Приложение 7 ОП ВО

Федеральное государственное бюджетное образовательное учреждение высшего образования
«РОССИЙСКАЯ АКАДЕМИЯ НАРОДНОГО ХОЗЯЙСТВА И ГОСУДАРСТВЕННОЙ СЛУЖБЫ ПРИ ПРЕЗИДЕНТЕ РОССИЙСКОЙ ФЕДЕРАЦИИ»

СЕВЕРО-ЗАПАДНЫЙ ИНСТИТУТ УПРАВЛЕНИЯ- филиал РАНХиГС

КАФЕДРА МЕЖДУНАРОДНЫХ ОТНОШЕНИЙ

Утверждено
Директором СЗИУ РАНХиГС
Хлутковым А.Д.

ПРОГРАММА МАГИСТРАТУРЫ

Мировая политика
(наименование образовательной программы)

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ,
реализуемой без применения электронного (онлайн) курса

Б1.О.03 «Международная информационная безопасность: теория и практика» / International information security: theory and practice

41.04.05 **«Международные отношения»**
(код, наименование направления подготовки/специальности)

очная
(форма обучения)

Год набора 2023

Санкт-Петербург, 2023 г.

Автор-составитель:
Доктор политических наук, профессор,
профессор кафедры международных отношений Н.А. Баранов

Заведующий кафедрой международных отношений:
Кандидат исторических наук, доцент М.А. Буланакова

РПД Б1.О.03 «Международная информационная безопасность: теория и практика» / International information security: theory and practice в новой редакции одобрена на заседании кафедры международных отношений исследований. Протокол от 30 июня 2022 г. № 13.

СОДЕРЖАНИЕ

Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения программы

1.1. Дисциплина Б1.О.03 «Международная информационная безопасность: теория и практика» / International information security: theory and practice обеспечивает овладение следующими компетенциями:

Код компетенции	Наименование компетенции	Код этапа освоения компетенции	Наименование компонента компетенции
УК-4	Способен применять современные коммуникативные технологии, в том числе на иностранном(ых) языке(ах), для академического и профессионального взаимодействия	**УК-4.1**	Способен устанавливать и развивать профессиональные контакты в соответствии с потребностями совместной деятельности, включать в обмен информацией и вырабатывать единую стратегии взаимодействия.
ОПК-1	Способен выстраивать профессиональную коммуникацию на государственном языке Российской Федерации и иностранном(ых) языке(ах) по профилю деятельности в мультикультурной среде на основе применения различных коммуникативных технологий с учетом специфики деловой и духовной культуры России и зарубежных стран	**ОПК-1.1**	Способен на знание основ профессиональной коммуникации с использованием иностранного языка, применение иностранного языка для решения задач профессионального развития.
ОПК-2	Способен осуществлять поиск и применять перспективные информационно-коммуникационные технологии и программные средства для комплексной постановки и решения задач профессиональной деятельности	**ОПК-2.1**	Способен привлекать информационные технологии и использовать их в реализации профессиональных задач.
ОПК-5	Способен выстраивать стратегию по продвижению публикаций по профилю деятельности в средствах	**ОПК-5.2**	Способен формировать умения собирать, обрабатывать и анализировать материалы СМИ.

	массовой информации на основе базовых принципов медиаменеджмента		
ОПК-7	Способен самостоятельно выстраивать стратегии представления результатов своей профессиональной деятельности, в том числе в публичном формате, на основе подбора соответствующих информационно-коммуникативных технологий и каналов распространения информации	**ОПК-7.2**	Способен вести дискуссии с применением различных информационных технологий для достижения задач профессиональной коммуникации.

1.2. В результате освоения дисциплины у студентов должны быть сформированы:

ОТФ/ТФ	*Код компонента компетенции*	*Результаты обучения*
	УК-4.1	*На уровне знаний:* - знание основ профессиональной коммуникации с использованием иностранного языка, а также владение представлениями в области психология общения; - риторических аспектов устной и письменной коммуникации на русском языке; иметь представление о качествах хорошей речи на русском языке; - риторических аспектов устной и письменной коммуникации на иностранном языке; иметь представление о качествах хорошей речи и приемах речевого воздействия на иностранном языке.
		На уровне умений:- анализировать языковой материал текстов на русском и иностранном языке в нормативном аспекте и вносить необходимые исправления нормативного характера. - производить редакторскую правку текстов научного и официально-делового стилей речи на русском и иностранном языке.
		На уровне навыков: создание на русском и иностранном языке письменных и устных текстов научного и официально-делового стилей речи для обеспечения профессиональной деятельности с использованием риторических приемов.
	ОПК-1.1	*На уровне знаний:* - методов повышения взаимопонимания при осуществлении коммуникации; - письменного и разговорного профессионально ориентированного иностранного языка;

ОТФ/ТФ	*Код компонента компетенции*	*Результаты обучения*
		- методов разработки долговременных программ языковой практики; - стилевых черт, языковых особенностей, особенностей жанровой реализации изучаемого иностранного языка.
		На уровне умений:- использовать социальные стратегии, подходящие для достижения коммуникационных целей в процессе межкультурного взаимодействия; - понять и проанализировать иностранный научный, статистический, аналитический и др. материалы; - готовить документы, вести деловую переписку на русском и иностранном языке - выстраивать собственное вербальное и невербальное поведение в соответствии с нормами культуры русского и изучаемого языка; - моделировать в профессиональной деятельности ситуации, которые бы требовали применения навыков устной и письменной речи изучаемого иностранного языка.
		На уровне навыков: - делового общения, ведения переговоров, дискуссий в области своей профессиональной деятельности, восприятия и анализа большого объема информации - строить высказывание, адекватно отражающее культурные ценности языка; - адаптации собственного поведения к стандартам русской и иноязычной культуры.
	ОПК-2.1	*На уровне знаний:*- особенностей работы с современными информационно-коммуникационными технологиями; - основных возможностей привлечения информационных технологий в коммуникативной международной практике.
		На уровне умений: - самостоятельно приобретать знания с помощью информационных технологий.
		На уровне навыков: - использования в практической деятельности новые знания и умения, в том числе в новых областях знаний, полученных на основе использования информационно-коммуникационных технологий.
	ОПК-5.2	*На уровне знаний:* - основных категорий и понятий информационно-аналитической работы, системы современных средств массовой информации.
		На уровне умений: - проводить анализ информационных ресурсов разного типа, составлять аналитические карты, информационные записки, обзоры прессы, собирать разнородную информацию.
		На уровне навыков: - анализа средств массовой информации, работы с публицистической информацией; - составления информационных обзоров, аналитических

ОТФ/ТФ	*Код компонента компетенции*	*Результаты обучения*
		информационных дайджестов, сравнения национальной прессы, написания научных статей
	ОПК-7.3	*На уровне знаний:* - основных структурных особенностей иностранного языка и правила сочетаемости элементов на фонетическом, морфологическом и грамматическом уровнях; - основных лексических единиц в рамках изучаемой дисциплины; - особенностей и отличий формального и неформального стилей общения.
		На уровне умений: - выбирать адекватные, с точки зрения поставленных профессиональных задач, языковые средства; - различать общий контекст ситуации; - использовать языковые средства, соответствующие разным формам общения; - логично выражать свои мысли.
		На уровне навыков: - ведения публичных дискуссий по различным каналам распространения информации с применением современных информационно-коммуникационных технологий.

2. Объем и место дисциплины Б1.О.03 «Международная информационная безопасность: теория и практика» / International information security: theory and practice в структуре ОП ВО

Объем дисциплины. Объем дисциплины составляет 3 зачетные единицы, 108 академических часов / 81 астрономический час.

Вид работы	Трудоемкость (в академ.часах/астрон.часах)
Общая трудоемкость	108/81
Контактная работа	36/27
Лекции	12/9
Практические занятия	24/18
Самостоятельная работа	72/54
Контроль	-
Виды текущего контроля	Устный опрос, доклад
Вид промежуточного контроля	Зачет с оценкой

Место дисциплины в структуре ОП ВО

Б1.О.03Дисциплина «Международная информационная безопасность: теория и практика» / International information security: theory and practice включена в обязательную

часть учебного плана по направлению 41.04.05 «Международные отношения» магистерской программы «Мировая политика».

Дисциплина реализуется в 1 семестре параллельно изучению следующих дисциплин: «Анализ международных ситуаций», «Политический консалтинг», «Конфликты в современном мире», «Основные траектории эволюции мирового порядка в XXI веке».

Доступ к системе дистанционных образовательных технологий осуществляется каждым обучающимся самостоятельно с любого устройства на портале: https://lms.ranepa.ru/. Пароль и логин к личному кабинету / профилю предоставляется студенту в деканате.

Все формы текущего контроля, проводимые в системе дистанционного обучения, оцениваются в системе дистанционного обучения. Доступ к видео и материалам лекций предоставляется в течение всего семестра. Доступ к каждому виду работ и количество попыток на выполнение задания предоставляется на ограниченное время согласно регламенту дисциплины, опубликованному в СДО. Преподаватель оценивает выполненные обучающимся работы не позднее 10 рабочих дней после окончания срока выполнения.

