Приложение 4

к образовательной программе

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Б1.В.ДВ.06.02 «Информационные войны»
(индекс, наименование дисциплины в соответствии с учебным планом)

38.03.01 Экономика
(код, наименование направления подготовки/специальности)

Инвестиционный бизнес
(наименование образовательной программы)

Очная/очно-заочная форма обучения
(форма обучения)

Год набора - 2025

Санкт-Петербург

Автор(ы)-составитель(и) РПД:

Рыжих Линда Викторовна, к.э.н., доцент кафедры менеджмента

Заведующий кафедрой:

Лабудин Александр Васильевич, доктор экономических наук, профессор, заведующий кафедрой менеджмента

Рабочая программа дисциплины Б1.В.ДВ.06.02 «Информационные войны» одобрена на заседании кафедры менеджмента факультета экономики и финансов СЗИУ РАНХиГС.

протокол № 7 от «27» августа 2025 г.

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. Содержание и структура дисциплины

4. Типы оценочных материалов, показатели и критерии их оценивания

5. Формы аттестации, типовые оценочные материалы для текущего контроля успеваемости обучающихся, критерии и шкалы оценивания по контрольным точкам

6. Формы промежуточной аттестации, критерии и шкала оценивания, типовые оценочные материалы по дисциплине

7. Методические материалы по освоению дисциплины

8. Учебная литература и ресурсы информационно-телекоммуникационной сети «Интернет»

9. 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

Дисциплина Б1.В.ДВ.06.02 «Информационные войны» обеспечивает формирование у обучающихся следующих универсальных, общепрофессиональных и профессиональных компетенций*:

ОТФ/ ТФ и реквизиты ПС *(при наличии)***	**Код компетенции ****	**Наименование Компетенции ****	**Код индикатора достижения компетенций ****	**Наименование индикатора достижения компетенций ****	**Образовательный результат ****
	УК ОС-5	Способен проявлять толерантность в условиях межкультурного разнообразия общества в социально-историческом и философском контекстах, соблюдать нормы этики и использовать дефектологические знания в социальной и профессиональной сферах	УК ОС-5.1	Обосновывает собственную позицию по вопросам толерантности и дискриминации	УК ОС-5.1 З-1 Знает социальные, этнические, конфессиональные и культурные особенности представителей социальных, в том числе этноконфессиональных общностей УК ОС-5.1 У-1 Умеет готовить специальные информационные мероприятия и применять их
	УК ОС-5	Способен проявлять толерантность в условиях межкультурного разнообразия общества в социально-историческом и философском контекстах, соблюдать нормы этики и использовать дефектологические знания в социальной и профессиональной сферах	УК ОС-5.2	Проявляет толерантность в общении в условиях межкультурного разнообразия общества	УК ОС-5.2 З-1 Знает содержание культурных особенностей и традиций народов России, обусловленных историческим контекстом становления российской цивилизации УК ОС-5.2 У-1 Умеет проявлять толерантность в общении в условиях межкультурного разнообразия общества

** Дисциплина может формировать компетенцию полностью или частично.*

***Должно соответствовать Приложению 1 к образовательной программе*

2. Объем и место дисциплины в структуре образовательной программы

Объем дисциплины

Объем дисциплины и виды учебной работы.

Общая трудоемкость дисциплины составляет 3 зачетные единицы/108 академических/81 астрономический час.

Теоретические занятия (лекции) проводятся по потокам. Общий объем лекционного курса по очной форме обучения составляет 16 академических часов, по очно-заочной форме обучения составляет 8 академических часов.

Практические занятия организуются по группам в виде семинаров в диалоговом режиме. Общий объем практических занятий по очной форме составляет 24 академических часов, по очно-заочной форме обучения составляет 12 академических часов.

Программой предусмотрена самостоятельная работа студентов по очной форме обучения в объеме 66 академических часов, по очно-заочной форме обучения в объеме 86 академических часов. В рамках самостоятельной работы студенты изучают теоретический материал в целях подготовки к устному опросу и тестированию, выполняют практико-ориентированные задания, готовятся к выполнению контрольных заданий.

Место дисциплины в структуре ОП ВО

Дисциплина Б1.В.ДВ.06.02 «Информационные войны» относится к циклу дисциплин по выбору по направлению бакалавриата 38.03.01 «Экономика», направленность (профиль) «Инвестиционный бизнес». Изучается по очной форме обучения в 7-ом семестре (первый семестр 4-го курса), по очно-заочной форме обучения в 9-ом семестре (первый семестр 5-го курса).

Курс опирается на знание следующих дисциплин: Б1.О.06 «Экономическая информатика», Б1.В.01 «Цифровое общество, введение в искусственный интеллект и разговорные боты», Б1.В.05 «Политология», «Цифровые технологии в менеджменте», Б1.В.ДВ.03.02 «Цифровая экономика», Б1.О.02 «Основы российской государственности».

Знания, умения и навыки, полученные при изучении дисциплины, используются студентами при подготовке и сдаче государственного экзамена.

Формой промежуточной аттестации в соответствии с учебным планом является зачет с оценкой.

3. Содержание и структура дисциплины

3.1. Структура дисциплины

Очная форма обучения

№ п/п	Наименование тем и (или) разделов		Объем дисциплины, ак.час												Форма текущего контроля успеваемости, промежуточной аттестации
		ВСЕГО	Контактная работа обучающихся с преподавателем по видам учебных занятий									Самостоятельная работа			
			Период теоретического обучения						Период промежуточной аттестации (сессия)						
			Занятия лекционного типа		Занятия семинарского типа		ИК	КСР	КЭ	Кат тэк	Контроль	СРкр	СРэк	СР	
			Л	ВЛ	ЛР	ПЗ									
Тема 1	Информационное общество	34	4			8								22	Д
Тема 2	Сущность, источники и средства	36	6			8								22	О, Д

	информационных войн													
Тема 3	Виды и технологии информационных войн	36	6			8							22	О, ПОЗ
Промежуточная аттестация		2							2					Зачет с оценкой
Итого		108	16			24			2				66	

Очно-заочная форма обучения

№ п/п	**Наименование тем и (или) разделов**		**Объем дисциплины, ак.час**												Форма текущего контроля успеваемости, промежуточной аттестации
		ВСЕГО	**Контактная работа обучающихся с преподавателем по видам учебных занятий**									**Самостоятельная работа**			
			Период теоретического обучения						**Период промежуточной аттестации (сессия)**						
			Занятия лекционного типа		**Занятия семинарского типа**		**ИК**	**КСР**	**КЭ**	**Кат тэк**	**Контро**	**СРкр**	**СРэк**	**СР**	
			Л	**ВЛ**	**ЛР**	**ПЗ**									

											л ь				
Тема 1	Информационное общество	36	2			4								30	Д
Тема 2	Сущность, источники и средства информационных войн	35	3			4								28	Д, Т
Тема 3	Виды и технологии информационных войн	35	3			4								28	О, Д, ПОЗ
Промежуточная аттестация		2							2						Зачет с оценкой
Итого		108	8			12								86	

Используемые сокращения:

Л – лекции - занятия, предусматривающие преимущественную передачу учебной информации обучающимся педагогическими работниками организации и (или) лицами, привлекаемыми организацией к реализации образовательных программ на иных условиях,).

