Приложение 4

к образовательной программе

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

К.М.01.ДЭ.01.01.06 Цифровая этика и безопасность в цифровой среде

(индекс, наименование дисциплины в соответствии с учебным планом)

38.03.04 Государственное и муниципальное управление

(код, наименование направления подготовки/специальности)

Лидеры регионов. Санкт-Петербург

(наименование образовательной программы)

очная

(форма обучения)

Год набора - 2026

Санкт-Петербург

Автор(ы)-составитель(и) РПД:

Шеина Анастасия Юрьевна, канд. экон. наук, доцент, доцент кафедры государственного и муниципального управления

Заведующий кафедрой:

Хлутков Андрей Драгомирович, д.э.н., доцент, заведующий кафедрой государственного и муниципального управления

Рабочая программа дисциплины К.М.01.ДЭ.01.01.06 «Цифровая этика и безопасность в цифровой среде» одобрена на заседании кафедры государственного и муниципального управления факультета Государственного и муниципального управления СЗИУ РАНХиГС. Протокол № 4 от 26 марта 2026 г.

СОДЕРЖАНИЕ

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

Дисциплина К.М.01.ДЭ.01.01.06 «Цифровая этика и безопасность в цифровой среде» обеспечивает формирование у обучающихся следующих профессиональных компетенций:

ОТФ/ТФ и реквизиты ПС *(при наличии)*	**Код компетенции**	**Наименование Компетенции**	**Код индикатора достижения компетенций**	**Наименование индикатора достижения компетенций**	**Образовательный результат**
С Организационное, документационное и информационное обеспечение деятельности руководителя организации С/07.6 Организация исполнения решений, осуществление контроля исполнения поручений руководителя С/10.6 Составление и оформление управленческой документации С/13.6 Обеспечение руководителя информацией Приказ Минтруда России «Об	ПК-2	Способен обеспечивать документационное и информационное сопровождения деятельности руководителя	ПК-2.3	Обеспечивает руководителя информационно-аналитическими материалами для принятия управленческих решений	ПК-2.3 З-1. Знает методы сбора и систематизации информации для подготовки аналитических материалов ПК-2.3 З-2. Знает технологии анализа данных и подготовки справочных материалов ПК-2.3 У-1. Умеет анализировать информацию и готовить справочно-аналитические материалы ПК-2.3 У-2. Умеет использовать цифровые инструменты для информационного обеспечения ПК-2.3 У-3. Владеет навыками информационно-аналитического сопровождения управленческой деятельности

утверждении профессионального стандарта «Специалист по организационному и документационному обеспечению управления организацией» от 15.06.2020 года № 333н					
Информационно-аналитическое проведение подготовки проекта A/01.6 Сбор и анализ первичной информации в рамках реализации проекта A/02.6 Подготовка финансово-экономического обоснования реализации проекта Приказ Минтруда России «Об утверждении профессионального стандарта «Специалист в сфере управления	ПК-7	Способен управлять жизненным циклом проекта и осуществлять его информационное сопровождение	ПК-7.4	Координирует участников проекта и обеспечивает взаимодействие заинтересованных сторон	ПК-7.4 З-1. Знает принципы командной работы и методы координации участников проекта ПК-7.4 З-2. Знает технологии управления коммуникациями и взаимодействием стейкхолдеров ПК-7.4 У-1. Умеет организовывать взаимодействие команды проекта и стейкхолдеров ПК-7.4 У-2. Умеет применять коммуникационные стратегии в проектной деятельности ПК-7.4 В-1. Владеет навыками управления коммуникациями и

проектами государственно-частного партнерства» от 20.07.2020, № 431					координации участников

2. Объем и место дисциплины в структуре образовательной программы

Объем дисциплины

Общая трудоемкость дисциплины составляет 2 зачетные единицы, 72 академических часа для очной формы обучения.

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

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

Объем академических часов, выделенных на контактную работу обучающихся с преподавателем, 32 ак. час.

Теоретические занятия (лекции) проводятся по потокам. Общий объем лекционного курса составляет 14 академических часов.

Практические занятия организуются по группам в виде семинаров в диалоговом режиме. Общий объем практических занятий 14 академических часов.

Программой предусмотрена самостоятельная работа студентов в объеме 40 академических часа на очной форме. В рамках самостоятельной работы студенты изучают теоретический материал в целях подготовки к устному опросу и тестированию, выполняют профессионально-исследовательское задание, готовятся к устному опросу и практическим контрольным заданиям.

Место дисциплины в структуре ОП ВО

Дисциплина **К.М.01.ДЭ.01.01.06 «Цифровая этика и безопасность в цифровой среде»** относится к треку «Технологии эффективного государственного и муниципального управления» профессиональных треков по выбору обучающегося комплексных модулей по программе «Лидеры регионов.Санкт-Петербург» по направлению подготовки 38.03.04 «Государственное и муниципальное управление» и изучается студентами в 7 семестре 4 курса.

Дисциплина реализуется после изучения:

К.М.01.ДЭ.01.01.03 Цифровое государственное управление и открытые данные,
Б1.О.02.ДЭ.02.02 Цифровые технологии в государственном и муниципальном управлении,
Б1.О.02.ДЭ.02.01, Архитектура цифрового государства,
Б1.О.01.02.07 Модуль "Цифровая грамотность"

Формой промежуточной аттестации в соответствии с учебным планом является зачет.

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	Этические вызовы цифровой трансформации государственного	14	2			2								10	Т, ПИЗ

	управления													
Тема 2	Информационная безопасность в органах государственной власти	18	4			4							10	ПИЗ
Тема 3	Этика применения ИИ-технологий в государственном секторе	18	4			4							10	ПИЗ
Тема 4	Цифровая этика руководителя в государственном секторе	18	4			4							10	ПИЗ
Промежуточная аттестация		4								4				Зачет
Итого		72	14			14				4			40	

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.
ПИЗ – профессионально-исследовательские задания.

В процессе обучения применяются следующие интерактивные формы: лекция-диалог, работа в малых группах, спарринг-партнерство.
Темы 1-4 могут быть освоены с применением ЭО и ДОТ с контролем в системе электронного обучения Академии.

