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 ДИСЦИПЛИНЫ

Спецсеминар "Искусственный интеллект в кибербезопасности"

Наименование дисциплины (модуля):

Теория информации и теория кодирования

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 №7, 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: отсутствуют

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**
ПК-6. Способен руководить проектами по созданию комплексных систем на основе аналитики больших данных в различных отраслях со стороны заказчика	ПК-6.1. Руководит проектами по построению комплексных систем на основе аналитики больших данных в различных отраслях со стороны заказчика	ПК-6.1. З-1. Знает методологию и принципы руководства проектами по созданию, поддержке и использованию комплексных систем на основе аналитики больших данных со стороны заказчика ПК-6.1. З-2. Знает специфику сфер и отраслей, для которых реализуется проект по аналитике больших данных ПК-6.1. У-1. Умеет решать задачи по руководству коллективной проектной деятельностью для создания, поддержки и использования комплексных систем на основе аналитики больших данных со стороны заказчика ПК-6.1. У-2. Умеет выявлять небольшие по масштабу проекты аналитики, которые потенциально могут представлять интерес для ряда подразделений / служб или для организации в целом ПК-6.1. У-3. Умеет выявлять области деловой деятельности, которые потенциально могут получить отдачу от аналитики

4. Объем дисциплины (модуля) составляет 13 з.е., в том числе 144 академических часа, отведенных на контактную работу обучающихся с преподавателем, 324 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:

№ раздела	Наименование раздела	Количество часов			Форма текущего контроля
		Всего	Семинарские занятия	Самостоятельная работа	
1	Спецсеминар (1 семестр)	72	36	36	Собеседование
2	Спецсеминар (2 семестр)	72	36	36	Собеседование
3.	Курсовая работа (2 семестр)	180		180	Защита курсовой работы
3	Спецсеминар (3 семестр)	72	36	36	Собеседование
4	Спецсеминар (4 семестр)	72	36	36	Собеседование
	Промежуточная аттестация (зачет):				
	ИТОГО	**468**	**144**	**324**	

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 рамках спецсеминара полностью отражает современную тенденцию в применении технологии искусственного интеллекта для построения новых систем кибербезопасности, а также в разработке новых методов и подходов к обеспечению безопасности самой технологии искусственного интеллекта. Содержание программы находится на стыке различных областей знания. Несомненно, основу здесь составляет математика. Слушатели программы познакомятся с различными математическими методами, которые используются как в защите информации, так и в технологиях искусственного интеллекта. Упор делается на методы дискретной математики (графы, теория кодирования, комбинаторика, булевы функции), на аппарат математической логики, линейной алгебры, теории игр, теории вероятностей и математической статистики.

Примерные темы курсовых работ:
1. Исследование и разработка детектора атак уклонением на искусственные нейронные сети.
2. Исследование и разработка анализатора данных на предмет содержания атакующих данных
3. Исследование и разработка комплекса имитации атак на глубокие нейронные сети
4. Исследование и разработка критериев оценки устойчивости моделей машинного обучения к внешним воздействиям

5. Исследование и разработка системы профилирования искусственной нейронной сети
6. Исследование и разработка формальных методов верификации ИНС
7. Исследование возможности применения существующих алгоритмов

