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
_____ Н.А. Андреева
«29» 04 2024 г.

Искусственный интеллект и машинное обучение в кибербезопасности Б1.О.24

рабочая программа дисциплины

Кафедра: **Информационной безопасности**
Направление подготовки: **10.03.01 Информационная безопасность**
Профиль: **Безопасность компьютерных систем (по отрасли или в сфере профессиональной деятельности)**
Формы обучения: **очная**

Распределение часов дисциплины по семестрам (для очной формы обучения (ОФО))

Вид учебной работы	ОФО	
	ЗЕ	часов
Общая трудоемкость дисциплины, в том числе (по семестрам, курсам):	4	144/5 сем
Контактная работа, в том числе (по семестрам, курсам):		68/5 сем
Лекции		34/5 сем
Лабораторных работ		16/5 сем
Практических занятий		18/5 сем
Семинаров		
Самостоятельная работа		76/5 сем
Контроль		
Число контрольных работ (по курсам)		
Число КР (по семестрам, курсам)		
Число КП (по семестрам, курсам)		
Число зачетов с оценкой с разбивкой по семестрам (курсам)		1/5 сем
Число экзаменов с разбивкой по семестрам (курсам)		

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

Рецензенты:
ведущий научный сотрудник «Ростовский-на-Дону НИИ радиосвязи»,
д.т.н., доцент Погорелов В.А.

Рабочая программа дисциплины
«Искусственный интеллект и машинное обучение в кибербезопасности»

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

Составлена на основании учебного плана
направления 10.03.01 «Информационная безопасность», профиля «Безопасность компьютерных систем (по отрасли или в сфере профессиональной деятельности)», одобренного Учёным советом СКФ МТУСИ, протокол № 9 от 22.04.2024, и утвержденного директором СКФ МТУСИ 22.04.2024 г.

Рассмотрена и одобрена на заседании кафедры
«Информационная безопасность»

Протокол от «24» апреля 2024 г. № 9

Зав. кафедрой _____ Д.В. Маршаков

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

Утверждаю
Зам. директора по УВР _____
-__ _____ 20__ г.
Рабочая программа пересмотрена, обсуждена и одобрена на заседании кафедры
"Информационная безопасность"

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

"Информационная безопасность"

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
"Информационная безопасность"

Протокол от _ _____ 20__ г. № _
Зав. кафедрой _____

---

1. Цели изучения дисциплины

Целями изучения дисциплины ***"Искусственный интеллект и машинное обучение в кибербезопасности "*** 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 ***проектно-технологической деятельностью.***

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.

3. Место дисциплины в структуре образовательной программы

Требования к предварительной подготовке обучающегося (предшествующие дисциплины, модули, темы):	
1	Б1.О.27 Основы информационной безопасности
Последующие дисциплины и практики, для которых освоение данной дисциплины необходимо:	
1	Б1.О.33 Комплексное обеспечение защиты информации объекта информатизации

Рабочая программа дисциплины для инвалидов и лиц с ограниченными возможностями здоровья разрабатывается индивидуально с учетом особенностей психофизического развития, индивидуальных возможностей и состояния здоровья таких обучающихся.

4. Структура и содержание дисциплины

4.1 Очная форма обучения, 4 года (всего 144 часов, 68 аудиторных часов, 76 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					
1.1	Лекция 1. Основные задачи, ветки и методы машинного обучения. Статистические подходы к машинному обучению	Л1.	2	ОПК-2	Л1.1 Л1.2 Л1.3
1.2	Лекция 2. Нейронные сети	Л2.	4	ОПК-2	Л1.1 Л1.2 Л1.3
1.3	Лекция 3. Модели простейшей и множественной регрессии. Полиномиальная регрессия	Л3.	4	ОПК-2	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.	4	ОПК-2	Л1.1 Л1.2 Л1.3
1.5	Практическое занятие 1 Использование однослойного перцептрона в практических задачах	ПЗ1	2	ОПК-2	Л1.1 Л1.2 Л1.3
1.6	Практическое занятие 2 Использование радиальных базисных функций	ПЗ2	4	ОПК-2	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 Л1.3
1.8	Лабораторная работа 2 Применение нейронных сетей для прогнозирования временных рядов	ЛР2	6	ОПК-2	Л1.1 Л1.2 Л1.3
1.9	Практическое занятие 3. Решение задачи классификация на основе алгоритма наивного байеса	ПЗ3	2	ОПК-2	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	38	ОПК-2	Л1.1 Л1.2 Л1.3
Модуль 2. Прикладные задачи искусственного интеллектах					
2.1	Лекция №5 Основы персональной информационной безопасности, вредоносное ПО, парольные системы.	Л5	4	ОПК-2	Л1.1 Л1.2 Л1.3

