

**Министерство науки и высшего образования Российской Федерации  
Федеральное государственное бюджетное образовательное учреждение высшего  
образования  
«ИРКУТСКИЙ НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ ТЕХНИЧЕСКИЙ  
УНИВЕРСИТЕТ»**

Структурное подразделение «Сибирская школа геонаук (119)»

**УТВЕРЖДЕНА:**  
на заседании ДОТ  
Протокол №29 от 10 апреля 2025 г.

**Рабочая программа дисциплины**

**«НАДЕЖНОСТЬ ИНФОРМАЦИОННЫХ СИСТЕМ / RELIABILITY OF INFORMATION  
SYSTEMS»**

---

Направление: 09.03.02 Информационные системы и технологии

---

Информационные технологии в науках о Земле и окружающей среде / Information  
Technologies in Earth and Environmental Sciences

---

Квалификация: Бакалавр

---

Форма обучения: очная

---

Документ подписан простой  
электронной подписью  
Составитель программы:  
Ланько Анна Викторовна  
Дата подписания: 13.12.2025

Документ подписан простой  
электронной подписью  
Утвердил: Ланько Анна  
Викторовна  
Дата подписания: 13.12.2025

Документ подписан простой  
электронной подписью  
Согласовал: Паршин  
Александр Вадимович  
Дата подписания: 13.01.2026

Год набора – 2025

Иркутск, 2025 г.



## **1 Перечень планируемых результатов обучения по дисциплине, соотнесённых с планируемыми результатами освоения образовательной программы**

**1.1 Дисциплина «Надежность информационных систем / Reliability of Information Systems» обеспечивает формирование следующих компетенций с учётом индикаторов их достижения**

Код, наименование компетенции	Код индикатора компетенции
ПКС-4 Способность управлять проектами в области информационных технологий, обеспечивая выполнение всех этапов проекта в рамках утвержденных параметров	ПКС-4.5

**1.2 В результате освоения дисциплины у обучающихся должны быть сформированы**

Код индикатора	Содержание индикатора	Результат обучения
ПКС-4.5	Способность идентифицировать риски ИТ-проектов посредством анализа возможностей реализации требований к программному обеспечению	<b>Знать</b> Основные принципы надежности ИС (доступность, целостность, отказоустойчивость), типы рисков ИТ-проектов (технические, операционные, связанные с ПО), модели оценки рисков, требования к ПО (функциональные, нефункциональные) и их влияние на реализацию проектов. <b>Уметь</b> Идентифицировать риски ИТ-проектов через анализ требований к ПО, оценивать вероятность и воздействие сбоев, разрабатывать матрицы рисков и планы минимизации для обеспечения этапов проекта. <b>Владеть</b> навыками анализа рисков, инструментами для моделирования сценариев и мониторинга надежности ИС.

## **2 Место дисциплины в структуре ООП**

Изучение дисциплины «Надежность информационных систем / Reliability of Information Systems» базируется на результатах освоения следующих дисциплин/практик: «Архитектура информационных систем / Information System Architecture», «Инфокоммуникационные системы и сети / Infocommunication Systems and Networks», «Проектирование информационных систем / Information Systems Design»

Дисциплина является предшествующей для дисциплин/практик: «Производственная практика: преддипломная практика / Manufacturing Practice: Undergraduate Practice»

## **3 Объем дисциплины**

Объем дисциплины составляет – 3 ЗЕТ

Вид учебной работы	Трудоемкость в академических часах (Один академический час соответствует 45 минутам астрономического часа)	
	Всего	Семестр № 8
Общая трудоемкость дисциплины	108	108
Аудиторные занятия, в том числе:		
лекции	13	13
лабораторные работы	26	26
практические/семинарские занятия	0	0
Самостоятельная работа (в т.ч. курсовое проектирование)	69	69
Трудоемкость промежуточной аттестации	0	0
Вид промежуточной аттестации (итогового контроля по дисциплине)	Зачет	Зачет

