Лебедева Екатерина Александровна
Подписано цифровой подписью: Лебедева Екатерина Александровна
Дата: 2026.06.23 11:52:22 +03'00'

Приложение 4

к образовательной программе

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Б1.В.ДВ.03.01 Организационные основы обеспечения информационной безопасности
(индекс, наименование дисциплины в соответствии с учебным планом)

09.04.01 Прикладная информатика
(код, наименование направления подготовки)

Информационные технологии в государственном и муниципальном управлении
(наименование образовательной программы)

очная, заочная форма обучения
(форма обучения)

Год набора – 2026

Нижний Новгород

Автор(ы)-составитель(и):

Акимова Екатерина Анатольевна, кандидат исторических наук, доцент, доцент кафедры истории и теории государства и права

Заведующий кафедрой:

Халин Алексей Алексеевич, доктор исторических наук, профессор, профессор, заведующий кафедрой истории и теории государства и права

Рабочая программа по дисциплине Б1.В.ДВ.03.01 Организационные основы обеспечения информационной безопасности одобрена на заседании кафедры истории и теории государства и права юридического факультета Нижегородского института управления – филиала РАНХиГС.

протокол № 2 от «23» сентября 2025 г.

СОДЕРЖАНИЕ

1. Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения программы
2. Объем и место дисциплины в структуре образовательной программы
3. Содержание и структура дисциплины
4. Типы оценочных материалов, показатели, критерии, шкалы оценивания
5. Формы аттестации и типовые оценочные материалы для текущего контроля успеваемости обучающихся
6. Формы промежуточной аттестации по дисциплине, типы оценочных материалов, показатели, критерии, шкалы оценивания
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.03.01 Организационные основы обеспечения информационной безопасности у обучающихся следующих профессиональных компетенций:

ОТФ/ТФ/ и реквизиты ПС	Код компетенции	Наименование компетенции	Код индикатора достижения компетенции	Наименование индикатора достижения компетенции	Образовательный результат
ПС: 06.015 Специалист по информационным системам, утв. приказом Минтруда и социальной защиты РФ от 13.07.2023 № 586н ТФ: D/08.7 Разработка инструментов и методов проектирования бизнес-процессов заказчика в рамках управления работами по сопровождению и проектами создания (модификации) ИС D/09.7 Разработка инструментов и методов адаптации бизнес-процессов заказчика к возможностям ИС в рамках управления работами по сопровождению и проектами создания (модификации) ИС.	ПК-6	способен выбирать методологию и технологию проектирования ИС с учетом проектных рисков.	ИПК-6.2	Применяет методы оценки и управления рисками ИТ-проектов.	ИПК-6.2 З-1 Знает содержание, цели, задачи и принципы разработки системы управления ИТ-рисками организации. ИПК-6.2 З-2 Знает инструменты и методы управления ИТ-рисками. Например, качественные методы (преимущества и недостатки применения, использование в процедурах идентификации рисков, построения реестров рисков) и количественные методы оценки рисков. ИПК-6.2 З-3 Знает современные концепции анализа и управления рисками в сфере информационных технологий. ИПК-6.2 У-1 Умеет выбирать подходящий математический инструментарий для решения задач анализа и оценки ИТ-рисков, в том числе с использованием ЭВМ и прикладных программных продуктов. ИПК-6.2 У-2 Умеет разрабатывать комплекс мероприятий по

ОТФ/ТФ/ и реквизиты ПС	Код компетенции	Наименование компетенции	Код индикатора достижения компетенции	Наименование индикатора достижения компетенции	Образовательный результат
					управлению рисками ИТ-проектов. ИПК-6.2 У-3 Умеет использовать специализированное программное обеспечение для проведения анализа ИТ-проектов и формирования планов и отчётности по управлению рисками.
ПС: 06.015 Специалист по информационным системам, утв. приказом Минтруда и социальной защиты РФ от 13.07.2023 № 586н ТФ: D/09.7 Разработка инструментов и методов адаптации бизнес-процессов заказчика к возможностям ИС в рамках управления работами по сопровождению и проектами создания (модификации) ИС D/17.7 Организационное и технологическое обеспечение разработки баз данных ИС в рамках управления работами по сопровождению и проектами создания (модификации) ИС	ПК-11	способен проектировать архитектуру и сервисы ИС предприятий и организаций в прикладной области	ИПК-11.2	Использует инструментарий проектирования архитектуры и сервисов ИС.	ИПК-11.2 З-1 Знает программные средства и платформы инфраструктуры информационных технологий организаций, которые используются в проектировании ИС. ИПК-11.2 З-2 Знает современные подходы и стандарты автоматизации организации (например, CRM, MRP, ERP, ITIL, ITSM). ИПК-11.2 З-3 Знает моделирование как методологическую основу проектирования ИС. Средства моделирования, виды моделей и методов моделирования. ИПК-11.2 У-1 Умеет использовать инструментарий проектирования архитектуры и сервисов информационных систем (ИС).

ОТФ/ТФ/ и реквизиты ПС	Код компетенции	Наименование компетенции	Код индикатора достижения компетенции	Наименование индикатора достижения компетенции	Образовательный результат
ПС: 06.015 Специалист по информационным системам, утв. приказом Минтруда и социальной защиты РФ от 13.07.2023 № 586н ТФ: D/17.7 Организационное и технологическое обеспечение разработки баз данных ИС в рамках управления работами по сопровождению и проектами создания (модификации) ИС	ПК-19	Способен использовать передовые методы оценки качества, надежности и информационной безопасности ИС в процессе эксплуатации прикладных ИС.	ИПК-19.2	Использует методы анализа основных концептуальных подходов к проблеме обеспечения информационной безопасности.	ИПК-19.2 З-1 Знает компоненты концептуальной модели безопасности информации. Угрозы информации, источники угроз, способы их реализации и цели, а также меры защиты информации от неправомерных действий, приводящих к нанесению ущерба. ИПК-19.2 З-2 Знает основные направления защиты информации. Правовая, организационная и инженерно-техническая защиты как выразители комплексного подхода к обеспечению информационной безопасности. ИПК-19.2 У-1 Умеет использовать методы моделирования для анализа значительного набора источников, объектов и действий, нарушающих безопасность. ИПК-19.2 У-2 Умеет анализировать угрозы информационной безопасности. ИПК-19.2 У-3 Умеет постраивать комплексную систему организационных мер для выбранного государственного или муниципального учреждения (предприятия, организации).

2. Объем и место дисциплины (модуля) в структуре образовательной программы

Общая трудоемкость дисциплины составляет 2 зачетных единицы (1 з.е. = 36/27 часов), 72 академических часа.

По очной форме обучения: количество академических часов, выделенных на контактную работу с преподавателем составляет 28 часов, из них, лекции - 8 часов, практические занятия – 16 часов, контактная работа на аттестацию в период промежуточной аттестации – 4 часов. Самостоятельная работа составляет – 44 часа.

По заочной форме обучения: количество академических часов, выделенных на контактную работу с преподавателем составляет 12 часов, из них, лекции – 4 часа, практические занятия – 8 часов. Самостоятельная работа составляет 56 часов. Контроль – 4 часа.

Дисциплина Б1.В.ДВ.03.01 Организационные основы обеспечения информационной безопасности является дисциплиной обязательной части. В соответствии с учебным планом изучается на 2 курсе в 1 семестре (очная форма обучения), на 2 курсе сессия 2 (заочная форма обучения). Освоение дисциплины опирается на объем теоретических знаний в области истории России; информатики; основы информационной безопасности, документоведение; а также на приобретенные ранее умения факторного и проблемного анализа; приобретенные ранее навыки работы с научной, справочной и официальной информацией; использования информационных технологий в исследовательских целях.

Дисциплина является основой для изучения следующих дисциплин:

Б1.В.ДВ.04.01– Актуальные проблемы информационного права;

Б1.В.ДВ.04.02– Правовые основы информационной безопасности;

Б1.В.ДВ.04.03 – Социально-психологические технологии адаптации к профессиональной деятельности.