2.2	Лекция №6 Симметричные системы шифрования, несимметричная криптография. Алгоритм шифрования RSA и Эль-Гамаля, электронная подпись	Л6	4	ОПК-2	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	4	ОПК-2	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	4	ОПК-2	Л1.1 Л1.2 Л1.3
2.5	Лекция №9. Основы биометрии, виды аутентификации и задача отбора признаков. Состязательные атаки на биометрические системы	Л9	4	ОПК-2	Л1.1 Л1.2 Л1.3
2.6	Практическое занятие №4. Обзор ПО информационной безопасности с использованием методов искусственного интеллекта	ПЗ4	6	ОПК-2	Л1.1 Л1.2 Л1.3
2.7	Практическое занятие №5 Криптоалгоритмы RSA и Эль Гамаля	ПЗ5	4	ОПК-2	Л1.1 Л1.2 Л1.3
2.8	Лабораторная работа № 3 Криптоалгоритм RSA	ЛР3	4	ОПК-2	Л1.1 Л1.2 Л1.3
2.9	Лабораторная работа № 4 Алгоритмы ЭЦП	ЛР4	2	ОПК-2	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	38	ОПК-2	Л1.1 Л1.2 Л1.3
	Итого		144		

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	Фаронов А.Е.	Основы информационной безопасности при работе на компьютере	М.: Интернет-Университет Информационных Технологий (ИНТУИТ), 2020.— 154 с	Э1
Л1.2	Галатенко, В. А.	Основы информационной безопасности :	Москва : Интернет-Университет Информационных Технологий	Э2

			(ИНТУИТ), Ай Пи Ар Медиа, 2020. — 266 с.	
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	М. М. Вулф, Н. Т. Разумовский, Р. Г. Прокди. .	Как защитить компьютер от вирусов	Спб: Наука и Техника, 2010. — 192 с.	Э4

5.1.3. Учебно-методическое обеспечение для самостоятельной работы обучающихся

Код	Авторы, составители	Заглавие	Издательство, год	Кол.
Л3.1	Гошко, С. В.	Технологии борьбы с компьютерными вирусами : практическое пособие	Москва : СОЛОН-ПРЕСС, 2016. — 351 с.	Э5

5.2. Электронные образовательные ресурсы

Э1	https://www.iprbookshop.ru/89453.html
Э2	https://www.iprbookshop.ru/97562.html
Э3	https://www.iprbookshop.ru/87995.html
Э4	https://www.iprbookshop.ru/35399.html
Э5	https://www.iprbookshop.ru/90288.html

5.3. Программное обеспечение

П.1	Linux (свободное ПО)
П.2	LibreOffice (свободное ПО)
П.3	Kaspersky Endpoint Security (лицензия)

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	Компьютерные аудитории с возможностью выхода в локальную сеть Филиала и Интернет
6.3 МТО рубежных контролей, экзамена	
1	Компьютерные аудитории с возможностью выхода в локальную сеть Филиала и Интернет

7. Методические рекомендации для обучающихся по самостоятельной работе

Указания по подготовке к различным видам занятий

Подготовка к лекционным занятиям осуществляется систематически и сводится к повторению изученного материала и отработке тем, вынесенных на самостоятельную работу. При этом должен быть доработан конспект лекций, а также получены ответы на контрольные вопросы, которые, как правило, приводятся в конце каждого раздела учебных пособий. Особое внимание необходимо уделить пониманию изучаемого материала. Зафиксировать вопросы, которые следует задать преподавателю.

Подготовка к лабораторным и практическим занятиям должна проводиться в объеме тех указаний, которые приводятся в каждом методическом пособии для проведения соответствующего занятия. Тема очередного занятия объявляется преподавателем накануне.

После повторения лекционного материала необходимо ознакомиться с предлагаемыми практическими заданиями, уяснить их суть, продумать порядок их выполнения, уточнить достаточность своих знаний для выполнения задания. Целесообразно выполнить возможные заготовки из состава отчета, который предстоит оформить на занятии. Это позволит выполнить и защитить работу в период плановых часов. Перед проведением каждого занятия должно быть полное представление о сути и порядке выполнения предстоящей работы.

Существенное значение имеет самостоятельная работа студента.

Темы для самостоятельного изучения для различных форм обучения, информационные источники и рекомендуемое время указаны в Разделе 4 настоящей Рабочей программы.

Самостоятельная работа студентов по дисциплине проводится в течение всего семестра и складывается из нескольких составляющих.

Подготовка к плановым аудиторным занятиям. В начале семестра студентов знакомят с календарным планом проведения всех видов учебных занятий. Чтобы студенты могли проверить качество своей подготовки к занятиям, в учебных пособиях и методических указаниях к лабораторным работам имеются вопросы для проверки уровня знаний перед выполнением работы и контрольные вопросы, позволяющие студенту оценить качество полученных результатов после выполнения работы. Предлагаемые студентам учебные пособия кроме контрольных вопросов содержат примеры с решениями и упражнения по основным темам.

Изучение технической литературы. Студенты самостоятельно изучают рекомендованную преподавателем техническую литературу.

Дополнительные самостоятельные исследования в лаборатории. Студенты, желающие получить более глубокие знания, имеют возможность выполнить дополнительные самостоятельные исследования в лаборатории. С этой целью в плановых лабораторных работах предусмотрены возможности для дополнительных исследований. Перечень разделов программы, предлагаемых для самостоятельных исследований, доводится до сведения студентов в начале семестра.

