

Документ подписан простой электронной подписью  
Информация о владельце:  
ФИО: Андрей Драгомирович Хлутков  
Должность: директор  
Дата подписания: 03.12.2024 22:18:04  
Уникальный программный ключ:  
880f7c07c583b07b775f6604a630281b15ca9fa2

**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

Директор СЗИУ РАНХиГС  
А.Д. Хлутков

**ПРОГРАММА МАГИСТРАТУРЫ**

**Мировая политика**

*(наименование образовательной программы)*

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

**Б1.В.ДВ.02.01 Цифровой суверенитет и институционализация цифровой  
управляемости: мировые практики / Digital sovereignty and institutionalization of  
digital governance: world practices**

*(код и наименование РПД)*

**41.04.05 «Международные отношения»**

*(код и наименование направления подготовки)*

**очная**

*(форма обучения)*

Год набора - 2024

Санкт-Петербург, 2024 г.

**Автор-составитель:**

кандидат политических наук, преподаватель кафедры международных отношений  
Лисенкова А.Д.

**Заведующий кафедрой международных отношений:**

кандидат исторических наук, доцент Буланакова М. А.

РПД Б1.В.ДВ.02.01 Цифровой суверенитет и институционализация цифровой управляемости: мировые практики / Digital sovereignty and institutionalization of digital governance: world practices одобрена на заседании методической комиссии, протокол от 04 июня 2024 г. № 3.

## СОДЕРЖАНИЕ

1. Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения образовательной программы
2. Объем и место дисциплины в структуре образовательной программы
3. Структура и содержание дисциплины
  - 3.1. Структура дисциплины
  - 3.2. Содержание дисциплины
4. Материалы текущего контроля успеваемости обучающихся
5. Оценочные материалы промежуточной аттестации по дисциплине
6. Методические материалы для освоения дисциплины
7. Учебная литература и ресурсы информационно-телекоммуникационной сети "Интернет"
  - 7.1. Основная литература
  - 7.2. Дополнительная литература
  - 7.3. Нормативные правовые документы и иная правовая информация
  - 7.4. Интернет-ресурсы
  - 7.5. Иные источники
8. Материально-техническая база, информационные технологии, программное обеспечение и информационные справочные системы

## 1. Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения образовательной программы

1.1 Дисциплина Цифровой суверенитет и институционализация цифровой управляемости: мировые практики / Digital sovereignty and institutionalization of digital governance: world practices обеспечивает овладение следующими компетенциями:

<i>Код компетенции</i>	<i>Наименование компетенции</i>	<i>Код компонента компетенции</i>	<i>Наименование компонента компетенции</i>
ПК-6	Способность понимать логику глобальных процессов и развития всемирной политической системы международных отношений, владеть знаниями об основных тенденциях развития ключевых интеграционных процессов современности	ПК-6.3	Способен сформировать навыки сравнительного анализа ключевых интеграционных процессов современности
ПК-9	Владеть политической и правовой спецификой положения регионов Российской Федерации и зарубежных стран в отношениях между государствами и понимать возможности и ограничения трансграничных и иных международных связей регионов	ПК-9.1	Способен сформировать знания о политической и правовой специфике положения регионов Российской Федерации и зарубежных стран в отношениях между государствами. Развитие понимания возможностей регионов в международном и трансграничном сотрудничестве
ОПК-2	Способен осуществлять поиск и применять перспективные информационно-коммуникационные технологии и программные средства для комплексной постановки и решения задач профессиональной деятельности	ОПК - 2.2	Формирует умение решать задачи профессиональной деятельности на основе применения соответствующих методов сбора и анализа данных
УК-5	Способен анализировать и учитывать разнообразие культур в процессе межкультурного взаимодействия	УК- 5.2	Обеспечивает создание недискриминационной среды взаимодействия при выполнении профессиональных задач

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

<i>ОТФ/ТФ</i>	<i>Код компонента компетенции</i>	<i>Результаты обучения</i>
	ПК-6.3	<p><b>На уровне знаний:</b> - основных компонентов, определяющих анализ процесса глобализации; - понимания природы процесса; - понятия интеграции, видов и форм интеграции.</p> <p><b>На уровне умений:</b> - выстраивать сравнительный анализ по разным направлениям: правовой целостности системы международных отношений, исторической динамики и обусловленности западной</p>

	<p>моделью, экономической целесообразностью развития сотрудничества в регионах;</p> <p>- сравнивать региональные модели интеграционного развития.</p> <p><b>На уровне навыков:</b> - анализа процессов глобализации в контексте множественности факторов;</p> <p>- сравнения различных регионов и стран по степени вовлеченности в процессы глобализации;</p> <p>- анализа эффективности интеграционного развития и значения интеграции для государств-участников</p>
ПК-9.1	<p><b>На уровне знаний:</b> - основных теоретических подходов к толкованию трансрегионализма, знание законодательного регулирования международной деятельности российских регионов</p> <p><b>На уровне умений:</b> - анализировать трансрегиональный потенциал регионов в международной деятельности государства</p> <p><b>На уровне навыков:</b> - анализа экономической эффективности и политической роли трансрегионального сотрудничества</p>
ОПК-2.2	<p><b>на уровне знаний:</b> особенности работы с современными информационно-коммуникационными технологиями</p> <p><b>на уровне умений:</b> самостоятельно приобретать знания с помощью информационных технологий</p> <p><b>на уровне навыков:</b> использовать в практической деятельности новые знания и умения, в том числе в новых областях знаний, полученных на основе использования информационно-коммуникационных технологий</p>
УК-5.2	<p><b>на уровне знаний:</b> особенности межкультурного взаимодействия с учетом ценностно-идеологических и культурно-конфессиональных различий;</p> <p>смысл и меру социальной и этической ответственности, возникающей в случае игнорирования особенностей межкультурного взаимодействия.</p> <p><b>на уровне умений:</b> с помощью навыков межкультурного взаимодействия разрешать существующие конфликтные ситуации, выстраивать высказывания, корректные с точки зрения всех языковых уровней; различать общий контекст ситуации;</p>

	<p>анализировать и учитывать разнообразие культур в профессиональной деятельности;</p> <p>принимать решения в нестандартных ситуациях, соблюдая принципы социальной и этической ответственности</p> <p><b>на уровне навыков:</b> навыками различения контекста ситуации в условиях межкультурного взаимодействия;</p> <p>практическим навыком чётко, последовательно и логично выражать свои мысли в устной коммуникации;</p> <p>методами принятия решений в нестандартных ситуациях, исключая негативные последствия социального и этического характера.</p>
--	---

## 2. Объем и место дисциплины в структуре образовательной программы

**Объем дисциплины.** Общая трудоемкость дисциплины (очное обучение) составляет 3 зачетные единицы 108 академ. часов /81 астрон. часа.

Дисциплина реализуется с применением дистанционных образовательных технологий (далее – ДОТ).

Вид работы	Трудоемкость (в академ. часах/астрон. часах)
<b>Общая трудоемкость</b>	<b>108/81</b>
<b>Контактная работа с преподавателем</b>	<b>36/27</b>
Лекции	12/9
Практические занятия	24/18
Лабораторные занятия	-
Практическая подготовка	-
Консультации	2/1,5
<b>Самостоятельная работа</b>	<b>70/52,5</b>
Контроль	-
Формы текущего контроля	УО, Д, Т
<b>Форма промежуточной аттестации</b>	<b>Зачет с оценкой – 2 семестр</b>

УО – устный опрос, Т-тестирование

**Место дисциплины в структуре ОП ВО.** Дисциплина Б1.В.ДВ.02.01 Цифровой суверенитет и институционализация цифровой управляемости: мировые практики / Digital sovereignty and institutionalization of digital governance: world practices является дисциплиной по выбору части, формируемой участниками образовательных отношений, учебного плана по направлению подготовки 41.04.05 «Международные отношения». Ее содержание лежит в основе или находится в тесной связи с рядом других дисциплин, которые изучаются в

процессе освоения магистерской программы «Мировая политика» и подготовки магистров по направлению подготовки 41.04.05 «Международные отношения».

