семинар 2.

1. Развитие интернета как ключевой инфраструктуры информационного общества. Назовите основные этапы создания Интернета и его характеристики.
2. Промышленная революция 4.0. и его драйвер – технология «блокчейн». Развитие «Интернета вещей» и промышленного «Интернета вещей».
3. Искусственный интеллект и перспективы его применения для развития информационного общества.
4. Цифровая дипломатия и социальные сети.

Раздел 2. МЕЖДУНАРОДНАЯ ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ: ОБЩИЕ ХАРАКТЕРИСТИКИ
Семинар 3.

1. Какие существует подходы к определению понятия «информационная безопасность»? В чём разница между «информационной безопасностью» и «кибербезопасностью»?
2. Информационно-психологические и информационно-технические аспекты информационной безопасности.
3. Подходы к определению «информационной безопасности», зафиксированные в официальных документах ООН и документах других международных организаций.

Семинар 4.

1. Раскройте содержание основных угроз международной информационной безопасности. Каковы принципы их классификации?
2. Характеристика понятия «информационное оружие». Типизация информационного оружия.
3. Перечислите основные субъекты, действующие в глобальном информационном пространстве и дайте их характеристику.
4. Международная безопасность и государственный суверенитет в эпоху цифровых технологий.

Семинар 5.

1. Определите особенности и суть содержания информационных войн. Теория и практика информационных войн в контексте цифровых информационно-коммуникационных технологий.
2. Приведите примеры применения цифровых технологий в локальных международных конфликтах.
3. Гибридная война: миф или реальность — теория или практика.
4. Использование информационно-коммуникационных технологий в военном деле.

Семинар 6.

1. Использование цифровых технологий и Интернета в преступных целях. Коммерческий потенциал информационной преступности.
2. Международный классификатор правонарушений в сфере компьютерной информации.
3. Информационный терроризм и трансформация международного терроризма.
4. Раскройте суть существующих предложений по противодействию информационной преступности и информационному терроризму.

Раздел 3. ПОДХОДЫ К ОБЕСПЕЧЕНИЮ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ЗАРУБЕЖНЫХ ГОСУДАРСТВАХ

Семинар 7.

1. Подходы США к обеспечению кибербезопасности и их эволюция. Национальная киберстратегия США.
2. Основополагающие документы США в области обеспечения кибербезопасности.
3. Политико-правовые аспекты обеспечения кибербезопасности в США.
4. Военно-политические институты, ответственные за обеспечение кибербезопасности США. Киберкомандование США. Спецслужбы США.
5. Сотрудничество правительства с частным сектором по вопросу обеспечения кибербезопасности. Инциденты кибербезопасности.

Семинар 8.

1. Подходы Китая к обеспечению информационной безопасности и их эволюция. Роль Коммунистической партии Китая в обеспечении национальной информационной безопасности.
2. Цивилизационный опыт Китая и китайская философия: уроки для современности.
3. Основополагающие документы КНР в области обеспечения информационной безопасности.
4. Политико-правовые аспекты обеспечения информационной безопасности в Китае.
5. Военно-политические институты, ответственные за обеспечение информационной безопасности КНР.

Семинар 9.

1. Стратегия кибербезопасности Европейского Союза.
2. Директивы и документы Европейского союза в области обеспечения кибербезопасности.
3. Политико-правовые аспекты обеспечения кибербезопасности в Европейском Союзе.
4. Европейское агентство по сетевой и информационной безопасности.
5. Политика ЕС по противодействию гибридным угрозам и в сфере кибердипломатии.

Семинар 10.
1. Обзор стратегий государств Ближнего Востока в сфере обеспечения кибербезопасности.
2. Сотрудничество стран Ближнего Востока в сфере противодействия киберугрозам.
3. Угрозы, с которыми сталкиваются страны Ближнего Востока.

Семинар 11.
1. Обзор стратегий государств Азиатско-Тихоокеанского региона в сфере обеспечения кибербезопасности.
2. Сотрудничество стран Азиатско-Тихоокеанского региона в сфере противодействия киберугрозам.
3. Угрозы, с которыми сталкиваются страны Азиатско-Тихоокеанского региона.

Студент по предложению преподавателя выступает по теме текущего практического занятия. Затем студенты группы в течение 10 мин. могут задавать вопросы по теме выступления. После этого до 5 мин. выступает назначенный в начале занятия оппонент. Кроме анализа выступления и соблюдения выступающим правил публичного выступления, оппонент, если владеет он информацией, добавляет по теме сообщения. Студенты по желанию так же добавляют информацию по теме рассматриваемого вопроса.