3. Содержание и структура дисциплины (модуля)

3.1. Структура дисциплины

Очная форма обучения

№ п/п	Наименование тем и (или) разделов	ВСЕГО	Объем дисциплины, ак.час											Форма текущего контроля успеваемости, промежуточной аттестации
			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.	Введение в проблему информационной безопасности	17	2	0	0	4	0	0	0	0		0	0	11	Опрос, тест, доклад, работа с источниками в микрогруппе
Тема 2.	Информационное противоборство и безопасность. Информационная	17	2	0	0	4	0	0	0	0		0	0	11	Опрос, тест, доклад, работа с источниками в

	война.													микрогруппе
Тема 3.	Нормативно-правовая база обеспечения информационной безопасности.	17	2	0	0	4	0	0	0	0	0	0	11	Опрос, тест, доклад, работа с источниками в микрогруппе
Тема 4.	Информационная безопасность в практике международных отношений.	17	2	0	0	4	0	0	0	0	0	0	11	Опрос, тест, доклад, работа с источниками в микрогруппе
Промежуточная аттестация		4	0	0	0	0	0	0	0	4	0	0	0	Зачет
Итого		72	8	0	0	16	0	0	0	4	0	0	44	

Заочная форма обучения

№ п/п	Наименование тем и (или) разделов	ВСЕГО	Объем дисциплины, ак.час												Форма текущего контроля успеваемости, промежуточной аттестации
			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	Введение в проблему информационной безопасности	17	1	0	0	2	0	0	0	0		0	0	14	Опрос, тест, доклад, работа с источниками в микрогруппе
Тема 2	Информационное противоборство и безопасность. Информационная война.	17	1	0	0	2	0	0	0	0		0	0	14	Опрос, тест, доклад, работа с источниками в микрогруппе

Тема 3	Нормативно-правовая база обеспечения информационной безопасности.	17	1	0	0	2	0	0	0	0	0	0	14	Опрос, тест, доклад, работа с источниками в микрогруппе
Тема 4	Информационная безопасность в практике международных отношений.	17	1	0	0	2	0	0	0	0	0	0	14	Опрос, тест, доклад, работа с источниками в микрогруппе
Промежуточная аттестация		4	0	0	0	0	0	0	0	4	0	0	0	Зачет
Итого		72	4	0	0	8	0	0	0	4	0	0	56	

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,).

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

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.

3.2 Содержание дисциплины

Тема 1. Введение в проблему информационной безопасности. ИПК-11.2

Понятие «информация». Информационное общество. Интернет. Критерии информационного общества. Современные тенденции и влияние на общество и государства процессов глобальной информатизации. Развитие информационного общества в России. Понятия «безопасность», «информационная безопасность». Транснациональные вызовы и угрозы безопасности, связанные с развитием информационных технологий. Субъекты международной информационной безопасности. Информатизация процесса производства и управления, глобальные сети и глобальное управление, расширение экономической географии, революция в военном деле. СМИ и глобальное медиа-пространство. Интернет как фактор формирования глобальной социально-экономической информационной среды.

Тема 2. Информационное противоборство и безопасность. Информационная война. ИПК-19.2

Противоборство и конфликты в информационной сфере. Понятия «информационная безопасность» и «кибер-безопасность». Новые объекты безопасности в информационной сфере. Информационные средства воздействия. Информационное оружие. Информационный терроризм и трансформация международного терроризма. Использование интернета в преступных целях.

Интересы государств и иных факторов мировой политики в информационной сфере. Применение общих принципов международного права к борьбе в информационной сфере. Включение информационной войны в международно-правовое понимание войны как вооруженного противоборства.

Тема 3. Нормативно-правовая база обеспечения информационной безопасности. ИПК-6.2

Государственная политика в сфере обеспечения информационной безопасности. Государственные органы РФ, контролирующие деятельность в области защиты информации. Нормативно-правовая база обеспечения информационной безопасности в России и за рубежом. Доктрина информационной безопасности Российской Федерации (2016). Стратегия национальной безопасности Российской Федерации (2021). Основы государственной политики Российской Федерации в области международной информационной безопасности (2021). Стратегия развития информационного общества в Российской Федерации на 2017 – 2030 гг. (2017). Государственная программа Российской Федерации «Информационное общество (2020). Концепция государственной системы

обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации (2014). Конвенция Совета Европы «О компьютерных преступлениях» (Будапешт, 2001). Концепция Конвенции ООН об обеспечении международной информационной безопасности (2017). Основные направления научных исследований в области обеспечения информационной безопасности Российской Федерации (2017). Проблема устаревания официальных документов.

Тема 4. Информационная безопасность в практике международных отношений. ИПК-19.2

Российские инициативы в области международной информационной безопасности, история их выдвижения и продвижения. Российско-американские отношения по вопросу международной информационной безопасности. Позиция Китая. Расстановка сил на мировой арене в связи с российскими инициативами по международной информационной безопасности. Переговорный процесс и международное сотрудничество в области обеспечения информационной безопасности.

Работа Комитетов ООН по безопасности и разоружению, по космосу, МСЭ, Группы восьми, Евросоюза, ШОС в области международной информационной безопасности.

Изменение расстановки сил на международной арене в 2014 г. после воссоединения Крыма с Россией – информационный аспект. Информационная война США и Великобритании против России. Перспективы установления международного контроля над информационными видами оружия и формирования глобального режима международной информационной безопасности и управления интернетом. Роль информационных войн в трансформации международных отношений в 2022 – 2026 гг.

4. Типы оценочных материалов, показатели и критерии оценивания

4.1. Оценочные материалы по дисциплине Б1.В.ДВ.03.01 Организационные основы обеспечения информационной безопасности входят в состав оценочных материалов по образовательной программе. Совокупность оценочных материалов по всем дисциплинам (модулям) образовательной программы составляют 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	Ответ считается верным, если правильно указаны цифры или буквы

		зависимости от задания) вариантов ответа (например, А1 или Б4).	
Задание закрытого типа с выбором нескольких правильных ответов из нескольких вариантов предложенных	Прочитайте текст, выберите правильные ответы	1.Внимательно прочитать текст задания и понять, что в качестве ответа ожидается несколько правильных ответов из предложенных вариантов. 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).	Ответ считается верным, если правильно установлены все соответствия (позиции из 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	Прочитайте текст, выберите	1.Внимательно прочитать текст задания и понять, что в качестве ответа ожидается	Ответ считается верным, если правильно указана цифра или буква и

типа с выбором одного правильного ответа из предложенных и обоснованием выбора	правильный ответ и запишите аргументы, обосновывающие выбор ответа	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. 5. Записать аргументы, обосновывающие выбор ответа (например, 4 текст обоснования).	приведены корректные аргументы, используемые при выборе ответа
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 Б1.В.ДВ.03.01 Организационные основы обеспечения информационной безопасности используются следующие формы текущего контроля успеваемости обучающихся (в том числе, задания к контрольным точкам):

Опрос, тест, доклад, работа с источниками в микрогруппе.

Задания к контрольным точкам:

Комбинированная комплексная проверочная работа №1

Комбинированная комплексная проверочная работа №2

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

Тема 1. Введение в проблему информационной безопасности. ИПК-11.2

Подготовка к практическому занятию:

– внимательно прочитать материал лекций, относящихся к данному занятию, ознакомиться с учебными материалами, включая электронные в соответствии с предложенным списком литературы в рабочей программе учебной дисциплины;

– подготовить развернутые ответы на вопросы для проведения опроса по теме практического занятия;

– понять, что осталось неясными и постараться получить на них ответ заранее;

– готовиться к практическому занятию можно как индивидуально, так и в составе малой группы.

Вопросы к практическому занятию для проведения опроса:

1. Понятия «информация», «безопасность», «информационная безопасность», их сущность, измерения.
2. Информационное общество в России. Роль Интернета в современном обществе.
3. Вызовы и угрозы безопасности, связанные с развитием информационных технологий.
4. Субъекты международной информационной безопасности.

Примерные тестовые задания:

Внимательно прочитать текст задания и понять, что в качестве ответа ожидается один или несколько предложенных вариантов.

Внимательно прочитать предложенные варианты ответа.

Выбрать один или несколько верный(ых) ответ(ов).

Записать только букву(ы)/цифру(ы) выбранного(ых) варианта(ов) ответа(ов).

1. Термин «национальная безопасность» появился в политическом лексиконе России:

1) в начале XX века;
2) со времени возникновения Российского государства;
3) в конце XX века;
4) после Второй мировой войны.

2. Составными частями национальной безопасности России являются:

1) безопасность регионов России;
2) безопасность от внешних и внутренних угроз;
3) безопасность каждого гражданина России;
4) экономическая, политическая, военная, социальная, экологическая, информационная безопасность.

3. Национальная безопасность должна определяться:

1) интересами крупного бизнеса;
2) интересами отдельных социальных групп;
3) долгосрочными интересами страны в целом;
4) интересами государственного аппарата.

4. В какой области обеспечение безопасности должно достигаться с помощью патентной защиты, таможенного регулирования

1) интеллектуальная безопасность;
2) информационная безопасность;
3) внешнеэкономическая безопасность;
4) промышленной безопасности.

5. Существуют следующие уровни безопасности:

1) местная, межрегиональная, глобальная;
2) национальная, региональная, глобальная;
3) межнациональная, региональная, всеобщая;
4) национальная, межрегиональная, всеобщая.

Темы докладов:

- Информационная безопасность: сущность, основные измерения.
- Этапы становления и совершенствования обеспечения информационной безопасности в СССР и РФ.
- Информационное общество: сущность, основные измерения.
- Основные модели информационного общества.
- Международная информационная безопасность.
- Западные модели информационного общества: от Д.Белла до К.Шваба.

Задание для работы с документами индивидуальная и в рамках микрогруппы:

Белл Д. Грядущее постиндустриальное общество. Опыт социального прогнозирования.

