

**МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ
ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«ЛУГАНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
ИМЕНИ ВЛАДИМИРА ДАЛЯ»**

**Институт управления и государственной службы
Кафедра производственного менеджмента**

УТВЕРЖДАЮ:
Директор Института управления и
государственной службы
Р.Г. Харьковский

(подпись)

« » 2023 года

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ

«Управление цифровыми рисками»

По направлению подготовки 38.04.02 Менеджмент

Магистерская программа «Управление организацией в цифровой экономике»

Луганск – 2023

Лист согласования РПУД

Рабочая программа учебной дисциплины «Управление цифровыми рисками» по направлению подготовки 38.04.02 Менеджмент, магистерская программа «Управление организацией в цифровой экономике» – ____ с.

Рабочая программа учебной дисциплины «Управление цифровыми рисками» разработана в соответствии с Федеральным государственным образовательным стандартом высшего образования по направлению подготовки 38.04.02 «Менеджмент» (утвержден приказом Министерства образования и науки Российской Федерации от 12 августа 2020 г. № 952).

СОСТАВИТЕЛЬ:

канд. экон. наук Жокабине Н.Ф.

Рабочая программа дисциплины утверждена на заседании кафедры производственного менеджмента «21» 03 2023 г., протокол № 11.

Заведующий кафедрой

производственного менеджмента _____

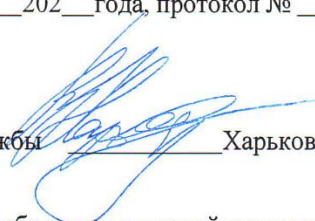


Родионов А.В.

Переутверждена: « » _____ 202 года, протокол № _____

Директор института

управления и государственной службы _____



Харьковский Р.Г.

Рекомендована на заседании учебно-методической комиссии института управления и государственной службы «12» 04 2023 г., протокол № 8.

Председатель учебно-методической
комиссии института _____



Резник А.А.

Структура и содержание дисциплины

1. Цели и задачи дисциплины, ее место в учебном процессе

Целью изучения дисциплины «Управление цифровыми рисками» является формирование у студентов знаний и навыков для интеллектуального управления цифровыми рисками, способствующих повышению безопасности и эффективности управленческих процессов.

Задачами изучения дисциплины «Управление цифровыми рисками» являются:

Освоение основных концепций и принципов интеллектуального управления цифровыми рисками.

Изучение современных ИТ-инструментов и технологий, используемых для управления рисками.

Понимание применения ИИ для идентификации, анализа и смягчения цифровых рисков.

Освоение методов интегрированного управления рисками.

Изучение процессов управления ИТ-продуктами для минимизации цифровых рисков.

Понимание использования ИИ для оптимизации и управления бизнес-процессами.

Освоение методов обеспечения кибербезопасности и защиты данных.

Изучение нормативно-правовых аспектов и политик, регулирующих управление цифровыми рисками.

2. Место дисциплины в структуре ООП ВО

Дисциплина относится к части, формируемой участниками образовательных отношений.

Основывается на базе дисциплин: «Современные методы управления», «Основы цифровой экономики», «Организация производства и услуг в условиях цифровой экономики», «Современный стратегический анализ».

Является основой для изучения следующих дисциплин: «Экономика цифровой организации (предприятия)», «Стратегия цифровой трансформации бизнеса», «Цифровой маркетинг», «Цифровые финансы».

Дисциплина посвящена совершенствованию имеющихся и получению новых знаний и практических навыков студентов в области управления цифровыми рисками, а также использования цифровых технологий при дальнейшем трудоустройстве и ежедневной практике, получения новых профессиональных компетенций в области управления в цифровой экономике.

Рабочая программа «Управление цифровыми рисками» разработана с учётом: требований рынка труда, государственных образовательных стандартов высшего образования, квалификационных требований.

Курс «Управление цифровыми рисками» является необходимым для освоения универсальной компетенций по направлению подготовки 38.04.02 Менеджмент, а также, самостоятельного занятия научно-исследовательской работой студента и написания выпускной

квалификационной работы – магистерской диссертации.

Дисциплина реализуется кафедрой производственного менеджмента.

3. Требования к результатам освоения содержания дисциплины

Код и наименование компетенции	Индикаторы достижений компетенции (по реализуемой дисциплине)	Перечень планируемых результатов
УК-1. Способен осуществлять критический анализ проблемных ситуаций на основе системного подхода, вырабатывать стратегию действий	УК-1.1. Знает методы анализа проблемных ситуаций на основе системного подхода; УК-1.2. Умеет осуществлять поиск вариантов решения поставленной проблемной ситуации на основе доступных источников информации; УК-1.3. Владеет способами решения поставленных задач, оценивания их достоинства и недостатки;	знать: теоретические основы и понятийный аппарат анализа проблемных ситуаций на основе системного подход; уметь: применять аналитический поиска вариантов решения поставленной проблемной ситуации на основе доступных источников информации; владеть: организационными и технологическими методами, принципами и инструментами, способами решения поставленных задач, оценивания их достоинства и недостатки;

4. Структура и содержание дисциплины

4.1. Объем учебной дисциплины и виды учебной работы

Вид учебной работы	Объем часов (зач. ед.)	
	Очная форма	Заочная форма
Общая учебная нагрузка (всего)	144 (4 зач. ед)	144 (4 зач. ед)
Обязательная аудиторная учебная нагрузка (всего) в том числе:	60	14
Лекции	24	6
Семинарские занятия	-	-
Практические занятия	36	6
Лабораторные работы	-	-
Курсовая работа (курсовой проект)	-	-
Другие формы и методы организации образовательного процесса (<i>расчетно-графические работы, индивидуальные задания и т.п.</i>)	-	-
Самостоятельная работа студента	84	130

(всего)		
Форма аттестации	зачет	зачет

4.2. Содержание разделов дисциплины

Тема 1. Введение в управление цифровыми рисками.

