

Документ подписан простой электронной подписью
Информация о владельце:
ФИО: Андрей Драгомирович Хлутков
Должность: директор
Дата подписания: 16.06.2026 21:27:41
Уникальный программный ключ:
880f7c07c583b07b775f6604a630281b13ca9fd2

Приложение 4
к образовательной программе

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Б1.В.ДЭ.02.02 «Управление цифровыми рисками»

(индекс, наименование дисциплины в соответствии с учебным планом)

38.04.04 Государственное и муниципальное управление

(код, наименование направления подготовки)

Цифровая трансформация в публичном управлении

(наименование образовательной программы)

заочная

(форма обучения)

Год набора-2026

Санкт-Петербург

Автор(ы)-составитель(и) РПД:

Медведева Надежда Васильевна, к.эконом.н., 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 Б1.В.ДЭ.02.02 «Управление цифровыми рисками» на заседании кафедры Государственного и муниципального управления факультета государственного и муниципального управления СЗИУ РАНХиГС.

Протокол № 3 от 26 марта 2026 г.

СОДЕРЖАНИЕ

1. Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения образовательной программы
2. Объем и место дисциплины в структуре образовательной программы
3. Содержание и структура дисциплины
4. Типы оценочных материалов, показатели и критерии их оценивания
5. Формы аттестации, типовые оценочные материалы для текущего контроля успеваемости обучающихся, критерии и шкалы оценивания по контрольным точкам
6. Формы промежуточной аттестации, критерии и шкала оценивания, типовые оценочные материалы по дисциплине
7. Методические материалы по освоению дисциплины
8. Учебная литература и ресурсы информационно-телекоммуникационной сети «Интернет»
9. Материально-техническая база, информационные технологии, программное обеспечение и информационные справочные системы

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

Дисциплина Б1.В.ДЭ.02.02 «Управление цифровыми рисками» обеспечивает формирование у обучающихся следующих профессиональных компетенций*:

ОТФ/ТФ и реквизиты ПС <i>(при наличии)</i>	Код компетенции	Наименование компетенции	Код индикатора достижения компетенций	Наименование индикатора достижения компетенций	Образовательный результат
06.014 Менеджер по информационным технологиям, утв. приказом Минтруда России от 30.08.2021 № 588н С/01.7 Управление стратегией развития ИТ-сервисов	ПКс-1	Способен участвовать в осуществлении стратегического управления в интересах общества и государства, включая постановку общественно значимых целей, формирование условий их достижения, организацию работы для получения максимально возможных результатов, организацию взаимодействия с внешней средой (другими государственными и муниципальными органами, организациями, гражданами) в данной деятельности	ПКс-1.2	Осуществляет постановку целей, формирование условий их достижения, организацию работы для получения максимально возможных результатов, организацию взаимодействия с внешней средой	ПКс-1.2. 3-1. Знает международные и отечественные стандарты, лучшие практики и фреймворки по разработке и реализации цифровой стратегии организации (региона, страны). ПКс-1.2. У-2. Умеет организовывать деятельность по разработке и выполнению цифровой стратегии организации (региона, страны).
D/03.8 Управление дорожной картой инновационной деятельности по	ПКс-3	Способен обеспечивать динамичное изменение организации (страны, региона, отрасли) путем	ПКс-3.2	Учитывает политические, социальные, экономические, экологические проблемы и использует	ПКс-3.2. 3-2. Знает организацию взаимодействия с широким кругом стейкхолдеров по вопросам цифровой трансформации. ПКс-3.2. У-3. Умеет повышать вовлеченность

цифровой трансформации		внедрения цифровых технологий, в том числе через составление прогнозов и динамичных дорожных карт инновационной деятельности по цифровой трансформации (с учетом имеющихся политических, социальных, экономических, экологических проблем) с использованием проектных методов		проектные методы при составлении прогнозов и дорожных карт по цифровой трансформации	широкого круга стейкхолдеров в цифровую трансформацию.
------------------------	--	---	--	--	--

** Дисциплина может формировать компетенцию полностью или частично.*

***Должно соответствовать Приложению 1 к образовательной программе*

2. Объем и место дисциплины в структуре образовательной программы

Общий объем дисциплины: 4,00 з.е., 144 ак. час.

Объем академических часов, выделенных на контактную работу обучающихся с преподавателем, 18 ак. час, из них 4 ак.час на лекции и 12 ак.час на практические занятия, 2 ак.час. на консультацию; 122 ак. час на самостоятельную работу обучающихся; 4 ак.час. на контроль.

Дисциплина Б1.В.ДЭ.02.02 «Управление цифровыми рисками» относится к профессиональному базису части, формируемой участниками образовательных отношений, и реализуется на 2-ом курсе заочной формы обучения после изучения дисциплин:

- Б1.О.02 Теория и механизмы современного государственного управления;
- Б1.О.03 Информационно-аналитические технологии государственного и муниципального управления;
- Б1. В.01 Развитие информационного общества: цифровая экономика.

3. Содержание и структура дисциплины

3.1. Структура дисциплины

Заочная форма обучения

№ п/п	Наименование тем и (или) разделов	ВСЕ ГО	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	К о н т р о л ь	СРкр		СРэк
Л	ВЛ	ЛР	ПЗ											
Тема 1.	Введение в управление рисками	28	1			2							25	Доклад, Тестирование
Тема 2.	Целеполагание и идентификация рисков	28	1			2							25	Опрос Тестирование, Контрольное задание
Тема 3.	Зоны рисков цифровой трансформации	30	1			4							25	Тестирование, Контрольное задание

Тема 4.	Риски применения сквозных цифровых технологий в публичном управлении	27				2						25	Тестирование, Контрольное задание
Тема 5.	Стратегии, методы, инструменты управления рисками	25	1			2						22	Тестирование, Контрольное задание
Промежуточная аттестация													Зачет с оценкой
Итого		144	4			12			2	4		122	

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 управление рисками ПКс-1.2. ПКс-3.2.

Понятие риска в контексте публичного управления: определение, сущность, компоненты (неопределённость, вероятность, последствия). Эволюция подходов к управлению рисками: от реактивного к проактивному управлению. Специфика цифровых рисков: отличие от традиционных рисков, повышенная динамика и взаимосвязанность. Основные виды цифровых рисков в публичном управлении: киберриски (утечки данных, кибератаки); риски автоматизации (сбои в работе систем, ошибки алгоритмов); репутационные риски (публичное восприятие цифровых инициатив); правовые риски (несоответствие нормативным требованиям). Роль управления рисками в цифровой трансформации органов публичной власти. Международные стандарты управления рисками (ISO 31000, COBIT) и их адаптация для системы публичного управления.

Тема 2. Целеполагание и идентификация рисков ПКс-1.2. ПКс-3.2.

Постановка целей управления рисками с учётом стратегии цифровой трансформации органа публичной власти. Принципы SMART при формулировании целей риск-менеджмента. Методы идентификации рисков: мозговой штурм с участием экспертов; анализ исторических данных о сбоях и инцидентах; чек-листы типовых цифровых рисков; SWOT-анализ цифровой инфраструктуры; метод Дельфи для экспертных оценок. Инструменты сбора информации: опросы сотрудников, анализ обращений граждан, мониторинг СМИ и соцсетей. Документирование выявленных рисков: реестр рисков, матрица рисков. Приоритизация рисков по критериям вероятности и воздействия.

Тема 3. Зоны рисков цифровой трансформации ПКс-3.2.

Понятие зоны риска цифровой трансформации: определение: зона риска — область деятельности органа публичной власти, где внедрение цифровых технологий создаёт новые уязвимости; отличие от видов рисков: зона — это «где?», вид — это «что?»; примеры: зона госуслуг, зона межведомственного взаимодействия, зона закупок ИТ. Зона стратегического планирования и целеполагания: риски неправильной постановки целей цифровой трансформации; несоответствие стратегии реальным возможностям органа публичной власти; отсутствие чётких KPI для оценки результатов. Зона ИТ-инфраструктуры и эксплуатации систем: несовместимость новых решений с унаследованными системами; сбои в

работе цифровых платформ (порталы госуслуг, СЭД); зависимость от облачных провайдеров; проблемы масштабирования пилотных проектов. Зона обработки и защиты данных: утечки персональных данных граждан; нарушение требований федерального закона «О персональных данных» и федерального закона «О безопасности критической информационной инфраструктуры Российской Федерации»; уязвимости в API и мобильных приложениях; недостаточная защита Big Data-хранилищ. Зона взаимодействия с гражданами и обществом: цифровое неравенство (доступ для пожилых, сельских жителей); низкий уровень доверия к цифровым сервисам; этические проблемы использования ИИ (профайлинг, дискриминация); рост социальной напряжённости из-за автоматизации. Зона управления персоналом и организационной культуры: сопротивление изменениям со стороны сотрудников; дефицит квалифицированных ИТ-специалистов; необходимость переобучения большого числа государственных и муниципальных служащих; изменение должностных обязанностей из-за внедрения ИИ. Другие зоны рисков цифровой трансформации. Методы идентификации зон рисков. Инструменты минимизации рисков по зонам.

