Аннотация к рабочей программе

дисциплины «Безопасность систем искусственного интеллекта»

1. Цель дисциплины

Формирование у студентов знаний и умений связанных с решением задач обеспечения безопасности систем искусственного интеллекта.

2. Задачи дисциплины

- изучение способов анализа угроз информационной безопасности систем искусственного интеллекта и основных общеметодологических принципов построения систем обеспечения информационной безопасности;
- получение навыков использования основных методов и средств проектирования систем обеспечения информационной безопасности, методов оценки качества систем и моделей, проведения аттестации защищаемых систем искусственного интеллекта.

3. Индикаторы компетенций, формируемые в результате освоения дисциплины:

ПК-8.1 Разрабатывает программное и аппаратное обеспечение технологий и систем искусственного интеллекта для решения профессиональных задач с учетом требований информационной безопасности в различных предметных областях;

ПК-8.2 Модернизирует программное и аппаратное обеспечение технологий и систем искусственного интеллекта для решения профессиональных задач с учетом требований информационной безопасности в различных предметных областях.

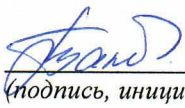
4. Разделы дисциплины

1. Проблемы информационной безопасности.
2. Источники, способы и результаты дестабилизирующего воздействия на информацию. Каналы и методы несанкционированного доступа к информации.
3. Моделирование процессов комплексной системы защиты информации. Нормативно-методическое обеспечение систем защиты информации. Управление комплексной системой защиты информации.

МИНОБРНАУКИ РОССИИ

Юго-Западный государственный университет

УТВЕРЖДАЮ:
И.о. декана факультета
фундаментальной и прикладной информатики.
(наименование ф-та полностью)


М.О. Таныгин
(подпись, инициалы, фамилия)

«18» 07. 2022 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Безопасность систем искусственного интеллекта
(наименование дисциплины)

ОПОП ВО 09.04.01 Информатика и вычислительная техника,
(шифр с наименованием направления подготовки (специальности))
программа «Киберфизические системы и искусственный интеллект»,
направленность (профиль) «Облачная и сетевая инфраструктура систем искусственного интеллекта»
(наименование направленности (профиля) или специализации)

форма обучения очная
(очная, очно-заочная, заочная)

Курск – 2022

Рабочая программа дисциплины составлена в соответствии с ФГОС ВО – магистратура по направлению подготовки 09.04.01 Информатика и вычислительная техника на основании учебного плана ОПОП ВО 09.04.01 Информатика и вычислительная техника, программа «Киберфизические системы и искусственный интеллект», направленность (профиль) «Облачная и сетевая инфраструктура систем искусственного интеллекта», одобренного Ученым советом университета (протокол № 5 от 27.12.2021 г.).

Рабочая программа дисциплины обсуждена и рекомендована к реализации в образовательном процессе для обучения студентов по ОПОП ВО 09.04.01 Информатика и вычислительная техника, программа «Киберфизические системы и искусственный интеллект», направленность (профиль) «Облачная и сетевая инфраструктура систем искусственного интеллекта»на заседании кафедры вычислительной техники№ 9 «18» февраля 2022 г.

(наименование кафедры, дата, номер протокола)

Зав. кафедрой _____ И.Е. Чернецкая

Разработчик программы

д.т.н., доцент _____ И.Е. Чернецкая

(ученая степень и ученое звание, Ф.И.О.)

Директор научной библиотеки _____ В.Г.Макаровская

Рабочая программа дисциплины пересмотрена, обсуждена и рекомендована к реализации в образовательном процессе на основании учебного плана ОПОП ВО 09.04.01 Информатика и вычислительная техника, программа «Киберфизические системы и искусственный интеллект», направленность (профиль) «Облачная и сетевая инфраструктура систем искусственного интеллекта», одобренного Ученым советом университета протокол №____«____»_____20___г., на заседании кафедры_____.

(наименование кафедры, дата, номер протокола)

Зав. кафедрой _____

Рабочая программа дисциплины пересмотрена, обсуждена и рекомендована к реализации в образовательном процессе на основании учебного плана ОПОП ВО 09.04.01 Информатика и вычислительная техника, программа «Киберфизические системы и искусственный интеллект», направленность (профиль) «Облачная и сетевая инфраструктура систем искусственного интеллекта», одобренного Ученым советом университета протокол №____«____»_____20___г., на заседании кафедры_____.