Предмет курса и его связь со смежными дисциплинами. Библиография. Теория рисков. Риск и неопределенность. Классификация рисков. Природа рисков.

Тема 2. Основы интеллектуального управления цифровыми рисками.

Определение интеллектуального управления цифровыми рисками. Основные принципы и концепции интеллектуального управления цифровыми рисками. Примеры применения интеллектуального управления цифровыми рисками. Ключевые компоненты систем интеллектуального управления цифровыми рисками.

Тема 3. Информационные технологии и инструменты для управления рисками.

Основные информационные технологии для управления рисками. Роль информационных технологий в системе управления рисками. Инструменты для анализа и оценки рисков. Методики и алгоритмы для оценки и прогнозирования рисков. Интеграция информационных технологий в управление рисками. Способы интеграции информационных технологий в существующие системы управления рисками. Оценка эффективности интеграции технологий в управление рисками.

Тема 4. Искусственный интеллект в управлении цифровыми рисками

Определение роли искусственного интеллекта в управлении цифровыми рисками. Основные применения ИИ для анализа и прогнозирования цифровых рисков. Технологии и алгоритмы ИИ для управления рисками. Обзор технологий ИИ, применяемых в управлении цифровыми рисками. Преимущества и вызовы применения ИИ в управлении цифровыми рисками. Оценка влияния ИИ на эффективность управления цифровыми рисками.

Тема 5. Управление бизнес-процессами с использованием искусственного интеллекта

Определение управления бизнес-процессами с использованием искусственного интеллекта. Основные применения ИИ для оптимизации бизнес-процессов. Технологии и методологии ИИ для управления бизнес-процессами. Обзор технологий и методологий ИИ для управления бизнес-процессами. Применение алгоритмов ИИ для анализа и оптимизации бизнес-процессов. Управление информационно-технологическими продуктами. Инструменты и технологии для управления ИТ-продуктами. Методы планирования, внедрения и поддержки ИТ-продуктов. Анализ результатов и внедрение улучшений на основе данных и отзывов пользователей.

Тема 6. Кибербезопасность

Определение кибербезопасности и ее значение для обеспечения управления цифровыми рисками. Основные угрозы и риски кибербезопасности. Успешные практики обеспечения кибербезопасности. Обзор инструментов и

методов защиты информации. Методики защиты от киберугроз и атак. Методы оценки эффективности мер кибербезопасности. Анализ инцидентов и корректировка стратегий защиты. Оптимизация систем кибербезопасности.

4.3. Лекции

№ п/п	Название темы	Объем часов	
		Очная форма	Заочная форма
1	Введение в управление цифровыми рисками	4	1
2	Основы интеллектуального управления цифровыми рисками	4	1
3	Информационные технологии и инструменты для управления рисками	4	1
4	Искусственный интеллект в управлении цифровыми рисками	4	1
5	Управление бизнес-процессами с использованием искусственного интеллекта	4	1
6	Кибербезопасность	4	1
Итого:		24	6

4.4. Практические (семинарские) занятия

№ п/п	Название темы	Объем часов	
		Очная форма	Заочная форма
1	Введение в управление цифровыми рисками	6	1
2	Основы интеллектуального управления цифровыми рисками	6	1
3	Информационные технологии и инструменты для управления рисками	6	1
4	Искусственный интеллект в управлении цифровыми рисками	6	1
5	Управление бизнес-процессами с использованием искусственного интеллекта	6	1
6	Кибербезопасность	6	1
Итого:		36	6

4.6. Самостоятельная работа студентов

№ п/п	Название темы	Вид СРС	Объем часов	
			Очная форма	Заочная форма
1	Введение в управление цифровыми рисками	подготовка к текущей и промежуточной аттестации	4	8
2	Основы интеллектуального управления цифровыми рисками	подготовка к текущей и промежуточной аттестации	4	8
3	Информационные технологии	подготовка к	4	8

	и инструменты для управления рисками	текущей и промежуточной аттестации		
4	Искусственный интеллект в управлении цифровыми рисками	подготовка к текущей и промежуточной аттестации	4	8
5	Управление бизнес-процессами с использованием искусственного интеллекта	подготовка к текущей и промежуточной аттестации	4	8
6	Кибербезопасность	подготовка к текущей и промежуточной аттестации	4	8
Итого:			84	148

4.7. Курсовая работа не предусмотрена учебным планом

5. Формы контроля освоения дисциплины

Текущая аттестация студентов производится в дискретные временные интервалы лектором и преподавателем, ведущими лекционные и практические занятия по дисциплине в следующих формах:

вопросы для обсуждения (в виде докладов и сообщений);

вопросы к контрольным работам;

темы рефератов;

тестовый контроль.

Фонды оценочных средств, включающие типовые задания, контрольные работы, тесты и методы контроля, позволяющие оценить результаты текущей и промежуточной аттестации обучающихся по данной дисциплине, помещаются в приложении к рабочей программе в соответствии с «Положением о фонде оценочных средств».

Форма аттестации по результатам освоения дисциплины проходит в форме зачета. Студенты, выполнившие 75% текущих и контрольных мероприятий на «отлично», а остальные 25 % на «хорошо», имеют право на получение итоговой отличной оценки.

В экзаменационную ведомость и зачетную книжку выставляются оценки по шкале, приведенной в таблице.

