

Федеральное государственное бюджетное образовательное учреждение  
высшего образования  
Московский государственный университет имени М.В. Ломоносова  
Факультет вычислительной математики и кибернетики

УТВЕРЖДАЮ

декан факультета вычислительной  
математики и кибернетики



*[Signature]*  
И.А. Соколов /

*[Signature]* 2021г.

## РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

**Наименование дисциплины (модуля):**

Вероятностные и квантовые алгоритмы

**Уровень высшего образования:**

магистратура

**Направление подготовки / специальность:**

01.04.02 "Прикладная математика и информатика" (3++)

**Направленность (профиль) ОПОП:**

Искусственный интеллект в кибербезопасности

**Форма обучения:**

очная

Рабочая программа рассмотрена и утверждена  
на заседании Ученого совета факультета ВМК  
(протокол № 4, от 29 сентября 2021 года)

Москва 2021

Рабочая программа дисциплины (модуля) разработана в соответствии с самостоятельно установленным МГУ образовательным стандартом (ОС МГУ) для реализуемых основных профессиональных образовательных программ высшего образования по направлению подготовки 01.04.02 "Прикладная математика и информатика" программы магистратуры в редакции приказа МГУ от 21 декабря 2021 года No 1404.

**1. Место дисциплины (модуля) в структуре ОПОП ВО:**

Дисциплина (модуль) относится к части дисциплин основной профессиональной образовательной программы, формируемых участниками образовательных отношений.

**2. Входные требования для освоения дисциплины (модуля), предварительные условия:**

Учащиеся должны владеть знаниями по теории вероятностей, математической статистике, машинному обучению в объеме, соответствующем основным образовательным программам бакалавриата по укрупненным группам направлений и специальностей 01.00.00 «Математика и механика», 02.00.00 «Компьютерные и информационные науки» и другим направлениям подготовки бакалавриата.

**3. Результаты обучения по дисциплине (модулю), соотнесенные с требуемыми компетенциями выпускников.**

Планируемые результаты обучения по дисциплине (модулю)		
Содержание и код компетенции.	Индикатор (показатель) достижения компетенции	Планируемые результаты обучения по дисциплине, сопряженные с индикаторами достижения компетенций
ОПК-8. Способен осуществлять эффективное управление проектами по разработке и внедрению систем искусственного интеллекта	<p>ОПК-8.1. Исследует архитектуру информационных систем предприятий и организаций; применяет методологии и технологии реинжиниринга, проектирования и аудита информационных систем различных классов</p> <p>ОПК-8.2. Применяет инструментальные средства поддержки технологии проектирования и аудита информационных систем и сервисов; методы оценки экономической эффективности и качества, управления надежностью и информационной безопасностью</p> <p>ОПК-8.3. Исследует особенности процессного подхода к управлению информационными системами и системами искусственного интеллекта; применяет системы управления качеством</p> <p>ОПК-8.4. Выбирает методологию и технологию проектирования информационных систем; обосновывает архитектуру информационных</p>	<p>ОПК-8.1. 3-1. Знает новые научные принципы и методы реинжиниринга, проектирования и аудита информационных систем для решения профессиональных задач</p> <p>ОПК-8.1. У-1. Умеет разрабатывать программное и аппаратное обеспечение информационных и автоматизированных систем для решения профессиональных задач</p> <p>ОПК-8.2. 3-1. Знает особенности модернизации программного и аппаратного обеспечения информационных и автоматизированных систем для решения профессиональных задач</p> <p>ОПК-8.2. У-1. Умеет модернизировать программное и аппаратное обеспечение информационных и автоматизированных систем для решения профессиональных задач</p> <p>ОПК-8.3. 3-1. Знает особенности процессного подхода к управлению информационными системами и системами искусственного интеллекта; системы управления качеством</p>