3.2. Содержание дисциплины

Тема 1. Этические вызовы цифровой трансформации государственного управления ПК-2.3

Цифровая трансформация как источник новых этических диллем. Характеристика гуманитарных угроз и возможностей использования цифровых и ИИ-технологий в государственном управлении. Проблема алгоритмической предвзятости и дискриминации в ГМУ. Работа с персональными данными граждан: проблемы утечки данных, этические и правовые ограничения в использовании данных. Цифровое неравенство как этическая проблема. Проблема дегуманизации решений в области ГМУ. Зарубежные и российские примеры этических пример в области цифровых и ИИ-технологий в государственном управлении.

Основные понятия: этические дилеммы, гуманитарные угрозы, утечка данных, цифровое неравенство, этические ограничения, данные, этика, цифровая трансформация.

Тема 2. Информационная безопасность в органах государственной власти ПК-2.3

Информационная безопасность. Соотношение понятий информационная безопасность, кибербезопасность, цифровая безопасность. Понятие «Цифровой суверенитет» Нормативно-правовые основы информационной безопасности. Доктрина информационной безопасности Российской Федерации. Основные угрозы информационной безопасности. Стандарты в области информационной безопасности. Модель триада информационной безопасности: конфиденциальность, целостность, доступность. Технические средства защиты. Организация системы информационной безопасности в органах власти. Понятие и виды социоинженерных атак. Рекомендации по формированию цифрового доверия к государственным органам с учетом разных видов социоинженерных атак.

Основные понятия: информационная безопасность, кибербезопасность, социоинженерные атаки, цифровое доверие, цифровая безопасность, конфиденциальность, целостность, доступность.

Тема 3 Этика применения ИИ-технологий в государственном секторе ПК-7.4

Методологические основы этики ИИ-технологий. Вопросы доверия к ИИ-технологиям в госсекторе. Модель доверенного искусственного интеллекта. Кодекс этики в сфере ИИ. Принципы применения ИИ-технологий. Модели ответственности применения ИИ-технологий.

Руководящие принципы в сфере роботов общего назначения. Типы рисков применения ИИ-технологий в госсекторе, их последствия и меры реагирования. Классификация информации и ограничения на ее обработку средствами ИИ для государственного служащего. Проведение этической и правовой оценки ИИ-решений. Психологические аспекты взаимодействия человека с ИИ.

Основные понятия: ии-технологии, доверенный ИИ, этика в сфере ИИ, персональные данные, этические риски, кодекс этики ИИ, принцип ответственности, принцип безопасности, принцип недискриминации, принцип сохранения разнообразия и защиты культурного наследия, принцип сохранения человеческого контроля

Тема 4. Цифровая этика руководителя в государственном секторе ПК-7.4

Понятия «Цифровая этика», «информационная этика». Цифровая этика руководителя в области ГМУ как аспект формирования цифрового доверия граждан к государству. Элементы цифровой этики. Принципы этичного поведения в цифровой среде. Цифровой этикет. Ответственность за управленческие решение и информационный контент. Этика ведения официальных аккаунтов. Интеллектуальная собственность. Цифровая репутация государственного служащего. Управление цифровой репутацией. Понятие цифрового следа государственного служащего. Цифровая гигиена. Цифровая компетентность руководителя в госсекторе.

Основные понятия: цифровая этика, информационная этика, цифровая репутация, цифровой след, цифровая грамотность.

4. Типы оценочных материалов, показатели и критерии оценивания

4.1. Оценочные материалы по дисциплине К.М.01.ДЭ.01.01.06 Цифровая этика и безопасность в цифровой среде 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):

Т – тестирование, ПИЗ – профессионально-исследовательские задания.

5.2. Типовые оценочные материалы для текущего контроля успеваемости обучающихся:

Тема 1. Этические вызовы цифровой трансформации государственного управления

Тестовые задания:

1) Что такое алгоритмическая предвзятость в контексте использования ИИ-технологий в государственном управлении?

А) Сбои в работе алгоритма из-за устаревшего оборудования

Б) Ситуация, когда алгоритм систематически принимает решения, ущемляющие права определённых групп граждан из-за нерепрезентативности обучающих данных

В) Предпочтение, которое разработчики отдают одним языкам программирования перед другими
Г) Ускорение работы алгоритма после обновления программного обеспечения
2. Установите соответствие между этическим вызовом и его конкретным проявлением в государственном управлении.
1 Алгоритмическая предвзятость
2 Проблема "чёрного ящика" (непрозрачность)
3 Цифровой суверенитет
4 Нарушение приватности / Утечка данных

А Чиновник не может объяснить гражданину, почему ИИ-система отказала в предоставлении выплаты, так как логика решения скрыта в "чёрном ящике" нейросети.
Б Зарубежная ИИ-платформа, используемая для подготовки аналитических записок, передаёт данные своих пользователей материнской компании, что создаёт угрозу национальной безопасности.
В ИИ-система отбора кадров на госслужбу, обученная на исторических данных, где преобладали мужчины, систематически занижает рейтинг кандидатов-женщин. |
Г В регионе внедрена система "социального рейтинга", которая без согласия граждан собирает данные об их покупках, перемещениях и круге общения для расчёта "благонадёжности".

ПИЗ по теме 1:

1. Приведите примеры этических дилемм, которые могут возникнуть или уже возникли при внедрении современных технологий в социальные сферы?

Тема 2. Информационная безопасность в органах государственной власти

ПИЗ по теме 2.

Вы – начальник отдела кадровой политики и безопасности администрации региона. За последние полгода в органах власти региона участились случаи успешных социоинженерных атак. Мошенники, используя методы психологического воздействия, получают доступ к служебной информации, убеждают сотрудников переводить денежные средства или передавать конфиденциальные данные.

Губернатор поручил вашему отделу:

1. Провести анализ типов социоинженерных атак, которым наиболее подвержены сотрудники.
2. Выявить категории сотрудников, которые чаще всего становятся жертвами.
3. Оценить риски и возможные последствия для органов власти.
4. Разработать классификацию атак и предложить меры профилактики.