В соответствии с учебным планом дисциплина Б1.В.ДВ.02.01 Цифровой суверенитет и институционализация цифровой управляемости: мировые практики / Digital sovereignty and institutionalization of digital governance: world practices изучается студентами во 2-м семестре 1 курса. Ее освоение реализуется после изучения:

Код	Название дисциплины
Б1.О.01	Анализ международных ситуаций
Б1.О.03	Информационно-коммуникационные технологии в мировой политике
Б1.О.09	Политический консалтинг
Б1.В.01	Мегатренды и глобальные проблемы
Б1.В.06	Конфликты в современном мире
Б1.В.ДВ.01.01	Национальные государства и негосударственные участники в мировой политике
Б1.В.ДВ.03.01	Этнокультурные процессы в мировой политике

Формы промежуточной аттестации – Зачет с оценкой.

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. Структура и содержание дисциплины

#### 3.1. Структура дисциплины

№ п/п	Наименование тем (разделов)	Объем дисциплины, час.					Форма текущего контроля успеваемости* *, промежуточно й аттестации	
		Всего	Контактная работа с преподавателем по видам учебных занятий					
			Л/ДО Т	ЛР/Д ОТ	ПЗ/ДО Т	КС Р*		
Тема 1	Место цифровых технологий в современной науке	17	2		4		10	УО, Т

	о международных отношениях													
Тема 2	Цифровые технологии и государственный суверенитет в теориях международных отношений	18	2		4		12	УО, Д						
Тема 3	Институционализация глобальной цифровой управляемости: опыт Организации Объединенных Наций	17	2		4		10	УО						
Тема 4	Цифровой суверенитет и институционализация цифровой управляемости: опыт РФ и евразийского пространства							18	2		4		14	УО, Т
Тема 5	Цифровой суверенитет и институционализация цифровой управляемости: опыт развитых стран							18	2		4		12	УО
Тема 6	Цифровой суверенитет и институционализация цифровой управляемости: опыт развивающихся стран и стран с переходной экономикой							18	2		4		12	УО, Д
<b>Промежуточная аттестация</b>			<b>Консультация – 2</b>					Зачет оценкой	с					
<b>ВСЕГО (академ/астроном)</b>		<b>108/81</b>	<b>12/9</b>		<b>24/18</b>	<b>2/1, 5</b>	<b>70/52, 5</b>							

Используемые сокращения:

Л – занятия лекционного типа (лекции и иные учебные занятия, предусматривающие преимущественную передачу учебной информации педагогическими работниками организации и (или) лицами, привлекаемыми организацией к реализации образовательных программ на иных условиях, обучающимся)<sup>1</sup>;

ЛР – лабораторные работы<sup>2</sup>;

ПЗ – практические занятия<sup>3</sup>;

КСР – индивидуальная работа обучающихся с педагогическими работниками организации и (или) лицами, привлекаемыми организацией к реализации образовательных программ на иных условиях (в том числе индивидуальные консультации)<sup>4</sup>;

ДОТ – занятия, проводимые с применением дистанционных образовательных технологий, в том числе с применением виртуальных аналогов профессиональной деятельности.

СР – самостоятельная работа, осуществляемая без участия педагогических работников организации и (или) лиц, привлекаемых организацией к реализации образовательных программ на иных условиях.

\*Не учитывается в общем объеме дисциплины

\*\*УО – устный опрос, Д – доклад, Т – тестирование

### 3.2. Содержание дисциплины

#### **Тема 1. Место цифровых технологий в современной науке о международных отношениях:**

Сущность понятий «цифровизация», «цифровые технологии», «информационно-коммуникационные технологии», «цифровая экономика», «цифровая дипломатия», «искусственный интеллект», «большие данные», «кибербезопасность» и «информационная безопасность». «Сетевые», «кибер-», «гибридные» и «информационные» войны. «Дипфейки». Различия и сущность понятий «цифровой суверенитет», «информационный суверенитет», «технологический суверенитет». Российские и зарубежные исследования в области влияния цифровых технологий на международные отношения.

#### **Тема 2. Цифровые технологии и государственный суверенитет в теориях международных отношений:**

<sup>1</sup> Абзац 2 пункта 31 Порядка организации и осуществления образовательной деятельности по образовательным программам высшего образования – программам бакалавриата, программам специалитета, программам магистратуры, утвержденного приказом Минобрнауки России от 05 апреля 2017 г. № 301 (ред. от 17.08.2020) (зарегистрирован Минюстом России 14 июля 2017г., регистрационный № 47415)

<sup>2</sup> См. абзац 2 пункта 31 Порядка организации и осуществления образовательной деятельности по образовательным программам высшего образования – программам бакалавриата, программам специалитета, программам магистратуры, утвержденного приказом Минобрнауки России от 05 апреля 2017 г. № 301 (ред. от 17.08.2020) (зарегистрирован Минюстом России 14 июля 2017г., регистрационный № 47415)

<sup>3</sup> См. абзац 2 пункта 31 Порядка организации и осуществления образовательной деятельности по образовательным программам высшего образования – программам бакалавриата, программам специалитета, программам магистратуры, утвержденного приказом Минобрнауки России от 05 апреля 2017 г. № 301 (ред. от 17.08.2020) (зарегистрирован Минюстом России 14 июля 2017г., регистрационный № 47415)

<sup>4</sup> Абзац 2 пункта 31 Порядка организации и осуществления образовательной деятельности по образовательным программам высшего образования – программам бакалавриата, программам специалитета, программам магистратуры, утвержденного приказом Минобрнауки России от 05 апреля 2017 г. № 301 (ред. от 17.08.2020) (зарегистрирован Минюстом России 14 июля 2017г., регистрационный № 47415)

Неолиберальные и неореалистические представления о государственном суверенитете. Критика постпозитивизма в отношении традиционных представлений о государственном суверенитете. Неолиберальное понимание влияния цифровых технологий. Концепции «мягкой», «острой», «умной» силы. «Цифровая» сила и «кибер-» сила. Копенгагенская школа, цифровая безопасность, киберугрозы и цифровой суверенитет. Социальный конструктивизм. Постпозитивистские и постмодернистские трактовки цифровизации международных отношений. Методы анализа цифровых международных отношений.

### **Тема 3. Институционализация глобальной цифровой управляемости: опыт Организации Объединенных Наций:**

Основные вызовы и угрозы цифровой управляемости (криптовалюты, роботизация и автоматизация труда, цифровое управление обществом, хакерские атаки, фейки и дипфейки, утечка персональных данных). Проблема доминирования транснациональных структур (Google, YouTube и др.) в цифровом пространстве. Деятельность ICANN и Internet Governance Forum. Декларация об использовании научно-технического прогресса в интересах мира и на благо человечества от 1975 г. Окинавская хартия Глобального информационного общества от 2000 г. Всемирная встреча на высшем уровне по вопросам информационного общества. Резолюция 70/125 «Итоговый документ совещания высокого уровня Генеральной Ассамблеи, посвященного общему обзору хода осуществления решений Всемирной встречи на высшем уровне по вопросам информационного общества» от 2015 г. Цифровизация и Цели в области устойчивого развития ООН. Стратегия Генерального секретаря в отношении новых технологий от 2018 г. Дорожная карта Генерального секретаря по цифровому сотрудничеству от 2020 г. Деятельность Международного союза электросвязи.

