ЮЖНО-УРАЛЬСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

УТВЕРЖДАЮ:
Руководитель направления

Электронный документ, подписанный ПЭП, хранится в системе электронного документооборота Южно-Уральского государственного университета
ЮУрГУ
СВЕДЕНИЯ О ВЛАДЕЛЬЦЕ ПЭП
Кому выдан: Соколинский Л. Б.
Пользователь: leonid.sokolinsky
Дата подписания: 20.07.2026

Л. Б. Соколинский

РАБОЧАЯ ПРОГРАММА

дисциплины 1.О.03 Защита информации методами искусственного интеллекта
для направления 09.04.04 Программная инженерия
уровень Магистратура
форма обучения очная
кафедра-разработчик Системное программирование

Рабочая программа составлена в соответствии с ФГОС ВО по направлению подготовки 09.04.04 Программная инженерия, утверждённым приказом Минобрнауки от 19.09.2017 № 932

Зав.кафедрой разработчика,
д.физ.-мат.н., проф.

Электронный документ, подписанный ПЭП, хранится в системе электронного документооборота Южно-Уральского государственного университета
ЮУрГУ
СВЕДЕНИЯ О ВЛАДЕЛЬЦЕ ПЭП
Кому выдан: Соколинский Л. Б.
Пользователь: leonid.sokolinsky
Дата подписания: 20.07.2026

Л. Б. Соколинский

Разработчик программы,
старший преподаватель

Электронный документ, подписанный ПЭП, хранится в системе электронного документооборота Южно-Уральского государственного университета
ЮУрГУ
СВЕДЕНИЯ О ВЛАДЕЛЬЦЕ ПЭП
Кому выдан: Никольская К. Ю.
Пользователь: nikolskaiaki
Дата подписания: 20.07.2026

К. Ю. Никольская

Челябинск

1. Цели и задачи дисциплины

Целью преподавания дисциплины является изучение основных концепций и практических аспектов в сфере защиты информации с использованием методов искусственного интеллекта. Задачами изучения дисциплины являются: 1. Ознакомить с основными задачами защиты информации, кейсами применения методов ИИ в защите информации. 2. Познакомить студентов с определением, классификацией и характеристиками сетевых атак и способов защиты, способами анализа сетевого трафика методами ИИ; 3. Рассмотреть основные технологические принципы устройства антивирусов, анализа вредоносной активности методами ИИ; 4. Разобрать на практике методы и способы противодействия мошенничеству, реализации антиспам-фильтров и антифрод-систем.

Краткое содержание дисциплины

В рамках дисциплины изучаются основные направления применения методов искусственного интеллекта в задачах защиты информации: противодействие сетевым атакам путем интеллектуального анализа данных о сетевом трафике, обнаружение вредоносной активности на вычислительных узлах, особенности реализации антивирусных программ с использованием ИИ, противодействие мошенничеству в прикладных сервисах и фильтрация спам-рассылок в почтовых сервисах.

2. Компетенции обучающегося, формируемые в результате освоения дисциплины

Планируемые результаты освоения ОП ВО (компетенции)	Планируемые результаты обучения по дисциплине
ОПК-1 Способен самостоятельно приобретать, развивать и применять математические, естественнонаучные, социально-экономические и профессиональные знания для решения нестандартных задач, в том числе в новой или незнакомой среде и в междисциплинарном контексте	Знает: основные типы сетевых атак и способы защиты, типы вредоносной активности, способы противодействия мошенничеству Умеет: применять наиболее подходящие алгоритмы машинного обучения и инструменты для задач защиты информации Имеет практический опыт: сбора данных в различных форматах; предварительной обработки данных; анализа и визуализации данных в задачах защиты информации
ОПК-2 Способен разрабатывать оригинальные алгоритмы и программные средства, в том числе с использованием современных интеллектуальных технологий, для решения профессиональных задач	Знает: виды сетевых атак и способы защиты от них Умеет: анализировать сетевой трафик методами искусственного интеллекта Имеет практический опыт: выявления вредоносной активности методами искусственного интеллекта
ОПК-4 Способен применять на практике новые научные принципы и методы исследований	Знает: методы искусственного интеллекта для решения задач защиты информации Умеет: применять алгоритмы машинного обучения и инструменты для задач защиты информации Имеет практический опыт: решения задачи защиты информации методами искусственного

