

Документ подписан простой электронной подписью  
Информация о владельце:  
ФИО: Романчук Иван Сергеевич  
Должность: Ректор  
Дата подписания: 03.03.2025 10:28:24  
Уникальный программный ключ:  
6319edc2b582ffdacea443f01d5779368d0957ac34f5cd074d81181530452479

Приложение к рабочей  
программе дисциплины

## МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ ПО ОРГАНИЗАЦИИ САМОСТОЯТЕЛЬНОЙ РАБОТЫ ОБУЧАЮЩИХСЯ

Наименование дисциплины	<i>Информационные войны в региональном измерении 7 семестр</i>
Направление подготовки	<i>41.03.01 Зарубежное регионоведение, 41.03.05 Международные отношения</i>
Направленность (профиль)	<i>Международно-политический анализ регионов мира Международная интеграция и международные организации</i>
Форма обучения	<i>очная</i>
Разработчик(и)	<i>Пустошинская Ольга Сергеевна, доцент</i>

1. Темы дисциплины для самостоятельного освоения обучающимися. Отсутствуют.

2. План самостоятельной работы.

№ п/п	Учебные встречи	Виды самостоятельной работы	Форма отчетности/ контроля	Количество баллов	Рекомендуемый бюджет времени на выполнение (ак.ч.)*
1	2	3	4	5	6
1.	<p><b>Лекция 1.</b> Понятие и основные характеристики информационной войны,</p> <p><b>Лекция 2.</b> Структура и виды информационных войн,</p> <p><b>Лекция 3.</b> Информационное оружие и этапы информационной войны,</p> <p><b>Лекция 4.</b> Концепции информационных войн стран, входящих в состав Европы, Азиатско-Тихоокеанского региона, Северной Америки, СНГ,</p> <p><b>Лекция 5.</b> Характеристика информационных войн с участием стран, входящих в состав Азиатско-Тихоокеанского региона, Ближнего Востока, Северной Америки, СНГ,</p> <p><b>Лекция 6.</b> Информационные войны и «цветные революции» как технологии реализации «гибридных войн»,</p>	Проработка лекций	Контрольные вопросы по темам	8 (по 1 баллу за каждую тему)	3 (по 0,4 ак. часа на ответ по каждой лекционной теме)

	<p><b>Лекция 7.</b> Информационная безопасность и ее обеспечение,</p> <p><b>Лекция 8.</b> Наднациональная информационная безопасность: правовая и институциональная составляющие</p>				
2.	<p><b>Семинар 1.</b> Понятие и основные характеристики информационной войны(1)</p> <p><b>Семинар 3.</b> Структура и виды информационных войн(1)</p> <p><b>Семинар 5.</b> Информационное оружие и этапы информационной войны(1)</p> <p><b>Семинар 7.</b> Концепции информационных войн стран, входящих в состав Европы, Азиатско-Тихоокеанского региона, Северной Америки, СНГ(1)</p> <p><b>Семинар 10.</b> Характеристика информационных войн с участием стран, входящих в состав Азиатско-Тихоокеанского региона, Ближнего Востока, Северной Америки, СНГ(1)</p> <p><b>Семинар 12.</b> Информационные войны и «цветные революции» как технологии реализации «гибридных</p>	Подготовка к практическому занятию	Фронтальный опрос	1	18 (по 2 ак. ч. на каждый семинар)

	<p>войн»(1)</p> <p><b>Семинар 14.</b> Информационная безопасность и ее обеспечение(1)</p> <p><b>Семинар 16.</b> Наднациональная информационная безопасность: правовая и институциональная составляющие(1)</p> <p><b>Семинар 17.</b> Наднациональная информационная безопасность: правовая и институциональная составляющие(2)</p>				
3.	<p><b>Семинар 1.</b> Понятие и основные характеристики информационной войны(1)</p> <p><b>Семинар 6.</b> Информационное оружие и этапы информационной войны(2)</p> <p><b>Семинар 8.</b> Концепции информационных войн стран, входящих в состав Европы, Азиатско-Тихоокеанского региона, Северной Америки, СНГ(2)</p> <p><b>Семинар 15.</b> Информационная безопасность и ее обеспечение(2)</p>	Подготовка к практическому занятию	Предоставление презентации группового доклада	3	16 (по 4 ак. ч. на каждый семинар)
4.	<p><b>Семинар 3.</b> Структура и виды информационных войн(1)</p> <p><b>Семинар 7.</b> Концепции информационных войн стран, входящих в состав</p>	Письменное задание	Эссе	2	20 (по 4 ак. ч. на каждый семинар)