Шкала оценивания	Характеристика знания предмета и ответов
зачтено	Студент глубоко и в полном объеме владеет программным материалом. Грамотно, исчерпывающе и логично его излагает в устной или письменной форме. При этом знает рекомендованную литературу, проявляет творческий подход в ответах на вопросы и правильно обосновывает принятые решения, хорошо владеет умениями и навыками при выполнении практических задач.

	Студент знает программный материал, грамотно и по сути излагает его в устной или письменной форме, допуская незначительные неточности в утверждениях, трактовках, определениях и категориях или незначительное количество ошибок. При этом владеет необходимыми умениями и навыками при выполнении практических задач.
	Студент знает только основной программный материал, допускает неточности, недостаточно четкие формулировки, непоследовательность в ответах, излагаемых в устной или письменной форме. При этом недостаточно владеет умениями и навыками при выполнении практических задач. Допускает до 30% ошибок в излагаемых ответах.
не зачтено	Студент не знает значительной части программного материала. При этом допускает принципиальные ошибки в доказательствах, в трактовке понятий и категорий, проявляет низкую культуру знаний, не владеет основными умениями и навыками при выполнении практических задач. Студент отказывается от ответов на дополнительные вопросы.

6. Учебно-методическое и информационное обеспечение дисциплины:

а) основная литература:

1. Курчеева, Г.И. Менеджмент в цифровой экономике: учебное пособие / Г.И. Курчеева, А.А. Алетдинова, Г.А. Клочков. – Новосибирск: Изд-во НГТУ, 2018. – 136 с.
2. Айдаркина, Е.Е. Теория и практика управления: учебное пособие / Е.Е. Айдаркина; Южный федеральный университет. – Ростов-на-Дону; Таганрог: Издательство Южного федерального университета, 2020. – 164 с.
3. Виханский, О.С. Менеджмент: учебник / О.С. Виханский, А.И. Наумов. – 6-е изд., перераб. и доп. – Москва: Магистр: ИНФРА-М, 2021. – 656 с.
4. Деминг, Э. Менеджмент нового времени: простые механизмы, ведущие к росту, инновациям и доминированию на рынке / Э. Деминг; пер. с англ. – Москва: Альпина Пабlisher, 2019. – 182 с.
5. Егоршин, А.П. Эффективный менеджмент организации: учебное пособие / А.П. Егоршин. – Москва: ИНФРА-М, 2021. – 388 с.
6. Кожевина, О.В. Управление изменениями: учебник / О.В. Кожевина. – 2-е изд., испр. и доп. – Москва: ИНФРА-М, 2019. – 304 с.
7. Цифровой бизнес: учебник / под науч. ред. О.В. Китовой. – Москва: ИНФРА-М, 2023. – 418 с. — (Высшее образование: Магистратура). — DOI 10.12737/textbook_5a0a8c777462e8.90172645. — ISBN 978-5-16-013017-0. — Текст: электронный. — URL: <https://znanium.com/catalog/product/1917620>.
8. Управление бизнесом в цифровой экономике: вызовы и решения: монография / под ред. И.А. Аренкова, Т.А. Лезиной, М.К. Ценжарик, Е.Г. Черновой. – Санкт-Петербург: СПбГУ, 2019. – 360 с. - ISBN 978-5-288-05966-7. - Текст: электронный. - URL: <https://znanium.com/catalog/product/1244177>.
9. Майклмен П. Цифровизация: Практические рекомендации по переводу бизнеса на цифровые технологии / П. Майклмен – Москва: Альпина

Публишер, 2019. – 252 с. - ISBN 978-5-9614-2849-0. – Текст: электронный // ЭБС "Консультант студента": [сайт]. - URL: <https://www.studentlibrary.ru/book/ISBN9785961428490.html>.

10. Информационные технологии в менеджменте (управлении): учебник и практикум для вузов / Ю.Д. Романова [и др.]; под редакцией Ю.Д. Романовой. – 2-е изд., перераб. и доп. – Москва: Издательство Юрайт, 2019. – 411 с. – (Высшее образование). – ISBN 978-5-534-11745-5. – Текст: электронный // ЭБС Юрайт [сайт]. – URL: <https://urait.ru/bcode/446052>.

11. Загеева, Л.А. Менеджмент в цифровой экономике: учебное пособие / Загеева Л.А., Маркова Е.С. – Липецк: Липецкий государственный технический университет, ЭБС АСВ, 2019. – 71 с. – ISBN 978-5-88247-977-9. – Текст: электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. – URL: <https://www.iprbookshop.ru/99162.html>.

б) дополнительная литература:

1. Абчук, В.А. Менеджмент в 2 ч. Часть 1: учебник и практикум для вузов / В.А. Абчук, С.Ю. Трапицын, В.В. Тимченко. – 3-е изд., испр. и доп. – Москва: Издательство Юрайт, 2020. – 239 с.

2. Абчук, В.А. Менеджмент в 2 ч. Часть 2: учебник и практикум для вузов / В.А. Абчук, С.Ю. Трапицын, В.В. Тимченко. – 3-е изд., испр. и доп. – Москва: Издательство Юрайт, 2021. – 249 с.

3. Курчеева, Г.И. Информационные технологии в цифровой экономике: учебное пособие / Г.И. Курчеева, И.Н. Томилов. – Новосибирск: Изд-во НГТУ, 2019. – 79 с.