#### 4 Структура и содержание дисциплины

##### 4.1 Сводные данные по содержанию дисциплины

###### Семестр № 8

№ п/п	Наименование раздела и темы дисциплины	Виды контактной работы						СРС		Форма текущего контроля
		Лекции		ЛР		ПЗ(СЕМ)				
№	Кол. Час.	№	Кол. Час.	№	Кол. Час.	№	Кол. Час.	№	Кол. Час.	
1	2	3	4	5	6	7	8	9	10	11
1	1. Принципы надежности ИС.	1	1					2	9	Устный опрос
2	2. Требования к ПО и их риски.	2	2							Устный опрос
3	3. Типы рисков ИТ-проектов.	3	2	1, 2	4					Устный опрос
4	4. Методы идентификации рисков.	4	2	3, 4	8					Устный опрос
5	5. Оценка вероятности и воздействия рисков.	5	2	5, 6	6			1, 3	20	Устный опрос
6	6. Планы минимизации рисков.	6	2	7, 8	4			1, 3	15	Устный опрос
7	7. Управление рисками в информационно- технологических проектах.	7	2	9, 10	4			1, 3, 4	25	Устный опрос
	Промежуточная аттестация									Зачет
	Всего		13		26				69	

##### 4.2 Краткое содержание разделов и тем занятий

## **Семестр № 8**

<b>№</b>	<b>Тема</b>	<b>Краткое содержание</b>
1	1. Принципы надежности ИС.	Доступность, целостность, отказоустойчивость, метрики надежности (MTBF, MTTR), влияние на ИТ-проекты.
2	2. Требования к ПО и их риски.	Функциональные и нефункциональные требования, анализ возможностей реализации, связь с параметрами проекта.
3	3. Типы рисков ИТ-проектов.	Технические, операционные, связанные с программным обеспечением, модели рисков (стандарт ISO 31000, руководство PMBOK).
4	4. Методы идентификации рисков.	Анализ сильных и слабых сторон, возможностей и угроз (SWOT), анализ видов и последствий отказов для программного обеспечения (FMEA), анализ опасностей и операбельности для программного обеспечения (HAZOP), мозговой штурм.
5	5. Оценка вероятности и воздействия рисков.	Матрицы рисков, количественные методы (метод Монте-Карло), триггеры рисков.
6	6. Планы минимизации рисков.	Стратегии (избегание, трансфер, принятие), мониторинг в рамках этапов проекта.
7	7. Управление рисками в информационно-технологических проектах.	Интеграция в этапы (руководство PMBOK), аудит надежности информационных систем, отчетность.

## **4.3 Перечень лабораторных работ**

### **Семестр № 8**

<b>№</b>	<b>Наименование лабораторной работы</b>	<b>Кол-во академических часов</b>
1	Лабораторная работа 1: Классификация рисков информационно-технологического проекта по типам.	2
2	Лабораторная работа 2: Анализ требований к программному обеспечению на предмет рисков.	2
3	Лабораторная работа 3: Построение анализа сильных и слабых сторон, возможностей и угроз (SWOT) для информационно-технологического проекта.	4
4	Лабораторная работа 4: Анализ видов и последствий отказов (FMEA) требований программного обеспечения.	4
5	Лабораторная работа 5: Составление матрицы рисков проекта.	4
6	Лабораторная работа 6: Моделирование рисков методом Монте-Карло в Microsoft Excel.	2
7	Лабораторная работа 7: Разработка плана минимизации рисков.	2
8	Лабораторная работа 8: Создание регистра	2

	рисков в Jira или Microsoft Project.	
9	Лабораторная работа 9: Анализ рисков на этапе реализации программного обеспечения.	2
10	Лабораторная работа 10: Оценка надежности информационных систем по метрикам (среднее время наработки на отказ - MTBF, среднее время восстановления - MTTR).	2

#### 4.4 Перечень практических занятий

Практических занятий не предусмотрено

#### 4.5 Самостоятельная работа

##### Семестр № 8

№	Вид СРС	Кол-во академических часов
1	Оформление отчетов по лабораторным и практическим работам	30
2	Подготовка к зачёту	9
3	Подготовка к практическим занятиям (лабораторным работам)	20
4	Подготовка к сдаче и защите отчетов	10

В ходе проведения занятий по дисциплине используются следующие интерактивные методы обучения: работа в малых группах

#### 5 Перечень учебно-методического обеспечения дисциплины

##### 5.1 Методические указания для обучающихся по освоению дисциплины

###### 5.1.1 Методические указания для обучающихся по лабораторным работам:

Лабораторная работа №1. Классификация рисков информационно-технологического проекта по типам.