	<p>систем и систем искусственного интеллекта</p> <p>ОПК-8.5. Управляет проектами по созданию (модификации) программного обеспечения, на всех стадиях жизненного цикла, оценивает эффективность и качество проекта; применяет современные методы управления проектами по разработке и внедрению систем искусственного интеллекта</p> <p>ОПК-8.6. Использует инновационные подходы к проектированию информационных систем и систем искусственного интеллекта; принимает решения по информатизации предприятий в условиях неопределенности</p> <p>ОПК-8.7. Проводит реинжиниринг прикладных и информационных процессов</p>	<p>ОПК-8.3. У-1. Умеет применять системы управления качеством</p> <p>ОПК-8.4. З-1. Знает методологию и технологию проектирования информационных систем</p> <p>ОПК-8.4. У-1. Умеет обосновывать архитектуру информационных систем и систем искусственного интеллекта</p> <p>ОПК-8.5. З-1. Знает особенности управления проектами по созданию (модификации) программного обеспечения на всех стадиях жизненного цикла,</p> <p>ОПК-8.5. У-1. Умеет оценивать эффективность и качество проекта; применять современные методы управления проектами и сервисами информационных систем и систем искусственного интеллекта</p> <p>ОПК-8.6. З-1. Знает инновационные подходы к проектированию информационных систем и систем искусственного интеллекта</p> <p>ОПК-8.6. У-1. Умеет принимать решения по информатизации предприятий в условиях неопределенности</p> <p>ОПК-8.7. З-1. Знает особенности процессного подхода, принципы реинжиниринга прикладных и информационных процессов</p> <p>ОПК-8.7. У-1. Умеет проводить реинжиниринг прикладных и информационных процессов</p>
--	---	---

<p>ПК-9. Способен создавать и применять методы объяснимого искусственного интеллекта для создания интерпретируемых интеллектуальных систем</p>	<p>ПК-9.1. Применяет методы объяснимого искусственного интеллекта для построения объяснимой модели интеллектуальной системы  ПК-9.2. Применяет методы объяснимого искусственного интеллекта для построения объясняющего интерфейса интеллектуальной системы</p>	<p>ПК-9.1. З-1. Знает структуры, виды обучения и типы объяснимых моделей интеллектуальной системы  ПК-9.1. У-1. Умеет строить объяснимые модели для всех типов интеллектуальных систем и методов их обучения, в том числе сетей глубокого обучения, обучения с подкреплением, пространственных, темпоральных, каузальных моделей интеллектуальных систем, вероятностных моделей, имитационного обучения.  ПК-9.2. З-1. Знает типы объясняющих интерфейсов для интеллектуальной системы объясняющих интерфейсов  ПК-9.2. У-1. Умеет строить объясняющие интерфейсы, в том числе на базе рефлексивных объяснений, рациональных объяснений, интерактивной визуализация, интерактивных объяснений динамических систем.</p>
--	---	--

4. Объем дисциплины (модуля) составляет 3 з.е., в том числе 54 академических часа, отведенных на контактную работу обучающихся с преподавателем, 54 академических часов на самостоятельную работу обучающихся.

5. Содержание дисциплины (модуля), структурированное по темам (разделам) с указанием отведенного на них количества академических часов и виды учебных занятий:

В курсе «Вероятностные и квантовые алгоритмы» рассматриваются различные модели вероятностных вычислений, вероятностный анализ алгоритмов, построение быстрых вероятностных алгоритмов для различных задач, важнейшие вероятностные классы сложности задач. Даются определения квантовых вычислений, рассматривается их связь с обычными алгоритмами, рассматриваются примеры построения быстрых квантовых алгоритмов.