4. Шаркова А.В. Развитие предпринимательства: концепции, цифровые технологии, эффективная система / А.В. Шаркова, М.А. Эскиндарова. – Москва: Дашков и К., 2019. – 605 с. – ISBN 978-5-394-03497-8. – Текст: электронный // ЭБС "Консультант студента": [сайт]. – URL: <https://www.studentlibrary.ru/book/ISBN9785394034978.html>.

5. Тихомирова, О.Г. Транзакционный менеджмент: геймификация управления компаниями и людьми: монография / О.Г. Тихомирова. – Москва: ИНФРА-М, 2021. – 178 с.

6. Мардас, А.Н. Основы менеджмента. Практический курс: учебное пособие для вузов / А.Н. Мардас, О.А. Гуляева. – 2-е изд., испр. и доп. – Москва: Издательство Юрайт, 2021. – 175 с.

в) Интернет-ресурсы:

Министерство образования и науки Российской Федерации – <http://минобрнауки.рф/>

Федеральная служба по надзору в сфере образования и науки – <http://obrnadzor.gov.ru/>

Министерство образования и науки Луганской Народной Республики – <https://minobr.su>

Информационно-аналитическая система – <http://www.spark-interfax.ru>

Информационная система «Единое окно доступа к образовательным ресурсам» – <http://window.edu.ru/>

Народный совет Луганской Народной Республики – <https://nslnr.su>

Портал Федеральных государственных образовательных стандартов высшего образования – <http://fgosvo.ru>

Федеральный портал «Российское образование» – <http://www.edu.ru/>

Федеральный центр информационно-образовательных ресурсов – <http://fcior.edu.ru/>

Электронно-библиотечная система «Консультант-студента» – <http://www.studentlibrary.ru/cgi-bin/mb4x>

Электронно-библиотечная система «StudMed.ru» – <https://www.studmed.ru>

Информационный ресурс библиотеки образовательной организации

Научная библиотека имени А. Н. Коняева – <http://biblio.dahluniver.ru/>

7. Материально-техническое и программное обеспечение дисциплины

Освоение дисциплины «Управление цифровыми рисками» предполагает использование академических аудиторий, соответствующих действующим санитарным и противопожарным правилам и нормам.

Прочее: рабочее место преподавателя, оснащенное компьютером с доступом в Интернет.

Программное обеспечение:

Функциональное назначение	Бесплатное программное обеспечение	Ссылки
Офисный пакет	Libre Office 6.3.1	https://www.libreoffice.org/ https://ru.wikipedia.org/wiki/LibreOffice
Операционная система	UBUNTU 19.04	https://ubuntu.com/ https://ru.wikipedia.org/wiki/Ubuntu
Браузер	Firefox Mozilla	http://www.mozilla.org/ru/firefox/fx
Браузер	Opera	http://www.opera.com
Почтовый клиент	Mozilla Thunderbird	http://www.mozilla.org/ru/thunderbird
Файл-менеджер	Far Manager	http://www.farmanager.com/download.php
Архиватор	7Zip	http://www.7-zip.org/
Графический редактор	GIMP (GNU Image Manipulation Program)	http://www.gimp.org/ http://gimp.ru/viewpage.php?page_id=8 http://ru.wikipedia.org/wiki/GIMP
Редактор PDF	PDFCreator	http://www.pdfforge.org/pdfcreator
Аудиоплеер	VLC	http://www.videolan.org/vlc/

8. Оценочные средства по дисциплине

Паспорт оценочных средств по учебной дисциплине «Управление цифровыми рисками»

Описание уровней сформированности и критериев оценивания
компетенций на этапах их формирования в ходе изучения дисциплины

Этап	Код компетенции	Уровни сформированности компетенции	Критерии оценивания компетенции
Начальный	УК-1. Способен осуществлять критический анализ проблемных ситуаций на основе системного подхода, вырабатывать стратегию действий	Пороговый	знать: теоретические основы и понятийный аппарат анализа проблемных ситуаций на основе системного подход;
Основной		Базовый	уметь: применять аналитический поиска вариантов решения поставленной проблемной ситуации на основе доступных источников информации;
Заключительный		Высокий	владеть: организационными и технологическими методами, принципами и инструментами, способами решения поставленных задач, оценивания их достоинства и недостатки;

Перечень компетенций (элементов компетенций), формируемых в результате освоения учебной дисциплины.

№ п/п	Код компетенции	Формулировка контролируемой компетенции	Индикаторы достижений компетенции (по дисциплине)	Темы учебной дисциплины	Этапы формирования (семестр изучения)
1.	УК-1	Способен осуществлять критический анализ проблемных ситуаций на основе системного подхода, вырабатывать стратегию действий	УК-1.1. Знает методы анализа проблемных ситуаций на основе системного подхода;	<i>Тема 1. Тема 2.</i>	2
			УК-1.2. Умеет осуществлять поиск вариантов решения поставленной проблемной ситуации на основе доступных источников информации;	<i>Тема 3. Тема 4.</i>	
			УК-1.3. Владеет способами решения поставленных задач, оценивания их достоинства и недостатки;	<i>Тема 5. Тема 6.</i>	