Цель работы: Освоить типологию рисков информационно-технологических проектов.

Ход выполнения:

- Выберите типичный ИТ-проект (разработка веб-приложения, мобильного приложения или корпоративной системы).
- Изучите описание проекта (техническое задание или кейс).
- Составьте список из 20–25 потенциальных рисков.
- Классифицируйте риски по типам: технические (сбои оборудования, несовместимость ПО), операционные (недостаток персонала, задержки поставок), связанные с программным обеспечением (ошибки кода, несоответствие требованиям).
- Заполните таблицу: №, описание риска, тип, примеры проявления.
- Сделайте выводы о доминирующих типах рисков для выбранного проекта.

Предполагаемый результат: Таблица классификации рисков с примерами (2–3 стр.).

Контрольные вопросы:

- Чем отличаются технические риски от операционных?
- Какие риски связаны с программным обеспечением?
- Роль классификации в управлении проектом.

Лабораторная работа №2. Анализ требований к программному обеспечению на предмет

рисков.

Цель работы: Научиться выявлять риски в требованиях к программному обеспечению.

Ход выполнения:

1. Получите спецификацию ПО (функциональные и нефункциональные требования).
2. Разделите требования на категории: функциональные (что делает система), нефункциональные (производительность, безопасность, масштабируемость).
3. Для каждого требования оцените: сложность реализации, неопределенность, возможные конфликты.
4. Выделите проблемные требования и опишите связанные риски (например, "требование к обработке 10000 одновременных пользователей - риск перегрузки сервера").
5. Составьте таблицу: требование, риск, вероятность (низкая/средняя/высокая), воздействие.
6. Предложите уточнения для рискованных требований.

Предполагаемый результат: Отчет с перечнем рисков требований (таблица + рекомендации).

Контрольные вопросы:

7. Что такое функциональные и нефункциональные требования?
8. Как требования влияют на параметры проекта?
9. Примеры рисков в требованиях к программному обеспечению.

Лабораторная работа №3. Построение анализа сильных и слабых сторон, возможностей и угроз (SWOT) для информационно-технологического проекта.

Цель работы: Освоить метод анализа сильных и слабых сторон, возможностей и угроз (SWOT) для идентификации рисков.

Ход выполнения:

1. Определите проект и его контекст (внутренняя/внешняя среда).
2. Заполните матрицу 2×2:
  - о Сильные стороны (Strengths): опыт команды, готовые технологии.
  - о Слабые стороны (Weaknesses): ограниченный бюджет, неопытный персонал.
  - о Возможности (Opportunities): новые рынки, технологии.
  - о Угрозы (Threats): конкуренты, изменения законодательства.
3. Для каждой угрозы оцените вероятность превращения в риск.
4. Составьте список приоритетных рисков из анализа угроз.
5. Постройте диаграмму или таблицу с выводами.

Предполагаемый результат: Матрица анализа сильных и слабых сторон, возможностей и угроз (SWOT) с выводами (1 стр.).

Контрольные вопросы:

6. Зачем используется анализ сильных и слабых сторон, возможностей и угроз (SWOT)?
7. Как угрозы превращаются в риски проекта?
8. Примеры сильных сторон информационно-технологического проекта.

Лабораторная работа №4. Анализ видов и последствий отказов (FMEA) требований программного обеспечения.

Цель работы: Изучить анализ видов и последствий отказов (FMEA) для программного обеспечения.

Ход выполнения:

1. Выберите 5–7 ключевых требований ПО.
2. Для каждого требования определите возможные виды отказов (например, "неверная авторизация").
3. Оцените по шкале 1–10:
  - о Серьезность (Severity) - последствия отказа.

- o Происхождение (Occurrence) - вероятность отказа.
  - o Обнаружение (Detection) - вероятность выявления.
4. Рассчитайте индекс приоритета риска ( $RPN = S \times O \times D$ ).
  5. Отсортируйте по убыванию  $RPN$ , предложите меры снижения.
  6. Заполните стандартную таблицу FMEA.