ВЛ – видео лекции.

ЛР – лабораторные работы.

ПЗ – практические занятия (за исключением лабораторных работ).

ИК – индивидуальные консультации.

КСР – контроль самостоятельной работы

КЭ – консультации перед экзаменом

Каттэк – контактная работа на аттестацию в период экзаменационных сессий
Контроль - контактная работа на аттестацию в период экзаменационных сессий для заочной формы обучения
СРкр – самостоятельная работа на подготовку курсовой работы/ курсового проекта.
СРэк – самостоятельная работа на подготовку к экзамену.
СР – самостоятельная работа в семестре на подготовку к учебным занятиям.
Т – тестирование.
Д – доклад.
О – опрос.
ПОЗ – практико-ориентированные задания.

В процессе обучения применяются следующие интерактивные формы: лекция-диалог, работа в малых группах, спарринг-партнерство.

3.2. Содержание дисциплины

Тема 1. Информационное общество. УК ОС-5.1. УК ОС-5.2.

Подходы к пониманию сущности информационного общества.

Рассматриваются концепции и подходы к определению понятия «информационное общество»: теория постиндустриального общества Дэниела Белла, концепция информационного капитализма Мануэля Кастельса, идеи Николаса Негропонте и Элвина Тоффлера. Обоснование перехода от индустриальной экономики к экономике, основанной на знаниях и информации.Основные характеристики информационного общества. Определение ключевых признаков информационного общества: глобализация коммуникаций, информатизация всех сфер общественной жизни, распространение цифровых технологий, рост значения информации и знаний как основного ресурса производства и управления обществом. Проблемы и угрозы, связанные с развитием информационного общества. Анализ негативных последствий информационного общества: цифровое неравенство, риски утраты приватности, проблемы информационной

перегрузки, влияние социальных сетей и медиа на поведение и мышление людей, возникновение новых форм манипуляций и психологического давления.

Тема 2. Сущность, источники и средства информационных войн. УК ОС-5.1, УК ОС-5.2.

Подходы к пониманию сущности информационных войн. Обзор теоретических подходов к изучению феномена информационных войн: геополитические трактовки (Джозеф Най, Нассир Абд аль-Хаким), кибернетические модели (Маркус Хеннер), культурологический подход (Хосе Луис Перальта). Определение целей и функций информационных войн в современной международной среде. Источники и средства информационно-психологического воздействия. Классификация инструментов информационно-психологической борьбы: пропаганда, контрпропаганда, манипуляция сознанием, использование средств массовой информации и массовых коммуникаций. Рассмотрение роли национальных институтов и негосударственных акторов в создании условий для начала и ведения информационных войн. Использование средств информационно-психологического воздействия при проведении информационных кампаний и информационных войн. Описание особенностей взаимодействия информационных технологий и традиционных средств массовой информации в рамках информационных операций. Анализ методик влияния на общественное мнение через управление информацией и контроль над каналами распространения сведений. Цель, особенности, основные направления ведения информационных войн. Характеристика структуры и содержания современных информационных войн: политическая составляющая, экономическая направленность, социально-культурные цели. Изучение специфики информационных воздействий в мирное и военное время, сравнение способов достижения стратегических целей путем информационной атаки и обороны.

Тема 3. Виды и технологии информационных войн. УК ОС-5.1, УК ОС-5.2.

Виды информационных войн, их характеристика. Классификация типов информационных войн: когнитивная, психологическая, кибернетическая, виртуальная, массовая. Оценка уровня и интенсивности информационного противостояния на разных уровнях: локальном, региональном, международном. Провокация в информационных войнах. Особый вид тактик провокационного характера: инсценировки, фальсификация фактов, создание ложных слухов и мифов. Описание моделей провоцирования конфликтов через масс-медиа и социальные сети. Типовая модель информационной войны. Представление классической схемы информационной войны: сбор информации, обработка данных, принятие решений, проведение операции. Выделение этапов развертывания конфликта и закрепления достигнутых результатов.

Информационное оружие: определение, особенности, виды. Изучение понятий «информационное оружие», выявление отличительных характеристик, классификация видов оружия по целям и последствиям. Обзор возможных эффектов воздействия информационных ударов на психику и сознание индивидов и сообществ. Манипулятивные техники в информационных процессах. Подробный разбор техник манипуляции в СМИ и социальных сетях: эффект поляризации, искажение информации, эксплуатация стереотипов, эвристики массового сознания. Особенности политического маркетинга и политтехнологий в процессе агитации и пропаганды. Информационная война как форма политической мобилизации. Оценка связи политических процессов и информационно-пропагандистских мероприятий. Примеры успешного применения информационных ресурсов для усиления политической активности населения и мобилизации электорального потенциала. Исследование информационных войн на современном этапе. Актуальные исследования и тенденции изменения природы информационных войн. Прогнозирование динамики информационных процессов и перспектив появления новых технологий. Методы сбора и обработки данных об информационных войнах и информационных потоках. Практические методики мониторинга, анализа и оценки состояния информационной среды. Применение специальных программных продуктов и инструментов анализа больших объемов данных (Big Data) для выявления тенденций и закономерностей в распространении информации.

4. Типы оценочных материалов, показатели и критерии оценивания

1.1. Оценочные материалы по дисциплине Б1.В.ДЭ.06.02 «Информационные войны» входят в состав оценочных материалов по образовательной программе. Совокупность оценочных материалов по всем дисциплинам образовательной программы составляет фонд оценочных средств (далее – ФОС). ФОС используется при проведении текущего контроля успеваемости и промежуточной аттестации обучающихся с целью оценивания достижения обучающимися планируемых результатов обучения.

4.2. ФОС разработан как комплекс проверочных заданий различного типа и уровня сложности, включает критерии и шкалы оценивания, а также «ключи» правильных ответов. ФОС формируется как отдельный документ и хранится в электронном виде, доступ к ФОС предоставлен ограниченному кругу лиц.

4.3. Для самостоятельной работы обучающихся при подготовке к текущему контролю успеваемости и

промежуточной аттестации в рабочих программах дисциплин размещены типовые проверочные задания, которые можно условно разделить на задания закрытого, комбинированного и открытого типов.