Показатели и критерии оценивания компетенций, описание шкал оценивания

№ п/п	Код компетенции	Индикаторы достижений компетенции	Планируемые результаты обучения по дисциплине	Контролируемые темы учебной дисциплины	Наименование оценочного средства
1.	УК-1. Способен осуществлять критический анализ проблемных ситуаций на основе системного	УК-1.1. Знает методы анализа проблемных ситуаций на основе системного подхода;	знать: теоретические основы и понятийный аппарат управления проектом на всех этапах его жизненного цикла; уметь: применять на практике информационные и телекоммуникационные технологии контроля логистических бизнес-процессов; владеть: методами оценки логистических рисков с помощью инновационных информационных технологий;	Тема 1. Тема 2.	Контрольные вопросы и задания, тестовые задания, разноуровневые задачи, практическое (прикладное задание)
		УК-1.2. Умеет осуществлять поиск вариантов решения поставленной проблемной ситуации на основе доступных источников информации;	знать: закономерности и особенности развития всех этапов жизненного цикла управления проектом; уметь: использовать инструменты и методы управления, современные информационные технологии для решения задач профессиональной деятельности;	Тема 3. Тема 4.	Контрольные вопросы и задания, тестовые задания, разноуровневые задачи, практическое (прикладное задание)

		УК-1.3. Владеет способами решения поставленных задач, оценивания их достоинства и недостатки;	знать: методы анализа управления рисками на различных этапах жизненного цикла проекта; уметь: эффективно выбирать и анализировать альтернативные варианты проектов для достижения намеченных результатов; владеть: приемами анализа рисков с помощью инновационных информационных технологий;	Тема 5. Тема 6.	Контрольные вопросы и задания, тестовые задания, разноуровневые задачи, практическое задание (прикладное задание)
--	--	---	---	--	--

1. Типовые тестовые задания (базовый уровень)

1. Комплексная программа управления рисками должна устанавливать единую структуру при работе с рисками и начинаться со стадии:

- А) идентификация рисков
- Б) система по анализу риска
- В) сбор информации по рискам
- Г) предварительная оценка рисков

2. Уровень риска, который является приемлемым, для конкретных условий определенной ситуации, с точки зрения критериев риска – это.....уровень риска:

- А) остаточный
- Б) оцененный
- В) конечный

3. Дерево решений (анализ дерева решений АДР) имеет ...

- А) три элемента
- Б) пять элементов
- Г) восемь элементов

4. Качественный и количественный анализы рисков – это ...

- А) последовательно идущие стадии одного процесса по работе с рисками, но количественный этап следует после качественного анализа
- Б) самостоятельные и не зависящие друг от друга процессы
- В) взаимодополняющие процессы, в которых количественный анализ выполняется первым

5. Итогом процесса обработки риска является ...
- А) решение о том, до какой степени детализации и дальнейших действий над ним, необходимо будет подвергнуть тот или иной риск
 - Б) план действий по решению устранения последствий риска
 - В) составление списка возможных рисков
6. Стандарт COBIT 5 for RISK (RiskIT) рассматривает подход к управлению рисками с ... аспектов
- А) двух
 - Б) трех
 - В) четырех
 - Г) пяти
7. Своп – это ...
- А) торгово-финансовая обменная операция
 - Б) операционная система
 - В) производный финансовый инструмент
 - Г) стоимостная мера риска
8. Неверно, что к ключевым элементам OCTAVE относится: ...
- А) идентификация информационных активов, подверженных риску и ущербу
 - Б) идентификация угроз для критичных информационных активов
 - В) определение уязвимости, ассоциированных с критичными информационными активами количественная оценка рисков
9. По характеру риски делятся на ... риски
- А) организационные, процессные, проектные и операционные
 - Б) чистые и спекулятивные
 - В) внешние и внутренние
 - Г) ретроспективные, текущие и перспективные
10. Термин «риск» произошел от французского слова *risqué* или итальянского *risico*, которое означает ...
- А) возможность или вероятность наступления событий с конкретными последствиями в результате определенных решений или действий
 - Б) предотвращение наступления конкретных и максимально возможных событий
 - В) максимально вероятные последствия в следствии конкретных рисков

Тесты:

(пороговый уровень)

1. У любого риска есть:
- А) причины и последствия
 - Б) только причины и вероятность

- В) только последствия и ущерб
- Г) факторы и следствия

2. Абсолютные показатели оценки риска основаны на:

- А) распределении прогнозируемых значений показателей
- Б) субъективных оценках величины риска
- В) фактических показателях финансовой документации

3. Реальное влияние при управлении по целям имеют руководители уровня:

- А) среднего
- Б) низшего
- В) высшего

4. Принятие рискового решения в управленческой практике должно осуществляться:

- А) только коллегиально
- Б) финансовым менеджером (риск-менеджером) единолично
- В) совместно

5. Виды анализа рисков:

- А) количественный и качественный
- Б) имитационное моделирование, количественный и качественный
- В) имитационное моделирование и качественный

6. Последствия риска могут быть:

- А) скорее положительными
- Б) как положительными, так и отрицательными
- В) только отрицательными

7. Риск – это:

- А) разновидность ситуации, объективно содержащая высокую вероятность невозможности осуществления цели
- Б) наличие факторов, при которых результаты действий не являются детерминированными, а степень возможного влияния этих факторов на результаты неизвестна
- В) следствие действия либо бездействия, в результате которого существует реальная возможность получения неопределенных результатов различного характера

8. Функциями субъекта управления в риск-менеджменте не является:

- А) прогнозирование
- Б) нормирование
- В) регулирование

9. Идентификация риска это:

- А) систематизация множества рисков на основании каких-либо признаков и критериев, позволяющих объединить подмножества рисков в более общие понятия
- Б) начальный этап системы мероприятий по управлению рисками, состоящий в систематическом выявлении рисков, характерных для определенного вида деятельности, и определении их характеристик
- В) систематическое научное исследование степени риска, которому подвержены конкретные объекты, виды деятельности и проекты

10. Мониторинг рисков это:

- А) периодический пересмотр рисков компании с целью корректировки их оценок, выявления новых рисков и оценки эффективности внедряемых мероприятий
- Б) анализ рисков с целью определения наиболее критичных с точки зрения вероятности и ущерба
- В) определение факторов и событий, которые могут негативно повлиять на цели компании

11. Правилами риск-менеджмента не является:

- А) риск - дело благородное
- Б) нельзя рисковать многим ради малого
- В) нельзя рисковать многим ради малого

12. Ключевая особенность современного подхода к управлению рисками заключается

- А) рассмотрении как позитивных, так и негативных рисков
- Б) наличии наработок, позволяющих определить возможные риски для каждой из отраслей
- В) использовании самых современных и точных математических методов

13. Конечной целью управления риском является:

- А) получение большей информации
- Б) перенос риска на другое лицо
- В) составление базы данных о рисках

14. Культура управления рисками это:

- А) создание в организации среды, способствующей выявлению, оценке и снижению рисков
- Б) разработка и внедрение мероприятий, которые могут исключить либо снизить уровень риска

В) периодический пересмотр рисков компании с целью корректировки их оценок,
выявления новых рисков

15. Выявление рисков это:

- А) определение факторов и событий, которые могут негативно повлиять на цели компании
- Б) определение уровня ущерба от риска и вероятности его наступления
- В) процесс минимизации рисков

16. Минимизация риска это:

- А) разработка и реализация мероприятий, направленных на предотвращение риска либо на снижение его последствий
- Б) перенос риска на третью сторону посредством заключения юридически обязывающих документов
- В) принятие риска

17. Реагирование на риски это:

- А) разработка и внедрение мероприятий, которые могут исключить либо снизить уровень риска
- Б) анализ рисков с целью определения наиболее критичных с точки зрения вероятности и ущерба
- В) определение факторов и событий, которые могут негативно повлиять на цели компании

18. Для рисков ситуации характерно

- А) наличие возможности отказа от принятого решения
- Б) отсутствие альтернативных решений
- В) наличие альтернативных решений

19. Главной функцией риск-менеджмента является:

- А) предотвращение банкротства компании в результате наступления случайных событий
- Б) оценка риска по каждому проекту в компании
- В) оценка риска для компании в целом

20. Показатели оценки риска делятся на группы:

- А) относительные, вероятностные, в условиях определённости
- Б) средние, статистические, экспертные
- В) в условиях определённости, в условиях частичной неопределённости, в условиях полной неопределённости

Методические рекомендации:

При использовании формы текущего контроля «Тестирование» студентам могут быть предложены задания на бумажном носителе.

Критерии и шкала оценивания по оценочному средству «Тесты»

Шкала оценивания (интервал баллов)	Критерий оценивания
5	Тесты выполнены на высоком уровне (правильные ответы даны на 90-100% тестов)
4	Тесты выполнены на среднем уровне (правильные ответы даны на 75-89% тестов)
3	Тесты выполнены на низком уровне (правильные ответы даны на 50-74% тестов)
2	Тесты выполнены на неудовлетворительном уровне (правильные ответы даны менее чем на 50% тестов)

2. Разноуровневые задачи и задания (базовый уровень)

Задание 1. Имеются данные о потерях, возникающие из-за отказа серверного оборудования. Оценить степень риска возникновения потерь.

Потери	Случаи возникновения потерь						
	1	2	3	4	5	6	7
Web-ресурс №1							
Web-ресурс №2							

Задание 2. Выручка оператора информационных ресурсов составляет 900 тыс. ден. ед., переменные затраты – 200 тыс. ден. ед., постоянные затраты – 270 тыс. ден. ед. Необходимо определить запас финансовой прочности. Оценить на сколько процентов изменится прибыль предприятия, если эксперты оценивают снижения спроса на услуги оператора информационных ресурсов на 15%? Какой процент прибыли удастся сохранить предприятию, если выручка упадет на 40%? Каким должен быть процент снижения выручки, при котором оператор информационных ресурсов полностью лишится прибыли?

Задание 3. Дайте определение и приведите пример понятий «риск» и «рискообразующий фактор».

На основании материала по истории теории риска постройте хронологию ключевых этапов развития теории. Дайте краткую биографическую справку для основоположников теории риска, охарактеризуйте их научный вклад.

Проанализируйте современные концепции менеджмента риска укажите специфические черты, достоинства и недостатки каждого из перечисленных подходов.

Изучите критерии выбора моделей менеджмента риска для различных категорий задач в сфере разработки, внедрения и использования информационных технологий.

Задачи и задания (высокий уровень)

Задание 1. Описание ситуации. Системный интегратор «Big&Co» был выбран в качестве генерального подрядчика по проекту внедрения информационной системы (ИС) в компании «Client Company». В соответствии с договором работы проводились в три этапа:

- 1) выбор решения и поставка ПО;
- 2) внедрение ИС;
- 3) постпроектное сервисное обслуживание.

Руководителем второго этапа работ был назначен Василий из числа менеджеров проектов «Big&Co». К моменту назначения Василия первый этап был уже завершен:

определен класс и вендор внедряемой ИС, ПО поставлено в соответствии со спецификацией.

Для выполнения работ второго этапа со стороны «Big&Co» были выделены архитектор ИТ-решения и консультант по внедрению ИС. Вместе с ними Василий разработал план-график

предстоящих работ, согласовал его с представителями «Client Company» внутри «Big&Co».

В соответствии с утвержденным планом было произведено проектирование ИС, разработано и согласовано с заказчиком техническое задание, после чего консультант по внедрению приступил к работе по настройке системы. По согласованному плану внедрение предполагалось вести поэтапно, при этом часть работ по подготовке системы к внедрению брал на себя заказчик.

