МИНИСТЕРСТВО ЦИФРОВОГО РАЗВИТИЯ, СВЯЗИ
И МАССОВЫХ КОММУНИКАЦИЙ РОССИЙСКОЙ ФЕДЕРАЦИИ
Северо-Кавказский филиал
ордена Трудового Красного Знамени федерального государственного
бюджетного образовательного учреждения высшего образования
«Московский технический университет связи и информатики»

Утверждаю
Зам. директора по УВР
_____ А.Г. Жуковский
«29» 08 2022 г.

Искусственный интеллект и машинное обучение Б1.О.24
рабочая программа дисциплины

Кафедра: Информатика и вычислительная техника
Направление подготовки: **10.03.01 Информационная безопасность**
Профиль: **Безопасность компьютерных систем.**
Формы обучения: **очная**

Распределение часов дисциплины по семестрам (для очной формы обучения), курсам (для заочной формы обучения)

Вид учебной работы	ОФ		ЗФ	
	ЗЕ	часов	ЗЕ	часов
Общая трудоемкость дисциплины, в том числе (по семестрам, курсам):	3	108/5сем		
Контактная работа, в том числе (по семестрам, курсам):		54/5сем		
Лекции		18/5сем		
Лабораторных работ		18/5сем		
Практических занятий		18/5сем		
Семинаров				
Самостоятельная работа		54/5сем		
Контроль				
Число контрольных работ (по курсам)				
Число КР (по семестрам, курсам)				
Число КП (по семестрам, курсам)				
Число зачетов с разбивкой по семестрам (курсам)				
Число экзаменов с разбивкой по семестрам (курсам)		1/5сем		

Программу составил:
Доцент кафедры ИВТ, к.т.н., с.н.с. Ткачук Е.О.

Рецензент:
Ведущий сотрудник ФГУП «РНИИРС, д.т.н., доцент Елисеев А.В.

Рабочая программа дисциплины
«Искусственный интеллект и машинное обучение »

разработана в соответствии с ФГОС ВО:
направления подготовки 10.03.01 «Информационная безопасность», утвержденным приказом Министерства образования и науки Российской Федерации от 17 ноября 2020г. N 1427.

Составлена на основании учебного плана
направления 10.03.01 «Информационная безопасность», профиля «Безопасность компьютерных систем», одобренного Учёным советом СКФ МТУСИ, протокол № 9 от 25.04.2022, и утвержденного директором СКФ МТУСИ 25.04.2022 г.

Рассмотрена и одобрена на заседании кафедры
«Информатика и вычислительная техника»

Протокол от «29» 08 2022г. № 1

Зав. кафедрой _____ С.В. Соколов

Визирование для использования в 20__/20__ уч. году

Утверждаю
Зам. директора по УВР ________________
«___» _______ 20__ г.
Рабочая программа пересмотрена, обсуждена и одобрена на заседании кафедры

«Информатика и вычислительная техника»

Протокол от «___» _______ 20__ г. № ____
Зав. кафедрой _____________________

Визирование для использования в 20__/20__ уч. году

Утверждаю
Зам. директора по УВР ________________
«___» _______ 20__ г.
Рабочая программа пересмотрена, обсуждена и одобрена на заседании кафедры
«Информатика и вычислительная техника»

Протокол от «___» _______ 20__ г. № ____
Зав. кафедрой _____________________

Визирование для использования в 20__/20__ уч. году

Утверждаю
Зам. директора по УВР ________________
«___» _______ 20__ г.
Рабочая программа пересмотрена, обсуждена и одобрена на заседании кафедры
«Информатика и вычислительная техника»

Протокол от «___» _______ 20__ г. № ____
Зав. кафедрой _____________________

Визирование для использования в 20__/20__ уч. году

Утверждаю
Зам. директора по УВР ________________
«___» _______ 20__ г.
Рабочая программа пересмотрена, обсуждена и одобрена на заседании кафедры
«Информатика и вычислительная техника»

Протокол от «___» _______ 20__ г. № ____
Зав. кафедрой _____________________

1. Цели изучения дисциплины

Целью освоения дисциплины является получение обучающимися систематизированных теоретических знаний о базовых принципах и методах построения интеллектуальных систем защиты информации, освоение ими типовых приемов решения практических задач защиты информации с использованием методов искусственного интеллекта, привитие базовых навыков анализа и проектирования интеллектуальных систем защиты информации с применением современных технологий интеллектуального анализа данных.