«Постиндустриальное общество [...] не является проекцией или экстраполяцией современных тенденций западного общества; это новый принцип социально-технологической организации и новый образ жизни, вытесняющий индустриальную систему, точно так же, как она сама вытеснила когда-то аграрную. В первую очередь, оно воплощается в утрате промышленностью, организованной на основе стандартизации и массового производства, своей центральной роли.

Это не означает, что производство товаров прекратится; ведь производство продуктов земледелия в западном мире продолжается и сегодня (причем продовольствия производится больше, чем когда бы то ни было ранее). Прежде всего понятие «постиндустриальное общество» представляет собой не эмпирическое описание, а «теоретическое построение», позволяющее увидеть главное в новых социальных формах.

Постиндустриальные тенденции не заменяют прежние социальные формы как некие «стадии» общественного развития. Они часто сосуществуют (как порой сосуществуют на пергаменте старые полустертые письмена и нанесенные поверх них новые), усложняя общество и природу его социальной структуры».

«Мир можно представить себе разделенным на три типа социальной организации. Первый из них – доиндустриальный. Это, прежде всего, добывающие виды хозяйственной деятельности: земледелие, извлечение полезных ископаемых, рыболовство, заготовка леса. До сих пор это удел большей части стран Африки, Латинской Америки и Юго-Восточной Азии, где этими видами хозяйственной деятельности занято 60 или более процентов рабочей силы. Я определяю это в целом как «взаимодействие человека с природой», которое подвержено капризам погоды и усложняется вследствие истощения почв, исчерпания лесных ресурсов и более высокой себестоимости добычи минералов и руд.

Второй тип социальной организации – индустриальный. Это фабричное хозяйство, основанное на приложении энергии к машинам для массового производства товаров.

К индустриальному типу относятся страны, расположенные на берегах Атлантики: Западная Европа, Соединенные Штаты и далее – Советский Союз и Япония. Труд здесь представляет собой взаимодействие с искусственной природой: соединение людей с машинами, организация ритмичной работы с высочайшей степенью координации.

Третий тип – постиндустриальное общество. Это деятельность, связанная в первую очередь с обработкой данных, управлением и информацией.

Это образ жизни, который во все возрастающей степени сводится к «взаимодействию людей друг с другом». Еще более важно то, что возникает новый принцип обновления, прежде всего знаний в их отношении к технологии».

«...Основные изменения в постиндустриальном обществе происходят прежде всего в технико-экономической сфере. Однако тот факт, что постиндустриальные перемены, в отличие от всех предшествующих технологических изменений, связаны с кодификацией теоретического знания, делает науку отличительный чертой этого общества».

«...Мне кажется полезным выделить некоторые новые черты постиндустриального общества.

1) *Центральная роль теоретического знания.* Каждое общество всегда опиралось на знания, но только в наши дни систематизация результатов теоретических исследований и материаловедения становится основой технологических инноваций. Это заметно, прежде всего, в новых, наукоемких отраслях промышленности – в производстве компьютеров, электронной, оптической техники, полимеров, – ознаменовавших своим развитием последнюю треть столетия.

2) *Создание новой интеллектуальной технологии.* Новые математические и экономические методы, такие, как компьютерное линейное программирование, цепи Маркова, стохастические процессы и т.п., служат технологической основой моделирования, имитации и других инструментов системного анализа и теории решений, позволяющих находить более эффективные, "рациональные" подходы к экономическим, техническим и даже социальным проблемам.

3) *Рост класса носителей знания.* Наиболее быстрорастущая группа общества – класс технических специалистов и профессионалов. В Соединенных Штатах эта группа, вместе с менеджерами, составляла в 1975 г. 25 процентов рабочей силы – восемь миллионов человек. К 2000 году класс технических специалистов и профессионалов будет самой многочисленной социальной группой.

4) *Переход от производства товаров к производству услуг.* В настоящее время в Соединенных Штатах примерно 65 человек из каждых 100 занято в сфере услуг. К 1980 г. это число возрастет до 70. Значительный сектор услуг существует в любом обществе. В доиндустриальный период это в основном класс тех, кто оказывает личные услуги по дому (в Англии это был самый многочисленный из всех классов до 1870 г.). В индустриальном обществе сфера услуг включает транспорт, финансы, которые играют вспомогательную роль в производстве товаров, а также бытовые услуги (косметические кабинеты, рестораны и т.д.). В постиндустриальном обществе появляются новые виды услуг, прежде всего в гуманитарной области (главным образом в здравоохранении, образовании и социальном обслуживании), а также услуги профессионалов и технических специалистов (например, проведение исследований и оценок, работа с компьютерами, осуществление системного анализа). Развитие этих служб [...] становится сдерживающим фактором экономического роста и источником постоянной инфляции.

5) *Изменения в характере труда.* В доиндустриальном мире жизнь представляет собой взаимодействие человека с природой, когда люди, объединившись в малые группы, тяжким трудом добывают себе пропитание на земле, в воде или в лесу и полностью зависят от капризов внешней среды. В индустриальном обществе труд – это взаимодействие человека с преобразованной природой, когда в процессе производства товаров люди становятся придатками машин.

Но в постиндустриальном мире труд является, прежде всего, взаимодействием между людьми (между чиновником и посетителем, врачом и пациентом, учителем и учащимся или между членами исследовательских групп, сотрудниками контор или работниками бригад обслуживания).

Тем самым из процесса труда и повседневной практики исключаются природа, искусственно созданные предметы, а остаются лишь люди, которые учатся взаимодействовать друг с другом. В истории

человеческого общества это совершенно новая, не имеющая аналогов ситуация.

6) *Роль женщин.* В индустриальном секторе (в частности, на фабрике) трудились в основном мужчины. Постиндустриальный сектор (например, услуги в гуманитарной области) предоставляет широкие возможности занятости и для женщин. Можно сказать, что впервые женщины получили надежную основу для экономической независимости. Этот факт находит подтверждение в постоянно растущей доле женщин в общей численности работающих, в увеличении числа семей (в настоящее время 60 процентов от их общего количества), в которых более одного человека занято на постоянной работе, и в росте числа разводов по инициативе женщин, ощущающих себя все менее экономически зависимыми от мужчин.

7) *Наука достигает своего зрелого состояния.* Возникшее в XVII веке научное сообщество явилось уникальным социальным институтом.

Оно обладало харизмой, поскольку в своих поисках истины всегда шло революционным путем и открывало доступ к своим методам и технологиям; его сила заключена в убеждении, что цель науки заключается в получении знания как такового, а не каких-либо способов его утилитарного применения. В отличие от других харизматических сообществ (главным образом религиозных групп и мессианских политических движений) оно не "рутинизирует" свои убеждения и не возводит их в ранг официальных догм. Однако до последнего времени научному сообществу не приходилось сталкиваться с такими явлениями, как бюрократизация научно-исследовательского процесса, подчинение научных поисков целям, устанавливаемым государством, оценка результатов исследований в зависимости от конкретной отдачи. В настоящее же время не только укрепилась связь науки и технологий; она вошла также составной частью в военную сферу и во многом определяет социальные потребности.

Все это составляет основную черту постиндустриального общества, и характер новых научных институтов имеет решающее значение для возможности свободного осуществления исследований и получения знаний в будущем. [...]

9) *Меритократия.* В постиндустриальном обществе, которое по своему характеру есть прежде всего общество технологическое, человек может занять престижное положение не столько по праву наследования или собственности (хотя оно может давать богатство или культурное преимущество), сколько вследствие образования и квалификации. Неизбежно, что вопрос о меритократии становится решающим нормативным вопросом. [...]".

Задание: **Ответьте на вопросы:**

1. Какую характеристику Д.Белл дает постиндутриальному обществу?
2. Какие три типа социальной организации выделяет Д.Белл? Как

можно охарактеризовать каждый тип социальной организации?

3. Какие черты постиндустриального общества выделяет Д.Белл?

4. Можно ли считать, что концепция Д.Белла отражает реальное состояние современного общества? Аргументируйте свой ответ.

Тема 2. Информационное противоборство и безопасность. Информационная война. ИПК-19.2

Подготовка к практическому занятию:

– внимательно прочитать материал лекций, относящихся к данному занятию, ознакомиться с учебными материалами, включая электронные в соответствии с предложенным списком литературы в рабочей программе учебной дисциплины;

– подготовить развернутые ответы на вопросы для проведения опроса по теме практического занятия;

– понять, что осталось неясными и постараться получить на них ответ заранее;

– готовиться к практическому занятию можно как индивидуально, так и в составе малой группы.

Вопросы к практическому занятию для проведения опроса:

1. Противоборство и конфликты в информационной сфере. Понятие «кибер-безопасность».
2. Новые объекты безопасности в информационной сфере.
3. Информационные средства воздействия. Информационное оружие.
4. Информационный терроризм и трансформация международного терроризма.
5. Интересы государств и иных факторов мировой политики в информационной сфере.
6. Информационные войны. Методы борьбы с ними.
7. Поведенческое противоборство как развитие информационного противоборства. Поведенческая война.

Примерные тестовые задания:

Внимательно прочитать текст задания и понять, что в качестве ответа ожидается один или несколько предложенных вариантов.