	интеллекта
ПК-5 Способен разрабатывать и модернизировать программное и аппаратное обеспечение технологий и систем искусственного интеллекта с учетом требований информационной безопасности в различных предметных областях	Знает: новые научные принципы и методы разработки программного и аппаратного обеспечения технологий и систем искусственного интеллекта для решения профессиональных задач в различных предметных областях; особенности модернизации программного и аппаратного обеспечения технологий и систем искусственного интеллекта для решения профессиональных задач в различных предметных областях Умеет: разрабатывать программное и аппаратное обеспечение технологий и систем искусственного интеллекта с учетом требований информационной безопасности для решения профессиональных задач в различных предметных областях; модернизировать программное и аппаратное обеспечение технологий и систем искусственного интеллекта с учетом требований информационной безопасности для решения профессиональных задач в различных предметных областях

3. Место дисциплины в структуре ОП ВО

Перечень предшествующих дисциплин, видов работ учебного плана	Перечень последующих дисциплин, видов работ
Нет	Не предусмотрены

Требования к «входным» знаниям, умениям, навыкам студента, необходимым при освоении данной дисциплины и приобретенным в результате освоения предшествующих дисциплин:

Нет

4. Объём и виды учебной работы

Общая трудоемкость дисциплины составляет 3 з.е., 108 ч., 38,25 ч. контактной работы

Вид учебной работы	Всего часов	Распределение по семестрам в часах
		Номер семестра
		1
Общая трудоёмкость дисциплины	108	108
Аудиторные занятия:	32	32
Лекции (Л)	16	16
Практические занятия, семинары и (или) другие виды аудиторных занятий (ПЗ)	16	16
Лабораторные работы (ЛР)	0	0

Самостоятельная работа (СРС)	69,75	69,75
Изучение основной и дополнительной литературы по защите информации	33,75	33.75
Подготовка к зачету	36	36
Консультации и промежуточная аттестация	6,25	6,25
Вид контроля (зачет, диф.зачет, экзамен)	-	зачет

5. Содержание дисциплины

№ раздела	Наименование разделов дисциплины	Объем аудиторных занятий по видам в часах			
		Всего	Л	ПЗ	ЛР
1	Введение в защиту информации	6	2	4	0
2	Управление данными и технологии ИИ в задачах защиты информации	2	2	0	0
3	Современный SOC	2	2	0	0
4	Управление угрозами, уязвимостями и рисками кибербезопасности	6	2	4	0
5	Защита информации в компьютерных сетях	6	2	4	0
6	Применение алгоритмов искусственного интеллекта в современных системах защиты информации	6	2	4	0
7	Безопасность систем искусственного интеллекта в системах защиты информации	2	2	0	0
8	Решение реальных кейсов по реализации алгоритмов искусственного интеллекта в системах защиты информации	2	2	0	0

5.1. Лекции

№ лекции	№ раздела	Наименование или краткое содержание лекционного занятия	Кол-во часов
1	1	Введение в защиту информации	2
2	2	Управление данными и технологии ИИ в задачах защиты информации	2
3	3	Современный SOC	2
4	4	Управление угрозами, уязвимостями и рисками кибербезопасности	2
5	5	Защита информации в компьютерных сетях	2
6	6	Применение алгоритмов искусственного интеллекта в современных системах защиты информации	2
7	7	Безопасность систем искусственного интеллекта в системах защиты информации	2
8	8	Решение реальных кейсов по реализации алгоритмов искусственного интеллекта в системах защиты информации	2