2. Планируемые результаты обучения

Изучение дисциплины направлено на формирование у выпускника способности решать профессиональные задачи в соответствии с ***эксплуатационным*** видом деятельности:

Результатом освоения дисциплины являются сформированные у выпускника следующие компетенции:

Компетенции выпускника, формируемые в результате освоения дисциплины (в части, обеспечиваемой дисциплиной)
ОПК-2: Способен применять информационно-коммуникационные технологии, программные средства системного и прикладного назначения, в том числе отечественного производства, для решения задач профессиональной деятельности
Знать:
- методы разработки оригинальных алгоритмов и программных продуктов с использованием современных технологий
Уметь:
- обосновывать выбор современных информационно- коммуникационных и интеллектуальных технологий, разрабатывать оригинальные программные средства для решения профессиональных задач
Владеть:
- методами разработки оригинальных программных средств, в том числе с использованием современных информационно- коммуникационных и интеллектуальных технологий, для решения профессиональных задач.
ОПК-8. Способен осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических документов в целях решения задач профессиональной деятельности
Знать:
-методики поиска, сбора и обработки информации; актуальные российские и зарубежные источники информации в сфере профессиональной деятельности; методы системного анализа
Уметь:
- применять методики поиска, сбора и обработки информации; осуществлять критический анализ и синтез информации, полученной из разных источников; применять системный подход для решения поставленных задач;
Владеть:
- практическим опытом поиска, сбора и обработки, критического анализа и синтеза информации; методикой системного подхода для решения поставленных задач.

3. Место дисциплины в структуре образовательной программы

Требования к предварительной подготовке обучающегося (предшествующие дисциплины, модули, темы):	
1	Дисциплина «Искусственный интеллект и машинное обучение» является логическим продолжением дисциплины Б1.О.11 «Основы информационной безопасности»», знание которой в объеме требований образовательной программы является необходимым.
2	Успешное освоение дисциплины «Искусственный интеллект и машинное обучение» базируется также на знаниях, приобретенных из дисциплин: Б1.О.06 «Физика», Б1.О.07 «Иностранный язык», Б1.О.12 «Введение в информационные технологии».
Последующие дисциплины и практики, для которых освоение данной дисциплины необходимо:	
1	Дисциплина является базовой для успешного освоения дисциплин: Б1.О.25 «Методы и средства криптографической защиты информации», Б1.О.29 «Основы управления информационной безопасностью», Б1.О.33 «Программно-аппаратные средства защиты информации», Б1.О.37 «Комплексное обеспечение защиты информации»

4. Структура и содержание дисциплины

4.1 Очная форма обучения, 4 года (всего 108 часов, 54 аудиторных часов, 54 часов самостоятельной работы)

Код зан.	Тема и краткое содержание занятия	Вид зан.	Кол. часов	Компетенции	УМИО
Курс 1, Семестр 2					
Модуль 1. Методы машинного обучения (Лекции 8, ПЗ 8, ЛР 10, СРС 28) 54 часа					
1.1	Лекция 1. Основные задачи, ветки и методы машинного обучения. Статистические подходы к машинному обучению	Л1.	2	ОПК-2, ОПК-8	Л1.1 Л1.2 Л1.3
1.2	Лекция 2. Нейронные сети	Л2.	2	ОПК-2, ОПК-8	Л1.1 Л1.2 Л1.3
1.3	Лекция 3. Модели простейшей и множественной регрессии. Полиномиальная регрессия	Л3.	2	ОПК-2, ОПК-8	Л1.1 Л1.2 Л1.3
1.4	Лекция 4. Вероятностный подход к решению задачи классификации на примере наивного байесовского классификатора и его обобщений	Л4.	2	ОПК-2, ОПК-8	Л1.1 Л1.2 Л1.3
1.5	Практическое занятие 1 Использование однослойного перцептрона в практических задачах	ПЗ1	2	ОПК-2, ОПК-8	Л1.1 Л1.2 Л1.3
1.6	Практическое занятие 2 Использование радиальных базисных функций	ПЗ2	4	ОПК-2, ОПК-8	Л1.1 Л1.2 Л1.3
1.7	Лабораторная работа 1 Использование нейронной сети в задачах регрессии	ЛР1	4	ОПК-2,	Л1.1 Л1.2