Самостоятельная работа на ПЭВМ. Для повышения эффективности самостоятельной работы студентам во второй половине дня предоставляется возможность выполнить в лаборатории самостоятельные исследования с использованием программно-аппаратного комплекса, состоящего из виртуальных электронных приборов, отображаемых на экране ПЭВМ, и моделирующих программ. Исследуемые схемы могут собираться из реальных компонентов на лабораторном стенде или виртуальных компонентов, хранящихся в библиотеке ПЭВМ.

Источники, рекомендуемые для углубленного изучения учебного материала

1. Николенко С., Кадурин А., Архангельская Е. Глубокое обучение. – СПб: Питер, 2018. – 480 с.
2. Паттерсон Дж., Гибсон А. Глубокое обучение с точки зрения практика. – ДМК Пресс, 2018. – 418 с.
3. Аггарвал Ч. Нейронные сети и глубокое обучение. – СПб: ООО «Диалектика», 2020. – 752 с.
4. Уорр К. Надежность нейронных сетей: укрепляем устойчивость ИИ к обману. – СПб: Питер, 2021. – 272 с.
5. Шолле Ф. Глубокое обучение на Python. – СПб: Питер, 2018. – 400 с.
6. Рашка С., Мирджалили В. Python и машинное обучение: машинное и глубокое обучение с использование Pethon, scikit-learn и TensorFlow. – СПб: ООО «Диалектика», 2020. – 848 с.
7. Барский, А. Б. Введение в нейронные сети : учебное пособие. — 3-е изд. — Москва, Саратов : Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2020. — 357 с.
8. Ракитский, А. А. Методы машинного обучения : учебно-методическое пособие. — Ново-

сибирск : Сибирский государственный университет телекоммуникаций и информатики, 2018. — 32 с.
9. Теория и практика машинного обучения : учебное пособие / В. В. Воронина, А. В. Михеев, Н. Г. Ярушкина, К. В. Святов. — Ульяновск : Ульяновский государственный технический университет, 2017. — 291 с.
10. Уоссермен Ф. Нейрокомпьютерная техника : Теория и практика. – Москва: Мир, 1992. – 236 с.

Использование Интернет-ресурсов

1. Электронный ресурс http://www.mathnet.ru
2. Электронный ресурс http://www.intuit.ru
3. Электронный ресурс https://habr.com/ru/hubs/machine_learning/articles/
4. Электронный ресурс https://stepik.org/course/401/

Рекомендации по подготовке к рубежным аттестациям

Подготовка к сдаче модуля сводится защите на дату проведения последнего занятия в рамках модуля всех практических и лабораторных занятий, а также к подготовке к ответам по тестовым заданиям.

Объем вопросов по каждому лабораторному и практическому занятию отражен в методических указаниях по проведению соответствующего занятия. Кроме того студент должен быть готов к пояснениям по сути практических приемов работы и доказыванию обоснованности принятых решений. Если работа не выполнена или не защищена своевременно, то это следует сделать в часы самоподготовки и консультаций до даты последнего занятия в рамках сдаваемого модуля.

Подготовка к выполнению теста обеспечивается изучением и повторением того материала, который изучался на лекционных занятиях и входе лабораторных и практических занятий. Материал повторяется по конспектам и учебным пособиям, указанным в списке литературы и методических указаниях.

Подготовка к зачету осуществляется на протяжении всего времени изучения дисциплины.

Для более конкретной, целенаправленной и качественной подготовки к зачету необходимо перед началом изучения дисциплины познакомиться с содержанием рабочей программы. Уяснить логику и последовательность изучения материала, уточнить конкретные конечные результаты, которые должны быть достигнуты в итоге изучения конкретных тем и занятий. Познакомиться с перечнем вопросов и заданий, выносимых на экзамен.

В ходе каждого занятия необходимо изучить все учебные вопросы и выполнить практические задания. Для оперативного оценивания уровня достижения учебных целей следует ответить на контрольные вопросы, которые имеются в руководстве для каждого практического и лабораторного занятия. В случае выявленных затруднений следует провести дополнительное изучение материала в часы самостоятельной работы или в период консультаций с преподавателем. Все учебные материалы должны быть отражены в конспекте, он должен дополняться и уточняться по мере отработки и уточнения учебных вопросов. Само ведение конспекта концентрирует внимание, упорядочивает знания, стимулирует активность в усвоении. К моменту выхода на непосредственную подготовку к зачету в конспекте не должно остаться непонятных вопросов.

В силу ограниченного времени, отводимого на непосредственную подготовку к зачету, целесообразно материал повторять в основном по отработанному конспекту. Это экономит время и дает возможность работать по уже знакомым записям, что улучшает запоминание материала. Остается спланировать работу в соответствии с имеющимся временем и жестко придерживаться намеченного плана. В период обязательных плановых предэкзаменационных консультаций необходимо уточнить организационные вопросы проведения экзамена и при необходимости - сложные вопросы по существу материала.

Дополнения и изменения в Рабочей программе