Внимательно прочитать предложенные варианты ответа.

Выбрать один или несколько верный(ых) ответ(ов).

Записать только букву(ы)/цифру(ы) выбранного(ых) варианта(ов) ответа(ов).

1. Государственная тайна - это:

1) защищаемые государством сведения в области его военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб безопасности страны;

2) ограничения доступа в отдельные отрасли экономики или на конкретные производства;

3) защищаемые банками и иными кредитными организациями сведения о банковских операциях;

4) защищаемая по закону информация, доверенная или ставшая известной лицу (держателю) исключительно в силу исполнения им своих профессиональных обязанностей.

2. Информационное оружие – это:

1) комплекс индивидуального и общественного сознания;

2) комплекс нормативно-правовой документации;

3) комплекс технических, программных и других средств, методов и технологий, предназначенных для распространения выгодной информации и дезинформации в системе формирования общественного мнения.

3. Что не относится к угрозам информационной безопасности:

1) сбои и отказы оборудования (технических средств);

2) классификация информации;

3) преднамеренные действия нарушителей и злоумышленников (обиженных лиц из числа персонала, преступников, шпионов, диверсантов).

4. К открытым источникам информация относятся.

1) Газеты, Радио, Новости;

2) информация, украденная у спецслужб;

3) из вскрытого сейфа;

4) украденная из правительственной организации.

5. Сложность обеспечения информационной безопасности является следствием:

1) невнимания широкой общественности к данной проблематике

2) все большей зависимости общества от информационных систем

3) быстрого прогресса информационных технологий, ведущего к постоянному изменению информационных систем и требований к ним

4) все более облегченной защитой на информационных устройствах и в сети Интернет.

Темы докладов:

- «Мягкая сила» как метод ведения информационной войны.
- Дж. Най и его концепции «мягкой» и «умной» сил.
- Дж.Ассанж и Э.Сноуден – разоблачители или игроки в стратегии информационных войн?
- «Цветные революции» как элемент информационных войн в мировой политике.

- Информационный терроризм в международной политике.

- Информационная война в мировой политике (от теории к практике).

- Поведенческое противоборство и поведенческая война.

Задание для работы с документами индивидуальная и в рамках микрогруппы:

Тема работы в микрогруппах: «Цветные революции на постсоветском пространстве».

Цель: выявить общее и особенное в проведении «цветных революций» на постсоветском пространстве и продумать варианты их предотвращения.

Предварительная работа:

1. Изучить работу Джин Шарп «От диктатуры к демократии» - http://www.aeinstein.org/wp-content/uploads/2013/10/FDTD_Russian.pdf

2. Изучить раздел «Цветные революции» в учебнике Василенко, И. А. Геополитика современного мира: учебник для вузов / И. А. Василенко. — 4-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2026.

3. Изучить материал по теме «Цветные революции» в СМИ (печатных, сети Интернет)

Студенческая группа разбивается на 4 микрогруппы. На основе лекционного материала, докладов на семинарском занятии и самостоятельной работы необходимо подготовить материалы по следующей схеме:

1. Государство до начала «цветной революции» (политический строй, социально-экономическая ситуация);
2. Причины расшатывания политической ситуации;
3. Повод «цветной революции»;
4. Этапы развития «цветной революции»;
5. Итоги и последствия «цветной революции»;
6. Оценка: изменилась ли в лучшую/худшую сторону ситуация в государстве?

Государства, где произошли «цветные революции»:

- Грузия (2003 г.);
- Украина (2004 г.);
- Киргизия (2005 г.);
- Украина (2014 г.);

Отчет по работе в микрогруппе делается в виде презентации.

Тема 3. Нормативно-правовая база обеспечения информационной безопасности. ИПК-6.2

Подготовка к практическому занятию:

– внимательно прочитать материал лекций, относящихся к данному занятию, ознакомиться с учебными материалами, включая электронные в

соответствии с предложенным списком литературы в рабочей программе учебной дисциплины;

– подготовить развернутые ответы на вопросы для проведения опроса по теме практического занятия;

– понять, что осталось неясными и постараться получить на них ответ заранее;

– готовиться к практическому занятию можно как индивидуально, так и в составе малой группы.

Вопросы к практическому занятию для проведения опроса:

1. Государственная политика в сфере обеспечения информационной безопасности.
2. Государственные органы РФ, контролирующие деятельность в области защиты информации.
3. Нормативно-правовая база обеспечения информационной безопасности в России и за рубежом.

Примерные тестовые задания:

Внимательно прочитать текст задания и понять, что в качестве ответа ожидается один или несколько предложенных вариантов.

Внимательно прочитать предложенные варианты ответа.

Выбрать один или несколько верный(ых) ответ(ов).

Записать только букву(ы)/цифру(ы) выбранного(ых) варианта(ов) ответа(ов).

1. Государственные органы РФ, контролирующие деятельность в области защиты информации:

1) Министерство юстиции Российской Федерации;
2) Служба внешней разведки Российской Федерации;
3) Федеральная служба безопасности;
4) Комитет Государственной думы по безопасности;
5) Министерство иностранных дел;
6) Министерство внутренних дел Российской Федерации;
7) Совет безопасности России.

2. Правовое обеспечение информационной безопасности – это:

1) документированные сведения, лежащие в основе решения задач, обеспечивающих функционирование системы;

2) широкое использование технических средств защиты информации;

3) нормативные документы по ИБ, требования которых являются обязательными в рамках сферы действия каждого подразделения.

3. В число уровней, на которых группируются меры обеспечения информационной безопасности, входят:

1) Законодательный;

2) Исполнительный;

3) судебный.

4. Специальная военная операция России на территории Украины:

1) началась 24 февраля 2022 г.

2) направлена на установление полного контроля над всей территорией Украины

3) целями СВО заявлены демилитаризация и денацификация Украины

4) основные военные действия в ходе СВО проходят на территории Западной Украины

5) в результате СВО Крым стал частью России

5. В 2016 г. были приняты следующие документы в сфере национальной безопасности:

1) Стратегия национальной безопасности РФ

2) Концепция внешней политики РФ

3) Военная доктрина

4) Доктрина информационной безопасности

5) Концепция общественной безопасности в РФ

6) Энергетическая стратегия России на период до 2030 г.

Темы докладов:

См. раздел «Работа с документами индивидуальная и в рамках микрогруппы».

Задание для работы с документами индивидуальная и в рамках микрогруппы:

В рамках практического занятия проводится подробный анализ существующих документов по информационной безопасности, оценивается степень их современности, приводятся примеры использования положений документов в современной мировой политике России и зарубежных стран.

Предусматривается разработка докладов по следующим темам:

1. Анализ деятельности государственных органов, контролирующих деятельность в области защиты информации.
2. Анализ Доктрины информационной безопасности
3. Анализ Стратегии национальной безопасности РФ
4. Анализ Стратегии развития информационного общества в РФ на 2017-2030гг.
5. Анализ Основ государственной политики РФ в области международной информационной безопасности на период до 2020 г.
6. Анализ Основных направлений научных исследований в области обеспечения информационной безопасности РФ.

7. Анализ Конвенции об обеспечении международной информационной безопасности (концепция)

8. Проблема устаревания официальных документов.

Документы, участвующие в разработке исследовательских проектов:

1. Доктрина информационной безопасности Российской Федерации. Утверждена 05.12.2016

2. Стратегия национальной безопасности Российской Федерации. Утверждена 02.07.2021

3. Стратегия развития информационного общества в Российской Федерации на 2017 – 2030 годы. Утверждена 09.05.2017.

4. Основы государственной политики РФ в области международной информационной безопасности. Утверждена 12.04.2021 г.

5. Основные направления научных исследований в области обеспечения информационной безопасности Российской Федерации. Утверждены 31.08.2017.

6. Государственная программа Российской Федерации «Информационное общество Утверждена 31.03.2020 г.

7. Указ Президента РФ «О совершенствовании государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации». Утвержден 22.12.2017 г.

8. Указ Президента РФ «О дополнительных мерах по обеспечению информационной безопасности РФ». Утвержден указом Президента РФ 01.05.2022

9. Федеральный закон №187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации». Утвержден 26 июля 2017 г.

10. Концепция Конвенции ООН об обеспечении международной информационной безопасности (проект, крайняя редакция 2021).

План выступления на представлении доклада

1. Обоснование актуальности выбранной темы.
2. Определение цели и задач.
3. Анализ источниковой базы исследования.
4. Выявление достоинств и недостатков документа, анализ степени соответствия документа современным политическим реалиям.
5. Предложения по корректировке данного документа.
6. Обзор аспектов реализации документа в политической жизни России и зарубежных стран.

Тема 4. Информационная безопасность в практике международных отношений. ИПК-19.2

Подготовка к практическому занятию:

– внимательно прочитать материал лекций, относящихся к данному занятию, ознакомиться с учебными материалами, включая электронные в соответствии с предложенным списком литературы в рабочей программе учебной дисциплины;

– подготовить развернутые ответы на вопросы для проведения опроса по теме практического занятия;

– понять, что осталось неясными и постараться получить на них ответ заранее;

– готовиться к практическому занятию можно как индивидуально, так и в составе малой группы.