	<p>Европы, Азиатско-Тихоокеанского региона, Северной Америки, СНГ(1)</p> <p><b>Семинар 14.</b> Информационная безопасность и ее обеспечение(1)</p> <p><b>Семинар 16.</b> Наднациональная информационная безопасность: правовая и институциональная составляющие(1)</p> <p><b>Семинар 16.</b> Наднациональная информационная безопасность: правовая и институциональная составляющие(2)</p>				
5.	<p><b>Семинар 4.</b> Структура и виды информационных войн(2)</p> <p><b>Семинар 11.</b> Характеристика информационных войн с участием стран, входящих в состав Азиатско-Тихоокеанского региона, Ближнего Востока, Северной Америки, СНГ(2)</p> <p><b>Семинар 13.</b> Информационные войны и «цветные революции» как технологии реализации «гибридных войн»(2)</p>	Письменное задание	Предоставление исследовательского проекта	3 балла для темы 4 по 7 баллов для тем 11, 13	12 (по 4 ак. ч. на каждый семинар)
	<p><b>Семинар 2.</b> Понятие и основные характеристики информационной войны(2)</p> <p><b>Семинар 5.</b> Концепции</p>	Письменное задание	Предоставление базы данных источников	3	6 (по 3 ак. ч. на каждый семинар)

	информационных войн стран, входящих в состав Европы, Азиатско-Тихоокеанского региона, Северной Америки, СНГ(3)				
7.	Зачет по дисциплине	Подготовка к зачету	Устное собеседование (ответ на вопрос)	9	19
				Итого ак. ч.	94

3. Требования и рекомендации по выполнению самостоятельных работ обучающихся, критерии оценивания.

#### **I. По лекционным темам дисциплины.**

Студенты отвечают на ключевой вопрос, поставленный в рамках каждой лекционной темы, в день проведения лекции. Всего у студентов имеется 5 попыток для внесения правильного варианта ответа на платформе LMS, где ответы автоматически оцениваются. Преподаватель получает от программного приложения отчет по каждому студенту.

##### *Критерии оценки.*

При выставлении баллов за лекции учитываются ответы студентов в совокупности с посещаемостью. 1 балл выставляется каждому студенту, посетившему лекцию и верно ответившему на контрольный вопрос. 0 баллов выставляется студенту или отсутствующему на лекции, или присутствовавшему на лекции, но неверно ответившему на ключевой вопрос лекции. Не оцениваются ответы на вопрос тех студентов, кто не посетил лекцию.

#### **II. По семинарским темам дисциплины.**

##### А. Подготовка индивидуальных заданий.

##### **Устный ответ: отчет студента о подготовке к фронтальному опросу.**

*Устный ответ* – краткое изложение материала обучающимися по каждому вопросу из списка вопросов, предложенных для обсуждения в ходе семинарского занятия.

Оцениваются: полнота ответов, умение студентов приводить примеры, иллюстрирующие факты из теории и политической практики, знакомство с материалом из научной литературы, рекомендованной преподавателем для изучения, а также самостоятельный поиск дополнительной литературы и источников, из которых студенты черпают необходимую информацию для подготовки развернутых ответов на поставленные вопросы.

Данное оценочное средство используется на первом, третьем, пятом, седьмом, десятом, двенадцатом, четырнадцатом, шестнадцатом и семнадцатом практических занятиях.

*Требования к подготовке устных ответов на вопросы по теме семинарского занятия.*

Организационные моменты. Ответы студентов озвучиваются в порядке, соответствующем очередности поднятых на занятии рук.

Содержательная часть ответов: соответствие материала поставленному вопросу, строгая логика изложения, смысловая завершенность ответа, научность языка, наличие примеров из теории и политической практики.

Временной регламент. Время выступления – не более 2 минут на один ответ.

##### *Критерии оценки.*

Совокупность ответов, артикулированных в ходе всего семинарского занятия, оценивается максимум в 1 балл. Они выставляются студенту при соблюдении вышеуказанных требований к содержательной части доклада, организационным моментам и

временному регламенту. 0 баллов выставляется при наличии значительных пробелов в содержательной части доклада или отсутствии доклада.

### **Эссе.**

*Эссе* – небольшой текст, в котором автор излагает собственные мысли по выбранной теме.

