

МИНОБРНАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ  
НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ  
ТОМСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

Институт прикладной математики и компьютерных наук

УТВЕРЖДАЮ  
Директор института прикладной  
математики и компьютерных наук  
А.В. Замятин  
« 02 » \_\_\_\_\_ 2021 г.



**Фонд оценочных средств по дисциплине**

Квантовые вычисления

Специальность

**10.05.01 Компьютерная безопасность**

*код и наименование специальности*

**Анализ безопасности компьютерных систем**

*наименование специализации*

ФОС составил:

канд. техн. наук,  
доцент кафедры компьютерной безопасности



В.Н. Тренькаев

Рецензент:

канд. техн. наук,  
заведующий кафедрой компьютерной безопасности



С.А. Останин

Фонд оценочных средств одобрен на заседании учебно-методической комиссии  
института прикладной математики и компьютерных наук (УМК ИПМКН)

Протокол от 17 июня 2021 г. № 05

Председатель УМК ИПМКН,  
д-р техн. наук, профессор



С.П. Сущенко

**Фонд оценочных средств (ФОС)** является элементом системы оценивания сформированности компетенций у обучающихся в целом или на определенном этапе ее формирования.

ФОС разрабатывается в соответствии с рабочей программой (РП) дисциплины и включает в себя набор оценочных материалов для проведения текущего контроля успеваемости и промежуточной аттестации по дисциплине.

### 1. Компетенции и результаты обучения, формируемые в результате освоения дисциплины

Компетенция	Индикатор компетенции	Код и наименование результатов обучения (планируемые результаты обучения, характеризующие этапы формирования компетенций)	Критерии оценивания результатов обучения			
			Отлично	Хорошо	Удовлетворительно	Неудовлетворительно
ОПК-1. Способен оценивать роль информации, информационных технологий и информационной безопасности в современном обществе, их значение для обеспечения объективных потребностей личности, общества и государства	ИОПК-1.1 Учитывает современные тенденции развития информационных технологий в своей профессиональной деятельности.	ОР-1.1.1 Знать: историю создания и основные характеристики квантового компьютера	Высокий уровень знаний; способность самостоятельного анализа проблем предметной области.	В целом успешные, но содержащие отдельные пробелы знания.	Фрагментарные, неполные знания без грубых ошибок.	Не имеет четкого представления об изучаемом материале, допускает грубые ошибки.
ОПК-3. Способен на основании совокупности математических методов	ИОПК-3.2 Осуществляет применение основных понятий, фактов, концепций, принципов математики и	ОР-3.2.1 Знать: математические основы квантовых вычислений и принципы работы квантового компьютера	Высокий уровень знаний; способность самостоятельного анализа проблем	В целом успешные, но содержащие отдельные пробелы знания.	Фрагментарные, неполные знания без грубых ошибок.	Не имеет четкого представления об изучаемом материале, допускает грубые ошибки.

разрабатывать, обосновывать и реализовывать процедуры решения задач профессиональной деятельности	информатики для решения задач профессиональной деятельности.		предметной области.			
ОПК-7. Способен создавать программы на языках высокого и низкого уровня, применять методы и инструментальные средства программирования для решения профессиональных задач, осуществлять обоснованный выбор инструментария программирования и способов организации программ	ИОПК-7.3 Демонстрирует навыки создания программ с применением методов и инструментальных средств программирования для решения различных профессиональных, исследовательских и прикладных задач.	ОР-7.3.1 Уметь: применять требуемый математический аппарат для вычисления значений квантовых схем.  ОР-7.3.2 Владеть: инструментальными средствами моделирования квантовых схем.	Отлично сформированное умение применять требуемый математический аппарат для вычисления значений квантовых схем.  Высокий уровень владения навыками использования инструментальных средств моделирования квантовых схем.	Хорошее умение применять требуемый математический аппарат для вычисления значений квантовых схем.  В целом успешные, но содержащие отдельные пробелы навыки использования инструментальных средств моделирования квантовых схем.	Удовлетворительное умение применять требуемый математический аппарат для вычисления значений квантовых схем.  Фрагментарные, неполные, но без грубых ошибок навыки использования инструментальных средств моделирования квантовых схем.	Неудовлетворительное умение применять требуемый математический аппарат для вычисления значений квантовых схем.  Фрагментарные, неполные, с грубыми ошибками навыки использования инструментальных средств моделирования квантовых схем.
ОПК-9. Способен решать задачи профессиональной деятельности с учетом текущего состояния и тенденций развития методов защиты информации в	ИОПК-9.1 Учитывает современные тенденции развития методов защиты информации в операционных системах, компьютерных сетях и системах управления базами данных при	ОР-9.1.1 Знать: основные квантовые алгоритмы, квантовые протоколы распределения ключей, квантовые протоколы передачи данных.	Высокий уровень знаний; способность самостоятельного анализа проблем предметной области.	В целом успешные, но содержащие отдельные пробелы знания.	Фрагментарные, неполные знания без грубых ошибок.	Не имеет четкого представления об изучаемом материале, допускает грубые ошибки.