Таким образом, ответственность за различные этапы работ возлагалась попеременно то на специалистов компании заказчика, то на специалистов компании-исполнителя.

График работ был построен так, что зачастую приступить к исполнению очередной операции было невозможно до завершения предшествующей.

Приступив работам, консультант по внедрению «Big&Co» обнаружил и сразу проинформировал Василия, что специалисты «Client Company» не могут уделять проектным работам достаточно времени, ссылаясь на недоукомплектованность штата, повышенную загрузку операционными задачами и низкий приоритет проекта.

Выполнение проектных работ стало затягиваться, возникла опасность срыва сроков, отношение сотрудников «Client Company» к проекту ухудшилось. Василий переговорил с представителем компании-заказчика и получил

заверения, что меры будут приняты. Вскоре выяснилось, что ситуация не изменилась. Василий повторно проинформировал «Client Company» и снова получил от вет, что проблема будет решена в кратчайшие сроки.

Консультант по внедрению тем временем докладывал, что на объектах он часть времени бездействует, ожидая, пока технические специалисты «Client Company» освободятся и смогут выполнить свою долю работ, предусмотренную согласованным планом.

Без их участия выполнить настройки ИС было невозможно, так как консультант «Big&Co», в соответствии с положениями политики по информационной безопасности Client Company, не имел прав доступа к модулю настройки внедряемой ИС. Предложение о предоставлении этих полномочий было не раз отвергнуто представителями «Client Company».

В этих условиях Василий принял решение об эскалации проблемы на уровень старшего менеджера из отдела продаж - Петра. Доложив Петру о ситуации, он предложил собрать рабочее совещание с привлечением высшего руководства «Client Company», чтобы найти выход. Петр высказал сомнение в пользе такого совещания и предоставил Василию карт-бланш, посоветовав решать проблему самостоятельно. Василий еще раз связался с представителями «Client Company» и предложил определить ключевые вехи, достижение которых позволило бы закрыть второй этап договора, а оставшуюся часть работ провести на этапе сервисного обслуживания.

Компромисс был найден, но: по причине выявленной некорректной работы внедряемой ИС отставание по срокам ликвидировать не удалось, а неприятие проекта сотрудниками «Client Company» усугубилось; ресурсы заметную часть времени использовались неэффективно; вследствие затягивания работ возникли накладки с планированием ресурсов и сбои по срокам в других проектах; в связи с падением выручки «Client Company», вызванным неблагоприятной экономической конъюнктурой, финансирование проекта было урезано.

Задание к выполнению работы

На основе приведенной информации о проекте и, при необходимости, дополнительных допущений идентифицируйте и классифицируйте риски (6-8 шт.) данного проекта.

Задание 3.

1. Загрузите ГОСТ Р ИСО/МЭК ТО 13335-3-2007 «МЕТОДЫ И СРЕДСТВА ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ. Часть 3 «Методы менеджмента безопасности информационных технологий».

2. Ознакомьтесь с Приложениями С, D и E ГОСТа.
3. Выберите три различных информационных актива организации.
4. Из Приложения D ГОСТа подберите три конкретных уязвимости системы защиты указанных информационных активов.
5. Пользуясь Приложением С ГОСТа напишите три угрозы, реализация которых возможна пока в системе не устранены названные в пункте 4 уязвимости.
6. Пользуясь одним из методов, предложенных в Приложении Е ГОСТа, произведите оценку рисков информационной безопасности.
7. Оценку ценности информационного актива производить на основании возможных потерь для организации в случае реализации угрозы.

3. Контрольные вопросы (базовый уровень)

1. Основные концепции и принципы разработки и внедрения информационно-технологических продуктов.
2. Методы и алгоритмы искусственного интеллекта, применимые для оптимизации и повышения эффективности бизнес-процессов.
3. Текущие тенденции и инновации в области информационных технологий и их влияние на бизнес-процессы.
4. Информационно-технологические продукты с использованием методов искусственного интеллекта, учитывающие потребности бизнеса.
5. Информационно-технологические решения, существующие для повышения эффективности бизнес-процессов.
6. Оцените влияние внедренных информационно-технологических продуктов на эффективность бизнес-процессов.

Контрольные вопросы (высокий уровень)

1. Поясните навыки работы с инструментами и платформами для разработки и внедрения информационно-технологических продуктов, включая системы управления проектами и инструменты разработки искусственного интеллекта.
2. Методы и технологии искусственного интеллекта и их применения в контексте бизнес-процессов.
3. Проекты по разработке и внедрению информационно-технологических продуктов, обеспечивающие их успешное завершение в рамках заданных сроков и бюджетов.
4. Основные концепции и методы бизнес-процессов, а также их роли и значимости в организации.
5. Принципы и технологии искусственного интеллекта для анализа и оптимизации бизнес-процессов.

6. Стратегические цели организации и способы интеграции искусственного интеллекта в бизнес-процессы для их достижения.
7. Анализ текущих бизнес-процессов, выявление их недостатков и возможностей для улучшения с помощью искусственного интеллекта.
8. Решения на основе искусственного интеллекта для оптимизации бизнес-процессов и их соответствие стратегическим целям организации.
9. Интеграция инструментов искусственного интеллекта и решений в существующие бизнес-процессы, координация их работы в различных подразделениях и обеспечение их синхронизации.