Вопросы к практическому занятию для проведения опроса:

1. Российские инициативы в области международной информационной безопасности.
2. Переговорный процесс и международное сотрудничество в области обеспечения информационной безопасности.
3. Работа Комитетов ООН по безопасности и разоружению, по космосу, МСЭ, Группы восьми, Группы семи, Евросоюза, ШОС в области международной информационной безопасности.
4. Изменение расстановки сил на международной арене в 2014 г.– информационный аспект (2014-2026 гг.).
5. Информационная война США и Великобритании против России (2014 – 2026 гг.)
6. Перспективы установления международного контроля над информационными видами оружия и формирования глобального режима международной информационной безопасности и управления интернетом.

Примерные тестовые задания:

Внимательно прочитать текст задания и понять, что в качестве ответа ожидается один или несколько предложенных вариантов.

Внимательно прочитать предложенные варианты ответа.

Выбрать один или несколько верный(ых) ответ(ов).

Записать только букву(ы)/цифру(ы) выбранного(ых) варианта(ов) ответа(ов).

1. Сложность обеспечения информационной безопасности является следствием:

1) злого умысла разработчиков информационных систем;

2) объективных проблем современной технологии программирования;

3) происков западных спецслужб, встраивающих "закладки" в аппаратуру и программы.

2. Меры информационной безопасности направлены на защиту от:

1) нанесения любого ущерба;

2) нанесения неприемлемого ущерба;

3) попыток похищения любого вида информации.

3. Сложность обеспечения информационной безопасности является следствием:

1) невнимания широкой общественности к данной проблематике;

2) все большей зависимости общества от информационных систем;

3) быстрого прогресса информационных технологий, ведущего к постоянному изменению информационных систем и требований к ним.

4. Компьютерная преступность в мире

1) остается на одном уровне;

2) снижается;

3) растет.

Темы докладов:

- Деятельность России в ООН по обеспечению международной информационной безопасности.
- Деятельность ОДКБ и ШОС по обеспечению международной информационной безопасности.
- Деятельность ЕС и США по обеспечению международной информационной безопасности.
- Информационная война США и Великобритании против России.

Задание для работы с документами индивидуальная и в рамках микрогруппы:

Тема работы в микрогруппах: «Вхождение Крыма в состав Российской Федерации и его геополитические последствия (информационный аспект)».

Цель: Изучить геополитические последствия вхождения территории полуострова Крым в состав Российской Федерации, а также изучить интерпретацию данного события в мировых СМИ.

Предварительная работа:

1. Изучить материал по теме «Вхождение Крыма в состав России» в СМИ (печатных, сети Интернет).

2. Изучить практику международных прецедентов включения в состав

/выхода из состава государств административных территорий (образования самостоятельных государств) по результатам проведенных референдумов (в СМИ – печатных, сети Интернет).

Студенческая группа разбивается на 4 микрогруппы. На основе лекционного материала, докладов на семинарском занятии и

самостоятельной работы необходимо подготовить материалы по следующей схеме:

1) Проанализировать юридические основания вхождения территории полуострова Крым в состав Российской Федерации.
2) Проанализировать юридические основания вхождения (выхода) указанной территории в состав (из состава) другого государства.
3) Сравнить международную практику с событиями в Крыму в 2014 г.
4) Проанализировать геополитические последствия обоих событий.
5) Оценить информационную составляющую данного события: освещение в СМИ в РФ и за рубежом.

Международные прецеденты включения в состав /выхода из состава государств административных территорий (образования самостоятельных государств) по результатам проведенных референдумов:

- вхождение области Саар в состав ФРГ (1957 г.);
- выход Черногории из состава Государственного союза Сербии и Черногории (ГССЧ) (2006г.);
- выход из состава Сербии и образование частично признанной Республики Косово (2008 г.);
- образование частично признанных государств Южной Осетии и Абхазии (2008 г.);

Отчет по работе в микрогруппе делается в виде презентации.

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 обучающийся	Коэффициент веса контрольной точки	Результат контрольной точки, участвующий в формировании итоговой балльной оценки по дисциплине (отражается в журнале БРС в СДО)
КТ 1	100	0,3	30
КТ 2	100	0,3	30
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 - 2.
Опрос:
Вопросы для опроса:

№ п.п.	Содержание вопроса
1.	Информационное общество в России. Роль Интернета в современном обществе.
2.	Вызовы и угрозы безопасности, связанные с развитием информационных технологий.
3.	Противоборство и конфликты в информационной сфере. Понятие «кибер-безопасность».
4.	Информационные средства воздействия. Информационное оружие.
5.	Информационный терроризм и трансформация международного терроризма.
6.	Интересы государств и иных факторов мировой политики в информационной сфере.
7.	Информационные войны. Методы борьбы с ними.
8.	Использование передовых методов информационной безопасности в процессе эксплуатации прикладных ИС как элемент борьбы с информационными войнами.

Критерии оценивания:

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	

КТ – 2.
Тема 3 – 4.
Опрос:

Вопросы для опроса:

№ п.п.	Содержание вопроса
1.	Государственная политика в сфере обеспечения информационной безопасности.
2.	Государственные органы РФ, контролирующие деятельность в области защиты информации.
3.	Обеспечение защиты информации в области проектирования архитектуры и сервисов ИС предприятий и организаций.
4.	Нормативно-правовая база обеспечения информационной безопасности в России и за рубежом.
5.	Российские инициативы в области международной информационной безопасности.
6.	Изменение расстановки сил на международной арене в 2014 г. после воссоединения Крыма с Россией – информационный аспект.
7.	Работа Комитетов ООН по безопасности и разоружению, по космосу, МСЭ, Группы восьми, Группы семи, Евросоюза, ШОС в области международной информационной безопасности.
8.	Информационная война США и Великобритании против России.
9.	Перспективы установления международного контроля над информационными видами оружия и формирования глобального режима международной информационной безопасности и управления интернетом.
10.	Переговорный процесс и международное сотрудничество в области обеспечения информационной безопасности.

Критерии оценивания опроса:

Диапазон баллов	Описание критерия
85-100	Обучающийся полно излагает материал (отвечает на вопрос), дает правильное определение основных понятий; обнаруживает понимание материала, может

	обосновать свои суждения, применить знания на практике, привести необходимые примеры не только из учебника, но и самостоятельно составленные; излагает материал последовательно и правильно с точки зрения норм литературного языка.
65-84	Обучающийся дает ответ, удовлетворяющий тем же требованиям, что и для оценки «отлично», но допускает 1–2 ошибки, которые сам же исправляет, и 1–2 недочета в последовательности и языковом оформлении излагаемого.
55-64	Обучающийся обнаруживает знание и понимание основных положений данной темы, но излагает материал неполно и допускает неточности в определении понятий или формулировке правил; не умеет достаточно глубоко и доказательно обосновать свои суждения и привести свои примеры; излагает материал непоследовательно и допускает ошибки в языковом оформлении излагаемого.
0-54	Обучающийся обнаруживает незнание вопроса, допускает ошибки в формулировке определений и правил, искажающие их смысл, беспорядочно и неуверенно излагает материал.

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

Для решения контрольных заданий обучающемуся разрешается использование сборника правовых актов и документов, хрестоматий по дисциплине, личных конспектов по заданным вопросам.

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

6.1. Промежуточная аттестация проводится в форме зачета
6.2. Типовые оценочные материалы промежуточной аттестации.

Типовые проверочные задания для самоподготовки обучающегося к промежуточной аттестации:

Тема 1. Введение в проблему информационной безопасности. ИПК-11.2

1. Задания открытого типа.
1.1. Вопросы открытого типа.

№ п.п.	Вопрос
1.	Перечислите основные этапы построения КСЗИ.
2.	Назовите ГОСТ с учётом которых должны быть разработаны требования к системе защиты информации.

1.2. Контрольные задания:

Задание 1.

Перечислите этапы внедрения системы защиты информации.

Задание 2.

Перечислите процессы выполняемые при обеспечении защиты информации в ходе эксплуатации аттестованной информационной системы.

2. Задания комбинированного типа:

2.1. Тестовые задания с обоснованием выбора.

№ п.п.	Содержание задания	Правильный ответ	Аргументы, обосновывающие выбор ответа
1.	Основополагающим документом по обеспечению национальной безопасности является: Варианты ответов: а) Доктрина информационной безопасности б) Стратегия национальной безопасности Российской Федерации	б) Стратегия национальной безопасности Российской Федерации	Основополагающим документом по обеспечению национальной безопасности страны является Стратегия национальной безопасности Российской Федерации. Этот документ принимается не реже, чем раз в шесть лет. Крайняя редакция принята указом Президента РФ от 02.07.2021 г. №400.
2.	Какая организация отвечает за противодействие компьютерным атакам на кредитно-финансовую систему РФ? Варианты ответов: а) Роскомнадзор б) ФСБ России в) Центробанк РФ г) Минцифры	в) Центробанк РФ	С 2018 года ЦБ РФ осуществляет мониторинг и противодействие кибератакам на финансовую инфраструктуру через Ситуационный центр и систему FinCERT.