Оцениваются: глубина и оригинальность идей, наличие аргументации и обоснования представленных в научной литературе точек зрения по выбранной теме, ясность и точность, логическая последовательность изложения мыслей, использование разнообразного словарного запаса. Использование приложений с искусственным интеллектом для подготовки эссе недопустимо, о чем студенты заранее ставятся в известность. Проверка текста на наличие генераций осуществляется преподавателем посредством системы «Антиплагиат.ВУЗ» (<https://antiplagiat.ru/>). Студентам, предоставившим преподавателю эссе с генерацией текста, выставляется 0 баллов. Образец оформления эссе предоставляется преподавателем.

Данное оценочное средство используется на третьем, седьмом, четырнадцатом, шестнадцатом и семнадцатом практических занятиях.

#### *Требования к написанию эссе.*

1. **Структура эссе:** титульный лист с указанием темы эссе и Ф.И.О. автора, номера группы и направления подготовки; основная часть, список изученной литературы.

2. **Содержание эссе:** изложение поднятой проблемы; краткое описание ее решений, содержащихся в изученной студентом литературе; описание выводов и собственных предложений по ее устранению.

3. **Оформление эссе:** объем эссе не более 5 страниц, машинописный способ приготовления на листах формата А-4.

#### Тематика эссе:

-*Расторгуев С.П.* «Информационная война», М., 1999. Ч. 2. М., 1999 // Электронная библиотека Evarist. URL: <https://evartist.narod.ru/text4/58.htm> (семинар 3);

-*Libicki M.* What is Information Warfare? Washington. 1995 // Электронная база статей Springer. URL: [https://link.springer.com/chapter/10.1057/9780230294189\\_4](https://link.springer.com/chapter/10.1057/9780230294189_4) (семинар 7);

-*Аронсон Э.* Эпоха пропаганды: механизмы убеждения – повседневное использование и злоупотребление. СПб., 2002 // Электронная библиотека RoyalLib. URL: [https://royallib.com/book/aronson\\_eliot/epoha\\_propagandi\\_mehanizmi\\_ubegdeniya\\_povsednevnoe\\_ispolzovanie\\_i\\_zloupotreblenie.html](https://royallib.com/book/aronson_eliot/epoha_propagandi_mehanizmi_ubegdeniya_povsednevnoe_ispolzovanie_i_zloupotreblenie.html) (семинар 14);

-*Шарп Д.* От диктатуры к демократии: стратегия и тактика освобождения. М., 2012 // Университетская библиотека Online. URL: <https://biblioclub.ru/index.php?page=book&id=100111> (семинар 16);

-*Esterle A.* National and European information security policies: гл. 2 монографии // Information Security: A new Challenge for EU: EU Institute for Security Studies. 2005. P. 31-56 // Цифровая библиотека JSTOR. URL: <https://www.jstor.org/stable/resrep07008.7?seq=1> (семинар 17).

#### *Критерии оценки.*

Эссе оценивается максимум в 2 балла. Они выставляются студенту при соблюдении вышеуказанных требований к содержательной части эссе, его структуре и оформлению. 1 балл выставляется при наличии малозначительных ошибок в содержательной части эссе, но соблюдении всех остальных требований. 0 баллов выставляется при наличии значительных ошибок в содержательной части эссе, существенном нарушении его структуры и оформления, а также отсутствии эссе у обучающегося.

### **Б. Подготовка групповых заданий.**

#### **Разработка базы данных.**

*База данных* – организованная система информации, содержащая сведения о различных источниках по конкретной теме.

Студентам предлагается подготовить (в форме таблицы) базу данных употребимости терминов, связанных с категорией «информационная война», в публичном дискурсе разных государств (семинар 2), а также базу данных исследований аналитических центров, изучающих разные аспекты информационных войн (семинар 9). Образец оформления базы данных предоставляется преподавателем.

Данное оценочное средство используется на втором и девятом практических занятиях. Оценивается умение студентов подготавливать полную базу данных для проведения исследования.

*Пример алгоритма разработки базы данных источников для семинара 2.*

№ п/п	ключевые понятия	содержание документов стран	
		страна А	страна Б
1.			
2.			
3.			
4.			
5.			
п...			

*Пример алгоритма разработки базы данных источников для семинара 9.*

№ п/п	название Центра	наименование материала	тип материала (отчет, статья, проч.) и год его создания	ключевые мысли, представленные в материале
1.				
2.				
3.				
4.				
5.				
п...				

