
УТВЕРЖДЕНА

Решением Ученого совета
АНО ВО «Центральный университет»
«25» мая 2026 г.
Протокол № 2

**Рабочая программа дисциплины (модуля)
«Искусственный интеллект в действии»**

Направление подготовки: 02.04.01 Математика и компьютерные науки

Направленность (профиль) подготовки: Управление цифровыми
продуктами и системами

Квалификация (степень) выпускника: магистр

Форма обучения: очная

Срок освоения программы: 2 года

Год набора: 2026

**Москва
2026**

Содержание

1. Краткая характеристика дисциплины (модуля)	3
2. Перечень планируемых результатов обучения.....	3
3. Тематический план.....	6
4. Содержание дисциплины (модуля).....	6
5. Учебно-методическое обеспечение	7
6. Материально-техническое обеспечение	7
7. Методические и оценочные материалы	9

1. Краткая характеристика дисциплины (модуля)

Рабочая программа дисциплины (модуля) «Искусственный интеллект в действии» составлена в соответствии с федеральным государственным образовательным стандартом высшего образования – магистратура по направлению 02.04.01 Математика и компьютерные науки, профиль Управление продуктами и системами, утвержденный приказом Министерства науки и высшего образования Российской Федерации № 810 от 23.08.2017 года.

Изучение дисциплины (модуля) «Искусственный интеллект в действии» позволяет сформировать практические навыки применения продвинутых алгоритмов машинного обучения, включая оптимизацию маршрутов, рекомендательные системы и обеспечение безопасности нейросетевых моделей.

Место дисциплины (модуля) в структуре образовательной программы

Настоящая дисциплина (модуль) включена в учебный план по программе подготовки магистратуры по направлению 02.04.01 Математика и компьютерные науки, профиль Управление продуктами и системами и входит в Блок Факультативные дисциплины.

Дисциплина (модуль) доступна к изучению на 1 курсе во 2 семестре.

Цель изучения дисциплины (модуля): подготовить обучающихся к практическому применению алгоритмов поиска и оптимизации, методов исследования и использования, а также к обеспечению безопасности моделей машинного обучения от враждебных атак.

Задачи изучения дисциплины (модуля):

- освоить принципы работы и области применения алгоритма поиска A^* в задачах на графах;
- изучить модели многоруких и контекстуальных многоруких бандитов для построения рекомендательных систем;
- рассмотреть принципы и методы враждебного машинного обучения;
- отработать навыки поиска уязвимостей и защиты моделей (на примере логистической регрессии) от враждебных атак;
- развить компетенции по планированию и проведению самостоятельной работы по разработке решений машинного обучения.

В результате освоения дисциплины (модуля) обучающийся должен:

знать:

- принципы работы и применения алгоритма поиска A^* в оптимизации маршрутов и задачах на графах;
- теоретические основы модели многоруких бандитов и модели контекстуальных многоруких бандитов, их применение к рекомендательным системам;
- принципы и применение методов враждебного машинного обучения;
- принципы и методы защиты нейросетей от враждебных атак.

уметь:

- применять алгоритм A^* для разработки решений в задачах оптимизации и поиска путей;
- реализовывать и применять алгоритм UCB-1;
- находить атаки на незащищенные модели машинного обучения;
- осуществлять защиту модели логистической регрессии от атак.

владеть:

- навыками планирования и проведения самостоятельной работы по разработке решения машинного обучения.

2. Перечень планируемых результатов обучения

Компетенции, формируемые в результате освоения дисциплины (модуля) при проведении учебных занятий в форме контактной работы обучающихся с педагогическими работниками Университета и в форме самостоятельной работы обучающихся:

Компетенция	Содержание компетенции	Индикатор компетенции	Перечень планируемых результатов обучения по дисциплине (модулю)
УК-6.	Способен определять и реализовывать приоритеты собственной деятельности и способы ее совершенствования на основе самооценки	УК-6.1.	Знает основные методы самооценки и анализа своей деятельности, а также принципы управления временем и целеполагания
		УК-6.2.	Умеет ставить реалистичные и достижимые цели, определять приоритеты в своей деятельности, а также разрабатывать и внедрять планы по совершенствованию своих навыков и компетенций на основе полученной самооценки
		УК-6.3.	Имеет практический опыт применения методов самооценки в своей профессиональной деятельности, включая участие в тренингах, семинарах и проектах, направленных на развитие личной эффективности и профессионального роста
ОПК-2.	Способен создавать и исследовать новые математические модели в естественных науках, совершенствовать и разрабатывать концепции, теории и методы	ОПК-2.1.	Знает основные математические модели и методы, используемые в естественных науках, включая статистическое моделирование, дифференциальные уравнения и численные методы, а также современные подходы к исследованию и анализу данных
		ОПК-2.2.	Умеет разрабатывать и адаптировать математические модели для решения конкретных проблем в естественных науках, проводить их анализ и верификацию, а также интерпретировать полученные результаты в контексте научных исследований

		ОПК-2.3.	Имеет практический опыт создания и исследования математических моделей в рамках научных проектов или исследований, включая участие в публикациях, конференциях или коллаборациях, где были разработаны и апробированы новые концепции и методы
ПК-3.	Способен решать задачи профессиональной деятельности в области управления цифровыми продуктами и системами, формулировать результаты анализа и выявлять последствия полученных данных для принятия обоснованных решений и оптимизации продуктов	ПК-3.1.	Знает методы и инструменты управления цифровыми продуктами и системами
		ПК-3.2.	Умеет применять аналитические инструменты и программное обеспечение для обработки и визуализации данных, а также формулировать выводы на основе проведенного анализа
		ПК-3.3.	Имеет опыт работы над реальными проектами в области управления цифровыми продуктами и системами, включая анализ пользовательского поведения и оптимизацию продуктов на основе полученных данных

3. Тематический план

№ п/п	Наименование раздела дисциплины (модуля)	Трудоемкость, академические часы				ТКУ (текущий контроль успеваемости)
		Очная форма				
		Аудиторная работа		Контроль	Самостояте льная работа	
		Лекции	Семинары (практичес кие занятия)			
1	Поиск и планирование в пространстве состояний	10	10		4	Домашние задания, Аудиторная работа
2	Стохастическое принятие решений и обучение с подкреплением (Bandits)	10	10		4	Домашние задания, Аудиторная работа
3	Безопасность и уязвимости алгоритмов машинного обучения	10	10		4	Домашние задания, Аудиторная работа
	Зачет с оценкой			4		Контрольная работа
Итого:		30	30	4	12	
Объем дисциплины (модуля) (в ак. ч.)		76				
Объем дисциплины (модуля) (в зач. ед.)		2				

4. Содержание дисциплины (модуля)

№п/п	Наименование раздела дисциплины (модуля)	Содержание дисциплины (модуля) по темам
1	Поиск и планирование в пространстве состояний	А* на графе А* в непрерывном пространстве: приложение к видео-играм
2	Стохастическое принятие решений и обучение с подкреплением (Bandits)	Бандиты 1: постановка задачи Бандиты 2: эксперты Бандиты 3: контекстуальные бандиты
3	Безопасность и уязвимости алгоритмов машинного обучения	Атаки на методы машинного обучения Защита методов машинного обучения

5. Учебно-методическое обеспечение

Университет располагает полным набором лицензионного и свободно распространяемого программного обеспечения, включая продукты отечественного производства.

Каждый студент в течение всего периода обучения получает индивидуальный неограниченный доступ к электронно-библиотечной системе и электронной информационно-образовательной среде университета. Эти системы предоставляют возможность доступа к ресурсам из любой точки, где есть подключение к сети Интернет, как на территории университета, так и за его пределами.

Студентам обеспечен удаленный доступ к современным профессиональным базам данных и информационным справочным системам.

Основная литература:

1. Барретт, С. Ф. Arduino: искусственный интеллект и машинное обучение : практическое руководство / С. Ф. Барретт ; с англ. Ю. В. Ревича. – Москва : ДМК Пресс, 2024. - 244 с. – ISBN 978-5-93700-276-1. - Текст : электронный. - URL: <https://znanium.ru/catalog/product/2205065>.