### **Тема 4. Цифровой суверенитет и институционализация цифровой управляемости: опыт РФ и евразийского пространства:**

Вызовы и угрозы цифровизации для национальной безопасности РФ. Стратегия национальной безопасности РФ от 2021 г., Доктрина информационной безопасности Российской Федерации от 2016 г., Основы государственной политики Российской Федерации в области международной информационной безопасности от 2021 г. Деятельность Министерства цифрового развития, связи и массовых коммуникаций РФ и Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций. Особенности блокировки и контроля за деятельностью иностранных агентов и нежелательных, террористических и экстремистских организаций в Интернет-пространстве. Проблемы и перспективы независимой российской цифровой среды (домены, алгоритмы шифрования, поисковые системы, социальные сети, навигационные системы, программное обеспечение и др.). Санкционные ограничения и импортозамещение. Соглашение о сотрудничестве государств-участников Содружества Независимых государств в области обеспечения информационной безопасности от 2012 г. Государственная программа «Цифровое развитие Беларуси на 2021-2025 годы» от 2021 г.

Электронное правительство Республики Казахстан. Место цифровых технологий в реализации публичной дипломатии на территории евразийского пространства.

**Тема 5. Цифровой суверенитет и институционализация цифровой управляемости: опыт развитых стран:**

Декларация о будущем Интернета от 2022 г. Эдвард Сноуден и WikiLeaks. Фактор Кремниевой долины. Влияние группы технологических корпораций Big Tech. Стратегия кибербезопасности ЕС на цифровое десятилетие от 2020 г. Доклад Научно-исследовательской службы Европейского парламента «Цифровой суверенитет для Европы» от 2020 г. Оборонная концепция ЕС «Стратегический компас» от 2022 г. (повышение возможностей анализа разведывательных данных, разработка кибер-дипломатического инструментария, противодействие манипулированию информацией). Цифровой суверенитет и институционализация цифровой управляемости в Австралии, Новой Зеландии, Израиле, Канаде, Великобритании и других развитых европейских государствах. Технологическая конкуренция «коллективного Запада» с Китаем и Россией. Цифровая публичная дипломатия США и других западных стран.

**Тема 6. Цифровой суверенитет и институционализация цифровой управляемости: опыт развивающихся стран и стран с переходной экономикой:**

Сущность понятия «цифровое неравенство». Белая книга «Интернет в Китае» от 2010 г. и система фильтрации контента «Золотой щит». Ограничение доступа к Интернету как механизм обеспечения цифрового и информационного суверенитета: опыт Кубы и КНДР. Кампания «Цифровая Индия». Декларация Бразилиа по итогам XI саммита государств – участников БРИКС от 2019 г. Деятельность альянса «Умная Африка». Стратегия цифровой трансформации от 2020 г. и Рамочная основа политики в области данных Африканского союза от 2022 г. Национальная цифровая стратегия Мексики на 2021-2024 гг. от 2021 г. Проблемы утери контроля над средствами коммуникации в развивающихся странах: нехватка квалифицированных кадров и цифровой самостоятельности.

*Course content*

**Topic 1. The place of digital technologies in modern science of international relations:**

The essence of ‘digitalization,’ ‘digital technologies,’ ‘information and communication technologies,’ ‘digital economy,’ ‘digital diplomacy,’ ‘artificial intelligence,’ ‘big data,’ ‘cybersecurity,’ and ‘information security.’ ‘Net-,’ ‘cyber-,’ ‘hybrid-’ and ‘information-’ wars. ‘Deepfakes.’ Differences and essence of the concepts ‘digital sovereignty,’ ‘information sovereignty,’ ‘technological sovereignty.’ Russian and international research in the field of the influence of digital technologies on international relations.

**Topic 2. Digital technologies and state sovereignty in theories of international relations:**

Neoliberal and neorealist ideas about state sovereignty. A critique of postpositivism regarding traditional ideas about state sovereignty. Neoliberal understanding of the influence of digital technologies. ‘soft,’ ‘sharp,’ ‘smart’ power. Digital power and cyber power. Copenhagen School, digital security, cyber threats, and digital sovereignty. Social constructivism. Postpositivist and

postmodern interpretations of the digitalization of international relations. Methods for analyzing digital international relations.

**Topic 3. Institutionalization of global digital governance: the experience of the United Nations:**

The main challenges and threats to digital governance (cryptocurrencies, robotization and labor automation, digital management of society, hacker attacks, fakes and deepfakes, personal data leakage). The problem of the dominance of transnational structures (Google, YouTube, etc.) in the digital space. Activities of ICANN and the Internet Governance Forum. Declaration on the Use of Scientific and Technological Progress in the Interests of Peace and for the Benefit of Mankind, 1975. Okinawa Charter on Global Information Society, 2000. World Summit on the Information Society. Resolution 70/125 'Outcome Document of the High-Level Meeting of the General Assembly on the Overall Review of the Implementation of the Outcomes of the World Summit on the Information Society,' 2015. Digitalization and the UN Sustainable Development Goals. The Secretary-General's Strategy on New Technologies, 2018. The Secretary-General's Roadmap for Digital Cooperation, 2020. Activities of the International Telecommunication Union.

**Topic 4. Digital sovereignty and institutionalization of digital governance: the experience of the Russian Federation and the Eurasian space:**

Challenges and threats of digitalization for the national security of the Russian Federation. National Security Strategy of the Russian Federation, 2021. Information Security Doctrine of the Russian Federation, 2016. Fundamentals of the State Policy in the Field of International Information Security, 2021. Activities of the Ministry of Digital Development, Communications and Mass Media of the Russian Federation and the Federal Service for Supervision of Communications, Information Technology and Mass Media. Features of blocking and monitoring the activities of foreign agents and undesirable, terrorist and extremist organizations in the Internet space. Problems and prospects of an independent Russian digital environment (domains, encryption algorithms, search engines, social networks, navigation systems, software, etc.). Sanctions and import substitution industrialization. Agreement on Cooperation between Member States of the Commonwealth of Independent States in the Field of Information Security, 2012. State program 'Digital Development of Belarus' for 2021-2025, 2021. Electronic government of the Republic of Kazakhstan. The place of digital technologies in the implementation of public diplomacy in the Eurasian space.

**Topic 5. Digital sovereignty and institutionalization of digital governance: experience of developed countries:**

Declaration for the Future of the Internet, 2022. Edward Snowden and WikiLeaks. The Silicon Valley factor. The influence of Big Tech. The EU's Cybersecurity Strategy for the Digital Decade, 2020. European Parliament Research Service paper 'Digital sovereignty for Europe,' 2020. A Strategic Compass for Security and Defence, 2022 (boosting intelligence capacities, developing Cyber Diplomacy Toolbox, counteracting the manipulation of information). Digital sovereignty and institutionalization of digital governance in Australia, New Zealand, Israel, Canada, the United Kingdom, and other developed European countries. Technological competition of the 'collective West' with China and Russia. Digital public diplomacy of the USA and other Western countries.

**Topic 6. Digital sovereignty and institutionalization of digital governance: experience of developing countries and countries in transition:**

The essence of the concept of 'digital inequality.' White Paper 'The Internet in China,' 2010 and the Golden Shield Project. Restriction of Internet access as a mechanism for ensuring digital and information sovereignty: the experience of Cuba and the DPRK. Digital India. XI BRICS Summit Brasilia Declaration, 2019. Activities of the Smart Africa Alliance. The Digital Transformation Strategy for Africa, 2020 and the AU Data Policy Framework, 2022. Mexico's National Digital Strategy, 2021-2024, 2021. Problems of loss of control over the means of communication in developing countries: lack of qualified personnel and digital independence.

