

МИНОБРНАУКИ РОССИИ
Федеральное государственное бюджетное
образовательное учреждение высшего образования
«Астраханский государственный университет имени В. Н. Татищева»
(Астраханский государственный университет им. В. Н. Татищева)

СОГЛАСОВАНО
Руководитель ОПОП

О. Н. Выборнова

«05» мая 2025 г.

УТВЕРЖДАЮ
И.о. Заведующего кафедрой
информационной безопасности
В. А. Черкасова

«05» мая 2025 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

«Системы искусственного интеллекта в информационной безопасности»

Составитель(и)

Демина Р.Ю., к.т.н., доц., доцент;

Согласовано с работодателями:

**Горбатенко С.Ю., заместитель директора ГБУ
АО «Инфраструктурный центр электронного
правительства»;
Лазарев Н.В., инженер 2 категории группы
контроля безопасности объектов критической
информационной безопасности управления
корпоративной защиты ООО «Газпром добыча
Астрахань»;**

Направление подготовки /
специальность

10.03.01 Информационная безопасность

Направленность (профиль) /
специализация ОПОП

**«Организация и технология защиты
информации»**

Квалификация (степень)

бакалавр

Форма обучения

очная, очно-заочная

Год приёма

2025

Курс

**4 (по очной форме)
5 (по очно-заочной форме)**

Семестр(ы)

**7 (по очной форме) /
9 (по очно-заочной форме)**

1. ЦЕЛИ И ЗАДАЧИ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)

1.1. Целями освоения дисциплины (модуля) «Системы искусственного интеллекта в информационной безопасности» являются овладение студентами основными методами теории интеллектуальных систем, приобретение навыков по использованию интеллектуальных систем в области информационной безопасности, изучение основных методов представления знаний и моделирования рассуждений.

1.2. Задачи освоения дисциплины (модуля):

- изучение теоретических моделей рассуждений, поведения, обучения в когнитивных науках, постановки проблем математического и информационного моделирования сложных систем;
- умение планировать процесс моделирования и вычислительного эксперимента;
- овладение навыками постановки задач и обработки результатов компьютерного моделирования.

2. МЕСТО ДИСЦИПЛИНЫ (МОДУЛЯ) В СТРУКТУРЕ ОПОП

2.1. Учебная дисциплина (модуль) «Системы искусственного интеллекта в информационной безопасности» относится к части, формируемой участниками образовательных отношений и осваивается в 7 семестре при очной форме обучения и в 9 – при очно-заочной.

2.2. Для изучения данной учебной дисциплины (модуля) необходимы следующие знания, умения, навыки, формируемые предшествующими учебными дисциплинами (модулями):

- введение в методы искусственного интеллекта
- теория вероятностей и математическая статистика;
- дискретная математика.

Знания: основные понятия теории вероятностей, математической статистики, дискретной математики.

Умения: решать типовые задачи теории вероятностей, математической статистики и дискретной математики.

Навыки: владеть методами оценки репрезентативности выборки и составления деревьев решений.

2.3. Последующие учебные дисциплины (модули) и (или) практики, для которых необходимы знания, умения, навыки, формируемые данной учебной дисциплиной (модулем):

- преддипломная практика.

3. ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ (МОДУЛЮ)

Процесс освоения дисциплины (модуля) направлен на формирование элементов следующей(их) компетенции(ий) в соответствии с ФГОС ВО и ОПОП ВО по данному направлению подготовки / специальности:

ПК 4 «Способен осуществлять внедрение систем защиты информации для обеспечения информационной безопасности автоматизированных систем».

ПК 5 «Способен администрировать средства защиты информации в компьютерных системах и сетях»

Таблица 1. Декомпозиция результатов обучения

Код компетенции	Код и наименование индикатора достижения компетенции ¹	Планируемые результаты обучения по дисциплине (модулю)		
		Знать (1)	Уметь (2)	Владеть (3)
ПК-4		основные угрозы безопасности информации и модели нарушителя в автоматизированных системах, содержание эксплуатационной документации автоматизированной системы, типовые средства, методы и протоколы идентификации, аутентификации и авторизации, основные меры по защите информации в автоматизированных системах, нормативные правовые акты в области защиты информации	администрировать программные средства системы защиты информации автоматизированных систем, устранять известные уязвимости автоматизированной системы, приводящие к возникновению угроз безопасности информации, применять аналитические и компьютерные модели автоматизированных систем и систем защиты информации, определять параметры настройки программного обеспечения системы защиты информации автоматизированной системы	методикой анализа структурных и функциональных схем защищенной автоматизированной системы
ПК-5		источники угроз информационной безопасности в компьютерных сетях и меры по их предотвращению; принципы функционирования программных средств	анализировать угрозы безопасности информации в компьютерных системах и сетях; настраивать правила обработки пакетов в компьютерных	навыками управления средствами межсетевого экранирования в компьютерных сетях, методикой оценки оптимальности выбора

¹ Указываются в соответствии с утвержденными в ОПОП ВО

Код компетенции	Код и наименование индикатора достижения компетенции ¹	Планируемые результаты обучения по дисциплине (модулю)		
		Знать (1)	Уметь (2)	Владеть (3)
		криптографической защиты информации; виды политик управления доступом и информационными потоками в компьютерных сетях; требования по составу и характеристикам подсистем защиты информации применительно к операционным системам; принципы работы и правила эксплуатации программно-аппаратных средств защиты информации	сетях; настраивать политики безопасности операционных систем, оценивать угрозы безопасности информации в компьютерных системах и сетях, противодействовать угрозам безопасности информации с использованием встроенных средств защиты информации операционных систем, настраивать антивирусные средства защиты информации в операционных системах	программно-аппаратных средств защиты информации и их режимов функционирования в операционных системах

4. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

Общая трудоемкость дисциплины в соответствии с учебным планом составляет 4 зачетные единицы (144 часа).

Трудоемкость отдельных видов учебной работы студентов очной, очно-заочной и заочной форм обучения приведена в таблице 2.1.