Задание 1. Классификация социоинженерных атак

Создайте таблицу классификации социоинженерных атак, используя

предложенные типы атак. Для каждого типа укажите: краткое описание; пример из практики, средства коммуникации (телефон, email, мессенджеры, личное общение); на какие качества человека давит атака

Задание 2. Анализ уязвимых категорий сотрудников

На основе статистики и экспертных оценок, определите, какие категории сотрудников органов власти наиболее часто становятся жертвами социоинженерных атак. Заполните таблицу, указав:

- Категорию сотрудников (должность, возраст, функционал);
- Факторы уязвимости (почему именно эта категория подвержена риску);
- Типы атак, которым они наиболее уязвимы (из классификации выше);
- Примеры реальных случаев (можно обобщённые).

Почему люди, хорошо знающие инструкции по безопасности, всё равно становятся жертвами социоинженерии? Какие психологические механизмы здесь работают?

Задание 3.

Для каждого типа социоинженерных атак (или для наиболее опасных) оцените возможные последствия для органа власти по шкале от 1 до 5 (где 5 – катастрофические последствия). Заполните матрицу рисков.

- Какие три типа атак вы считаете наиболее опасными для органов власти и почему?
- Какие последствия являются наиболее критичными (необратимыми)?

Задание 4

Разработка памятки «5 правил защиты от социальной инженерии»

На основе проведённого анализа разработайте краткую памятку (не более 5 пунктов) для сотрудников органов власти, которая поможет им распознавать социоинженерные атаки и противостоять им. Каждый пункт должен содержать:

- Конкретное правило;
- Краткое пояснение (почему это важно);
- Пример нарушения правила.

Тема 3 Этика применения ИИ-технологий в государственном секторе

ПИЗ по теме 3.

Напишите краткое эссе, по теме «Этика применения ИИ-технологий в государственном секторе» на конкретном примере, с постановкой проблемы, аргументацией Вашей позиции.

Например,

«Проблема распределения ответственности при использовании ИИ в госорганах»:

Аннотация: Если ИИ-система принимает ошибочное решение, причинившее вред гражданину, кто должен нести ответственность? Разработчик, обучивший модель на некачественных данных? Чиновник, утвердивший решение? Орган власти, внедривший систему? В эссе необходимо проанализировать различные модели распределения ответственности, оценить их применимость в российском правовом поле и предложить оптимальный подход для госсектора.

Тема 4. Цифровая этика руководителя в государственном секторе

ПИЗ по теме 4.

В условиях цифровой трансформации каждый государственный служащий, особенно руководитель, становится публичной фигурой. Информация, размещённая в открытых источниках (социальные сети, форумы, комментарии, фото), формирует цифровой след, который влияет на доверие граждан, решения кадровых служб и репутацию органа власти в целом. По данным исследований, 70% работодателей проверяют кандидатов в соцсетях, а для госслужбы этот показатель стремится к 100%.

Цель задания: сформировать у студентов навыки аудита цифрового следа, оценки репутационных рисков и разработки стратегии управления цифровой репутацией.

Задание 1

Дайте определения следующим понятиям (кратко, 1-2 предложения): Цифровой след, Активный цифровой след, Пассивный цифровой след, Цифровая репутация, Управление репутацией, Цифровой сквоттинг, Фейковые новости (применительно к репутации), Репутационный аудит.

Задание 2. Классификация цифрового следа с позиции активный/пассивный цифровой след:

Пост в социальных сетях, История поиска в Яндексе, Лайк под постом коллеги, Геолокация телефона, Комментарий соц сети, Данные о покупках по банковской карте, Фото, на котором вас отметили друзья, Подписка на паблики, Просмотр видео на платформе, Участие в онлайн-опросе

Задание 3

Самодиагностика: аудит собственного цифрового следа

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	0,1	10
КТ - 2	100	0,2	20
КТ- 3	100	0,2	20
КТ - 4	100	0,1	10
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.
Тестирование.
Практическое контрольное задание (ПИЗ).

КТ-2
Тема 2.
Профессионально-исследовательское задание (ПИЗ).

КТ-3
Тема 3.
Профессионально-исследовательское задание (ПИЗ).

КТ-4
Тема 4.
Профессионально-исследовательское задание (ПИЗ).

К 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 ПИЗ:*

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 заданий	*30*	*Количество выполненных заданий от 85% до 100%*
	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 (ПИЗ), тестовых заданий студенту разрешается использование 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 (зачет) проводится в форме ответа на теоретические вопросы и решения задания.

Зачет проводится в период сессии в соответствии с текущим графиком учебного процесса, утвержденным в соответствии с установленным в СЗИУ порядком. Продолжительность зачета с оценкой для каждого студента не может превышать четырех академических часов. Зачет не может начинаться ранее 9.00 часов и заканчиваться позднее 21.00 часа. Зачет проводится в аудитории, в которую запускаются одновременно не более 5 человек. Время на подготовку ответов по билету каждому обучающемуся отводится 45 минут. При явке на зачет обучающийся должен иметь при себе зачетную книжку. Во время зачета обучающиеся по решению преподавателя могут пользоваться учебной программой дисциплины и справочной литературой.

6.2. Типовые оценочные материалы промежуточной аттестации.

Вопросы для подготовки к зачету

Изложите теоретические основы по данной теме (дайте определения, перечислите и назовите) и обоснуйте (аргументируйте и продемонстрируйте) свое отношение к данной теме (на конкретном примере):

1. Этические дилеммы, возникающие в процессе цифровой трансформации
2. Гуманитарные угрозы, связанные с использованием цифровых технологий и ии-технологий в госуправлении
3. Возможные проявления алгоритмической предвзятости и дискриминации в управленческих решениях?
4. Проблемные аспекты в работе с персональными данными
5. Приведите примеры утечек персональных данных граждан и последствий таких нарушений.
6. Понятие «цифрового неравенства» и почему оно становится серьезной этической проблемой.