2. Форд, М. Архитекторы интеллекта: вся правда об искусственном интеллекте от его создателей : практическое руководство / М. Форд. - Санкт-Петербург : Питер, 2020. - 416 с. - (Серия «Библиотека программиста»). - ISBN 978-5-4461-1254-8. - Текст : электронный. - URL: <https://znanium.com/catalog/product/1733710>.

Дополнительная литература:

1. Бессмертный, И. А. Интеллектуальные системы : учебник и практикум для вузов / И. А. Бессмертный, А. Б. Нугуманова, А. В. Платонов. — 2-е изд. — Москва : Издательство Юрайт, 2026. — 250 с. — (Высшее образование). — ISBN 978-5-534-20734-7. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/583859>.

2. Бурков, А. Инженерия машинного обучения : практическое руководство / А. Бурков ; пер. с англ. А. А. Слинкина. - Москва : ДМК Пресс, 2022. - 306 с. - ISBN 978-5-93700-125-2. - Текст : электронный. - URL: <https://znanium.com/catalog/product/2109491>.

6. Материально-техническое обеспечение

Университет располагает материально-технической базой, соответствующей действующим противопожарным правилам и нормам и обеспечивающей проведение всех видов дисциплинарной и междисциплинарной подготовки, практической и научно-исследовательской работ обучающихся, предусмотренных учебным планом.

Помещения, которые представляют собой учебные аудитории для проведения занятий лекционного типа, занятий семинарского (практического) типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации, а также помещения для самостоятельной работы и помещения для хранения и профилактического обслуживания учебного оборудования. Помещения укомплектованы специализированной мебелью и техническими средствами обучения, служащими для представления учебной информации большой аудитории.

Изучение дисциплины (модуля) обеспечивается в учебных аудиториях, оснащенных:

- столами и стульями;
- компьютерной техникой;
- механическими калькуляторами;
- специализированным оборудованием, включая демонстрационное оборудование.

Помещения для самостоятельной работы обучающихся, в том числе приспособленные для использования инвалидами и лицами с ограниченными возможностями здоровья, оснащены компьютерной техникой с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду Университета.

Обучающимся предоставляется доступ (в том числе удаленный) к ресурсам информационно-телекоммуникационной сети «Интернет», электронным ресурсам (в том числе электронным библиотечным системам, современным профессиональным базам данных и информационным справочным системам):

№	Наименование портала (издания, курса, документа)	Ссылка
1.	Научная электронная библиотека elibrary.ru библиотека	https://elibrary.ru/defaultx.asp
2.	База данных для IT-специалистов	https://habr.com
3.	База данных ScienceDirect	https://www.sciencedirect.com
4.	Официальный сайт Министерства науки и высшего образования Российской Федерации	https://minobrnauki.gov.ru/
5.	Федеральный портал «Российское образование»	https://www.edu.ru/
6.	Информационная система "Единое окно доступа к образовательным ресурсам"	http://window.edu.ru/
7.	Единая коллекция цифровых образовательных ресурсов	http://school-collection.edu.ru/
8.	Федеральный центр информационно - образовательных ресурсов	http://fcior.edu.ru/

Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине (модулю), в том числе комплект лицензионного программного обеспечения, современные профессиональные базы данных и информационные справочные системы:

Наименование ПО	Производство	Лицензионное / свободно распространяемое
Операционные системы:		
Microsoft Imagine (Windows Client, Server)	зарубежное	лицензионное
Браузеры:		
Яндекс.Браузер	отечественное	свободно распространяемое
Google Chrome	зарубежное	свободно распространяемое
Офисные приложения:		
Microsoft Imagine (Visio, OneNote)	зарубежное	лицензионное
TeXstudio	зарубежное	свободно распространяемое
Adobe Acrobat Reader	зарубежное	свободно распространяемое
Программное обеспечение для планирования и учета времени:		
Toggle app	зарубежное	свободно распространяемое
Системы управления проектами:		
Microsoft Imagine (Project)	зарубежное	лицензионное
Системы управления базами данных:		
Microsoft Imagine (SQL Server)	зарубежное	лицензионное
Системы резервного копирования (backup):		
Acronis Backup Advanced for HyperV	зарубежное	лицензионное
Справочно-правовые системы:		

