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 ПРОГРАММАПРАКТИКИ

Наименование практики:

Преддипломная практика

Уровень высшего образования:
магистратура

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. **Наименование практики, ее вид и тип:** Преддипломная практика

Вид практики: производственная
Тип: преддипломная практика

2.Цели и задачи практики

Целью преддипломной практики является формирование и развитие профессиональных знаний в сфере прикладной математики и информатики, закрепление полученных теоретических знаний по основным дисциплинам направления и специальным дисциплинам программы, овладение необходимыми компетенциями в соответствии с учебным планом подготовки.

Задачи практики:

- разработка, применение и реализация в современных программных комплексах алгоритмов компьютерной математики;
- разработка и реализация системного и прикладного программного обеспечения,
- верификация и тестирование программного обеспечения;
- разработка принципов функционирования информационно-коммуникационных систем, систем автоматического управления и анализа данных;
- разработка технической документации и методического обеспечения продукции в сфере информационных технологий, управление технической информацией;
- подбор необходимых материалов для выполнения выпускной квалификационной работы (магистерской диссертации).

3. Место практики в структуре ОПОП

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

Практика это вид учебной работы, основным содержанием которой является выполнение практических учебных, учебно-исследовательских, научно-исследовательских, производственных, творческих заданий на учебно-производственной базе факультета.

Практика направлена на приобретение студентами умений и навыков по направлению подготовки 01.04.02 «Прикладная математика и информатика».

Практика студентов является обязательной частью основной образовательной программы подготовки студентов.

4. Способ проведения практики:
Стационарный, распределенный

5. Место и период проведения практики.
Сроки проведения практики устанавливаются в соответствии с учебным планом и годовым календарным учебным графиком, с учетом теоретической подготовленности студентов, возможностей баз практик. Прохождение учебных и производственных практик может осуществляться в режиме продолжения теоретического обучения.
Производственная (преддипломная практика) проводится на факультете, в академических институтах, компаниях и фирмах. Преддипломная практика, проводимая вне факультета,

осуществляется на основе договоров или писем-подтверждений (в случае приема малых групп практикантов на безвозмездной основе) от организаций, которые предоставляют места для прохождения практики студентам факультета.
Практика проводится в 4 семестре (распределенно).

6. Требования к результатам освоения практики

В соответствии с целями основной профессиональной образовательной программы освоение практики направлено на формирование следующих компетенций и получение следующих результатов обучения:

Планируемые результаты обучения по дисциплине (модулю)		
Содержание и код компетенции.	**Индикатор (показатель) достижения компетенции**	**Планируемые результаты обучения по дисциплине, сопряженные с индикаторами достижения компетенций**
ПК-3. Способен разрабатывать и применять методы и алгоритмы машинного обучения для решения задач	ПК-3.3. Разрабатывает унифицированные и обновляемые методологии описания, сбора и разметки данных, а также механизмы контроля за соблюдением указанных методологий	ПК-3.3. З-1. Знает унифицированные и обновляемые методологии описания, сбора и разметки данных, а также механизмы контроля за соблюдением указанных методологий ПК-3.3. У-1. Умеет разрабатывать унифицированные и обновляемые методологии описания, сбора и разметки данных, а также механизмы контроля за соблюдением указанных методологий
ПК-5. Способен руководить проектами по созданию, поддержке и использованию системы искусственного интеллекта на основе нейросетевых моделей и методов	ПК-5.3. Руководит проектами по разработке систем искусственного интеллекта на основе моделей глубоких нейронных сетей и нечетких моделей и методов	ПК-5.3. З-1. Знает принципы построения моделей глубоких нейронных сетей и глубокого машинного обучения (с подкреплением и без) ПК-5.3. З-2. Знает подходы к применению моделей на основе нечеткой логики в системах искусственного интеллекта ПК-5.3. 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

ОПК-9. Способен применять методы системного анализа и программное обеспечение для системного моделирования с целью решения задач в сфере исследовательской деятельности	ОПК-9.2. Настраивает, конфигурирует и адаптирует программные средства системного моделирования для постановки и решения задач в сфере исследовательской деятельности	ОПК-9.2. З-1. Знает основные программные средства, используемые для системного моделирования в сфере исследовательской деятельности ОПК-9.2. З-2. Знает принципы работы, системную архитектуру и основные технические характеристики программных средств, используемых для системного моделирования в сфере исследовательской деятельности ОПК-9.2. У-1. Умеет сформулировать задачу и гипотезу исследования с использованием программного кода средств системного моделирования ОПК-9.2. У-2. Умеет конфигурировать и адаптировать типовые программные средства системного анализа и моделирования для решения задач в сфере исследовательской деятельности

7. **Структура и содержание практики.** Объем практики: **4** зачетных единиц – всего **144 часов**- самостоятельная работа студента).