Критерии оценивания работы студента на семинаре (выступление)

Оценка	Критерии
8-10 баллов (отлично)	1) полное раскрытие темы; 2) правильные формулировки; 3) ответ структурирован; 4) высказывает и обосновывает собственные суждения и взгляды на проблему; 5) активно дискутирует.
5-7 баллов (хорошо)	1) недостаточно полное раскрытие темы; 2) некоторые фактологические ошибки; 3) ответ структурирован; 4) высказывает собственные суждения и взгляды на проблему; 5) дискутировать.
1-4 балла (удовлетворительно)	1) частичное раскрытие темы; 2) наличие фактологических ошибок; 3) ответ недостаточно структурирован; 4) не способен достаточно глубоко и доказательно обосновать свои суждения и взгляды на проблему; 5) слабо вовлечён в дискуссию.

0 баллов (неудовлетворительно)	1) нераскрытые темы; 2) большое количество фактологических ошибок; 3) ответ не структурирован; 4) не способен высказывать и обосновывать собственные суждения и взгляды на проблему; 5) отсутствие интереса к ведению дискуссии.

В течении учебного семестра на практическом занятии студент по его желанию может выступить **с сообщением** по предложенной ему теме или с другой после ее согласования с преподавателем.

Сообщение студента с презентацией может продолжаться порядка 10-15 мин. Затем студенты группы в течение 10 мин. могут задавать вопросы по теме выступления. Студенты по желанию добавляют информацию по теме сообщения.

Заданный вопрос не засчитывается если он задан не по теме выступления, или фактически вопросом не является.

Дополнение не засчитывается, если выступающий не привел новой информации или не произвел анализа выступления или сообщения.

Критерии оценки участия студента в дискуссии (вопросы, дополнения)

Оценка	Критерии
6 баллов	Задано 3 вопроса или сделано 3 дополнения, позволившие более полно раскрыть обсуждаемую тему, либо уточнить использовавшиеся в сообщении формулировки, либо исправить фактологические ошибки
4 балла	Задано 2 вопроса или сделано 2 дополнения, позволившие более полно раскрыть обсуждаемую тему, либо уточнить использовавшиеся в сообщении формулировки, либо исправить фактологические ошибки
2 балла	Задан 1 вопрос или сделано 1 дополнение, позволившие более полно раскрыть обсуждаемую тему, либо уточнить использовавшиеся в сообщении формулировки, либо исправить фактологические ошибки

Темы сообщений:

1. Социальные сети как инструмент дипломатии.
2. Использование искусственного интеллекта в военных целях в США.
3. Использование искусственного интеллекта в военных целях в Китае.
4. Использование искусственного интеллекта в военных целях в странах Ближнего Востока.
5. Кибероружие – оружие массового поражения?
6. Стратегия информационной безопасности Китая и её связь с традиционной китайской военной философией
7. Разоблачения американского спецагента Эдварда Снодуена и их влияние на мировой политических процесс.
8. История взаимоотношений российско-американских взаимоотношений по вопросу обеспечения кибербезопасности.
9. Возможен ли государственный суверенитет в киберпространстве?
10. Крупные инциденты в области информационной безопасности: 2000-2021.

11. Инициативы частных компаний в сфере обеспечения международной кибербезопасности.
12. Космическая кибербезопасность: взгляд в будущее.
13. Позиции США и Китая по вопросам международного управления интернетом.
14. Роль Шанхайской организации сотрудничества в обеспечении международной информационной безопасности.
15. БРИКС как площадка международного сотрудничества в сфере информационной безопасности.

Критерии оценивания сообщения с презентацией:

	17-20 баллов	**13-17 баллов**	**7-12 баллов**	**0 баллов**
Полнота раскрытия проблемы	Студент полностью раскрыл проблему	Студент достаточно полно раскрыл проблему	Студент не полностью раскрыл проблему	Студент не раскрыл проблему
Использование источников, литературы и фактологического материала по теме. Достоверность используемой информации	Студент использовал большой объем материала. Используемая информация полностью достоверна.	Студент использовал достаточный объем материала. Используемая информация достоверна.	Студент использовал небольшой объем материала. Используемая информация не полностью достоверна	Объем используемого материала минимален. Используемая информация недостоверна.
Наличие грамотных итогов и выводов исследования. Получение достоверных результатов	Итоги и выводы исчерпывающи. Результаты полностью достоверны	Наличие достаточных итогов и выводов. Результаты достоверны	Итоги и выводы приемлемы. Результаты лишь частично достоверы	Отсутствие итогов и выводов/выводы неверны Результаты недостоверны/не получены
Наглядность презентации, владение лексикой.	Результаты представлены очень наглядно. Владение лексикой	Результаты вполне наглядны. Хорошее владение лексикой	Результаты не полностью наглядны. Средний уровень владения лексикой.	Презентация не даёт представления о проведении исследования/отсутствие презентации. Слабый уровень владения лексикой
Самостоятельность исследования	Материал не скопирован. Литература и источники	Небольшая часть материала скопирована. Достаточная	Большая часть материала скопирован	Материал полностью скопирован, либо

	творчески переработаны. Наличие собственных суждений касательно рассматриваемой проблемы	степень творческой переработки источников и литературы. Наличие собственных суждений касательно рассматриваемой проблемы.	а. Слабая степень творческой переработки источников и литературы.	отсутствует творческая переработка источников и литературы. Отсутствие собственных суждений касательно рассматриваемой проблемы.

В конце семестра, в рамках зачетной недели проводится контрольная работа.

Примерные вопросы для контрольной работы:

1. Понятие международной информационной безопасности.
2. Обозначьте ключевые отличия информационной безопасности от кибербезопасности.
3. Перечислите основные угрозы международной информационной безопасности.
4. Принципы классификации и источники угроз МИБ.
5. Какие субъекты действуют в информационном пространстве?
6. Понятие «информационная войны».
7. Характеристика понятия «информационное оружие».
8. Что такое кибертерроризм?

Студент в течение 30 минут письменно отвечает на восемь вопросов.

Критерии оценивания контрольной работы

Оценка	Критерии
10 баллов	Студент даёт исчерпывающие ответы на всем вопросы, а также даёт правильное определение ключевых понятий. Его ответ последователен и структурирован.
6 баллов	Студент даёт правильные ответы на все вопросы и правильное определение ключевых понятий, но допускает 1-2 ошибки. Его ответ структурирован.
3 балла	Студент даёт неполные (или поверхностные) ответы на вопросы, и допускает неточности при определении ключевых понятий. Его ответ слабо структурирован.
0 баллов	Студент даёт неправильные ответы, допускает ошибки при определении ключевых понятий. Его ответ не структурирован.

8.3 Оценочные материалы текущего контроля - *в форме зачета*

В соответствии с Положением «О балльно-рейтинговой системе оценки успеваемости студентов Иркутского государственного университета», студент, набравший в результате текущей работы по дисциплине (Sтек) менее 40 баллов, не допускается к сдаче зачета, и ему выставляется 0 сессионных баллов (Sсес = 0).

Студент, набравший в течение семестра (Sтек) 40 и более баллов, допускается к сдаче зачета по дисциплине, на котором может набрать (Sсес) до 30 баллов.

Если на зачете сумма баллов студента составляет менее 10, то зачет считается не сданным.

Если на зачете студент набирает 10 и более баллов, то они прибавляются к сумме баллов за текущую работу, которые фиксируются в зачетной книжке студента.

Итоговый семестровый рейтинг ($S_{итог}$)	**Академическая оценка**
менее 60 баллов	не зачтено
60-100 баллов	зачтено

Вопросы к зачету:

1. Информационное общество. Понятие информационного общества.
2. Формирование глобального информационного пространства и информационного общества. Современные тенденции развития глобального информационного общества.
3. Развитие интернета как ключевой инфраструктуры информационного общества. Основные характеристики интернета.
4. Промышленная революция 4.0. Развитие «Интернета вещей» и социальных сетевых сервисов. «Большие данные» (big data). Блокчейн – новая эпоха интернета.
5. Искусственный интеллект – новые вызовы.
6. Международные отношения под воздействием научно-технического прогресса.
7. Понятие международной информационной безопасности.
8. Информационная безопасность и кибербезопасность: сравнительный анализ исследовательских дискурсов и политической практики.
9. Существующие угрозы международной информационной безопасности. Принципы классификации и источники угроз МИБ.
10. Субъекты, действующие в информационном пространстве: государства; хакеры и хакерские группы; организованные преступные группировки; террористы.
11. Субъекты информационного воздействия – государства и негосударственные акторы.
12. Международная безопасность и государственный суверенитет в эпоху цифровых технологий.
13. Понятия «информационная война», «информационное противоборство», «информационное оружие»: существующие подходы к определению.
14. Характеристика понятия «информационное оружие». Типизация информационного оружия.
15. Теория и практика информационных войн в контексте цифровых информационно-коммуникационных технологий.
16. Концепция деятельности Народно-освободительной армии Китая в информационном пространстве.
17. Концепции информационных операций Вооруженных сил США.
18. Концепции информационных операций в странах Ближнего Востока.
19. Концепции информационных операций в странах Азиатско-Тихоокеанского региона.
20. Гибридная война: миф или реальность — теория или практика.
21. Использование информационных технологий в противоправных целях.
22. Кибертерроризм — актуальная проблема современных международных отношений.
23. Применение общих принципов международного права к борьбе в информационной сфере. Международное право вооруженных конфликтов и его применимость к