КонсультантПлюс: справочно-правовая система	отечественное	лицензионное
Средства антивирусной защиты:		
Kaspersky Endpoint Security для бизнеса Стандартный Russian Edition	отечественное	лицензионное
Среды разработки:		
Visual Studio Code	зарубежное	свободно распространяемое
Bash (Unix shell)	зарубежное	свободно распространяемое
Anaconda	зарубежное	свободно распространяемое
Robotic Operating System	зарубежное	свободно распространяемое
CopelliaSim	зарубежное	свободно распространяемое
Google Colaboratory	зарубежное	свободно распространяемое
Пакеты программных средств и библиотек:		
AutoPsy	зарубежное	свободно распространяемое
Interactive Disassembler (IDA)	зарубежное	свободно распространяемое
Системы управления библиографической информацией:		
Zotero	зарубежное	свободно распространяемое
Сервисы и службы:		
Bind	зарубежное	свободно распространяемое
Docker	зарубежное	свободно распространяемое

7. Методические и оценочные материалы

Методические указания для обучающихся по освоению дисциплины (модуля)

В процессе изучения дисциплины (модуля) «Искусственный интеллект в действии» в рамках текущего контроля успеваемости используются такие виды учебной работы как лекции, семинары, домашние задания, аудиторная работа, контрольная работа, а также различные виды самостоятельной работы обучающихся по заданию преподавателя, направленные на развитие навыков профессиональной лексики, закрепление практических профессиональных компетенций, поощрение инициатив.

Лекция – систематическое, последовательное, монологическое изложение преподавателем учебного материала, как правило, теоретического характера.

В процессе лекций рекомендуется вести конспект лекций: кратко и схематично фиксировать основные идеи, выводы и обобщения лекции; выделять важные мысли, ключевые слова и термины. Необходимо отметить вопросы или материалы, которые вызывают затруднения, и попытаться найти ответы в рекомендованной литературе. Если разобраться в материале не удастся, следует сформулировать вопрос и задать его преподавателю на консультации или во время семинарского (практического) занятия.

Семинар – это форма учебной деятельности, проводимая в учебном заведении под руководством преподавателя, где студенты активно участвуют в обсуждениях, практических заданиях и других формах взаимодействия.

Для успешной подготовки к семинару рекомендуется заранее ознакомиться с темой занятия и основными материалами, чтобы иметь возможность активно участвовать в обсуждении. Также полезно подготовить вопросы и идеи для обсуждения, что поможет глубже понять материал и продемонстрировать заинтересованность.

Домашнее задание – набор задач по темам недели.

При работе над домашними заданиями важно внимательно ознакомиться с требованиями и сроками выполнения. Рекомендуется разбивать задания на этапы, чтобы избежать перегрузки и лучше усвоить материал, использовать различные источники

информации, включая учебники и онлайн-ресурсы, для более глубокого понимания темы.

Аудиторная работа – активная работа студента на семинаре, его ответы на вопросы преподавателя и участие в дискуссии.

Для успешного участия в семинаре студентам рекомендуется заранее ознакомиться с темой обсуждения, прочитать необходимые материалы и подготовить вопросы. Важно активно слушать и вовлекаться в дискуссию, высказывая свои мнения и аргументируя их. При ответах на вопросы преподавателя стоит быть уверенным, четким и логичным, опираясь на изученный материал. Также полезно поддерживать диалог с однокурсниками, чтобы обогатить обсуждение и расширить свои знания.

Контрольная работа – письменная работа с набором задач, которые нужно решить за ограниченное время.

Цель контрольной работы – получить специальные знания по одной или нескольким темам дисциплины и продемонстрировать навыки их практического применения.

Самостоятельная работа – работа студентов, направленная на углубленное изучение отдельных тем и вопросов учебной дисциплины (модуля).