7.1. Структура практики по разделам.

№ раздела	**Наименование раздела**	**Количество часов**			**Форма текущего контроля**
		Всего	**Контактная работа**	**Самостоятельная работа**	
1	Подготовительный этап	18		18	Собеседование
2	Основной этап.	108		108	Собеседование
3	Заключительный этап	18		18	Собеседование
	Промежуточная аттестация (зачет):				
	ИТОГО	**144**	**0**	**144**	

Оценка или зачет по производственной практике проставляется после отчета студента перед специальной комиссией с участием руководителя практики от кафедры.

7.2. Содержание разделов практики

N раз-дела	**Наименование раздела практики**	**Содержание раздела**
1	Подготовительный этап,	Инструктаж по технике безопасности и правилам охраны труда. Получение задания на практику. Сбор и анализ литературных данных по теме магистерской диссертации; подготовка обзора литературы или реферата по выбранной теме.
2	Основной этап.	Постановка целей и задач научного исследования (определение целей и задачи исследования,постановка гипотез, определение необходимых информационных источников, анализ и оценка данных источников информации для выполнения магистерской диссертации
3	Заключительный этап	Обработка и анализ полученной информации, подготовка письменного отчета по практике. Подготовка отчета о Преддипломной практике, тезисов доклада на конференции, рукописи статьи. Отчет о работе заслушивается на заседании комиссии по Преддипломной практике, лабораторном научном коллоквиуме, кафедральной научной мини-сессии и пр.

8. **Форма промежуточной аттестации (по итогам практики):** составление и защита письменного отчета. Исходя из содержания плана практики, характеристики с места практики, отзыва руководителя практики и защиты отчета выставляется дифференцированная оценка.

9. Оценочные средства, необходимые для оценивания полученных студентом результатов обучения и компетенций

9.1. Типовые задания для проведения промежуточной аттестации

Формой отчетности по итогам практики является составление отчета и его защита до начала экзаменационной сессии.

Промежуточная аттестация по результатам прохождения преддипломной практики проходит в виде защиты студентом отчета (форма отчета приведена в Приложении 1) на научном семинаре кафедры. По результатам защиты отчета студент получает аттестацию, если комиссия дала положительную оценку его работы по каждому из приведенных ниже критериев:

1. объем выполненных работ и результаты текущего контроля (оценивается на основе характеристики работы студента, данной его научным руководителем);

2. информированность о состоянии аналогичных исследований в данной области прикладной информатики и математики (оценивается на основе письменного отчета и устной защиты студента);

3. ответы на вопросы по теме исследования (оценивается на основе устной защиты студента);

4. аргументированность заключений и выводов (оценивается на основе письменного отчета и устной защиты студента);

5. качество презентации материала (оценивается на основе устной защиты студента).

Студенты, не выполнившие программы практики по уважительной причине, направляются на практику вторично, в свободное от- учебы время. Студенты, не выполнившие программы практики без уважительной причины или получившие неудовлетворительную оценку, могут быть отчислены как имеющие академическую задолженность в порядке предусмотренном положением о курсовых экзаменах и зачетах или, по представлению кафедры, направляются на практику вторично, в свободное от учебы время.

Примеры заданий на преддипломную практику:

Тема 1. Исследование и разработка детектора атак уклонением на искусственные нейронные сети.

Задание.
Атаки уклонения заключаются в том, что атакующий модифицирует тестовые данные, стараясь обмануть систему (ее классификатор или прогнозный механизм).
Требуется разработать методы и подходы к выявлению атак уклонением в режиме реального времени. И далее реализовать разработанные методы в программном обеспечении.

Общий план выполнения работы

1. Сбор и систематизация литературы по теме исследования
2. Подготовка обзора литературы по теме исследования
3. Выбор наиболее подходящих методов и подходов к выявлению атак уклонением
4. Разработка или модификация методов и подходов для данного типа нейронной сети, подбор параметров методов.
5. Реализация метода в программном коде
6. Разработка системы тестирования детектора.
7. Подготовка текста магистерской диссертации.