Таблица 2.1. Трудоемкость отдельных видов учебной работы по формам обучения

Вид учебной и внеучебной работы	для очной формы обучения	для очно-заочной формы обучения
Объем дисциплины в зачетных единицах	4	4
Объем дисциплины в академических часах	144	144
Контактная работа обучающихся с преподавателем (всего), в том числе (час.):		
- занятия лекционного типа, в том числе:	18	9
- практическая подготовка (если предусмотрена)	0	0
- занятия семинарского типа (семинары, практические, лабораторные), в том числе:	36	18

Вид учебной и внеучебной работы	для очной формы обучения	для очно-заочной формы обучения
- практическая подготовка (если предусмотрена)	0	0
- в ходе подготовки и защиты курсовой работы ²	0	0
- консультация (предэкзаменационная) ³	1	1
- промежуточная аттестация по дисциплине ⁴	0,25	0,25
Самостоятельная работа обучающихся (час.)	88,75	115,75
Форма промежуточной аттестации обучающегося (зачет/экзамен), семестр (ы)	экзамен – 7 семестр	экзамен – 9 семестр

Содержание дисциплины, структурированное по темам (разделам) с указанием отведенного на них количества академических часов и видов учебных занятий и самостоятельной работы, для каждой формы обучения представлено в таблице 2.2.

Таблица 2.2. Структура и содержание дисциплины (модуля)

Раздел, тема дисциплины (модуля)	для очной формы обучения							КР / КП	СР, час.	Итого часов	Форма текущего контроля успеваемости и, форма промежуточной аттестации [по семестрам]
	Контактная работа, час.										
	Л		ПЗ		ЛР						
Л	в т.ч. ПП	ПЗ	в т.ч. ПП	ЛР	в т.ч. ПП						
Семестр 1.											
Раздел I. Жизненный цикл модели машинного обучения в задачах защиты информации											
<i>Тема 1. Введение в системы искусственного интеллекта в информационной безопасности</i>	2	0	0	0	4	0	0	10	16		
<i>Тема 2. Обучающее множество в задачах защиты информации</i>	2	0	0	0	4	0	0	10	16		
<i>Тема 3. Моделирование и прогнозирование в задачах защиты информации</i>	2	0	0	0	4	0	0	10	16		
<i>Тема 4. Оценка и оптимизация моделей в сфере информационной безопасности</i>	2	0	0	0	4	0	0	10	16		

² Числовые данные в данной строке соответствуют трудоемкости, указанной в учебном плане в столбце «КР/КП» Если курсовая работа не предусмотрена – необходимо удалить строку «Контактная работа в ходе подготовки и защиты курсовой работы».

³ Числовые данные в данной строке соответствуют трудоемкости, указанной в учебном плане в столбце «Конс. (для гр.)»

⁴ Числовые данные в данной строке соответствуют трудоемкости, указанной в учебном плане в столбце «КПА»

Раздел, тема дисциплины (модуля)	Контактная работа, час.							КР / КП	СР, час.	Итого часов	Форма текущего контроля успеваемости и, форма промежуточ ной аттестации [по семестрам]
	Л		ПЗ		ЛР						
	Л	в т.ч. ПП	ПЗ	в т.ч. ПП	ЛР	в т.ч. ПП					
Раздел II. Примеры прикладных задач из сферы информационной безопасности											
<i>Тема 5. Атаки на системы искусственного интеллекта</i>	2	0	0	0	4	0	0	10	16		
<i>Тема 6. Задача обнаружения вредоносного программного обеспечения</i>	2	0	0	0	4	0	0	10	16		
<i>Тема 7. Задача поиска аномалий пользовательского трафика</i>	2	0	0	0	4	0	0	10	16		
<i>Тема 8. Задача распознавания лиц</i>	2	0	0	0	4	0	0	10	16		
<i>Тема 9. Задача распознавания «дипфейков»</i>	2	0	0	0	4	0	0	8,7 5	14, 75		
Консультации	1										
Контроль промежуточной аттестации									0,25		Экзамен
ИТОГО за семестр:	18	0	0	0	36	0	0	88, 75	144		
Итого за весь период	18	0	0	0	36	0	0	88, 75	144		

для очно-заочной формы обучения

Раздел, тема дисциплины (модуля)	Контактная работа, час.							КР / КП	СР, час.	Итого часов	Форма текущего контроля успеваемости и, форма промежуточ ной аттестации [по семестрам]
	Л		ПЗ		ЛР						
	Л	в т.ч. ПП	ПЗ	в т.ч. ПП	ЛР	в т.ч. ПП					
Семестр 1.											
Раздел I. Жизненный цикл модели машинного обучения в задачах защиты информации											
<i>Тема 1. Введение в системы искусственного интеллекта в информационной безопасности</i>	1	0	0	0	2	0	0	13	16		

Раздел, тема дисциплины (модуля)	Контактная работа, час.							КР / КП	СР, час.	Итого часов	Форма текущего контроля успеваемости и, форма промежуточ ной аттестации [по семестрам]
	Л		ПЗ		ЛР						
	Л	в т.ч. ПП	ПЗ	в т.ч. ПП	ЛР	в т.ч. ПП					
<i>Тема 2. Обучающее множество в задачах защиты информации</i>	1	0	0	0	2	0	0	13	16		
<i>Тема 3. Моделирование и прогнозирование в задачах защиты информации</i>	1	0	0	0	2	0	0	13	16		
<i>Тема 4. Оценка и оптимизация моделей в сфере информационной безопасности</i>	1	0	0	0	2	0	0	13	16		
Раздел II. Примеры прикладных задач из сферы информационной безопасности											
<i>Тема 5. Атаки на системы искусственного интеллекта</i>	1	0	0	0	2	0	0	13	16		
<i>Тема 6. Задача обнаружения вредоносного программного обеспечения</i>	1	0	0	0	2	0	0	13	16		
<i>Тема 7. Задача поиска аномалий пользовательского трафика</i>	1	0	0	0	2	0	0	13	16		
<i>Тема 8. Задача распознавания лиц</i>	1	0	0	0	2	0	0	13	16		
<i>Тема 9. Задача распознавания «дипфейков»</i>	1	0	0	0	2	0	0	11, 75	14, 75		
Консультации	1										
Контроль промежуточной аттестации								0,25	Экзамен		
ИТОГО за семестр:	18	0	0	0	36	0	0	88, 75	144		
Итого за весь период	18	0	0	0	36	0	0	88, 75	144		

Примечание: Л – лекция; ПЗ – практическое занятие, семинар; ЛР – лабораторная работа; ПП – практическая подготовка; КР / КП – курсовая работа / курсовой проект; СР – самостоятельная работа