3. Содержание и структура дисциплины Б1.О.03 «Международная информационная безопасность: теория и практика» / International information security: theory and practice

3.1.Структура дисциплины

Очная форма обучения

№ п/п	Наименование тем (разделов),	Объем дисциплины, час.						Форма текущего контроля успеваемости, промежут. аттестации
		Всего	Контактная работа обучающихся с преподавателем по видам учебных занятий				СР	
			Л/ ДОТ	ЛР /Д ОТ	ПЗ/ ДОТ	КСР*		
Тема 1	Информационная безопасность как следствие трансформации информационных коммуникаций	20	2		4		12	УО, Д
Тема 2	Политико-правовой режим глобальной информационной безопасности	20	2		4		12	УО, Д
Тема 3	Угрозы международной информационной безопасности	16	**2**		4		12	УО, Д
Тема 4	Информационная война в системе международных отношений	20	2		4		12	УО, Р
Тема 5	Цифровые технологии в мировой политике	16	**2**		4		12	УО, Д, Э
Тема 6	Государственная политика Российской Федерации в области международной	16	2		4		12	УО

	информационной безопасности							
Промежуточная аттестация								Зачет с оценкой
Всего:		**108 /81**	**12/ 9**		**24/ 16**	**2/1,5**	**72/54**	

УО - устный опрос, Д- доклад, Р – реферативный обзор, Э - эссе
* в объем не включается

Содержание дисциплины

Тема 1. Информационная безопасность как следствие трансформации информационных коммуникаций

Информация и информационное общество. Информационная революция. Теория информационного общества как методология анализа политических процессов. Современные характеристики информационного общества: политические аспекты. Информационные аспекты современной мировой политики. Технологический прогресс и трансформация мировой политики. Информационная безопасность: национальное и глобальное в мировой политике. Информационная безопасность в годы Первой и Второй мировых войн. Приоритеты трансформации информационных коммуникаций второй половины XX века. Национальный и международный информационный ресурс коммуникационных технологий телевещания. Внедрение спутниковой коммуникации в международную ин6формационную индустрию телевидения, радио и телефонии. Панорама международного иновещания на рубеже тысячелетия. Цифровая технологическая революция в традиционных для XX века информационных коммуникациях. Цифровой информационно-коммуникационный прорыв США. Формирование глобальной цифровой инфраструктуры в контексте обеспечения международной информационной безопасности.

Тема 2. Политико-правовой режим глобальной информационной безопасности

Информационно-коммуникационные технологии и международная деятельность. Информационное оружие и международная безопасность. Международное сотрудничество в сфере информации. Деятельность Группы правительственных экспертов ООН. Глобальный технологический трансфер. Проблема «цифрового разрыва» в рамках информационного общества. Всемирный Саммит по информационному обществу, Женева, 12 декабря 2003 г. Построение информационного общества — глобальная задача в новом тысячелетии. Доклад рабочей группы по управлению Интернетом, июнь 2005 г. Всемирный Саммит по информационному обществу, Тунис, 16–18 ноября 2005 г. Тунисское обязательство. Тунисская программа для информационного общества. Форум по вопросам управления Интернетом.

Тема 3. Угрозы международной информационной безопасности

Перечень угроз информационной безопасности в повестке международных организаций. Международная безопасность и государственный суверенитет в эпоху цифровых ИКТ. Использование ИКТ в преступных целях. Кибертерроризм как проблема современных международных отношений. Политика в области информационной безопасности США и НАТО. Институты НАТО, отвечающие за кибербезопасность. Центр передового опыта по совместной защите от киберугроз НАТО. Центр стратегических коммуникаций НАТО. Европейский центр передового опыта по противодействию гибридным угрозам. Концепции информационной безопасности ведущих стран мира: США, Китая, Франции, Германии, Великобритании, Индии, Бразилии. США и международная кибербезопасность. Национальная стратегия кибербезопасности США. Принципы Стратегии национальной безопасности США.

Тема 4. Информационная война в системе международных отношений

Причины появления феномена «информационной войны». Информационные войны как войны нового поколения. Информационно-психологическое воздействие. Характеристика составляющих информационной войны. Информационная пропаганда.

Технологии политической пропаганды в условиях цифровизации. Информационная агрессия. Признаки информационных войн. Главная цель информационной войны. Особенности информационной борьбы. Информационное оружие. Основные технологии ведения информационных войн. Манипулятивный потенциал глобальных СМИ. Каналы и средства ведения информационных войн. Гибридные войны: особенности информационного воздействия. Теория и практика гибридных войн и «цветных революций» в контексте применения ИКТ.

Тема 5. Цифровые технологии в мировой политике

Особенности использования цифровых технологий во внешнеполитическом процессе. Цифровая (электронная) дипломатия. Исследования использования социальных сетей в дипломатической практике. Электронная дипломатия США. Основные проекты электронной дипломатии Госдепа США. Профессиональная служебная сеть американских дипломатов. Виртуальный студенческий сервис по международной проблематике. Узел социальных сетей. Офис сетевой активности. Центр электронных коммуникаций. Глобальная сеть для всех загранучреждений США. Программа «Эффект виртуального присутствия». Технологии Big Data и микротаргеттинга. Информационно-аналитические службы России: «Медиалогия», «Призма», «ГЛАСС», «Демон Лапласа» против террористов. Геоинформационные системы по глобальным техногенным, природогенным и иным чрезвычайным ситуациям. Биометрические технологии в консульской службе. Электронные визы.

Тема 6. Государственная политика Российской Федерации в области международной информационной безопасности

Основные угрозы и факторы, влияющие на обеспечение международной информационной безопасности. Основные принципы обеспечения международной информационной безопасности. Основные меры предотвращения конфликтов в информационном пространстве. Основные меры противодействия использованию информационного пространства в террористических целях. Основные меры противодействия использованию информационно-коммуникационных технологий в преступных целях. Меры укрепления доверия в области обеспечения международной информационной безопасности. Национальные интересы России в информационной сфере. Основные информационные угрозы и состояние информационной безопасности. Стратегические цели и основные направления обеспечения информационной безопасности. Международные форумы по кибербезопасности. Работа Группы правительственных экспертов ООН (2004-2017). Дипломатические инициативы России по обеспечению МИБ.

Topic 1. Information security as a consequence of the transformation of information communications

Information and information society. The information revolution. The theory of information society as a methodology for analyzing political processes. Modern characteristics of the information society: political aspects. Information aspects of modern world politics. Technological progress and transformation of world politics. Information security: national and global in world politics. Information security during the First and Second World Wars. Priorities for the transformation of information communications in the second half of the twentieth century. National and international information resource of communication technologies of broadcasting. The introduction of satellite communications into the international information industry of television, radio and telephony. Panorama of international foreign broadcasting at the turn of the millennium. The digital technological revolution in traditional information communications for the twentieth century. The digital information and communication breakthrough of the USA. The formation of a global digital infrastructure in the context of ensuring international information security.

Topic 2. The political and legal regime of global information security

Information and communication technologies and international activities. Information

weapons and international security. International cooperation in the field of information. Activities of the UN Group of Governmental Experts. Global technology transfer. The problem of the "digital divide" within the information society. World Summit on the Information Society, Geneva, December 12, 2003. Building an information society is a global challenge in the new millennium. Report of the Internet Governance Working Group, June 2005 World Summit on the Information Society, Tunis, November 16-18, 2005 The Tunisian commitment. Tunisian Program for the Information Society. Internet Governance Forum.

Topic 3. Threats to international information security

The list of threats to information security is on the agenda of international organizations. International security and State sovereignty in the era of digital ICT. The use of ICT for criminal purposes. Cyberterrorism as a problem of modern international relations. Information security policy of the United States and NATO. NATO institutions responsible for cybersecurity. The Center of Excellence for Joint Protection against Cyber Threats of NATO. The NATO Strategic Communications Center. The European Center of Excellence for Countering Hybrid Threats. Information security concepts of the leading countries of the world: USA, China, France, Germany, Great Britain, India, Brazil. The United States and international cybersecurity. The US National Cybersecurity Strategy. Principles of the US National Security Strategy.

Topic 4. Information warfare in the system of international relations

The causes of the phenomenon of "information warfare". Information wars as wars of a new generation. Informational and psychological impact. Characteristics of the components of the information war. Information propaganda. Technologies of political propaganda in the context of digitalization. Information aggression. Signs of information wars. The main purpose of the information war. Features of information warfare. Information weapons. The main technologies of information warfare. The manipulative potential of global media. Channels and means of conducting information wars. Hybrid wars: features of information impact. Theory and practice of hybrid wars and "color revolutions" in the context of the use of ICT.

