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 /
«_14_» октября 2021г.

РАБОЧАЯ ПРОГРАММА ПРАКТИКИ

Наименование практики:

Научно-исследовательская работа

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 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. **Наименование практики, ее вид и тип:** научно-исследовательская работа

Вид практики: производственная
Тип: научно-исследовательская работа

2.Цели и задачи практики

Целью научно-исследовательской работы 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:

- сбор, анализ и обработка научной информации по тематике исследования в области прикладной математики и информатики;
- планирование исследования и выбор методов решения поставленных задач в области прикладной математики и информатики;
- проведение исследования в области прикладной математики и информатики с применением выбранных методов и средств;
- анализ полученных результатов и подготовка рекомендаций по продолжению исследования;
- подготовка научных публикаций, отдельных разделов аналитических обзоров и отчетов по результатам научно-исследовательской работы в области прикладной математики и информатики;
- представление результатов научно-исследовательской деятельности, выступление с сообщениями и докладами по тематике проводимых исследований в области прикладной математики и информатики;
- подбор необходимых материалов для выполнения выпускной квалификационной работы (магистерской диссертации).

3. Место практики в структуре ОПОП

Дисциплина (модуль) относится к обязательной части основной профессиональной образовательной программы.

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.

Входные требования для освоения практики, предварительные условия.

Перечень дисциплин, которые должны быть освоены для начала прохождения научно-исследовательской работы:

современная философия и методология науки, история и методология прикладной математики и информатики.

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.
Практика проводится в 3 семестре (распределённо).
6.
7. 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**
ОПК-5. Способен разрабатывать алгоритмы и программные средства для решения задач в области создания и применения искусственного интеллекта	ОПК-5.2. Разрабатывает оригинальные программные средства для решения задач в области создания и применения искусственного интеллекта	ОПК-5.2. З-1. Знает принципы разработки оригинальных программных средств для решения профессиональных задач ОПК-5.2. У-1. Умеет разрабатывать оригинальные программные средства для решения задач в области создания и применения искусственного интеллекта
ОПК-6. Способен адаптировать и применять на практике классические и новые научные принципы и методы исследований для решения задач в области создания и применения технологий и систем искусственного интеллекта и методы исследований	ОПК-6.2. Решает профессиональные задачи на основе применения новых научных принципов и методов исследования	ОПК-6.2. З-1. Знает особенности решения профессиональные задачи на основе применения новых научных принципов и методов исследования ОПК-6.2. У-1. Умеет разрабатывать, контролировать, оценивать и исследовать компоненты профессиональной деятельности; планировать самостоятельную деятельность в решении профессиональных задач

ОПК-7. Способен использовать методы научных исследований и математического моделирования в области проектирования и управления системами искусственного интеллекта	ОПК-7.2. Осуществляет методологическое обоснование научного исследования, создание и применение библиотек искусственного интеллекта	ОПК-7.2. З-1. Знает приемы методологического обоснования научного исследования, методы организации библиотек искусственного интеллекта ОПК-7.2. У-1. Умеет проводить методологическое обоснование научного исследования, в том числе посредством создания и использования библиотек искусственного интеллекта

7. Структура и содержание практики. Объем практики: **24** зачетных единиц – всего **864 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	36		36	Собеседование
2	Основной этап.	684		684	Собеседование
3	Заключительный этап	144		144	Собеседование
	Промежуточная аттестация (экзамен):				
	ИТОГО	**864**	**0**	**864**	

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 «НИР»**	**Содержание раздела**
1	Подготовительный этап,	Планирование научно-исследовательской работы, ознакомление студента с заданием на практику
2	Основной этап.	Анализ информационных ресурсов по избранной теме. Математическая постановка задачи. Выбор методов решения задачи. Разработка алгоритмов и программного обеспечения. Проведение расчетов
3	Заключительный этап	Обработка и анализ полученной информации, подготовка письменного отчета по практике. Подготовка отчета о НИР, тезисов доклада на конференции, рукописи статьи. Отчет о работе

		заслушивается на заседании комиссии по НИР, 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

Промежуточная аттестация по результатам выполнения НИР проходит в виде защиты студентом отчета на научном семинаре (коллоквиуме) лаборатории (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 математики и информатики (оценивается на основе письменного отчета о НИР 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 о НИР и устной защиты студента);
5. качество презентации материала (оценивается на основе устной защиты студента).

Примеры постановки задач НИР:

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.

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.

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.

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.

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.

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.

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.

Структура отчета о выполненной НИР

1. Титульный лист, ФИО студента, ФИО научного руководителя
2. Тема магистерской диссертации
3. Индивидуальное задание студента
4. Отчет по результатам научно-исследовательской работы
5. Отзыв научного руководителя с указанием аттестации студента по результатам научно-исследовательской работы

Отчет по НИР подписывается студентом и научным руководителем.

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 «Зачтено» 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 зачетно» 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 экзаменам 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.

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.

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, 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.