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
_____ /И.А. Соколов /
«___» _____2021г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Наименование дисциплины:

Математические основы верификации программ

Уровень высшего образования:

магистратура

Направление подготовки / специальность:

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

Направленность (профиль) ОПОП:

Перспективные методы искусственного интеллекта
в сетях передачи и обработки данных

Форма обучения:

очная

Рабочая программа рассмотрена и утверждена
на заседании Ученого совета факультета ВМК
(протокол №7, от 29 сентября 2021 года)

Москва 2021

Рабочая программа дисциплины (модуля) разработана в соответствии с Федеральным государственным образовательным стандартом высшего образования (ФГОС ВО) для реализуемых основных профессиональных образовательных программ высшего образования по направлению подготовки 01.04.02 "Прикладная математика и информатика" утвержденного Приказом Министерства образования и науки РФ от 10 января 2018 г. N 13.

1. Место дисциплины (модуля) в структуре ОПОП ВО:
Дисциплина (модуль) относится к части дисциплин основной профессиональной образовательной программы, формируемых участниками образовательных отношений.
Дисциплина входит в магистерскую образовательную программу «Перспективные методы искусственного интеллекта в сетях передачи и обработки данных» как дисциплина по выбору, изучается в 3-м семестре.

2. Входные требования для освоения дисциплины (модуля), предварительные условия (если есть):
Изучение дисциплины базируется на освоении знаний по дискретной математике, математической логике, системам программирования 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):

Планируемые результаты обучения по дисциплине (модулю)		
Формируемые компетенции (*код и наименование компетенции*)	**Индикаторы достижения компетенций (*код и наименование индикатора*)**	**Результаты обучения *(знания, умения)***
ПК-6. Способен руководить проектами по созданию комплексных систем на основе аналитики больших данных в различных отраслях	ПК-6.1. Осуществляет руководство проектом по построению комплексных систем на основе аналитики больших данных в различных отраслях	ПК-6.1. З-1. Знает функциональность современных инструментальных средств и систем программирования в области создания моделей искусственных нейронных сетей, в том числе сетей-трансформеров и сетей с автоматически генерируемой архитектурой ПК-6.1. У-1. Умеет проводить оценку и выбор моделей искусственных нейронных сетей и инструментальных средств для решения задач машинного обучения ПК-6.1. У-2. Умеет применять современные инструментальные методы и средства обучения моделей искусственных нейронных сетей
	ПК-6.2. Применяет варианты использования больших данных, определений, словарей и эталонной архитектуры больших данных при руководстве проектами по построению комплексных систем на основе аналитики больших данных в различных отраслях	ПК-6.2. З-1. Знает принципы построения систем искусственного интеллекта на основе искусственных нейронных сетей, методы и подходы к планированию и реализации проектов по созданию систем искусственного интеллекта ПК-6.2. У-1. Умеет руководить выполнением коллективной проектной деятельности для создания, поддержки и использования систем искусственного интеллекта на основе искусственных нейронных сетей

	ПК-6.3. Проводит планирование, управление, развертывание, аудит безопасности и защиты персональных данных при работе с большими данными и руководит операционной деятельностью, связанной с безопасностью и защитой персональных данных при работе с большими данными	ПК-6.3. З-1. Знает принципы построения моделей глубоких нейронных сетей и глубокого машинного обучения ПК-6.3. З-2. Знает подходы к применению моделей на основе нечеткой логики в системах искусственного интеллекта ПК-6.3. У-1. Умеет руководить выполнением коллективной проектной деятельности для создания, поддержки и использования систем искусственного интеллекта на основе моделей глубоких нейронных сетей и нечетких моделей и методов

4. Объем дисциплины (модуля) составляет 3 з.е., в том числе 72 академических часа на контактную работу обучающихся с преподавателем – 36 академических часов занятий лекционного типа, 36 академических часов занятий практического типа, 36 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:

5.1. Структура дисциплины (модуля) по темам (разделам) с указанием отведенного на них количества академических часов и виды учебных занятий (в строгом соответствии с учебным планом)

Наименование разделов и тем дисциплины (модуля), **Форма промежуточной аттестации по дисциплине (модулю)**	**Номинальные трудозатраты обучающегося**			**Всего академических часов**	**Форма текущего контроля успеваемости* (наименование)**
	Контактная работа (работа во взаимодействии с преподавателем) Виды контактной работы, академические часы		**Самостоятельная работа обучающегося, академические часы**		
	Занятия лекционного типа	Занятия семинарского типа			
Тема 1. Задача верификации информационных систем и общие подходы к ее решению	8	8	8	24	контрольная работа