действиям в информационной сфере. Взгляд из США, Китая и других зарубежных стран.
24. Позиция Китая по вопросу применения права международных конфликтов к информационной сфере.
25. Позиция США по вопросу применения права международных конфликтов к информационной сфере.
26. Позиция стран Ближнего Востока по вопросу применения права международных конфликтов к информационной сфере.
27. Позиция стран Азиатско-Тихоокеанского региона по вопросу применения права международных конфликтов к информационной сфере.
28. Основополагающие документы, регулирующие государственную политику Китая в области международной информационной безопасности.
29. Эволюция подходов США к обеспечению международной информационной безопасности.
30. Национальная киберстратегия США.
31. Национальная киберстратегия Китая.
32. Национальная киберстратегия Ирана.
33. Национальная киберстратегия Японии.
34. Национальная киберстратегия Индии.
35. Национальная киберстратегия Великобритании.
36. Взаимодействие США по вопросу обеспечения международной информационной безопасности с другими субъектами международных отношений.
37. Сотрудничество в области международной информационной безопасности в рамках ШОС. БРИКС как площадка международного сотрудничества в сфере информационной безопасности.
38. Деятельность НАТО в сфере обеспечения международной информационной безопасности.

Критерии оценивания студента на зачете

Оценка	Критерии
«Отлично» (30 баллов)	1. Студент исчерпывающе излагает материал, даёт правильное определение ключевых понятий, приводит примеры; 2. не допускает ошибок; 3. ответ структурирован; 4. высказывает и обосновывает собственные суждения и взгляды на проблему; 5. даёт правильные ответы на дополнительные вопросы.
«Хорошо» (20 баллов)	1. Студент хорошо излагает материал, даёт правильное определение ключевых понятий, приводит некоторые примеры; 2. допускает 1-2 ошибки; 3. ответ структурирован; 4. Студент высказывает собственные суждения и взгляды на проблему; 5. Студент даёт правильные ответы на дополнительные вопросы.
«Удовлетворительно» (10 баллов)	1. Студент неполно излагает материал, допускает неточности при определении ключевых понятий, приводит недостаточно примеров; 2. допускает несколько ошибок; 3. ответ слабо структурирован; 4. не умеет достаточно глубоко и доказательно обосновать свои суждения и взгляды на проблему;

	5. допускает некоторые ошибки в ответах на дополнительные вопросы.
«Неудовлетворительно» (0 баллов)	1. Студент обнаруживает незнание (либо же поверхностное знание) материала, допускает ошибки при определении ключевых понятий, не способен привести свои примеры; 2. Допускает серьезные ошибки; 3. ответ не структурирован; 4. не способен высказывать и обосновывать собственные суждения и взгляды на проблему; 5. не отвечает на дополнительные вопросы.

Диагностическая работа (Контроль формирования компетенций)