(наименование кафедры, дата, номер протокола)

Зав. кафедрой _____

1 Цель и задачи дисциплины. Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения основной профессиональной образовательной программы

1.1 Цель дисциплины

Формирование у студентов знаний и умений связанных с решением задач обеспечения безопасности систем искусственного интеллекта.

1.2 Задачи дисциплины

- изучение способов анализа угроз информационной безопасности систем искусственного интеллекта и основных общеметодологических принципов построения систем обеспечения информационной безопасности;
- получение навыков использования основных методов и средств проектирования систем обеспечения информационной безопасности, методов оценки качества систем и моделей, проведения аттестации защищаемых систем искусственного интеллекта.

1.3 Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения основной профессиональной образовательной программы

Таблица 1.3 – Результаты обучения по дисциплине

Планируемые результаты освоения основной профессиональной образовательной программы (компетенции, закрепленные за дисциплиной)		*Код и наименование индикатора достижения компетенции, закрепленного за дисциплиной*	*Планируемые результаты обучения по дисциплине, соотнесенные с индикаторами достижения компетенций*
код компетенции	*наименование компетенции*		
ПК-8	Способен разрабатывать и модернизировать программное и аппаратное обеспечение технологий и систем искусственного интеллекта с учетом требований информационной безопасности в различных	ПК-8.1 Разрабатывает программное и аппаратное обеспечение технологий и систем искусственного интеллекта для решения профессиональных задач с учетом требований информационной безопасности в различных предметных областях	***Знать:*** новые научные принципы и методы разработки программного и аппаратного обеспечения технологий и систем искусственного интеллекта для решения профессиональных задач в различных предметных областях ***Уметь:*** разрабатывать программное и аппаратное обеспечение технологий и систем искусственного интеллекта ***Владеть (****или* ***Иметь опыт деятельности):*** разработкой программного и аппаратного обеспечения технологий и систем искусственного интеллекта с учетом требований

Планируемые результаты освоения основной профессиональной образовательной программы (компетенции, закрепленные за дисциплиной)		*Код и наименование индикатора достижения компетенции, закрепленного за дисциплиной*	*Планируемые результаты обучения по дисциплине, соотнесенные с индикаторами достижения компетенций*
код компетенции	*наименование компетенции*		
	предметных областях		информационной безопасности для решения профессиональных задач в различных предметных областях
		ПК-8.2 Модернизирует программное и аппаратное обеспечение технологий и систем искусственного интеллекта для решения профессиональных задач с учетом требований информационной безопасности в различных предметных областях	***Знать:*** особенности модернизации программного и аппаратного обеспечения технологий и систем искусственного интеллекта для решения профессиональных задач в различных предметных областях ***Уметь:*** модернизировать программное обеспечение технологий и систем искусственного интеллекта с учетом требований информационной безопасности для решения профессиональных задач в различных предметных областях ***Владеть (****или* ***Иметь опыт деятельности):*** навыками модернизации аппаратного обеспечения технологий и систем искусственного интеллекта с учетом требований информационной безопасности для решения профессиональных задач в различных предметных областях

2 Указание места дисциплины в структуре основной профессиональной образовательной программы

Дисциплина «Безопасность систем искусственного интеллекта» является элективной дисциплиной, входит в часть, формируемую участниками образовательных отношений, основной профессиональной образовательной программы – программы магистратуры 09.04.01 Информатика и вычислительная техника, программа «Киберфизические системы и искусственный интеллект», направленность (профиль) «Облачная и сетевая инфраструктура систем искусственного интеллекта» в Модуль «Сети и центры обработки данных» Комплексного модуля профиля «Облачная и сетевая инфраструктура систем искусственного интеллекта». Дисциплина изучается в 4 семестре на 2 курсе.

3 Объем дисциплины в зачетных единицах с указанием количества академических или астрономических часов, выделенных на контактную работу обучающихся с преподавателем (по видам учебных занятий) и на самостоятельную работу обучающихся

Общая трудоемкость (объем) дисциплины составляет 4 зачетные единицы (з.е.), 144 академических часа.