Наименование и краткое содержание разделов и тем дисциплины, форма промежуточной аттестации по дисциплине	Всего (часы)	В том числе								
		Контактная работа (работа во взаимодействии с преподавателем), часы					Самостоятельная работа учащегося, часы			
		из них					из них			
Занятия лекционного типа	Занятия семинарского типа	Групповые консультации	Индивидуальные консультации	Учебные занятия, направленные на проведение текущего контроля успеваемости: коллоквиумы, практические контрольные занятия и др.	Всего	Выполнение домашних заданий	Подготовка рефератов и т.п..	Всего		
<b>Тема 1. Вероятностный анализ детерминированных алгоритмов</b> Сложность и полиномиальность в среднем. Задача упаковки. Выполнимость КНФ. Точность алгоритма для почти всех	<b>18</b>	8	-	-	-	-	<b>8</b>	4	-	<b>4</b>

ВХОДОВ										
<b>Тема 2. Вероятностные алгоритмы и их анализ</b> Вероятностная проверка тождеств. Вероятностные методы в перечислительных задачах. Вероятностные методы в параллельных вычислениях. Максимальное по включению независимое множество в графе. Протокол византийского соглашения. Вероятностное округление для задачи «MAX-SAT»	<b>34</b>	16	-	-	-	-	<b>16</b>	5	-	<b>5</b>
<b>Тема 3. Методы дерандомизации</b> Метод условных вероятностей для дерандомизации алгоритмов. Детерминированный алгоритм для задачи «Максимальная выполнимость», построенный путем дерандомизации. Его сложность.	<b>8</b>	4	-	-	-	-	<b>4</b>	2	-	<b>2</b>
<b>Тема 4. Классы сложности вероятностных вычислений</b>	<b>18</b>	8	-	-	-	-	<b>8</b>	3	-	<b>3</b>

Классы $RP/coRP$ , $BPP$ , $PP$ . Их связи с классами $P$ и $NP$ .											
<b>Тема 5. Квантовые алгоритмы</b> Определение квантовых вычислений. Квантовый поиск: алгоритм Гровера.	<b>24</b>	12	-	-	-	-	<b>12</b>	4		<b>4</b>	
<b>Промежуточная аттестация –зачет</b>	<b>6</b>	-	-	2	-	4	<b>6</b>	36	-	<b>36</b>	
<b>Итого</b>	<b>108</b>						<b>54</b>				<b>54</b>

6. Фонд оценочных средств (ФОС, оценочные и методические материалы) для оценивания результатов обучения по дисциплине (модулю).

6.1. Типовые контрольные задания или иные материалы для проведения текущего контроля успеваемости, критерии и шкалы оценивания

Примеры задач для текущего контроля знаний

1. Является ли набор вентилей, содержащий  $H$ ,  $T$  (Адамара и  $\pi/8$ ) и двухкубитный вентиль  $CZ$  универсальным для квантовых вычислений? Ответ обосновать.

2. Постройте квантовую схему для симуляции трехкубитного Гамильтониана  $H=X_1 \otimes Y_2 \otimes Z_3$ , т.е. схему, осуществляющую преобразование  $e^{i\Delta t H}$  для произвольного  $\Delta t$

3. Постройте квантовую схему, которая осуществляет обратное квантовое преобразование Фурье.

4. Рассмотрим 9-кубитный код Шора. Покажите, что фазовая ошибка в любом из первых трех кубитов может быть исправлена применением оператора  $Z_1 \otimes Z_2 \otimes Z_3$

6.2. Типовые контрольные задания или иные материалы для проведения промежуточной аттестации по дисциплине, критерии и шкалы оценивания

**Список тем вопросов для зачета.**



В билете 2 вопроса – один из части А и один из части В.

Часть А – ответ без подготовки, но по любым материалам (конспекты, книжки и т.д.). Проверяется, насколько осознаны все доказательства (основной вопрос – «почему?»). Определения и формулировки утверждений – без конспектов.