3. Задания закрытого типа.

3.1. Тестовые задания.

Тест 1.

Внимательно прочитать текст задания и понять, что в качестве ответа ожидается только один из предложенных вариантов.
Внимательно прочитать предложенные варианты ответа.
Выбрать один верный ответ.
Записать только букву выбранного варианта ответа.

1. Что понимается под информационной безопасностью?
A) Защита информации от несанкционированного доступа
B) Хранение информации в облаке
C) Создание веб-сайтов
D) Разработка программного обеспечения
Правильный ответ: A

2. Какой из следующих методов является примером кибератаки?
A) Фишинг
B) Обновление программного обеспечения
C) Использование антивируса
D) Создание резервных копий
Правильный ответ: A

Тест 2.
Внимательно прочитать текст задания и понять, что в качестве ответа ожидается несколько правильных ответов из предложенных вариантов.
Внимательно прочитать предложенные варианты ответа.
Выбрать несколько правильных ответов.
Записать только буквы выбранного варианта ответа.

1. Что такое конфиденциальность информации?
A) Возможность получить информацию за приемлемое время
B) Защита информации от несанкционированного доступа
C) Непротиворечивость и корректность данных
D) Обеспечение работоспособности информационной системы
Правильный ответ: B

2. Что означает целостность информации?
A) Информация доступна только авторизованным пользователям
B) Информация не была изменена несанкционированно
C) Информация может быть получена в любой момент
D) Информация зашифрована
Правильный ответ: B

Тема 2. Информационное противоборство и безопасность. Информационная война. ИПК-19.2

1. Задания открытого типа.

1.1. Вопросы открытого типа.

№ п.п.	Вопрос
1.	Дайте определение политики информационной безопасности.
2.	Дайте определение понятию «информационная война»

1.2. Контрольные задания.

Задание 1.

Назовите три основных принципа информационной безопасности (триада CIA).

Задание 2.

Какая современная угроза глобальной безопасности характеризуется целенаправленным использованием цифровых технологий для атак на критическую инфраструктуру государств?

2. Задания комбинированного типа.

2.1. Тестовые задания с обоснованием выбора.

№ п.п.	Содержание задания	Правильный ответ	Аргументы, обосновывающие выбор ответа
1.	Что такое информационная война? A) Обмен информацией между государствами B) Целенаправленное воздействие на информационное пространство противника с целью достижения политических, экономических или военных преимуществ C) Создание и распространение развлекательного контента D) Проведение социологических опросов	B) Целенаправленное воздействие на информационное пространство противника с целью достижения политических, экономических или военных преимуществ	Информационная война подразумевает активные действия по воздействию на информационное пространство оппонента — дезинформацию, пропаганду, кибератаки, манипуляции общественным мнением. Остальные варианты не отражают сути понятия.
2.	Какой из перечисленных методов относится к инструментам информационного противоборства? A) Строительство новых	B) Распространение фейковых новостей в социальных сетях	Фейковые новости — один из ключевых инструментов информационного противоборства: они формируют ложное представление о событиях,

	школ B) Распространение фейковых новостей в социальных сетях C) Проведение спортивных соревнований D) Развитие сельского хозяйства		манипулируют общественным мнением, создают напряжённость. Остальные варианты не связаны с информационными операциями.

3. Задания закрытого типа.

3.1. Тестовые задания.

Тест 1.

Внимательно прочитать текст задания и понять, что в качестве ответа ожидается только один из предложенных вариантов.

Внимательно прочитать предложенные варианты ответа.

Выбрать один верный ответ.

Записать только букву выбранного варианта ответа.

1.Что является целью информационной безопасности в условиях информ ационной войны?
A) Увеличение числа пользователей интернета
B) Обеспечение целостности, конфиденциальности и доступности инфор мации, защита от дезинформации и кибератак
C) Развитие социальных сетей
D) Создание новых медиаплатформ
Правильный ответ: B

2. Что такое фейк (fake news)?
A) Новость, опубликованная в официальном СМИ
B) Ложная информация, представленная как достоверная, с целью ввести в заблуждение
C) Научная статья в рецензируемом журнале
D) Сообщение от государственного органа
Правильный ответ: B

Тест 2.

Внимательно прочитать текст задания и понять, что в качестве ответа ожидается несколько правильных ответов из предложенных вариантов.

Внимательно прочитать предложенные варианты ответа.

Выбрать несколько правильных ответов.

Записать только буквы выбранного варианта ответа.

1.Какой инструмент чаще всего используется для распространения дезин формации?
A) Научные журналы
B) Социальные сети и мессенджеры
C) Библиотеки
D) Учебники
Правильный ответ: B

2.Что такое DDoS-атака?
A) Атака на систему с использованием вредоносного ПО
B) Атака, при которой множество компьютеров одновременно отправляют запросы на сервер, перегружая его
C) Метод шифрования данных
D) Способ защиты от вирусов
Правильный ответ: B

Тема 3. Нормативно-правовая база обеспечения информационной безопасности. ИПК-6.2

1. Задания открытого типа.

1.1. Вопросы открытого типа.

№ п.п.	Вопрос
1.	Какими документами должен руководствоваться специалист по защите информации при составлении плана мероприятий по улучшению защищённости объекта информатизации?
2.	Что регулирует Федеральный закон "О защите персональных данных"?

1.2. Контрольные задания.

Задание 1.

Объясните, почему соблюдение требований ФСТЭК и ФСБ критиче ски важно для организаций, работающих с конфиденциальной информац ией. Приведите два примера последствий несоблюдения этих требований .

Задание 2.

В чем состоит угроза дальнейшего развития ИИ и тотальной цифровизации?

2. Задания комбинированного типа.

2.1. Тестовые задания с обоснованием выбора.

№ п.п.	Содержание задания	Правильный ответ	Аргументы, обосновывающие выбор ответа
1.	Какой федеральный закон РФ определяет основные принципы защиты персональных данных? A) ФЗ № 149-ФЗ «Об информации, информационных технологиях и о защите информации» B) ФЗ № 152-ФЗ «О персональных данных» C) ФЗ № 98-ФЗ «О коммерческой тайне» D) ФЗ № 5485-1 «О государственной тайне»	B) ФЗ № 152-ФЗ «О персональных данных»	ФЗ № 152-ФЗ регулирует обработку персональных данных, устанавливает права субъектов данных и обязанности операторов, определяет требования к защите. Остальные законы касаются иных видов информации.
2.	Какой закон регулирует отношения в сфере информации, информационных технологий и защиты информации в РФ? A) ФЗ № 390-ФЗ «О безопасности» B) ФЗ № 149-ФЗ «Об информации, информационных технологиях и о защите информации» C) Конституция РФ D) УК РФ	B) ФЗ № 149-ФЗ «Об информации, информационных технологиях и о защите информации»	ФЗ № 149-ФЗ устанавливает общие принципы регулирования информационных отношений, определяет категории информации, регулирует доступ и распространение данных, а также вопросы защиты информации.

3. Задания закрытого типа.

3.1. Тестовые задания.

Тест 1.

Внимательно прочитать текст задания и понять, что в качестве ответа ожидается только один из предложенных вариантов.

Внимательно прочитать предложенные варианты ответа.

Выбрать один верный ответ.

Записать только букву выбранного варианта ответа.

1. Что регулирует ФЗ № 5485-1?
A) Коммерческую тайну
B) Государственную тайну
C) Персональные данные
D) Авторские права
Правильный ответ: B

2.Какой документ устанавливает требования к защите информации в госу дарственных информационных системах?
A) Приказ ФСТЭК России № 17
B) Приказ ФСБ России № 378
C) Постановление Правительства РФ № 1119
D) Указ Президента РФ № 646
Правильный ответ: A

Тест 2.

Внимательно прочитать текст задания и понять, что в качестве ответа ожидается несколько правильных ответов из предложенных вариантов.

Внимательно прочитать предложенные варианты ответа.

Выбрать несколько правильных ответов.

Записать только буквы выбранного варианта ответа.

1.Какой нормативный акт регулирует вопросы криптографической защит ы информации?
A) ФЗ № 149-ФЗ
B) Приказ ФСБ России № 378
C) ГОСТ Р 34.10-2012
D) Постановление Правительства РФ № 313
Правильный ответ: B

2. Специальная военная операция России на территории Украины:
1) началась 24 февраля 2022 г.
2) направлена на установление полного контроля над всей территорией Украины
3) целями СВО заявлены демилитаризация и денацификация Украины
4) основные военные действия в ходе СВО проходят на территории Западной Украины
5) в результате СВО Крым стал частью России
Правильный ответ: 1,3,5

Тема 4. Информационная безопасность в практике международных отношений. ИПК-19.2

1. Задания открытого типа.

1.1. Вопросы открытого типа.