Тема 4. Риски применения сквозных цифровых технологий в публичном управлении ПКс-3.2.

Классификация сквозных технологий и их риски: Большие данные (Big Data): утечки, предвзятость алгоритмов, нарушение конфиденциальности. Искусственный интеллект: непрозрачность решений, дискриминация, ошибки распознавания. Блокчейн: масштабируемость, энергопотребление, юридические пробелы. Интернет вещей (IoT): уязвимости устройств, перехват данных. Облачные вычисления: зависимость от провайдера, трансграничная передача данных. Правовые ограничения: федеральный закон «О персональных данных», федеральный закон «О безопасности критической информационной инфраструктуры Российской Федерации». Этические аспекты: баланс между безопасностью и приватностью граждан. Сценарии реализации рисков: сбой системы распознавания лиц в полиции; утечка медицинских данных из единой базы; атака на «умные» системы ЖКХ. Международный опыт регулирования цифровых технологий в управлении.

Тема 5. Стратегии, методы, инструменты управления рисками ПКс-1.2. ПКс-3.2.

Стратегии реагирования на риски: избегание (отказ от высокорисковых технологий); снижение (внедрение защитных мер); передача (страхование киберрисков); принятие (резервирование бюджета на ликвидацию последствий). Методы количественной оценки: VaR для финансовых потерь; FMEA (анализ видов и последствий отказов). Методы качественной оценки: матрица рисков 5×5 ; сценарный анализ («что если»). Цифровые инструменты: SIEM-системы (мониторинг событий информационной безопасности); платформы киберразведки; дашборды для визуализации рисков. Нормативные механизмы: регламенты информационной безопасности, политики доступа, планы реагирования на инциденты. Культура риск-менеджмента: обучение персонала, регулярные учения.

4. Типы оценочных материалов, показатели и критерии оценивания

4.1. Оценочные материалы по дисциплине Б1.В.ДЭ.02.02 «Управление цифровыми рисками» 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	<ol style="list-style-type: none"> 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	<ol style="list-style-type: none"> 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

<p>Задание закрытого типа с выбором нескольких правильных ответов из нескольких вариантов предложенных</p>	<p>Прочитайте текст, выберите правильные ответы</p>	<ol style="list-style-type: none"> 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). 	<p>Ответ считается верным, если правильно установлены все соответствия (позиции из одного столбца верно сопоставлены с позициями другого)</p>
<p>Задание закрытого типа на установление последовательности</p>	<p>Прочитайте текст и установите последовательность</p>	<ol style="list-style-type: none"> 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). 	<p>Ответ считается верным, если правильно указана вся последовательность цифр</p>
<p>Задание комбинированного типа с выбором одного правильного ответа из</p>	<p>Прочитайте текст, выберите правильный ответ и запишите аргументы,</p>	<ol style="list-style-type: none"> 1. Внимательно прочитать текст задания и понять, что в качестве ответа ожидается только один из предложенных вариантов. 2. Внимательно прочитать предложенные варианты ответа. 	<p>Ответ считается верным, если правильно указана цифра или буква и приведены корректные аргументы, используемые при выборе ответа</p>

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

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.ДЭ.02.02 «Управление цифровыми рисками» используются следующие формы текущего контроля успеваемости обучающихся (в том числе, задания к контрольным точкам):

доклад, опрос, тестирование, контрольное задание.

5.2. Типовые оценочные материалы для текущего контроля успеваемости обучающихся:

Тема 1. Введение в управление рисками

Темы для докладов:

1. Эволюция подходов к управлению рисками: от реактивного к проактивному управлению в публичном секторе.
2. Специфика цифровых рисков в системе государственного управления: отличия от традиционных рисков.
3. Организационные риски цифровой трансформации органов публичной власти: сопротивление изменениям, нехватка компетенций, слабая межведомственная координация.
4. Репутационные риски цифровых инициатив: кейсы запусков государственных сервисов.
5. Правовые риски цифровой трансформации: соответствие федерального закона «О персональных данных» и федерального закона «О безопасности критической информационной инфраструктуры Российской Федерации».
6. Применение международного стандарта ISO 31000 и его российских аналогов в управлении рисками органов публичной власти.
7. Технологические риски внедрения цифровых решений в публичном управлении: зависимость от вендоров, устаревание технологий, проблемы совместимости систем.

Тестирование:

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.

В чём ключевое отличие проактивного подхода к управлению рисками от реактивного в контексте цифровой трансформации органов публичной власти?

А) проактивный подход требует больших финансовых затрат, а реактивный реализуется за счёт текущих бюджетов без дополнительного финансирования;

Б) проактивный подход фокусируется на прогнозировании и предотвращении рисков до их реализации, а реактивный — на устранении последствий уже произошедших инцидентов;

В) проактивный подход применяется только в коммерческих организациях, а реактивный — в государственных структурах;

Г) проактивный подход исключает любые риски, а реактивный предполагает их сознательное принятие.

Какой из перечисленных методов наиболее эффективен для идентификации цифровых рисков на этапе планирования внедрения новой информационной системы в муниципалитете?

А) проведение анонимного опроса граждан о предполагаемых неудобствах от новой системы;

Б) анализ исторических данных о сбоях в аналогичных системах других регионов с учётом специфики местного контекста и потенциальных угроз;

В) назначение ответственного сотрудника, который единолично определит все возможные риски;

Г) игнорирование потенциальных рисков на основании успешного опыта внедрения в коммерческих компаниях.

Вы руководитель отдела цифровизации регионального правительства. При внедрении платформы электронного документооборота выявлен риск утечки персональных данных из-за недостаточной защиты API. Какая стратегия управления рисками будет наиболее рациональной в данной ситуации?

А) полностью отказаться от внедрения платформы и продолжить использовать бумажный документооборот;

Б) передать ответственность за защиту данных подрядчику (на аутсорсинг) без дополнительного контроля;

В) внедрить дополнительные меры защиты API (шифрование, аутентификация), провести аудит безопасности и обучение сотрудников, сохранив внедрение платформы;

Г) принять риск без каких-либо действий, сославшись на низкую вероятность инцидента.

Какая комбинация показателей KPI наиболее объективно отражает эффективность системы управления рисками в органе публичной власти, реализующем цифровую трансформацию?

А) количество проведённых совещаний по рискам и объём бюджета, выделенного на кибербезопасность;

Б) доля рисков с реализованными мерами реагирования и снижение частоты инцидентов за отчётный период;

В) число обученных сотрудников и количество опубликованных нормативных актов по информационной безопасности;

Г) количество установленных камер видеонаблюдения и число зафиксированных нарушений.

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 выбранных вариантов ответа.

Какие из перечисленных характеристик относятся к специфике цифровых рисков в системе публичного управления?

А) высокая динамика изменений: цифровые риски быстро эволюционируют под влиянием новых технологий;

Б) взаимосвязанность и каскадный эффект: сбой в одной системе может затронуть смежные сервисы;

В) зависимость от человеческого фактора: ошибки персонала и инсайдерские угрозы усиливают риски;

Г) стабильность и предсказуемость: цифровые риски легко прогнозировать на долгосрочную перспективу;

Д) изолированность: цифровые риски не влияют на традиционные процессы управления.

Какие роли участвуют в процессе управления рисками в органе публичной власти?

А) руководитель органа власти — утверждает стратегию управления рисками и выделяет ресурсы;

Б) менеджер по рискам — координирует процесс, ведёт реестр рисков, организует мониторинг;

В) рядовой сотрудник отдела кадров — единолично принимает решения по реагированию на все выявленные риски;

Г) эксперты подразделений — идентифицируют и оценивают отраслевые риски в своей зоне ответственности;

Д) представитель подрядной организации — полностью берёт на себя управление всеми рисками проекта без участия органа публичной власти.

Какие показатели КРІ наиболее объективно отражают эффективность системы управления рисками в органе публичной власти, реализующем цифровую трансформацию?