Предполагаемый результат: Таблица анализа видов и последствий отказов (FMEA) с расчетами  $RPN$ .

Контрольные вопросы:

7. Что такое индекс приоритета риска ( $RPN$ )?
8. Этапы анализа видов и последствий отказов (FMEA)?
9. Применение анализа видов и последствий отказов (FMEA) в информационно-технологических проектах.

Лабораторная работа №5. Составление матрицы рисков проекта.

Цель работы: Научиться оценивать вероятность и воздействие рисков.

Ход выполнения:

1. Возьмите список из 15–20 рисков из предыдущих работ.
2. Оцените каждый риск:
  - o Вероятность (низкая 1–3, средняя 4–6, высокая 7–10).
  - o Воздействие (низкое 1–3, среднее 4–6, критическое 7–10).
3. Рассчитайте уровень риска (вероятность  $\times$  воздействие).
4. Постройте матрицу  $5 \times 5$  с цветовой маркировкой (зеленый/желтый/красный).
5. Выделите 5–7 высокоприоритетных рисков для дальнейшей работы.

Предполагаемый результат: Матрица рисков с цветовой маркировкой и приоритетным списком.

Контрольные вопросы:

6. Как определяется уровень риска в матрице?
7. Что такое триггеры рисков?
8. Примеры высокоприоритетных рисков.

Лабораторная работа №6. Моделирование рисков методом Монте-Карло в Microsoft Excel.

Цель работы: Освоить количественное моделирование рисков методом Монте-Карло.

Ход выполнения:

1. Создайте таблицу задач проекта (10–15 задач) с оптимистичными, пессимистичными и наиболее вероятными сроками.
2. Используйте формулу PERT:  $(O + 4M + P)/6$  для ожидаемого времени.
3. В колонке "Случайное время" примените функцию РАНДСУММ или RAND() для моделирования вариаций ( $\pm 20\%$ ).
4. Рассчитайте суммарное время проекта для 1000 итераций (копировать вниз).
5. Постройте гистограмму распределения сроков и вероятностей (P80, P90).
6. Сделайте выводы о рисках сроков.

Предполагаемый результат: График распределения сроков/бюджета с вероятностями (P80/P90).

Контрольные вопросы:

7. Принцип метода Монте-Карло?
8. Какие параметры моделировать?
9. Интерпретация результатов моделирования.

Лабораторная работа №7. Разработка плана минимизации рисков.

Цель работы: Научиться разрабатывать стратегии управления рисками.

Ход выполнения:

1. Возьмите 5–7 высокоприоритетных рисков из матрицы.
2. Для каждого риска определите стратегию:
  - o Избегание (изменить план).

- о Смягчение (уменьшить вероятность/воздействие).
  - о Трансфер (страхование, аутсорсинг).
  - о Принятие (резервирование).
3. Укажите ответственного, сроки реализации, ресурсы.
4. Составьте таблицу плана с колонками: риск, стратегия, ответственный, статус.
5. Добавьте план мониторинга (триггеры, частота проверки).

Предполагаемый результат: План минимизации рисков в табличном виде (1–2 стр.).

Контрольные вопросы:

6. Стратегии управления рисками (4 типа)?
7. Когда применять трансфер риска?
8. Мониторинг реализации плана.

Лабораторная работа №8. Создание регистра рисков в Jira или Microsoft Project.

Цель работы: Освоить инструменты управления рисками проектов.

Ход выполнения (Jira):

1. Создайте проект в Jira, добавьте тип задачи "Risk".
2. Создайте поля: Риск, Вероятность, Воздействие, Статус, Ответственный, Стратегия.
3. Заполните 10–15 рисков с оценками из предыдущих работ.
4. Настройте дашборд с фильтрами по приоритету и статусу.
5. Добавьте уведомления при изменении статуса.

Ход выполнения (MS Project):

6. Создайте пользовательское поле "Risk Level".
7. Добавьте задачи-риски с оценками вероятности/воздействия.
8. Постройте диаграмму Ганта рисков с фильтрами.