Тема 2. Исследование и разработка анализатора данных на предмет содержания атакующих данных

Задание.
Многие атаки на системы искусственного интеллекта заключаются в том, что атакующий модифицирует тестовые данные, стараясь обмануть систему (ее классификатор или прогнозный механизм).
Требуется разработать статистические методы и подходы к определению в тестовых данных вредоносных компонентов. И далее реализовать разработанные методы в программном обеспечении.

Общий план выполнения работы

1. Сбор и систематизация литературы по теме исследования
2. Подготовка обзора литературы по теме исследования
3. Выбор наиболее подходящих методов и подходов к определению в тестовых данных вредоносных компонентов

4. Разработка или модификация методов и подходов для данного типа нейронной сети, подбор параметров методов.
5. Реализация метода в программном коде
6. Разработка системы тестирования правильности работы программы.
7. Разработка подхода к оценке качества работы методов.
8. Проведение тестирования и оценки качества работы методов.
9. Подготовка текста магистерской диссертации.

Тема 3. Исследование и разработка комплекса имитации атак на глубокие нейронные сети

Задание.
Глубокие нейронные сети уязвимы для состязательных атак, несмотря на их огромный успех во многих областях искусственного интеллекта. Состязательная атака - это метод, который вызывает умышленную неправильную классификацию путем добавления незаметных возмущений к допустимым входным данным. На сегодняшний день исследователи разработали множество видов состязательных методов атаки. Однако с точки зрения практического развертывания эти методы страдают рядом недостатков, таких как длительное время создания атаки, высокая стоимость памяти, недостаточная надежность и низкая переносимость. Чтобы устранить эти недостатки, предлагается создать программу-генератор состязательных атак с учетом содержимого, позволяющий проводить в реальном времени недорогие и высоконадежные состязательные атаки.

Общий план выполнения работы
1. Сбор и систематизация литературы по теме исследования
2. Подготовка обзора литературы по теме исследования
3. Выбор наиболее подходящих методов и подходов к генерации состязательных атак
4. Реализация метода в программном коде
5. Разработка системы тестирования правильности работы программы.
6. Разработка подхода к оценке качества работы методов.
7. Проведение тестирования и оценки качества работы методов.
8. Подготовка текста магистерской диссертации.

Тема 4. Исследование и разработка критериев оценки устойчивости моделей машинного обучения к внешним воздействиям

Задание.
Все системы машинного обучения подвержены состязательным атакам. Естественно, что степени воздействия необходимо как-то измерять. Это необходимо для сравнения между собой разных решений и для оценки механизмов защиты. Например, один из часть используемых здесь подходов – это оценка минимальных возмущений в данных, которые “обманывают” систему. Необходимо разработать критерий оценки устойчивости моделей машинного обучения к внешним воздействиям, а также использую эталонные реализации большинства опубликованных методов состязательных атак, предложить метод настройки их параметров, минимизирующий возможность реализации атаки.

Общий план выполнения работы
1. Сбор и систематизация литературы по теме исследования
2. Подготовка обзора литературы по теме исследования
3. Выбор наиболее подходящих методов и подходов к оценке устойчивости
4. Реализация метода в программном коде
5. Разработка системы тестирования правильности работы программы.
6. Разработка системы подбора параметров эталонных реализаций систем машинного обучения Foolbox.

7. Проведение тестирования и оценки качества работы методов.
8. Подготовка текста магистерской диссертации.

Тема 5. Исследование и разработка системы профилирования искусственной нейронной сети

Задание.
Разработать профилировщик искусственной нейронной сети, который позволяет выделять реально работающие в той или иной ситуации нейроны, а также производить тестирование производительности и потребления ресурсов.

Общий план выполнения работы
1. Сбор и систематизация литературы по теме исследования
2. Подготовка обзора литературы по теме исследования
3. Выбор наиболее подходящих методов и подходов к решению задачи профилирования
4. Реализация метода в программном коде
5. Разработка системы тестирования правильности работы программы.
6. Разработка подхода к оценке качества работы методов.
7. Проведение тестирования и оценки качества работы методов.
8. Подготовка текста магистерской диссертации.

Тема 6. Исследование и разработка формальных методов верификации ИНС

Задание.
Формальные методы верификации являются единственным способом, который обеспечивает подтверждение работы нейронной. Технически они сводятся к формулированию предикатов, описывающих ограничения для нейронной сети и формальной проверки таких наборов условий. Требуется описать формальные методы верификации, сформулировать подходы, реализовать их на практике, описать возможности и существенные ограничения.