5.2. Практические занятия, семинары

№ занятия	№ раздела	Наименование или краткое содержание практического занятия, семинара	Кол-во часов
1-2	1	Семинар "Ведение в защиту информации"	4
3-4	4	Анализ сетевого трафика методами ИИ	4
5-6	5	Анализ вредоносных программ методами искусственного интеллекта	4
7-8	6	Анализ почтовых сервисов методами ИИ	4

5.3. Лабораторные работы

Не предусмотрены

5.4. Самостоятельная работа студента

Выполнение СРС			
Подвид СРС	Список литературы (с указанием разделов, глав, страниц) / ссылка на ресурс	Семестр	Кол-во часов
Изучение основной и дополнительной литературы по защите информации	Основная литература 1 (стр. 15-26) и 2 (стр. 12-20). Дополнительная литература 1 (стр. 5-20).	1	33,75
Подготовка к зачету	Основная литература 1 (стр. 50-60), 2 (стр. 25-50), 3 (стр. 5-50), 4 (стр. 6-12). Дополнительная литература 1 (стр. 23-31).	1	36

6. Фонд оценочных средств для проведения текущего контроля успеваемости, промежуточной аттестации

Контроль качества освоения образовательной программы осуществляется в соответствии с Положением о балльно-рейтинговой системе оценивания результатов учебной деятельности обучающихся.

6.1. Контрольные мероприятия (КМ)

№ КМ	Се-местр	Вид контроля	Название контрольного мероприятия	Вес	Макс. балл	Порядок начисления баллов	Учи-тыва-ется в ПА
1	1	Проме-жуточная аттестация	Итоговое тестирование	-	40	Зачет проводится в виде компьютерного тестирования. Тест содержит 40 равнозначных вопросов. За каждый правильный ответ в тесте начисляется 1 балл. За каждый неправильный ответ - 0 баллов.	зачет
2	1	Текущий контроль	Тестирование по усвоению материала лекционного занятия № 1 «Введение в защиту информации»	2	2	Проводится в виде компьютерного тестирования. Тест содержит 5 равнозначных вопросов. За каждый правильный ответ в тесте начисляется 0,4 балла. За каждый неправильный ответ - 0 баллов.	зачет
3	1	Текущий контроль	Тестирование по усвоению материала лекционного занятия № 2 «Управление данными и технологии ИИ в задачах защиты информации»	2	2	Проводится в виде компьютерного тестирования. Тест содержит 5 равнозначных вопросов. За каждый правильный ответ в тесте начисляется 0,4 балла. За каждый неправильный ответ - 0 баллов.	зачет
4	1	Текущий	Тестирование по	2	2	Проводится в виде компьютерного	зачет