Таблица 3 – Объем дисциплины

Виды учебной работы	Всего, часов
Общая трудоемкость дисциплины	144
Контактная работа обучающихся с преподавателем по видам учебных занятий (всего)	24,1
в том числе:	
лекции	0
лабораторные занятия	12
практические занятия	12
Самостоятельная работа обучающихся (всего)	119,9
Контроль (подготовка к экзамену)	0
Контактная работа по промежуточной аттестации (всего АттКР)	0,1
в том числе:	
зачет	0,1
зачет с оценкой	не предусмотрен
курсовая работа (проект)	не предусмотрена
экзамен (включая консультацию перед экзаменом)	не предусмотрен

4 Содержание дисциплины, структурированное по темам (разделам) с указанием отведенного на них количества академических часов и видов учебных занятий

4.1 Содержание дисциплины

Таблица 4.1.1 – Содержание дисциплины, структурированное по темам (разделам)

№ п/п	Раздел (тема) дисциплины	Содержание
1	Проблемы информационной безопасности	Методологические основы комплексной системы защиты информации систем искусственного интеллекта. Определение состава защищаемой информации. Политика безопасности
2	Источники, способы и результаты дестабилизирующего воздействия на информацию. Каналы и методы несанкционированн	Модель ISO/OSI и стек протоколов TCP/IP. Проблемы безопасности IP – сетей. Основные виды сетевых атак. Спам. Фишинг и фарминг. Угрозы и уязвимости проводных корпоративных сетей. Угрозы и уязвимости беспроводных сетей. Фрагментарный и комплексный подходы к проблеме обеспечения безопасности информационных систем. Пути решения проблем защиты информации в сетях.

	ого доступа к информации	
3	Моделирование процессов комплексной системы защиты информации. Нормативно-методическое обеспечение систем защиты информации. Управление комплексной системой защиты информации	**Технологии межсетевых экранов** Классификация межсетевых экранов. Функции межсетевых экранов: фильтрация трафика, выполнение функций посредничества. Дополнительные возможности межсетевых экранов: идентификация и аутентификация пользователей, трансляция сетевых адресов, регистрация и анализ событий. Варианты исполнения межсетевых экранов. Особенности функционирования межсетевых экранов на различных уровнях модели OSI. Формирование политики межсетевого взаимодействия. Основные схемы подключения межсетевых экранов. Персональные и распределенные межсетевые экраны. Проблемы безопасности межсетевых экранов. **Технологии защиты от вирусов** Классификация компьютерных вирусов. Загрузочные вирусы. Файловые вирусы. Вирусы-сценарии. Макровирусы. Троянские программы. Черви. Жизненный цикл вирусов. Основные каналы распространения вредоносных программ. Методы обнаружения компьютерных вирусов: обнаружение, основанное на сигнатурах, обнаружение программ подозрительного поведения, метод “белого списка”, обнаружение вирусов при помощи эмуляции работы программы, эвристический анализ. Обзор современных антивирусных программ. Построение системы антивирусной защиты корпоративной сети. **Технологии анализа защищенности и обнаружения сетевых атак** Концепция адаптивного управления безопасностью. Технология анализа защищенности. Средства анализа защищенности сетевых протоколов и сервисов. Средства анализа защищенности операционной системы. Общие требования к выбираемым средствам анализа защищенности. Средства обнаружения сетевых атак. Методы анализа сетевой информации. Классификация систем обнаружения атак. Компоненты и архитектура системы обнаружения атак. Особенности систем обнаружения атак на сетевом и операционном уровнях. Методы реагирования. Обзор современных средств обнаружения атак. **Требования к системам защиты информации** Показатели защищенности средств вычислительной техники от несанкционированного доступа. Классы защищенности автоматизированных систем. Основные требования и рекомендации по защите информации, составляющей служебную или коммерческую тайну, а также персональных данных. Требования к защите информации в автоматизированных системах, локальных вычислительных сетях, на рабочих местах пользователей ПК. Требования к защите информации при работе с системами управления базами данных. Требования к защите информации при взаимодействии абонентов с сетями общего пользования.

Таблица 4.1.2 –Содержание дисциплины и его методическое обеспечение

№ п/п	Раздел (тема) дисциплины	Виды деятельности			Учебно-методические материалы	Формы текущего контроля успеваемости *(по неделям семестра)*	Компетенции
		лек., час	№ лаб.	№ пр.			
1	2	3	4	5	6	7	8
1	Проблемы информационной безопасности		1	1	У-1, 2,4,5, МУ-1,2	С(3)	ПК-8
2	Источники, способы и результаты дестабилизирующего воздействия на информацию. Каналы и методы несанкционированного доступа к информации		2	2	У -1,3,5,7 МУ-1,2	С (7)	ПК-8
3	Моделирование процессов комплексной системы защиты информации. Нормативно-методическое обеспечение систем защиты информации. Управление комплексной системой защиты информации		3	3	У -1-9 МУ-1,2	С,КО (11)	ПК-8

С – собеседование, КО – контрольный опрос.