Задания закрытого типа — это тестовые задания, в которых каждый вопрос сопровождается готовыми вариантами ответов, из которых необходимо выбрать один или несколько правильных.

Задания комбинированного типа – это тестовые задания, в которых каждый вопрос сопровождается готовыми вариантами ответов, из которых необходимо выбрать один или несколько правильных и обосновать свой выбор.

Задания открытого типа — это задания, в которых на каждый вопрос должен быть предложен развернутый обоснованный ответ.

В зависимости от типа задания рекомендованы определенная последовательность выполнения и система оценивания выполнения заданий.

4.4. Типы заданий, сценарии выполнения, критерии оценивания

ТИП ЗАДАНИЯ	ИНСТРУКЦИЯ	СЦЕНАРИИ ВЫПОЛНЕНИЯ	КРИТЕРИИ ОЦЕНИВАНИЯ
Задание закрытого типа с выбором одного правильного ответа из нескольких вариантов предложенных	Прочитайте текст, выберите правильный ответ	1.Внимательно прочитать текст задания и понять, что в качестве ответа ожидается только один из предложенных вариантов. 2. Внимательно прочитать предложенные вариант-ты ответа. 3. Выбрать один верный ответ. 4. Записать только номер (или букву) выбранного варианта ответа (например, 3 или В).	Ответ считается верным, если правильно указана цифра или буква
Задание закрытого типа на установление соответствия	Прочитайте текст и установите соответствие	1.Внимательно прочитать текст задания и понять, что в качестве ответа ожидаются пары элементов. 2. Внимательно прочитать оба списка: список 1 – вопросы, утверждения, факты, понятия и т.д.; список 2 – утверждения, свойства объектов и т.д. 3. Сопоставить элементы списка 1 с элементами списка 2, сформировать пары элементов. 4. Записать попарно буквы и цифры (в зависимости от задания) вариантов ответа (например, А1 или Б4).	Ответ считается верным, если правильно указаны цифры или буквы
Задание закрытого типа с выбором нескольких	Прочитайте текст, выберите правильные ответы	1.Внимательно прочитать текст задания и понять, что в качестве ответа ожидается несколько правильных ответов из предложенных вариантов.	Ответ считается верным, если правильно установлены все соответствия (позиции из

правильных ответов из нескольких вариантов предложенных		2. Внимательно прочитать предложенные вариант-ты ответа. 3. Выбрать несколько правильных ответов. 4. Записать только номера (или буквы) выбранного варианта ответа (например, 1 4 или А Г).	одного столбца верно сопоставлены с позициями другого)
Задание закрытого типа на установление последовательности	Прочитайте текст и установите последовательность	1. Внимательно прочитать текст задания и понять, что в качестве ответа ожидается последовательность элементов. 2. Внимательно прочитать предложенные варианты ответа. 3. Построить верную последовательность из предложенных элементов. 4. Записать буквы/цифры (в зависимости от задания) вариантов ответа в нужной последовательности (например, БВА или 135).	Ответ считается верным, если правильно указана вся последовательность цифр
Задание комбинированного типа с выбором одного правильного ответа из предложенных и обоснованием выбора	Прочитайте текст, выберите правильный ответ и запишите аргументы, обосновывающие выбор ответа	1.Внимательно прочитать текст задания и понять, что в качестве ответа ожидается только один из предложенных вариантов. 2. Внимательно прочитать предложенные варианты ответа. 3. Выбрать один верный ответ. 4. Записать только номер (или букву) выбранного варианта ответа.	Ответ считается верным, если правильно указана цифра или буква и приведены корректные аргументы, используемые при выборе ответа

		5. Записать аргументы, обосновывающие выбор ответа (например, 4 текст обоснования).	
Задание открытого типа с развернутым ответом	Прочитайте текст и запишите развернутый обоснованный ответ	1. Внимательно прочитать текст задания и понять суть вопроса. 2.Продумать логику и полноту ответа. 3.Записать ответ, используя четкие компактные формулировки. 4.В случае расчетной задачи, записать решение и ответ	Ответ считается верным: 1. Отсутствие фактических ошибок. 2. Раскрытие объема используемых понятий (полнота ответа). 3.Обоснованность ответа (наличие аргументов). 4. Логическая последовательность излагаемого материала.

4.5. Общая шкала оценивания результатов текущего контроля успеваемости и промежуточной аттестации обучающихся с применением БРС

Итоговая балльная оценка	Традиционная система	Бинарная система	ECTS	
			Для традиционной системы	Для бинарной системы
95-100	Отлично	Зачтено	A	P/ Passed
85-94			B	P/ Passed
75-84	Хорошо		C	P/ Passed
65-74			D	P/ Passed
55-64	Удовлетворительно		E	P/ Passed
0-54	Неудовлетворительно	Не зачтено	F	F/Failed

Соотношение баллов за текущий контроль успеваемости и промежуточную аттестацию, а также повторную промежуточную аттестацию:

Максимальная сумма баллов за текущий контроль успеваемости	Максимальная сумма баллов за промежуточную аттестацию	Максимальная итоговая балльная оценка	Максимальная сумма баллов за повторную промежуточную аттестацию
60 баллов	40 баллов	100 баллов	100 баллов

5. Формы аттестации, типовые оценочные материалы для текущего контроля успеваемости обучающихся, критерии и шкалы оценивания по контрольным точкам

5.1. В ходе реализации дисциплины используются следующие формы текущего контроля успеваемости обучающихся (в том числе, задания к контрольным точкам): тестирование, доклад, опрос, практико-ориентированные задания.

Тема 1. Информационное общество.

Типовые темы для докладов по теме 1.

1. Новые профессии и рынки труда в условиях информационного общества.
2. Влияние информационных технологий на политическую активность и социальное взаимодействие.
3. Цифровая экономика и её роль в трансформации общественных структур.
4. Становление и развитие культуры креативного класса в российском обществе.
5. Трансформация культуры потребления информации в эпоху

мобильных устройств.

6. Роль социальных сетей в изменении образа мышления и поведения людей.

Тема 2. Сущность, источники и средства информационных войн.

Типовые темы для докладов по теме 2.

1. Историко-теоретические предпосылки зарождения информационных войн.
2. Понятие и сущность информационной агрессии: современные подходы и дискуссии.
3. Информационный терроризм: понятие, признаки, примеры реализации.
4. Социальные сети и мессенджеры как средство ведения информационных операций.
5. Политическая психология и информационные войны: механизмы воздействия на массовое сознание.

Типовые тестовые задания по теме 2.