Таблица 3. Матрица соотнесения разделов, тем учебной дисциплины (модуля) и формируемых компетенций

Раздел, тема дисциплины (модуля)	Кол-во часов	Код компетенции		Общее количество компетенций
		ПК-4	ПК-5	
Раздел I. Жизненный цикл модели машинного обучения в задачах защиты информации				
<i>Тема 1. Введение в системы искусственного интеллекта в информационной безопасности</i>	16	+	+	2
<i>Тема 2. Обучающее множество в задачах защиты информации</i>	16	+	+	2
<i>Тема 3. Моделирование и прогнозирование в задачах защиты информации</i>	16	+	+	2
<i>Тема 4. Оценка и оптимизация моделей в сфере информационной безопасности</i>	16	+	+	2
Раздел II. Примеры прикладных задач из сферы информационной безопасности				
<i>Тема 5. Атаки на системы искусственного интеллекта</i>	16	+	+	2
<i>Тема 6. Задача обнаружения вредоносного программного обеспечения</i>	16	+	+	2
<i>Тема 7. Задача поиска аномалий пользовательского трафика</i>	16	+	+	2
<i>Тема 8. Задача распознавания лиц</i>	16	+	+	2
<i>Тема 9. Задача распознавания «дипфейков»</i>	14,75	+	+	2
Итого	142,75			

Краткое содержание каждой темы дисциплины (модуля)

Раздел I. Жизненный цикл модели машинного обучения в задачах защиты информации

Тема 1. Введение в системы искусственного интеллекта в информационной безопасности. Принятие решений на основе данных: традиционный подход, подход с машинным обучением (преимущества и сложности). Сбор и подготовка данных. Обучение модели. Оценка производительности. Оптимизация производительности. Способы повышения эффективности.

Тема 2. Обучающее множество в задачах защиты информации. Важность качества обучающего множества с точки зрения информационной безопасности. Специфика сбора данных в сфере информационной безопасности. Сбор данных: входные признаки, целевая переменная, объем и репрезентативность обучающей выборки. Подготовка данных к моделированию: категориальные признаки, отсутствующие данные, проектирование признаков, нормализация данных. Визуализация данных: мозаичные диаграммы, диаграмма размаха, графики плотности, диаграммы рассеяния.

Тема 3. Моделирование и прогнозирование в задачах защиты информации. Основы моделирования с машинным обучением в сфере информационной безопасности: поиск связи между входными данными и целевой переменной, методы моделирования, обучение с учителем и без. Специфика сложности классификации и предсказаний в сфере информационной безопасности. Классификация: построение классификатора и получение предсказаний, классификация сложных нелинейных данных, классификация в случае множества классов. Регрессия: построение регрессора и генерация прогнозов, регрессия для сложных нелинейных данных.

Тема 4. Оценка и оптимизация моделей в сфере информационной безопасности. Нюансы проверки моделей в сфере информационной безопасности. Оценка прогностической точности на новых данных: проблема переобучения, скользящий контроль, перекрестная проверка. Оценка моделей классификации: таблица сопряженности, ROC-кривые, оценка многоклассовых классификаторов. Оценка моделей регрессии: показатели эффективности регрессионных моделей, исследование остатков. Оптимизация модели путем подбора параметров: параметры настройки алгоритмов и сеточный поиск.

Раздел II. Примеры прикладных задач из сферы информационной безопасности.

Тема 5. Атаки на системы искусственного интеллекта. Атаки на обучающее множество. Возможные негативные последствия. Состязательные атаки. Детектирование состязательных атак.

Тема 6. Задача обнаружения вредоносного программного обеспечения. Методы обнаружения вредоносного программного обеспечения. Признаки, извлекаемые из вредоносных файлов. Алгоритмы обучения, применяемые для обучения антивирусных классификаторов.

Тема 7. Задача поиска аномалий пользовательского трафика. Проблема ботов. Проблема DDos-атак. Задача определения нелегитимного трафика.

Тема 8. Задача распознавания лиц. Признаки, извлекаемые из изображений лиц. Алгоритмы распознавания. Проблема распознавания. Распознавание по походке.

Тема 9. Задача распознавания «дипфейков». Морально-этические аспекты создания «дипфейков»: легальное и зловредное применение. Морфинг. «Дипфейки». Методы распознавания искусственно сгенерированных изображений.

5. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ПО ПРЕПОДАВАНИЮ И ОСВОЕНИЮ ДИСЦИПЛИНЫ (МОДУЛЯ)

5.1. Указания для преподавателей по организации и проведению учебных занятий по дисциплине (модулю)

Для организаций лекционных занятий необходим проектор и доска. Для проведения лабораторных занятий требуется компьютерный класс с установленными средами разработки на языках программирования высокого уровня и программный пакет WEKA.

5.2. Указания для обучающихся по освоению дисциплины (модулю)

Таблица 4. Содержание самостоятельной работы обучающихся

для очной формы обучения

Вопросы, выносимые на самостоятельное изучение	Кол-во часов	Форма работы
Раздел I. Жизненный цикл модели машинного обучения в задачах защиты информации		Опросы, лабораторные работы
Тема 1. Введение в системы искусственного интеллекта в информационной безопасности	10	Подготовка к опрос
Тема 2. Обучающее множество в задачах защиты информации	10	Выполнение лабораторной работы 1
Тема 3. Моделирование и прогнозирование в задачах защиты информации	10	Выполнение лабораторной работы 2
Тема 4. Оценка и оптимизация моделей в сфере информационной безопасности	10	Выполнение лабораторной работы 3
Раздел II. Примеры прикладных задач из сферы информационной безопасности		
Тема 5. Атаки на системы искусственного интеллекта	10	Выполнение лабораторной работы 4
Тема 6. Задача обнаружения вредоносного программного обеспечения	10	Презентация реферата
Тема 7. Задача поиска аномалий пользовательского трафика	10	Выполнение лабораторной работы 5
Тема 8. Задача распознавания лиц	10	Презентация реферата
Тема 9. Задача распознавания «дипфейков»	8,75	Выполнение лабораторной работы 6