№ п.п.	Вопрос
1.	Что такое «правила ответственного поведения государств в киберпространстве»?
2.	Назовите три ключевых направления международного сотрудничества в сфере информационной безопасности.

1.2. Контрольные задания.

Задание 1.

Объясните, почему международное регулирование киберпространс тва затруднено. Укажите три основные проблемы и предложите один спо соб их преодоления.

Задание 2.

Опишите, как кибератаки могут повлиять на международные отно шения. Приведите два конкретных примера таких атак и их последствия.

2. Задания комбинированного типа.

2.1. Тестовые задания с обоснованием выбора.

№ п.п.	Содержание задания	Правильный ответ	Аргументы, обосновывающие выбор ответа
1.	Что понимается под «информационной войной» в международных отношениях? A) Обмен информацией между дипломатическими ведомствами разных стран B) Целенаправленное использование информационных технологий для воздействия на общественное мнение и политические процессы других государств C) Создание международных информационных сетей D) Развитие телекоммуникационной инфраструктуры	B) Целенаправленное использование информационных технологий для воздействия на общественное мнение и политические процессы других государств	Информационная война подразумевает использование информационных технологий и методов для достижения политических целей, включая пропаганду, дезинформацию, кибератаки на критическую инфраструктуру других государств. Остальные варианты описывают обычные информационные процессы без агрессивного воздействия.
2.	Какой международный	A) Будапештская	Будапештская конвенция —

	документ устанавливает базовые принципы кибербезопасности и противодействия киберпреступности? A) Будапештская конвенция о киберпреступности (2001) B) Всеобщая декларация прав человека C) Женевские конвенции D) Парижская конвенция по охране промышленной собственности	конвенция о киберпреступности (2001)	первый и основной международный договор, направленный на борьбу с киберпреступностью, гармонизацию законодательства и международное сотрудничество в этой сфере. Остальные документы не касаются вопросов кибербезопасности.

3. Задания закрытого типа.

3.1. Тестовые задания.

Тест 1.

Внимательно прочитать текст задания и понять, что в качестве ответа ожидается только один из предложенных вариантов.

Внимательно прочитать предложенные вариант-ты ответа.

Выбрать один верный ответ.

Записать только букву выбранного варианта ответа.

1.Какая организация ООН занимается вопросами международной инфор мационной безопасности?
A) ЮНЕСКО
B) МАГАТЭ
C) МСЭ (Международный союз электросвязи)
D) ВОЗ
Правильный ответ: C

2. Что такое «кибератака государственного уровня»?
A) Атака на сайт частной компании
B) Кибератака, спонсируемая или осуществляемая государством против другой страны
C) Вирусное заражение домашнего компьютера
D) Спам-рассылка
Правильный ответ: B

Тест 2.

Внимательно прочитать текст задания и понять, что в качестве ответа ожидается только один из предложенных вариантов.

Внимательно прочитать предложенные вариант-ты ответа.

Выбрать несколько верных ответов.

Записать только букву выбранного варианта ответа.

1.Какой принцип международного права нарушается при проведении киб ератак на гражданскую инфраструктуру?
A) Принцип невмешательства во внутренние дела
B) Принцип суверенитета
C) Принцип неприменения силы и угрозы силой
D) Все вышеперечисленные
Правильный ответ: D

6.3. Критерии и шкала оценивания на основе БРС.

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 обучающийся 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, 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.	20-29
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. обучающийся не	0-19

способен ответить на вопросы даже при дополнительных наводящих вопросах преподавателя.	

6.4. Для решения контрольных заданий обучающемуся разрешается использование хрестоматийных материалов.

7. Методические материалы по освоению дисциплины (модуля)

Подготовка к лекциям.

Главное в период подготовки к лекционным занятиям – научиться методам самостоятельного умственного труда, сознательно развивать свои творческие способности и овладевать навыками творческой работы. Для этого необходимо строго соблюдать дисциплину учебы и поведения. Четкое планирование своего рабочего времени и отдыха является необходимым условием для успешной самостоятельной работы. В основу его нужно положить рабочие программы изучаемых в семестре дисциплин. Каждому обучающемуся следует составлять еженедельный и семестровый планы работы, а также план на каждый рабочий день. С вечера всегда надо распределять работу на завтрашний день. В конце каждого дня целесообразно подводить итог работы: тщательно проверить, все ли выполнено по намеченному плану, не было ли каких-либо отступлений, а если были, по какой причине это произошло. Нужно осуществлять самоконтроль, который является необходимым условием успешной учебы. Если что-то осталось невыполненным, необходимо изыскать время для завершения этой части работы, не уменьшая объема недельного плана.

Самостоятельная работа на лекции.

Слушание и запись лекций – сложный вид вузовской аудиторной работы. Внимательное слушание и конспектирование лекций предполагает интенсивную умственную деятельность обучающегося. Краткие записи лекций, их конспектирование помогает усвоить учебный материал. Конспект является полезным тогда, когда записано самое существенное, основное и сделано это самим обучающимся. Не надо стремиться записать дословно всю лекцию. Такое «конспектирование» приносит больше вреда, чем пользы. Запись лекций рекомендуется вести по возможности собственными формулировками. Желательно запись осуществлять на одной странице, а следующую оставлять для проработки учебного материала самостоятельно в домашних условиях. Конспект лекции лучше подразделять на пункты, параграфы, соблюдая красную строку. Этому в большой степени будут способствовать пункты плана лекции, предложенные преподавателям. Принципиальные места, определения, формулы и другое следует сопровождать замечаниями «важно», «особо важно», «хорошо запомнить» и т.п. Можно делать это и с помощью разноцветных маркеров или ручек. Лучше если они будут собственными, чтобы не приходилось просить их у однокурсников и тем самым не отвлекать их во время лекции. Целесообразно

разработать собственную «маркографию» (значки, символы), сокращения слов. Не лишним будет и изучение основ стенографии. Работая над конспектом лекций, всегда необходимо использовать не только учебник, но и ту литературу, которую дополнительно рекомендовал лектор. Именно такая серьезная, кропотливая работа с лекционным материалом позволит глубоко овладеть знаниями.

Подготовка к практическим занятиям.

Подготовку к каждому практическому занятию каждый обучающийся должен начать с ознакомления с планом практического занятия, который отражает содержание предложенной темы. Тщательное продумывание и изучение вопросов плана основывается на проработке текущего материала лекции, а затем изучения обязательной и дополнительной литературы, рекомендованную к данной теме. На основе индивидуальных предпочтений обучающемуся необходимо самостоятельно выбрать тему доклада по проблеме практического занятия и по возможности подготовить по нему презентацию. Если программой дисциплины предусмотрено выполнение практического задания, то его необходимо выполнить с учетом предложенной инструкции (устно или письменно). Все новые понятия по изучаемой теме необходимо выучить наизусть и желательно внести в глоссарий, который целесообразно вести с самого начала изучения курса. Результат такой работы должен проявиться в способности обучающегося свободно ответить на теоретические вопросы практического занятия, его выступлении и участии в коллективном обсуждении вопросов изучаемой темы, правильном выполнении практических заданий и контрольных работ.

Работа с источниками.

В процессе подготовки к практическим занятиям, обучающимся необходимо обратить особое внимание на самостоятельное изучение рекомендованной учебно-методической (а также научной и популярной) литературы. Самостоятельная работа с учебниками, учебными пособиями, научной, справочной и популярной литературой, материалами периодических изданий и Интернета, статистическими данными является наиболее эффективным методом получения знаний, позволяет значительно активизировать процесс овладения информацией, способствует более глубокому усвоению изучаемого материала, формирует у обучающихся свое отношение к конкретной проблеме. Более глубокому раскрытию вопросов способствует знакомство с дополнительной литературой, рекомендованной преподавателем, что позволяет обучающимся проявить свою индивидуальность в рамках выступления на занятиях, выявить широкий спектр мнений по изучаемой проблеме.

Вопросы для самостоятельной подготовки к лекционным и практическим занятиям:

1. Понятия «информация», «безопасность», «информационная безопасность», их сущность, измерения.

2. Информационное общество в России. Роль Интернета в современном обществе.

3. Вызовы и угрозы безопасности, связанные с развитием информационных технологий.

4. Субъекты международной информационной безопасности.

5. Противоборство и конфликты в информационной сфере. Понятие «кибер-безопасность».

6. Новые объекты безопасности в информационной сфере.

7. Информационные средства воздействия. Информационное оружие.

8. Информационный терроризм и трансформация международного терроризма.

9. Интересы государств и иных факторов мировой политики в информационной сфере.

10. Информационные войны. Методы борьбы с ними. Использование передовых методов информационной безопасности в процессе эксплуатации прикладных ИС как элемент борьбы с информационными войнами.

11. Государственная политика в сфере обеспечения информационной безопасности.

12. Государственные органы РФ, контролирующие деятельность в области защиты информации. Обеспечение защиты информации в области проектирования архитектуры и сервисов ИС предприятий и организаций.

13. Нормативно-правовая база обеспечения информационной безопасности в России и за рубежом.