1. Что такое информационная война?
а) военное столкновение двух стран с использованием вооруженных сил;
б) конфликт, проводимый исключительно посредством физического уничтожения противника;
в) процесс оказания целенаправленного информационного воздействия на сознание, волю и поведение оппонентов с целью добиться выгодных изменений ситуации;
г) формирование позитивного имиджа государства среди союзников.
2. Какие элементы относятся к средствам ведения информационных войн?
а) телевидение, радио, газеты, соцсети, рекламные ролики;
б) армейская техника, танки, авиация;
в) физическое уничтожение инфраструктуры противника;
г) экономические санкции и торговые эмбарго.
3. Какой термин обозначает процесс преднамеренного искажения действительности с целью вызвать определенное эмоциональное состояние у целевой аудитории?
а) дезинформация;
б) репортаж;
в) контент-анализ;
г) экспертное заключение.
4. Как называется совокупность каналов передачи информации, обеспечивающих доступ пользователей к данным?
а) центр принятия решений;
б) информационная инфраструктура;
в) рекламное агентство;

г) управление персоналом.
5. Чем является кибератака в контексте информационных войн?
а) атака вирусов и вредоносных программ на компьютерные системы противника;
б) вооруженный конфликт в физическом пространстве;
в) способ укрепления экономических связей;
г) средство повышения культурного уровня общества.
6. По каким критериям оценивается эффективность информационных кампаний?
а) количество жертв среди мирного населения;
б) объем выпущенной продукции предприятиями оборонного комплекса;
в) изменение настроений и мнений целевых аудиторий;
г) стоимость проведённой рекламной акции.
7. Что представляет собой фейк-ньюс?
а) специально подготовленная новость, содержащая недостоверную информацию с целью ввести аудиторию в заблуждение;
б) независимая аналитическая статья;
в) интервью известных политиков;
г) объективный репортаж журналиста.

Тема 3. Виды и технологии информационных войн.

Типовые темы для докладов по теме 3.

1.Классификация информационных войн: исторические этапы эволюции.
2.Психологическая война: механизм воздействия на коллективное сознание.
3.Тенденции развития современных информационных войн: прогноз и перспективы.
4.Информационные войны в киберпространстве: типы и специфика.
5.Традиционные и новые технологии ведения информационных войн.
6.Информация как оружие: технологические аспекты и инструменты.

Типовые вопросы для опроса по теме 3

1.Назовите основные классификации информационных войн и дайте характеристику каждой из них.
2.Что такое психологическая война и какие методы используются для её ведения?
3.Какими техническими возможностями обладает современная информационная война?
4.Какова роль соцсетей и интернет-платформ в современной информационной борьбе?
5. Что означает термин «информационное оружие» и какими свойствами оно обладает?
6. Какие меры профилактики необходимы для минимизации рисков информационной агрессии?

Типовые ПОЗ по теме 3.

1. Кейс «Выявление признаков информационной войны»

На основе исходных данных изучите публичный конфликт между двумя компаниями/брендами (например, судебные иски, обмен заявлениями в СМИ). Выявите 3–4 признака информационной войны (по критериям: ограничение доступа к информации, тиражирование однотипных нарративов, создание негативного фона).

Исходные данные: подборка статей, пресс-релизов, постов в соцсетях по конкретному кейсу.

2. Представьте, что ваша организация стала объектом информационной атаки (распространение слухов, фейков, негативных публикаций). Сформулируйте 3–5 тезисов контрнарратива, который:

-опровергает ложные утверждения;

-подчёркивает реальные действия компании;

-обращается к ценностям целевой аудитории.

Исходные данные: сценарий атаки (например, «компания скрывает вред от своего продукта»).

3.Спланируйте условную информационную операцию (для госструктуры или бизнеса) по одной из целей:

-дискредитация конкурента;

-продвижение нового продукта;

-снижение паники в кризисной ситуации.

Укажите: каналы распространения, ключевые месседжи, целевые группы, KPI успеха.

4. Проанализируйте несколько примеров фейковых новостей (из открытых источников). Для каждого:

-определите технологию создания (подмена контекста, монтаж, ложные эксперты);

-укажите признаки, по которым можно распознать фейк;

-предложите способ опровержения.

5. Составьте список из 5–7 потенциальных уязвимостей вашей организации (или вымышленной) для информационных атак. Для каждой выбранной организации:

-опишите сценарий реализации;

-предложите меру защиты (например, мониторинг соцсетей, тренинг сотрудников).

5.2. Типовые оценочные материалы для текущего контроля успеваемости обучающихся (вне контрольных точек):

приведены в п.6.2.

5.3.Один или несколько тематических блоков дисциплины завершаются контрольной точкой (далее – КТ). Текущий контроль успеваемости по

дисциплине предусматривает не менее 2 (двух) и не более 10 (десяти) КТ в течение периода освоения дисциплины.

Максимальное количество баллов за любой тип работ в рамках КТ составляет 100 (сто) баллов.

Распределение весовых коэффициентов по КТ в рамках текущего контроля успеваемости по дисциплине и формулы расчета:

Наименование контрольной точки	Максимальное количество баллов за работу в рамках КТ, которое может набрать студент	Коэффициент веса контрольной точки	Результат контрольной точки, участвующий в формировании итоговой балльной оценки по дисциплине (отражается в журнале БРС в СДО)
КТ - 1	100	0,20	20
КТ - 2	100	0,40	40
Итого:	х	0,6	60

Формула расчета результата контрольной точки:
Результат контрольной точки = Количество баллов за работу в рамках КТ х Коэффициент веса контрольной точки.

5.4. Формы текущего контроля успеваемости обучающихся в рамках КТ и типовые оценочные материалы:

КТ-1
Тема 1, Тема 2
Тестирование.
Доклад.

КТ-2
Тема 3
Опрос.
ПОЗ.
Доклад.

Для каждой формы текущего контроля успеваемости обучающихся в рамках КТ определены критерии оценивания результатов выполнения задания.

1. *Критерии оценивания тестирования:*

Критерии оценки	Диапазон баллов	Описание критерия
Количество правильных ответов	*0*	*Количество правильных ответов менее 55%*
	25	*Количество правильных ответов от 55% до 64%*
	50	*Количество правильных ответов от 65% до 74%*
	75	*Количество правильных ответов от 75% до 84%*
	100	*Количество правильных ответов от 85% до 100%*
Итого максимально:	100	

2. *Критерии оценивания опроса:*

Критерии оценки	Диапазон баллов	Описание критерия
Содержание и раскрытие темы	*0-20*	*Ответ полностью и точно раскрывает суть вопроса. Приведены ключевые факты, понятия, даты или данные. Раскрытие глубокое, а не поверхностное.*
Логика и структура ответа	*0-20*	*Ответ структурирован, есть тезис, аргументация и вывод. Мысли изложены последовательно, аргументы логично связаны и подкрепляют основную мысль.*
Грамотность и терминология	*0-20*	*Специальная терминология используется корректно. Ответ изложен научным, соответствующим дисциплине.*
Аргументация	*0-20*	*Все утверждения подкреплены доказательствами: примерами, формулами, ссылками на теории, цитатами или конкретными данными. Отсутствуют голословные утверждения.*
Полнота и лаконичность	*0-20*	*Дан исчерпывающий ответ на поставленный вопрос без избыточной, нерелевантной информации. Ответ демонстрирует умение выделять главное и*