Предполагаемый результат: Рабочий риск-регистр с статусами и дашбордом.

Контрольные вопросы:

9. Что содержит риск-регистр?
10. Преимущества Jira для управления рисками.
11. Интеграция с другими инструментами.

Лабораторная работа №9. Анализ рисков на этапе реализации программного обеспечения.

Цель работы: Идентифицировать риски интеграции надежности на этапе разработки.

Ход выполнения:

1. Разделите этап реализации на подэтапы: кодирование, тестирование, развертывание.
2. Для каждого подэтапа составьте список рисков (баги, регрессии, downtime).
3. Оцените риски по матрице (вероятность × воздействие).
4. Предложите меры: автоматизированное тестирование, CI/CD, резервное копирование.
5. Свяжите риски с метриками надежности (доступность, MTBF).
6. Составьте отчет с рекомендациями по DevOps-практикам.

Предполагаемый результат: Отчет по рискам этапа реализации (таблица + меры).

Контрольные вопросы:

7. Риски этапа тестирования программного обеспечения.
8. Как обеспечить надежность при развертывании?
9. Роль DevOps в управлении рисками.

Лабораторная работа №10. Оценка надежности информационных систем по метрикам.

Цель работы: Рассчитать метрики надежности информационных систем.

Ход выполнения:

1. Получите данные о сбоях: общее время работы, количество отказов, время восстановления.
2. Рассчитайте:

- о MTBF = общее время / количество отказов.
- о MTTR = суммарное время восстановления / количество отказов.
- о Доступность =  $MTBF / (MTBF + MTTR) \times 100\%$ .
- 3. Сравните с целевыми значениями (99.9%, "три девятки").
- 4. Постройте график трендов надежности по периодам.
- 5. Сделайте выводы и рекомендации по улучшению.

Предполагаемый результат: Таблица метрик надежности с выводами и графиком.

Контрольные вопросы:

6. Формулы расчета среднего времени наработки на отказ (MTBF) и среднего времени восстановления (MTTR)?
7. Что такое доступность системы (uptime)?
8. Цели уровня доступности 99.9% (три девятки).

### **5.1.2 Методические указания для обучающихся по самостоятельной работе:**

Рекомендации по самостоятельной работе:

1. Рекомендации по самостоятельной подготовке к лабораторным работам
  - Изучите теоретический материал по теме лабораторной работы. Ознакомьтесь с учебниками, лекциями и дополнительными источниками, чтобы понимать цели и задачи работы, основные понятия и методы, используемые в лабораторном задании1.
  - Внимательно ознакомьтесь с методическими указаниями и требованиями к лабораторной работе. Обратите внимание на последовательность выполнения этапов, используемое программное обеспечение, форматы исходных и выходных данных, требования к визуализации и анализу результатов.
  - Подготовьте исходные данные. Проверьте наличие всех необходимых файлов, убедитесь в их корректности (форматы, структура, отсутствие ошибок и пропусков данных).
  - Освойте необходимые функции и инструменты программного обеспечения. Повторите работу с теми модулями и инструментами, которые будут использоваться в лабораторной работе.
  - Планируйте время. Разделите выполнение работы на этапы: подготовка данных, выполнение анализа, оформление визуализации, написание отчета.
2. Рекомендации по оформлению отчетов по лабораторным работам
  - Структурируйте отчет по стандартной схеме:
  - Титульный лист (название работы, ФИО, группа, дата)
  - Цель работы
  - Краткое описание исходных данных
  - Описание используемых методов и программного обеспечения
  - Последовательное изложение этапов работы с иллюстрациями (скриншотами, графиками, картами)
  - Анализ полученных результатов (выявленные особенности, сравнение с теорией, интерпретация)
  - Выводы и рекомендации
  - Список использованных источников
  - Используйте качественные иллюстрации. Все графические материалы должны быть четкими, снабжены подписями, масштабами, легендами и пояснениями.
  - Формулируйте выводы по существу. Кратко и ясно отражайте основные результаты работы, выявленные закономерности, достоинства и ограничения применяемых методов.
  - Оформляйте отчет в соответствии с требованиями ДОТ. Соблюдайте стандарты

оформления текста, таблиц, рисунков и ссылок на источники.