А) доля рисков с реализованными мерами реагирования (например, 80% выявленных рисков имеют план снижения);

Б) снижение частоты и тяжести инцидентов за отчётный период (например, на 30% меньше сбоев в работе систем);

В) количество проведённых совещаний по рискам за квартал;

Г) время реагирования на инциденты (например, среднее время локализации кибератаки — не более 2 часов);

Д) объём бюджета, выделенного на кибербезопасность, без привязки к результатам.

Тест 3.

Внимательно прочитать текст задания и понять, что в качестве ответа ожидается последовательность элементов.

Внимательно прочитать предложенные варианты ответа.

Построить верную последовательность из предложенных элементов.

Записать буквы (в зависимости от задания) вариантов ответа в нужной последовательности.

Установите правильную последовательность этапов цикла управления рисками в органе публичной власти, реализующем цифровую трансформацию.

А) мониторинг и пересмотр реестра рисков.

Б) выбор стратегии реагирования на риски (избежание, снижение, передача, принятие).

В) качественная и количественная оценка выявленных рисков (по критериям вероятности и воздействия).

Г) идентификация рисков с использованием методов: мозговой штурм, анализ исторических данных, чек-листы.

Д) реализация мер по снижению рисков и документирование результатов.

Тема 2. Целеполагание и идентификация рисков

Вопросы для опроса:

1. Раскройте принципы SMART в определении измеримых целей управления рисками в органе публичной власти. Приведите конкретный пример цели цифровой трансформации, соответствующей этим принципам.

2. Назовите специфические цифровые риски, ограничивающие достижение стратегических целей цифровой трансформации муниципалитета (например, по внедрению электронного документооборота). Назовите 2–3 риска и кратко поясните связь каждого с конкретной целью.

3. Опишите, как метод Дельфи может быть применён для идентификации рисков при планировании новой информационной системы и охарактеризуйте его преимущество перед обычным мозговым штурмом в деятельности органа публичной власти.

4. Раскройте процесс анализа рисков запуска портала госуслуг и назовите используемые источники данных для идентификации потенциальных угроз. Перечислите минимум 3 источника и укажите, какую информацию по рискам можно из них извлечь.

5. Охарактеризуйте понятие «триггер риска» в управлении рисками органа публичной власти. Приведите 2–3 примера триггеров для следующих типов рисков: кибератаки, сбой в работе системы, сопротивление персонала внедрению новой платформы.

6. Раскройте порядок определения «владельца риска» для угрозы утечки персональных данных в муниципальной информационной системе. Укажите кто может им быть (конкретная должность/подразделение) и какие обязанности на него возлагаются.

7. Раскройте отличия качественной оценки вероятности риска (низкая/средняя/высокая) от количественной (в процентах или баллах). Назовите ситуации для органа публичной власти, в которых предпочтительнее использовать каждый из подходов.

8. Постройте фрагмент матрицы рисков (вероятность × воздействие) для трех выявленных рисков внедрения ИИ-системы в региональном правительстве. Для каждого риска укажите: краткое описание, оценку вероятности (качественная или количественная), оценку воздействия (высокая/средняя/низкая) и итоговый приоритет (критический/высокий/средний/низкий).

9. Опишите факторы, которые могут привести к недооценке воздействия риска при анализе цифровой инициативы в органе публичной власти. Приведите 2–3 фактора и поясните, как они искажают реальную картину (например, неучёт репутационных потерь или каскадного эффекта).

10. Опишите инструменты автоматизации (ПО, платформы, сервисы), которые могут облегчить процесс идентификации и оценки цифровых рисков в органе публичной власти. Назовите 2–3 инструмента и укажите, какие задачи риск-менеджмента они помогают решить (сбор данных, визуализация, прогнозирование и т.д.).

Тестирование:

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.

Какой метод идентификации рисков предполагает анонимный сбор и обработку экспертных оценок в несколько раундов для достижения консенсуса?

- А) мозговой штурм;
- Б) метод Дельфи;
- В) SWOT-анализ;
- Г) анализ чек-листов.

Что такое «триггер риска» в контексте управления рисками органа публичного управления?

- А) конечный результат реализации риска, приводящий к ущербу;
- Б) ранний признак или симптом, сигнализирующий о начале реализации риска;
- В) стратегия реагирования на риск (избежание, снижение и т. д.);
- Г) документ, фиксирующий выявленный риск в реестре.

Какой инструмент позволяет визуализировать риски по двум критериям — вероятности и воздействия — для определения приоритетов реагирования?

- А) реестр рисков;
- Б) план реагирования на инциденты;
- В) матрица рисков;
- Г) отчёт о статусе управления рисками.

Какая шкала оценки вероятности риска чаще всего используется на этапе первичной идентификации в органах публичной власти, когда точные данные отсутствуют?

- А) количественная (в процентах: 10%, 30%, 70%);
- Б) денежная (в рублях потенциального ущерба);
- В) качественная (низкая/средняя/высокая);
- Г) временная (в днях до реализации риска).

Какое действие выполняется первым в цикле управления рисками при запуске цифровой инициативы в органе публичной власти?

- А) выбор стратегии реагирования;
- Б) идентификация рисков;
- В) мониторинг и пересмотр реестра рисков;

Г) реализация мер по снижению рисков.

Контрольные задания:

Задание 1.

Региональное министерство здравоохранения планирует внедрить единую информационную систему учёта пациентов для всех поликлиник области. На этапе планирования рабочая группа должна сформулировать измеримые цели внедрения и идентифицировать ключевые риски, способные помешать их достижению.

Сформулируйте 3 измеримые цели внедрения ЕИС, соответствующие принципам SMART.

Идентифицируйте 3–4 ключевых риска, которые могут помешать достижению этих целей. Для каждого риска укажите его причину и триггер (ранний признак реализации).

Задание 2.

Муниципалитет запускает портал обратной связи с гражданами для сбора предложений по благоустройству города. Команда проекта должна провести первичную идентификацию и оценку рисков.

Используя метод мозгового штурма, перечислите 4 потенциальных риска проекта.

Для каждого риска оцените вероятность (низкая/средняя/высокая) и воздействие (низкое/среднее/высокое).

Постройте фрагмент матрицы рисков (4×4), разместите в ней выявленные риски и определите их приоритет (высокий/средний/низкий).

Тема 3. Зоны рисков цифровой трансформации ПКс-3.2.

Тестирование:

Тест 1. Установите соответствие между термином, приводимым в столбце слева, и высказыванием (или определением) из правого столбца (*между зоной рисков цифровой трансформации и характерным для нее риском*): к каждой позиции, данной в левом столбце, подберите соответствующую позицию из правого столбца.

1	Зона ИТ-инфраструктуры и эксплуатации систем	А	Утечка персональных данных из-за недостаточной защиты API.
2	Зона обработки и	Б	Сбой в работе портала госуслуг из-за

	защиты данных		перегрузки серверов.
3	Зона закупок и взаимодействия с подрядчиками	В	Затягивание сроков внедрения по причине формальных правил государственных и муниципальных закупок.
4	Зона управления персоналом и организационной культуры	Г	Сопrotивление сотрудников внедрению новой системы электронного документооборота.

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 в таблицу (например, 1/А или 4/Б):

1	2	3	4

Контрольные задания:

Задание 1.

Администрация города запускает систему «Умный транспорт» для мониторинга и управления городским автобусным парком: установка GPS-трекеров, интеграция с картами пробок, мобильное приложение для пассажиров. На этапе планирования рабочая группа должна проанализировать зоны рисков.

Выделите 3 ключевые зоны рисков для этого проекта (из перечня зон темы 3).

Для каждой зоны укажите 2 характерных риска и их возможные последствия для муниципалитета.

Предложите по 1 инструменту минимизации для каждой зоны.

Задание 2.

Региональное министерство образования внедряет единую цифровую платформу для школ: электронный журнал, система отчётности, личный кабинет учителя и родителя. При анализе рисков команда выделила зону нормативного регулирования как приоритетную.

Укажите 3 риска в зоне нормативного регулирования для этого проекта.

Для каждого риска определите триггер (ранний признак реализации).

Предложите стратегию реагирования на каждый риск и кратко обоснуйте выбор.

Тема 4. Риски применения сквозных цифровых технологий в публичном управлении

Тестирование:

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.

Какая мера наиболее эффективна для минимизации риска утечки персональных данных при использовании Big Data в системе публичного управления?

- А) увеличение числа сотрудников, имеющих доступ к данным;
- Б) анонимизация и псевдонимизация данных перед анализом;
- В) хранение всех данных в одном централизованном хранилище;
- Г) отказ от использования внешних источников данных.

Какой триггер может сигнализировать о реализации риска взлома IoT-инфраструктуры «Умного города»?