				ОПК-8	Л1.3
1.8	Лабораторная работа 2 Применение нейронных сетей для прогнозирования временных рядов	ЛР2	6	ОПК-2, ОПК-8	Л1.1 Л1.2 Л1.3
1.9	Практическое занятие 3. Решение задачи классификация на основе алгоритма наивного байеса	ПЗ3	2	ОПК-2, ОПК-8	Л1.1 Л1.2 Л1.3
	1. Примеры и классификация задач машинного обучения. 2. Типы данных, обработка данных. 3. Меры сходства, метрики, ультраметрики. 4. Гауссовское распределение и распределения, с ним связанные. 5. Коэффициент корреляции. 6. Однофакторная линейная регрессия. 7. Проверка гипотез о коэффициентах регрессии	СРС	28	ОПК-2, ОПК-8	Л1.1 Л1.2 Л1.3
Модуль 2. Прикладные задачи искусственного интеллектах (Лекции 10, ПЗ 10, ЛР 8, СРС 26) 54 часа					
2.1	Лекция №5 Основы персональной информационной безопасности, вредоносное ПО, парольные системы.	Л5	2	ОПК-2, ОПК-8	Л1.1 Л1.2 Л1.3
2.2	Лекция №6 Симметричные системы шифрования, несимметричная криптография. Алгоритм шифрования RSA и Эль-Гамаля, электронная подпись	Л6	2	ОПК-2, ОПК-8	Л1.1 Л1.2 Л1.3
2.3	Лекция №7 Базовые понятия информационной безопасности, методы защиты информации. Роль ИИ в кибербезопасности, оценка алгоритмов машинного обучения	Л7	2	ОПК-2, ОПК-8	Л1.1 Л1.2 Л1.3
2.4	Лекция №8. Применение МО для обнаружения сетевых атак и аномалий, межсетевые экраны и системы обнаружения вторжений	Л8	2	ОПК-2, ОПК-8	Л1.1 Л1.2 Л1.3
2.5	Лекция №9. Основы биометрии, виды аутентификации и задача отбора признаков. Состязательные атаки на биометрические системы	Л9	2	ОПК-2, ОПК-8	Л1.1 Л1.2 Л1.3
2.6	Практическое занятие №4. Обзор ПО информационной безопасности с использованием методов искусственного интеллекта	ПЗ4	6	ОПК-2, ОПК-8	Л1.1 Л1.2 Л1.3
2.7	Практическое занятие №5 Криптоалгоритмы RSA и Эль Гамаля	ПЗ5	4	ОПК-2, ОПК-8	Л1.1 Л1.2 Л1.3
2.8	Лабораторная работа № 3 Криптоалгоритм RSA	ЛР3	4	ОПК-2, ОПК-8	Л1.1 Л1.2 Л1.3
2.9	Лабораторная работа № 4 Алгоритмы ЭЦП	ЛР4	4	ОПК-2, ОПК-8	Л1.1 Л1.2

					Л1.3
2.10	1. Алгоритм CART. 2. Алгоритм C4.5. 3. Линейные классификаторы. 4. Алгоритм обучения персептрона. 5. Теорема Новикова. 6. 2-х-слойный персептрон. 7. Многослойные нейронные сети. 8. Метод обратного распространения ошибки	СРС	26	ОПК-2, ОПК-8	Л1.1 Л1.2 Л1.3
	Экзамен			ОПК-2, ОПК-8	Л1.1 Л1.2 Л1.3
Итого – 108 часов					

5. Учебно-методическое и информационное обеспечение дисциплины

5.1. Рекомендуемая литература

5.1.1. Основная литература

Код	Авторы, составители	Заглавие	Издательство, год	Кол.
Л1.1	Орлов, А. И.	Искусственный интеллект: статистические методы анализа данных : учебник /	Москва : Ай Пи Ар Медиа, 2022. — 843 с	Э1
Л1.2	Д. Рутковская, М. Пилиньский, Л. Рутковский	Нейронные сети, генетические алгоритмы и нечеткие системы	Москва :Гор. линия-Телеком, 2013. - 384 с.	Э2
Л1.3	Шаньгин В. Ф.	Информационная безопасность и защита информации	Саратов: Профобразование, 2019. — 702 с. — ISBN 978-5-4488-0070-2	Э3

5.1.2. Дополнительная литература

Код	Авторы, составители	Заглавие	Издательство, год	Кол.
Л2.1	О.И. Шелухин, Д.Ж. Сакалема, А.С. Филинова	Обнаружение вторжений в компьютерные сети (сетевые аномалии): Учебное пособие для вузов /.. ISBN 978-5-9912-0323-4, 500 экз. - Текст : электронный. - URL:	Москва : Гор. линия-Телеком, 2013. - 220 с.: ил.;	Э4

5.1.3. Учебно-методическое обеспечение для самостоятельной работы обучающихся

Код	Авторы, составители	Заглавие	Издательство, год	Кол.
Л3.1	Нестеров С.А.	Основы информационной безопасности [Электронный ресурс]: учебное пособие/— Электрон. текстовые данные.	СПб.: Санкт-Петербургский политехнический университет Петра Великого, 2014. — 322 с.	Э5