		укладываться в требуемый объем.
Итого максимально:	100	

3. Критерии оценивания доклада:

Критерии оценки	Диапазон баллов	Описание критерия
Содержание и раскрытие темы	*0-20*	*Детальное, последовательное описание всех этапов с конкретными примерами*
Грамотность изложения	*0-20*	*Соблюдены все правила грамматики, орфографии и пунктуации*
Стилистика	*0-20*	*Единый стиль изложения, точные формулировки, уместное использование терминов, лаконичность*
Логика изложения	*0-20*	*Чёткая последовательность изложения, логические связи между частями текста, аргументы подтверждают выводы*
Оригинальность	*0-20*	*Уникальный подход к теме, нестандартные решения, инновационные идеи, собственная позиция автора*
Итого максимально:	100	

4. Критерии оценивания практико-ориентированного задания (ПОЗ):

Критерии оценки	Диапазон баллов	Описание критерия
Содержание и раскрытие выбранных понятий	*31-50*	*Детальное, последовательное описание всех понятий на примере выбранной системы*
	16-30	*Поверхностное описание без привязки к выбранной системе*
	0-15	*Понятия раскрыты минимально или не раскрыты вовсе*
Достоверность и актуальность информации	*16-20*	*Представленная информация подтверждена ссылками на источники*
	0-15	*Представленная информация частично подтверждена ссылками на источники или не подтверждена*
Количество выполненных	*30*	*Количество выполненных заданий от 85% до 100%*

заданий	*15*	*Количество выполненных заданий от 55% до 84%*
	0	*Количество выполненных заданий менее 55%*
Итого максимально:	100	

5.5. Описание дополнительных материалов и оборудования, необходимых для выполнения проверочных заданий (*при необходимости*).

Для решения задач открытого типа (кейсов, ПОЗ), тестовых заданий студенту разрешается использование калькулятора; программ для работы с электронными таблицами для обработки, анализа и визуализации данных. Для построения интеллект-карты и моделей в различных нотациях студенту можно использовать любой соответствующий онлайн-инструмент.

6. Формы промежуточной аттестации, критерии и шкала оценивания, типовые оценочные материалы по дисциплине

6.1. Промежуточная аттестация проводится в форме **зачета с оценкой**.

Зачёт проводится посредством устного опроса студента (диалога преподавателя со студентом) по билетам, цель которого заключается в выявлении индивидуальных достижений студента по пониманию основных положений дисциплины. Билеты содержат контрольные вопросы: по 3 вопроса (задания) в билете.

При реализации промежуточной аттестации в ЭО/ДОТ могут быть использованы следующие формы: устно в ДОТ - в форме обоснованных ответов на задания различного типа; письменно в СДО - в форме письменного решения заданий различного типа; тестирование в СДО.

6.2. Типовые оценочные материалы промежуточной аттестации.

Вопросы для подготовки к зачету.

1. Понятие информационной войны: определение, сущность, отличительные признаки.
2. Информационная война в системе современных конфликтов: место и роль.
3. Основные субъекты информационных войн: государства, негосударственные структуры, медиа, отдельные акторы.
4. Цели и задачи информационных войн на разных уровнях (стратегическом, оперативном, тактическом).

5. Правовое регулирование информационных войн: международные нормы и национальные законодательства.
6. Основные виды информационных войн (по М. Либики и другим классификациям).
7. Командно-управленческая информационная война: цели, методы, примеры.
8. Разведывательная информационная война: инструменты и каналы получения данных.
9. Электронная война: технические аспекты и воздействие на инфраструктуру.
10. Кибервойна: понятие, отличия от других видов, ключевые угрозы.
11. Экономическая информационная война: механизмы влияния на экономику противника.
12. Сетевая война: специфика, платформы, тактики ведения.
13. Основные технологии ведения информационных войн: обзор и характеристика.
14. Дезинформация и фейки: способы создания, распространения и распознавания.
15. Метод «информационного мусора»: механизм действия и цели применения.
16. Техника «смещение понятий»: примеры и последствия использования.
17. Информационное табу и цензура: сходства и различия, эффекты воздействия.
18. Рефлексивное управление: суть метода и примеры реализации.
19. Использование социальных сетей как инструмента информационной войны.
20. Медиавирусы и вирусный контент: принципы создания и распространения.
21. Боты и автоматизированные аккаунты: роль в информационных кампаниях.
22. Манипуляция поисковыми системами и алгоритмами рекомендаций.
23. Традиционные СМИ в информационных войнах: телевидение, радио, печатные издания.

24. Новые медиа как инструмент информационных войн: соцсети, мессенджеры, блоги.
25. Альтернативные платформы: даркнет, закрытые чаты, анонимные форумы.
26. Роль лидеров мнений и инфлюенсеров в информационных кампаниях.
27. Особенности распространения информации через мессенджеры и закрытые группы.
28. Государственные меры противодействия информационным войнам: правовые, технические, организационные.
29. Корпоративная защита от информационных атак: стратегии и инструменты.
30. Индивидуальная медиаграмотность: навыки распознавания и противодействия дезинформации.
31. Методы верификации информации в условиях информационной войны.
32. Роль образования и просвещения в формировании устойчивости к информационным атакам.
33. Международные механизмы регулирования и предотвращения информационных войн.
34. Анализ конкретных примеров информационных войн (на выбор: конфликты последних 10–15 лет).
35. Роль социальных сетей в эскалации и деэскалации информационных конфликтов.
36. Влияние информационных войн на общественное мнение: механизмы и последствия.
37. Этика информационных войн: моральные и гуманитарные аспекты.
38. Прогнозы развития информационных войн: новые технологии и тренды.
39. Влияние искусственного интеллекта на ведение информационных войн.
40. Перспективы международного регулирования информационных конфликтов.