В процессе самостоятельной работы студенты взаимодействуют с рекомендованными материалами при минимальном участии преподавателя. Задачи студента включают работу с конспектами лекций (обработка текста), повторное изучение учебных материалов планов и тезисов ответов, изучение дополнительных тем, выполнение учебно-исследовательских заданий и другое.

Система оценивания результатов обучения по дисциплине (модулю)

Критерии получения уровня и оценивания сформированности компетенций по дисциплине (модулю) «Искусственный интеллект в действии»

Оценивание уровня учебных достижений обучающихся по дисциплине (модулю) осуществляется в виде текущего контроля успеваемости и промежуточной аттестации.

Промежуточная аттестация по дисциплине (модулю) осуществляется в форме **зачета с оценкой**, при этом проводится оценка компетенций, сформированных по дисциплине.

Для оценивания текущего контроля успеваемости и промежуточной аттестации используется десятибалльная шкала оценивания, которая соотносится с традиционной пятибалльной шкалой следующим образом, если иное не указано в силлабусе дисциплины:

Десятибалльная оценка	Пятибалльная оценка	Оценка за зачет	Общая характеристика результата обучения по дисциплине (модулю)
10	Отлично	Зачтено	Студент полностью владеет знаниями, изложенными в рабочей программе, и глубоко осмысляет дисциплину. Он самостоятельно и логически последовательно отвечает на все вопросы, акцентируя внимание на наиболее важном. Умеет анализировать, сравнивать, классифицировать, обобщать, конкретизировать и систематизировать изученный материал, выделяя ключевые моменты и устанавливая причинно-следственные связи. Четко формулирует ответы, уверенно интерпретирует результаты анализов и других
9	Отлично	Зачтено	
8	Отлично	Зачтено	

Десятибалльная оценка	Пятибалльная оценка	Оценка за зачет	Общая характеристика результата обучения по дисциплине (модулю)
			исследований, а также решает сложные задачи. Студент хорошо знаком с методами исследования, необходимыми для практической деятельности, и умеет связывать теоретические аспекты дисциплины (модуля) с практическими задачами.
7	Хорошо	Зачтено	Студент обладает знаниями предмета почти в полном объеме рабочей программы и самостоятельно, логически последовательно и всесторонне отвечает на все вопросы, акцентируя внимание на наиболее значимых моментах. Он умеет анализировать, сравнивать, классифицировать, обобщать, конкретизировать и систематизировать изученный материал, выделяя его ключевые аспекты и устанавливая причинно-следственные связи. Формулирует свои ответы, уверенно интерпретирует результаты анализов и других исследований, а также решает сложные ситуационные задачи. Студент хорошо знаком с методами исследования, необходимыми для практической деятельности, и умеет связывать теоретические аспекты предмета с практическими задачами.
6	Хорошо	Зачтено	
5	Удовлетворительно	Зачтено	Студент обладает базовыми знаниями по дисциплине, но испытывает трудности при самостоятельных ответах и использует неточные формулировки. В ходе ответов он допускает ошибки, касающиеся сути вопросов. Студент способен решать только самые простые задачи и владеет лишь минимальным набором методов исследования.
4	Удовлетворительно	Зачтено	
3	Не сдан	Не зачтено	Студент не овладел обязательным минимумом знаний по предмету и не может ответить на вопросы, даже если преподаватель задает дополнительные наводящие вопросы.

Дисциплина (модуль) «Искусственный интеллект в действии» оценивается следующим образом:

Активность	Вес	Количество	Описание
Домашние задания	60%	5	Набор задач по темам недели
Аудиторная работа	10%	4	Активная работа студента на занятии
Зачёт с оценкой	30%	1	Контрольная работа - письменная работа с набором задач, которые нужно решить за ограниченное время

Формула расчёта итоговой оценки по дисциплине (модулю) «Искусственный интеллект в действии»: $\langle 0,6 \times \text{среднее за домашние задания} + 0,1 \times \text{среднее за аудиторную работу} + 0,3 \times \text{зачёт с оценкой} \rangle$.