Формируемая ПК	Индикаторы компетенции	Вопросы, задания	Правильные ответы
ПК-5 Владеет методами разрешения политических конфликтов, организации политической социализации молодежи, политической мобилизации масс, с использованием технологий и каналов массовой коммуникации и средств массовой информации	ИДК ПК 5.1 Собирает, обрабатывает, анализирует, интерпретирует документальные, печатные, телевизионные и ИНТЕРНЕТ источники с целью формирования взгляда на существующую в регионе социально-политическую ситуацию	1. Дайте определение понятию «киберпространство».	Электронная (включая фотоэлектронные и пр.) среда, в (посредством) которой информация создаётся, передаётся, принимается, хранится, обрабатывается и уничтожается.
		2. Дайте определение понятию «киберсилы».	Киберсилы - кибератаки, организованные для проведения кибероперацій.
		3. Дайте определение понятию «киберэксфильтрация» .	Тип кибероперации, связанный с копированием или изъятием каких-либо данных.
		4. Дайте определение понятию «кибероборона».	Организованная совокупность средств и действий для защиты, смягчения и эффективного восстановления дот вражедных воздействий кибератак.
		5. Что такое кибертерроризм?	Политически или идеологически мотивированное использование ИТ-технологий для проведения атак на системы управления объектами жизнеобеспечения, компьютерные системы, популярные информационные ресурсы и т. п. с целью дестабилизировать обстановку в регионе или в стране в плане безопасности, причинить серьезные разрушительные последствия для критически важных инфраструктур и/или вызвать панику и посеять страх среди гражданского населения.
		6. Дайте определение понятию «киберугроза»	Обнаруженная или установленная угроза использования

			киберуязвимости
		7. Дайте определение понятию «цифровая дипломатия».	**Цифровая (электронная) дипломатия**) — использование возможностей сети интернет и информационно-коммуникационных технологий (ИКТ) для решения дипломатических задач.
		8. Что такое DDoS-атака?	DDoS-атаки, или «отказ в обслуживании» - кибератака, при которой когда заражённых устройств объединяются в ботнеты и начинают одновременно посылать сигналы на какой-либо объект, систему, сайт, сеть и т.д., в результате чего последние не выдерживают нагрузки и «отказывают».
		9. Дайте определение понятию «киберконфликт»	Напряженная ситуация между и/или среди государств и/или политически организованных групп, при которой враждебные (нежелательные) кибератаки провоцируют (приводят) к ответным действиям.
		10. Дайте определение понятию «средства киберсдерживания»	Признанный механизм, который считается действенным для препятствования киберконфликту, или угрожающей деятельности в киберпространстве.
		11. Какая из инициатив в области обеспечения МИБ принадлежит США? a) Глобальная инициатива по безопасности данных (2020) b) Программа действий по продвижению ответственного поведения государств в киберпространстве (2020) c) Инициатива по борьбе с вымогателями (2021) d) Парижский призыв к доверию и безопасности в киберпространстве (2018)	b) Программа действий по продвижению ответственного поведения государств в киберпространстве (2020)
		12. Какая из инициатив	a) Глобальная инициатива по

		в области обеспечения МИБ принадлежит Китаю? a) Глобальная инициатива по безопасности данных (2020) b) Программа действий по продвижению ответственного поведения государств в киберпространстве (2020) c) Инициатива по борьбе с вымогателями (2021) d) Парижский призыв к доверию и безопасности в киберпространстве (2018)	безопасности данных (2020)
		13. В стратегии кибербезопасности Японии обозначены следующие ключевые принципы: a) обеспечение свободного обмена информацией; b) обеспечение новых мер в ответ на то, что риски становятся более серьезными; c) принятие адекватных мер в отношении киберугроз на основании оценки рисков; d) принятие мер и взаимодействие с другими государствами на основании их собственной социальной ответственности. e) Всё вышеперечисленное	e) Всё вышеперечисленное
		14. Кибербразведка это a) сбор и обработка ценной информации с использованием	d) a) и b)

		кибероперaций; b) сбор ценной информации о кибератакивах другого субъекта/объекта. c) свойство киберобъекта, которое в потенциале может быть использовано для проведения кибероперации. d) a) и b)	
		15. Какие существуют виды кибератак? a) Фишинг b) Троян c) DDoS-атака d) Ботнет e) Backdoor. f) Черви g) Классические файловые вирусы h) Вирусы-вымогатели i) Всё вышеперечисленное	i) Всё вышеперечисленное
	ИДК ПК 5.2 Определяет стадии реально существующих политических конфликтов в онлайн и киберпространстве, в том числе прямо или косвенно связанных с национальными проблемами, предлагает пути их разрешения	1. Назовите основных бенефициаров переговорного процесса по вопросу МИБ на международном уровне	Россия, США
		2. Какая структура в США отвечает за проведение кибероперaций и достижения военно-политических целей в киберпространстве?	Киберкомандование США
		3. Что такое «Великий Китайский файрвол»?	Совокупность IT-систем и организационных мероприятий с целью контроля интернет-трафика на границе с КНР. Важнейшая функция состоит в блокировке доступа к запрещенным правительством КНР данным и онлайн-сервисам
		4. Американский бывший сотрудник ЦРУ и Агентства национальной безопасности, США.	Эдвард Сноуден.