- А) увеличение количества обращений в техподдержку по вопросам ЖКХ;
- Б) аномальный трафик на серверах, к которым подключены датчики;
- В) рост числа пользователей мобильного приложения муниципалитета;
- Г) задержка публикации годового отчёта администрации.

Какой риск является ключевым при переходе органа публичной власти на облачную платформу для документооборота?

- А) риск снижения мотивации сотрудников;
- Б) риск прекращения услуг провайдера из-за санкций или банкротства;
- В) риск увеличения количества бумажных документов;
- Г) риск изменения цветовой схемы интерфейса СЭД.

Какой инструмент минимизации рисков наиболее эффективен для предотвращения сбоев в работе ИИ-системы распределения соцвыплат?

- А) запрет на обжалование решений системы гражданами.
- Б) поэтапное внедрение с пилотным тестированием на ограниченной группе получателей.
- В) увеличение размера выплат для компенсации возможных ошибок.
- Г) замена ИИ-системы на традиционные методы расчёта.

Какой риск наиболее специфичен для применения искусственного интеллекта в системе публичного управления?

- А) перерасход бюджета на закупку оборудования;
- Б) предвзятость алгоритмов, приводящая к дискриминации отдельных групп граждан;
- В) сбой в работе системы из-за отключения электроэнергии;
- Г) утечка данных из-за человеческого фактора.

Задания комбинированного типа:

1. Тестовые задания с обоснованием выбора одного правильного ответа из предложенных и обоснованием выбора.

№ п.п.	Содержание задания	Правильный ответ	Аргументы, обосновывающие выбор ответа
1.	<p>Какой риск является наиболее критичным при внедрении системы искусственного интеллекта для автоматического распределения социальных выплат?</p> <p>Варианты ответов:</p> <p>А) риск увеличения нагрузки на ИТ-инфраструктуру муниципалитета;</p> <p>Б) риск предвзятости алгоритма, приводящий к дискриминации отдельных категорий граждан;</p>		

	<p>В) риск снижения мотивации сотрудников соцзащиты;</p> <p>Г) риск роста затрат на электроэнергию для работы серверов.</p>		
2.	<p>Какая мера наиболее эффективна для минимизации риска утечки персональных данных при использовании Big Data в системе здравоохранения региона?</p> <p>Варианты ответов:</p> <p>А) полный запрет на сбор данных о пациентах с хроническими заболеваниями;</p> <p>Б) анонимизация и псевдонимизация данных перед загрузкой в аналитическую систему;</p> <p>В) увеличение числа сотрудников, имеющих полный доступ к базе данных пациентов;</p> <p>Г) хранение всех данных исключительно на локальных серверах медучреждений без интеграции.</p>		

2. Тестовые задания с обоснованием выбора одного правильного ответа из предложенных и обоснованием выбора.

№ п.п.	Содержание задания	Правильный ответ	Аргументы, обосновывающие выбор ответа
--------	--------------------	------------------	--

1.	<p>Какой риск является наиболее критичным при внедрении блокчейн-платформы для учёта государственных закупок?</p> <p>Варианты ответов:</p> <p>А) риск высокой энергоёмкости системы консенсуса, ведущей к росту операционных затрат;</p> <p>Б) необратимость ошибочных записей в реестре, затрудняющая исправление ошибок в контрактах;</p> <p>В) риск низкой скорости транзакций из-за перегрузки сети;</p> <p>Г) риск недостаточной масштабируемости при росте числа участников закупок.</p>		
2.	<p>Какая мера наиболее эффективна для минимизации риска взлома IoT-датчиков в системе «Умного города» (например, датчиков загрязнения воздуха или уровня шума)?</p> <p>Варианты ответов:</p> <p>А) полный запрет на удалённое обновление прошивки устройств;</p> <p>Б) сегментация сети и изоляция IoT-устройств от критически важных</p>		

<p>инфраструктур; В) использование одинаковых паролей для всех датчиков для упрощения администрирования; Г) отказ от шифрования данных, передаваемых датчиками, для снижения нагрузки на процессоры устройств.</p>		
--	--	--

Контрольные задания:

Задание 1.

Сбой в работе ИИ-системы распределения соцвыплат

В регионе внедрили ИИ-систему для автоматического распределения субсидий малоимущим семьям. Через месяц работы система начала отказывать в выплатах семьям, которые объективно имеют право на поддержку. Граждане массово обращаются в администрацию с жалобами.

Выявите 3–4 возможные причины сбоя (технические, этические, организационные).

Определите зоны рисков, затронутые в этой ситуации (используйте классификацию из темы 3).

Предложите 3–4 меры реагирования для устранения текущей проблемы и предотвращения подобных сбоев в будущем. Укажите ответственных за реализацию каждой меры.

Тема 5. Стратегии, методы, инструменты управления рисками

Тестирование:

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.

Какая стратегия предполагает осознанное решение не предпринимать специальных мер по устранению риска, а зарезервировать ресурсы на ликвидацию последствий?

- А) избегание риска;
- Б) снижение риска;
- В) передача риска;
- Г) принятие риска.

Какой инструмент позволяет визуализировать и приоритизировать риски по вероятности и воздействию?

- А) реестр рисков;
- Б) матрица рисков 5×5;
- В) план аварийного восстановления;
- Г) дорожная карта проекта.

Какой метод идентификации рисков предполагает привлечение экспертов для достижения консенсуса через анонимные опросы?

- А) мозговой штурм;
- Б) SWOT-анализ;
- В) метод Дельфи;
- Г) анализ сценариев.

Что означает показатель RTO в плане аварийного восстановления?

- А) максимальный допустимый объём потерянных данных;
- Б) максимальное время восстановления системы после сбоя;
- В) периодичность резервного копирования данных;
- Г) количество резервных копий, хранящихся одновременно.

Какой инструмент управления рисками включает разделы: идентификатор риска, описание, вероятность, воздействие, стратегия реагирования, ответственный, сроки?

- А) матрица рисков;
- Б) план управления проектом;
- В) реестр рисков;
- Г) дашборд мониторинга.

Контрольные задания:

Задание 1.

Блокчейн для голосования на муниципальных выборах

Муниципалитет тестирует блокчейн-платформу для дистанционного электронного голосования (ДЭГ). Пилот запланирован на ближайших выборах в городской совет. Команда проекта должна оценить риски и предложить меры реагирования.

Определите 3 основных риска, связанных с применением блокчейна в ДЭГ.

Для каждого риска сформулируйте: сценарий реализации (кратко, 2–3 предложения); триггер (признак начала реализации); стратегию реагирования (избежание, снижение, передача, принятие).

Разработайте чек-лист из 5 пунктов для проверки готовности платформы к пилотному запуску.

Задания открытого типа:

1. Вопросы открытого типа с развернутым ответом.

№ п.п.	Вопрос	Ответ
1.	Опишите стратегию «снижение риска» в контексте внедрения ИИ-системы для анализа обращений граждан в органе публичной власти. Приведите 3–4 конкретных примера мер, которые позволят снизить вероятность и/или воздействие рисков при таком внедрении.	
2.	В чём принципиальное отличие стратегии «передача риска» от стратегии «принятие риска» при реализации проекта цифровой трансформации в муниципалитете? Приведите по одному реалистичному примеру для каждой стратегии.	

2. Вопросы открытого типа с развернутым ответом.

№ п.п.	Вопрос	Ответ
1.	Перечислите обязательные разделы реестра рисков для проекта миграции государственных информационных систем в облако. Для каждого раздела кратко укажите, какую информацию он должен содержать. Приведите 3 примера рисков с заполнением реестра (идентификатор, описание, стратегия реагирования и т. д.).	

2.	Какие требования федеральных законов (укажите названия) необходимо учитывать при управлении рисками цифровой трансформации в органах публичной власти? Приведите 3 конкретных примера, как эти законы влияют на выбор инструментов управления рисками.	
----	--	--

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	0,1	10
КТ 2	100	0,2	20
КТ 3	100	0,3	30
Итого:	x	0,6	60

Формула расчета результата контрольной точки:

Результат контрольной точки = Количество баллов за работу в рамках КТ X Коэффициент веса контрольной точки.

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

КТ – 1.

Тема 1.

Доклад

КТ – 2.

Тема 2.

Устный опрос

КТ – 3.

Темы 1-5.

Тестирование

Темы 2-5.