для очно-заочной формы обучения

Вопросы, выносимые на самостоятельное изучение	Кол-во часов	Форма работы
Раздел I. Жизненный цикл модели машинного обучения в задачах защиты информации		Опросы, лабораторные работы
Тема 1. Введение в системы искусственного интеллекта в информационной безопасности	13	Подготовка к опрос
Тема 2. Обучающее множество в задачах защиты информации	13	Выполнение лабораторной работы 1
Тема 3. Моделирование и прогнозирование в задачах защиты информации	13	Выполнение лабораторной работы 2
Тема 4. Оценка и оптимизация моделей в сфере информационной безопасности	13	Выполнение лабораторной работы 3
Раздел II. Примеры прикладных задач из сферы информационной безопасности		
Тема 5. Атаки на системы искусственного интеллекта	13	Выполнение лабораторной работы 4
Тема 6. Задача обнаружения вредоносного программного обеспечения	13	Презентация реферата
Тема 7. Задача поиска аномалий пользовательского трафика	13	Выполнение лабораторной работы 5
Тема 8. Задача распознавания лиц	13	Презентация реферата
Тема 9. Задача распознавания «дипфейков»	11,75	Выполнение лабораторной работы 6

5.3. Виды и формы письменных работ, предусмотренных при освоении дисциплины (модуля), выполняемые обучающимися самостоятельно

Лабораторные работы. На ЯВУ или с помощью программной среды WEKA необходимо провести эксперимент, предложенный в рамках лабораторной работы. Для отчета требуется предоставить обученную модель и отчет с результатами эксперимента.

Опрос. Студентам требуется подготовиться к ответам на вопросы по прошедшей теме занятия.

Реферат. Студентам требуется проанализировать отечественную и зарубежную литературу и представить реферат на тему используемых подходов к решению задач информационной безопасности.

6. ОБРАЗОВАТЕЛЬНЫЕ И ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ

6.1. Образовательные технологии

Таблица 5. Образовательные технологии, используемые при реализации учебных занятий

Раздел, тема дисциплины (модуля)	Форма учебного занятия		
	Лекция	Практическое занятие, семинар	Лабораторная работа
<i>Раздел I. Жизненный цикл модели машинного обучения в задачах защиты информации</i>			
<i>Тема 1. Введение в системы искусственного интеллекта в информационной безопасности</i>	Обзорная лекция, лекция-презентация	Не предусмотрено	Фронтальный опрос
<i>Тема 2. Обучающее множество в задачах защиты информации</i>	Обзорная лекция, лекция-презентация	Не предусмотрено	Анализ ситуаций и имитационных моделей
<i>Тема 3. Моделирование и прогнозирование в задачах защиты информации</i>	Интерактивная лекция	Не предусмотрено	Анализ ситуаций и имитационных моделей
<i>Тема 4. Оценка и оптимизация моделей в сфере информационной безопасности</i>	Интерактивная лекция	Не предусмотрено	Анализ ситуаций и имитационных моделей
<i>Раздел II. Примеры прикладных задач из сферы информационной безопасности</i>			
<i>Тема 5. Атаки на системы искусственного интеллекта</i>	Интерактивная лекция	Не предусмотрено	Анализ ситуаций и имитационных моделей
<i>Тема 6. Задача обнаружения вредоносного программного обеспечения</i>	Интерактивная лекция	Не предусмотрено	Групповая дискуссия после заслушивания рефератов
<i>Тема 7. Задача поиска аномалий пользовательского трафика</i>	Интерактивная лекция	Не предусмотрено	Анализ ситуаций и имитационных моделей
<i>Тема 8. Задача распознавания лиц</i>	Интерактивная лекция	Не предусмотрено	Групповая дискуссия после заслушивания рефератов
<i>Тема 9. Задача распознавания «дипфейков»</i>	Интерактивная лекция	Не предусмотрено	Анализ ситуаций и имитационных моделей

6.2. Информационные технологии

Информационные технологии, используемые при реализации различных видов учебной и внеучебной работы:

- использование возможностей интернета в учебном процессе (использование сайта преподавателя (рассылка заданий, предоставление выполненных работ, ответы на вопросы, ознакомление обучающихся с оценками и т. д.));
- использование электронных учебников и различных сайтов (например, электронных библиотек, журналов и т. д.) как источников информации;
- использование возможностей электронной почты преподавателя;
- использование средств представления учебной информации (электронных учебных пособий и практикумов, применение новых технологий для проведения очных (традиционных) лекций и семинаров с использованием презентаций и т. д.);
- использование интегрированных образовательных сред, где главной составляющей являются не только применяемые технологии, но и содержательная часть, т. е. информационные ресурсы (доступ к мировым информационным ресурсам, на базе которых строится учебный процесс);
- использование виртуальной обучающей среды (LMS Moodle «Электронное образование») или иных информационных систем, сервисов и мессенджеров]

6.3. Программное обеспечение, современные профессиональные базы данных и информационные справочные системы

6.3.1. Программное обеспечение

Наименование программного обеспечения	Назначение
Adobe Reader	Программа для просмотра электронных документов
Платформа дистанционного обучения LMS Moodle	Виртуальная обучающая среда
Mozilla FireFox	Браузер
Microsoft Office 2013, Microsoft Office Project 2013, Microsoft Office Visio 2013	Офисная программа
7-zip	Архиватор
Microsoft Windows 7 Professional	Операционная система
Kaspersky Endpoint Security	Средство антивирусной защиты
Microsoft Visual Studio	Среда разработки
Python	Среда разработки
Weka	Среда моделирования

6.3.2. Современные профессиональные базы данных и информационные справочные системы

- Электронный каталог Научной библиотеки АГУ на базе MARK SQL НПО «Информ-систем»: <https://library.asu.edu.ru>.
- Электронный каталог «Научные журналы АГУ»: <http://journal.asu.edu.ru/>.
- Универсальная справочно-информационная полнотекстовая база данных периодических изданий ООО «ИВИС»: <http://dlib.eastview.com/>
- Электронно-библиотечная система eLibrary. <http://elibrary.ru>

- Справочная правовая система КонсультантПлюс: <http://www.consultant.ru>
- Информационно-правовое обеспечение «Система ГАРАНТ»: <http://garant-astrakhan.ru>

7. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ ПРОВЕДЕНИЯ ТЕКУЩЕГО КОНТРОЛЯ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ПО ДИСЦИПЛИНЕ (МОДУЛЮ)

7.1. Паспорт фонда оценочных средств

При проведении текущего контроля и промежуточной аттестации по дисциплине (модулю) «Системы искусственного интеллекта в информационной безопасности» проверяется сформированность у обучающихся компетенций, указанных в разделе 3 настоящей программы. Этапность формирования данных компетенций в процессе освоения образовательной программы определяется последовательным освоением дисциплин (модулей) и прохождением практик, а в процессе освоения дисциплины (модуля) – последовательным достижением результатов освоения содержательно связанных между собой разделов, тем.