Текущий контроль успеваемости обучающихся по дисциплине (модулю)

Примерные домашние задания

Домашнее задание 1. Поиск и планирование в пространстве состояний

1. Реализуйте алгоритм A^* для поиска пути на графе. Убедитесь, что он:
 - корректно обрабатывает узлы и ребра,
 - использует допустимую эвристическую функцию,
 - демонстрирует оптимальность найденного пути.
2. Примените алгоритм A^* в непрерывном пространстве (например, для навигации в видео-игре):
 - адаптируйте алгоритм для работы с координатами,
 - оцените производительность в реальном времени
3. Подготовьте отчет о сравнении различных эвристик:
 - влияние на скорость работы,
 - влияние на качество пути

Домашнее задание 2. Стохастическое принятие решений и обучение с подкреплением (Bandits)

1. Смоделируйте задачу многорукого бандита:
 - опишите постановку задачи,
 - выберите метрики эффективности (regret).
2. Реализуйте алгоритм UCB-1 (или алгоритм для экспертов):
 - продемонстрируйте работу алгоритма на синтетических данных,
 - сравните со случайной стратегией.
3. Примените контекстуальные бандиты для рекомендательной системы:
 - используйте контекстную информацию о пользователе,
 - оцените качество рекомендаций.

Домашнее задание 3. Безопасность и уязвимости алгоритмов машинного обучения

1. Найдите и реализуйте атаку на незащищенную модель машинного обучения.
2. Осуществите защиту модели логистической регрессии от атак:
 - примените методы регуляризации или adversarial training,
 - оцените устойчивость модели.
3. Составьте план разработки решения машинного обучения с учетом безопасности:
 - включите этапы тестирования на уязвимости,
 - предусмотрите меры защиты на этапе внедрения.

Примерные вопросы для подготовки к занятию

Тема 1. Поиск и планирование в пространстве состояний

1. В чем заключается основное отличие алгоритма A^* от алгоритма Дейкстры и жадного поиска по первому наилучшему соответствию?
2. Какие свойства должна иметь эвристическая функция, чтобы гарантировать оптимальность пути, найденного алгоритмом A^* ?
3. Как адаптируется алгоритм A^* для работы в непрерывном пространстве, например, для навигации персонажа в видео-игре?
4. Какие существуют способы дискретизации непрерывного пространства для применения поисковых алгоритмов на графах?
5. Какие вычислительные ограничения необходимо учитывать при внедрении A^*

в реальном времени в игровых движках?

Тема 2. Стохастическое принятие решений и обучение с подкреплением (Bandits)

1. В чем состоит дилемма «исследование против использования» (exploration vs. exploitation) в задаче о многоруких бандитах?
2. Как рассчитывается верхняя доверительная граница в алгоритме UCB-1 и какой параметр отвечает за баланс исследования?
3. В чем ключевое различие между задачей о многоруких бандитах и задачей об экспертах с точки зрения получаемой обратной связи?
4. Как использование контекстной информации меняет постановку задачи и архитектуру решения в контекстуальных бандитах?
5. Где в управлении продуктами и системами наиболее целесообразно применять модели бандитов вместо классических A/B тестов?

Тема 3. Безопасность и уязвимости алгоритмов машинного обучения

1. Что такое враждебные примеры (adversarial examples) и как они влияют на работу модели машинного обучения?
2. В чем разница между атаками типа «уклонение» (evasion) и «отравление» (poisoning) данных?
3. Как работает метод adversarial training для повышения устойчивости нейросетей?
4. Какие специфические уязвимости имеют линейные модели (например, логистическая регрессия) по сравнению с глубокими сетями?
5. Какие метрики помимо точности (accuracy) необходимо использовать для оценки защищенности модели машинного обучения?