		контроль	усвоению материала лекционного занятия № 3 «Современный SOC»			тестирования. Тест содержит 5 равнозначных вопросов. За каждый правильный ответ в тесте начисляется 0,4 балла. За каждый неправильный ответ - 0 баллов.	
5	1	Текущий контроль	Тестирование по усвоению материала лекционного занятия № 4 «Управление угрозами, уязвимостями и рисками кибербезопасности»	2	2	Проводится в виде компьютерного тестирования. Тест содержит 5 равнозначных вопросов. За каждый правильный ответ в тесте начисляется 0,4 балла. За каждый неправильный ответ - 0 баллов.	зачет
6	1	Текущий контроль	Тестирование по усвоению материала лекционного занятия № 5 «Защита информации в компьютерных сетях»	2	2	Проводится в виде компьютерного тестирования. Тест содержит 5 равнозначных вопросов. За каждый правильный ответ в тесте начисляется 0,4 балла. За каждый неправильный ответ - 0 баллов.	зачет
7	1	Текущий контроль	Тестирование по усвоению материала лекционного занятия № 6 «Применение алгоритмов искусственного интеллекта в современных системах защиты информации»	2	2	Проводится в виде компьютерного тестирования. Тест содержит 5 равнозначных вопросов. За каждый правильный ответ в тесте начисляется 0,4 балла. За каждый неправильный ответ - 0 баллов.	зачет
8	1	Текущий контроль	Тестирование по усвоению материала лекционного занятия № 7 «Безопасность систем искусственного интеллекта в системах защиты информации»	2	2	Проводится в виде компьютерного тестирования. Тест содержит 5 равнозначных вопросов. За каждый правильный ответ в тесте начисляется 0,4 балла. За каждый неправильный ответ - 0 баллов.	зачет
9	1	Текущий контроль	Тестирование по усвоению материала лекционного занятия № 8 «Решение реальных кейсов по реализации алгоритмов искусственного интеллекта в системах защиты информации»	2	2	Проводится в виде компьютерного тестирования. Тест содержит 5 равнозначных вопросов. За каждый правильный ответ в тесте начисляется 0,4 балла. За каждый неправильный ответ - 0 баллов.	зачет
10	1	Текущий контроль	Практическое задание № 1 «Семинар «Ведение в защиту информации»	10	10	Общий балл при оценке складывается из следующих показателей: За доклад - 3 балла: 1. Доклад рассказан, а не прочитан с листа или слайдов. (1 балл) 2. Презентация к докладу оформлена	зачет

						по требованиям. (1 балл) 3. Докладчик ответил на все вопросы студентов и преподавателя. (1 балл) За реферат - 7 баллов: 1. Число страниц реферата: не менее 15 без титульного листа, оглавления и списка литературы. (1 балла) Число страниц реферата: от 10 до 15 без титульного листа, оглавления и списка литературы. (1 балл) 2. Число источников (по теме, естественно): более 15. (1 балл) Число источников (по теме, естественно): от 10 до 15. (1 балл) 3. Оригинальность текста (проверка на антиплагиат) без титульного листа, оглавления и списка литературы: не менее 80%. (2 балла) 4. Оформление по требованиям: реферат выполнен согласно требованиям, приложенным к заданию. (1 балл) 5. При проверке на антиплагиат без титульного листа, оглавления и списка литературы не должно быть отметки, что есть сгенерированный текст. Если данная отметка будет присутствовать, то задание оценивается на 0 баллов, без возможности исправления. Общий максимальный балл за задание: 10.	
11	1	Текущий контроль	Практическая работа № 2 «Анализ сетевого трафика методами ИИ»	10	10	Студентом предоставляется оформленный отчет. Оценивается качество оформления, правильность выводов и ответы на вопросы (задаются 5 вопросов). При оценивании результатов мероприятия используется балльно-рейтинговая система оценивания результатов учебной деятельности обучающихся (утверждена приказом ректора от 24.05.2019 г. № 179) Если хотя бы одно из нижеперечисленных условий не будет выполнено, то за задание ставится 0 баллов, без возможности исправления: - файл крепится в формате .ipynb. - точность у алгоритма должна быть не менее 70% по метрике точности F1-score для каждого класса на валидационной выборке. Валидационная выборка – выборка, которую не видел алгоритм машинного обучения ни на тестовой,	зачет