Таблица 6. Соответствие разделов, тем дисциплины (модуля), результатов обучения по дисциплине (модулю) и оценочных средств

Контролируемый раздел, тема дисциплины (модуля)	Код контролируемой компетенции	Наименование оценочного средства
Раздел I. Жизненный цикл модели машинного обучения в задачах защиты информации	ПК-4, ПК-5	Лабораторные работы, опрос
Тема 1. Введение в системы искусственного интеллекта в информационной безопасности	ПК-4, ПК-5	Опрос
Тема 2. Обучающее множество в задачах защиты информации	ПК-4, ПК-5	Лабораторная работа 1
Тема 3. Моделирование и прогнозирование в задачах защиты информации	ПК-4, ПК-5	Лабораторная работа 2
Тема 4. Оценка и оптимизация моделей в сфере информационной безопасности	ПК-4, ПК-5	Лабораторная работа 3
Раздел II. Примеры прикладных задач из сферы информационной безопасности	ПК-4, ПК-5	Лабораторные работы, реферат
Тема 5. Атаки на системы искусственного интеллекта	ПК-4, ПК-5	Лабораторная работа 4
Тема 6. Задача обнаружения вредоносного программного обеспечения	ПК-4, ПК-5	Реферат
Тема 7. Задача поиска аномалий пользовательского трафика	ПК-4, ПК-5	Лабораторная работа 5
Тема 8. Задача распознавания лиц	ПК-4, ПК-5	Реферат
Тема 9. Задача распознавания «дипфейков»	ПК-4, ПК-5	Лабораторная работа 6

7.2. Описание показателей и критериев оценивания компетенций, описание шкал оценивания

Таблица 7. Показатели оценивания результатов обучения в виде знаний

Шкала оценивания	Критерии оценивания
5 «отлично»	демонстрирует глубокое знание теоретического материала, умение обоснованно излагать свои мысли по обсуждаемым вопросам, способность

Шкала оценивания	Критерии оценивания
	полно, правильно и аргументированно отвечать на вопросы, приводить примеры
4 «хорошо»	демонстрирует знание теоретического материала, его последовательное изложение, способность приводить примеры, допускает единичные ошибки, исправляемые после замечания преподавателя
3 «удовлетворительно»	демонстрирует неполное, фрагментарное знание теоретического материала, требующее наводящих вопросов преподавателя, допускает существенные ошибки в его изложении, затрудняется в приведении примеров и формулировке выводов
2 «неудовлетворительно»	демонстрирует существенные пробелы в знании теоретического материала, не способен его изложить и ответить на наводящие вопросы преподавателя, не может привести примеры

Таблица 8. Показатели оценивания результатов обучения в виде умений и владений

Шкала оценивания	Критерии оценивания
5 «отлично»	демонстрирует способность применять знание теоретического материала при выполнении заданий, последовательно и правильно выполняет задания, умеет обоснованно излагать свои мысли и делать необходимые выводы
4 «хорошо»	демонстрирует способность применять знание теоретического материала при выполнении заданий, последовательно и правильно выполняет задания, умеет обоснованно излагать свои мысли и делать необходимые выводы, допускает единичные ошибки, исправляемые после замечания преподавателя
3 «удовлетворительно»	демонстрирует отдельные, несистематизированные навыки, испытывает затруднения и допускает ошибки при выполнении заданий, выполняет задание по подсказке преподавателя, затрудняется в формулировке выводов
2 «неудовлетворительно»	не способен правильно выполнить задания

7.3. Контрольные задания и иные материалы, необходимые для оценки результатов обучения по дисциплине (модулю)

Раздел I. Жизненный цикл модели машинного обучения в задачах защиты информации

Тема 1. Введение в системы искусственного интеллекта в информационной безопасности

Опрос

- a. Исследование предметной области. Формулировка задачи.
- b. Объекты, признаки, виды признаков, целевая переменная.
- c. Обучающее и проверочное множества.
- d. Обучение модели
- e. Алгоритмы обучения
- f. Оценка качество модели
- g. Оптимизация модели.

Тема 2. Обучающее множество в задачах защиты информации

Лабораторная работа 1.

Цель: разработать классификатор, который мог бы отличать корректные почтовые сообщения от спама.

Задачи:

1. Найдите или возьмите предложенный датасет.

2. Визуализируйте аналитику по датасету. В каких пропорциях представлены объекты в обучающем множестве?
3. Выберите подходящий алгоритм распознавания.
4. Обучите классификатор с использованием перекрестной проверки.
5. Для каждого классификатора вычислите:
 - матрицу сопряженности
 - верность(точность) и частоту ошибок
 - TP, TN, FP, FN - частоту ошибок и правильного распознавания каждого класса
6. Повторите шаг 3, построив модель с использованием других алгоритмов.
7. Для классификаторов, обученных с использованием разных алгоритмов, постройте график покрытия. Определите по нему наилучший классификатор.

Тема 3. Моделирование и прогнозирование в задачах защиты информации

Лабораторная работа 2

Цель: разработать регрессор, который мог бы предсказывать какое-либо фактическое значение.

Задачи:

1. Найдите или возьмите предложенный датасет.
2. Выберите подходящий алгоритм прогнозирования.
3. Оцените качество прогнозирования с использованием квадратного корня из среднеквадратичной ошибки и с использованием анализа остатков.
4. Сделайте вывод, какие именно признаки оказывают наиболее существенное влияние на целевую переменную.

Тема 4. Оценка и оптимизация моделей в сфере информационной безопасности

Лабораторная работа 3.

Цель: Обучить кластеризатор, который смог бы определять категории фейковых новостей.

Задачи:

1. Найдите или возьмите предложенный датасет.
2. Выберите подходящий алгоритм кластеризации.
3. На какие кластеры были разбиты данные? Сколько кластеров получилось? В чем вы не согласны с предложенным разбиением?