### 3. Рекомендации по самостоятельной проработке отдельных разделов тем

- Изучайте рекомендованную литературу и дополнительные источники. Используйте учебники, статьи, электронные ресурсы, профессиональные базы данных и справочные материалы, указанные в рабочей программе дисциплины1.
- Выполняйте конспектирование ключевых понятий и алгоритмов. Составляйте краткие записи по основным определениям, алгоритмам, этапам работы с ПО, особенностям визуализации и анализа данных.
- Практикуйтесь в самостоятельном выполнении типовых заданий. Решайте задачи, связанные с обработкой и визуализацией геолого-геофизических данных, используя различные программные средства.
- Формулируйте вопросы и уточнения для обсуждения на занятиях. Записывайте непонятные моменты, чтобы получить разъяснения у преподавателя или в ходе дискуссии.
- Анализируйте примеры из практики. Изучайте реальные кейсы решения задач геофизики, сравнивайте разные подходы и делайте выводы о целесообразности их применения.

### 4. Общие рекомендации

- Развивайте навыки поиска и критического анализа информации. Пользуйтесь современными информационными ресурсами, анализируйте достоверность и актуальность найденных данных.
- Акцентируйте внимание на интеграции знаний и умений. Страйтесь связывать теоретические знания с практическими задачами, анализируйте, как выбранные методы и технологии влияют на качество и достоверность графического представления информации.
- Соблюдайте академическую честность. Все результаты, представленные в отчетах, должны быть получены самостоятельно, с обязательным указанием источников заимствованных данных и иллюстраций.

## **6 Фонд оценочных средств для контроля текущей успеваемости и проведения промежуточной аттестации по дисциплине**

### **6.1 Оценочные средства для проведения текущего контроля**

#### **6.1.1 семестр 8 | Устный опрос**

##### **Описание процедуры.**

Опрос может проводиться:

Фронтально — в форме беседы с группой, когда вопросы задаются всей группе, а ответы даются по очереди или по желанию.

Индивидуально — каждый студент отвечает на один или несколько вопросов, давая развернутый, связный ответ, часто с примерами и пояснениями.

Комбинированно — сочетаются оба подхода, а также используются дополнительные методы (например, письменные карточки, рецензирование ответов товарищей)

##### **Критерии оценивания.**

полнота и правильность ответа;

понимание и осознанность материала;

логичность и последовательность изложения;

корректность терминологии;

способность отвечать на уточняющие вопросы

## 6.2 Оценочные средства для проведения промежуточной аттестации

### 6.2.1 Критерии и средства (методы) оценивания индикаторов достижения компетенции в рамках промежуточной аттестации

Индикатор достижения компетенции	Критерии оценивания	Средства (методы) оценивания промежуточной аттестации
ПКС-4.5	полнота и правильность ответа; понимание и осознанность материала; логичность и последовательность изложения; корректность терминологии; способность отвечать на уточняющие вопросы	устный опрос

### 6.2.2 Типовые оценочные средства промежуточной аттестации

#### 6.2.2.1 Семестр 8, Типовые оценочные средства для проведения зачета по дисциплине

##### 6.2.2.1.1 Описание процедуры

К зачету допускаются студенты сдавшие все отчеты по лабораторным (практическим) работам. Зачёт проводится в форме устного опроса или тестирования, включающего 5 вопросов — по одному из каждой основной темы курса. В некоторых случаях допускается комбинированная форма: тест + устный опрос.

Время на ответ ограничено, ответы должны быть чёткими, логичными и аргументированными.

В случае неудовлетворительного результата студенту предоставляется возможность пересдачи в установленные сроки. При повторном не сдаче возможна дополнительная консультация и индивидуальное собеседование. Оценка выставляется по шкале с учётом полноты и правильности ответов.

Примерные вопросы к зачету:

Раздел I. Основы надежности информационных систем

1. Принципы надежности информационных систем (доступность, целостность, отказоустойчивость).
2. Метрики надежности: среднее время наработка на отказ (MTBF) и среднее время восстановления (MTTR).
3. Функциональные и нефункциональные требования к программному обеспечению.
4. Влияние требований на параметры информационно-технологического проекта.