<p>операционных системах, компьютерных сетях и системах управления базами данных, а также методов и средств защиты информации от утечки по техническим каналам, сетей и систем передачи информации</p>	<p>решении задач своей профессиональной деятельности.</p>					
<p>ПК-2. Способен разрабатывать требования к программно-аппаратным средствам защиты информации компьютерных систем и сетей</p>	<p>ИПК-2.2 Разрабатывает математические модели, реализуемые в средствах защиты информации.</p> <p>ИПК-2.3. Проводит исследования с целью нахождения наиболее целесообразных практических решений по обеспечению защиты информации</p>	<p>ОП-2.2.1 Уметь: излагать и демонстрировать на примерах квантовые алгоритмы и протоколы.</p> <p>ОП-2.2.2 Владеть: навыками анализа и синтеза квантовых схем.</p>	<p>Отлично сформированное умение излагать и демонстрировать на примерах основные квантовые алгоритмы и протоколы.</p> <p>Высокий уровень владения навыками анализа и синтеза квантовых схем.</p>	<p>Хорошее умение излагать и демонстрировать на примерах основные квантовые алгоритмы и протоколы.</p> <p>В целом успешные, но содержащие отдельные пробелы навыки анализа и синтеза квантовых схем.</p>	<p>Удовлетворительное умение излагать и демонстрировать на примерах основные квантовые алгоритмы и протоколы.</p> <p>Фрагментарные, неполные, но без грубых ошибок навыки анализа и синтеза квантовых схем.</p>	<p>Неудовлетворительное умение излагать и демонстрировать на примерах основные квантовые алгоритмы и протоколы.</p> <p>Фрагментарные, неполные, с грубыми ошибками навыки анализа и синтеза квантовых схем.</p>

## 2. Этапы формирования компетенций и виды оценочных средств

№	Этапы формирования компетенций (разделы дисциплины)	Код и наименование результатов обучения	Вид оценочного средства (тесты, задания, кейсы, вопросы и др.)
1.	Введение в квантовые вычисления	ОР-1.1.1 Знать: историю создания и основные характеристики квантового компьютера	лабораторные работы, контрольные задания, опросы на занятиях
2.	Математические основы квантовых вычислений	ОР-3.2.1 Знать: математические основы квантовых вычислений и принципы работы квантового компьютера	лабораторные работы, контрольные задания, опросы на занятиях
3.	Квантовые схемы	ОР-7.3.1 Уметь: применять требуемый математический аппарат для вычисления значений квантовых схем. ОР-7.3.2 Владеть: инструментальными средствами моделирования квантовых схем. ОР-2.2.2 Владеть: навыками анализа и синтеза квантовых схем.	лабораторные работы, контрольные задания, опросы на занятиях
4.	Квантовые протоколы	ОР-9.1.1 Знать: основные квантовые алгоритмы, квантовые протоколы распределения ключей, квантовые протоколы передачи данных. ОР-2.2.1 Уметь: излагать и демонстрировать на примерах квантовые алгоритмы и протоколы.	лабораторные работы, контрольные задания, опросы на занятиях
5.	Квантовые алгоритмы	ОР-9.1.1 Знать: основные квантовые алгоритмы, квантовые протоколы распределения ключей, квантовые протоколы передачи данных. ОР-2.2.1 Уметь: излагать и демонстрировать на примерах квантовые алгоритмы и протоколы. ОР-2.2.2 Владеть: навыками анализа и синтеза квантовых схем. ОР-7.3.2 Владеть: инструментальными	лабораторные работы, контрольные задания, опросы на занятиях

		средствами моделирования квантовых схем.	
6.	Квантовая коррекция ошибок	ОР-9.1.1 Знать: основные квантовые алгоритмы, квантовые протоколы распределения ключей, квантовые протоколы передачи данных.	лабораторные работы, контрольные задания, опросы на занятиях

### 3. Типовые контрольные задания или иные материалы, необходимые для оценки образовательных результатов обучения

3.1. Типовые задания для проведения текущего контроля успеваемости по дисциплине

Типовые варианты заданий для лабораторных работ:

1. Реализация квантовой схемы Базис Белла. Выполнить моделирование квантовой схемы для создания состояния Белла с использованием системы IBM Quantum Experience и объяснить полученные результаты.
2. Реализация квантовой схемы Reverse CNOT. С использованием системы IBM Quantum Experience выполнить моделирование квантовой схемы, реализующей двухкубитовый вентиль Reverse CNOT на базе двухкубитового вентиля CNOT, объяснить полученные результаты моделирования.
3. Реализация квантовой схемы SWAP. С использованием системы IBM Quantum Experience выполнить моделирование квантовой схемы, реализующей двухкубитовый вентиль SWAP на базе двухкубитовых вентилях CNOT и Reverse CNOT, объяснить полученные результаты моделирования.
4. Алгоритм Дойча. С использованием системы IBM Quantum Experience выполнить моделирование квантовой схемы, реализующей алгоритм Дойча для выбранной сбалансированной булевой функции, объяснить полученные результаты моделирования.
5. Алгоритм Бернштейна – Вазирани. С использованием системы IBM Quantum Experience выполнить моделирование квантовой схемы, реализующей алгоритм Бернштейна – Вазирани для нахождения скрытой строки длины 2, объяснить полученные результаты моделирования. Прокомментировать построение квантового оракула для булевой функции, которая скрывает задуманную строку.
6. Алгоритм Гровера. С использованием системы IBM Quantum Experience выполнить моделирование квантовой схемы, реализующей алгоритм Гровера для выбранной булевой функции от двух переменных, объяснить полученные результаты моделирования.