Раздел II. Машинное обучение в задачах информационной безопасности

Тема 5. Атаки на системы искусственного интеллекта

Лабораторная работа 4.

Цель: симитировать состязательную атаку на модель компьютерного зрения и реализовать метод детектирования.

Задачи:

1. Разработать модель компьютерного зрения, которая бы классифицировала объекты, изображенные на фотографиях.
2. Провести состязательную атаку на собственную модель
3. Разработать и проверить способы детектирования состязательных атак.

Тема 6. Задача обнаружения вредоносного программного обеспечения

Реферат 1. Различные подходы к обнаружению вредоносного программного обеспечения с использованием методов машинного обучения.

Тема 7. Задача поиска аномалий пользовательского трафика

Лабораторная работа 5.

Цель: Выявить основные закономерности в предложенной статистике по посещаемости web-сайта.

Задачи:

4. Определить основные тенденции в посещаемости сайта в зависимости от времени суток, от дня недели, от дня месяца.
5. Проверить как выявленные тенденции соответствуют часовому поясу пользователей.
6. Выявить аномалии в трафике.

Тема 8. Задача распознавания лиц

Реферат 2. Различные подходы к распознаванию лиц на изображениях и в видео.

Тема 9. Задача распознавания «дипфейков»

Лабораторная работа 6.

Цель: искусственно сгенерировать изображение и разработать метод детектирования.

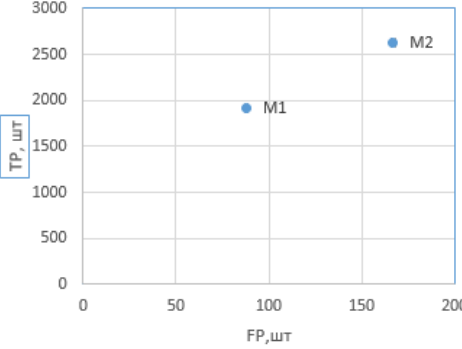
Задачи:

1. Искусственно сгенерировать изображение/видео.
2. Разработать и проверить способы детектирования искусственно сгенерированных изображений.

Таблица 9. Примеры оценочных средств с ключами правильных ответов

№ п/п	Тип задания	Формулировка задания	Правильный ответ	Время выполнения (в минутах)
ПК 4 «Способен осуществлять внедрение систем защиты информации для обеспечения информационной безопасности автоматизированных систем».				
1.	Задание закрытого типа	Что такое нормализация данных? 1. Усреднение данных 2. Преобразование категориальных признаков в численные 3. Преобразование численных признаков в категориальные 4. Подгонка под единую шкалу	3	1
2.		Укажите соответствие между типами входных/целевых признаков и диаграммой, которую целесообразно использовать для визуализации 1. Входной признак- категориальный, целевая переменная- категориальная 2. Входной признак- категориальный, Целевая переменная- числовая 3. Входной признак- числовой, Целевая переменная- категориальная 4. Входной признак- числовой, Целевая переменная- числовая а. Диаграмма рассеяния б. Диаграмма размаха с. График плотности д. Мозаичная диаграмма	1-d 2-с 3-b 4-a	5

№ п/п	Тип задания	Формулировка задания	Правильный ответ	Время выполнения (в минутах)
3.		Если вам необходимо из аудиозаписи выделить голоса различных людей, то какую задачу вы будете решать? 1. Понижения размерности 2. Регрессии 3. Классификации 4. Кластеризации	4	2
4.		Для оценки эффективности регрессора применяют: 1. Точность 2. Верность 3. Долю истинно положительных результатов 4. Квадратный корень из среднеквадратичной ошибки 5. Частотой ошибки	4	3
5.		Какой алгоритм основан на гипотезе «Набор слабых обучающих алгоритмов способен создать сильный обучающий алгоритм»? 1. Бустинг 2. Случайный лес 3. Нейронные сети 4. Наивный Байес	1	3
6.	Задание открытого типа	Что делать в случае, если в обучающем множестве отсутствуют какие-либо данные	Существует несколько стратегий: <ul style="list-style-type: none"> • создать новую категорию для отсутствующих данных • удалить экземпляры с отсутствующими данными • подставить значение предшествующего экземпляра • заместить отсутствующее значение средним значением столбца • заместить с помощью модели МО 	5
7.		Что такое точность классификации?	Точность-это доля правильно	2

№ п/п	Тип задания	Формулировка задания	Правильный ответ	Время выполнения (в минутах)
			распознанных экземпляров.	
8.		Какие признаки называются категориальными?	Признаки называются категориальными, если их можно отнести к какой-либо группе, но при этом не важен порядок	2
9.		В чем выражается проблема переобучения?	Модель эффективно работает только с теми данными, на которых была обучена	3
10.		В проверочном множестве 800 объектов: 300 объектов класса <i>a</i> , 500 объектов класса <i>b</i> . Правильно были распознаны 275 объектов класса <i>a</i> и 480 объектов класса <i>b</i> . Рассчитайте верность (accuracy) классификатора.	0,94	3
ПК 5 «Способен администрировать средства защиты информации в компьютерных системах и сетях»				
11.	Задание закрытого типа	<p>На рисунке представлен график покрытия, изображающий сравнение двух моделей. Какая модель доминирует?</p> <p>График покрытия</p>  <p>1) M1 2) M2 3) Ни одна</p>	3	3
12.		<p>ROC-кривая описывает...</p> <p>1) зависимость ложных срабатываний от размера обучающего множества 2) чувствительность модели к разным порогам классификации</p>	2	4

№ п/п	Тип задания	Формулировка задания	Правильный ответ	Время выполнения (в минутах)
		3) качество модели при тестировании с использованием различных проверочных множеств 4) частоту истинно положительных ответов модели		
13.		Как связаны между собой AUC и ROC 1) ROC-«кривая ошибок», а AUC – площадь под ней 2) ROC- «кривая правильных ответов» , а AUC- площадь над ней 3) ROC – график, а AUC- оптимальное пороговое значение 4) AUC-«кривая ошибок», а ROC- площадь под ней 5) AUC - «кривая правильных ответов», а ROC - площадь над ней 6) AUC – график, а ROC - оптимальное пороговое значение	1	3
14.		Выберите верное утверждение: 1) Чем ближе к 1 индекс корреляции, тем выше качество модели множественной регрессии. 2) Чем ближе к 0 коэффициент детерминации, тем выше качество модели множественной регрессии. 3) Независимость остатков проверяется с помощью критерия Дарбина – Уотсона. 4) Качество регрессора характеризуется фактом обоснованной зависимости остатков от целевой переменной.	1, 3	5
15.		Для решения каких задач информационной безопасности обычно используются методы машинного обучения? 1) Распознавание лиц 2) Составление модели нарушителя	1,4	5