*Критерии оценки.*

Разработка базы данных оценивается максимум в 3 балла. Они выставляются студенту, который подготовил полную базу данных, дающую возможность сформироваться всестороннему представлению об объекте исследования. 2 балла выставляется при наличии неполной базы данных, незначительно затрудняющей понимание объекта исследования. 1 балл выставляется при наличии неполной базы данных, значительно затрудняющей понимание объекта исследования и приводящей к существенному искажению знаний о нем. 0 баллов выставляется при отсутствии результатов работы.

**Устные доклады с презентационным сопровождением.**

*Устный доклад* – развернутое изложение материала студентом по выбранной теме.

*Презентация* – визуальное представление ключевых положений устного доклада по выбранной теме с задействованием специальных программ и технических средств.

Оцениваются: понимание выбранной темы, полнота сформулированных выводов по итогам теоретического анализа, качество подготовленных презентаций (по структуре, содержанию, оформлению), умение студентов отбирать и систематизировать материал по выбранной теме, приводить примеры, иллюстрирующие артикулированную информацию, качество и разнообразие подобранных источников для подготовки доклада.

Данное оценочное средство используется на первом, девятом, одиннадцатом, тринадцатом и пятнадцатом практических занятиях.

*Требования к подготовке групповых докладов.*

Организационная часть. Групповой доклад готовится 4–5 студентами из расчета в 30 человек обучающихся. Предусматривается сопровождение доклада презентационным



рядом.

Содержательная часть: объем – не более 10 страниц, соответствие выбранной теме, внутреннее единство, строгая логика изложения, смысловая завершенность раскрываемой темы, научность языка.

Временной регламент. Время выступления – не более 10 минут, не более 10 минут на обсуждение.

*Требования к подготовке презентаций.*

Структура презентации: не более 5 слайдов; первый слайд должен содержать название темы доклада, Ф.И.О. автора, номер группы и наименование направления подготовки; последующие слайды должны раскрывать тему доклада; последний слайд должен содержать список использованной для раскрытия темы литературы. Оформление презентации: единый стиль, сочетаемость цветов, ограниченное, удобочитаемое количество объектов на слайде, использование анимационных объектов. Временной регламент выступления с презентацией: 7–10 минут.

*Критерии оценки.*

Доклад оценивается максимум в 3 балла. Они выставляются студенту при соблюдении всех вышеуказанных требований к содержательной части доклада. 2 балла выставляется при наличии несущественных ошибок в его содержательной части, касающихся научного стиля языка, но соблюдении иных вышеуказанных требований. 1 балл выставляется при наличии несущественных ошибок в его содержательной части, касающихся логики изложения материала, но соблюдении иных вышеуказанных требований. 0 баллов выставляется при наличии значительных нарушений в содержательной части доклада или отсутствии доклада у студента.

**Реализация исследовательского проекта.**

*Исследовательский проект* – набор взаимоувязанных и контролируемых видов научной деятельности, направленных на достижение полезных исследовательских или практико-профессиональных результатов, учитывающий ограничения по времени и иным ресурсам и осуществляемый согласно разработанному плану.

Студентам предлагается: включиться в реализацию проектной методики «интерпретация рисунка» (семинар 4), реализовать и оформить результаты ситуационного анализа (семинары 11, 13). По итогам исследования составляется аналитический отчет (образец предоставляется преподавателем).

*Требования к составлению аналитического отчета.*

1. Структура и содержание отчета: вводная часть (включает описание проблемы, постановку целей и задач по ее разрешению), основная часть (описание аналитического инструментария и осуществление международно-политического анализа), резолютивная часть (описание итогов международно-политического анализа, выводы, рекомендации).

2. Оформление отчета: не более 10 страниц, машинописный способ приготовления на листах формата А-4.

3. Артикуляция результатов исследования в студенческой группе, их обсуждение.

Перед проведением ситуационного анализа рекомендуется изучить специальную литературу, в которой содержатся соответствующие алгоритмы.

*Рекомендуемый список литературы по ситуационному анализу.*

1. *Попова О.В.* Политический анализ и прогнозирование: учебник / О.В. Попова. – Москва: Аспект Пресс, 2011. – 464 с. – ISBN 978-5-7567-0621-5. – Текст: электронный. – URL: <https://znanium.com/catalog/product/1038584>. Режим доступа: по подписке.