Общий план выполнения работы
1. Сбор и систематизация литературы по теме исследования
2. Подготовка обзора литературы по теме исследования
3. Классификация формальных методов верификации.
4. Выбор и подготовка эталонной нейронной сети из разного числа нейронов для тестирования методов.
5. Реализация методов в программном код
6. Разработка системы тестирования правильности работы программы.
7. Проведение тестирования и оценки качества работы методов формальной верификации, установления их ограничений.
8. Подготовка текста магистерской диссертации.

Тема 7. Исследование возможности применения существующих алгоритмов

Задание.
Гомоморфное шифрование – это шифрование данных, которое позволяет использовать зашифрованные варианты в моделях машинного обучения и получать зашифрованные же результаты, которые могут быть расшифрованы владельцем данных. Требуется разработать модель федеративной нейронной сети, поддерживающую возможность обучения на зашифрованных данных.

Общий план выполнения работы

1. Сбор и систематизация литературы по теме исследования
2. Подготовка обзора литературы по теме исследования
3. Обзор существующих методов гомоморфного шифрования.
4. Описание достоинств и недостатков методов гомоморфного шифрования.
5. Выбор метода гомоморфного шифрования для использования в обучении федеративной нейронной сети.
6. Реализация нейронной сети и метода обучения на зашифрованных данных в программном код
7. Разработка системы тестирования правильности работы программы.
8. Изучения реализации и выявление ограничений используемых методов.
9. Подготовка текста магистерской диссертации.

9.2. Критерии и шкалы оценивания

Результаты обучения («знает», «умеет», «владеет», имеет навык или опыт»), которые оцениваются в ходе текущего контроля и промежуточной аттестации по практике, соотнесенные с формируемыми компетенциями выпускников образовательной программы, приведены в п.6 настоящей программы.

Оценка «Зачетно» выставляется студенту, полностью и с высоким качеством выполнившему Программу практики; глубоко и всесторонне изучившему содержание, формы и методы научно-исследовательской работы; вовремя представившему все отчетные документы; четко и обстоятельно доложившему о результатах прохождения практики; в ответах на вопросы показавшему глубокие знания и умения в области прикладной математики и информатики; получившему положительный отзыв от руководителя практики.

Оценка «Не зачтено» выставляется студенту, не выполнившему Программу практики и индивидуальное задание; не представившему все отчетные документы; слабо знающему содержание и организацию научно-исследовательской работы; получившему неудовлетворительный отзыв от организации (учреждения, предприятия), в которой студент проходил практику.

Оценка по практике приравнивается к зачетам по теоретическому обучению и учитывается при подведении итогов общей успеваемости студентов в текущем семестре или следующем за проведением практики семестре, если практики проводится в выделенные недели после окончания сессии.

10. Ресурсное обеспечение:

а) основная литература:

1. ГОСТ 19.701-90 (ИСО 5807-85) Единая система программной документации. Схемы алгоритмов, программ, данных и систем. Условные обозначения и правила выполнения

2. ГОСТ 2.105–95. ЕСКД. Общие требования к текстовым документам [Текст]. – Взамен ГОСТ 2.105-79, ГОСТ 2.906–71; введён 1996–07–01 – М.: Изд-во стандартов, 1996. – 37с.

3. ГОСТ 2.106-96. ЕСКД. Текстовые документы [Текст]. – Взамен ГОСТ 2.106-68, ГОСТ 2.108-68, ГОСТ 2.112–70; введён 1997–07–01. 01. – М.: Изд-во стандартов, 1997.

4. ГОСТ 2.759–82 ЕСКД. Обозначения условные графические в схемах. Элементы аналоговой техники [Текст]. – Введён 1983–07–01. – М.: Изд-во стандартов, 1988.

5. ГОСТ 19.101-77 Виды программ и программных документов [Текст]. – Введён 1980–01–01. – М.: Изд-во стандартов, 1988.

6. ГОСТ 19.105-78 Единая система программной документации. Общие требования к программным документам [Текст]. – Введён 1980–01–01. – М.: Изд-во стандартов, 1988.

7. ГОСТ 19.503-79 Единая система программной документации. Руководство системного программиста. Требования к содержанию и оформлению [Текст]. – Введён 1980–01–01. – М.: Изд-во стандартов, 1988.

8. ГОСТ 19.504-79 Единая система программной документации. Единая система программной документации (ЕСПД). Руководство программиста. [Текст]. – Введён 1980–01–01. – М.: Изд-во стандартов, 1988.