Примерные задания для контрольной работы

Контрольные вопросы по дисциплине «Искусственный интеллект в действии»

1. Запишите основную формулу оценки вершины $f(n)$ в алгоритме A^* и кратко расшифруйте каждое слагаемое (g , h).
2. Верно ли утверждение: «Алгоритм A^* всегда находит оптимальный путь независимо от выбранной эвристической функции»? Ответ обоснуйте.
3. Предложите один способ адаптации алгоритма A^* для работы в непрерывном пространстве (например, для навигации в видео-игре без сетки).
4. В чем заключается основная дилемма «исследование против использования» (exploration vs exploitation) в задаче о многоруких бандитах?
5. Задача: Рассчитайте значение верхней доверительной границы (UCB-1) для руки, если среднее вознаграждение = 0.5, общее количество шагов $t = 100$, количество выборов этой руки $n = 10$ (параметр исследования $C = 2$).
6. Какое дополнительное входное данные используют контекстуальные бандиты по сравнению с классической постановкой задачи?
7. Дайте определение понятию «враждебный пример» (adversarial example) в контексте машинного обучения.
8. Задача: Определите тип атаки по описанию: «Злоумышленник вносит искажения в обучающую выборку до начала процесса обучения модели». (Варианты: Evasion, Poisoning).
9. Опишите суть метода быстрых градиентных знаков (FGSM) для генерации враждебных примеров.
10. Назовите один известный метод защиты моделей машинного обучения от враждебных атак и кратко опишите принцип его действия.

Задания для промежуточной аттестации по дисциплине (модулю)

№ п/п	Задание	Ответ	Компетенция
1.	Какой документ составляется для планирования этапов разработки решения машинного обучения?	План работы / Roadmap / Планирование задач / Индивидуальный план развития	УК-6
2.	Какой метод используется для самооценки компетенций в области искусственного интеллекта?	SWOT-анализ / Самоанализ / Self-assessment / Оценка навыков	УК-6
3.	Какой инструмент помогает управлять временем при проведении экспериментов с моделями?	Тайм-менеджмент / Планировщик / Timeboxing / Календарь	УК-6
4.	Какая формула используется для оценки вершины в математической модели алгоритма A*?	$f(n) = g(n) + h(n)$ / Оценка стоимости / Формула A* / Математическая модель	ОПК-2
5.	Какое свойство эвристической функции проверяется при верификации модели поиска пути?	Допустимость / Admissibility / Не завышенная оценка / Consistency / Проверка адекватности	ОПК-2
6.	Какая математическая модель описывает задачу стохастического принятия решений (бандиты)?	Вероятностная модель / Distribution / Статистическое моделирование / Математическая модель	ОПК-2
7.	Какой численный метод используется для выбора действия в алгоритме UCB-1?	Верхняя доверительная граница / UCB / Confidence Bound / Численные методы	ОПК-2
8.	Как адаптируется математическая модель бандитов для учета контекста пользователя?	Калибровка параметров / Адаптация модели / Contextual Bandits / Настройка модели	ОПК-2
9.	Какой метод используется для математического описания возмущений во враждебных атаках?	Градиентный спуск / FGSM / Perturbation / Численные методы	ОПК-2
10.	Как верифицируется разработанная модель на устойчивость к атакам?	Сравнение с данными / Валидация модели / Verification / Проверка адекватности / Robustness	ОПК-2
11.	Где применяется алгоритм A* для оптимизации цифрового продукта?	Навигация в видео-играх / Pathfinding / Игровые движки / Продуктовые фичи	ПК-3
12.	Какая метрика измеряет эффективность рекомендательной системы на бандитах?	Regret / Накопленное сожаление / Reward / Эффективность продукта	ПК-3
13.	Какой метод используется для принятия обоснованных решений вместо классических A/B тестов?	Контекстуальные бандиты / Эксперименты / Data-driven выводы / Эксперименты	ПК-3
14.	Что анализируется для оценки рисков безопасности цифрового продукта?	Уязвимости модели / Security Risk / Threat Model / Анализ данных	ПК-3

15.	Какой инструмент применяется для обработки данных при обучении моделей защиты?	Python / SQL / BI-системы / Аналитические инструменты / Data Tools	ПК-3
16.	Как интерпретируются результаты анализа уязвимостей для бизнеса?	Научные выводы / Интерпретация результатов / Business Insights / Анализ результатов	ПК-3