Topic 5. Digital technologies in world politics

Features of the use of digital technologies in the foreign policy process. Digital (electronic) diplomacy. Research on the use of social networks in diplomatic practice. Electronic diplomacy of the USA. The main projects of electronic diplomacy of the US State Department. A professional service network of American diplomats. Virtual student service on international issues. A social media node. Office of network activity. Electronic Communications Center. A global network for all U.S. foreign missions. The program "Virtual presence effect". Big Data and microtargeting technologies. Information and analytical services of Russia: "Medialogy", "Prism", "GLASS", "Laplace's Demon" against terrorists. Geoinformation systems for global man-made, natural and other emergency situations. Biometric technologies in the consular service. Electronic visas.

Topic 6. State policy of the Russian Federation in the field of international information security

The main threats and factors affecting international information security. The basic principles of ensuring international information security. The main measures to prevent conflicts in the information space. The main measures to counter the use of information space for terrorist purposes. The main measures to counter the use of information and communication technologies for criminal purposes. Confidence-building measures in the field of international information security. Russia's national interests in the information sphere. The main information threats and the state of information security. Strategic goals and main directions of information security. International cybersecurity forums. The work of the UN Group of Governmental Experts (2004-2017). Russia's diplomatic initiatives to ensure the IIB.

4. **Материалы текущего контроля успеваемости обучающихся и фонд оценочных средств промежуточной аттестации по дисциплине Б1.О.03 «Международная информационная безопасность: теория и практика» / International information security: theory and practice**

4.1. Формы и методы текущего контроля успеваемости, обучающихся и промежуточной аттестации.

4.1.1. В ходе реализации дисциплины «Внешнеполитический процесс и современная внешнеполитическая стратегия России**» используются следующие методы текущего контроля успеваемости обучающихся:**

– при проведении занятий лекционного типа: устный опрос

– при проведении занятий семинарского типа: устный опрос, доклад, контрольная работа, реферат, эссе.

Тема и/или раздел	*Методы текущего контроля успеваемости*
Тема 1. Информационная безопасность как следствие трансформации информационных коммуникаций	УО, Д
Тема 2. Политико-правовой режим глобальной информационной безопасности	УО, Д
Тема 3. Угрозы международной информационной безопасности	УО, Д
Тема 4. Информационная война в системе международных отношений	УО, Р
Тема 5. Цифровые технологии в мировой политике	УО, Д, Э
Тема 6. Государственная политика Российской Федерации в области международной информационной безопасности	УО

4.2. Типовые материалы текущего контроля успеваемости обучающихся

Типовые оценочные материалы по темам 1-6

Примеры вопросов устного опроса

1. Хартия глобального информационного общества – основные положения и значение документа.
2. Охарактеризуйте субъекты глобального информационного общества - функции, методы, каналы, преимущества, недостатки:

- государства;
- крупный бизнес;
- транснациональные медиакорпорации;
- гражданские институты, некоммерческие и неправительственные организации;
- транснациональные социальные сети;
- индивидуумы.

3. Приведите примеры осуществления государствами основных информационных государственных стратегий – экстравертной и интравертной
4. В чем заключается конкуренция в сфере глобальных информационных потоков?
5. Характеристика информации: содержание и форма.
6. Основные жанры международной информации: новости, политический комментарий, публицистика и документальное кино.
7. Основные положения Декларации тысячелетия Организации Объединенных Наций от 8 сентября 2000 года, касающихся информационного общества.
8. Всемирный по Женевскому саммит по информационному обществу 2003 г.: принятые документы и международное значение.
9. Тунисская программа для информационного общества 2005 г.: характеристика документа.
10. Тунисское обязательство 2005 г.: содержание и вектор развития

информационного развития.

11. Доклад рабочей группы по управлению Интернетом: рабочее определение понятия управление Интернетом и аспектов государственной политики, касающихся управления Интернетом.

12. Рекомендации рабочей группы по управлению Интернетом в отношении механизмов управления Всемирной сетью.

13. Охарактеризуйте деятельность Международной корпорации по распределению адресов и номеров (International Corporation for Assigned Names and Number – ICANN).

14. Форум по вопросам управления Интернетом: задачи, состав участников, деятельность.

15. Участие США в международной деятельности по обеспечению кибербезопасности.

16. Оказание США помощи другим странам в обеспечении кибербезопасности.

17. Институты НАТО, отвечающие за кибербезопасность.

18. Деятельность Центра передового опыта по совместной защите от киберугроз, базирующегося в Таллине.

19. Кибербезопасность в странах Европы.

20. Киберстратегия Министерства внутренней безопасности США.

21. Национальная стратегия кибербезопасности США 2018 г.

Примерный перечень докладов:

1. Основные направления информационного противоборства.
2. Обеспечение безопасности открытых информационных сетей.
3. Информационная безопасность бизнеса через Интернет - B2B, B2C, B2G.
4. Информационно-психологическая безопасность.
5. Характеристика и виды информационного оружия.
6. Факторы, способствующие использованию информационного оружия.
7. Характеристика кибертерроризма.
8. Привести конкретные примеры кибертерроризма.
9. Информационная инфраструктура и ее особенности.
10. Меры противодействия информационному терроризму.
11. Психологический и экономический аспекты кибертерроризма.
12. Характеристика целей, подвергаемых атакам кибертерроризма.
13. Интересы личности, общества и государства в информационной сфере.
14. Угрозы международной информационной безопасности.
15. Международные организации и системы международного управления как объекты информационной безопасности.
16. Субъекты информационного воздействия.
17. Источники угроз информационной безопасности.
18. История появления информационных войн.
19. Информационное противоборство в Первую мировую войну.
20. Информационное противоборство во Второй мировой войне.
21. Информационное противоборство в годы «холодной войны».
22. Информационное противоборство и информационная война: соотношение понятий.
23. Информационная война и информационно-психологическая война: соотношение понятий.
24. Цель информационной войны и ее особенности.
25. Информационное оружие: характеристика и его использование в информационной войне.
26. Отличий информационной войны от обычной.
27. Механизм информационно-психологической борьбы.

28. Риски и угрозы виртуализации: нарушение адекватности восприятия реальности.
29. Риски и угрозы виртуализации: формирование медиазависимости.
30. Риски и угрозы виртуализации: увеличение возможностей для обмана и манипуляции сознанием.
31. Риски и угрозы виртуализации: распространение негативного медиаконтента.
32. Риски и угрозы виртуализации: деструктивные действия в киберпространстве.

Темы эссе

Эссе – самостоятельная работа, связанная с изложением собственной позиции студента относительно предложенной темы не менее, чем на 4 страницах (текст Time News Roman, 14 пт, 1,5 интервал).

1. Какие существуют угрозы личности, обществу и государству в информационном пространстве и какова их приоритетность?
2. Какими должны быть, по вашему мнению, основные принципы управления всемирной сетью?
3. Почему США доминируют в киберпространстве и какова перспектива дальнейшего его развития?
4. В чем заключается сущность проблемы «цифрового разрыва» в рамках информационного общества?
5. Чем занимается Группа правительственных экспертов ООН и каковы результаты ее работы?
6. В чем может заключаться международное сотрудничество в сфере информации?
7. В чем заключаются криминальные интересы в информационной сфере?
8. Каковы особенности международного информационного терроризма?
9. Почему хакерские атаки представляют опасность для современной информационной инфраструктуры?
10. Почему средства воздействия на психику относятся к информационному оружию?
11. Охарактеризуйте приемы достижения террористических целей.
12. В чем заключается опасность проявлений кибертерроризма для государства, для бизнеса и для общества?
13. В чем состоит опасность использования террористическими организациями информационных технологий?
14. В чем и почему не совпадают интересы личности, общества и государства в информационной области?
15. Почему средства массовой информации являются приоритетными объектами информационной безопасности?
16. Приведите примеры современных информационных войн и расскажите об их особенностях (Россия и Запад, Россия и США, США и Китай, Россия и Украина и т.д.).
17. В чем заключается американская политика сдерживания России?
18. Чем объясняется новый виток информационной войны США против России?
19. Есть ли разница между информационным вмешательством государства и вмешательством частных лиц в политику другого государства?
20. Какие последствия может иметь информационная война США против России?
21. Ведет ли Россия информационную войну против США и по каким направлениям?

Темы рефератов

1. Реферативный обзор книги Мануэля Кастельса «Информационная эпоха: экономика, общество и культура».
2. Реферативный обзор книги Фрэнка Уэбстера «Теории информационного общества».
3. Реферативный обзор книги Дэниэла Белла «Грядущее постиндустриальное

общество».

4. Реферативный обзор книги Э. Бернайза «Пропаганда».
5. Реферативный обзор книги Г. Лассуэла «Техника пропаганды в мировой войне».
6. Реферативный обзор книги А.М. Цуладзе «Политические манипуляции или покорение толпы».
7. Реферативный обзор книги Г. Почепцова «Психологические/информационные операции как технологии воздействия на массовое сознание в XX веке».
8. Реферативный обзор книги Л. Войтасика «Психология политической пропаганды».
9. Реферативный обзор статьи Ариэля Коэна «Россия и США: новый виток информационной войны».