1. Алгоритм динамического программирования для задачи упаковки подмножеств. Его полиномиальность «в среднем».
2. Алгоритм динамического программирования для задачи «Выполнимость КНФ». Его полиномиальность «в среднем».
3. Жадный алгоритм для задачи о покрытии. Его точность для почти всех входов.
4. Вероятностный алгоритм проверки тождеств для многочлена. Оценка вероятности ошибки.
5. Полностью полиномиальная рандомизированная аппроксимационная схема с двумя параметрами для задачи о мощности объединения множеств. Следствие для задачи о числе выполняющих наборов для ДНФ.
6. Параллельный алгоритм для поиска максимального по включению независимого множества в графе. Оценка времени его работы.
7. Вероятностный протокол византийского соглашения. Оценка числа раундов.
8. Приближенный вероятностный алгоритм для задачи «Максимальная выполнимость» на основе линейной релаксации. Оценка его точности в среднем.
9. Метод условных вероятностей для дерандомизации алгоритмов. Детерминированный алгоритм для задачи «Максимальная выполнимость», построенный путем дерандомизации. Его сложность.
10. Классы сложности  $RP$ ,  $coRP$ ,  $RP_{weak}$ ,  $RP_{strong}$ . Их соотношение с классами  $NP$ ,  $coNP$  и между собой.
11. Классы сложности  $BPP$ ,  $BPP_{weak}$ ,  $BPP_{strong}$ . Соотношение между ними.
12. Классы сложности  $PP$ ,  $PP_{weak}$ . Их соотношение между собой и с классами  $NP$ ,  $PSPACE$ .
13. Теорема о связи вычислений булевыми схемами и обратимыми схемами.
14. Квантовые схемы для двух операторов отражения относительно гиперплоскости, их сложность.
15. Квантовый алгоритм Гровера для задачи поиска, его сложность.

Часть В – ответ без конспектов с короткой подготовкой (с доказательствами).

16. Вероятностный алгоритм Фрейвалда для проверки матричного тождества. Оценка вероятности ошибки.
17. Класс сложности  $ZPP$ . Его соотношение с классами  $RP$ ,  $coRP$ .
18. Тензорное произведение линейных пространств, теорема о его согласованности со скалярным произведением (для унитарных пространств).
19. Тензорное произведение линейных операторов, теорема о его дистрибутивности при действии на разложимый вектор.

Часть С – ответ без конспектов по любым определениям и формулировкам. В частности, всем будет задан вопрос:

20. Определение квантового компьютера, квантовой схемы и квантовых вычислений.

**Методические материалы для проведения процедур оценивания результатов обучения**

В билете 2 вопроса – один из части А и один из части В.

Часть А – ответ без подготовки, но по любым материалам (конспекты, книжки и т.д.). Проверяется, насколько осознаны все доказательства (основной вопрос – «почему?»). Определения и формулировки утверждений – без конспектов.

Часть В – ответ без конспектов с короткой подготовкой (с доказательствами).

Часть С – ответ без конспектов по любым определениям и формулировкам.

<b>ШКАЛА И КРИТЕРИИ ОЦЕНИВАНИЯ результатов обучения (РО) по дисциплине (модулю)</b>				
Оценка РО и соответствующие ви- ды оценочных средств	2 (не зачтено)	3 (зачтено)	4 (зачтено)	5 (зачтено)
<b>Знания</b> <i>Экзамен</i>	Отсутствие знаний	Фрагментарные знания	Общие, но не структуриро- ванные знания	Сформированные систе- матические знания
<b>Умения</b> <i>Практические зада- ния</i>	Отсутствие умений	В целом успешное, но не си- стематическое умение	В целом успешное, но со- держательное отдельные пробелы умение (допускает не- точности неприципиально- го характера)	Успешное и системати- ческое умение
<b>Навыки (владения, опыт дея- тельности)</b> <i>Экзамен, практиче- ские занятия</i>	Отсутствие навыков (владений, опыта)	Наличие отдельных навыков (наличие фрагментарного опыта)	В целом, сформированные навыки (владения), но ис- пользуемые не в активной форме	Сформированные навыки (владения), применяемые при решении задач

7. Ресурсное обеспечение:

7.1. Перечень основной и дополнительной литературы

**Основная литература**

- 1) Введение в квантовые вычисления. Квантовые алгоритмы : учеб. пособие. / С. С. Сысоев ; С.-Петерб. гос. ун-т. - СПб. : Изд-во С.-Петерб. ун-та, 2019. - 143