Критерии оценки курсовой работы
Курсовая работа оценивается «отлично», если
1. Тема работы четко сформулирована, тема раскрыта полностью, дано обоснование ее актуальности.
2. Работа выполнена самостоятельно, присутствуют собственные обобщения, заключения и выводы.
3. Использовано оптимальное количество литературы и источников по теме работы, их изучение проведено на высоком уровне.
4. Работа выполнена и представлена в срок,
5. Работа безукоризненна в отношении оформления (орфография, пунктуация, стиль)
6. Оформление текста (цитирование, ссылки, оформление списка использованных источников и т.д.) строго соответствует требованиям стандарта.
Курсовая работа оценивается «хорошо», если:
1. Тема работы четко сформулирована, работы в целом раскрыта.
2. Работа выполнена самостоятельно, присутствуют собственные обобщения, заключения и выводы.
3. Использованы основная литература и источники по теме работы, однако работа имеет недостатки в проведенном исследовании, прежде всего в изучении источников.
4. Работа выполнена в срок и представлена в срок.
5. Работа безукоризненна в отношении оформления (орфография, пунктуация, стиль)
6. В оформлении текста (цитирование, ссылки, оформление списка использованных источников и т.д.) нет грубых ошибок.
Курсовая работа оценивается «удовлетворительно», если:
1. Тема работы четко сформулирована, но раскрыта недостаточно полно.
2. Работа выполнена самостоятельно, но собственные обобщения, заключения и выводы не достаточно полно сформулированы.
3. Литературные источники по теме работы использованы в недостаточном объеме, их анализ слабый или вовсе отсутствует.
4. Работа выполнена с нарушениями графика.
5. В отношении оформления (орфография, пунктуация, стиль) есть недостатки.
6. В оформлении текста (цитирование, ссылки, оформление списка использованных источников и т.д.) допущены отступление от требований стандарта.
Курсовая работа не может быть оценена положительно, если:
1. Вся работа или какая-либо ее часть, является плагиатом, скомпилирована из фрагментов работ других авторов и носит несамостоятельный характер, т.е. если студент выдает чужую работу за свою. Использование текстов, взятых на специальных сайтах сети Интернет, в качестве «своей» работы также является плагиатом.
2. Содержание курсовой работы не соответствует ее теме.
3. При написании работы были использованы источники и литература, не соответствующие заявленной теме.
4. Нарушены орфографические, пунктуационные, стилистические нормы при оформлении работы.
5. Оформление текста (цитирование, ссылки, оформление списка использованных источников и т.д.) не соответствует требованиям стандарта.

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

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

Оценка «Зачтено» выставляется студенту, полностью и с высоким качеством выполнившему Программу спецсеминара; глубоко и всесторонне изучившему содержание, формы и методы научной работы; вовремя представившему все отчетные документы.

Оценка «Незачтено» выставляется студенту, не выполнившему Программу спецсеминара и индивидуальное задание.

ШКАЛА И КРИТЕРИИ ОЦЕНИВАНИЯ результатов обучения (РО) по дисциплине (модулю)				
Оценка РО и соответствующие виды оценочных средств	2 (не зачтено)	3 (зачтено)	4 (зачтено)	5 (зачтено)
Знания Зачет	Отсутствие знаний	Фрагментарные знания	Общие, но не структурированные знания	Сформированные систематические знания
Умения 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) Зачет, практические занятия	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. Цилькер Б.Я., Орлов С.А. Организация ЭВМ и систем. СПб, «Питер», 2007
2. Степанов А.Н. Архитектура вычислительных систем и компьютерных сетей. СПб, «Питер», 2006
3. Крейгон Х. Архитектура компьютеров и ее реализация. М., «Мир», 2004

Дополнительная литература

1. Корнеев В.В. Вычислительные системы. М, «Гелиос АРВ», 2004
2. Королев Л.Н. Архитектура процессоров электронных вычислительных машин. М., Факультет ВМиК МГУ, 2003
3. Воеводин В.В., Воеводин Вл.В. Параллельные вычисления. СПб, «БХВ – Петербург», 2002
4. Королев Л.Н. Структуры ЭВМ и их математическое обеспечение. М., Наука, 1978

7.2. Перечень лицензионного программного обеспечения, в том числе отечественного производства

При реализации дисциплины может быть использовано следующее программное обеспечение:

1. Операционная система Ubuntu 18.04.
2. Программный продукт Python 3.5.1 (64-bit) Python Software Foundation
3. 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.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

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

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

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.

доцент факультета ВМК МГУ И. В. Чижов.

10. Язык преподавания - русский.