		которые передал газетам The Guardian и The Washington Post секретную информацию АНБ, касающуюся тотальной слежки американских спецслужб.	
		5. Перечислите правительственные инициативы в сфере обеспечения МИБ	«Парижский призыв к доверию и безопасности в киберпространстве» (Франция), «Женевский диалог об ответственном поведении в киберпространстве» (Швейцария)
		6. Основной нормативно-правовой акт, регулирующий сферу интернет-безопасности КНР.	Закон об интернет-безопасности КНР.
		7. Перечислите основные Российские инициативы в области международной информационной безопасности	Концепция Конвенции ООН об обеспечении международной информационной безопасности (2021 г.) Правила поведения в области обеспечения международной информационной безопасности (Письмо постоянных представителей Казахстана, Китая, Кыргызстана, Российской Федерации, Таджикистана и Узбекистана при Организации Объединенных Наций от 9 января 2015 года на имя Генерального секретаря) Проект Конвенции Организации Объединенных Наций о сотрудничестве в сфере противодействия информационной преступности от 11 октября 2017 года
		8. Подразделение Народно-освободительной армии Китая, базирующееся в Шанхае, отвечает за проведение военных операций в области компьютерных сетей.	Подразделение 61398 Народно-освободительной армии Ктиая
		9. Дайте определение понятию «кибероборона»	Организованная совокупность средств и действий для защиты, смягчения и эффективного восстановления от

			враждебных воздействий кибератак.
		10. Дайте определение понятию «кибервойна»	Высшая степень киберконфликта между или среди государств, во время которой государства предпринимают кибератаки против киберинфраструктур противника, е как часть военной кампании
		11. Первая в истории кибератака, приведшая к физическому разрушению критической инфраструктуры: a) Кибератака вируса Stuxnet на иранский завод по обогащению урана в г. Нетенз b) Кибератака Not-Petya c) кибератака вре доносного ПО на американскую трубопроводную систему Colonial Pipeline	a) Кибератака вируса Stuxnet на иранский завод по обогащению урана в г. Нетенз
		12. Какие страны обозначены в качестве угроз в Национальной стратегии кибербезопасности США 2023г.:: a) Россия, Китай, Иран, Северная Корея; b) Албания, Греция, Македония c) Северная Корея, Ирак, Ливия d) Канада, Франция, германия	a) Россия, Китай, Иран
		13. В соответствии с Соглашением между правительствами государств - членов ШОС о сотрудничестве в области обеспечения международной информационной безопасности (Екатеринбург, 16 июня 2009 г.) основными угрозами в	g) Всё вышеперечисленное

		области МИБ признаны: a) разработка и применение информационного оружия, подготовка и ведение информационной войны; b) информационный терроризм; c) информационная преступность; d) использование доминирующего положения в информационном пространстве в ущерб интересам и безопасности других государств; e) распространение информации, наносящей вред общественно-политической и социально-экономической системам, духовной, нравственной и культурной среде других государств; f) угрозы безопасному, стабильному функционированию глобальных и национальных информационных инфраструктур, имеющие природный и (пли) техногенный характер. g) Всё вышеперечисленное	
		14. В рамках каких международных организаций Россия продвигает инициативы в области МИБ: a) ООН, ШОС, СНГ, ОДКБ, БРИКС, ОБСЕ, АСЕАН b) НАТО, ШОС,	a) ООН, ШОС, СНГ, ОДКБ, БРИКС, ОБСЕ, АСЕАН

		ACEAH, AUKUS, QUAD c) БРИКС, G20, ООН, СНГ d) G7, ООН, ОДКБ, АСЕАН	
		15. Международная организация, в рамках которой проходит ключевой переговорный процесс по вопросу обеспечения МИБ: a) ШОС b) БРИКС c) ООН d) ОДКБ e) ОБСЕ	c) ООН

Разработчик:

Старший преподаватель, к.и.н. С.А. Себекин

Программа составлена в соответствии с требованиями ФГОС ВО по направлению и профилю подготовки 41.03.04 Политология с изменениями и дополнениями от 8.02.2021 г.

Программа рассмотрена на заседании кафедры политологии, истории и регионоведения
Протокол № 6 от «01» апреля 2024 г.

Зав. кафедрой _____Ю.А. Зуляр

Настоящая программа, не может быть воспроизведена ни в какой форме без предварительного письменного разрешения кафедры-разработчика программы