14. Российские инициативы в области международной информационной безопасности.

15. Переговорный процесс и международное сотрудничество в области обеспечения информационной безопасности.

16. Работа Комитетов ООН по безопасности и разоружению, по космосу, МСЭ, Группы восьми, Группы семи, Евросоюза, ШОС в области международной информационной безопасности.

17. Изменение расстановки сил на международной арене в 2014 г. после воссоединения Крыма с Россией – информационный аспект. Информационная война США и Великобритании против России.

18. Перспективы установления международного контроля над информационными видами оружия и формирования глобального режима международной информационной безопасности и управления интернетом.

Для самостоятельной подготовки к лекционным и практическим занятиям рекомендуется использовать электронные информационно-

образовательные ресурсы Нижегородского института управления – филиала РАНХиГС - http://lms.ranepa.ru/.

8. Учебная литература и ресурсы информационно-телекоммуникационной сети Интернет

8.1. Основная литература

1. Баранова, Е. К. Информационная безопасность и защита информации : учебное пособие / Е.К. Баранова, А.В. Бабаш. — 4-е изд., перераб. и доп. — Москва : РИОР : ИНФРА-М, 2026. — 384 с. — (Высшее образование). — ISBN 978-5-369-02005-0. - Текст : электронный. - URL: https://znanium.ru/catalog/document?id=477891&ysclid=mnrzvhosr660760924 (дата обращения: 09.04.2026). – Режим доступа: по подписке.

2. Ищейнов, В. Я. Организационное и техническое обеспечение информационной безопасности. Защита конфиденциальной информации : учебное пособие / В.Я. Ищейнов, М.В. Мецатунян. — Москва : ИНФРА-М, 2024. — 256 с. — (Высшее образование: Специалитет). - ISBN 978-5-16-016535-6. - Текст : электронный. - URL: https://znanium.ru/catalog/product/2139841 (дата обращения: 07.06.2026). – Режим доступа: по подписке

3. Клименко, И. С. Информационная безопасность и защита информации: модели и методы управления : монография / И.С. Клименко. — Москва : ИНФРА-М, 2026. — 180 с. — (Научная мысль). — DOI 10.12737/monography_5d412ff13c0b88.75804464. - ISBN 978-5-16-015149-6. - Текст : электронный. - URL: https://znanium.ru/catalog/product/2238628 (дата обращения: 07.06.2026). – Режим доступа: по подписке

4. Ковалев, Д. В. Информационная безопасность: Учебное пособие / Ковалев Д.В., Богданова Е.А. - Ростов-на-Дону:Южный федеральный университет, 2016. - 74 с.: ISBN 978-5-9275-2364-1. - Текст : электронный. - URL: https://znanium.ru/catalog/product/997105 (дата обращения: 07.06.2026). – Режим доступа: по подписке.

5. Сычев, Ю. Н. Стандарты информационной безопасности. Защита и обработка конфиденциальных документов : учебное пособие / Ю.Н. Сычев. — 2-е изд., перераб. и доп. — Москва : ИНФРА-М, 2024. — 602 с. — (Высшее образование: Специалитет). — DOI 10.12737/2143785. - ISBN 978-5-16-019905-4. - Текст : электронный. - URL: https://znanium.ru/catalog/product/2143785 (дата обращения: 07.06.2026). – Режим доступа: по подписке.

8.2. Дополнительная литература

1. Добровольский, В. С. Управление интеллектуальной безопасностью : организационные и правовые основы информационной безопасности : учебное пособие / В. С. Добровольский. - Москва : Изд. Дом МИСиС, 2014. - 224 с. - ISBN 978-5-87623-789-7. - Текст :

электронный. - URL: **https://znanium.ru/catalog/product/1281124_2**. (дата обращения: 07.06.2026). – Режим доступа: по подписке.

2. Информационная безопасность: вчера, сегодня, завтра: сборник статей по материалам VI Всероссийской научно-практической конференции (Москва, 12 апреля 2023 г.) / отв. ред. В. В. Арутюнов. - Москва : РГГУ, 2023. - 133 с. - ISBN 978-5-7281-3273-8. - Текст : электронный. - URL: https://znanium.ru/catalog/product/2161284 (дата обращения: 07.06.2026).

3. Федоров, А. В. Политологические основы информационной безопасности : учебно-методическое пособие / А. В. Федоров. - Москва : МГТУ им. Баумана, 2019. - 36 с. - ISBN 978-5-7038-5253-8. - Текст : электронный. - URL: **https://znanium.com/catalog/product/2013674** (дата обращения: 07.06.2026). – Режим доступа: по подписке.

4. Чернышов, А. Н. Межсекторное взаимодействие в социальной сфере как фактор обеспечения экономической безопасности: теоретическая основа, исторический и современный опыт, методология развития : монография / А. Н. Чернышов, А. В. Чернышова. - Нижний Новгород : НИУ РАНХиГС, 2022. - 244 с. - ISBN 978-5-00036-282-2. - Текст : электронный. - URL: https://znanium.ru/catalog/product/2223479 (дата обращения: 07.06.2026). – Режим доступа: по подписке

8.3. Нормативные правовые документы и иная правовая информация

1. Федеральный закон «Об образовании в Российской Федерации» от 29.12.2012 №273-ФЗ

2. Приказ Министерства науки и высшего образования Российской Федерации от 06.04.2021 №245 «Об утверждении Порядка организации и осуществления образовательной деятельности по образовательным программам высшего образования - программам бакалавриата, программам специалитета, программам магистратуры»

3. Приказ РАНХиГС Об утверждении положения о единой балльно-рейтинговой системе оценивания успеваемости студентов Академии и ее использовании при проведении текущей и промежуточной аттестации от 12.12.2024 №02-2531.

8.4. Интернет-ресурсы

1. Открытый текст. Электронное периодическое издание. Текст истории. История России. URL: https://opentextnn.ru/

2. Справочно-правовая система «КонсультантПлюс» — URL: www.consultant.ru

3. Справочно-правовая система «Гарант» — URL: www.garant.ru.

4. Библиотека Гумер. Право и юриспруденция. — URL: http://www.gumer.info/bibliotek_Buks/Pravo/_Index_Pravo.php

5. Конституция Российской Федерации. — URL: http://www.constitution.ru/index.htm

6. Электронная Библиотека Диссертаций Российской государственной библиотеки ЭБД РГБ. — URL: http://diss.rsl.ru

7. Библиотека электронных ресурсов Исторического факультета МГУ им. М.В.Ломоносова http://www.hist.msu.ru/ER/Etext/index.html

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

9.1. Материально-техническая база

Перечень материально-технического обеспечения:

1. Учебные аудитории, оборудованные для проведения учебных занятий лекционного и семинарского типа, групповых и индивидуальных консультаций, коллоквиумов, мероприятий текущего контроля и промежуточной аттестации, в том числе мультимедийным оборудованием для демонстрации электронных презентаций и аудио- и видеоматериалов;
2. Компьютерные классы для выполнения групповых тестовых и иных заданий, а также для самостоятельной работы обучающихся оснащенные компьютерной техникой и обеспечением доступа к сети «Интернет» и доступа в электронную информационно- образовательную среду организации;
3. Специализированные аудитории и лаборатории;
4. Библиотека с обеспечением печатными изданиями или электронно-библиотечная система обеспечивающая доступ к электронным изданиям (электронная библиотека);
5. Читальный зал;
6. Технические средства обучения: персональные компьютеры; компьютерные проекторы; звуковые динамики; программные средства, обеспечивающие просмотр видеофайлов в форматах AVI, MPEG-4, DivX, RMVB, WMV и др.

9.2. Информационные технологии, программное обеспечение:

При осуществлении образовательного процесса по дисциплине используется информационные технологии и программное обеспечение:

1. Современная операционная система.
2. Kaspersky Endpoint Security (или аналог).
3. Средство просмотра файлов формата pdf.
4. Современные офисные средства (текстовые и табличные редакторы, средства работы с презентационными материалами и т.д.).
5. Архиватор 7-Zip.
6. Система дистанционного обучения.
7. Автоматизированная библиотечная система.

9.3. Информационные справочные системы:

1. https://www.iprbookshop.ru – Электронно-библиотечная система

[ЭБС]«IPRSMART»(ранее–IPRBooks)

2. https://e.lanbook.com -Электронно-библиотечная система [ЭБС] «Лань».
3. https://znanium.ru - Электронно-библиотечная система [ЭБС] «Znanium.com».
4. https://www.book.ru - Электронно-библиотечная система[ЭБС]«Book.ru».
5. https://ibooks.ru-Электронно-библиотечная система [ЭБС]«ibooks.ru».
6. https://ranepalib.miflib.ru - Электронная библиотека издательства «МИФ».
7. https://eivis.ru–Ивис (EastView). Полные тексты российских научных и практических журналов, а также газет центральной прессы России. Доступ с ip-адресов локальной сети Института.
8. http://www.consultant.ru/-Справочно-правоваясистема «Консультант».
9. http://www.garant.ru/Справочно-правоваясистема «Гарант».