Тема 2. Табличные, символьные и теоретико-автоматные методы верификации моделей программ	10	10	10	30	контрольная работа
Тема 3. Методы верификации информационных систем реального времени	10	10	10	30	контрольная работа
Тема 4. Метод повышения эффективности алгоритмов верификации	8	8	8	24	контрольная работа
Другие виды самостоятельной работы (отсутствуют)	—	—			—
Промежуточная аттестация (экзамен)					
Итого	*36*	*36*	*36*	108	—

5.2. Содержание разделов (тем) дисциплины

№ п/п	Наименование разделов (тем) дисциплины	Содержание разделов (тем) дисциплин
1.	Тема 1. Задача верификации информационных систем и общие подходы к ее решению	Задача верификации аппаратуры и программного обеспечения. Зачем нужна формальная верификация программ. Основные подходы к задаче формальной верификации. Принципы верификации моделей программ. Исторические сведения. Достижения методов формальной верификации программ. Алгоритмические и комбинаторные трудности применения метода верификации моделей программ. Общие принципы дедуктивной верификации программ. Операционная семантика императивных программ. Формальная постановка задачи верификации программ. Логика Хоара: правила вывода и свойства. Автоматизация проверки правильности программ. Моделирование схем. Системы переходов - модели Крипке. Представление систем переходов формулами логики предикатов первого порядка. Синхронные и асинхронные схемы. Степень детализации представления. Трансляция описаний программ и схем в модели Крипке
2.	Тема 2. Табличные, символьные и теоретико-автоматные методы верификации моделей программ	Темпоральная логика деревьев вычислений CTL. Синтаксис и семантика CTL. Примеры спецификаций моделей в терминах формул CTL. Темпоральная логика линейного времени PLTL. Синтаксис и семантика PLTL. Свойства живости и безопасности. Ограничения справедливости. Задача верификации моделей (model-checking). Табличный алгоритм верификации моделей для CTL. Обоснование корректности и сложности табличного алгоритма верификации моделей. Проблема “комбинаторного взрыва”. Символьные средства описания моделей. Двоичные разрешающие диаграммы (BDD). Алгоритм редукции BDD к каноническому виду (OBDD). Выполнение операций над OBDD: унарные и бинарные булевы операции, квантификация, проверка выполнимости, подсчет числа единиц. Общие представления о сложности в классе OBDD Представления неподвижной точки в CTL. Алгоритм символьной верификации моделей в CTL. Табличная верификация моделей для PLTL. Обобщенные автоматы Бюхи, трансляция формул LTL в автоматы. Сведение задачи проверки выполнимости формул PLTL к проблеме пустоты для

		автоматов Бюхи. Алгоритм двойного поиска в глубину с возвратом (DDFS) для проверки пустоты автомата Бюхи.
3.	Тема 3. Методы верификации информационных систем реального времени	Временные автоматы как формальные модели распределенных систем реального времени. Вычисления временных автоматов. Примеры использования временных автоматов для моделирования встроенных систем. Зеноновские вычисления. Синтаксис и семантика Timed CTL. Примеры формальных спецификаций поведения встроенных систем при помощи TCTL. Задача верификации моделей программ реального времени. Отношение эквивалентности часов и регионы. Регионные системы переходов. Оценка числа регионов. Сведение задачи верификации временных автоматов относительно TCTL к задаче верификации моделей Крипке относительно CTL
4.	Тема 4. Метод повышения эффективности алгоритмов верификации	Отношения бисимуляционной эквивалентности (бисимуляции) и симуляционного квазипорядка (симуляции) на моделях Крипке. Равновыполнимостьтемпоральных формул на бисимуляционно эквивалентных моделях Крипке. Вычисление классов бисимуляционной эквивалентности на конечных моделях Крипке. Упрощение моделей Крипке при помощи отношений симуляции и ибисимуляции. Редукция моделей Крипке по конусу влияния. Абстракции данных при построении моделей Крипке. Верификация моделей программ для вычислений ограниченной длины (bounded model checking, BMC). Сведение задачи BMC к задаче проверки выполнимости булевых формул (SAT). Применение автоматических средств решения задачи SAT для решения задачи BMC Интерполяционная теорема Крейга для исчисления высказываний. Построение интерполянта на основе доказательства невыполнимости КНФ. Интерполяционный алгоритм МакМиллана

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 (в отсутствие утвержденных соответствующих локальных нормативных актов на факультете)

Вопросы для контрольных работ

1. Доказательство корректности императивных программ с помощью логики Хоара. Методы построения инвариантов программ.

Типовая задача. Записать в виде предусловия и постусловия требование корректности программы, записанное на естественном языке

а).программа записывает в переменную prod произведение значений x и y

б).программа записывает в переменные quo, rem частное и остаток от деления положительного значения x на положительное значение y

в).программа меняет местами значения переменных x, y

г).программа записывает в переменную N наибольший общий делитель значений x, y

д).программа записывает в переменную m максимальный элемент непустого массива s[0 : n−1]

е).программа разворачивает непустой массив s[0 : n−1] задом наперёд

2. Устройство и возможности практического применения пакеты построения и преобразования ROBDD CUDD

Типовая задача. Построить ROBDD для заданного порядка переменных, реализующую ту же функцию, что и заданная формула.