4.2 Лабораторные работы и (или) практические занятия

4.2.1 Лабораторные работы

Таблица 4.2.1 – Лабораторные работы

№ п/п	Наименование лабораторных работ	Объём, час.
1	Предпроектное обследование. Аналитическое обоснование необходимости создания СЗИ.	4
2	Техническое (частное техническое) задание на разработку СЗИ. Проектирование комплексной системы защиты информации	4
3	Технический проект КСЗИ.	4
Итого:		12

4.2.2 Практические занятия

Таблица 4.2.2 – Практические занятия

№ п/п	Наименование практических занятий	Объём, час.
1	Методологические основы комплексной системы защиты информации систем искусственного интеллекта. Определение состава защищаемой информации	4
2	Источники, способы и результаты дестабилизирующего воздействия на информацию. Каналы и методы несанкционированного доступа к информации	4
3	Моделирование процессов комплексной системы защиты информации. Нормативно-методическое обеспечение систем защиты информации. Управление комплексной системой защиты информации	4
Итого:		12

4.3 Самостоятельная работа студентов (СРС)

Таблица 4.3 – Самостоятельная работа студентов

№ раздела (темы)	Наименование раздела (темы) дисциплины	Срок выполнения	Время, затрачиваемое на выполнение СРС, час.
1	Проблемы информационной безопасности	1-2 недели	20
2	Источники, способы и результаты дестабилизирующего воздействия на информацию. Каналы и методы несанкционированного доступа к информации	3-7 недели	20
3	Моделирование процессов комплексной системы защиты информации. Нормативно-методическое обеспечение систем защиты информации. Управление комплексной системой защиты информации	8-11 недели	20
4	Выполнение контрольной работы	1-11 недели	59,9
Итого			119,9

5 Перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине

Студенты могут при самостоятельном изучении отдельных тем и вопросов дисциплин пользоваться учебно-наглядными пособиями, учебным оборудованием и методическими разработками кафедры в рабочее время, установленное Правилами внутреннего распорядка работников.

Учебно-методическое обеспечение для самостоятельной работы обучающихся по данной дисциплине организуется:

библиотекой университета:

- библиотечный фонд укомплектован учебной, методической, научной, периодической, справочной и художественной литературой в соответствии с УП и данной РПД;
- имеется доступ к основным информационным образовательным ресурсам, информационной базе данных, в том числе библиографической, возможность выхода в Интернет.

кафедрой:

- путем обеспечения доступности всего необходимого учебно-методического и справочного материала;
- путем предоставления сведений о наличии учебно-методической литературы, современных программных средств.
- путем разработки:

– методических рекомендаций, пособий по организации самостоятельной работы студентов;

– тем рефератов;

– вопросов к зачету;

–методических указаний к выполнению лабораторных работ и т.д.

типографией университета:

– помощь авторам в подготовке и издании научной, учебной и методической литературы;

–удовлетворение потребности в тиражировании научной, учебной и методической литературы.

6 Образовательные технологии

Реализация компетентностного подхода предусматривает широкое использование в образовательном процессе активных и интерактивных форм проведения занятий в сочетании с внеаудиторной работой с целью формирования универсальных, общепрофессиональных и профессиональных компетенций обучающихся.

7Фонд оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине

7.1 Перечень компетенций с указанием этапов их формирования в процессе освоения основной профессиональной образовательной программы

Таблица 7.1 – Этапы формирования компетенций

Код и наименование компетенции	Этапы* формирования компетенций и дисциплины (модули), практики, НИР, при изучении которых формируется данная компетенция		
	начальный	основной	завершающий
ПК-8 Способен разрабатывать и модернизировать программное и аппаратное обеспечение технологий и систем искусственного интеллекта с учетом требований информационной безопасности в различных предметных областях	Технологии программирования и инструментальные средства разработки систем искусственного интеллекта, Технологии построения сетей нового поколения	Учебная технологическая (проектно-технологическая) практика	Производственная преддипломная практика, Мобильные и сетевые архитектуры комплексных систем искусственного интеллекта, Безопасность систем искусственного интеллекта, Отказоустойчивые и масштабируемые вычислительные системы, Методы и средства защиты облачной и сетевой инфраструктуры, Технологии широкополосной цифровой связи, Защита информации, Технологии беспроводной связи