						ни на обучающей выборке. - описание набора данных: о чем набор данных, какие признаки, что должно получится в итоге – какое предсказание. Общий балл при оценке складывается из следующих показателей: - Реализован алгоритм машинного обучения. Алгоритм можно реализовать с использованием библиотек или реализовать его самому. (6 баллов) - Набор данных разделен на три выборки вручную, а не с помощью автоматических функций. (1 балл) - Дана ссылка на использованный набор данных непосредственно в коде или прикреплен преобразованный набор данных, который был получен из исходного. (1 балл). - Код покрыт комментариями. Комментарии – что делает та или иная функция, что за переменные. (1 балл) - Код покрыт документацией. Документация – это объяснение результатов, после отработки алгоритма; какие параметры вы настраивали и почему. (1 балл) Общий максимальный балл за задание: 10.	
12	1	Текущий контроль	Практическая работа № 3 «Анализ вредоносных программ методами искусственного интеллекта»	10	10	Студентом предоставляется оформленный отчет. Оценивается качество оформления, правильность выводов и ответы на вопросы (задаются 5 вопросов). При оценивании результатов мероприятия используется балльно-рейтинговая система оценивания результатов учебной деятельности обучающихся (утверждена приказом ректора от 24.05.2019 г. № 179) Если хотя бы одно из нижеперечисленных условий не будет выполнено, то за задание ставится 0 баллов, без возможности исправления: - файл крепится в формате .ipynb. - точность у алгоритма должна быть не менее 70% по метрике точности F1-score для каждого класса на валидационной выборке. Валидационная выборка – выборка, которую не видел алгоритм машинного обучения ни на тестовой, ни на обучающей выборке.	зачет

						- описание набора данных: о чем набор данных, какие признаки, что должно получится в итоге – какое предсказание. Общий балл при оценке складывается из следующих показателей: - Реализован алгоритм машинного обучения. Алгоритм можно реализовать с использованием библиотек или реализовать его самому. (6 баллов) - Набор данных разделен на три выборки вручную, а не с помощью автоматических функций. (1 балл) - Дана ссылка на использованный набор данных непосредственно в коде или прикреплен преобразованный набор данных, который был получен из исходного. (1 балл). - Код покрыт комментариями. Комментарии – что делает та или иная функция, что за переменные. (1 балл) - Код покрыт документацией. Документация – это объяснение результатов, после отработки алгоритма; какие параметры вы настраивали и почему. (1 балл) Общий максимальный балл за задание: 10.	
13	1	Текущий контроль	Практическая работа № 4 «Анализ почтовых сервисов методами ИИ»	10	10	Студентом предоставляется оформленный отчет. Оценивается качество оформления, правильность выводов и ответы на вопросы (задаются 5 вопросов). При оценивании результатов мероприятия используется балльно-рейтинговая система оценивания результатов учебной деятельности обучающихся (утверждена приказом ректора от 24.05.2019 г. № 179) Если хотя бы одно из нижеперечисленных условий не будет выполнено, то за задание ставится 0 баллов, без возможности исправления: - файл крепится в формате .ipynb. - точность у алгоритма должна быть не менее 70% по метрике точности F1-score для каждого класса на валидационной выборке. Валидационная выборка – выборка, которую не видел алгоритм машинного обучения ни на тестовой, ни на обучающей выборке. - описание набора данных: о чем	зачет

						набор данных, какие признаки, что должно получится в итоге – какое предсказание. Общий балл при оценке складывается из следующих показателей: - Реализован алгоритм машинного обучения. Алгоритм можно реализовать с использованием библиотек или реализовать его самому. (6 баллов) - Набор данных разделен на три выборки вручную, а не с помощью автоматических функций. (1 балл) - Дана ссылка на использованный набор данных непосредственно в коде или прикреплен преобразованный набор данных, который был получен из исходного. (1 балл). - Код покрыт комментариями. Комментарии – что делает та или иная функция, что за переменные. (1 балл) - Код покрыт документацией. Документация – это объяснение результатов, после отработки алгоритма; какие параметры вы настраивали и почему. (1 балл) Общий максимальный балл за задание: 10.	