№ п/п	Тип задания	Формулировка задания	Правильный ответ	Время выполнения (в минутах)
		3) Прогнозирование числа кибер-атак 4) Обнаружение аномалий в сетевом трафике 5) Построение модели угроз		
16.		Укажите соответствие между мерами схожести и формулами по которым они вычисляются 1) Евклидово расстояние 2) Квадрат евклидова расстояния 3) Расстояние городских кварталов (манхэттенское расстояние) 4) Расстояние Чебышева а) $\rho(x, x') = \max(x_i - x'_i)$ б) $\rho(x, x') = \sum_i^n (x_i - x'_i)^2$ в) $\rho(x, x') = \sqrt{\sum_i^n (x_i - x'_i)^2}$ г) $\rho(x, x') = \sum_i^n x_i - x'_i $	1) -с 2) -b 3) -d 4)-a	5
17.	Задания открытого типа	Какая информация хранится в матрицах сопряженности по результатам тестирования классификатора?	Информация о правильно и неправильно распознанных объектах каждого класса: FP, TP, FN, TN	5
18.		Перечислите основные типы алгоритмов кластеризации	<ul style="list-style-type: none"> • Иерархический • k-средних • с-средних • Выделение связанных компонент • Минимальное покрывающее дерево • Послойная кластеризация 	5

Полный комплект оценочных материалов по дисциплине (модулю) (фонд оценочных средств) хранится в электронном виде на кафедре, утверждающей рабочую программу дисциплины (модуля).

7.4. Методические материалы, определяющие процедуры оценивания результатов обучения по дисциплине (модулю)

Таблица 10. Технологическая карта рейтинговых баллов по дисциплине (модулю)

№ п/п	Контролируемые мероприятия	Количество мероприятий / баллы	Максимальное количество баллов	Срок представления
Основной блок				
1.	Выполнение лабораторной работы	6/4	24	
2.	Выполнение контрольной работы	3/4	12	
3.	Тест	1/4	4	
Всего			40	-
Блок бонусов				
4.	Посещение занятий без пропусков	1	3	
5.	Своевременное выполнение всех заданий	1	3	
6.	Активность студента на занятии	1	4	
Всего			10	-
Дополнительный блок**				
7.	<i>Зачет (Диф.зачет) / Экзамен</i>		50	
Всего			50	-
ИТОГО			100	-

Таблица 11. Система штрафов (для одного занятия)

Показатель	Балл
Опоздание на занятие	- 1
Нарушение учебной дисциплины	- 1
Неготовность к занятию	- 2
Пропуск занятия без уважительной причины	- 2

Таблица 12. Шкала перевода рейтинговых баллов в итоговую оценку за семестр по дисциплине (модулю)

Сумма баллов	Оценка по 4-балльной шкале	
90–100	5 (отлично)	Зачтено
85–89	4 (хорошо)	
75–84		
70–74		
65–69	3 (удовлетворительно)	
60–64		
Ниже 60	2 (неудовлетворительно)	Не зачтено

При реализации дисциплины (модуля) в зависимости от уровня подготовленности обучающихся могут быть использованы иные формы, методы контроля и оценочные средства, исходя из конкретной ситуации.

8. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

8.1. Основная литература

1. Кольер, Р. Машинное обучение в Elastic Stack / Р. Кольер, К. Монтонен, Б. Азарми; пер. с англ. В. С. Яценкова. - Москва : ДМК Пресс, 2021. - 380 с. - ISBN 978-5-93700-107-8. - Текст : электронный // ЭБС "Консультант студента" : [сайт]. - URL : <https://www.studentlibrary.ru/book/ISBN9785937001078.html> (дата обращения: 21.12.2022). - Режим доступа : по подписке. Андреева Г. М. Социальная психология: учебник. М.: Аспект Пресс, 2002. 364 с. (23 экз.).
2. Машинное обучение с использованием библиотеки H2O / Д. Кук - Москва : ДМК Пресс, 2018. - ISBN 978-5-97060-508-0. - Текст : электронный // ЭБС "Консультант студента" : [сайт]. - URL : <https://www.studentlibrary.ru/book/ISBN9785970605080.html> (дата обращения: 21.12.2022). - Режим доступа : по подписке.
3. Машинное обучение с использованием библиотеки H2O / Д. Кук - Москва : ДМК Пресс, 2018. - ISBN 978-5-97060-508-0. - Текст : электронный // ЭБС "Консультант студента" : [сайт]. - URL : <https://www.studentlibrary.ru/book/ISBN9785970605080.html> (дата обращения: 21.12.2022). - Режим доступа : по подписке.
4. Python и машинное обучение / С. Рашка - Москва : ДМК Пресс, 2017. - ISBN 978-5-97060-409-0. - Текст : электронный // ЭБС "Консультант студента" : [сайт]. - URL : <https://www.studentlibrary.ru/book/ISBN9785970604090.html> (дата обращения: 21.12.2022). - Режим доступа : по подписке.
5. Python и машинное обучение / С. Рашка - Москва : ДМК Пресс, 2017. - ISBN 978-5-97060-409-0. - Текст : электронный // ЭБС "Консультант студента" : [сайт]. - URL : <https://www.studentlibrary.ru/book/ISBN9785970604090.html> (дата обращения: 21.12.2022). - Режим доступа : по подписке.
6. Горбаченко, В. И. Машинное обучение : учебное пособие / В. И. Горбаченко, К. Е. Савенков, М. А. Малахов. — Москва : Ай Пи Ар Медиа, 2023. — 217 с. — ISBN 978-5-4497-1860-0. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: <https://www.iprbookshop.ru/125886.html> (дата обращения: 28.11.2022). — Режим доступа: для авторизир. пользователей. - DOI: <https://doi.org/10.23682/125886>
7. Павлова, А. И. Искусственные нейронные сети : учебное пособие / А. И. Павлова. — Москва : Ай Пи Ар Медиа, 2021. — 190 с. — ISBN 978-5-4497-1165-6. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: <https://www.iprbookshop.ru/108228.html> (дата обращения: 21.12.2022). — Режим доступа: для авторизир. пользователей. - DOI: <https://doi.org/10.23682/108228>
8. Барский, А. Б. Введение в нейронные сети : учебное пособие / А. Б. Барский. — 3-е изд. — Москва, Саратов : Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2020. — 357 с. — ISBN 978-5-4497-0309-5. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: <https://www.iprbookshop.ru/89426.html> (дата обращения: 21.12.2022). — Режим доступа: для авторизир. пользователей