7.2 Описание показателей и критериев оценивания компетенций на различных этапах их формирования, описание шкал оценивания

Таблица 7.2 – Показатели и критерии оценивания компетенций, шкала оценивания

Код компетенции/ этап *(указывается название этапа из п.7.1)*	Показатели оценивания компетенций *(индикаторы достижения компетенций, закрепленные за дисциплиной)*	Критерии и шкала оценивания компетенций		
		Пороговый уровень («удовлетворительно)	Продвинутый уровень (хорошо»)	Высокий уровень («отлично»)
ПК-8/ завершающий	ПК-8.1 Разрабатывает программное и аппаратное обеспечение технологий и систем искусственного интеллекта для решения профессиональных задач с учетом требований	***Знать:*** на удовлетворительном уровне новые научные принципы и методы разработки программного и аппаратного обеспечения технологий и систем искусственного интеллекта для решения	***Знать:*** новые научные принципы и методы разработки программного и аппаратного обеспечения технологий и систем искусственного интеллекта для решения профессиональных задач в различных	***Знать:*** на высоком уровне новые научные принципы и методы разработки программного и аппаратного обеспечения технологий и систем искусственного интеллекта для решения

Код компетенции/ этап *(указывается название этапа из п.7.1)*	Показатели оценивания компетенций *(индикаторы достижения компетенций, закрепленные за дисциплиной)*	Критерии и шкала оценивания компетенций		
		Пороговый уровень («удовлетворительно)	Продвинутый уровень (хорошо»)	Высокий уровень («отлично»)
	информационной безопасности в различных предметных областях ПК-8.2 Модернизирует программное и аппаратное обеспечение технологий и систем искусственного интеллекта для решения профессиональных задач с учетом требований информационной безопасности в различных предметных областях	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 ***Уметь:*** под руководством модернизировать программное и аппаратное обеспечение технологий и систем искусственного интеллекта с учетом требований информационной безопасности для решения профессиональных задач в различных предметных областях ***Владеть*** ***(****или* ***Иметь опыт деятельности):*** Первоначальными навыками применения современных технических решений создания объектов и систем связи (телекоммуникационн	предметных областях; особенности модернизации программного и аппаратного обеспечения технологий и систем искусственного интеллекта для решения профессиональных задач в различных предметных областях ***Уметь:*** модернизировать программное и аппаратное обеспечение технологий и систем искусственного интеллекта с учетом требований информационной безопасности ***Владеть*** ***(****или* ***Иметь опыт деятельности):*** навыками применения современных технических решений создания объектов и систем связи (телекоммуникационных систем) и ее компонентов, новейшего оборудования и программного	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 ***Уметь:*** модернизировать программное и аппаратное обеспечение технологий и систем искусственного интеллекта с учетом требований информационной безопасности для решения профессиональных задач в различных предметных областях ***Владеть*** ***(****или* ***Иметь опыт деятельности):*** на высоком уровне навыками применения

Код компетенции/ этап *(указывается название этапа из п.7.1)*	Показатели оценивания компетенций *(индикаторы достижения компетенций, закрепленные за дисциплиной)*	Критерии и шкала оценивания компетенций		
		Пороговый уровень («удовлетворительно)	Продвинутый уровень (хорошо»)	Высокий уровень («отлично»)
		ых систем) и ее компонентов, новейшего оборудования и программного обеспечения для систем искусственного интеллекта	обеспечения для систем искусственного интеллекта	современных технических решений создания объектов и систем связи (телекоммуникационных систем) и ее компонентов, новейшего оборудования и программного обеспечения для систем искусственного интеллекта

7.3 Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций в процессе освоения основной профессиональной образовательной программы

Таблица 7.3 - Паспорт комплекта оценочных средств для текущего контроля успеваемости

№ п/п	Раздел (тема) дисциплины	Код контролируемой компетенции (или ее части)	Технология формирования	Оценочные средства		Описание шкал оценивания
				наименование	№№ заданий	
1	2	3	4	5	6	7
1	Проблемы информационной безопасности	ПК-8	Практическое занятие №1, лабораторная работа №1, СРС	вопросы для собеседования контрольные вопросы к лаб№1	1-10 1-3	Согласно табл.7.2