Контрольные задания

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

1. Критерии оценивания доклада

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

2. Критерии оценивания опроса

Критерии оценки	Диапазон баллов	Описание критерия
<i>Теоретический уровень знаний</i>	0-25	<i>Обучающийся полно и последовательно излагает материал по существу темы, обнаруживает понимание материала, дает правильное определение основных понятий, правильно использует нормы литературного языка</i>
<i>Подкрепление материалов фактическими данными (статистические данные или др.)</i>	0-25	<i>Обучающийся может применять знания на практике, приводит примеры динамики развития явления (на основании статических данных или конкретных фактов) из учебника и самостоятельно</i>
<i>Способность делать выводы</i>	0-25	<i>Обучающийся способен доказательно обосновать свои суждения, приводит аргументированные выводы</i>
<i>Качество ответов на вопросы</i>	0-25	<i>Обучающийся точно формулирует ответы, демонстрирует уместное использование терминов, находит нестандартные решения</i>
Итого максимально:	100	

3. Критерии оценивания тестирования

Критерии оценки	Диапазон баллов	Описание критерия
<i>Количество правильных ответов</i>	0	<i>Количество правильных ответов менее 55%</i>
	25	<i>Количество правильных ответов от 55% до 64%</i>
	50	<i>Количество правильных ответов от 65% до 74%</i>

	75	<i>Количество правильных ответов от 75% до 84%</i>
	100	<i>Количество правильных ответов от 85% до 100%</i>
Итого максимально:	100	

4. Критерии оценивания решения контрольного задания

Критерии оценки	Диапазон баллов	Описание критерия
<i>Активность Качество практических рекомендаций Структура и логика</i>	0-20	<i>Детальное, последовательное излагает мысли; решение структурировано;</i>
<i>Качество практических рекомендаций Обоснованность и аргументация</i>	0-20	<i>Решение соответствует поставленным вопросам; наличие аргументов в пользу предложенного решения; Обучающийся объясняет почему выбран именно данный вариант решения</i>
<i>Полнота раскрытия темы задания и владение терминологией</i>	0-20	<i>Обучающийся раскрывает тему; дает ссылки на законодательство</i>
<i>Правильные ответы на дополнительные вопросы</i>	0-20	<i>Обучающийся отвечает на дополнительные вопросы; даёт правильное определение основных понятий; обнаруживает понимание материала, может обосновать свои суждения, применить знания на практике, привести необходимые примеры</i>
<i>Оригинальность</i>	0-20	<i>Уникальный подход к теме, нестандартные решения, инновационные идеи, собственная позиция автора</i>

Итого максимально:	100	
--------------------	-----	--

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

Для решения контрольных заданий обучающемуся разрешается использование калькулятора.

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

6.1. Промежуточная аттестация (зачет с оценкой) проводится в письменной форме. Обучающийся получает экзаменационный билет с вариантами вопросов и заданием. На выполнение заданий даётся 40-60 минут. По завершении подготовки необходимо представить ответы в письменном виде, подробно изложив ход выполнения задания, сделать выводы (*при необходимости*).

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

6.2. Типовые оценочные материалы промежуточной аттестации

Вопросы для подготовки к зачету с оценкой:

1. Понятие управления рисками (risk management) в публичном управлении.
2. Жизненный цикл управления рисками: основные этапы.
3. Принципы управления рисками в системе публичного управления.
4. Международные стандарты управления рисками (ISO 31000, COSO ERM): общая характеристика.
5. Адаптация международных стандартов управления рисками для органов публичной власти.
6. Стратегия избегания риска: сущность и примеры применения в системе публичного управления.
7. Стратегия снижения риска: методы и инструменты реализации.
8. Стратегия передачи риска: механизмы и сферы применения в органах публичной власти.
9. Стратегия принятия риска: условия целесообразности в проектах цифровой трансформации.

10. Метод мозгового штурма для идентификации рисков: алгоритм и ограничения.
11. Метод Дельфи: особенности применения для оценки рисков в системе публичного управления.
12. SWOT-анализ как инструмент выявления рисков: структура и применение.
13. Анализ сценариев («что если») в управлении рисками: суть и примеры использования.
14. Качественная оценка рисков: матрица рисков 3×3 и 5×5, правила построения.
15. Количественная оценка рисков: расчёт ожидаемых потерь.
16. Моделирование Монте-Карло для прогнозирования сценариев рисков: возможности и ограничения.
17. Реестр рисков (risk register): структура и обязательные поля.
18. План управления рисками проекта цифровой трансформации: ключевые разделы.
19. Гибкие контракты с поставщиками: роль SLA и KPI в управлении рисками.
20. Дорожная карта внедрения с этапами пилотирования: значение для минимизации рисков.
21. Специфика управления рисками при внедрении ИИ в госуправление.
22. Аудит алгоритмов ИИ на предвзятость: методы и нормативные требования.
23. Механизмы обжалования решений ИИ-систем в органах публичной власти.
24. Управление рисками Big Data: анонимизация данных и соответствие федеральному закону «О персональных данных».
25. Сегментация сетей как мера защиты IoT-инфраструктуры «Умного города».
26. Юридические аспекты использования смарт-контрактов на блокчейне в системе публичного управления.
27. Резервное копирование и планы аварийного восстановления для облачных решений.
28. Организационные инструменты управления рисками: создание подразделений и назначение ответственных.
29. Программы обучения государственных и муниципальных служащих основам кибербезопасности: содержание и цели.
30. Вовлечение граждан в тестирование цифровых сервисов: формы и эффекты.

31. Федеральный закон «О персональных данных»: основные требования к управлению рисками.

32. Федеральный закон «О безопасности критической информационной инфраструктуры Российской Федерации»: влияние на выбор инструментов управления рисками.

33. Постановление Правительства РФ «Об утверждении Правил формирования и ведения единого реестра российских программ для электронных вычислительных машин и баз данных и единого реестра программ для электронных вычислительных машин и баз данных из государств - членов Евразийского экономического союза, за исключением Российской Федерации»: требования к импортозамещению ПО и их роль в управлении рисками.

34. ГОСТ Р ИСО 31000-2019 «Менеджмент риска»: применение в органах публичной власти.

35. Процессуальные инструменты мониторинга рисков: аудиты безопасности и пентесты.

36. Системы SIEM: назначение и возможности в управлении рисками публичного управления.

37. Отчётность по рискам: виды и требования к представлению информации.

38. Карты рисков (heat maps) и дашборды KRI: назначение и принципы построения.

39. Культура управления рисками в органе публичной власти: элементы и способы формирования.

40. Пост-мортем-анализ инцидентов: этапы и значение для совершенствования системы риск-менеджмента.

Типовые задания для зачета с оценкой

Проанализируйте представленное задание, определите, установите и укажите свое отношение к затронутой теме сформулируйте ответ по заданию, дайте ему обоснование.

Задание 1.

Проблемы с «Умным освещением»

В городе установили «умные» фонари с датчиками движения. Иногда фонари не загораются ночью, хотя датчики работают. Жители жалуются.

Назовите 1 возможную техническую причину сбоя.

Предложите 1 быстрое решение проблемы.

Укажите, кого из сотрудников муниципалитета нужно привлечь для устранения сбоя.

Задание 2.

Утечка данных из электронной почты госоргана

Сотрудник муниципалитета случайно отправил письмо с персональными данными граждан не тем адресатам.

Назовите 1 последствие утечки для органа публичной власти.

Перечислите 2 действия, которые нужно сделать сразу после обнаружения ошибки.

Предложите 1 меру, чтобы избежать подобных ситуаций в будущем.

Задание 3.

Сбой облачной системы документооборота

Облачная система электронного документооборота муниципалитета не работает уже 2 часа. Сотрудники не могут отправлять и получать документы.

Назовите 1 возможную причину сбоя.

Предложите 2 способа продолжить работу органа публичной власти без СЭД на время сбоя.

Укажите, кому нужно сообщить о проблеме в первую очередь.

Типовые проверочные задания для самоподготовки обучающегося к промежуточной аттестации:

ТИП ЗАДАНИЯ	СЦЕНАРИИ ВЫПОЛНЕНИЯ	ТИПОВЫЕ ЗАДАНИЯ
Задание закрытого типа с выбором одного правильного ответа из нескольких вариантов предложенных	1. Внимательно прочитать текст задания и понять, что в качестве ответа ожидается только один из предложенных вариантов. 2. Внимательно прочитать предложенные варианты ответа. 3. Выбрать один верный ответ. 4. Записать только номер (или букву) выбранного варианта ответа (например, 2 или А).	1. Какой триггер сигнализирует о реализации риска прекращения услуг облачного провайдера для системы электронного документооборота (СЭД) госоргана? А) Увеличение числа обращений в техподдержку по вопросам авторизации. Б) Уведомление провайдера о прекращении поддержки сервиса из-за санкций или банкротства. В) Кратковременный сбой в работе мобильного приложения СЭД. Г) Рост числа внутренних пользователей системы.
		2. Почему применение блокчейна для учёта земельных участков в РФ требует особого внимания к нормативному регулированию?