Оценочные средства	**Показатели оценки**	**Критерии оценки**
Устный опрос	Корректность и полнота ответов	Сложный вопрос: полный, развернутый, обоснованный ответ – 5 Правильный, но не аргументированный ответ – 4 Неверный ответ – 2 Обычный вопрос: полный, развернутый, обоснованный ответ – 5 Правильный, но не аргументированный ответ – 4 Неверный ответ – 2. Простой вопрос: Правильный ответ – 5 Неправильный ответ – 2
Доклад	– соблюдение регламента (15 мин.); – характер источников (более трех источников); – подача материала (презентация); – ответы на вопросы (владение материалом).	Каждый критерий оценки доклада оценивается по пятибалльной шкале
Эссе	– используемые понятия строго соответствуют теме; – умело используются приемы сравнения и обобщения для анализа взаимосвязи понятий и явлений; – изложение ясное и четкое, приводимые доказательства логичны; – приведены соответствующие теме и проблеме примеры.	– **Знание** и понимание теоретического материала, проблематики эссе – 5 – **Умение** анализировать и оценивать информацию, полученную в ходе изучения дисциплины – 4
Реферат	– актуальность проблемы и темы;	**Проверяет умения и навыки** обучающегося в работе с информационными базами и аналитическими материалами; умение

	– полнота и глубина раскрытия основных понятий проблемы; – умение работать с литературой, систематизировать и структурировать материал; – грамотность и культура изложения.	составлять обзоры и прогнозировать деятельность многосторонних международных структур, оценивать эффект реализации стратегий и нормативных документов МО. Обоснование проблемы и источниковой базы - max - 5 структура анализа и полнота раскрытия проблемы - max - 5 соблюдение требований к оформлению, стиль, цитирование max - 5

Typical assessment materials for topics 1-6

Examples of oral survey questions

1. Charter of the Global Information Society – main provisions and significance of the document.
2. Describe the subjects of the global information society - functions, methods, channels, advantages, disadvantages:
- states;
- big business;
- transnational media corporations;
- civil institutions, non-profit and non-governmental organizations;
- transnational social networks;
- individuals.
3. Give examples of the implementation by states of basic informational state strategies - extroverted and introverted
4. What is the competition in the field of global information flows?
5. Characteristics of information: content and form.
6. Main genres of international information: news, political commentary, journalism and documentary films.
7. The main provisions of the United Nations Millennium Declaration of September 8, 2000 regarding the information society.
8. Geneva World Summit on the Information Society 2003: adopted documents and international significance.
9. Tunisian Program for the Information Society 2005: characteristics of the document.
10. Tunisian Commitment 2005: content and vector of information development.
11. Report of the Internet Governance Working Group: Working definition of Internet governance and public policy aspects related to Internet governance.
12. Recommendations of the Internet Governance Working Group regarding mechanisms for governing the World Wide Web.
13. Describe the activities of the International Corporation for Assigned Names and Numbers (ICANN).
14. Forum on Internet governance: objectives, participants, activities.
15. US participation in international cybersecurity activities.
16. Give examples of modern information wars and tell us about their features (Russia and the West, Russia and the USA, the USA and China, Russia and Ukraine, etc.).
17. What is the American policy of containing Russia?
18. What explains the new round of the US information war against Russia?
19. Is there a difference between government information intervention and private interference in the politics of another state?
20. What consequences could the US information war against Russia have?

21. Is Russia waging an information war against the United States and in what areas?

Sample list of reports:
1. Main directions of information warfare.
2. Ensuring the security of open information networks.
3. Information security of business via the Internet - B2B, B2C, B2G.
4. Information and psychological security.
5. Characteristics and types of information weapons.
6. Factors promoting the use of information weapons.
7. Characteristics of cyber terrorism.
8. Give specific examples of cyber terrorism.
9. Information infrastructure and its features.
10. Measures to counter information terrorism.
11. Psychological and economic aspects of cyber terrorism.
12. Characteristics of targets subject to cyberterrorism attacks.
13. Interests of the individual, society and state in the information sphere.
14. Threats to international information security.
15. International organizations and systems of international management as objects of information security.
16. Subjects of information influence.
17. Sources of threats to information security.
18. The history of the emergence of information wars.
19. Information warfare in the First World War.
20. Information warfare in World War II.
21. Information warfare during the Cold War.
22. Information confrontation and information war: the relationship of concepts.
23. Information warfare and information-psychological warfare: the relationship of concepts.
24. The purpose of information warfare and its features.
25. Information weapons: characteristics and their use in information warfare.
26. Differences between information warfare and conventional warfare.
27. Mechanism of information and psychological warfare.
28. Risks and threats of virtualization: violation of the adequacy of the perception of reality.
29. Risks and threats of virtualization: the formation of media dependence.
30. Risks and threats of virtualization: increased opportunities for deception and manipulation of consciousness.
31. Risks and threats of virtualization: dissemination of negative media content.
32. Risks and threats of virtualization: destructive actions in cyberspace.

Essay Topics
An essay is an independent work related to the presentation of the student's own position regarding the proposed topic on at least 4 pages (Text Time News Roman, 14 pt, 1.5 spacing).
1. What threats exist to individuals, society and the state in the information space and what is their priority?
2. What should be, in your opinion, the basic principles of managing the World Wide Web?
3. Why does the United States dominate cyberspace and what are the prospects for its further development?
4. What is the essence of the problem of the "digital divide" within the information society?
5. What does the UN Group of Governmental Experts do and what are the results of its work?
6. What might international cooperation in the field of information consist of?
7. What are the criminal interests in the information sphere?
8. What are the features of international information terrorism?
9. Why are hacker attacks a threat to modern information infrastructure?

10. Why are means of influencing the psyche classified as information weapons?
11. Describe the methods of achieving terrorist goals.
12. What is the danger of cyber terrorism for the state, for business and for society?
13. What is the danger of terrorist organizations using information technology?
14. In what and why do the interests of the individual, society and the state in the information field do not coincide?
15. Why are the media priority objects of information security?
16. Give examples of modern information wars and tell us about their features (Russia and the West, Russia and the USA, the USA and China, Russia and Ukraine, etc.).
17. What is the American policy of containing Russia?
18. What explains the new round of the US information war against Russia?
19. Is there a difference between government information intervention and private interference in the politics of another state?
20. What consequences could the US information war against Russia have?
21. Is Russia waging an information war against the United States and in what areas?

Abstract topics

1. Abstract review of the book "The Information Age: Economy, Society and Culture" by Manuel Castells.
2. Abstract review of Frank Webster's book "Theories of the Information Society."
3. Abstract review of the book "The Coming Post-Industrial Society" by Daniel Bell.
4. Abstract review of the book by E. Bernays "Propaganda".
5. Abstract review of the book by G. Lasswell "Propaganda Techniques in World War."
6. Abstract review of the book by A.M. Tsuladze "Political manipulation or conquering the crowd."
7. Реферативный обзор книги Г. Почепцова «Психологические/информационные операции как технологии воздействия на массовое сознание в XX веке».
8. Реферативный обзор книги Л. Войтасика «Психология политической пропаганды».
9. Реферативный обзор статьи Ариэля Коэна «Россия и США: новый виток информационной войны».

Evaluation tools	**Indicators assessments**	**Criteria assessments**
survey	Correctness and completeness of answers	Difficult question: complete, detailed, reasoned answer – 5 The correct but not reasoned answer is 4 Incorrect answer – 2 Common question: complete, detailed, reasoned answer – 5 The correct but not reasoned answer is 4 Incorrect answer – 2. Simple question: The correct answer is 5 Incorrect answer – 2
Report	compliance with regulations (15 min.); □ nature of sources (more than three sources); □ presentation of material (presentation); answers to questions	Each report evaluation criterion is assessed on a five-point scale

	(mastery of the material).	
essay	□ the concepts used strictly correspond to the topic; □ techniques of comparison and generalization are skillfully used to analyze the relationship of concepts and phenomena; □ the presentation is clear and concise, the evidence provided is logical; examples relevant to the topic and problem are given.	□ Knowledge and understanding of theoretical material, essay topics – 5 Ability to analyze and evaluate information obtained during the study of the discipline – 4
abstract	□ relevance of the problem and topic; - completeness and depth of disclosure of the basic concepts of the problem; □ ability to work with literature, systematize and structure material; literacy and culture of presentation.	Tests the student's skills and abilities in working with information databases and analytical materials; the ability to compile reviews and forecast the activities of multilateral international structures, evaluate the effect of implementing strategies and regulatory documents of the Ministry of Defense. Justification of the problem and source base - max - 5 structure of analysis and completeness of problem disclosure - max - 5 compliance with design requirements, style, citation max - 5

5.1**.** Экзамен проводится с применением следующих методов (средств):
Устный ответ по вопросам зачета.
Промежуточная аттестация проводится в форме: зачет с оценкой.