#### 4. Материалы текущего контроля успеваемости обучающихся

В ходе реализации дисциплины Б1.В.ДВ.02.01 Цифровой суверенитет и институционализация цифровой управляемости: мировые практики / Digital sovereignty and institutionalization of digital governance: world practices используются следующие формы текущего контроля успеваемости обучающихся:

Тема (раздел)	Формы (методы) текущего контроля успеваемости
Тема 1. Место цифровых технологий в современной науке о международных отношениях	УО, Т
Тема 2. Цифровые технологии и государственный суверенитет в теориях международных отношений	УО, Д
Тема 3. Институционализация глобальной цифровой управляемости: опыт Организации Объединенных Наций	УО
Тема 4. Цифровой суверенитет и институционализация цифровой управляемости: опыт РФ и евразийского пространства	УО, Т
Тема 5. Цифровой суверенитет и институционализация цифровой управляемости: опыт развитых стран	УО
Тема 6. Цифровой суверенитет и институционализация цифровой управляемости: опыт развивающихся стран и стран с переходной экономикой	УО, Д

#### Типовые материалы текущего контроля успеваемости обучающихся

##### *Материалы для устного опроса*

##### **Тема 1. Место цифровых технологий в современной науке о международных отношениях**

1. Раскройте понятия «цифровой суверенитет» и «цифровизация».
2. Объясните различия между понятиями «цифровой суверенитет», «информационный суверенитет», «технологический суверенитет».

3. Какие особенности можно выделить в российских и зарубежных исследованиях в области влияния цифровых технологий на международные отношения?
4. В чем заключаются угрозы от дипфейков?

***Тема 3. Институционализация глобальной цифровой управляемости: опыт Организации Объединенных Наций***

1. С какими проблемами сталкивается цифровая управляемость на глобальном уровне?
2. Охарактеризуйте деятельность ICANN и Internet Governance Forum.
3. Как отражены проблемы, касающиеся цифровизации в Целях в области устойчивого развития ООН?

***Тема 4. Цифровой суверенитет и институционализация цифровой управляемости: опыт РФ и евразийского пространства***

1. На что направлена деятельность Министерства цифрового развития, связи и массовых коммуникаций РФ и Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций
2. Перечислите проблемы и перспективы независимой российской цифровой среды.
3. Охарактеризуйте место цифровых технологий в реализации публичной дипломатии на евразийском пространстве.

***Примеры тем докладов***

***Тема 2. Цифровые технологии и государственный суверенитет в теориях международных отношений***

1. Теоретические подходы к осмыслению государственного суверенитета.
2. Теоретические подходы к осмыслению цифрового суверенитета.
3. Концепции «мягкой», «острой», «умной» силы и цифровой суверенитет.
4. Постпозитивистские и постмодернистские трактовки цифровизации международных отношений.
5. Методы анализа цифровых международных отношений

***Тема 5. Цифровой суверенитет и институционализация цифровой управляемости: опыт развитых стран***

1. Институционализация цифровой управляемости и цифровой суверенитет США и Канады.
2. Институционализация цифровой управляемости и цифровой суверенитет Европейского союза и других развитых европейских государств.
3. Институционализация цифровой управляемости и цифровой суверенитет развитых

азиатских стран.

4. Институционализация цифровой управляемости и цифровой суверенитет Австралии и Новой Зеландии.
5. Институционализация цифровой управляемости и цифровой суверенитет Израиля.

***Тема 6. Цифровой суверенитет и институционализация цифровой управляемости: опыт развивающихся стран и стран с переходной экономикой***

1. Институционализация цифровой управляемости и цифровой суверенитет Индии.
2. Институционализация цифровой управляемости и цифровой суверенитет Китая.
3. Институционализация цифровой управляемости и цифровой суверенитет наименее развитых азиатских государств.
4. Институционализация цифровой управляемости и цифровой суверенитет африканских государств.
5. Институционализация цифровой управляемости и цифровой суверенитет латиноамериканских государств.

***Примеры промежуточного контроля в форме тестирования***

Тестирование проводится в форме закрытых вопросов (выбор из четырех вариантов ответа).

Инструкция для обучающегося: необходимо выбрать один правильный вариант из предложенных ответов, обозначить кружком соответствующую букву.

**1. Какое государство не подписывало в 2000 г. Окинавская хартию Глобального информационного общества от 2000 г.?**

- A. Россия
- B. США
- C. Китай
- D. Япония

**2. Декларация об использовании научно-технического прогресса в интересах мира и на благо человечества была принята в...?**

- A. 2005 г.
- B. 2013 г.
- C. 1975 г.
- D. 1986 г.

**3. МСЭ:**

- A. Международный союз экономистов
- B. Международный союз электросвязи
- C. Международное сообщество электроники
- D. Мировой совет электронизации

**4. ICANN является:**

- A. Международной межправительственной организацией
- B. Специализированным учреждением ООН
- C. Международной некоммерческой организацией
- D. Подразделением Государственного департамента США

**5. Какая из перечисленных Целей в области устойчивого развития ООН в большей степени отвечает за развитие цифровых технологий?**

- A. Цель 7
- B. Цель 5
- C. Цель 15
- D. Цель 9

**6. Какая структура отвечает за блокировку ресурсов иностранных агентов в РФ?**

- A. Росстандарт
- B. Роскомнадзор
- C. Роспатент
- D. Росаккредитация

**7. Крупнейшей российской поисковой системой является?**

- A. Google
- B. Rambler
- C. Mail
- D. Yandex

**8. В каком году была принята Доктрина информационной безопасности Российской Федерации?**

- A. 2022
- B. 2014
- C. 2016
- D. 2021

**9. Министром цифрового развития, связи и массовых коммуникаций РФ является:**

- A. К.А. Чуйченко
- B. М.Г. Решетников
- C. Г. О. Греф
- D. М.И. Шадаев

**10. В каком году компания Microsoft объявила о постепенном сокращении своего бизнеса в РФ?**

- A. 2021
- B. 2022
- C. 2023
- D. 2024

**5. Оценочные материалы промежуточной аттестации по дисциплине**

Зачет с оценкой проводится в устной форме по билетам. Содержание билета по дисциплине состоит из двух частей: теоретические вопросы и практические задания.

### Оценочные материалы промежуточной аттестации

<i>Компонент компетенции</i>	<i>Промежуточный / ключевой индикатор оценивания</i>	<i>Критерий оценивания</i>
ПК-6.3	Формирует навыки сравнительного анализа ключевых интеграционных процессов современности	Демонстрирует навыки сравнительного анализа ключевых интеграционных процессов современности
ПК-9.1	Формирует знания о политической и правовой специфике положения регионов Российской Федерации и зарубежных стран в отношениях между государствами. Развивает понимания возможностей регионов в международном и трансграничном сотрудничестве.	Демонстрирует знания о политической и правовой специфике положения регионов Российской Федерации и зарубежных стран в отношениях между государствами
ОПК-2.2	Формирует умение решать задачи профессиональной деятельности на основе применения соответствующих методов сбора и анализа данных	Демонстрирует умения решения практических задач профессиональной деятельности на основе применения соответствующих методов сбора и анализа данных
УК-5.2	Обеспечивает создание недискриминационной среды взаимодействия при выполнении профессиональных задач	Демонстрирует навыки межкультурного взаимодействия разрешать существующие конфликтные ситуации

### Типовые оценочные материалы промежуточной аттестации

#### Примерный перечень вопросов к зачету с оценкой:

##### *Теоретический блок:*

1. Место цифровых технологий в современных международных отношениях.
2. «Цифровой суверенитет», «информационный суверенитет», «технологический суверенитет»: сущность и различия понятий.