№ п/п	Раздел (тема) дисциплины	Код контролируемой компетенции (или ее части)	Технология формирования	Оценочные средства		Описание шкал оценивания
				наименование	№№ заданий	
1	2	3	4	5	6	7
2	Источники, способы и результаты дестабилизирующего воздействия на информацию. Каналы и методы несанкционированного доступа к информации	ПК-8	Практическое занятие №2, лабораторная работа №2, СРС	вопросы для собеседования контрольные вопросы к лаб№2	11-30 1-3	Согласно табл.7.2
3	Моделирование процессов комплексной системы защиты информации. Нормативно-методическое обеспечение систем защиты информации. Управление комплексной системой защиты информации	ПК-8	Практическое занятие №3, лабораторная работа №3, СРС, КО	вопросы для собеседования	31-50	Согласно табл.7.2
				контрольные вопросы к лаб№3	1-3	
				контрольный опрос	1-10	

С – собеседование, КО – контрольный опрос.

Контрольные вопросы и задания

Оценочные средства планируемых результатов обучения представлены в виде фондов оценочных средств (ФОС), разработанных в соответствии с локальным нормативным актом университета. В целях освоения компетенций, указанных в рабочей программе дисциплины, предусмотрены следующие вопросы, задания текущего контроля:

ПК-8. Способен разрабатывать и модернизировать программное и аппаратное обеспечение технологий и систем искусственного интеллекта с учетом требований информационной безопасности в различных предметных областях

ПК-8.1. Разрабатывает программное и аппаратное обеспечение технологий и систем искусственного интеллекта для решения профессиональных задач с учетом требований информационной безопасности в различных предметных областях.

Студент должен знать новые научные принципы и методы разработки программного и аппаратного обеспечения технологий и систем искусственного интеллекта для решения профессиональных задач в различных предметных областях

Вопросы, задания:
1. Какие основные принципы обеспечения безопасности систем искусственного интеллекта?
2. На какие направления можно декомпозировать задачу обеспечения безопасности систем искусственного интеллекта?
3. Каковы основные участники процесса обеспечения безопасности систем искусственного интеллекта?
4. Каковы основные стадии процесса обеспечения безопасности систем искусственного интеллекта?
5. Какие группы нормативной документации применяются при обеспечении безопасности систем искусственного интеллекта?

Студент должен уметь разрабатывать программное и аппаратное обеспечение технологий и систем искусственного интеллекта с учетом требований информационной безопасности для решения профессиональных задач в различных предметных областях

Вопросы, задания:
1. Опишите построения системы защиты в рамках разработки программного и аппаратного обеспечения технологий и систем искусственного интеллекта
2. Приведите примеры документов, которые формируются при построении системы защиты в рамках разработки программного и аппаратного обеспечения технологий и систем искусственного интеллекта
3. Какие классы СЗИ применяются при проектировании системы защиты в рамках разработки программного и аппаратного обеспечения технологий и систем искусственного интеллекта?
4. Опишите организационные мероприятия, которые должны применяться при внедрении системы защиты в рамках разработки программного и аппаратного обеспечения технологий и систем искусственного интеллекта.
5. Опишите виды и методы испытаний, которые должны проводиться после внедрения системы защиты в рамках разработки программного и аппаратного обеспечения технологий и систем искусственного интеллекта.

ПК-8.2. Модернизирует программное и аппаратное обеспечение технологий и систем искусственного интеллекта для решения профессиональных задач с учетом требований информационной безопасности в различных предметных областях

Студент должен знать особенности модернизации программного и аппаратного обеспечения технологий и систем искусственного интеллекта для решения профессиональных задач в различных предметных областях

Вопросы, задания:
1. Каков порядок построения системы защиты в рамках модернизации программного и аппаратного обеспечения технологий и систем искусственного интеллекта?
2. Какие основные документы разрабатываются при построении системы защиты?
3. Какие классы СЗИ применяются при проектировании системы защиты в рамках модернизации программного и аппаратного обеспечения технологий и систем искусственного интеллекта?
4. Какой организационные мероприятия должны применяться при внедрении системы защиты?
5. Какие виды и методы испытаний должны проводиться после внедрения системы защиты?

Студент должен уметь модернизировать программное и аппаратное обеспечение технологий и систем искусственного интеллекта с учетом требований информационной безопасности для решения профессиональных задач в различных предметных областях

Вопросы, задания:
1. Приведите примеры требований, которые должны учитываться при выборе средств защиты.
2. Опишите, какие задачи решают и какими возможностями обладают средства защиты информации от несанкционированного доступа.
3. Опишите, какие задачи решают и какими возможностями обладают сетевые средства защиты информации.
4. Опишите, какие задачи решают и какими возможностями обладают криптографические средства защиты информации.
5. Опишите, какие задачи решают и какими возможностями обладают средства антивирусной защиты и анализа защищенности.