6.2. Процедура проведения, критерии оценивания

Вид промежуточной аттестации	Процедура проведения	Критерии оценивания
зачет	При оценивании результатов учебной деятельности обучающегося по дисциплине используется балльно-рейтинговая система оценивания результатов учебной деятельности обучающихся (Положение о БРС утверждено приказом ректора от 24.05.2019 г. № 179, в редакции приказа ректора от 10.03.2022 г. No 25-13/09). Процедура прохождения промежуточной аттестации осуществляется согласно Положению о текущем контроле успеваемости и промежуточной аттестации (приказ ректора от 27.02.2024 № 33-13/09). Оценка за дисциплину формируется на основе полученных оценок за контрольно-рейтинговые мероприятия текущего контроля следующим образом: • Зачтено: Величина рейтинга обучающегося по дисциплине 60…100 %. • Незачтено: Величина рейтинга обучающегося по дисциплине 0…59 %. Если студент согласен с оценкой, полученной по результатам текущего контроля, то он может в день, предшествующий промежуточной аттестации дать свое согласие на автомат в личном кабинете. В случае явки студента на промежуточную аттестацию, давшего свое согласие на автомат в личном кабинете, студент имеет право пройти мероприятия текущего контроля по дисциплине на	В соответствии с пп. 2.5, 2.6 Положения

	промежуточной аттестации для улучшения своего рейтинга в день ее проведения. Снижение оценки в этом случае запрещено. Если студент не дал согласия в личном кабинете, то он может согласиться с оценкой лично на промежуточной аттестации в день ее проведения. Если студент не согласен с оценкой, то он имеет право пройти контрольно-рейтинговые мероприятия на промежуточной аттестации для улучшения своего рейтинга в день ее проведения. Фиксация результатов учебной деятельности по дисциплине проводится в день промежуточной аттестации на основе согласия студента, данного им в личном кабинете. При отсутствии согласия в журнале дисциплины фиксация результатов происходит при личном присутствии студента. Если студент не дал согласие в личном кабинете и не явился на промежуточную аттестацию – ему выставляется «неявка». Промежуточная аттестация проводится в форме тестирования. Тестирование проводится в системе edu.susu.ru. Тест содержит 40 вопросов, на выполнение теста дается 60 минут. В этом случае оценка за дисциплину рассчитывается на основе полученных оценок за контрольно-рейтинговые мероприятия текущего контроля и промежуточной аттестации.	

6.3. Паспорт фонда оценочных средств

Компетенции	Результаты обучения	№ КМ											
		1	2	3	4	5	6	7	8	9	10	11	12	13
ОПК-1	Знает: основные типы сетевых атак и способы защиты, типы вредоносной активности, способы противодействия мошенничеству	+			+		+							
ОПК-1	Умеет: применять наиболее подходящие алгоритмы машинного обучения и инструменты для задач защиты информации	+									+			
ОПК-1	Имеет практический опыт: сбора данных в различных форматах; предварительной обработки данных; анализа и визуализации данных в задачах защиты информации	+											+	+
ОПК-2	Знает: виды сетевых атак и способы защиты от них	+					+			+				
ОПК-2	Умеет: анализировать сетевой трафик методами искусственного интеллекта	+										+		
ОПК-2	Имеет практический опыт: выявления вредоносной активности методами искусственного интеллекта	+										+		
ОПК-4	Знает: методы искусственного интеллекта для решения задач защиты информации	+	+			+		+						
ОПК-4	Умеет: применять алгоритмы машинного обучения и инструменты для задач защиты информации	+										+		+
ОПК-4	Имеет практический опыт: решения задачи защиты информации методами искусственного интеллекта	+									+			
ПК-5	Знает: новые научные принципы и методы разработки программного и аппаратного обеспечения технологий и систем искусственного интеллекта для решения профессиональных задач в различных предметных областях; особенности модернизации программного и аппаратного обеспечения технологий и систем искусственного интеллекта для решения профессиональных задач в различных предметных областях	+		+					+	+				

ПК-5	Умеет: разрабатывать программное и аппаратное обеспечение технологий и систем искусственного интеллекта с учетом требований информационной безопасности для решения профессиональных задач в различных предметных областях; модернизировать программное и аппаратное обеспечение технологий и систем искусственного интеллекта с учетом требований информационной безопасности для решения профессиональных задач в различных предметных областях	+									+	+		

Типовые контрольные задания по каждому мероприятию находятся в приложениях.