8.2. Дополнительная литература

1. Паттерсон, Дж. , Гибсон А. Глубокое обучение с точки зрения практика / Паттерсон Дж. , Гибсон А. , пер. с англ. А. А. Слинкина. - Москва : ДМК Пресс, 2018. - 418 с. - ISBN 978-5-97060-481-6. - Текст : электронный // ЭБС "Консультант студента" : [сайт]. - URL : <https://www.studentlibrary.ru/book/ISBN9785970604816.html> (дата обращения: 21.12.2022). - Режим доступа : по подписке.
2. (Манро), Р. Машинное обучение с участием человека / Монарх Р. (Манро) ; перевод В. И. Бахур. — Москва : ДМК Пресс, 2022. — 498 с. — ISBN 978-5-97060-934-7. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: <https://www.iprbookshop.ru/125122.html> (дата обращения: 20.10.2022). — Режим доступа: для авторизир. Пользователей
3. Яхьяева, Г. Э. Нечеткие множества и нейронные сети : учебное пособие / Г. Э. Яхьяева. — 4-е изд. — Москва : Интернет-Университет Информационных Технологий

(ИНТУИТ), Ай Пи Ар Медиа, 2020. — 315 с. — ISBN 978-5-4497-0665-2. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: <https://www.iprbookshop.ru/97552.html> (дата обращения: 21.12.2022). — Режим доступа: для авторизир. Пользователей

4. Барский, А. Б. Искусственный интеллект и логические нейронные сети : учебное пособие / А. Б. Барский. — Санкт-Петербург : Интермедия, 2019. — 360 с. — ISBN 978-5-4383-0155-4. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: <https://www.iprbookshop.ru/95270.html> (дата обращения: 21.12.2022). — Режим доступа: для авторизир. пользователей

8.3. Интернет-ресурсы, необходимые для освоения дисциплины (модуля)

1. Электронно-библиотечная система (ЭБС) ООО «Политехресурс» «Консультант студента». Многопрофильный образовательный ресурс «Консультант студента» является электронной библиотечной системой, предоставляющей доступ через сеть Интернет к учебной литературе и дополнительным материалам, приобретенным на основании прямых договоров с правообладателями. Каталог в настоящее время содержит около 15000 наименований. www.studentlibrary.ru.

2. Kaggle. Система организации конкурсов по исследованию данных, а также социальная сеть специалистов по обработке данных и машинному обучению. www.kaggle.com

9. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

Для проведения лекционных занятий необходима мультимедийная аудитория, оснащенная компьютерной презентационной техникой.

Для проведения лабораторных занятий необходима аудитория, оснащенная компьютерами.

10. ОСОБЕННОСТИ РЕАЛИЗАЦИИ ДИСЦИПЛИНЫ (МОДУЛЯ) ПРИ ОБУЧЕНИИ ИНВАЛИДОВ И ЛИЦ С ОГРАНИЧЕННЫМИ ВОЗМОЖНОСТЯМИ ЗДОРОВЬЯ

Рабочая программа дисциплины (модуля) при необходимости может быть адаптирована для обучения (в том числе с применением дистанционных образовательных технологий) лиц с ограниченными возможностями здоровья, инвалидов. Для этого требуется заявление обучающихся, являющихся лицами с ограниченными возможностями здоровья, инвалидами, или их законных представителей и рекомендации психолого-медико-педагогической комиссии. При обучении лиц с ограниченными возможностями здоровья учитываются их индивидуальные психофизические особенности. Обучение инвалидов осуществляется также в соответствии с индивидуальной программой реабилитации инвалида (при наличии).

Для лиц с нарушением слуха возможно предоставление учебной информации в визуальной форме (краткий конспект лекций; тексты заданий, напечатанные увеличенным шрифтом), на аудиторных занятиях допускается присутствие ассистента, а также сурдопереводчиков и тифлосурдопереводчиков. Текущий контроль успеваемости осуществляется в письменной форме: обучающийся письменно отвечает на вопросы, письменно выполняет практические задания. Доклад (реферат) также может быть представлен в письменной форме, при этом требования к содержанию остаются теми же, а требования к качеству изложения материала (понятность, качество речи, взаимодействие с аудиторией и т. д.) заменяются на соответствующие требования, предъявляемые к письменным работам (качество оформления текста и списка литературы, грамотность, наличие иллюстрационных материалов и т. д.). Промежуточная аттестация для лиц с нарушениями слуха проводится в письменной форме, при этом используются общие критерии оценивания. При необходимости время подготовки к ответу может быть увеличено.

Для лиц с нарушением зрения допускается аудиальное предоставление информации, а также использование на аудиторных занятиях звукозаписывающих устройств (диктофонов и т. д.). Допускается присутствие на занятиях ассистента (помощника), оказывающего

обучающимся необходимую техническую помощь. Текущий контроль успеваемости осуществляется в устной форме. При проведении промежуточной аттестации для лиц с нарушением зрения тестирование может быть заменено на устное собеседование по вопросам.

Для лиц с ограниченными возможностями здоровья, имеющих нарушения опорно-двигательного аппарата, на аудиторных занятиях, а также при проведении процедур текущего контроля успеваемости и промежуточной аттестации могут быть предоставлены необходимые технические средства (персональный компьютер, ноутбук или другой гаджет); допускается присутствие ассистента (ассистентов), оказывающего обучающимся необходимую техническую помощь (занять рабочее место, передвигаться по аудитории, прочитать задание, оформить ответ, общаться с преподавателем).