3. Российские исследования в области влияния цифровых технологий на международные отношения.
4. Зарубежные исследования в области влияния цифровых технологий на международные отношения.
5. Теоретические представления о государственном суверенитете и цифровых технологиях.
6. Концепция «мягкой» силы, публичная дипломатия и цифровые технологии: теория и практика.
7. Методы анализа цифровых международных отношений.
8. Основные вызовы и угрозы цифровой управляемости.
9. Проблема доминирования транснациональных структур в цифровом пространстве.
10. Деятельность ICANN и Internet Governance Forum.
11. Цифровизация и Цели в области устойчивого развития ООН.
12. Опыт Организации Объединенных Наций в институционализации глобальной цифровой управляемости.
13. Перспективы независимой российской цифровой среды в условиях санкционного давления и технологической конкуренции «коллективного Запада» с Китаем и Россией.
14. Цифровой суверенитет России и российский опыт институционализации цифровой управляемости.
15. Цифровой суверенитет и опыт институционализации цифровой управляемости государств евразийского пространства.
16. Сотрудничество в области институционализации цифровой управляемости на евразийском пространстве.
17. Цифровой суверенитет и опыт институционализации цифровой управляемости развитых стран.
18. Цифровой суверенитет ЕС и европейский опыт институционализации цифровой управляемости на наднациональном уровне.
19. Цифровой суверенитет США и американский опыт институционализации цифровой управляемости.
20. Цифровой суверенитет и опыт институционализации цифровой управляемости развивающихся стран и стран с переходной экономикой.
21. Ограничение доступа к Интернету как механизм обеспечения цифрового и информационного суверенитета: опыт Кубы и КНДР.
22. Проблемы утери контроля над средствами коммуникации в развивающихся странах.

#### ***Практические задания:***

1. Составьте таблицу, раскрывающую сущность понятий «цифровизация», «цифровые технологии», «информационно-коммуникационные технологии».
2. Составьте таблицу, раскрывающую сущность понятий «цифровая экономика», «цифровая дипломатия», «искусственный интеллект», «большие данные».
3. Составьте таблицу, раскрывающую сущность и различие понятий «кибербезопасность» и «информационная безопасность».

4. Составьте схему, отражающие ключевые компоненты цифрового суверенитета государства.
5. Составьте информационно-аналитическую справку о текущем состоянии цифровой управляемости в ООН.
6. Подготовьте таблицу, раскрывающую эволюцию цифровой управляемости в ООН.
7. Составьте информационно-аналитическую справку о текущем состоянии цифровой управляемости в ЕАЭС и СНГ.
8. Составьте информационно-аналитическую справку о текущем состоянии цифровой управляемости в РФ.
9. Подготовьте таблицу, раскрывающую эволюцию цифровой управляемости в РФ.
10. Укажите основные проблемы для сохранения цифрового суверенитета РФ.
11. Составьте информационно-аналитическую справку о текущем состоянии цифровой управляемости в государствах евразийского пространства.
12. Составьте информационно-аналитическую справку о текущем состоянии цифровой управляемости в США.
13. Составьте информационно-аналитическую справку о текущем состоянии наднациональной цифровой управляемости в ЕС.
14. Составьте информационно-аналитическую справку о текущем состоянии наднациональной цифровой управляемости в Африке.
15. Составьте информационно-аналитическую справку о текущем состоянии наднациональной цифровой управляемости в Латинской Америке.
16. Сравните вызовы и угрозы для цифрового суверенитета развитых стран и развивающихся или стран с переходной экономикой.
17. Сравните уровень развития цифровой управляемости в развитых странах и развивающихся или странах с переходной экономикой.
18. Сравните уровень институционального и нормативно-правового развития цифровой управляемости на международном, наднациональном и национальном уровне (на примере ООН, ЕАЭС и РФ).
19. Сравните уровень институционального и нормативно-правового развития цифровой управляемости на международном, наднациональном и национальном уровне (на примере ООН, ЕС и любого государства-члена ЕС).
20. Составьте записку о приоритетах и особенностях деятельности ICANN.
21. Составьте записку о приоритетах и особенностях деятельности Internet Governance Forum.
22. Соотнесите процессы цифровизации с Целями в области устойчивого развития ООН.

### **Sample questions for the test with an assessment**

#### *Theoretical part:*

1. The place of digital technologies in modern international relations.
2. ‘Digital sovereignty’, ‘information sovereignty’, ‘technological sovereignty’: understanding the essence and differences of the concepts.

3. Russian research in the field of the influence of digital technologies on international relations.
4. International research in the field of the influence of digital technologies on international relations.
5. Theoretical notions of state sovereignty and digital technologies.
6. Soft power, public diplomacy and digital technologies: theory and practice.
7. Methods for analyzing digital international relations.
8. The main challenges and threats to digital governance.
9. The problem of the dominance of transnational structures in the digital space.
10. The activities of the ICANN and the Internet Governance Forum.
11. Digitalization and the UN Sustainable Development Goals.
12. The United Nations experience in the institutionalization of global digital governance.
13. Prospects for an independent Russian digital environment under sanctions pressure and technological competition of the ‘collective West’ with China and Russia.
14. Russia's digital sovereignty and Russian experience in the institutionalization of digital governance.
15. Digital sovereignty and the experience of the institutionalization of digital governance of Eurasian states.
16. Cooperation in the field of institutionalization of digital governance in the Eurasian space.
17. Digital sovereignty and the experience of the institutionalization of digital governance in developed countries.
18. EU digital sovereignty and the European experience of the institutionalization of digital governance at supranational level.
19. US digital sovereignty and the American experience of the institutionalization of digital governance.
20. Digital sovereignty and the experience of the institutionalization of digital governance in developing countries and countries in transition.
21. Restriction of Internet access as a mechanism for ensuring digital and information sovereignty: the experience of Cuba and the DPRK.
22. Problems of loss of control over means of communication in developing countries.

***Practical tasks:***

1. Create a table revealing the essence of ‘digitalization,’ ‘digital technologies,’ ‘information and communication technologies.’
2. Create a table revealing the essence of the concepts ‘digital economy,’ ‘digital diplomacy,’ ‘artificial intelligence,’ ‘big data.’
3. Create a table revealing the essence and differences between the concepts of ‘cyber security’ and ‘information security.’
4. Create a scheme reflecting the key components of the digital sovereignty of the state.
5. Compose an analytical and informational summary on the current state of digital governance in the UN.
6. Prepare a table revealing the evolution of digital governance in the UN.
7. Create an analytical and informational summary on the current state of digital governance in the EAEU and the CIS.
8. Create an analytical and informational summary on the current state of digital governance in the Russian Federation.
9. Prepare a table revealing the evolution of digital governance in the Russian Federation.
10. Specify the main problems for preserving the digital sovereignty of the Russian Federation.