Критерии и шкала оценивания по оценочному средству «Контрольные вопросы»

Шкала оценивания (интервал баллов)	Критерий оценивания
5	Студент в полном объеме осветил рассматриваемую проблематику, привел аргументы в пользу своих суждений, владеет профильным понятийным (категориальным) аппаратом и т.п.)
4	Студент в целом осветил рассматриваемую проблематику, привел аргументы в пользу своих суждений, допустив некоторые неточности и т.п.)
3	Студент допустил существенные неточности, изложил материал с ошибками, не владеет в достаточной степени профильным категориальным аппаратом и т.п.)
2	Раскрытие вопроса представлено на неудовлетворительном уровне или не представлено (студент не готов, не выполнил задание и т.п.)

Тематика контрольных работ:

1. Работа с платформами корпоративного управления, управления рисками и соблюдение требований.
2. Примените техники разработки и реализации стратегий управления рисками.
3. Методы мониторинга и оценки эффективности мер по управлению рисками.
4. Методы и инструменты мониторинга рисков в реальном времени, такие как системы контроля и отчетности.
5. Принципы и стандарты отчетности по управлению рисками.
6. Информационные технологии для автоматизации мониторинга и отчетности по рискам.
7. Системы мониторинга для отслеживания рисков и их изменений в режиме реального времени.
8. Генерация и интерпретация отчетов по управлению рисками с использованием специализированного ПО.
9. Представление результатов мониторинга и отчетности заинтересованным сторонам.

10. Использование ИТ-инструментов для мониторинга рисков.
11. Техника составления отчетов и представления данных о рисках.
12. Методы визуализации и презентации данных для отчетности по управлению рисками.

Критерии и шкала оценивания по оценочному средству «Контрольная работа»

Шкала оценивания (интервал баллов)	Критерий оценивания
5	Контрольная работа выполнена на высоком уровне (правильные ответы даны на 90-100% вопросов/задач)
4	Контрольная работа выполнена на среднем уровне (правильные ответы даны на 75-89% вопросов/задач)
3	Контрольная работа выполнена на низком уровне (правильные ответы даны на 50-74% вопросов/задач)
2	Контрольная работа выполнена на неудовлетворительном уровне (правильные ответы даны менее чем на 50%)

Оценочные средства промежуточной аттестации (зачет)

Теоретические вопросы:

1. Основные виды и категории рисков, присущие бизнес-процессам и ИТ-системам.
2. Современные информационные технологии и инструменты для идентификации и оценки рисков, такие как системы управления рисками и аналитические платформы.
3. Методы и модели оценки рисков, включая количественный и качественный анализ рисков.
4. ИТ-инструменты для выявления потенциальных рисков и их анализа.
5. Оценка степень вероятности и возможные последствия рисков с помощью специализированного ПО.
6. Разработка карты рисков и оценку ее влияния на бизнес-процессы.
7. Работы с системами управления рисками.
8. Техники количественного и качественного анализа рисков с использованием ИТ-инструментов.
9. Методы визуализации данных для представления карт рисков и отчетов.
10. Основные подходы и методы управления рисками, такие как избегание, снижение, передача и принятие рисков.
11. Охарактеризуйте информационные системы и платформы для мониторинга и управления рисками.
12. Принципы стратегий и планов реагирования на риски.
13. Стратегии управления рисками с использованием информационных технологий.
14. Оценка эффективности реализованных стратегий и корректировка их по мере необходимости.

15. Характеристика информационных систем для мониторинга выполнения планов управления рисками.
16. Определение роли искусственного интеллекта в управлении цифровыми рисками.
17. Основные применения ИИ для анализа и прогнозирования цифровых рисков.
18. Технологии и методологии ИИ для управления бизнес-процессами.
19. Методы планирования, внедрения и поддержки ИТ-продуктов.
20. Анализ результатов и внедрение улучшений на основе данных и отзывов пользователей.
21. Определение кибербезопасности и ее значение для обеспечения управления цифровыми рисками.
22. Основные угрозы и риски кибербезопасности. Успешные практики обеспечения кибербезопасности.
23. Обзор инструментов и методов защиты информации. Методики защиты от киберугроз и атак.
24. Методы оценки эффективности мер кибербезопасности.
25. Анализ инцидентов и корректировка стратегий защиты. Оптимизация систем кибербезопасности.

Критерии и шкала оценивания по оценочному средству «Зачет»

Шкала оценивания	Характеристика знания предмета и ответов
зачтено	Студент глубоко и в полном объеме владеет программным материалом. Грамотно, исчерпывающе и логично его излагает в устной или письменной форме. При этом знает рекомендованную литературу, проявляет творческий подход в ответах на вопросы и правильно обосновывает принятые решения, хорошо владеет умениями и навыками при выполнении практических задач.
	Студент знает программный материал, грамотно и по сути излагает его в устной или письменной форме, допуская незначительные неточности в утверждениях, трактовках, определениях и категориях или незначительное количество ошибок. При этом владеет необходимыми умениями и навыками при выполнении практических задач.
	Студент знает только основной программный материал, допускает неточности, недостаточно четкие формулировки, непоследовательность в ответах, излагаемых в устной или письменной форме. При этом недостаточно владеет умениями и навыками при выполнении практических задач. Допускает до 30% ошибок в излагаемых ответах.
не зачтено	Студент не знает значительной части программного материала. При этом допускает принципиальные ошибки в доказательствах, в трактовке понятий и категорий, проявляет низкую культуру знаний, не владеет основными умениями и навыками при выполнении практических задач. Студент отказывается от ответов на дополнительные вопросы.

Лист изменений и дополнений

№ п/п	Виды дополнений и изменений	Дата и номер протокола заседания кафедры (кафедр), на котором были рассмотрены и одобренны изменения и дополнения	Подпись (с расшифровкой) заведующего кафедрой (заведующих кафедрами)