5.2. Оценочные материалы промежуточной аттестации

Компонент компетенции	*Промежуточный / ключевой индикатор оценивания*	*Критерий оценивания*
УК-4.1	Устанавливает и развивает профессиональные контакты в соответствии с потребностями совместной деятельности, включает в обмен информацию и выработку единой стратегии взаимодействия	Способен устанавливать и развивать профессиональные контакты в соответствии с потребностями совместной деятельности, включать в обмен информацию и выработку единой стратегии взаимодействия
ОПК-1.1	Формирует знания основ профессиональной коммуникации с использованием иностранного языка, применяет иностранный язык для решения задач профессионального развития	Способен формировать знания основ профессиональной коммуникации с использованием иностранного языка, применять иностранный язык для решения задач профессионального развития
ОПК-2.1	Формирует умение привлекать информационные технологии и использовать их в реализации профессиональных задач.	Способен формировать умение привлекать информационные технологии и использовать их в реализации профессиональных задач
ОПК-5.2	Формирует знания о системе международных и национальных СМИ.	Способен использовать умения собирать, обрабатывать и анализировать материалы

	Использует умения собирать, обрабатывать и анализировать материалы СМИ	СМИ
ОПК-7.2	Использует навыки публичных выступлений на русском и иностранном языках	Способен вести дискуссии с применением различных информационных технологий для достижения задач профессиональной коммуникации

Типовые оценочные материалы промежуточной аттестации

Вопросы к зачету с оценкой

1. Субъекты глобального информационного общества.
2. Информационные государственные стратегии.
3. Управление международной информацией.
4. Хартия глобального информационного общества.
5. Информационно-коммуникационные технологии и международная деятельность.
6. Вызовы глобальной технологической революции.
7. Современные ИКТ как инструмент «мягкой силы» государства.
8. «Интернет вещей» и технология блокчэйн в информационном обществе.
9. Подходы России к развитию цифровых технологий в документах стратегического планирования.
10. Интернационализация управления сетью «Интернет».
11. Всемирные саммиты по информационному обществу.
12. Основные принципы управления всемирной сетью.
13. Виртуализация как признак информационного общества.
14. Политические, экономические, социальные и культурные последствия виртуализации.
15. Особенности использования цифровых технологий во внешнеполитическом процессе.
16. Цифровая (электронная) дипломатия.
17. Электронная дипломатия США.
18. Информационно-аналитические службы России
19. Технологии Big Data и микротаргеттинга.
20. Геоинформационные системы по глобальным техногенным, природогенным и иным чрезвычайным ситуациям.
21. Биометрические технологии в консульской службе.
22. Основные направления информационного противоборства.
23. Новые объекты информационной безопасности: безопасность открытых информационных сетей, информационная безопасность бизнеса, информационно-психологическая безопасность.
24. Информационный терроризм.
25. Интересы в информационной сфере.
26. Угрозы международной информационной безопасности.
27. Информационная безопасность в дипломатической практике - национальное и международное измерение.
28. Группа правительственных экспертов ООН.

29. Дипломатические инициативы России по обеспечению международной информационной безопасности.
30. Доктрина информационной безопасности Российской Федерации (2016).
31. Национальная стратегия кибербезопасности США (2018).
32. Объект и субъект информационного противоборства.
33. Информационное оружие.
34. Мониторинг глобального информационного пространства информационно-аналитическими системами США и их союзников.
35. Гибридные войны.
36. Центры информационного противоборства в Европе.

Questions for the test with an assessment

1. Subjects of the global information society.
2. Information state strategies.
3. International information management.
4. The Charter of the Global Information Society.
5. Information and communication technologies and international activities.
6. Challenges of the global technological revolution.
7. Modern ICT as a tool of the "soft power" of the state.
8. The Internet of Things and blockchain technology in the information society.
9. Russia's approaches to the development of digital technologies in strategic planning documents.
10. Internationalization of Internet network management.
11. World Summits on the Information Society.
12. The basic principles of managing the world Wide web.
13. Virtualization as a sign of the information society.
14. Political, economic, social and cultural implications of virtualization.
15. Features of the use of digital technologies in the foreign policy process.
16. Digital (electronic) diplomacy.
17. Electronic diplomacy of the USA.
18. Information and analytical services of Russia
19. Big Data and microtargeting technologies.
20. Geoinformation systems for global man-made, natural and other emergency situations.
21. Biometric technologies in the consular service.
22. The main directions of information warfare.
23. New objects of information security: security of open information networks, business information security, information and psychological security.
24. Information terrorism.
25. Interests in the information sphere.
26. Threats to international information security.
27. Information security in diplomatic practice is a national and international dimension.
28. The UN Group of Governmental Experts.
29. Russia's diplomatic initiatives to ensure international information security.
30. The Information Security Doctrine of the Russian Federation (2016).
31. The National Cybersecurity Strategy of the United States (2018).
32. The object and subject of information warfare.
33. Information weapons.
34. Monitoring of the global information space by the information and analytical systems of the United States and its allies.
35. Hybrid wars.
36. Information warfare centers in Europe.

Шкала оценивания

Оценка результатов производится на основе Положения о текущем контроле успеваемости обучающихся и промежуточной аттестации обегающихся по образовательным программам среднего профессионального и высшего образования в федеральном государственном бюджетном образовательном учреждении высшего образования «Российская академии народною хозяйства и государственной службы при Президенте Российской Федерации», утвержденного Приказом Ректора РАНХиГС при Президенте РФ от 30.01.2018 г. № 02-66 (п.10 раздела 3 (первый абзац) и п.11), а также Решения Ученого совета Северо-западного института управления РАНХиГС при Президенте РФ от 19.06.2018, протокол № 11.

Зачёт/Отлично выставляется в случае, если обучающийся показывает высокий уровень компетентности, знания программного материала, учебной литературы, раскрывает и анализирует проблему с точки зрения различных авторов. Обучающийся показывает не только высокий уровень теоретических знаний, но и видит междисциплинарные связи. Профессионально, грамотно, последовательно, хорошим языком четко излагает материал, аргументированно формулирует выводы. Знает в рамках требований к направлению и профилю подготовки нормативную и практическую базу. На вопросы отвечает кратко, аргументировано, уверенно, по существу. Способен принимать быстрые и нестандартные решения.

Зачёт/Хорошо выставляется в случае, если обучающийся показывает достаточный уровень компетентности, знания материалов занятий, учебной и методической литературы, нормативов и практики его применения. Уверенно и профессионально, грамотным языком, ясно, четко и понятно излагает состояние и суть вопроса. Знает теоретическую и практическую базу, но при ответе допускает несущественные погрешности. Обучающийся показывает достаточный уровень профессиональных знаний, свободно оперирует понятиями, методами оценки принятия решений, имеет представление: о междисциплинарных связях, увязывает знания, полученные при изучении различных дисциплин, умеет анализировать практические ситуации, но допускает некоторые погрешности. Ответ построен логично, материал излагается хорошим языком, привлекается информативный и иллюстрированный материал, но при ответе допускает незначительные ошибки, неточности по названным критериям, которые не искажают сути ответа;

Зачёт/Удовлетворительно выставляется в случае, если обучающийся показывает слабое знание материалов занятий, отсутствует должная связь между анализом, аргументацией и выводами. На поставленные вопросы отвечает неуверенно, допускает погрешности. Обучающийся владеет практическими навыками, привлекает иллюстративный материал, но чувствует себя неуверенно при анализе междисциплинарных связей. В ответе не всегда присутствует логика, аргументы привлекаются недостаточно веские. На поставленные вопросы затрудняется с ответами, показывает недостаточно глубокие знания.

Зачёт/Неудовлетворительно выставляется в случае, если обучающийся показывает слабые знания материалов занятий, учебной литературы, теории и практики применения изучаемого вопроса, низкий уровень компетентности, неуверенное изложение вопроса. Обучающийся показывает слабый уровень профессиональных знаний, затрудняется при анализе практических ситуаций. Не может привести примеры из реальной практики. Неуверенно и логически непоследовательно излагает материал. Неправильно отвечает на вопросы или затрудняется с ответом.

Зачет с оценкой организуется в период сессии в соответствии с текущим графиком учебного процесса, утвержденным в соответствии с установленным в СЗИУ порядком. Продолжительность зачета для каждого студента не может превышать четырех

академических часов. Зачет не может начинаться ранее 9.00 часов и заканчиваться позднее 21.00 часа. Зачет проводится в аудитории, в которую запускаются одновременно не более 5 человек. Время на подготовку ответов по билету каждому обучающемуся отводится 30-40 минут. При явке на зачет обучающийся должен иметь при себе зачетную книжку. Во время зачета обучающиеся по решению преподавателя могут пользоваться учебной программой дисциплины и справочной литературой.

В случае применения дистанционного режима промежуточной аттестации она проводится следующим образом: устно в ДОТ/письменно с прокторингом/ тестирование с прокторингом. Для успешного освоения курса учащемуся рекомендуется ознакомиться с литературой, размещенной в разделе 6, и материалами, выложенными в ДОТ.