11. Create an informational and analytical summary of the current state of digital governance in the states of the Eurasian space.
12. Create an informational and analytical summary on the current state of digital governance in the USA.
13. Create an analytical and informational summary on the current state of supranational digital governance in the EU.
14. Create an analytical and informational summary on the current state of supranational digital governance in Africa.
15. Create an analytical and informational summary on the current state of supranational digital governance in Latin America.
16. Compare the challenges and threats to digital sovereignty of developed countries and developing countries or countries in transition.
17. Compare the level of development of digital governance in developed countries and developing countries or countries in transition.
18. Compare the level of institutional and regulatory development of digital governance at the international, supranational and national levels (UN, EAEU, Russia).
19. Compare the level of institutional and regulatory development of digital governance at the international, supranational and national levels (UN, EAEU, Russia).
20. Write a note on the priorities and features of ICANN.
21. Write a note on the priorities and features of the Internet Governance Forum.
22. Relate digitalization processes to the UN Sustainable Development Goals.

### ***Шкала оценивания***

Оценка результатов производится на основе Положения о текущем контроле успеваемости обучающихся и промежуточной аттестации обучающихся по образовательным программам среднего профессионального и высшего образования в федеральном государственном бюджетном образовательном учреждении высшего образования «Российская академия народного 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.

**Зачет/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.

**Зачет/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;

**Зачет/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.

**Зачет/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 по дисциплине Б1.В.ДВ.02.01 Цифровой суверенитет и институционализация цифровой управляемости: мировые практики / Digital sovereignty and institutionalization of digital governance: world practices проводится в учебной аудитории с наличием компьютера или в компьютерном классе для выполнения практической части задания.

В аудитории для подготовки к ответу на экзаменационные вопросы допускается присутствие шести студентов. Для подготовки к ответу отводится от 20 до 40 минут.

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 для освоения дисциплины**

Указанная дисциплина изучается студентами очной формы обучения на протяжении 2-го семестра 1-го курса и завершается зачетом с оценкой. В ходе обучения основными видами учебных занятий являются лекции и практические занятия, индивидуальные консультации.

Предметная область изучаемой дисциплины включает теоретические основы мировой политики, экономические, правовые, этические и другие компоненты мировых политических процессов, а также тенденции мирового политического развития.

Дисциплина направлена на формирование у магистрантов комплексного понимания мировых практик институционализации цифровой управляемости и сохранения цифрового суверенитета и практических знаний о проблемах, определяющих развитие нормативно-правовых и институциональных основ на международном уровне (ООН), в рамках интеграционных объединений (ЕС, ЕАЭС), в РФ и государствах евразийского пространства, в развитых и развивающихся странах или странах с переходной экономикой.

В ходе лекций рассматриваются основные понятия тем, связанные с ними теоретические и практические проблемы, даются рекомендации для самостоятельной работы и подготовки к практическим занятиям.

В ходе практических занятий углубляются и закрепляются знания обучающихся по ряду рассмотренных на лекциях вопросов; развиваются навыки ведения публичной дискуссии, умения аргументировать и защищать выдвигаемые в них положения, а также их соотношение с практикой дипломатической работы.

При подготовке к практическим занятиям каждый обучающийся должен:

- Изучить рекомендованную учебную литературу;
- Подготовить ответы на все вопросы к практическому занятию.

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

### ***Методические рекомендации по организации самостоятельной работы студентов магистратуры***

Самостоятельная внеаудиторная работа по курсу включает изучение учебной и научной литературы, повторение лекционного материала, подготовку к практическим занятиям, а также к текущему и итоговому контролю.

Практические занятия предусматривают совершенствование навыков работы с первоисточниками и историко-правовым материалом, методологии изучения предметной специфики курса.

Вопросы, не рассмотренные на лекциях и практических занятиях, должны быть изучены в ходе самостоятельной работы. Контроль самостоятельной работы над учебной программой курса осуществляется в ходе практических занятий методом устного опроса или ответов на контрольные вопросы тем. В ходе самостоятельной работы каждый магистрант обязан прочитать основную и по возможности дополнительную литературу по изучаемой теме. Обучающийся должен готовиться к предстоящему практическому занятию по всем, обозначенным в методическом пособии вопросам. Не проясненные (дискуссионные) в ходе самостоятельной работы вопросы следует выписать в конспект лекций и впоследствии прояснить их на практических занятиях или индивидуальных консультациях с ведущим преподавателем.

### ***Методические рекомендации к подготовке доклада на практическом занятии***

Доклад обучающегося (участие в диспуте) на практическом занятии представляет собой устное выступление с использованием конспекта, плана доклада, схем, рисунков, иллюстраций и т. д. Целью доклада для студента должны выступать достаточно глубокое изучение какой-либо из проблем в истории формирования и развития интеллектуального пространства своей страны, проведение сравнительного анализа в рамках рассматриваемого вопроса, демонстрация способностей свободного рассуждения на исследуемую тематику, организации дискуссии, готовность ответа на поставленные вопросы. Не рассматривается в качестве доклада и не может быть оценено неотрывное чтение заранее подготовленного конспекта.

При подготовке к докладу студент должен уяснить цели и задачи исследования, предварительно ознакомиться с рекомендуемой литературой и иными источниками, в том числе и из глобальных информационных систем (Internet и др.). Необходимо сопоставить позиции отдельных авторов, провести по возможности их критический анализ, а при необходимости – сформировать аргументы для обоснования своей точки зрения.

Письменную часть работы рекомендуется проводить, прежде всего, не в целях полного конспектирования всего материала, а для формирования плана выступления, с обозначением ключевых вопросов темы, схем, графиков и т. д. В выступлении оцениваются, в первую очередь, способности студентов к изложению изученного материала, свободное им владение.

## **7. Учебная литература и ресурсы информационно-телекоммуникационной сети «Интернет»**

### ***7.1. Основная литература***

1. Научно-технологический прогресс и современные международные отношения: учебник: в 2 томах / под общей редакцией А. В. Бирюкова [и др.]. — Москва: Аспект Пресс, 2023 — Том 1 — 2023. — 368 с. — ISBN 978-5-7567-1270-4. — Текст: электронный // Лань: электронно-библиотечная система. — URL: <https://e.lanbook.com/book/364709> (дата обращения: 23.04.2024). — Режим доступа: для авториз. пользователей.

2. Цифровые международные отношения : учебное пособие : в 2 томах / под редакцией Е. С. Зиновьевой, С. В. Шитькова. — Москва: Аспект Пресс, 2023 — Том 1 — 2023. — 354 с. — ISBN 978-5-7567-1252-0. — Текст: электронный // Лань: электронно-библиотечная система. — URL: <https://e.lanbook.com/book/364712> (дата обращения: 23.04.2024). — Режим доступа: для авториз. пользователей.

3. Цифровые международные отношения : сборник научных трудов : в 2 томах / под редакцией Е. С. Зиновьевой, С. В. Шитькова. — Москва: Аспект Пресс, 2023 — Том 2 — 2023. — 475 с. — ISBN 978-5-7567-1269-8. — Текст: электронный // Лань: электронно-библиотечная система. — URL: <https://e.lanbook.com/book/364715> (дата обращения: 23.04.2024). — Режим доступа: для авториз. пользователей.