7. Опишите зарубежные и российские случаи подходов к разрешению этических проблем в цифровом государстве.
8. Назовите основные направления преодоления дегуманизации решений в государственном управлении.
9. Какие законодательные нормы регулируют использование больших данных в российском госуправлении?
10. Дайте характеристику российским и зарубежным примерам внедрения принципов этического использования ИИ в государственно-управленческих процессах.
11. Чем отличаются понятия «информационная безопасность», «кибербезопасность» и «цифровая безопасность»?
12. Перечислите ключевые положения доктрины информационной безопасности Российской Федерации.
13. Определите основную угрозу конфиденциальности данных органов государственной власти.
14. Какие стандарты применяются для обеспечения информационной безопасности в государственных структурах?
15. Охарактеризуйте роль модели триады C-I-A «конфиденциальность—целостность—доступность» в обеспечении информационной безопасности.
16. Какие существуют методы технических средств защиты данных в органах власти?
17. Приведите классификацию социоинженерных атак
18. Какие рекомендации следует учитывать для повышения уровня цифрового доверия граждан к государству с учетом социоинженерных атак
19. В чём заключаются методологические основы этики применения ИИ-технологий?
20. Как повысить осознанный уровень доверия населения к технологиям искусственного интеллекта в госструктурах?
21. Раскройте содержание Кодекса этики в сфере ИИ и укажите ключевые пункты документа.
22. Перечислите основные типы рисков, связанных с применением ИИ-технологий в государственном секторе.
23. Обоснуйте необходимость соблюдения принципа недискриминации при внедрении ИИ в государственные процессы.
24. Назовите возможные причины возникновения ошибок и сбоев в работе ИИ-моделей и способы их предотвращения.
25. Расскажите о роли человеческой экспертизы в принятии решений, поддерживаемых искусственным интеллектом.
26. Какие механизмы контроля и проверки надёжности рекомендательных моделей на основе ИИ используются в государственном управлении?

27. Определите границы ответственности разработчиков и пользователей ИИ-систем в государственном секторе.
28. Объясните значение классификации информации и ограничений на её обработку средствами ИИ для государственных служащих.
29. Дайте определение понятий «цифровая этика» и «информационная этика».
30. Какие элементы входят в структуру цифровой этики руководителя в области государственного управления?
31. Какова ответственность руководителей государственных структур за принимаемые ими управленческие решения и публикуемый информационный контент?
32. Изложите рекомендации к ведению официальных социальных сетей государственными органами и должностными лицами.
33. Что включает в себя понятие интеллектуальной собственности в цифровой среде и какое отношение оно имеет к руководителям государственного сектора?
34. Почему важна забота о своей цифровой репутации и каким образом государственный служащий должен управлять своим цифровым профилем?
35. О каком понятии идет речь, когда говорят о «цифровом следе» государственного служащего?
36. Что понимается под термином «цифровая гигиена» и как она связана с работой государственных чиновников?
37. Объясните взаимосвязь цифровой компетенции руководителя и эффективности реализации цифровой стратегии ведомства.

Типовые задания для зачета

1. Как повысить осознанный уровень доверия населения к технологиям искусственного интеллекта в госструктурах?
2. Какие стандарты применяются для обеспечения информационной безопасности в государственных структурах?

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	1.Внимательно прочитать текст задания и понять, что в качестве ответа ожидается только один из предложенных вариантов. 2. Внимательно прочитать	1) Что такое алгоритмическая предвзятость в контексте использования ИИ-технологий в государственном управлении? А) Сбои в работе алгоритма из-за устаревшего оборудования

предложенных	предложенные варианты ответа. 3. Выбрать один верный ответ. 4. Записать только номер (или букву) выбранного варианта ответа (например, 3 или В).	Б) Ситуация, когда алгоритм систематически принимает решения, ущемляющие права определённых групп граждан из-за нерепрезентативности обучающих данных В) Предпочтение, которое разработчики отдают одним языкам программирования перед другими Г) Ускорение работы алгоритма после обновления программного обеспечения
		Начальник отдела документационного обеспечения администрации города получил на служебную электронную почту письмо от имени главы администрации. В письме содержалось срочное поручение: перевести крупную сумму денег со счёта администрации на счёт подрядчика для оплаты срочных работ по ликвидации аварии. Письмо было оформлено в официальном стиле, содержало подпись и логотип администрации. Начальник отдела, не проверяя информацию по телефону, перевёл деньги. Через день выяснилось, что счёт подрядчика был фальшивым, а письмо — фишинговым. Вопрос: Какое «фундаментальное правило кибербезопасности» было нарушено в первую очередь, и какое действие руководителя является наиболее правильным для предотвращения подобных инцидентов в будущем? А Было нарушено правило использования антивирусного программного обеспечения. Руководитель должен немедленно закупить самый дорогой антивирус и установить его на все компьютеры. Б Нарушено правило «трёхфакторной аутентификации». Руководитель обязан внедрить систему биометрической идентификации для подтверждения всех

		финансовых операций. В Нарушен принцип «доверяй, но проверяй» — отсутствовала обязательная процедура подтверждения финансовых поручений по альтернативному каналу связи (например, по телефону). Руководитель должен ввести регламент, согласно которому любые финансовые операции подтверждаются личным звонком руководителю или его заместителю. |Г Нарушена политика парольной защиты. Руководитель должен ужесточить требования к сложности паролей и заставить всех сотрудников сменить пароли немедленно.
Задание закрытого типа на установление соответствия	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).	1. Установите соответствие между этическим вызовом и его конкретным проявлением в государственном управлении. 1 Алгоритмическая предвзятость 2 Проблема "чёрного ящика" (непрозрачность) 3 Цифровой суверенитет 4 Нарушение приватности / Утечка данных А Чиновник не может объяснить гражданину, почему ИИ-система отказала в предоставлении выплаты, так как логика решения скрыта в "чёрном ящике" нейросети. Б Зарубежная ИИ-платформа, используемая для подготовки аналитических записок, передаёт данные своих пользователей материнской компании, что создаёт угрозу национальной безопасности. В ИИ-система отбора кадров на госслужбу, обученная на исторических данных, где преобладали мужчины, систематически занижает рейтинг кандидатов-женщин. | Г В регионе внедрена система "социального