Типовые контрольные задания для текущего контроля:

1. Основные постулаты квантовой теории.
2. Линейное пространство.

3. Унитарные операторы.
4. Обратимые вычисления.
5. Обратимые вентили.
6. Принципы функционирования квантового компьютера.
7. Декогеренция и ошибки квантовых вычислений.
8. Кубит. Квантовый регистр.
9. Квантовый вентиль X.
10. Квантовый вентиль Y.
11. Квантовый вентиль Z.
12. Квантовый вентиль H.
13. Квантовый вентиль S.
14. Квантовый вентиль T.
15. Квантовый вентиль NOT.
16. Квантовый вентиль CNOT.
17. Квантовый вентиль CCNOT.
18. Невозможность клонирования кубита.
19. Состояние Белла.
20. Квантовый параллелизм.

### 3.2. Типовые задания для проведения промежуточной аттестации по дисциплине

#### Примерный перечень вопросов к экзамену:

1. Основные постулаты квантовой теории.
2. Принципы функционирования квантового компьютера.
3. Декогеренция и ошибки квантовых вычислений.
4. Кубит. Квантовый регистр.
5. Унитарные операторы и квантовые вычисления.
6. Однокубитовые вентили.
7. Двухкубитовые вентили.
8. Трехкубитовые вентили.
9. Простые квантовые схемы.
10. Невозможность клонирования кубита.
11. Алгоритм Дойча-Джозса.
12. Алгоритм Саймона.
13. Алгоритм Гровера.
14. Алгоритм Бернштейна – Вазирани.
15. Квантовое преобразование Фурье.
16. Алгоритм Шора.
17. Квантовое плотное кодирование.
18. Квантовая телепортация.
19. Квантовый протокол распределения ключей (BB84).
20. Квантовый протокол распределения ключей (B92).
21. Квантовый протокол распределения ключей (E91).
22. Общая схема квантовых кодов.
23. Трехкубитовый квантовый код.



#### **4. Методические материалы, определяющие процедуры оценивания образовательных результатов обучения**

4.1. Методические материалы для оценки текущего контроля успеваемости по дисциплине.

Текущий контроль подразумевает выполнение лабораторных работ/контрольных заданий. Выполнение лабораторной работы/контрольного задания оценивается в 100 баллов:

0-20 Студент не разбирается в задаче, не знает методов решения, не отвечает, либо отвечает, но с грубыми ошибками на вопросы преподавателя.

21-40 Студент слабо разбирается в задаче, плохо знает методы решения, не отвечает, либо отвечает, но с ошибками на вопросы преподавателя.

41-60 Студент в целом удовлетворительно разбирается в задаче, использует методы решения при подсказке преподавателя, отвечает на вопросы неуверенно, но с негрубыми ошибками. Представляет работу на защите удовлетворительно.

61-80 Студент в целом уверенно разбирается в задаче, знает и использует методы решения практически самостоятельно, отвечает на вопросы с замечаниями. Представляет работу на защите в целом хорошо, с замечаниями.

81-100 Студент отлично разбирается в задаче, знает и использует методы решения самостоятельно, отвечает на вопросы уверенно. Представляет работу на защите отлично, уверенно.

Допуском до экзамена является выполнение 80% лабораторных работ/контрольных заданий, с оценкой за каждую не менее 80 баллов.

4.2. Методические материалы для проведения промежуточной аттестации по дисциплине.

Промежуточный контроль знаний по дисциплине осуществляется в форме экзамена, который подразумевает подготовку студента и ответов в устной/письменной форме на несколько контрольных вопросов по всему курсу. Критерии выставления оценок:

Отлично - студент в совершенстве овладел всеми теоретическими вопросами обязательного материала по разделам лекционного курса, показал все требуемые умения и навыки при выполнении заданий на лабораторных занятиях.

Хорошо - студент овладел обязательным материалом по разделам лекционного курса, возможно с некоторыми недостатками, а также показал все требуемые умения и навыки при выполнении заданий на лабораторных занятиях.

Удовлетворительно - студент имеет недостаточно глубокие знания по теоретическим разделам обязательного материала дисциплины, но показал все требуемые умения и навыки при выполнении заданий на лабораторных занятиях.

Неудовлетворительно - студент имеет существенные пробелы по отдельным теоретическим разделам специальной дисциплины или не показал требуемые умения и навыки при выполнении заданий на лабораторных занятиях.