7. Учебно-методическое и информационное обеспечение дисциплины

Печатная учебно-методическая документация

а) основная литература:

Не предусмотрена

б) дополнительная литература:

Не предусмотрена

в) отечественные и зарубежные журналы по дисциплине, имеющиеся в библиотеке:

1. Вестник УрФО : Безопасность в информационной сфере / Юж.-Урал. гос. ун-т; ЮУрГУ. - Челябинск : Издательство ЮУрГУ, 2011-. -

г) методические указания для студентов по освоению дисциплины:

1. Методические указания

из них: учебно-методическое обеспечение самостоятельной работы студента:

1. Методические указания

Электронная учебно-методическая документация

№	Вид литературы	Наименование ресурса в электронной форме	Библиографическое описание
1	Основная литература	ЭБС издательства Лань	Баланов, А. Н. Кибербезопасность : учебное пособие для вузов / А. Н. Баланов. — 2-е изд., стер. — Санкт-Петербург : Лань, 2025. — 680 с. — ISBN 978-5-507-52709-0. — Текст : электронный // Лань : электронно-библиотечная система. — Режим доступа: для авториз. пользователей. https://e.lanbook.com/book/457463
2	Основная литература	ЭБС издательства Лань	Баланов, А. Н. Защита информационных систем. Кибербезопасность : учебное пособие для вузов / А. Н. Баланов. — 2-е изд., стер. — Санкт-Петербург : Лань, 2025. — 280 с. — ISBN 978-5-507-50467-1. — Текст : электронный // Лань : электронно-библиотечная система. — Режим доступа: для авториз. пользователей. https://e.lanbook.com/book/457463
3	Дополнительная литература	ЭБС издательства	Волков, В. Э. Публично-правовое регулирование цифровых технологий: блокчейн, искусственный интеллект,

		Лань	виртуальная реальность : учебное пособие / В. Э. Волков. — Самара : Самарский университет, 2023. — 118 с. — ISBN 978-5-7883-1889-9. — Текст : электронный // Лань : электронно-библиотечная система. — Режим доступа: для авториз. пользователей. https://e.lanbook.com/book/406502
4	Основная литература	ЭБС издательства Лань	Безопасность систем искусственного интеллекта : учебное пособие / П. С. Ложников, А. Е. Самотуга, С. С. Жумажанова, А. Е. Сулавко. — Омск : ОмГТУ, 2023 — Часть 2 : Доверенный искусственный интеллект — 2023. — 74 с. — ISBN 978-5-8149-3731-5. — Текст : электронный // Лань : электронно-библиотечная система. — Режим доступа: для авториз. пользователей. https://e.lanbook.com/book/421598
5	Основная литература	ЭБС издательства Лань	Баланов, А. Н. Искусственный интеллект. Понимание, применение и перспективы : учебник для вузов / А. Н. Баланов. — 2-е изд., стер. — Санкт-Петербург : Лань, 2025. — 312 с. — ISBN 978-5-507-52357-3. — Текст : электронный // Лань : электронно-библиотечная система. — Режим доступа: для авториз. пользователей. https://e.lanbook.com/book/448697

Перечень используемого программного обеспечения:

Нет

Перечень используемых профессиональных баз данных и информационных справочных систем:

Нет

8. Материально-техническое обеспечение дисциплины

Вид занятий	№ ауд.	Основное оборудование, стенды, макеты, компьютерная техника, предустановленное программное обеспечение, используемое для различных видов занятий
Зачет	114-1 (2)	Компьютерный класс, имеется выход в интернет
Лекции	114-1 (2)	Компьютер и проектор
Практические занятия и семинары	114-1 (2)	Компьютерный класс, имеется выход в интернет