2. *Ерхов Г.П.* Изучение курса «Анализ международных ситуаций» / Г.П. Ерхов. – Донецк: ДонНУ, 2020. – 109 с. – Текст: электронный. – URL: <http://repo.donnu.ru:8080/jspui/bitstream/123456789/4783/1/3436.pdf>. Режим доступа: свободный.

*Требования к подготовке исследовательского проекта.*

Качественные характеристики: критический разбор кейсов, научный стиль изложения

выводов по результатам исследования, их полнота, наличие соответствующих визуализированных вариантов итогового результата – регистрационных таблиц, кодировочных матриц, моделей, графиков (в зависимости от вида использованной методики).

Методические критерии: четкое соблюдение процедуры применения выбранной методики исследования.

Технические характеристики. Структура презентации: не более 5 слайдов; первый слайд должен содержать название темы доклада, Ф.И.О. автора, номер группы и наименование направления подготовки; последующие слайды должны раскрывать этапы, процедуру и результаты исследования. Оформление презентации: единый стиль, сочетаемость цветов, ограниченное, удобочитаемое количество объектов на слайде, использование анимационных объектов. Временной регламент выступления с презентацией: 7–10 минут.

*Критерии оценки.*

По теме 4 проектная деятельность оценивается максимум в 3 балла. Они выставляются студенту при соблюдении всех вышеуказанных требований к качественным, методическим и техническим критериям разработки и реализации проекта. 2 балла выставляется при незначительных нарушениях требований к научному изложению выводов и их полноте, оформлению итогового результата, но соблюдении всех иных вышеуказанных требований. 1 балл выставляется при незначительных нарушениях требований к научному изложению выводов и их полноте, оформлению итогового результата, незначительном искажении критического взгляда на ситуацию, но соблюдении всех иных вышеуказанных требований. 0 баллов ставится при наличии систематических ошибок в выполненном задании, а также в случае отсутствия результатов исследования у исполнителя.

По темам 11 и 13 проектная деятельность оценивается максимум в 7 баллов. Они выставляются студенту при соблюдении всех вышеуказанных требований к качественным, методическим и техническим критериям разработки и реализации проекта. 6 баллов выставляется при нарушении научного стиля изложения выводов, но соблюдении всех иных вышеуказанных требований. 5 баллов выставляется при незначительных нарушениях требований к научному изложению выводов и оформлению итогового результата, но соблюдении всех иных вышеуказанных требований. 4 балла выставляется при множественных нарушениях требований к научному изложению выводов, оформлению итогового результата, визуализации результатов исследования, но соблюдении всех иных вышеуказанных требований. 3 балла выставляется при множественных нарушениях требований к научному изложению выводов, оформлению итогового результата, визуализации результатов исследования, а также незначительных нарушениях процедуры исследования. 2 балла выставляется при систематических нарушениях процедуры исследования (вне зависимости от соблюдения иных вышеуказанных требований). 1 балл выставляется при множественных нарушениях процедуры исследования (вне зависимости от соблюдения иных вышеуказанных требований). 0 баллов ставится в случае отсутствия результатов исследования у исполнителя.

### **III. Подготовка к промежуточной аттестации.**

*Устное собеседование* – итоговая беседа студента с преподавателем на зачете, в ходе которого выявляется качество сформированного знаниевого и функционального компонентов обучения. Зачет завершается оценкой, выраженной в словесной форме («зачтено» или «не зачтено»).

Студентам предлагается ответить на 1 вопрос из нижеприведенного списка вопросов, выданного преподавателем в начале семестра. В случае, если студент дает неполный ответ на вопрос, преподаватель имеет право задать уточняющие вопросы.

Оцениваются качество и полнота ответа, отражающие степень подготовки студента к зачету.

*Критерии оценки.*

При проведении промежуточной аттестации максимальный балл за оценку готовности к зачету составляет 9. В случае получения неверного ответа от студента на поставленный вопрос результаты студента считаются неудовлетворительными, и он направляется на пересдачу (0 баллов). В случае получения неполного ответа на вопрос преподаватель артикулирует дополнительные вопросы, позволяющие ему определиться между оценками «зачтено» и «не зачтено» (1–8 баллов). Для получения оценки «зачтено» студент должен дать исчерпывающий ответ на вопрос (9 баллов).

В случае, если студент отвечает на меньшую оценку (при сопоставлении с оценкой, полученной в ходе балльно-рейтинговой квалификации по итогам освоения курса), преподаватель ставит фактическую оценку за ответ на зачете.