Типовые проверочные задания для самоподготовки обучающегося к промежуточной аттестации:

ТИП ЗАДАНИЯ	СЦЕНАРИИ ВЫПОЛНЕНИЯ	ТИПОВЫЕ ЗАДАНИЯ
Задание закрытого типа с выбором одного правильного ответа из нескольких вариантов предложенных	1.Внимательно прочитать текст задания и понять, что в качестве ответа ожидается только один из предложенных вариантов. 2. Внимательно прочитать предложенные варианты ответа. 3. Выбрать один верный ответ. 4. Записать только номер (или букву) выбранного варианта ответа (например, 3 или В).	1. Какой из перечисленных методов является наиболее характерным для проведения информационных операций с целью дискредитации политического оппонента в социальных сетях? А. Публикация научных статей, опровергающих его политическую программу. Б. Организация публичных дебатов с участием экспертов и журналистов. В. Создание и распространение мемов и карикатур, высмеивающих его личностные качества или политические взгляды. Г. Финансирование благотворительных проектов, направленных на повышение его общественной репутации.
		2. Что такое информационная война в широком смысле? А. Военные действия с применением информационных технологий. А. Б. Комплекс мероприятий, направленных на достижение информационного превосходства над противником. В. Распространение ложной информации в СМИ. Г. Кибератаки на компьютерные сети.
		3. Что такое "информационное превосходство"? А. Превосходство в количестве компьютерной техники. А. Б. Способность контролировать информационное пространство и эффективно использовать информацию для достижения целей. Б. В. Превосходство в скорости передачи данных. В. Г. Превосходство в количестве новостных каналов. своего имиджа.
		4. Какой вид информационного воздействия направлен на изменение ценностей, убеждений и мировоззрения целевой аудитории? А. Дезинформация. Б. Пропаганда. В. Реклама. Г. PR (связи с общественностью).
		5. Что такое "информационная безопасность"? А. Защита компьютерной техники от поломок. Б. Состояние защищенности информации и поддерживающей инфраструктуры от случайных или преднамеренных воздействий, наносящих ущерб владельцам или пользователям информации. В. Защита от спама. Г. Защита авторских прав.
Задание закрытого типа на установление соответствия	1.Внимательно прочитать текст задания и понять, что в качестве ответа ожидаются пары	1. Установите соответствие между понятиями/определениями в левой колонке и соответствующими терминами/категориями в

	элементов. 2. Внимательно прочитать оба списка: список 1 – вопросы, утверждения, факты, понятия и т.д.; список 2 – утверждения, свойства объектов и т.д. 3. Сопоставить элементы списка 1 с элементами списка 2, сформировать пары элементов. 4. Записать попарно буквы и цифры (в зависимости от задания) вариантов ответа (например, А1 или Б4).	правой колонке. **Понятие** / **Термин/Категория** 1. Распространение тенденциозной информации с целью дискредитации — А. Информационная безопасность. 2. Выработка гипотезы проектного решения — Б. Дезинформация. 3. Разработка паспорта проекта — В. Пропаганда. 4. Реализация проекта — Г. Черный пиар. 2. Установите соответствие между видом информационной атаки и его описанием. **Описание атаки** / **Вид атаки** 1.Попытки получить несанкционированный доступ к конфиденциальной информации — А. Фишинг. 2.Распространение вредоносного программного обеспечения — Б. DDoS-атака. 3. Массовая рассылка электронных писем с целью обмана и получения личных данных — В. Взлом 4. Создание искусственного трафика для перегрузки сервера — Г. Распространение вирусов/малвари 3. Установите соответствие между описанием инструмента информационной атаки и его видом (методом реализации). **Описание инструмента** / **Вид инструмента/Метод** 1. Создание ложных учетных записей в социальных сетях — А. Боты. 2. Использование психологических приемов для убеждения аудитории — Б. SMM (Social Media Marketing). 3. Комплекс мер по продвижению информации в социальных сетях — В. Психологические операции.

<table>
<tr><td></td><td></td><td>
<table>
<tr><td>4. Автоматизированные аккаунты для распространения информации</td><td>Г. Фейковые аккаунты.</td></tr>
</table>
4. Установите соответствие между описанием акторов информационных войн и их видом.
<table>
<tr><th>Описание актора</th><th>Вид актора</th></tr>
<tr><td>1. Государственные структуры, осуществляющие информационную политику</td><td>А. СМИ.</td></tr>
<tr><td>2. Организации, формирующие общественное мнение.</td><td>Б. Киберпреступники</td></tr>
<tr><td>3. Лица, совершающие атаки на информационные системы</td><td>В. Государство.</td></tr>
<tr><td>4. Организации, распространяющие информацию</td><td>Г. Неправительственные организации (НПО).</td></tr>
</table>
5. Установите соответствие между мерой защиты от информационных войн и её областью.
<table>
<tr><th>Мера защиты</th><th>Область защиты</th></tr>
<tr><td>1. Регулярное обновление программного обеспечения</td><td>А. Защита информационной инфраструктуры.</td></tr>
<tr><td>2. Критическое мышление и проверка информации.</td><td>Б. Защита сознания.</td></tr>
<tr><td>3. Разработка и внедрение политик информационной безопасности</td><td>В. Техническая защита</td></tr>
<tr><td>4. Создание систем резервного копирования данных</td><td>Г. Организационная защита.</td></tr>
</table>
</td></tr>
<tr><td>Задание закрытого типа с выбором нескольких правильных ответов из нескольких вариантов предложенных</td><td>1.Внимательно прочитать текст задания и понять, что в качестве ответа ожидается несколько правильных ответов из предложенных вариантов.

2. Внимательно прочитать предложенные варианты ответа.

3. Выбрать несколько правильных ответов.

4. Записать только номера (или</td><td>1. Какие из перечисленных признаков характерны для информационной войны?

А. Использование исключительно легальных методов воздействия
Б. Целенаправленное манипулирование общественным сознанием
В. Применение киберсредств для нарушения работы инфраструктуры
Г. Отсутствие долгосрочных стратегических целей
Д. Системность и планомерность действий</td></tr>
</table>

	буквы) выбранного варианта ответа (например, 1 4 или А Г).	Е. Отказ от использования СМИ и соцсетей
		2. Какие каналы распространения информации чаще всего задействуются в информационных войнах? А. Телевидение и радио Б. Официальные государственные документы В. Социальные сети и мессенджеры Г. Научные монографии Д. Новостные сайты и блоги Е. Форумы и онлайн-сообщества
		3. Какие цели могут преследоваться в ходе информационной войны? А. Дестабилизация общественно-политической ситуации Б. Повышение уровня доверия к власти В. Дискредитация оппонентов и их идей Г. Распространение объективной информации Д. Формирование определённого эмоционального фона Е. Укрепление межгосударственного сотрудничества
		4. Какие методы относятся к технологиям информационного воздействия? А. Фейк-новости и дезинформация Б. Публичные дебаты с аргументами обеих сторон В. Троллинг и провокации в онлайн-среде Г. Массовое распространение мемов с заданным посылом Д. Прозрачное цитирование первоисточников Е. Создание «вирусного» контента с манипулятивным подтекстом
		5. Какие субъекты могут выступать участниками информационных войн? А. Государственные структуры Б. Международные корпорации В. Отдельные частные лица без ресурсов Г. Неправительственные организации (НПО) Д. Образовательные учреждения Е. Кибергруппировки и хакерские сообщества
Задание закрытого типа на установление последовательности	1. Внимательно прочитать текст задания и понять, что в качестве ответа ожидается последовательность элементов. 2. Внимательно прочитать предложенные варианты ответа. 3. Построить верную	1. Установите хронологическую последовательность этапов развития информационных войн (от раннего к современному). А. Письменная пропаганда и слухи в античных войнах (например, Пелопоннесская война) Б. Радио и кинопропаганда, массовые СМИ