6. Методические материалы по освоению дисциплины

Методические рекомендации по работе над конспектом лекций во время и после проведения лекции.

Обучающимся рекомендуется в ходе лекционных занятий выполнять следующее: вести конспектирование учебного материала, обращать внимание на категории, формулировки, раскрывающие содержание тех или иных явлений и процессов, научные выводы и практические рекомендации по их применению, задавать преподавателю вопросы.

Целесообразно в конспектах лекций рабочих конспектах формировать поля, на которых возможно делать пометки из рекомендованной литературы, дополняющие материал прослушанной лекции, а также подчеркивающие особую важность тех или иных положений.

Методические рекомендации к семинарским (практическим) занятиям.

На семинарских занятиях в зависимости от темы занятия выполняется поиск информации по решению проблем, выработка индивидуальных или групповых решений, решение задач, итоговое обсуждение с обменом знаниями, участие в круглых столах, разбор конкретных ситуаций, командная работа, решение индивидуальных тестов, участие в деловых играх.

При подготовке к семинарским занятиям каждый обучающийся должен:

- изучить рекомендованную учебную литературу;
- подготовить ответы на все вопросы семинара.

При подготовке к семинарским занятиям необходимо обратить внимание на виды работ, которые определены заданием. Существенный акцент делается на умение студента выполнять индивидуальные письменные задания, а также на работу студента с большим объемом информации, как в электронном, так и в печатном виде.

При подготовке к семинарским занятиям важно проработать материал лекций по конкретной теме, ознакомиться с указанной литературой и выполнить все необходимые практические задания. Для семинарских занятий лучше завести отдельную папку с файлами или тетрадь со съемными листами для удобства работы.

Подготовка к контрольным мероприятиям.

При подготовке к контрольным мероприятиям обучающийся должен освоить теоретический материал, повторить материал лекционных и практических занятий, материал для самостоятельной работы по указанным преподавателям темам.

Самостоятельная работа осуществляется в виде изучения литературы, эмпирических данных по публикациям и конкретных ситуаций, подготовке индивидуальных работ, работа с лекционным материалом, самостоятельное изучение отдельных тем дисциплины; поиск и обзор учебной литературы, в т.ч. электронных источников; научной литературы, справочников и справочных изданий, нормативной литературы и информационных изданий.

Учебно-методическое обеспечение самостоятельной работы

Тема 1. Информационная безопасность как следствие трансформации информационных коммуникаций

Основная литература

1. Ковалев А.А., Шамахов В.А. Военная безопасность России и ее информационная политика в эпоху цивилизационных конфликтов. Москва: РИОР, 2019. 184 с.

2. Международная информационная безопасность: теория и практика. В трех томах. Том 1: Учебник для вузов / Под общ. ред. А.В. Крутских. М.: Издательство «Аспект Пресс», 2021. 381 с.

3. Осавелюк Е.А. Информационная безопасность государства и общества в контексте деятельности СМИ. СПб.: Лань, 2019. 89 с.

4. Федоров А.В., Зиновьева Е.С. Информационная безопасность: политическ5ая теория и дипломатическая практика. М.: МГИМО-Университет, 2017. 357 с. С. 38-169.

Дополнительная литература

Глобализация: на грани реального и виртуального. Коллективная моног8рафия / Отв. ред. Н.А. Баранов. СПб: ООО «Геополитика и безопасность», ИД «ПЕТРОПОЛИС», 2020. 292 с. С. 124-142.

Кастельс М. Гапактика Интернет: Размышления об Интернете, бизнесе и обществе / Пер. с англ. А. Матвеева nод ред. В. Харитонова. Екатеринбург: У - Фактория (npи участии изд-ва Гуманитарного ун-та), 2004. 328 с.

Кастельс М. Информационная эпоха: экономика, общество и культура: Пер. с англ. под науч. ред. О.И. Шкаратана. М.: ГУ ВШЭ, 2000. 608 с.

Мировой порядок – время перемен: Сборник статей / Под ред. А.И. Соловьева, О.В. Гаман-Голутвиной. М.: Издательство «Аспект Пресс», 2019. С. 168-178. 375 с.

Неймарк М.А. Эволюция внешнеполитической стратегии России. Москва: Проспект, 2020. 320 с. С. 203-211.

Словарь - справочник по информационной безопасности для парламентской ассамблеи ОДКБ / Под общ ред. М.Л. Вуса и М.М. Кучерявого. СПб.: СПИИРАН. Изд-во «Анатолия», «Полиграфические технологии», 2014. 96 с.

Современная политическая наука: Методология. Научное издание / Отв. ред. О.В. Гаман-Голутвина, А.И. Никитин. 2-е изд., испр. и доп. М.: Издательство «Аспект Пресс», 2019. С. 742-758.

Тема 2. Политико-правовой режим глобальной информационной безопасности

Основная литература

1. Ковалев А.А., Шамахов В.А. Военная безопасность России и ее информационная политика в эпоху цивилизационных конфликтов. Москва: РИОР, 2019. 184 с.

2. Международная информационная безопасность: теория и практика. В трех томах. Том 1: Учебник для вузов / Под общ. ред. А.В. Крутских. М.: Издательство «Аспект Пресс», 2021. 381 с.

3. Осавелюк Е.А. Информационная безопасность государства и общества в контексте деятельности СМИ. СПб.: Лань, 2019. 89 с.

4. Федоров А.В., Зиновьева Е.С. Информационная безопасность: политическ5ая теория и дипломатическая практика. М.: МГИМО-Университет, 2017. 357 с. С. 197-252.

Дополнительная литература

Декларация принципов. Всемирный Саммит по информационному обществу, Женева, 12 декабря 2003 г. URL: http://www.library.ru/1/act/docs/deklarprincip.rtf

Декларация тысячелетия Организации Объединенных Наций от 8 сентября 2000 года. URL: http://www.un.org/ru/documents/decl_conv/declarations/summitdecl.shtml.

Доклад рабочей группы по управлению Интернетом, июнь 2005 г. // Official website «Working Group on Internet Governance». URL: http://www.wgig.org/docs/WGIGReport-Russian.doc

Крутских А. Об итогах работы Группы правительственных экспертов ООН по достижениям в сфере информатизации и телекоммуникаций в 2016 году // Международная жизнь. 2017. Специальный выпуск: Россия и информационная безопасность. С.92-95.

Современная мировая политика: прикладной анализ / Отв. ред. А.Д. Богатуров. – 2-е изд., испр. И доп. М.: Аспект Пресс, 2010. 592 с. С.477-490.

Современные международные отношения: Учебник / Под ред. А.В. Торкунова, А.В. Мальгина. М.: Аспект Пресс, 2012. 688 с. С.558-564.

Стратегия развития информационного общества в Российской Федерации на 2017-2030 годы. Утверждена Указом Президента РФ от 09.05.2017г. N203 // Официальный сайт Президента России. URL: http://static.kremlin.ru/media/acts/files/0001201705100002.pdf

Тунисская программа для информационного общества, 15.11.2005 г. URL: http://www.un.org/ru/events/pastevents/pdf/agenda_wsis.pdf

Тунисское обязательство, 15.11.2005 г. URL: http://www.mcbs.ru/files/documents/Documents/tunisskoe_obyazatelstvo.pdf

Memorandum of Understanding between the U.S. Department of Commerce and Internet Corporation for Assigned Names and Numbers // Official website ICANN. URL: https://www.icann.org/resources/unthemed-pages/icann-mou-1998-11-25-en

Тема 3. Угрозы международной информационной безопасности

Основная литература

1. Ковалев А.А., Шамахов В.А. Военная безопасность России и ее информационная политика в эпоху цивилизационных конфликтов. Москва: РИОР, 2019. 184 с.

2. Международная информационная безопасность: теория и практика. В трех томах. Том 1: Учебник для вузов / Под общ. ред. А.В. Крутских. М.: Издательство «Аспект Пресс», 2021. 381 с. С. 189-206, 244-262.

3. Осавелюк Е.А. Информационная безопасность государства и общества в контексте деятельности СМИ. СПб.: Лань, 2019. 89 с.

4. Федоров А.В., Зиновьева Е.С. Информационная безопасность: политическ5ая теория и дипломатическая практика. М.: МГИМО-Университет, 2017. 357 с. С. 170-196.

Дополнительная литература

Кефели И.Ф. Асфатроника: на пути к теории глобальной безопасности. СПб.: ИПЦ СЗИУ РАНХиГС, 2020. 228 с. С. 23-54.

Стратегия национальной кибербезопасности Соединенных Штатов Америки. Сентябрь 2018 года.

Тема 4. Информационная война в системе международных отношений

Основная литература

1. Ковалев А.А., Шамахов В.А. Военная безопасность России и ее информационная политика в эпоху цивилизационных конфликтов. Москва: РИОР, 2019. 184 с.