		<p>А) Блокчейн автоматически гарантирует юридическую силу всех записей без дополнительных процедур.</p> <p>Б) Действующее законодательство (Земельный кодекс РФ, ФЗ № 218 «О государственной регистрации недвижимости») не предусматривает прямого признания блокчейна как основного реестра прав.</p> <p>В) Технология блокчейна полностью исключает возможность судебных споров о правах на землю.</p> <p>Г) Все сделки с недвижимостью уже обязаны регистрироваться исключительно через блокчейн-платформы.</p>								
<p>Задание закрытого типа на установление соответствия</p>	<p>1. Внимательно прочитать текст задания и понять, что в качестве ответа ожидаются пары элементов.</p> <p>2. Внимательно прочитать оба списка: список 1 – вопросы, утверждения, факты, понятия и т.д.; список 2 – утверждения, свойства объектов и т.д.</p> <p>3. Сопоставить элементы списка 1 с элементами списка 2, сформировать пары элементов.</p> <p>4. Записать попарно буквы и цифры (в зависимости от задания) вариантов ответа (например, А1 или Б4).</p>	<p>1. Установите соответствие между термином, приводимым в столбце слева (зоной риска), и определением из правого столбца (инструментом минимизации): к каждой позиции, данной в левом столбце, подберите соответствующую позицию из правого столбца</p> <table border="1" data-bbox="852 1039 1444 1926"> <tr> <td data-bbox="852 1039 1118 1211">1. Зона стратегического планирования и целеполагания</td> <td data-bbox="1118 1039 1444 1211">А) проведение пентестов и аудита безопасности</td> </tr> <tr> <td data-bbox="852 1211 1118 1420">2. Зона ИТ-инфраструктуры и эксплуатации систем</td> <td data-bbox="1118 1211 1444 1420">Б) поэтапное внедрение и пилотирование новых решений</td> </tr> <tr> <td data-bbox="852 1420 1118 1675">3. Зона обработки и защиты данных</td> <td data-bbox="1118 1420 1444 1675">В) чёткое формулирование целей по SMART и разработка KPI цифровой трансформации</td> </tr> <tr> <td data-bbox="852 1675 1118 1926">4. Зона взаимодействия с гражданами и обществом</td> <td data-bbox="1118 1675 1444 1926">Г) организация обучающих семинаров и создание видеоинструкций для граждан</td> </tr> </table>	1. Зона стратегического планирования и целеполагания	А) проведение пентестов и аудита безопасности	2. Зона ИТ-инфраструктуры и эксплуатации систем	Б) поэтапное внедрение и пилотирование новых решений	3. Зона обработки и защиты данных	В) чёткое формулирование целей по SMART и разработка KPI цифровой трансформации	4. Зона взаимодействия с гражданами и обществом	Г) организация обучающих семинаров и создание видеоинструкций для граждан
1. Зона стратегического планирования и целеполагания	А) проведение пентестов и аудита безопасности									
2. Зона ИТ-инфраструктуры и эксплуатации систем	Б) поэтапное внедрение и пилотирование новых решений									
3. Зона обработки и защиты данных	В) чёткое формулирование целей по SMART и разработка KPI цифровой трансформации									
4. Зона взаимодействия с гражданами и обществом	Г) организация обучающих семинаров и создание видеоинструкций для граждан									

		<p>2. Установите соответствие между термином, приводимым в столбце слева (зоной риска), и определением из правого столбца (триггером риска): к каждой позиции, данной в левом столбце, подберите соответствующую позицию из правого столбца.</p> <table border="1" data-bbox="852 450 1445 1422"> <tr> <td data-bbox="852 450 1118 663">1. зона нормативного регулирования и соответствия требованиям</td> <td data-bbox="1118 450 1445 663">А) резкий рост числа обращений в техподдержку от пожилых пользователей</td> </tr> <tr> <td data-bbox="852 663 1118 916">2. зона взаимодействия с гражданами и обществом</td> <td data-bbox="1118 663 1445 916">Б) публикация проекта нового закона, ужесточающего требования к хранению данных</td> </tr> <tr> <td data-bbox="852 916 1118 1169">3. зона управления персоналом и организационно й культуры</td> <td data-bbox="1118 916 1445 1169">В) увеличение числа инцидентов ИБ после подключения нового подрядчика</td> </tr> <tr> <td data-bbox="852 1169 1118 1422">4. зона закупок и взаимодействия с подрядчиками</td> <td data-bbox="1118 1169 1445 1422">Г) низкий процент активных пользователей новой системы среди сотрудников в первые 2 недели</td> </tr> </table>	1. зона нормативного регулирования и соответствия требованиям	А) резкий рост числа обращений в техподдержку от пожилых пользователей	2. зона взаимодействия с гражданами и обществом	Б) публикация проекта нового закона, ужесточающего требования к хранению данных	3. зона управления персоналом и организационно й культуры	В) увеличение числа инцидентов ИБ после подключения нового подрядчика	4. зона закупок и взаимодействия с подрядчиками	Г) низкий процент активных пользователей новой системы среди сотрудников в первые 2 недели
1. зона нормативного регулирования и соответствия требованиям	А) резкий рост числа обращений в техподдержку от пожилых пользователей									
2. зона взаимодействия с гражданами и обществом	Б) публикация проекта нового закона, ужесточающего требования к хранению данных									
3. зона управления персоналом и организационно й культуры	В) увеличение числа инцидентов ИБ после подключения нового подрядчика									
4. зона закупок и взаимодействия с подрядчиками	Г) низкий процент активных пользователей новой системы среди сотрудников в первые 2 недели									
<p>Задание закрытого типа с выбором нескольких правильных ответов из нескольких вариантов предложенных</p>	<p>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).</p>	<p>1. Какие факторы необходимо учитывать при выборе облачного провайдера для госоргана? А) соответствие требованиям федерального закона «О персональных данных»; Б) наличие у провайдера сертификата соответствия требованиям федерального закона «О безопасности критической информационной инфраструктуры Российской Федерации»; В) расположение дата-центров исключительно на территории Российской Федерации; Г) количество стран, в которых работает</p>								

		<p>провайдер; Д) наличие мобильного приложения у провайдера.</p> <p>2. Какие меры обеспечивают защиту персональных данных при использовании Big Data в системе публичного управления? А) анонимизация и псевдонимизация данных перед анализом; Б) шифрование данных в покое и при передаче; В) увеличение числа сотрудников с доступом к полным наборам данных; Г) регулярный аудит безопасности и оценка уязвимостей; Д) хранение всех данных в одном централизованном хранилище без сегментации</p>
<p>Задание закрытого типа на установление последовательности</p>	<p>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, БАВ или 135).</p>	<p>1. Расположите в правильной последовательности шаги создания и ведения реестра рисков в органе публичной власти. А) актуализация реестра: внесение новых рисков, обновление статусов, закрытие реализованных или неактуальных рисков; Б) заполнение полей для каждого риска: описание, вероятность, воздействие, ответственный, меры реагирования, статус; В) утверждение формы реестра рисков и регламента его ведения приказом руководителя органа публичной власти; Г) первичное внесение выявленных рисков в реестр на основе результатов идентификации; Д) регулярный мониторинг и предоставление отчётов на основе данных реестра (например, раз в квартал).</p> <p>2. Установите верную последовательность действий при реагировании на инцидент информационной безопасности (например, утечку данных) в органе публичной власти. А) устранение причин инцидента (например, закрытие уязвимости в</p>

		<p>системе, блокировка атакующего IP-адреса);</p> <p>Б) локализация инцидента — ограничение распространения угрозы (изоляция заражённого сегмента сети, отключение сервиса);</p> <p>В) анализ причин инцидента и корректировка реестра рисков: внесение нового риска или актуализация существующего;</p> <p>Г) уведомление ответственных лиц и заинтересованных сторон (руководство, ИТ-отдел, при необходимости — правоохранительные органы);</p> <p>Д) фиксация инцидента: сбор логов, скриншотов, других доказательств;</p> <p>Е) восстановление работоспособности системы (восстановление данных из бэкапа, перезапуск сервисов).</p>
<p>Задание комбинированного типа с выбором одного правильного ответа из предложенных и обоснованием выбора</p>	<p>1. Внимательно прочитать текст задания и понять, что в качестве ответа ожидается только один из предложенных вариантов.</p> <p>2. Внимательно прочитать предложенные варианты ответа.</p> <p>3. Выбрать один верный ответ.</p> <p>4. Записать только номер (или букву) выбранного варианта ответа.</p> <p>5. Записать аргументы, обосновывающие выбор ответа (например, 4 текст обоснования).</p>	<p>1. При оценке риска сбоя в работе портала госуслуг из-за DDoS-атаки вы получили следующие данные: вероятность — средняя (3 из 5), потенциальный ущерб — высокий (5 из 5). Какая стратегия реагирования будет оптимальной согласно матрице рисков?</p> <p>А) избежание риска — временно отключить портал до устранения угрозы;</p> <p>Б) снижение риска — внедрить систему защиты от DDoS и усилить мониторинг;</p> <p>В) передача риска — заключить договор страхования без дополнительных технических мер;</p> <p>Г) принятие риска — оставить всё как есть, сославшись на то, что атаки не всегда успешны.</p> <p>2. Вы анализируете риски внедрения ИИ-системы для прогнозирования загруженности дорог в городе. Выявлен риск предвзятости алгоритма из-за некачественных данных. Какой метод оценки риска наиболее уместен на данном этапе?</p> <p>А) расчёт VaR в денежном выражении без учёта качественных факторов;</p>