		рейтинга", которая без согласия граждан собирает данные об их покупках, перемещениях и круге общения для расчёта "благонадёжности". 2. Установите соответствие между технологией ИИ и примером ее применения: 1) Компьютерное зрение a) Обработка обращений граждан 2) Обработка естественного языка b) Подбор вакансии для безработного на основе его профиля 3) Предиктивная аналитика c) Автоматический контроль заполняемости контейнеров ТКО по фото 4) Рекомендательные системы d) Прогнозирование нагрузки на поликлиники в период эпидемии гриппа
Задание закрытого типа с выбором нескольких правильных ответов из нескольких вариантов предложенных	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 буквы) выбранного варианта ответа (например, 1 4 или А Г).	1. Какие из перечисленных ситуаций с наибольшей вероятностью являются попытками социоинженерной атаки на сотрудника органа власти? **Варианты ответа:** А Получение электронного письма от имени начальника управления с просьбой срочно перевести деньги на новый счёт подрядчика, реквизиты которого изменились. Б Звонок от «сотрудника ФСБ», который сообщает об утечке данных и требует немедленно сообщить пароль от служебного аккаунта для проверки. В Обнаружение на парковке возле здания администрации USB-флешки с надписью «Зарплата за декабрь». Г Приглашение по электронной почте на бесплатный вебинар по повышению

		квалификации от неизвестного образовательного центра. Д. Сообщение в мессенджере от коллеги с просьбой проголосовать за ребёнка в конкурсе, перейдя по ссылке. Е. Объявление на сайте госзакупок о проведении открытого конкурса с завышенной начальной ценой контракта. 2. Какие из перечисленных задач относятся к компетенции компьютерного зрения? (выберите ВСЕ подходящие варианты) - А) Распознавание государственных номеров автомобилей - Б) Анализ тональности обращения граждан - В) Обнаружение ям на дорогах по видео с камер - Г) Прогнозирование количества обращений в скорую помощь - Д) Подсчет количества людей в общественном транспорте
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 последовательность из предложенных элементов. 4. Записать буквы/цифры (в зависимости от задания) вариантов ответа в нужной последовательности	1. Региональное министерство транспорта решило внедрить систему компьютерного зрения для автоматического выявления ям на дорогах. Вы как руководитель проекта должны выстроить правильную последовательность этапов внедрения, чтобы минимизировать риски и добиться результата. Предложенные этапы (действия): А Провести пилотное тестирование модели на ограниченном участке дорог и оценить её точность в реальных условиях. Б Осуществить сбор и разметку данных (фото и видео дорог с ямами и без, в разное время суток и погоду). В Масштабировать решение на весь

	(например, БВА или 135).	регион, обеспечить техническую поддержку и дообучение модели. Г Сформулировать бизнес-требования: какие именно дефекты нужно выявлять, с какой точностью, в каком формате выдавать отчёты. Д Разработать или доработать модель машинного обучения на основе собранных данных. Е Обучить сотрудников работе с новой системой и интегрировать её в существующие процессы (поручения дорожным службам). Ваша задача: Постройте правильную последовательность этапов жизненного цикла ИИ-проекта, записав буквы в нужном порядке. 2. В финансовый отдел администрации города поступил звонок от мужчины, представившегося сотрудником ФСБ. Он сообщил бухгалтеру о якобы выявленной попытке несанкционированного доступа к счетам администрации и потребовал срочно перевести бюджетные средства на «безопасный счёт» для их сохранности. Бухгалтер, испытывая стресс и доверие к «представителю власти», выполнил указания и перевёл деньги. Позже выяснилось, что счёт принадлежал мошенникам, а номер телефона, с которого звонили, был подменён. Этапы атаки (перемешаны) 1 Бухгалтер переводит денежные средства на указанный мошенниками счёт. 2 Злоумышленник представляется сотрудником ФСБ и сообщает о якобы выявленной угрозе (утечка данных,

		попытка взлома). 3 Мошенники собирают открытые данные об администрации, её сотрудниках, структуре, контрагентах (из сайта, соцсетей, открытых баз данных). 4 Злоумышленник оказывает психологическое давление: требует срочных действий, запрещает сообщать коллегам, угрожает ответственностью за разглашение «секретной операции». 5 Мошенники определяют конкретную цель (бухгалтера) и получают его номер телефона (из открытых источников, утечек или путём обзвона приёмной). | 6 Злоумышленник диктует реквизиты «безопасного счёта» и контролирует процесс перевода, оставаясь на связи. |
Задание комбинированного типа с выбором одного правильного ответа из предложенных и обоснованием выбора	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. 5. Записать аргументы, обосновывающие выбор ответа (например, 4 текст обоснования).	1. Администрация города заказала разработку системы компьютерного зрения для автоматического выявления незаконных свалок. Подрядчик обучил нейросеть на 50 000 фотографий из открытых баз данных (интернет-стоки, фотографии свалок в Европе). Во время тестирования система показала точность 98% и была принята в эксплуатацию. Однако после запуска в городскую среду система стала пропускать 40% реальных свалок и, наоборот, принимать за мусор тени от деревьев, лужи и свежеуложенный асфальт. Вопрос: Какова наиболее вероятная причина провала проекта? Предлагаемые варианты ответов: А. Подрядчик использовал устаревшую архитектуру нейросети, которая не подходит для задач компьютерного зрения. Б. Обучающая выборка данных не соответствовала реальным условиям применения (отличался ландшафт, освещение, типы мусора), что вызвало проблему дрейфа и нерепрезентативности