На **контрольную работу** студенту выдается индивидуальное задание (по вариантам), заключающееся в выборе и описании технического решения по применению технологии (или нескольких технологий) беспроводной связи в конкретной системе искусственного интеллекта.

Работа выполняется в письменной форме в течение 10 недель с момента выдачи задания. Контрольный срок сдачи – последний месяц семестра.

Примерное содержание контрольной работы

1. Титульный лист.

2. Формулировка варианта задания.
3. Основная часть, включающая:
   - Описание объекта защиты;
   - Определение актуальных угроз безопасности информации;
   - Определение требований к системе защиты;
   - Выбор технических решений системы защиты;
   - Определение необходимого набора организационно-распорядительных документов.

4) Список использованных источников (включая источники Интернет).

Примерный список вариантов контрольной работы:

1. Разработка модели угроз и нарушителя для типовой системы искусственного интеллекта.

2. Разработка технического задания на систему защиты для типовой системы искусственного интеллекта.

3. Разработка ответа о предпроектном обследовании для типовой системы искусственного интеллекта.

4. Разработка технического проекта для типовой системы искусственного интеллекта.

Вопросы промежуточной аттестации

1. Какие основные принципы обеспечения безопасности систем искусственного интеллекта?
2. На какие направления можно декомпозировать задачу обеспечения безопасности систем искусственного интеллекта?
3. Каковы основные участники процесса обеспечения безопасности систем искусственного интеллекта?
4. Каковы основные стадии процесса обеспечения безопасности систем искусственного интеллекта?
5. Какие группы нормативной документации применяются при обеспечении безопасности систем искусственного интеллекта?
6. Каков порядок построения системы защиты в рамках разработки программного и аппаратного обеспечения технологий и систем искусственного интеллекта?
7. Какие основные документы разрабатываются при построении системы защиты в рамках разработки программного и аппаратного обеспечения технологий и систем искусственного интеллекта?
8. Какие классы СЗИ применяются при проектировании системы защиты в рамках разработки программного и аппаратного обеспечения технологий и систем искусственного интеллекта?
9. Какой организационные мероприятия должны применяться при внедрении системы защиты в рамках разработки программного и аппаратного обеспечения технологий и систем искусственного интеллекта?
10. Какие виды и методы испытаний должны проводиться после внедрения системы

защиты в рамках разработки программного и аппаратного обеспечения технологий и систем искусственного интеллекта?
11. Каков порядок построения системы защиты в рамках модернизации программного и аппаратного обеспечения технологий и систем искусственного интеллекта?
12. Какие основные документы разрабатываются при построении системы защиты в рамках модернизации программного и аппаратного обеспечения технологий и систем искусственного интеллекта?
13. Какие классы СЗИ применяются при проектировании системы защиты в рамках модернизации программного и аппаратного обеспечения технологий и систем искусственного интеллекта?
14. Какой организационные мероприятия должны применяться при внедрении системы защиты в рамках модернизации программного и аппаратного обеспечения технологий и систем искусственного интеллекта?
15. Какие виды и методы испытаний должны проводиться после внедрения системы защиты в рамках модернизации программного и аппаратного обеспечения технологий и систем искусственного интеллекта?
16. Какие требования должны учитываться при выборе средств защиты?
17. Какие задачи решают и какими возможностями обладают средства защиты информации от несанкционированного доступа?
18. Какие задачи решают и какими возможностями обладают сетевые средства защиты информации?
19. Какие задачи решают и какими возможностями обладают криптографические средства защиты информации?
20. Какие задачи решают и какими возможностями обладают средства антивирусной защиты и анализа защищенности?

Полностью оценочные материалы и оценочные средства для проведения текущего контроля успеваемости представлены в УММ по дисциплине.

Типовые задания для проведения промежуточной аттестации обучающихся

Промежуточная аттестация по дисциплине проводится в форме зачета. Зачет проводится в виде компьютерного тестирования.

Для тестирования используются контрольно-измерительные материалы (КИМ) – вопросы и задания в тестовой форме, составляющие банк тестовых заданий (БТЗ) по дисциплине, утвержденный в установленном в университете порядке.

Проверяемыми на промежуточной аттестации элементами содержания являются темы дисциплины, указанные в разделе 4 настоящей программы. Все темы дисциплины отражены в КИМ в равных долях (%). БТЗ включает в себя не менее 100 заданий и постоянно пополняется. БТЗ хранится на бумажном носителе в составе УММ и электронном виде в ЭИОС университета.