*Перечень вопросов для подготовки к зачету.*

1. Понятие информационной войны и его соотношение с терминами «информационная война», «информационное противоборство», «сетевая война», «гибридная война».

2. Психологический подход к интерпретации информационной войны.

3. Социально-коммуникативный подход к интерпретации информационной войны.

4. Интегративный подход к интерпретации информационной войны.

5. Геополитический подход к интерпретации информационной войны.

6. Конфликтологический подход к интерпретации информационной войны.

7. Системный подход к интерпретации информационной войны.

8. Информационная война как средство борьбы.

9. Информационная война как средство продвижения имиджа.

10. Информационная война как средство фальсификации исторических фактов.

11. Структура информационной войны.

12. Виды информационных войн.

13. Информационный терроризм.

14. Хакерство.

15. Информационные войны первого поколения.

16. Информационные войны второго поколения.

17. Информационная кампания.

18. Способы ведения информационной войны.

19. Формы информационной борьбы.

20. Этапы информационной войны.

21. Понятие и виды информационного оружия.

22. Материалы информационно-психологического воздействия.

23. Концепция «трех войн» КНР.

24. Информационная война как способ достижения территориальных целей Японии.

25. Использование информационного оружия Европейским союзом в целях реализации публичной дипломатии.

26. Объединенная доктрина информационных операций США.

27. Доктрина информационной безопасности Российской Федерации.

28. Информационная война в армяно-азербайджанских отношениях (1998–2009 гг.).

29. Информационная война в российско-грузинских отношениях (1991–2012 гг.).

30. Информационная война в российско-украинских отношениях (2013–2024 гг.).

31. Информационная война в американо-иракских отношениях (2003–2011 гг.).

32. Информационная война в японо-китайских отношениях (2013–2014 гг.).

33. Взаимосвязь категорий «информационная война», «гибридная война» и «цветная революция».

34. Возможности применения информационного оружия на каждом этапе реализации «цветных революций».

35. Причины и условия перерастания «цветной революции» в «гибридную войну».

36. Сценарий «цветной революции» в Югославии. Практика применения информационного оружия.

37. Сценарий «цветной революции» в Грузии. Практика применения информационного оружия.

38. Сценарий «цветной революции» в Ливии. Практика применения информационного оружия.

39. Сценарий «цветной революции» в Египте. Практика применения информационного оружия.

40. Сценарий «цветной революции» в Тунисе. Практика применения информационного оружия.

41. Сценарий «цветной революции» в Сирии. Практика применения информационного оружия.

42. Сценарий «цветной революции» на Украине. Практика применения информационного оружия.

43. Понятие, цели защиты информации и ее виды.

44. Защита государства от информационно-психологического воздействия.

45. Защита государства от информационно-технического воздействия.

46. Защита государства от непреднамеренных взаимных радиоэлектронных помех.

47. Защита государства от средств радиоэлектронного поражения противника.

48. Защита государства от радиоэлектронной разведки.

49. Защита государства от средств функционального поражения.

50. Система обеспечения информационной безопасности и ее объекты в сфере обороны.

51. Система обеспечения информационной безопасности и ее объекты во внешней политике.

52. Содержание Окинавской хартии глобального информационного общества от 22 июля 2000 г. и ее значение для обеспечения международной информационной безопасности государств.

53. Содержание доклада правительственных экспертов по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности от 30 июля 2010 г. и его значение для обеспечения международной информационной безопасности государств.

54. Содержание Резолюции Генеральной Ассамблеи ООН А/69/435 от 2 декабря 2014 г. «Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности» и ее значение для обеспечения международной информационной безопасности государств.

55. Содержание докладов Генерального секретаря ООН от 16 июля 2013 г., 9 сентября 2013 г. и 30 июня 2014 г. «Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности» и их значение для обеспечения международной информационной безопасности государств.

56. Международные организации, играющие значительную роль в обеспечении международной информационной безопасности государств.

57. Характеристика системы обеспечения информационной безопасности в Европейском Союзе.

58. Характеристика системы обеспечения информационной безопасности в Японии.

59. Характеристика системы обеспечения информационной безопасности в США.

60. Характеристика системы обеспечения информационной безопасности в Российской Федерации.

4. Рекомендации по самоподготовке к промежуточной аттестации по дисциплине.

В целях эффективной организации **самостоятельной подготовки к промежуточной аттестации** необходимо следовать нижеприведенным правилам.