#### Дополнительная литература

- 1) Кузюрин Н.Н., Фомин С.А. Эффективные алгоритмы и сложность вычислений: Учебное пособие. – М.: МФТИ, 2007, стр. 99-120, 129-160, 169-173, 227-244.
- 2) Кузюрин Н.Н., Фомин С.А. Эффективные алгоритмы и сложность вычислений (авторское электронное издание), стр. 122-147, 161-195, 207-212, 273-291.
- 3) А. Китаев, А. Шень, М. Вялый. Классические и квантовые вычисления. – М.: МЦМНО, ЧеРо, 1999, стр. 48-58, 66-71.

7.2. Перечень лицензионного программного обеспечения, в том числе отечественного производства При реализации дисциплины может быть использовано следующее программное обеспечение:

Программное обеспечение для подготовки слайдов лекций MS PowerPoint, MS Word

Программное обеспечение для создания и просмотра pdf-документов Adobe Reader

Издательская система LaTeX

Язык программирования Python и среда разработки Jupiter Notebook (вместе с библиотеками numpy, scikit-learn, pandas)

Язык программирования R и среда разработки R Studio

7.3. Перечень профессиональных баз данных и информационных справочных систем

1. <http://www.edu.ru> – портал Министерства образования и науки РФ

2. <http://www.ict.edu.ru> – система федеральных образовательных порталов «ИКТ в образовании»

3. <http://www.openet.ru> - Российский портал открытого образования

4. <http://www.mon.gov.ru> - Министерство образования и науки Российской Федерации

5. <http://www.fasi.gov.ru> - Федеральное агентство по науке и инновациям

7.4. Перечень ресурсов информационно-телекоммуникационной сети «Интернет»

1. Math-Net.Ru [Электронный ресурс] : общероссийский математический портал / Математический институт им. В. А. Стеклова РАН ; Российская академия наук, Отделение математических наук. - М. : [б. и.], 2010. - Загл. с титул. экрана. - Б. ц.

URL: <http://www.mathnet.ru>

2. Университетская библиотека Online [Электронный ресурс] : электронная библиотечная система / ООО "Директ-Медиа" . - М. : [б. и.], 2001. - Загл. с титул. экрана. - Б. ц. URL: [www.biblioclub.ru](http://www.biblioclub.ru)
3. Универсальные базы данных East View [Электронный ресурс] : информационный ресурс / East View Information Services. - М. : [б. и.], 2012. - Загл. с титул. экрана. - Б. ц. URL: [www.ebiblioteka.ru](http://www.ebiblioteka.ru)
4. Научная электронная библиотека eLIBRARY.RU [Электронный ресурс] : информационный портал / ООО "РУНЭБ" ; Санкт-Петербургский государственный университет. - М. : [б. и.], 2005. - Загл. с титул. экрана. - Б. ц. URL: [www.eLibrary.ru](http://www.eLibrary.ru)

#### 7.5. Описание материально-технического обеспечения.

Факультет ВМК, ответственный за реализацию данной Программы, располагает соответствующей материально -технической базой, включая современную вычислительную технику, объединенную в локальную вычислительную сеть, имеющую выход в Интернет. Используются специализированные компьютерные классы, оснащенные современным оборудованием. Материальная база факультета соответствует действующим санитарно-техническим нормам и обеспечивает проведение всех видов занятий (лабораторной, практической, дисциплинарной и междисциплинарной подготовки) и научно-исследовательской работы обучающихся, предусмотренных учебным планом.

8. Соответствие результатов обучения по данному элементу ОПОП результатам освоения ОПОП указано в Общей характеристике ОПОП.

9. Разработчик (разработчики) программы.

10.

д.ф.- м.н., профессор Алексеев Валерий Борисович ([vbalekseev@rambler.ru](mailto:vbalekseev@rambler.ru))

10. Язык преподавания - русский.