	последовательность из предложенных элементов. 4. Записать буквы/цифры (в зависимости от задания) вариантов ответа в нужной последовательности (например, Б,В,А или 1,3,4,2).	(XX в., Вторая мировая война) В. Печатная пропаганда: книги, брошюры, газеты (эпоха Возрождения — XIX в.) Г. Интернет и социальные сети, бот-сети, фейки (XXI в.)
		2. Расположите этапы информационной операции в логической последовательности. А. Анализ целевой аудитории и уязвимостей Б. Запуск кампании и мониторинг реакции В. Разработка нарративов и контента Г. Выбор каналов распространения (СМИ, соцсети, мессенджеры) Д. Корректировка сообщений на основе обратной связи
		3. Установите последовательность действий при опровержении фейка. А. Подготовка контрсообщения с доказательной базой Б. Публикация опровержения через доверенные каналы В. Проверка фактов и поиск первоисточника Г. Мониторинг снижения вовлечённости в фейк Д. Фиксация фейка (дата, источник, распространение)
		4. Расположите уровни воздействия информационной войны по глубине влияния (от поверхностного к глубинному). А. Пересмотр ценностных установок и идентичности Б. Подрыв доверия к институтам (власть, СМИ, наука) В. Формирование эмоционального фона (страх, гнев) Г. Изменение оценок конкретных событий
		5. Установите последовательность фаз кибер-информационной атаки. Оценка личного вклада каждого участника и командной работы в целом А. Проникновение (взлом, фишинг) Б. Закрепление в системе (установка вредоносного ПО) В. Рекогносцировка (сбор данных о цели) Г. Сокрытие следов Д. Выполнение задачи (утечка данных, дезорганизация)
Задание комбинированного типа с выбором одного правильного ответа из предложенных и	1.Внимательно прочитать текст задания и понять, что в качестве ответа ожидается только один из предложенных вариантов. 2. Внимательно прочитать	1. Какой метод является ключевым для распространения дезинформации в социальных сетях? Выбранный ответ обоснуйте. Варианты ответов: А. Публикация научных статей в

обоснованием выбора	предложенные варианты ответа. 3. Выбрать один верный ответ. 4. Записать только номер (или букву) выбранного варианта ответа. 5. Записать аргументы, обосновывающие выбор ответа (например, 4 текст обоснования).	рецензируемых журналах Б. Массовое репостирование контента через бот-сети В. Рассылка официальных пресс-релизов Г. Проведение открытых публичных дебатов
		2. Что отличает информационную войну от обычной пропаганды? Выбранный ответ обоснуйте. Варианты ответов: А. Использование исключительно правдивой информации Б. Отсутствие целевой аудитории В. Комплексный характер: сочетание медиа, кибер- и психотехнологий Г. Ориентация только на внешнюю аудиторию.за счёт увеличения зелёных насаждений
		3. Какой фактор наиболее важен для повышения устойчивости общества к информационным атакам? Выбранный ответ обоснуйте. Варианты ответов: А. Полная блокировка иностранных СМИ Б. Развитие медиаграмотности и критического мышления В. Запрет на использование соцсетей Г. Увеличение числа государственных СМИ
		4. Какая цель чаще всего преследуется в ходе информационной операции против государства? Выбранный ответ обоснуйте. Варианты ответов: А. Повышение доверия к власти Б. Стимулирование экономического роста В. Делегитимация институтов власти и дестабилизация Г. Распространение научно-популярных знаний
		5. Какой инструмент наиболее эффективен для оперативного опровержения фейка? Выбранный ответ обоснуйте. Варианты ответов: А. Долгосрочная образовательная кампания Б. Официальное заявление через доверенные СМИ и соцсети В. Подача судебного иска против автора фейка Г. Игнорирование фейка в надежде, что он «самоуничтожится»
Задание открытого типа с развернутым	1. Внимательно прочитать текст задания и понять суть вопроса.	Задание 1. Опишите три ключевых отличия информационной войны от традиционной военной кампании. Приведите примеры для каждого

ответом	2.Продумать логику и полноту ответа. 3.Записать ответ, используя четкие компактные формулировки. 4.В случае расчетной задачи, записать решение и ответ	отличия.
		Задание 2. Перечислите пять основных каналов распространения дезинформации в современном мире. Для каждого канала укажите один специфический метод манипуляции, характерный именно для него.
		Задание 3. Опишите алгоритм действий государства по противодействию масштабной информационной атаке (не менее 5 шагов). Для каждого шага укажите конкретный инструмент или механизм реализации.
		Задание 4. Приведите три примера исторических информационных войн (разные эпохи). Для каждого примера укажите: -период и стороны конфликта; -основной метод воздействия; -ключевой результат.
		Задание 5. Объясните, почему критическое мышление считается главным защитным механизмом от информационных манипуляций. Приведите три конкретных навыка, которые входят в его состав, и покажите, как каждый из них помогает противостоять дезинформации.

6.3. Критерии и шкала оценивания на основе БРС.

Критерии и балльная шкала определяются преподавателем

КРИТЕРИИ ОЦЕНИВАНИЯ	РЕЗУЛЬТАТ В БАЛЛАХ
Дан полный, в логической последовательности развернутый ответ на поставленный вопрос, где он продемонстрировал знания предмета в полном объеме учебной программы, достаточно глубоко осмысливает дисциплину, самостоятельно, и исчерпывающе отвечает на дополнительные вопросы, приводит собственные примеры по проблематике поставленного вопроса, решил предложенные практические задания без ошибок	40
Дан развернутый ответ на поставленный вопрос, где студент демонстрирует знания, приобретенные на лекционных и семинарских занятиях, а также полученные посредством изучения обязательных учебных материалов по курсу, дает аргументированные ответы, приводит примеры, в ответе присутствует свободное владение монологической речью, логичность и последовательность ответа. Однако допускается неточность в ответе. Решил предложенные практические задания с небольшими неточностями.	30-39
Дан ответ, свидетельствующий в основном о знании процессов изучаемой дисциплины, отличающийся недостаточной глубиной и полнотой раскрытия темы,	20-29

знанием основных вопросов теории, слабо сформированными навыками анализа явлений, процессов, недостаточным умением давать аргументированные ответы и приводить примеры, недостаточно свободным владением монологической речью, логичностью и последовательностью ответа. Допускается несколько ошибок в содержании ответа и решении практических заданий.	
Дан ответ, который содержит ряд серьезных неточностей, обнаруживающий незнание процессов изучаемой предметной области, отличающийся неглубоким раскрытием темы, незнанием основных вопросов теории, несформированными навыками анализа явлений, процессов, неумением давать аргументированные ответы, слабым владением монологической речью, отсутствием логичности и последовательности. Выводы поверхностны. Решение практических заданий не выполнено, т.е. студент не способен ответить на вопросы даже при дополнительных наводящих вопросах преподавателя.	0-19

6.4. Описание дополнительных материалов и оборудования, необходимых для выполнения проверочных заданий (*при необходимости*).