		данных. В. Городская администрация не закупила достаточно мощные серверы для обработки видео в реальном времени. Г. Программисты допустили ошибки в коде при интеграции нейросети в городскую систему видеонаблюдения. 2. В департамент имущественных отношений областной администрации поступил звонок. Звонивший представился сотрудником ФСБ Ивановым и сообщил секретарю, что в компьютерной системе департамента зафиксирована хакерская атака и происходит утечка данных. Для её нейтрализации необходимо срочно предоставить удалённый доступ к рабочему компьютеру начальника департамента. Звонивший говорил уверенно, использовал профессиональную терминологию, назвал реальные фамилии руководителей (взятые с официального сайта) и настаивал на немедленных действиях, угрожая уголовной ответственностью за сокрытие факта взлома. Секретарь, испугавшись, передала трубку начальнику департамента, который, находясь под давлением, продиктовал свои логин и пароль для удалённого доступа. Через неделю выяснилось, что с использованием этих данных были похищены документы по стратегическим объектам недвижимости, а на счета администрации были направлены поддельные платёжные поручения. Какая первичная и системная ошибка со стороны руководства и сотрудников департамента сделала возможной успешную реализацию данной социоинженерной атаки? А Отсутствие современного антивирусного программного обеспечения

		на рабочих компьютерах Б Нарушение секретарём инструкции по пропускному режиму (она не должна была соединять звонящего с руководителем) В Отсутствие в организации обязательной процедуры верификации любых запросов, связанных с доступом к информации или действиями с бюджетными средствами, по альтернативным каналам связи Г Начальник департамента не прошёл своевременно повышение квалификации по информационной безопасности Д Использование для удалённого доступа недостаточно сложных паролей
Задание открытого типа с развернутым ответом	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	Обоснуйте необходимость соблюдения принципа недискриминации при внедрении ИИ в государственные процессы. Определите границы ответственности разработчиков и пользователей ИИ-систем в государственном секторе.

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 студент демонстрирует знания, приобретенные на лекционных и семинарских занятиях, а также полученные посредством	30-39

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.	
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. 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*).

Для решения задач открытого типа (ПИЗ), тестовых заданий студенту разрешается использование 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.

7. Методические материалы по освоению дисциплины

К.М.01.ДЭ.01.01.06 Цифровая этика и безопасность в цифровой среде представляют собой одну из ведущих дисциплин по выбору в подготовке бакалавров, обучающихся по направлению 38.03.04. «Государственное и муниципальное управление». Изучение данного курса позволит будущему руководителю получить теоретические знания о этических аспектах применения цифровых технологий, дискриминационных угрозах применения ИИ-технологий, изучить опыт использования цифровых

технологий с точки зрения возможностей и рисков, уметь определять зоны повышенного риска, обеспечивать кибербезоасность. Для реализации данной цели необходимо внимательно ознакомиться со структурой и содержанием дисциплины, последовательно изучить его основные темы. Большое место при освоении дисциплины отводится самостоятельной работе по изучению современной отечественной и западной литературой. В первую очередь необходимо изучить основную литературу, затем — дополнительную. Именно знакомство с дополнительной литературой, часть которой существует в печатном, а часть – в электронном виде, способствует более глубокому освоению изучаемого материала. Для изучения основных вопросов образовательной программы необходимо конспектировать материалы лекций, работать с рекомендованной преподавателем литературой, а также ресурсами информационно-телекоммуникационной сети «Интернет». Для приобретения навыков активного использования знаний полезно обсуждать плановые и возникающие вопросы, а также решаемые задачи на практических занятиях. Чтобы легче и прочнее усвоить материал следует постоянно использовать конкретные примеры, сравнения из уже полученных областей наук. Для закрепления изученного материала даны вопросы по каждой теме дисциплины, на которые следует самостоятельно найти ответы. Важной составной частью учебного процесса в вузе являются практические занятия. Практические занятия проводятся главным образом по дисциплинам, требующим закрепления навыков решения задач, и помогают студентам глубже усвоить учебный материал, приобрести умения применять принципы системного подхода к решению разнообразных задач, определять и оценивать ресурсы и существующие ограничения разного рода проектов. При подготовке к практическим занятиям необходимо проанализировать конспект лекции, ознакомиться с рекомендованной литературой по соответствующей теме, осуществить подготовку по рекомендованным в рабочей программе вопросам для обсуждения темы, выполнить домашнее задание (при необходимости).
Необходимо помнить, что на лекции обычно рассматривается не весь материал, а только его часть. Остальная его часть восполняется в процессе самостоятельной работы. В связи с этим работа с рекомендованной литературой обязательна. Особое внимание при этом необходимо обратить на содержание основных положений и выводов, объяснение явлений и фактов, уяснение практического приложения рассматриваемых теоретических вопросов. В процессе этой работы студент должен стремиться понять и запомнить основные положения рассматриваемого материала, примеры, поясняющие его, а также разобраться в

иллюстративном материале. В процессе подготовки к занятиям рекомендуется взаимное обсуждение материала, во время которого закрепляются знания, а также приобретается практика в изложении и разъяснении полученных знаний, развивается речь. При необходимости следует обращаться за консультацией к преподавателю (в том числе по электронной почте). Планируя консультацию, необходимо хорошо продумать вопросы, которые требуют разъяснения. Заканчивать подготовку следует составлением плана (конспекта) по изучаемому материалу (вопросу). Это позволяет составить концентрированное, сжатое представление по изучаемым вопросам. Записи имеют первостепенное значение для самостоятельной работы студентов. Они помогают понять построение изучаемого материала, выделить основные положения, проследить их логику. Кроме того, ведение записей способствует превращению чтения в активный процесс, мобилизует, наряду со зрительной, и моторную память. Следует помнить: у студента, систематически ведущего записи, создается свой индивидуальный фонд методических материалов для быстрого повторения изученных вопросов, для мобилизации накопленных знаний. Особенно важны и полезны записи тогда, когда в них находят отражение мысли, возникшие при самостоятельной работе. После изучения базовых тем курса проводится текущий контроль знаний студентов в виде опроса или письменного тестирования. Типовые тесты и задания по темам дисциплины приведены в специальном разделе данной рабочей программы. Подготовка к текущему и промежуточному контролю предполагает изучение представленных вопросов к зачету, работу над тестами, представленными в данной рабочей программе, выполнение семестровой проектной работы по применению системного подхода и методов системного анализа к выбранной системе. Работа в малых группах – это одна из самых популярных форм проведения занятий, так как она дает всем обучающимся (в том числе и стеснительным) возможность участвовать в работе, практиковать навыки сотрудничества, межличностного общения (в частности, умение активно слушать, вырабатывать общее мнение, разрешать возникающие разногласия). Цель данной формы проведения занятий: продемонстрировать сходство или различия определенных явлений, выработать стратегию или разработать план, выяснить отношение различных групп участников к одному и тому же вопросу. В ходе этой работы дополнительно решаются следующие задача: развитие навыков общения и взаимодействия в группе, формирование ценностно-ориентационного единства группы, поощрение к гибкой смене социальных ролей в зависимости от ситуации. Группа студентов делится на