		<p>Б) качественный анализ с привлечением экспертов по ИИ и транспортной инфраструктуре для оценки потенциального воздействия на безопасность движения;</p> <p>В) опора исключительно на мнение разработчика системы без независимой проверки;</p> <p>Г) игнорирование риска на основании того, что система уже успешно работает в другом городе.</p>
Задание открытого типа с развернутым ответом	<p>1. Внимательно прочитать текст задания и понять суть вопроса.</p> <p>2. Продумать логику и полноту ответа.</p> <p>3. Записать ответ, используя четкие компактные формулировки.</p> <p>4. В случае расчетной задачи записать решение и ответ</p>	<p>1. Почему качественная оценка рисков (матрица 5×5) часто предпочтительнее количественной (расчёт ожидаемых потерь) в проектах публичного управления? Приведите 2 аргумента и пример ситуации, где качественная оценка более уместна.</p>
		<p>2. Объясните, как построить матрицу рисков 5×5 для проекта внедрения IoT-датчиков контроля качества воздуха в «Умном городе». Опишите шкалу оценки вероятности и воздействия, приведите 2–3 примера рисков с их позиционированием в матрице.</p>

6.3. Критерии и шкала оценивания на основе БРС.

КРИТЕРИИ ОЦЕНИВАНИЯ	РЕЗУЛЬТАТ В БАЛЛАХ
<p>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</p>	40
<p>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.</p>	30-39
<p>Дан ответ, свидетельствующий в основном о знании процессов</p>	20-29

<p>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.</p>	
<p>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 способен ответить на вопросы даже при дополнительных наводящих вопросах преподавателя.</p>	<p>0-19</p>

6.4. Для решения контрольных заданий обучающемуся разрешается использование калькулятора.

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 10 письменно). Все новые понятия по изучаемой теме необходимо выучить наизусть и 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.

Структура практического занятия:

В зависимости от содержания и количества отведенного времени на изучение каждой темы может практическое занятие состоять из четырех-пяти частей:

1. Обсуждение теоретических вопросов, определенных программой дисциплины.
2. Доклад и/ или выступление с презентациями по проблеме практического занятия.
3. Обсуждение выступлений по теме – дискуссия.
4. Выполнение практического задания с последующим разбором полученных результатов или обсуждение практического задания, выполненного дома, если это предусмотрено программой.
5. Подведение итогов занятия.

Первая часть – обсуждение теоретических вопросов - проводится в виде фронтальной беседы со всей группой и включает выборочную проверку преподавателем теоретических знаний обучающихся. Примерная продолжительность — до 15 минут. Вторая часть — выступление обучающихся с докладами, которые должны сопровождаться презентациями с целью усиления наглядности восприятия, по одному из вопросов практического занятия. Обязательный элемент доклада – представление и анализ статистических данных, обоснование социальных последствий любого экономического факта, явления или процесса. Примерная продолжительность — 20-25 минут. После докладов следует их обсуждение – дискуссия. В ходе этого этапа практического занятия могут быть заданы уточняющие вопросы к докладчикам. Примерная продолжительность – до 15-20 минут. Если программой предусмотрено выполнение практического задания в рамках конкретной темы, то преподавателями определяется его содержание и дается время на его выполнение, а затем идет обсуждение результатов. Если практическое задание должно было быть выполнено дома, то на практическом занятии преподаватель проверяет его выполнение (устно или письменно). Примерная продолжительность – 15-20 минут. Подведением итогов заканчивается практическое занятие. Обучающимся должны быть объявлены оценки за работу и даны их четкие обоснования. Примерная продолжительность — 5 минут.

Методические рекомендации по подготовке доклада.

Подготовка доклада способствует формированию навыков исследовательской работы, расширяет познавательные интересы, приучает критически мыслить. При написании доклада по заданной теме составляется план, подбираются основные источники. В процессе работы с источниками, систематизируют полученные сведения, делают выводы и обобщения.

Подготовка доклада требует от обучающегося большой самостоятельности и серьезной интеллектуальной работы, которая принесет наибольшую пользу, если будет включать с себя следующие этапы: изучение наиболее важных научных работ по данной теме, перечень которых дает сам преподаватель; анализ изученного материала, выделение наиболее значимых для раскрытия темы фактов, мнений разных ученых и научных положений; обобщение и логическое построение материала доклада, например, в форме развернутого плана; написание текста доклада с соблюдением требований научного стиля.

Построение доклада включает три части: вступление, основную часть и заключение. Во вступлении указывается тема доклада, устанавливается логическая связь ее с другими темами или место рассматриваемой проблемы среди других проблем, дается краткий обзор источников, на материале которых раскрывается тема и т. п. Основная часть должна иметь четкое логическое построение, в ней должна быть раскрыта тема доклада. В заключении обычно подводятся итоги, формулируются выводы, подчеркивается значение рассмотренной проблемы и т. п.

Работа с литературными 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.

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

8.1. Основная литература

1. Белов, П. Г. Управление рисками, системный анализ и моделирование : учебник и практикум для вузов / П. Г. Белов. — Москва : Издательство Юрайт, 2026. — 721 с. — (Высшее образование). — ISBN 978-5-534-17939-2. — Текст : электронный // Образовательная платформа Юрайт [сайт]. —

URL: <https://urait.ru/bcode/599038>

2. Воронцовский, А. В. Управление рисками : учебник и практикум для вузов / А. В. Воронцовский. — 2-е изд. — Москва : Издательство Юрайт, 2026. — 485 с. — (Высшее образование). — ISBN 978-5-534-12206-0. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/583504>

3. Вяткин, В. Н. Риск-менеджмент : учебник / В. Н. Вяткин, В. А. Гамза, Ф. В. Маевский. — 2-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2026. — 365 с. — (Высшее образование). — ISBN 978-5-9916-3502-8. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/583030>

4. Камолов, С. Г. Цифровое государственное управление : учебник для вузов / С. Г. Камолов, Н. Д. Александров. — 2-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2026. — 287 с. — (Высшее образование). — ISBN 978-5-534-21027-9. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/588737>

5. Козырь, Н. С. Анализ и оценка рисков информационной безопасности : учебник для вузов / Н. С. Козырь, В. Н. Хализев. — Москва : Издательство Юрайт, 2026. — 157 с. — (Высшее образование). — ISBN 978-5-534-17866-1. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/590420>

6. Риск-ориентированное государственное и муниципальное управление : учебник для вузов / под научной редакцией С. Е. Прокофьева, О. В. Паниной. — Москва : Издательство Юрайт, 2026. — 108 с. — (Высшее образование). — ISBN 978-5-534-21957-9. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/590709>

7. Трофимов, В. В. Цифровые технологии : учебник для вузов / В. В. Трофимов. — Москва : Издательство Юрайт, 2026. — 141 с. — (Высшее образование). — ISBN 978-5-534-21710-0. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/582239>

8.2. Дополнительная литература

8. Алиев, О. И. Управление рисками. Экономические риски : учебник для вузов / О. И. Алиев, А. М. Кипкеева. — Москва : Издательство Юрайт, 2026. — 137 с. — (Профессиональное образование). — ISBN 978-5-534-18402-0. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/590313>

9. Абрамов, В. С. Функциональные стратегии : учебник и практикум для вузов / В. С. Абрамов, С. В. Абрамов. — 5-е изд., перераб. и доп. — Москва :

Издательство Юрайт, 2026. — 164 с. — (Высшее образование). — ISBN 978-5-534-21906-7. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/582408>