Не используются

7. Методические материалы по освоению дисциплины

При подготовке к аудиторным занятиям студенты должны ознакомиться с соответствующими темами, материал по которым содержится в указанной в данной рабочей программе основной литературе. При подготовке ответов на контрольные вопросы по теме, а также при выполнении практических заданий по уже пройденной теме, студенты используют рекомендованную в данной рабочей программе дополнительную литературу.

При посещении лекций студент обязан вести конспект и при проведении контроля предоставление преподавателю конспектов лекций является обязательным.

Проведение семинарских занятий предполагает активное обсуждение предлагаемых вопросов в рамках устного опроса, тем докладов, а также выполнение практического задания. Для этого всем студентам необходимо готовиться к каждому семинару, используя предлагаемые источники из списка основной литературы.

Цель докладов более глубоко раскрыть изучаемые темы за счет привлечения дополнительных источников, поиск которых осуществляют сами студенты на основе использования фондов библиотеки СЗИУ РАНХиГС и других общедоступных библиотек города, а также электронных информационных баз в интернет-классе научной библиотеки СЗИУ РАНХиГС, а также электронной полнотекстовой базы журнальных статей «Интегрум» с сайта научной библиотеки СЗИУ РАНХиГС.

Выбор темы доклада определяется самим студентом в рамках предлагаемой к обсуждению общей темы семинарского занятия. Тема и структура доклада согласовывается с преподавателем. Помимо теории вопроса в рамках доклада студенту необходимо отразить практические аспекты ее применения, продемонстрировав не только свои знания, но и умение использовать их для решения практических задач.

При подготовке к аудиторным занятиям студенты должны ознакомиться с практическим заданием.

8. Учебная литература и ресурсы информационно-телекоммуникационной сети Интернет

8.1. Основная литература

1.Беляев, Д. Разруха в головах. Информационная война против России / Д. Беляев; предисл. Н. Стариков. — Москва ; Санкт-Петербург : Питер, 2021. — 256 с.

2. Бухарин, С. Н. Методы и технологии информационных войн / С. Н. Бухарин, В. В. Цыганов. — Москва: Академический проект, 2022. — 382 с. — (Социально-политические технологии).

3. Воронова, О. Е. Информационно-психологическая безопасность России в условиях новых глобальных угроз : монография / О. Е. Воронова. — Москва: Аспект Пресс, 2021. — 240 с.

4. Коровин, В. Третья мировая сетевая война / В. Коровин. — Москва ; Санкт-Петербург : Питер, 2021. — 352 с.

8.2. Дополнительная литература

1. Зеленков, М. Ю. Современные информационные войны: стратегии и инструменты / М. Ю. Зеленков. — Москва: Дашков и К°, 2021. — 320 с.

2. Ковалёв, В. А. Информационная безопасность и противодействие информационным войнам / В. А. Ковалёв. — Санкт-Петербург: Питер, 2020. — 272 с.

3. Манойло, А. В. Государственная политика в сфере информационных войн: современные вызовы / А. В. Манойло. — Москва: Горячая линия — Телеком, 2023. — 416 с.

4. Почепцов, Г. Г. Информационные войны нового поколения / Г. Г. Почепцов. — Москва: РИПОЛ классик, 2021. — 352 с.

5. Расторгуев, С. П. Психология информационных войн: когнитивные методы воздействия / С. П. Расторгуев. — Москва: Академический проект, 2022. — 240 с.

8.3. Нормативные правовые документы и иная правовая информация

1.Федеральный закон от 9 февраля 2009 г. № 8-ФЗ «Об обеспечении доступа к информации о деятельности государственных органов и органов местного самоуправления» // СПС «Консультант-Плюс».

2. Федеральный закон от 27.07.2006 N 149-ФЗ (ред. от 24.11.2014) «Об информации, информационных технологиях и о защите информации» // СПС «Консультант-Плюс».

3. Федеральный закон от 10.01.2002 № 1-ФЗ "Об электронной цифровой подписи" // Собр. законодательства Рос. Федерации. − 2002 − № 2

4. Федеральный закон от 27.07.2006 № 152-ФЗ "О персональных данных" // Собр.законодательства Рос. Федерации. − 2006 − № 31

5. «О правовой охране программ для электронных вычислительных машин и баз данных» (Закон РФ № 3523-1).

8.4 Интернет-ресурсы

Обучающимся обеспечен доступ к материалам курса в СДО Академии http://lms.ranepa.ru, а так же через сайт научной библиотеки к следующим подписным электронным ресурсам:

Русскоязычные ресурсы

- Электронные учебники электронно-библиотечной системы (ЭБС) *«Айбукс»*
- Электронные учебники электронно-библиотечной системы (ЭБС) *«Юрайт»*
- Электронные учебники электронно-библиотечной системы (ЭБС) *«Лань»*
- Электронные учебники электронно-библиотечной системы (ЭБС) «*ZNANIUM.COM*»
- Электронные учебники электронно-библиотечной системы (ЭБС) «BOOK.RU»
- Электронные учебники электронно-библиотечной системы (ЭБС) *«IPR SMART»*

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

№ п/п	Наименование
1.	Специализированные залы для проведения лекций, оснащенные персональным компьютером/ноутбуком и мультимедийным проектором
2.	Аудитории и компьютерные классы, оборудованные посадочными местами и персональными компьютерами с выходом в Интернет для проведения практических занятий
3.	«МТС Линк» — российская платформа для онлайн-коммуникаций и совместной работы команд; «Яндекс Телемост» — сервис для

	видеоконференций от Яндекса; Я-мессенджер
4.	Технические средства обучения: персональные компьютеры; программные средства, обеспечивающие просмотр видеофайлов в форматах AVI, MPEG-4, DivX, RMVB, WMV; программы для работы с электронными таблицами для обработки, анализа и визуализации данных; соответствующие онлайн-инструменты для построения интеллект-карты и моделей в различных нотациях
5.	Научная библиотека (в т.ч. электронные информационные ресурсы научной библиотеки)
6.	СДО Академии https://lms.ranepa.ru/