Раздел II. Идентификация и анализ рисков

5. Типы рисков информационно-технологических проектов (технические, операционные, связанные с программным обеспечением).
6. Анализ сильных и слабых сторон, возможностей и угроз (SWOT) - назначение и структура.
7. Анализ видов и последствий отказов (FMEA) для программного обеспечения.

8. Индекс приоритета риска (RPN) и его расчет.
9. Анализ опасностей и операбельности (HAZOP) в информационно-технологических проектах.

**Раздел III. Оценка и управление рисками**

10. Матрица рисков: вероятность × воздействие, цветовая маркировка.
11. Триггеры рисков и их роль в мониторинге.
12. Метод Монте-Карло для моделирования рисков.
13. Стратегии управления рисками (избегание, трансфер, смягчение, принятие).
14. Содержание регистра рисков.

**Раздел IV. Обеспечение надежности в проектах**

15. Интеграция управления рисками в этапы проекта по руководству РМВОК.
16. Риски этапа тестирования программного обеспечения.
17. Роль DevOps в обеспечении надежности систем.
18. Расчет доступности системы (uptime) по формуле MTBF / (MTBF + MTTR).
19. Цели уровня доступности "три девятки" (99.9%).
20. Классифицируйте риски: сбой сервера, задержка найма разработчиков, ошибка в алгоритме.
21. Рассчитайте RPN для отказа авторизации (S=8, O=4, D=6).
22. Опишите принцип моделирования методом Монте-Карло в Microsoft Excel.
23. Что содержит риск-регистр в Jira?
24. По данным: 1000 часов работы, 5 отказов, 10 часов восстановления - рассчитайте MTBF и доступность.
25. Разработайте план минимизации для риска "несоответствие требованиям заказчика" (стратегия, ответственный, мониторинг).

#### **6.2.2.1.2 Критерии оценивания**

<b>Зачтено</b>	<b>Не засчитано</b>
выставляется студенту, твердо знающему программный материал, грамотно и по существу его излагающему, который не допускает существенных неточностей в ответе на вопросы, правильно применяет теоретические положения при решении практических задач;	выставляется студенту, который не знает значительной части программного материала, допускает существенные ошибки, не может ответить на дополнительные вопросы

## **7 Основная учебная литература**

1. Бычков, А. А. Надежность информационных систем : учебное пособие / А. А. Бычков. — Ростов-на-Дону : ЮФУ, 2024. — 135 с. — ISBN 978-5-9275-4794-4.
2. Папировская, Л. И. Надежность информационных систем : учебное пособие / Л. И. Папировская, Т. Б. Ефимова, М. А. Колотилина. — Самара : СамГУПС, 2018. — 64 с.

## **8 Дополнительная учебная литература и справочная**

1. Надежность информационных систем : методические указания по выполнению работ / Иркут. нац. исследоват. техн. ун-т, 2015. - 33.

## **9 Ресурсы сети Интернет**

1. <http://library.istu.edu/>
2. <https://e.lanbook.com/>

## **10 Профессиональные базы данных**

1. <http://new.fips.ru/>
2. <http://www1.fips.ru/>

## **11 Перечень информационных технологий, лицензионных и свободно распространяемых специализированных программных средств, информационных справочных систем**

1. Лицензионное программное обеспечение Системное программное обеспечение
2. Лицензионное программное обеспечение Пакет прикладных офисных программ
3. Лицензионное программное обеспечение Интернет-браузер

## **12 Материально-техническое обеспечение дисциплины**

1. Учебная аудитория для проведения лекционных занятий, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации. Оснащение: комплект учебной мебели, рабочее место преподавателя, доска. Мультимедийное оборудование (в том числе переносное): мультимедийный проектор, экран, акустическая система, компьютер с выходом в интернет.
2. Учебная аудитория для проведения лабораторных/практических (семинарских) занятий, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации. Оснащение: комплект учебной мебели, рабочее место преподавателя, доска. Мультимедийное оборудование (в том числе переносное): мультимедийный проектор, экран, акустическая система, компьютер с выходом в интернет.