10. Белов, П.Г. Системный анализ и программно-целевой менеджмент рисков : учебник и практикум для вузов / П.Г. Белов.- Москва : Издательство Юрайт, 2026. — 289 с. — (Высшее образование). — ISBN 978-5-534-17939-2. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/viewer/sistemnyy-analiz-i-programmno-celevoy-menedzhment-riskov-598787#page/2>

11. Воронцовский, А. В. Оценка рисков : учебник и практикум для вузов / А. В. Воронцовский. — Москва : Издательство Юрайт, 2026. — 179 с. — (Высшее образование). — ISBN 978-5-534-02411-1. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/584929>

12. Государственное антикризисное управление : учебник для вузов / под общей редакцией Е. В. Охотского. — 2-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2025. — 465 с. — (Высшее образование). — ISBN 978-5-534-21408-6. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/571295>

13. Информационные технологии в менеджменте (управлении) : учебник и практикум для вузов / под редакцией Ю. Д. Романовой. — 3-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2026. — 467 с. — (Высшее образование). — ISBN 978-5-534-17037-5. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/582997>

14. Кипкеева, А. М. Управление экономическими рисками : учебник для вузов / А. М. Кипкеева, О. И. Алиев. — Москва : Издательство Юрайт, 2026. — 137 с. — (Высшее образование). — ISBN 978-5-534-18390-0. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/590312>

15. Козырь, Н. С. Аудит информационной безопасности : учебник для вузов / Н. С. Козырь. — Москва : Издательство Юрайт, 2026. — 36 с. — (Высшее образование). — ISBN 978-5-534-20647-0. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/590419>

16. Козырь, Н. С. Оценка рисков и аудит информационной безопасности : учебник для вузов / Н. С. Козырь, В. Н. Хализев. — Москва : Издательство Юрайт, 2026. — 190 с. — (Высшее образование). — ISBN 978-5-534-17864-7. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/590417>

17. Панарина, М. М. Корпоративная безопасность. Управление рисками и комплаенс в эпоху цифровизации : учебное пособие для вузов / М. М. Панарина. —

3-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2026. — 181 с. — (Высшее образование). — ISBN 978-5-534-17777-0. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/589053>

18. Прокофьев, С. Е. Государственный менеджмент : учебник и практикум для вузов / С. Е. Прокофьев, С. Г. Еремин, А. И. Галкин. — Москва : Издательство Юрайт, 2026. — 248 с. — (Высшее образование). — ISBN 978-5-534-15813-7. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/589094>

19. Сергеев, Л. И. Цифровая экономика : учебник для вузов / Л. И. Сергеев, Д. Л. Сергеев, А. Л. Юданова ; под редакцией Л. И. Сергеева. — 2-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2026. — 437 с. URL: <https://urait.ru/bcode/588254>

20. Сологубова Г.С. Составляющие цифровой трансформации : монография / Г.С. Сологубова. — Москва : Издательство Юрайт, 2026. — 147 с. — ISBN 978-5-534-11335-8. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/viewer/sostavlyayuschie-cifrovoy-transformacii-586953#page/2>

21. Тимошенко, С. П. Надежность технических систем и техногенный риск : учебник и практикум для вузов / С. П. Тимошенко, Б. М. Симонов, В. Н. Горошко. — 2-е изд., испр. и доп. — Москва : Издательство Юрайт, 2026. — 551 с. — (Высшее образование). — ISBN 978-5-534-19935-2. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/583341>

22. Черненко, В. А. Антикризисное управление : учебник и практикум для вузов / В. А. Черненко, Н. Ю. Шведова. — 5-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2026. — 408 с. — (Высшее образование). — ISBN 978-5-9916-1322-4. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/600150>

23. Чертыковцев, В. К. Математическая теория рисков. Анализ рисков в социально-экономической сфере : учебник для вузов / В. К. Чертыковцев. — Москва : Издательство Юрайт, 2026. — 102 с. — (Высшее образование). — ISBN 978-5-534-14457-4. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/588773>

8.3. Нормативные правовые документы или иная правовая литература

1. Конституция Российской Федерации: принята всенародным голосованием 12 декабря 1993 г. (с изменениями на 4 октября 2022 года) // Официальный интернет-портал правовой информации www.pravo.gov.ru, 06.10.2022, N 0001202210060013.

2. Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных» // Собр. законодательства РФ. 2006. № 31 (ч. I). Ст. 3451.

3. Федеральный закон от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» // Собр. законодательства РФ. 2017. № 31 (ч. I). Ст. 4736.

4. Указ Президента РФ от 07 мая 2024 г. № 309 «О национальных целях развития Российской Федерации на период до 2030 года и на перспективу до 2036 года» // Собр. законодательства РФ. 2024. № 20. Ст. 2584.

5. Приказ Минтруда России от 28 декабря 2021 г. № 926 «Об утверждении Рекомендаций по выбору методов оценки уровней профессиональных рисков и по снижению уровней таких рисков» // <https://docs.cntd.ru/document/728029758?section=text>

6. Приказ Минтруда России от 18 апреля 2025 г. № 264н «Об утверждении профессионального стандарта «Специалист по управлению рисками» // Официальный интернет-портал правовой информации www.pravo.gov.ru, 29.05.2025, № 0001202505290007

7. ГОСТ Р 58771-2019 Менеджмент риска. Технологии оценки риска (Переиздание) // <https://docs.cntd.ru/document/1200170253?section=text>

8. ГОСТ Р 59516-2021 Информационные технологии (ИТ). Менеджмент информационной безопасности. Правила страхования рисков информационной безопасности // <https://docs.cntd.ru/document/1200179668?section=text>

9. ГОСТ Р 59339-2021 Системная инженерия. Защита информации в процессе управления рисками для системы // <https://docs.cntd.ru/document/1200179457?section=text>

10. ГОСТ Р 71207-2024 Защита информации. Разработка безопасного программного обеспечения. Статический анализ программного обеспечения. Общие требования // <https://docs.cntd.ru/document/1304734159?section=text>

11. ГОСТ Р 70262.2-2025 Защита информации. Идентификация и аутентификация. Уровни доверия аутентификации // <https://docs.cntd.ru/document/1312989681?section=text>

12. Методические рекомендации по управлению риском информационной безопасности и обеспечению операционной надежности (утв. Банком России 21.03.2024 N 7-МР) // https://www.consultant.ru/document/cons_doc_LAW_473013/

8.4. Интернет-ресурсы

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

Русскоязычные ресурсы

1. Образовательная платформа ЮРАЙТ <https://urait-ru.idp.nwipa.ru/>

2. Электронно-библиотечная система «Znanium.com» <https://znanium-com.idp.nwipa.ru/catalog/books/theme>

3. Электронные учебники электронно-библиотечной системы (ЭБС) «Айбукс» http://www.nwapa.spb.ru/index.php?page_id=76

4. Статьи из журналов и статистических изданий Ист Вью http://www.nwapa.spb.ru/index.php?page_id=76

Англоязычные ресурсы

EBSCO Publishing- доступ к мультидисциплинарным полнотекстовым базам данных различных мировых издательств по бизнесу, экономике, финансам, бухгалтерскому учету, гуманитарным и естественным областям знаний, рефератам и полным текстам публикаций из научных и научно – популярных журналов.

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

8.5. Иные источники

1. Административно-управленческий портал [Электронный ресурс] / AUP.Ru. — Электрон. дан. — Режим доступа: <http://www.aup.ru/>, свободный. — Загл. с экрана.

2. Проблемы теории и практики управления [Электронный ресурс]. — Электрон. журн. — М.: Финпресс. — Режим доступа к журн.: <http://www.urtp.ru/>. — Загл. с экрана.

3. Российская государственная библиотека [Электронный ресурс] / Центр информ. технологий РГБ ; ред. Власенко Т.В. ; Web-мастер Козлова Н.В. — Электрон. дан. — М.: Рос. гос. б-ка, 1997. — Режим доступа: <http://www.rsl.ru>, свободный. — Загл. с экрана. — Яз. рус., англ. 32

4. Центр стратегических разработок [Электронный ресурс]/ Аплекс. — Электрон. дан. — М.: Центр стратегических разработок, 1999-2004. — Режим доступа: <http://www.csrg.ru>, свободный. — Загл. с экрана.

5. Гарант [Электронный ресурс]: информационно – правовой портал / ООО «НПП «Гарант – сервис». - [М.], 2012. – Режим доступа: <http://www.garant.ru/>

6. КонсультантПлюс – правовая поддержка [Электронный ресурс]: офиц.сайт Компании «КонсультантПлюс»/ Компания «КонсультантПлюс». – М.,1997 – 2012.-Режим доступа: <http://www.consultant.ru/>

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.