### ***7.2. Дополнительная литература***

1. Гаврилов Е.О. Цифровой суверенитет в условиях глобализации: философский и правовой аспекты / Е.О. Гаврилов // Вестник КемГУ. Гуманитарные и общественные науки. - 2020. - № 4 (2). - С. 146-152. - URL: <https://elibrary.ru/item.asp?id=43995797> (дата обращения: 23.04.2024).
2. Кочетков А.П., Маслов К.В. Цифровой суверенитет как основа национальной безопасности России в глобальном цифровом обществе / А.П. Кочетков, К.В. Маслов // Вестник Московского университета. Сер. 12. Политические науки. - 2022. - №2. - С. 31-45. - URL: <https://elibrary.ru/item.asp?id=50793293> (дата обращения: 23.04.2024).
3. Малик Е.Н. Киберагрессия коллективного Запада как геополитическая угроза цифровому суверенитету России / Е.Н. Малик // Вестник Прикамского социального института. - 2023. - № 2 (95). - С. 126-131. - URL: <https://elibrary.ru/item.asp?id=54745591> (дата обращения: 23.04.2024).
4. Симонова Л.Н., Пономарев Е.А. Цифровой суверенитет, вызовы и риски цифровизации в Латинской Америке // Латинская Америка. - 2023. - № 11. - С. 6-22. - URL: <https://elibrary.ru/item.asp?id=54945880> (дата обращения: 23.04.2024).
5. Смирнов А.И. Современные информационные технологии в международных отношениях : монография. – М.: Издательство «МГИМО-Университет», 2017. – 334 с. URL: [https://mgimo.ru/upload/iblock/b41/%D0%A1%D0%BC%D0%B8%D1%80%D0%BD%D0%BE%D0%B2\\_%D0%A1%D0%98%D0%A2%D0%9C%D0%9E\\_10\\_2017.pdf](https://mgimo.ru/upload/iblock/b41/%D0%A1%D0%BC%D0%B8%D1%80%D0%BD%D0%BE%D0%B2_%D0%A1%D0%98%D0%A2%D0%9C%D0%9E_10_2017.pdf) (дата обращения: 23.04.2024).
6. Jia K., Chen S. Global Digital Governance: Paradigm Shift and an Analytical Framework / K. Jia, S. Chen // Global Public Policy and Governance. 2022. Vol. 2. P. 283-305. URL: <https://link.springer.com/article/10.1007/s43508-022-00047-w> (дата обращения: 23.04.2024).
7. Robles-Carrillo M. Sovereignty vs. Digital Sovereignty / M. Robles-Carrillo // Journal of Digital Technologies and Law. - 2023. - № 1(3). - P. 673–690. - URL: <https://elibrary.ru/item.asp?id=54320909> (дата обращения: 23.04.2024).
8. Digital Sovereignty: African Perspectives / P. Gehl Sampath & F. Tregenna, eds. - Johannesburg : DSI/NRF South African Research Chair in Industrial Development, 2022. - URL: <https://digitalsovereigntyafrika.wordpress.com/wp-content/uploads/2022/02/digital-sovereignty-african-perspectives-10.pdf> (дата обращения: 23.04.2024).
9. Donnelly S., Ríos Camacho E., Heidebrecht S. Digital Sovereignty as Control: The Regulation of Digital Finance in the European Union / S. Donnelly, E. Ríos Camacho, S. Heidebrecht // Journal of European Public Policy. - 2023. - P. 1-24. - URL: <https://www.tandfonline.com/doi/epdf/10.1080/13501763.2023.2295520?needAccess=true> (дата обращения: 23.04.2024).

Наименование темы или раздела дисциплины (модуля)	Список рекомендуемой литературы	
	Основная (№ из перечня)	Дополнительная (№ из перечня)

<b>Тема 1.</b> Место цифровых технологий в современной науке о международных отношениях	1,2,3	1,7
<b>Тема 2.</b> Цифровые технологии и государственный суверенитет в теориях международных отношений	2	5
<b>Тема 3.</b> Институционализация глобальной цифровой управляемости: опыт Организации Объединенных Наций	1,2,3	6
<b>Тема 4.</b> Цифровой суверенитет и институционализация цифровой управляемости: опыт РФ и евразийского пространства	1,2,3	2,3
<b>Тема 5.</b> Цифровой суверенитет и институционализация цифровой управляемости: опыт развитых стран	1,2,3	5,9
<b>Тема 6.</b> Цифровой суверенитет и институционализация цифровой управляемости: опыт развивающихся стран и стран с переходной экономикой	1,2,3	4,8

### **7.3. Нормативные правовые документы и иная правовая информация**

1. Государственная программа «Цифровое развитие Беларуси» на 2021 – 2025 годы, 2021 [Электронный ресурс] // Министерство связи и информатизации Республики Беларусь. URL: <https://www.mpt.gov.by/ru/gosudarstvennaya-programma-cifrovoe-razvitie-belarusi-na-2021-2025-gody> (дата обращения: 14.04.2024).

2. Декларация Бразилиа по итогам XI саммита государств – участников БРИКС от 2019 г. [Электронный ресурс] // Президент России. URL: <http://kremlin.ru/supplement/5458> (дата обращения: 14.04.2024).

3. Декларация об использовании научно-технического прогресса в интересах мира и на благо человечества. Принята резолюцией 3384 (XXX) Генеральной Ассамблеи от 10 ноября 1975 года [Электронный ресурс] // Организация Объединенных Наций. URL: [https://www.un.org/ru/documents/decl\\_conv/declarations/science.shtml](https://www.un.org/ru/documents/decl_conv/declarations/science.shtml) (дата обращения: 09.04.2024).

4. Доктрина информационной безопасности Российской Федерации. Утверждена Указом Президента Российской Федерации от 05.12.2016 г. № 646 [Электронный ресурс] // Российская газета. URL: <https://rg.ru/documents/2016/12/06/doktrina-infobezobasnost-site-dok.html> (дата обращения: 09.04.2024).

5. Концепция внешней политики Российской Федерации. Утверждена Указом Президента Российской Федерации от 31.03.2023 г. № 229 [Электронный ресурс] //

Российская газета. URL: <https://rg.ru/documents/2023/03/31/prezident-ukaz229-site-dok.html> (дата обращения: 09.04.2024).

6. Окинавская хартия Глобального информационного общества от 2000 г. [Электронный ресурс] // Президент России. URL: <http://www.kremlin.ru/supplement/3170> (дата обращения: 14.04.2024).

7. Основы государственной политики Российской Федерации в области международной информационной безопасности. Указ Президента Российской Федерации от 12.04.2021 г. № 213. [Электронный ресурс] URL: <http://static.kremlin.ru/media/events/files/ru/RR5NtCWkkZPTuc5TrdHURpA4vpN5UTwM.pdf> (дата обращения: 09.04.2024).

8. Соглашение о сотрудничестве государств-участников Содружества Независимых государств в области обеспечения информационной безопасности от 23.11.2013 г. [Электронный ресурс] // Правительство Российской Федерации. URL: <http://pravo.gov.ru/proxy/ips/?docbody=&nd=102169115&intelsearch=%EF%F0%EE%F2%E8%E2%EE%E4%E5%E9%F1%F2%E2%E8%FF+%F2%E5%F0%F0%EE%F0%E8%E7%EC%F3> (дата обращения: 09.04.2024).

9. Стратегия Генерального секретаря в отношении новых технологий от 2018 г. [Электронный ресурс] // Организация Объединенных Наций. URL: <https://www.un.org/en/newtechnologies/images/pdf/SGs-Strategy-on-New-Technologies-RU.pdf> (дата обращения: 14.04.2024).

10. Стратегия национальной безопасности Российской Федерации. Утверждена указом Президента Российской Федерации от 02.07.2021 г. № 400 [Электронный документ] // Президент России. URL: <http://www.kremlin.ru/acts/bank/47046> (дата обращения: 09.04.2024).

11. Стратегия развития информационного общества в Российской Федерации на 2017 – 2030 годы. Принята Указом Президента Российской Федерации от 09.05.2017 г. № 203 [Электронный ресурс] // Президент России. URL: <http://www.kremlin.ru/acts/bank/41919> (дата обращения: 09.04.2024).