3. Устройство программно-инструментального средства верификации моделей программ SMV. Язык описания моделей и задания спецификаций в системе SMV. Примеры применения системы SMV на практике. Верификации простых моделей с использованием системы SMV: описание моделей, формальное задание спецификаций, проверка выполнимости спецификаций.

4. Язык описания систем взаимодействующих процессов Promela. Примеры описаний распределенных систем. Примеры применения с программно-инструментального средства верификации моделей программ SPIN на практике. Верификации простых моделей с использованием системы SPIN: описание моделей, формальное задание спецификаций, проверка выполнимости спецификаций.

5. Язык описания сетей конечных временных автоматов в программно-инструментальном средстве верификации моделей программ UPPAAL. Примеры описаний сетей конечных временных автоматов. Язык запросов системы UPPAAL. Верификация простых сетей временных автоматов при помощи средства верификации UPPAAL.

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

Вопросы к экзамену

1. Основные методы верификации аппаратуры и программного обеспечения – тестирование, имитационное моделирование, дедуктивный анализ, верификация моделей.
2. Преимущества метода верификации моделей. Алгоритмические и комбинаторные трудности применения метода верификации моделей.
3. Общие принципы дедуктивной верификации программ.
4. Операционная семантика императивных программ.
5. Логика Хоара: правила вывода и свойства. Формальная постановка задачи верификации программ.
6. Автоматизация проверки правильности программ.
7. Моделирование схем. Системы переходов (модели Крипке).
8. Представление систем переходов формулами логики предикатов первого порядка.
9. Синхронные схемы. Моделирование электронных схем.
10. Асинхронные схемы. Моделирование параллельных программ.
11. Временные автоматы. Моделирование информационных систем реальноговремни.
12. Формальные языки спецификации моделей. Построение модели автомата (протокола, управляющего алгоритма) на языках описания моделей программ (SMV, Promela, сети временных автоматов).
13. Двоичные разрешающие диаграммы (BDD). Алгоритм редукции BDD к каноническому виду (ROBDD).
14. Выполнение операций над ROBDD: унарные и бинарные Булевы операции, операция ITE (мультплексорная функция от трех переменных), квантификация, проверка выполнимости, подсчет числа единиц.
15. Эффективная машинная реализация ROBDD на основе хэш-таблиц. Общие представления о сложности в классе ROBDD (зависимость сложности от порядка переменных, сложность умножения целых чисел).
16. Реализация алгоритмов работы с ROBDD на примере одного из распространенных пакетов (CUDD, ABCD, и др.).
17. Конъюнктивные нормальные формы (CNF). Задачи выполнимости КНФ. Сведение задачи выполнимости булевой формулы (или схемы) к задаче выполнимости КНФ.

18. Алгоритм DPLL. Эвристические методы повышения производительности на примере существующего SAT-солвера (Chaff, BerkMin, MiniSat, etc.) Схемные SAT-солверы (решение задачи выполнимости схемы без сведения к КНФ).
19. Темпоральная логика деревьев вычислений CTL. Синтаксис и семантика CTL. Примеры спецификаций моделей в терминах формул CTL.
20. Темпоральная логика линейного времени PLTL. Синтаксис и семантика PLTL.
21. Свойства живости и безопасности.
22. Ограничения справедливости.
23. Задача верификации моделей (model-checking).
24. Табличный алгоритм верификации моделей для CTL.
25. Обоснование корректности и сложности табличного алгоритма верификации моделей.
26. Проблема “комбинаторного взрыва”.
27. Представления неподвижной точки.
28. Алгоритм символьной верификации моделей для CTL.
29. Особенности реализации алгоритма: учет ограничений справедливости, расщепленные отношения переходов, рекомбинация произведений.
30. Табличная верификация моделей для PLTL.
31. Обобщенные автоматы Бюхи, трансляция формул LTL в автоматы.
32. Сведение задачи проверки выполнимости формул PLTL к проблеме пустоты для автоматов Бюхи.
33. Алгоритм двойного поиска в глубину с возвратом (DDFS) для проверки пустоты автомата Бюхи.
34. Временные автоматы как формальные модели распределенных систем реального времени. Вычисления временных автоматов.
35. Примеры использования временных автоматов для моделирования встроенных систем. Задача верификации временных автоматов. Зеноновские вычисления.
36. Синтаксис и семантика Timed CTL. Примеры формальных спецификаций поведения встроенных систем при помощи TCTL. Задача верификации моделей программ реального времени.
37. Отношение эквивалентности часов и регионы. Регионные системы переходов. Оценка числа регионов.
38. Сведение задачи верификации временных автоматов относительно TCTL к задаче верификации моделей Крипке относительно CTL.
39. Отношения бисимуляционной эквивалентности (бисимуляции) и симуляционногоквазипорядка (симуляции) на моделях Крипке.
40. Равновыполнимостьтемпоральных формул на бисимуляционно эквивалентных моделях Крипке.
41. Вычисление классов бисимуляционной эквивалентности на конечных моделях Крипке.
42. Упрощение моделей Крипке при помощи отношений симуляции и ибисимуляции.
43. Редукция моделей Крипке по конусу влияния.
44. Абстракции данных при построении моделей Крипке
45. Верификация моделей программ для вычислений ограниченной длины (boundedmodelchecking, BMC).
46. Сведение задачи BMC к задаче проверки выполнимости булевых формул (SAT).
47. Применение автоматических средств решения задачи SAT для решения задачи BMC.