**Правило 1:** повторить пройденный в рамках дисциплины материал (это поможет закрепить приобретенные знания и подготовиться к зачету):

- начните с общего обзора дисциплины, освежите в памяти основные темы, прочитайте конспекты лекций;

- используйте активные методы повторения, такие как обсуждение тем с одногруппниками (групповой тренинг); ответы на вопросы, помещенные в конце глав учебников, рекомендованных к изучению преподавателем; создание карточек-подсказок; поиск примеров из практики, подтверждающих научные факты; многократный пересказ прочитанного в лекциях / учебниках / научных статьях и монографиях материала сразу после его прочтения; запоминание с отсроченным воспроизведением материала (пересказ выученного материала через установленный для себя промежуток времени – каждые 3 часа, день, сутки и т.д.);

- ознакомьтесь заново с практическими заданиями, которые выполнялись на семинарских занятиях и предполагали самостоятельную подготовку к ним;

- не забывайте делать перерывы во время повторения материала, чтобы избежать усталости и повысить эффективность работы коры головного мозга, отвечающей за долговременную память человека;

- в утренние или дневные часы предшествующего зачету дня повторите ключевые моменты по каждой теме, вечером рекомендуется расслабиться, дать мозгу отдохнуть.

**Правило 2:** обратить внимание на наиболее сложные темы дисциплины (начните изучение с них, чтобы подробно разобраться в тонких моментах и уделить больше времени многоаспектным вопросам):

- тема 4 «Концепции информационных войн стран, входящих в состав Европы, Азиатско-Тихоокеанского региона, Северной Америки, СНГ»;

- тема 5 «Характеристика информационных войн с участием стран, входящих в состав Азиатско-Тихоокеанского региона, Ближнего Востока, Северной Америки, СНГ».

**Правило 3:** подробно ознакомиться со списком литературы по дисциплине, который рекомендовал для изучения преподаватель в начале учебного процесса.

**Рекомендуемый для изучения список литературы по дисциплине.**

*Основная литература:*

*Украинцев Ю.Д.* Информатизация общества: учебное пособие (Глава 8). – СПб.: – Издательство «Лань», 2022. – 220 с. – Текст: электронный // Лань: электронно-библиотечная система. – URL: <https://reader.lanbook.com/book/207002#1>. Режим доступа: для авториз. пользователей.

*Цыганов В.В., Бухарин С.Н.* Информационный менеджмент: механизмы управления и борьбы в бизнесе и политике: Словарь-справочник. – М.: Академический проект, 2020. – 506 с. – URL: <https://www.iprbookshop.ru/epd-reader?publicationId=94866>. Режим доступа: для авториз. пользователей.

*Дербин Е.А.* Информационное противоборство: концептуальные основы обеспечения информационной безопасности: учебное пособие / Е.А. Дербин, А.В. Царегородцев. – Москва: ИНФРА-М, 2024. – 267 с. – (Высшее образование). – DOI 10.12737/2084342. – ISBN 978-5-16-019050-1. – Текст: электронный. – URL: <https://znanium.ru/catalog/product/2084342>. – Режим доступа: по подписке.

*Дополнительная литература:*

*Клименко И.С.* Информационная безопасность и защита информации: модели и методы управления: монография / И.С. Клименко. – Москва: ИНФРА-М, 2024. – 180 с. – (Научная мысль). – DOI 10.12737/monography\_5d412ff13c0b88.75804464. – ISBN 978-5-16-015149-6. – Текст: электронный. – URL: <https://znanium.com/catalog/product/2052391>. – Режим доступа: по подписке.

*Звягин А.А.* Россия в гибридной войне. Информационно-психологическая безопасность: монография / А.А. Звягин, Б.А. Артамонов, И.А. Мельников. – 2-е изд., перераб. и доп. – Москва: ИНФРА-М, 2024. – 329 с. – (Научная мысль). – ISBN 978-5-16-

112272-3. – Текст: электронный. – URL: <https://znanium.ru/catalog/product/2134590>. Режим доступа: по подписке.

Информационная война в условиях специальной военной операции. Опыт лингвистического анализа : монография / под общ. ред. *О.И. Калинина*. – Москва: ФЛИНТА, 2024. – 272 с. – ISBN 978-5-9765-5336-1. – Текст: электронный. – URL: <https://znanium.ru/catalog/product/2138733>. Режим доступа: по подписке.