несколько малых групп. Количество групп определяется числом творческих заданий, которые будут обсуждаться в процессе занятия. Малые группы формируются либо по желанию студентов, либо по родственной тематике для обсуждения. Каждая малая группа обсуждает творческое задание в течение отведенного времени. Основной этап – проведение обсуждения творческого задания. Заслушиваются суждения, предлагаемые каждой малой группой по творческому заданию. Преподаватель дает оценочное суждение и работе малых групп, по решению творческих заданий, и эффективности предложенных путей решения.

Учебно-методическое обеспечение самостоятельной работы

Наименование темы или раздела дисциплины	**Вопросы для самопроверки**
Тема 1. Этические вызовы цифровой трансформации государственного управления	1. Этические дилеммы, возникающие в процессе цифровой трансформации 2. Гуманитарные угрозы связанные с использованием цифровых технологий и ии-технологий в госуправлении
Тема 2. Информационная безопасность в органах государственной власти	1. Охарактеризуйте роль модели триады C-I-A «конфиденциальность—целостность—доступность» в обеспечении информационной безопасности. 2. Какие существуют методы технических средств защиты данных в органах власти? 3. Приведите классификацию социоинженерных атакк 4. Какие рекомендации следует учитывать для повышения уровня цифрового доверия граждан к государству с учетом социоинженерных атак
Тема 3. Этика применения ИИ-технологий в государственном секторе	Анализ этического регулирования применения ИИ-технологий в российской и зарубежной практике
Тема 4. Цифровая	1. Что включает в себя понятие интеллектуальной

этика руководителя в государственном секторе	собственности в цифровой среде и какое отношение оно имеет к руководителям государственного сектора? 2. Почему важна забота о своей цифровой репутации и каким образом государственный служащий должен управлять своим цифровым профилем? 3. О каком понятии идет речь, когда говорят о «цифровом следе» государственного служащего? 4. Что понимается под термином «цифровая гигиена» и как она связана с работой государственных чиновников?

8. Учебная литература и ресурсы информационно-телекоммуникационной сети Интернет

8.1. Основная литература

1. Современная этика - Канке В.А. - НИЦ ИНФРА-М - 2021 - https://znanium.com/catalog/product/975126 - 1042344 - ZNANIUM

2. Энтин, В. Л. Авторское право в виртуальной реальности (новые возможности и вызовы цифровой эпохи): Научное / Энтин В.Л. - М.:Статут, 2017. - 216 с.: ISBN 978-5-8354-1305-8. - Текст : электронный. - URL: https://znanium.com/catalog/product/1013817

3. Гаспарян Д.Э. Прикладные проблемы внедрения этики искусственного интеллекта в России. Отраслевой анализ и судебная система : монография / Д. Э. Гаспарян, Е.М. Стырин — 2-ое изд., перераб. и доп. — Москва : Издательский дом ВШЭ, 2021. — 112 с. — (Высшее образование). — ISBN 978-5-7598-2351-3. — Текст : электронный // Научная электронная библиотека Elibrary: [сайт]. — URL: https://www.elibrary.ru/item.asp?id=45615180 (дата обращения: 20.02.2026)
4. Быльева Д.С. Этика искусственного интеллекта: практикум : учебное пособие / Д. С. Быльева, В. В. Лобатюк. — Санкт-Петербург : ПОЛИТЕХ-ПРЕСС (СПбПУ), 2023. — 82 с. — (Высшее образование). - ISBN 978-5-7422-8469-7. — Текст : электронный // ПОЛИТЕХ Электронная библиотека [сайт]. — URL: https://elib.spbstu.ru/dl/2/i24-12.pdf/info (дата обращения: 20.02.2026).
5. Формирование цифрового доверия в рамках социоинженерных атак : монография / А. А. Азаров, Е. И .Кузнецова, А. А. Матвеев [и др.] ; отв. ред. Е. И. Кузнецова. – Санкт-Петербург : ИПЦ СЗИУ РАНХиГС, 2025. - 178 с. – ISBN 978-5-89781-882-2. - Текст : электронный. - URL: https://znanium.ru/catalog/product/2238890 (дата обращения: 20.02.2026).

8.2. Дополнительная литература

8. Калинин Д.М. Этика и доверие: границы применения генеративного ИИ в государственных решениях : научная статья / Д. М. Калинин, М. М. Мчедловафыв // Вестник Национального института бизнеса. Выпуск №2 (58)/2025 / Москва : Вестник НИБ, 2025. — С. 275-298. — Текст : электронный. —URL: https://nibmoscow.ru/varhiv/ (дата обращения: 20.02.26)

9. Алферова Е.В. Искусственный интеллект в государственном управлении: правовой потенциал и риски применения / Е. В. Алферова. // Социальные и гуманитарные науки. Отечественная и зарубежная литература. Сер. 4, Государство и право / Москва : ИНИОН РАН, 2025. — Текст : электронный. — URL: https://inion-journalaw.ru/issue.php?id=33 (дата обращения: 20.02.26)
10. *Кодекс этики в сфере применения ИИ-технологий* - *https://a-ai.ru/* (дата обращения: 20.02.2026).