5.2. Электронные образовательные ресурсы

Э1	https://www.iprbookshop.ru/117029.html
Э2	https://znanium.com/catalog/product/414545
Э3	https://www.iprbookshop.ru/87995.html
Э4	https://znanium.com/catalog/product/421968
Э5	https://www.iprbookshop.ru/43960

5.3. Программное обеспечение

П.1	1. AVAST Free Antivirus 2. AVG AntiVirus Free 3. Dr.Web Antivirus 4. Антивирус Касперского 5. ESET NOD32 Антивирус 6. AVZ Antivirus 7. Avira Free Antivirus 8. Norton AntiVirus 9. McAfee Antivirus 10. Emsisoft Anti-Malware	Антивирусное ПО. Свободное, условно свободное или триал-версии.

	11. BullGuard Antivirus 12. Protector Plus Antivirus 13. Panda Antivirus 14. Ashampoo Anti-Virus 14. G Data AntiVirus 16. K7 AntiVirus 17. VIRUSfighter 18. Twister Antivirus	
П.2	1. Wise Folder Hider 2. Secure Folders 3. Anvide Lock Folder 4. Folder Lock 5. Easy File Locker 6. Folder Guard 7. DEKSI USB Security 8. Locker (защита папок и дисков) 9. Advanced Hider 10. Hide Folders XP 11. Hide Files	Программное обеспечение по защите и сокрытию файлов и папок. Свободное, условно свободное или триал-версии.
П.3	1. TrustPort Tools 2. Cryptic Disk 3. Locker (скрытие файлов) 4. Max File Encryption 5. Secure Disk 6. Masker 7.1 7. Fox Secret 8. HideInPicture 1.0 9. Шифровальщик 10. Advanced Encryption Package 11. Gpg4win 12. Cryptic Disk Professional 13. CyberSafe Files Encryption 14. Steganos Privacy Suite 15. Lavasoft Privacy Toolbox 16. pkiImage Free Edition	Программное обеспечение по шифрованию, безвозвратному удалению, стеганографии. Свободное, условно свободное или триал-версии.
П.4	1. Hetman Partition Recovery 2. Active File Recovery 3. R-Studio 7.6 4. Auslogics File Recovery 5. Active UNDELETE 6. Paragon Rescue Kit 7. Wise Data Recovery 8. Puran File Recovery 9. O&O DiskRecovery 10. Tenorshare Any Data Recovery 11. Power Data Recovery 12. GetDataBack	Программное обеспечение по восстановлению данных. Свободное, условно свободное или триал-версии.

	13. Recover My Files	
	14. R-Undelete	
	15. Handy Recovery	
	16. Ashampoo Undeleter	
П.5	1. Iperius Backup 2. FBackup 3. Backup4all 4. Uranium Backup Free 5. Simple Data Backup 6. Personal Backup 7. Back4Sure 8. SyncBackFree 9. Handy Backup 10. EASEUS Todo Backup 8.0 Free Edition 11. Exiland Backup Free 4.0 12. Nero BackItUp 13. Paragon Rescue Kit 14.0 Free 14. Action Backup 15. LimBackup 16. AVSbackup 17. ExtraBackup 18. Cobian Backup 19. Backup & Recovery 10 Build 9169 Free Edition 20. Information Backup System	Программное обеспечение по резервному копированию данных. Свободное, условно свободное или триал-версии.
П.6	MS Word – с лицензией	
П.7	Power Point – с лицензией	

6. Материально-техническое обеспечение дисциплины

6.1 МТО лекционных занятий	
1	Лекционная аудитория, оборудованная интерактивной доской, проектором
6.2 МТО лабораторных работ и практических занятий	
1	Компьютерная аудитория с выходом в интернет
6.3 МТО рубежных контролей, экзамена	
1	Компьютерная аудитория

7. Методические указания для обучающихся по освоению дисциплины

7.1 Указания по самостоятельной работе студента

Достижение целей эффективной подготовки студентов в вузах невозможно без их целеустремленной самостоятельной работы. При этом, безусловно, нельзя обойтись без живого общения и консультирования со стороны профессорско-преподавательского состава Самостоятельная работа студентов является составной частью учебной работы и имеет целью закрепление и углубление полученных знаний и навыков, поиск и приобретение новых знаний, в том числе с использованием автоматизированных обучающих курсов (систем), а также выполнение учебных заданий, подготовку к предстоящим занятиям, зачетам и экзаменам. Обязательным компонентом самостоятельной работы студентов

является внеаудиторный практикум по иностранному языку.