*Кушнерук С.Л.* Идеологическое миромоделирование в контексте информационно-психологической войны: монография / С.Л. Кушнерук. – Москва: ФЛИНТА, 2023. – 232 с. – ISBN 978-5-9765-5274-6. – Текст: электронный. – URL: <https://znanium.com/catalog/product/2079222>. Режим доступа: по подписке.

*Леона А.В.* Информационно-психологическая война в философском и лингвистическом осмыслении: монография / А.В. Леона, О.В. Фельде, К.В. Волчок. – Красноярск: Сибирский федеральный университет, 2022. – 152 с. – ISBN 978-5-7638-4633-1. – Текст: электронный. – URL: <https://znanium.com/catalog/product/2091871>. Режим доступа: по подписке.

*Лепский В.Е.* Технологии управления в информационных войнах (от классики к постнеклассике) / В.Е. Лепский. – Москва: Когито-Центр, 2016. – 161 с. – ISBN 978-5-89353-499-3. – Текст: электронный // Цифровой образовательный ресурс IPR SMART: [сайт]. – URL: <https://www.iprbookshop.ru/88122.html>. Режим доступа: для авторизир. пользователей.

*Макаренко С.И.* Информационное противоборство и радиоэлектронная борьба в сетевых войнах начала XXI века: монография / С.И. Макаренко. – Санкт-Петербург, 2017. – 546 с. – ISBN 978-5-9909412-1-2. – Текст: электронный // Лань: электронно-библиотечная система. – URL: <https://e.lanbook.com/book/>. Режим доступа: для авториз. пользователей.

*Манойло А.В.* Государственная информационная политика в особых условиях: монография. Москва, 2003. – 388 с. – URL: [https://yurbus.su/f/manoyloav\\_gos\\_informatsionnaya\\_politika\\_chast\\_1.pdf](https://yurbus.su/f/manoyloav_gos_informatsionnaya_politika_chast_1.pdf) Режим доступа: свободный.

### **Вопросы для самопроверки перед зачетом.**

*Тема 1 «Понятие и основные характеристики информационной войны».*

1.1. Каковы основные характеристики информационной войны, отличающие ее от традиционных войн?

1.2. Какие факторы способствуют возникновению информационных войн в современном мире?

*Тема 2 «Структура и виды информационных войн».*

2.1. Какие существуют виды информационных войн?

2.2. Какие элементы входят в структуру информационной войны?

*Тема 3 «Информационное оружие и этапы информационной войны».*

3.1. Что такое информационное оружие?

3.2. Как информационное оружие используется в контексте информационных войн?

*Тема 4 «Концепции информационных войн стран, входящих в состав Европы, Азиатско-Тихоокеанского региона, Северной Америки, СНГ».*

4.1. В чем заключаются отличия во взглядах к информационному нападению и информационной защите стран, входящих в состав Европы, Азиатско-Тихоокеанского региона, Северной Америки, СНГ?

4.2. Как определяется информационная война во внешнеполитических / стратегических документах стран, входящих в состав Европы, Азиатско-Тихоокеанского региона, Северной Америки, СНГ?

*Тема 5 «Характеристика информационных войн с участием стран, входящих в состав Азиатско-Тихоокеанского региона, Ближнего Востока, Северной Америки, СНГ».*

5.1. Какие примеры информационных войн можно привести в отношении стран, входящих в состав Азиатско-Тихоокеанского региона, Ближнего Востока, Северной

Америки, СНГ?

5.2. Какова роль информационных войн в современных конфликтах, затрагивающих страны, входящие в состав Азиатско-Тихоокеанского региона, Ближнего Востока, Северной Америки, СНГ?

*Тема 6 «Информационные войны и «цветные революции» как технологии реализации «гибридных войн».*

1.1. Как информационные войны способствуют возникновению и развитию «цветных революций»?

1.2. В чем заключается связь между «гибридными войнами» и использованием информационных / цифровых технологий?

*Тема 7 «Информационная безопасность и ее обеспечение».*

7.1. Что такое информационная безопасность?

7.2. Соблюдение каких индивидуальных и общественных правил уменьшает риски распространения информационных угроз?

*Тема 8 «Наднациональная информационная безопасность: правовая и институциональная составляющие».*

8.1. Какие глобальные угрозы информационного характера существуют в современном мире?

8.2. Какие наднациональные структуры ориентированы на решение проблем глобальной информационной безопасности?