8.3. Нормативные правовые документы и иная правовая информация

Законы Российской Федерации

- Федеральный закон РФ от 23.08.1996 № 127-ФЗ «О науке и государственной научно-технической политике»
- Федеральный закон РФ от 04.08.2023 № 478-ФЗ «О развитии технологических компаний в Российской Федерации»
- Федеральный закон от 28 декабря 2024 г. № 523-ФЗ «О технологической политике в Российской Федерации и о внесении изменений в отдельные законодательные акты Российской Федерации»
- Федеральный закон от 31 июля 2020 г. № 258-ФЗ «Об экспериментальных правовых режимах в сфере цифровых инноваций в Российской Федерации»
- Федеральный закон от 26.07.2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации»
- 149-ФЗ «Об информации, информационных технологиях и о защите информации»
- Федеральный закон "Об информации, информационных технологиях и о защите информации" от 27.07.2006 N 149-ФЗ (последняя редакция)
- Федеральный закон "Об электронной подписи" от 06.04.2011 N 63-ФЗ (последняя редакция)
- Федеральный закон "О персональных данных" от 27.07.2006 N 152-ФЗ (последняя редакция)

Указы Президента Российской Федерации

- Указ Президента РФ от 18.06.2024 № 529 «Об утверждении приоритетных направлений научно-технологического развития и перечня важнейших наукоемких технологий»
- Указ Президента РФ от 07.07.2011 № 899 «Об утверждении приоритетных направлений развития науки, технологий и техники в Российской Федерации и перечня критических технологий Российской Федерации»
- Указ Президента РФ от 28.02.2024 № 145 «О Стратегии научно-технологического развития Российской Федерации»
- Указ Президента РФ от 07.05.2024 № 309 «О национальных целях развития Российской Федерации на период до 2030 года и на перспективу до 2036 года»
- Указ Президента РФ от 10 октября 2019 г. N 490 "О развитии искусственного интеллекта в Российской Федерации" (с изменениями и дополнениями)

Иные документы:

- Доктрина информационной безопасности Российской Федерации *(утверждена Указом Президента РФ № 646 от 5 декабря 2016 г.)*
- Федеральный закон «Об информации, информационных технологиях и о защите информации» от 27.07.2006 N 149-ФЗ // https://www.consultant.ru/document/cons_doc_LAW_61798/, 16.09.2024.
  Федеральный закон «О безопасности критической информационной инфраструктуры Российской Федерации» от 26.07.2017 N 187-ФЗ // https://www.consultant.ru/document/cons_doc_LAW_220885/ , 16.09.2024.
- Федеральный проект «Информационная безопасность» // https://digital.gov.ru/ru/activity/directions/874/#section-materials, 1.09.2024.

- Национальный проект «Экономика данных и цифровая трансформация государства» на 2025–2030 годы
- ГОСТ Р ИСО/МЭК 20547-3-2024 "Информационные технологии. Эталонная архитектура больших данных. Часть 3. Эталонная архитектура";
- ГОСТ Р ИСО/МЭК 24029-2-2024 "Искусственный интеллект. Оценка робастности нейронных сетей. Часть 2. Методология использования формальных методов";
- ГОСТ Р 71476-2024 (ИСО/МЭК 22989:2022) "Искусственный интеллект. Концепции и терминология искусственного интеллекта".Также вводятся стандарты, закрепленные за техническим

комитетом по стандартизации № 053 "Основные нормы и правила по обеспечению единства измерений" (ТК 053).

- ГОСТ Р 58776-2019 «Средства мониторинга поведения и прогнозирования намерений людей. Термины и определения» — стандарт описывает основные характеристики алгоритмов ИИ, унифицирует терминологию с общемировой практикой и является своего рода фундаментом для методологически грамотного развития систем распознавания девиантного поведения.

8.4 Интернет-ресурсы

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

Русскоязычные ресурсы

1. Электронные учебники электронно-библиотечной системы (ЭБС) «Айбукс» http://www.nwapa.spb.ru/index.php?page_id=76
2. Научно-практические статьи по экономики и и менеджменту Издательского дома «Библиотека Гребенникова» http://www.nwapa.spb.ru/index.php?page_id=76
3. Статьи из журналов и статистических изданий Ист Вью http://www.nwapa.spb.ru/index.php?page_id=76

Англоязычные ресурсы

4. EBSCO Publishing- доступ к мультидисциплинарным полнотекстовым базам данных различных мировых издательств по бизнесу, экономике, финансам, бухгалтерскому учету, гуманитарным и естественным областям знаний, рефератам и полным текстам публикаций из научных и научно – популярных журналов.
5. Emerald – крупнейшее мировое издательство, специализирующееся на электронных журналах и базах данных по экономике и менеджменту. Имеет статус основного источника профессиональной информации для преподавателей, исследователей и специалистов в области менеджмента.

Иные источники

Электронно-библиотечная система ЭБС «Айбукс» (электронные учебники) доступна по адресу http://www.ibooks.ru с любого компьютера СЗИУ без регистрации;

электронная библиотека ИД «Гребенников» (научно-практические статьи по маркетингу, рекламе, менеджменту, логистике, финансам и

управлению персоналом) доступна со всех компьютеров СЗИУ по адресу http://grebennikon.ru.

Доступ в систему ИНТЕГРУМ (российские газеты, журналы, статистика, адресно-справочные и правовые базы данных, информация РОСПАТЕНТа и ГОСКОМСТАТа).

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

№ п/п	Наименование
1.	Специализированные залы для проведения лекций.
2.	Специализированная мебель и оргсредства: аудитории и компьютерные классы, оборудованные посадочными местами (в том числе для проведения занятий лабораторного типа).
3.	Технические средства обучения: Многофункциональный мультимедийный комплекс в лекционной аудитории; звуковые динамики; программные средства, обеспечивающие просмотр видеофайлов.
4.	Персональные компьютеры с доступом к электронному каталогу, полнотекстовым базам, подписным ресурсам и базам данных научной библиотеки СЗИУ РАНХиГС.
5.	Технические средства обучения: Персональные компьютеры; компьютерные проекторы; звуковые динамики; программные средства, обеспечивающие просмотр видеофайлов в форматах AVI, MPEG-4, DivX, RMVB, WMV.