Самостоятельная работа организуется преподавателями, обеспечивается и контролируется кафедрами. Она предусматривает, как правило, разработку рефератов, выполнение расчетно-графических, вычислительных работ, моделирования и других творческих заданий в соответствии с учебной программой (тематическим планом изучения дисциплины). Основная цель данного вида занятий состоит в обучении курсантов методам самостоятельной работы с учебным материалом.

Материал, подлежащий обработке на самостоятельных занятиях, намечается при разработке программы самостоятельной работы. Опыт, накопленный кафедрами в организации самостоятельных занятий, что материал выделяемый на такие занятия, должен удовлетворять следующим требованиям:

- быть изложенным в учебнике достаточно полно и с примерами;
- обеспечиваться достаточным количеством литературы, учебных пособий. учебно-методических материалов, образцов техники
- содержать материал. углубляющий знания, полученные на лекции;
- осваивать проблемные еще не полностью решенные вопросы.

Проведению самостоятельной работы (как и любого другого вида занятий) должна предшествовать подготовка как преподавателя, так и обучаемых.

Постановку задачи обучаемым на проведение самостоятельного занятия преподаватель осуществляет на одном из занятия, предшествующему данному. Он разъясняет смысл занятия и указывает, что к нему студенты должны приготовить. Задание на самостоятельную работу должно быть выдано заблаговременно с тем, чтобы слушатели имели время на информационный поиск в библиотеке необходимых пособий.

Методику самостоятельной работы все обучаемые выбирают индивидуально, но методика достижения конечной цели может определяться преподавателем и включать: последовательность изучения и усвоения учебно-методического материала, пособий, руководств, наставлений, техники и т.д.; определение главного в изучаемом материале, материале, который необходимо законспектировать; просмотр учебных кинофильмов и их обсуждение; работу студентов по индивидуальным заданиям; опрос обучаемых в течении 7-10 минут с целью проверки усвоения главного из прочитанного материала.

При возникновении затруднений у обучаемых в разрешении вопросов задания преподавателю необходимо предусмотреть, чтобы каждый обучаемый мог получить оперативную консультацию по любому вопросу, если же при самостоятельной работе возникают затруднения по одному и тому же материалу (вопросу) у многих обучаемых, то желательно провести групповую консультацию.

Для контроля усвоения учебного материала целесообразно проводить в групповое собеседование или обсуждение изучаемого материала, проведение контрольных работ и т.п. Контрольные мероприятия при должной их организации позволяют не только оценивать знания материала, но и углубить и закрепить его у обучаемых.

Приветствуется использование компьютеров, которое:

- расширяет информационную баз) учебных занятий;
- повышает активность обучаемых, из пассивного получателя информации они превращаются в её добытчиков:
- способствует развитию способностей к анализу и обобщению, улучшает связанность, широту и глубину мышления;
- облегчает усвоение абстрактного материала, позволяет многое из него представить в виде конкретных образов;
- приучает к точности, аккуратности, последовательности действий способствует развитию самостоятельности.

Компьютерные технологии и программные продукты для выполнения самостоятельной работы по освоению учебного материала необходимо использовать в соответствии с указаниями методических разработок раздела 5 настоящей Рабочей программы.

Для более углубленного изучения материала по дисциплине целесообразно использовать учебные курсы сайта http://www.intuit.ru/ .

Таблица 7.1 – Учебный материал, выносимый на самостоятельное изучение студентам очной формы обучения

№	Темы, разделы, вынесенные на самостоятельную подготовку, вопросы для подготовки к практическим и лабораторным занятиям; курсовые работы, содержание контрольных работ; рекомендации по использованию литературы, ЭВМ и др.	Часов всего: 54	Неделя
Модуль 1 – 28 часов			
1	Примеры и классификация задач машинного обучения.	4	1,2
2	Типы данных, обработка данных.	4	3
3	Меры сходства, метрики, ультраметрики.	4	4
4	Гауссовское распределение и распределения, с ним связанные.	4	5
5	Коэффициент корреляции.	4	6
6	Однофакторная линейная регрессия.	4	7
7	Проверка гипотез о коэффициентах регрессии	4	8
Модуль 2 – 26 часов			
8	Алгоритм CART.	3	9
9	Алгоритм C4.5.	3	10
10	Линейные классификаторы.	3	11
11	Алгоритм обучения персептрона.	3	12
12	Теорема Новикова.	3	13
13	2-х-слойный персептрон.	3	14
14	Многослойные нейронные сети.	4	15
15	Метод обратного распространения ошибки	4	16

Дополнения и изменения в рабочей программе