12. Указ о дополнительных мерах по обеспечению информационной безопасности Российской Федерации от 01.05.2022 г. № 250 [Электронный ресурс] // Президент России. URL: <http://www.kremlin.ru/acts/bank/47796> (дата обращения: 09.04.2024).

13. Указ о мерах по обеспечению ускоренного развития отрасли информационных технологий в России от 02.03.2022 г. № 83 [Электронный ресурс] // Президент России. <http://kremlin.ru/events/president/news/67893> (дата обращения: 09.04.2024).

14. A Strategic Compass for Security and Defence, 2022 [Электронный ресурс] // European External Action Service. URL: [https://www.eeas.europa.eu/sites/default/files/documents/strategic\\_compass\\_en3\\_web.pdf](https://www.eeas.europa.eu/sites/default/files/documents/strategic_compass_en3_web.pdf) (дата обращения: 14.04.2024).

15. AU Data Policy Framework, 2022 [Электронный ресурс] // African Union. URL: <https://au.int/sites/default/files/documents/42078-doc-AU-DATA-POLICY-FRAMEWORK-ENG1.pdf> (дата обращения: 14.04.2024).

16. Declaration for the Future of the Internet [Электронный ресурс] // U.S. Department of State. 2022. URL: <https://www.state.gov/wp-content/uploads/2022/04/Declaration-for-the-Future-for-the-Internet.pdf> (дата обращения: 09.04.2024).

17. Digital sovereignty for Europe [Электронный ресурс] // European Parliament. 2020. URL:

[https://www.europarl.europa.eu/RegData/etudes/BRIE/2020/651992/EPRS\\_BRI\(2020\)651992\\_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/BRIE/2020/651992/EPRS_BRI(2020)651992_EN.pdf) (дата обращения: 09.04.2024).

18. Digital Transformation Strategy for Africa (2020-2030), 2020 [Электронный ресурс] // African Union. URL: <https://au.int/sites/default/files/documents/38507-doc-dts-english.pdf> (дата обращения: 14.04.2024).

19. Joint Communication to the European Parliament and the Council: The EU's Cybersecurity Strategy for the Digital Decade [Электронный ресурс] // European Commission. URL: <https://ec.europa.eu/newsroom/dae/redirection/document/72164> (дата обращения: 09.04.2024).

20. Resolution adopted by the General Assembly on 16 December 2015 70/125. Outcome document of the high-level meeting of the General Assembly on the overall review of the implementation of the outcomes of the World Summit on the Information Society [Электронный ресурс] // United Nations. URL: [https://unctad.org/system/files/official-document/ares70d125\\_en.pdf](https://unctad.org/system/files/official-document/ares70d125_en.pdf) (дата обращения: 09.04.2024).

21. Road map for digital cooperation: implementation of the recommendations of the High level Panel on Digital Cooperation. Report of the Secretary-General, 2020 [Электронный ресурс] // United Nations. URL: <https://documents.un.org/doc/undoc/gen/n20/102/51/pdf/n2010251.pdf?token=AhF51z86Wb5VotjHga&fe=true> (дата обращения: 14.04.2024).

22. The Internet in China, 2010 [Электронный ресурс] // Information Office of the State Council of the People's Republic of China. URL: [http://www.china.org.cn/government/whitepaper/node\\_7093508.htm](http://www.china.org.cn/government/whitepaper/node_7093508.htm) (дата обращения: 14.04.2024).

#### **7.4. Интернет-ресурсы**

СЗИУ располагает доступом через сайт научной библиотеки <http://nwapa.spb.ru/> к следующим подписным электронным ресурсам:

**Подписные электронные ресурсы, доступные СЗИУ через сайт научной библиотеки <http://nwapa.spb.ru/>**

#### **Русскоязычные ресурсы**

- Электронные учебники электронно-библиотечной системы (ЭБС) «Айбукс».
- Электронные учебники электронно-библиотечной системы (ЭБС) «Лань».
- Научно-практические статьи по финансам и менеджменту Издательского дома «Библиотека Гребенникова».
- Статьи из периодических изданий по общественным и гуманитарным наукам «Ист-Вью».
- Энциклопедии, словари, справочники «Рубрикон».
- Полные тексты диссертаций и авторефератов Электронная Библиотека Диссертаций РГБ.
- Информационно-правовые базы – Консультант плюс, Гарант.

#### **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.

- Emerald – крупнейшее мировое издательство, специализирующееся на электронных журналах и базах данных по экономике и менеджменту. Имеет статус основного источника профессиональной информации для преподавателей, исследователей и специалистов в области менеджмента.

### **7.5. Иные источники**

#### **Русскоязычные журналы**

1. Вестник Волгоградского государственного университета. Серия 4 История. Регионоведение. Международные отношения – URL: <https://hfrir.jvolsu.com/index.php/ru/>
2. Вестник МГИМО-Университета – URL: <http://www.vestnik.mgimo.ru/>
3. Вестник международных организаций: образование, наука, новая экономика – URL: <http://iorj.hse.ru/>
4. Вестник РУДН. Международные отношения – URL: [https://journals.rudn.ru/international-relations/index/index/ru\\_RU](https://journals.rudn.ru/international-relations/index/index/ru_RU)
5. Информационные войны – URL: <http://pstmprint.ru/information-wars/>
6. Международные процессы – URL: [https://www.intertrends.ru/jour?locale=ru\\_RU](https://www.intertrends.ru/jour?locale=ru_RU)
7. Мировая экономика и международные отношения – URL: <https://www.imemo.ru/publications/periodical/meimo>
8. Россия в глобальной политике – URL: <https://globalaffairs.ru/>
9. Современная Европа – URL: <http://www.sov-europe.ru/>
10. Legal Issues in the Digital Age – URL: <https://lida.hse.ru/>

#### **Сайты международных организаций и интеграционных объединений**

1. Евразийский экономический союз – URL: <http://www.eaeunion.org/>
2. Программа развития ООН – URL: <https://www.un.org/ru/ga/undp/>
3. Форум ООН по управлению Интернетом – URL: <https://www.intgovforum.org/ru/about>
4. European Union – URL: [http://europa.eu/index\\_en.htm](http://europa.eu/index_en.htm)
5. United Nations – URL: <http://www.un.org>.

#### **Сайты российских и зарубежных исследовательских центров**

1. Российский совет по международным делам – URL: <http://russiancouncil.ru>
2. Совет по внешней и оборонной политике – URL: <https://svop.ru/>
3. ПИР-Центр – URL: [www.pircenter.org](http://www.pircenter.org)
4. Центр комплексных европейских и международных исследований – URL: <https://cceis.hse.ru/>
5. Electronic Frontier Foundation – URL: <https://www.eff.org/about>
6. Electronic Privacy Information Center – URL: <https://epic.org/>
7. Center for Long-Term Cybersecurity – URL: <https://cltc.berkeley.edu/>

## 8. Материально-техническая база, информационные технологии, программное обеспечение и информационные справочные системы

Дисциплина Б1.В.ДВ.02.01 Цифровой суверенитет и институционализация цифровой управляемости: мировые практики / Digital sovereignty and institutionalization of digital governance: world practices 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)

Информационные справочные системы: <http://www.garant.ru/>; <http://www.kodeks.ru/> и другие.

№ п/п	Наименование
1.	Специализированные залы для проведения лекций:
2.	Специализированная мебель и орг.средства: аудитории и компьютерные классы, оборудованные посадочными местами
3.	Технические средства обучения: Персональные компьютеры; компьютерные проекторы; звуковые динамики; программные средства, обеспечивающие просмотр видеофайлов в форматах AVI, MPEG-4, DivX, RMVB, WMV.