9. ГОСТ 19.505-79 Единая система программной документации. Единая система программной документации (ЕСПД). Руководство оператора. Требования к содержанию и оформлению [Текст]. – Введён 1980–01–01. – М.: Изд-во стандартов, 1988.

10. ГОСТ 7.82–2001. Библиографическая запись. Библиографическое описание электронных ресурсов [Текст]. – Введён 2002–07–01. – Москва.

б) ресурсы 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

3. Универсальные базы данных EastView [Электронный ресурс] : информационный ресурс / EastViewInformationServices. - М. : [б. и.], 2012. - Загл. с титул. экрана. - Б. ц.
URL: 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

в) Материально-техническая база

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.

11. Язык преподавания: русский

12. Авторы программы

доцент факультета ВМК МГУ И. В. Чижов.

ПРИЛОЖЕНИЕ 1

- 1 -

ДНЕВНИК
преддипломной практики
Студента 2 курса магистратуры факультета вычислительной математики и кибернетики

_____
(Фамилия имя отчество)

магистерская программа_____

_____

группа _____

Тема преддипломной практики _____

_____

_____

_____

Руководитель практики от факультета _____
(должность, звание)

_____
(Фамилия Имя Отчество)

Место прохождения практики_____

_____

Руководитель практики от организации_____
(должность, звание)

_____
(Фамилия Имя Отчество)

Подписи:
Студент:

Руководители:

Решение кафедральной комиссии по приему отчета

ОЦЕНКА_____
(оценка по преддипломной практике проставляется в зачетную книжку на стр. 30-31)

Подпись председателя комиссии
Подписи членов комиссии

ОТРЫВНОЙ ЛИСТ ДНЕВНИКА
преддипломной практики
(Заполняется и сдается в учебную часть 2 курса магистратуры **до 20 февраля**)
студента 2 курса магистратуры факультета вычислительной математики и кибернетики

_____
(Фамилия имя отчество)

магистерская программа _____

_____

группа _____

Тема преддипломной практики _____

_____

_____

_____

Руководитель практики от факультета _____
(должность, звание)

_____
(Фамилия Имя Отчество)

Место прохождения практики_____

_____

_____

Руководитель практики от организации_____
(должность, звание)

_____
(Фамилия Имя Отчество)

Тема магистерской диссертации

_____

_____

Подписи:
Студент:

Научный руководитель:

ЗАДАНИЕ ПРЕДДИПЛОМНОЙ ПРАКТИКИ

Календарный план выполнения задания преддипломной практики:

1 Неделя

2 Неделя

3 Неделя

4 Неделя

5 Неделя

6 Неделя

7 Неделя

8 Неделя

9 Неделя

10 Неделя

11 Неделя

12 Неделя

Краткий отчет студента о выполнении задания преддипломной практики:
(подробный отчет студента и отзыв руководителя прилагаются на отдельных листах)

Подпись студента Дата

Краткий отзыв руководителя(ей) преддипломной практики:
(должен содержать рекомендуемую оценку)

Подпись руководителя Дата

КРАТКАЯ ИНСТРУКЦИЯ

По охране труда при использовании на рабочем месте персональных компьютеров.

ПОМНИТЕ! Неправильное обращение с ПК, кабелями может привести к тяжелому поражению электрическим током, вызвать загорание аппаратуры.

ЗАПРЕЩАЕТСЯ:

-трогать разъемы соединительных кабелей во время работы ПК;

- класть диски и рабочие материалы на бумажных носителях на монитор и клавиатуру;
- работать во влажной одежде и влажными руками;
- вытирать пыль с ПК при его включенном состоянии.

ЗАПОМНИТЕ!

При появлении запаха гари следует немедленно прекратить работу, выключить аппаратуру и сообщить об этом руководителю подразделения. В случае пожара – немедленно сообщить в пожарную охрану и самостоятельно принять возможные меры к спасению людей, имущества и ликвидации пожара.

При аварии электрической сети или пожаре должен быть немедленно отключен главный сетевой рубильник.

Перед началом работы следует убедиться в отсутствии видимых повреждений аппаратуры и рабочей мебели.

По окончании работы:

- отключить вилку штепсельной розетки (в компьютерных классах факультета ВМК этого делать не нужно);
- обо всех недостатках, обнаруженных во время работы, известить руководителя подразделения.

Подпись студента_____ /_____/

Дата _____