2. Международная информационная безопасность: теория и практика. В трех томах. Том 1: Учебник для вузов / Под общ. ред. А.В. Крутских. М.: Издательство «Аспект Пресс», 2021. 381 с. С. 216-243.

3. Осавелюк Е.А. Информационная безопасность государства и общества в контексте деятельности СМИ. СПб.: Лань, 2019. 89 с.

4. Федоров А.В., Зиновьева Е.С. Информационная безопасность: политическ5ая теория и дипломатическая практика. М.: МГИМО-Университет, 2017. 357 с.

Дополнительная литература

Анненков В. Информационно-психологическое противоборство: современные аспекты // Современный мир и геополитика / Отв. ред. М.А. Неймарк. Москва: Издательство «Канон+» РООИ «Реабилитация», 2015. 448 с. С. 116-126.

Воронова О.Е. Информационно-психологическая безопасность России в условиях новых глобальных угроз. М.: Издательство «Аспект Пресс», 2019. 240 с. С. 97-213.

Джоуэт Г., О`Доннел В. Пропаганда и убеждение. Пер. с англ. Х.: Издательство «Гуманитарный центр»/ О.И. Ткаченко, 2021. 496 с.

Информационно-когнитивная безопасность. Коллективная монография / Под ред. И.Ф. Кефели, Р.М. Юсупова. Санкт-Петербург: ИД «ПЕТРОПОЛИС», 2017. 300 с. С.14-30, 43-73.

Кефели И.Ф. Асфатроника: на пути к теории глобальной безопасности. СПб.: ИПЦ СЗИУ РАНХиГС, 2020. 228 с. С. 143-156.

Манойло А.В. Информационные и гибридные конфликты. Учебное пособие для вузов. М.: Горячая линия – Телеком, 2020. 464 с. С. 67-139, 346-394.

Пропагандистский дискурс в условиях цифровизации / отв. ред. В. А. Ачкасова и Г. С. Мельник. СПб.: СПбГУ, 2021. 520 с. С. 166-292.

Смирнов А.И. Современные информационные технологии в международных отношениях: монография. Москва: МГИМО-Университет, 2017. 334 с. С. 263-292.

Тема 5. Цифровые технологии в мировой политике

Основная литература

1. Ковалев А.А., Шамахов В.А. Военная безопасность России и ее информационная политика в эпоху цивилизационных конфликтов. Москва: РИОР, 2019. 184 с.

2. Международная информационная безопасность: теория и практика. В трех томах. Том 1: Учебник для вузов / Под общ. ред. А.В. Крутских. М.: Издательство «Аспект Пресс», 2021. 381 с.

3. Осавелюк Е.А. Информационная безопасность государства и общества в контексте деятельности СМИ. СПб.: Лань, 2019. 89 с.

4. Федоров А.В., Зиновьева Е.С. Информационная безопасность: политическ5ая теория и дипломатическая практика. М.: МГИМО-Университет, 2017. 357 с.

Дополнительная литература

Мировой порядок – время перемен: Сборник статей / Под ред. А.И. Соловьева, О.В. Гаман-Голутвиной. М.: Издательство «Аспект Пресс», 2019. С. 168-178. 375 с.

Смирнов А.И. Современные информационные технологии в международных отношениях: монография. Москва: МГИМО-Университет, 2017. 334 с.

Современная политическая наука: Методология. Научное издание / Отв. ред. О.В. Гаман-Голутвина, А.И. Никитин. 2-е изд., испр. и доп. М.: Издательство «Аспект Пресс», 2019. С. 742-758.

Сурма И. Цифровая дипломатия США в дискурсе глобальной политики // Современный мир и геополитика / Отв. ред. М.А. Неймарк. Москва: Издательство «Канон+» РООИ «Реабилитация», 2015. 448 с. С. 327-350.

Тема 6. Государственная политика Российской Федерации в области международной информационной безопасности

Основная литература

1. Ковалев А.А., Шамахов В.А. Военная безопасность России и ее информационная политика в эпоху цивилизационных конфликтов. Москва: РИОР, 2019. 184 с.
2. Международная информационная безопасность: теория и практика. В трех томах. Том 1: Учебник для вузов / Под общ. ред. А.В. Крутских. М.: Издательство «Аспект Пресс», 2021. 381 с.
3. Осавелюк Е.А. Информационная безопасность государства и общества в контексте деятельности СМИ. СПб.: Лань, 2019. 89 с.
4. Современная мировая политика: учебник. Москва: Проспект, 2021. 600 с. С. 87-94.
5. Федоров А.В., Зиновьева Е.С. Информационная безопасность: политическ5ая теория и дипломатическая практика. М.: МГИМО-Университет, 2017. 357 с. С. 286-340.

Дополнительная литература

Доктрина информационной безопасности Российской Федерации от 5 декабря 2016 г. URL: http://www.scrf.gov.ru/security/information/document5/

Концепция Конвенции ООН об обеспечении международной информационной безопасности. http://www.scrf.gov.ru/security/information/document112/

Основы государственной политики Российской Федерации в области международной информационной безопасности (Утверждены Указом Президента Российской Федерации от 12 апреля 2021 г. № 213). http://www.scrf.gov.ru/security/information/document114/

Манойло А.В. Информационные и гибридные конфликты. Учебное пособие для вузов. М.: Горячая линия – Телеком, 2020. 464 с. С. 328-345.

Неймарк М.А. Эволюция внешнеполитической стратегии России. Москва: Проспект, 2020. 320 с. С. 203-211.

Смирнов А.И. Современные информационные технологии в международных отношениях: монография. Москва: МГИМО-Университет, 2017. 334 с. С. 293-297.

7. Учебная литература и ресурсы информационно-телекоммуникационной сети "Интернет"

7.1. Основная литература

1. Ковалев А.А., Шамахов В.А. Военная безопасность России и ее информационная политика в эпоху цивилизационных конфликтов. Москва: РИОР, 2019. 184 с.
2. Международная информационная безопасность: теория и практика. В трех томах. Том 1: Учебник для вузов / Под общ. ред. А.В. Крутских. М.: Издательство «Аспект Пресс», 2021. 381 с. С. 62-88.
3. Осавелюк Е.А. Информационная безопасность государства и общества в контексте деятельности СМИ. СПб.: Лань, 2019. 89 с.
4. Современная мировая политика: учебник. Москва: Проспект, 2021. 600 с.
5. Федоров А.В., Зиновьева Е.С. Информационная безопасность: политическ5ая теория и дипломатическая практика. М.: МГИМО-Университет, 2017. 357 с.

7.2. Дополнительная литература

1. Анненков В. Информационно-психологическое противоборство: современные аспекты // Современный мир и геополитика / Отв. ред. М.А. Неймарк. Москва: Издательство «Канон+» РООИ «Реабилитация», 2015. 448 с. С. 116-126.
2. Воронова О.Е. Информационно-психологическая безопасность России в условиях новых глобальных угроз. М.: Издательство «Аспект Пресс», 2019. 240 с.
3. Глобализация: на грани реального и виртуального. Коллективная моног8рафия / Отв. ред. Н.А. Баранов. СПб: ООО «Геополитика и безопасность», ИД «ПЕТРОПОЛИС», 2020. 292 с.
4. Джоуэт Г., О`Доннел В. Пропаганда и убеждение. Пер. с англ. Х.: Издательство «Гуманитарный центр»/ О.И. Ткаченко, 2021. 496 с.
5. Информационно-когнитивная безопасность. Коллективная монография / Под ред. И.Ф. Кефели, Р.М. Юсупова. Санкт-Петербург: ИД «ПЕТРОПОЛИС», 2017. 300 с.
6. Кастельс М. Гапактика Интернет: Размышления об Интернете, бизнесе и обществе / Пер. с англ. А. Матвеева nод ред. В. Харитонова. Екатеринбург: У - Фактория (npи участии изд-ва Гуманитарного ун-та), 2004. 328 с.
7. Кастельс М. Информационная эпоха: экономика, общество и культура: Пер. с англ. под науч. ред. О.И. Шкаратана. М.: ГУ ВШЭ, 2000. 608 с.
8. Кефели И.Ф. Асфатроника: на пути к теории глобальной безопасности. СПб.: ИПЦ СЗИУ РАНХиГС, 2020. 228 с.
9. Манойло А.В. Информационные и гибридные конфликты. Учебное пособие для вузов. М.: Горячая линия – Телеком, 2020. 464 с.
10. Манойло А.В., Петренко А.И., Фролов Д.Б. Государственная информационная политика в условиях информационно-психологической войны. – М.: Издательство "Горячая линия-Телеком", 2017. – 542 с. - 978-5-9912-0253-4 – URL: https://idp.nwipa.ru:2278/book/111080
11. Мировой порядок – время перемен: Сборник статей / Под ред. А.И. Соловьева, О.В. Гаман-Голутвиной. М.: Издательство «Аспект Пресс», 2019. С. 168-178. 375 с.
12. Неймарк М.А. Эволюция внешнеполитической стратегии России. Москва: Проспект, 2020. 320 с. С. 203-211.
13. Пропагандистский дискурс в условиях цифровизации / отв. ред. В. А. Ачкасова и Г. С. Мельник. СПб.: СПбГУ, 2021. 520 с.
14. Словарь - справочник по информационной безопасности для парламентской ассамблеи ОДКБ / Под общ ред. М.Л. Вуса и М.М. Кучерявого. СПб.: СПИИРАН. Изд-во «Анатолия», «Полиграфические технологии», 2014. 96 с.
15. Смирнов А.И. Современные информационные технологии в международных отношениях: монография. Москва: МГИМО-Университет, 2017. 334 с.
16. Современная политическая наука: Методология. Научное издание / Отв. ред. О.В. Гаман-Голутвина, А.И. Никитин. 2-е изд., испр. и доп. М.: Издательство «Аспект Пресс», 2019. С. 742-758.
17. Сурма И. Цифровая дипломатия США в дискурсе глобальной политики // Современный мир и геополитика / Отв. ред. М.А. Неймарк. Москва: Издательство «Канон+» РООИ «Реабилитация», 2015. 448 с. С. 327-350.
18. Сурма И.В. Возможности и приоритеты России и США в глобальном информационном пространстве // Россия и современный мир / Отв. ред. М.А. Неймарк. Москва: Издательство «Канон+» РООИ «Реабилитация», 2016. 512 с. С. 71-94.
19. Цветкова Н .А. Публичная дипломатия как инструмент идеологической и политической экспансии США в мире, 1914–2014 гг. Дис… д-ра ист. наук по спец. 07.00.15.