48. Интерполяционная теорема Крейга для исчисления высказываний. Построение интерполянта на основе доказательства невыполнимости КНФ.
49. Интерполяционный алгоритм МакМиллана.
50. Адаптивный метод верификации моделей программ CEGAR.

ШКАЛА И КРИТЕРИИ ОЦЕНИВАНИЯ результатов обучения (РО) по дисциплине				
Оценка виды оценочных средств	2 (не зачтено)	3 (зачтено)	4 (зачтено)	5 (зачтено)
Знания *(виды оценочных средств: опрос, тесты)*	Отсутствие знаний	Фрагментарные знания	Общие, но не структурированные знания	Сформированные систематические знания
Умения *(виды оценочных средств: практические задания)*	Отсутствие умений	В целом успешное, но не систематическое умение	В целом успешное, но содержащее отдельные пробелы умение (допускает неточности непринципиального характера)	Успешное и систематическое умение
Навыки (владения, опыт деятельности) *(виды оценочных средств: выполнение и защита курсовой работы, отчет по практике, отчет по НИР и т.п.)*	Отсутствие навыков (владений, опыта)	Наличие отдельных навыков (наличие фрагментарного опыта)	В целом, сформированные навыки (владения), но используемые не в активной форме	Сформированные навыки (владения), применяемые при решении задач

7. Ресурсное обеспечение:
7.1. Перечень основной и дополнительной литературы

Основная литература

1. Ю.Г. Карпов. Modelchecking: верификации параллельных и распределенных программных систем. Изд-во БХВ-Петербург, 2010, 552 с.

Дополнительная литература

1. ChristelBaier. Joost-Pieter Katoen. Principles of **Model Checking**. The MIT Press. Cambridge, Massachusetts. London, England, 2008, 980 pp
2. Э.М. Кларк, О. Грамберг, Д. Пелед. «Верификация моделей программ». Москва, 2002, изд-во МЦНМО, 415 с.
3. M. R. A. Huth, M.D. Ryan. Logic in Computer Science: Modelling and Reasoning about Systems. Cambridge University Press, 2002, 387 p.
4. Kenneth L. McMillan, Interpolation and SAT-Based Model Checking. Proceedings of CAV 2003, p. 1-13.
5. Karl S. Brace, Richard L. Rudell and Randal E. Bryant. Efficient Implementation of a BDD Package. In Proceedings of the 27th ACM/IEEE Design Automation Conference (DAC 1990), pages 40–45. IEEE Computer Society Press, 1990.
6. Daniel Kroening, OferStrichman. Decision Procedures. Springer, 2008, 304 p.

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

1. Операционная система Ubuntu 18.04.
2. Операционная система ALT Linux MATE Starterkit 9 лицензия GPL
3. Программный продукт UPPAAL (http://www.uppaal.org/) академическая лицензия
4. Пакет программ CUDD построения и преобразования ROBDD
5. Программно-инструментальное средство верификации моделей программ NuSMV
6. Программно-инструментальное средство верификации моделей программ SPIN
7. Операционная система Microsoft Windows 10 Education академическая лицензия

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.mon.gov.ru - Министерство образования и науки Российской Федерации

7.4. Перечень ресурсов информационно-телекоммуникационной сети «Интернет»

1. NuSMV: a new symbolic model checker. http://nusmv.fbk.eu/.
2. CUDD: CU Decision Diagram Package. http://vlsi.colorado.edu/~fabio/CUDD/.
3. SPIN: http://spinroot.com/spin/whatispin.html

7.5. Описание материально-технического обеспечения.

Образовательная организация, ответственная 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 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.

д.ф.- м.н., профессор Захаров Владимир Анатольевич
к.ф.-м.н, доцент Подымов Владислав Васильевич