СПб.: СПбГУ, 2015. 552 с.

20. Шахуд З. Роль информационных технологий во внешней политике Российской Федерации в арабском мире. Дис… канд полит. наук по спец. 23.00.04. СПб.: СПбГУ, 2020. 138 с.

7.3 Нормативные правовые документы и иная правовая информация

Концепция внешней политики Российской Федерации (утверждена Указом Президента Российской Федерации 30 ноября 2016 г. № 640).

Военная доктрина Российской Федерации (утверждена Указом Президента РФ от 25.12.2014 N Пр-2976).

Декларация принципов. Всемирный Саммит по информационному обществу, Женева, 12 декабря 2003 г. URL: http://www.library.ru/1/act/docs/deklarprincip.rtf

Декларация тысячелетия Организации Объединенных Наций от 8 сентября 2000 года. URL: http://www.un.org/ru/documents/decl_conv/declarations/summitdecl.shtml

Доклад рабочей группы по управлению Интернетом, июнь 2005 г. // Official website «Working Group on Internet Governance». URL: http://www.wgig.org/docs/WGIGReport-Russian.doc

Доктрина информационной безопасности Российской Федерации (утверждена Указом Президента Российской Федерации от 5 декабря 2016 г. № 646).

Основы государственной политики Российской Федерации в области международной информационной безопасности (Утверждены Указом Президента Российской Федерации от 12 апреля 2021 г. № 213). http://www.scrf.gov.ru/security/information/document114/.

Конвенция об обеспечении международной информационной безопасности. http://www.scrf.gov.ru/security/information/document112/

Выписка из Основных направлений научных исследований в области обеспечения информационной безопасности Российской Федерации. http://www.scrf.gov.ru/security/information/document155/

Memorandum of Understanding between the U.S. Department of Commerce and Internet Corporation for Assigned Names and Numbers // Official website ICANN. URL: https://www.icann.org/resources/unthemed-pages/icann-mou-1998-11-25-en

Стратегия национальной безопасности Российской Федерации (утв. Указом Президента РФ от 2 июля 2021 г. N 400).

Стратегия развития информационного общества в Российской Федерации на 2017-2030 годы. Утверждена Указом Президента РФ от 09.05.2017г. N203 // Официальный сайт Президента России. URL: http://static.kremlin.ru/media/acts/files/0001201705100002.pdf

Тунисская программа для информационного общества, 15.11.2005 г. URL: http://www.un.org/ru/events/pastevents/pdf/agenda_wsis.pdf

Тунисское обязательство, 15.11.2005 г. URL: http://www.mcbs.ru/files/documents/Documents/tunisskoe_obyazatelstvo.pdf

7.4. Интернет-ресурсы

Для освоения дисциплины следует пользоваться доступом через сайт научной библиотеки http://nwapa.spb.ru/ к следующим подписным электронным ресурсам:

Русскоязычные ресурсы:

- электронные учебники электронно-библиотечной системы (ЭБС) «**Айбукс**»;
- электронные учебники электронно–библиотечной системы (ЭБС) «**Лань**»;
- статьи из периодических изданий по общественным и гуманитарным наукам «**Ист-Вью**»
- энциклопедии, словари, справочники «**Рубрикон**»;
- полные тексты диссертаций и авторефератов **Электронная Библиотека Диссертаций РГБ;**

Англоязычные ресурсы:

- EBSCO Publishing - доступ к мультидисциплинарным полнотекстовым базам данных различных мировых издательств по бизнесу, экономике, финансам, бухгалтерскому учету, гуманитарным и естественным областям знаний, рефератам и полным текстам публикаций из научных и научно–популярных журналов.

7.5. Иные ресурсы

Русскоязычные журналы:

1. Вестник международных организаций – URL: http://iorj.hse.ru/
2. Вестник МГИМО-Университета – URL: http://www.vestnik.mgimo.ru/
3. Журнал международного права и международных отношений – URL: http://www.beljournal.evolutio.info/
4. Индекс безопасности – URL: http://www.pircenter.org/security-index
5. Обозреватель - Observer – URL: http://observer.materik.ru/observer/index.html
6. Ойкумена. Регионоведческие исследования – URL: http://www.ojkum.ru/
7. Пространственная экономика – URL: http://spatial-economics.com/en/
8. Россия и Америка в XXI в. – URL: http://www.rusus.ru/
9. Россия и АТР – URL: http://www.riatr.ru/
10. Российский внешнеэкономический вестник – URL: http://www.rfej.ru/rvv

Сайты международных организаций

1. EEAS - http://eeas.europa.eu/
2. European Union - http://europa.eu/index_en.htm
3. United Nations – http://www.un.org.
4. International Monetary Fund – http://www.imf.org.
5. Practical Action - http://practicalaction.org
6. World Bank – http://www.worldbank.org.
7. World Trade Organization – http://www.wto.org.
8. Официальный сайт ОБСЕ – URL:http://www.osce.org/ru/

Сайты российских и зарубежных исследовательских центров

1. Российский институт стратегических исследований – URL: https://riss.ru/
2. ПИР-Центр – URL: http://www.pircenter.org/
3. Валдайский клуб – URL: http://ru.valdaiclub.com/
4. Интернет-портал Перспективы – URL: http://www.perspektivy.info/
5. Новое восточное обозрение – URL: http://ru.journal-neo.org/
1. American Enterprise Institute for Public Policy Research – URL: http://www.aei.org/
2. The Brookings Institution – URL: https://www.brookings.edu/
3. Carnegie Endowment for International Peace – URL: http://carnegieendowment.org/
4. Global Go To Think Tank. Index Report.2016.–URL: http://repository.upenn.edu/cgi/viewcontent.cgi?article=1011&context=think_tanks
5. The Heritage Foundation – URL: http://www.heritage.org
6. Hudson Institute – URL: https://hudson.org/
7. RAND corporation – URL: http://www.rand.org/
8. Национальный исследовательский институт мировой экономики и международных отношений имени Е.М. Примакова Российской академии наук- URL: http://www.imemo.ru/
9. Stockholm International Peace Research Institute [Электронныйресурс].-URL:https://www.sipri.org/
10. РСМД – URL: http://russiancouncil.ru/
11. Chatham House, the Royal Institute of International Affairs – URL: https://www.chathamhouse.org/About#sthash.hjcIkgcH.dpuf https://www.chathamhouse.org

8. Материально-техническая база, информационные технологии, программное

обеспечение и информационные справочные системы

Курс включает использование программного обеспечения Microsoft Excel, Microsoft Word, Microsoft Power Point для подготовки текстового и табличного материала, графических иллюстраций.

Методы обучения с использованием информационных технологий (компьютерное тестирование, демонстрация мультимедийных материалов)

Интернет-сервисы и электронные ресурсы (поисковые системы, электронная почта, профессиональные тематические чаты и форумы, системы аудио и видео конференций, онлайн энциклопедии, справочники, библиотеки, электронные учебные и учебно-методические материалы). Кроме вышеперечисленных ресурсов, используются следующие информационные справочные системы: http://uristy.ucoz.ru/; http://www.garant.ru/; http://www.kodeks.ru/ и другие.

№ п/п	Наименование
1.	Специализированные залы для проведения лекций:
2.	Специализированная мебель и оргсредства: аудитории и компьютерные классы, оборудованные посадочными местами
3.	Технические средства обучения: Персональные компьютеры; компьютерные проекторы; звуковые динамики; программные средства, обеспечивающие просмотр видеофайлов