Для проверки *знаний* используются вопросы и задания в различных формах:

– закрытой (с выбором одного или нескольких правильных ответов),

– открытой (необходимо вписать правильный ответ),
– на установление правильной последовательности,
– на установление соответствия.

Умения, навыки (или опыт деятельности) и компетенции проверяются с помощью компетентностно-ориентированных задач (ситуационных, производственных или кейсового характера) и различного вида конструкторов. Все задачи являются многоходовыми. Некоторые задачи, проверяющие уровень сформированности компетенций, являются многовариантными. Часть умений, навыков и компетенций прямо не отражена в формулировках задач, но они могут быть проявлены обучающимися при их решении.

В каждый вариант КИМ включаются задания по каждому проверяемому элементу содержания во всех перечисленных выше формах и разного уровня сложности. Такой формат КИМ позволяет объективно определить качество освоения обучающимися основных элементов содержания дисциплины и уровень сформированности компетенций.

7.4 Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций

Процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций, регулируются следующими нормативными актами университета:

– положение П 02.016–2018 «О балльно-рейтинговой системе оценивания результатов обучения по дисциплинам (модулям) и практикам при освоении обучающимися образовательных программ»;

– методические указания, используемые в образовательном процессе, указанные в списке литературы.

Для *текущего контроля успеваемости* по дисциплине в рамках действующей в университете балльно-рейтинговой системы применяется следующий порядок начисления баллов:

Таблица 7.4 – Порядок начисления баллов в рамках БРС

Форма контроля	Минимальный балл		Максимальный балл	
	балл	примечание	балл	примечание
1	2	3	4	5
Лабораторные работы №1 - №3	0	Не предоставил отчет	24	Выполнил и защитил
Самостоятельная работа	0	Не участвовал в опросе	12	Доля правильных ответов более 80%
Контрольная работа		Не выполнил	12	Выполнил и защитил
Итого	0		48	

Форма контроля	Минимальный балл		Максимальный балл	
	балл	примечание	балл	примечание
1	2	3	4	5
Посещаемость	0	Не посещал занятия	16	Посещал все занятия
Зачет	0		36	Доля правильных ответов более 80%
Итого	0		100	

Для промежуточной аттестации обучающихся, проводимой в виде тестирования, используется следующая методика оценивания знаний, умений, навыков и (или) опыта деятельности. В каждом варианте КИМ –16 заданий (15 вопросов и одна задача).

Каждый верный ответ оценивается следующим образом:

- задание в закрытой форме –2балла,
- задание в открытой форме – 2 балла,
- задание на установление правильной последовательности – 2 балла,
- задание на установление соответствия – 2 балла,
- решение компетентностно-ориентированной задачи – 6 баллов.

Максимальное количество баллов за тестирование –36 баллов.

8 Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины

8.1 Основная учебная литература

1. Мирошников, А. И. Основы информационной безопасности и защита информации : учебное пособие / А. И. Мирошников, А. С. Сысоев. — Липецк : Липецкий государственный технический университет, ЭБС АСВ, 2022. — 107 с. — ISBN 978-5-00175-160-1. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: https://www.iprbookshop.ru/128718.html (дата обращения: 12.03.2023). — Режим доступа: для авторизир. пользователей

2. Загинайлов, Ю. Н. Теория информационной безопасности и методология защиты информации : учебное пособие / Ю. Н. Загинайлов. - Москва ; Берлин : Директ-Медиа, 2015. - 253 с. - URL: http://biblioclub.ru/index.php?page=book&id=276557 (дата обращения 31.08.2021) . - Режим доступа: по подписке. - Текст : электронный.

3. Галатенко, В. А. Основы информационной безопасности : учебное пособие / В. А. Галатенко. — 3-е изд. — Москва : Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2020. — 266 с. — ISBN 978-5-4497-0675-1. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: https://www.iprbookshop.ru/97562.html (дата обращения: 22.11.2023). — Режим доступа: для авторизир. пользователей

4. Методологические основы построения защищенных автоматизированных систем : учебное пособие / А. В. Душкин, О. В. Ланкин, С. В. Потехецкий [и др.]. – Воронеж: ВГУИТ, 2013. - 258 с. - URL: http://biblioclub.ru/index.php?page=book&id=255851 (дата обращения 04.03.2022) . - Режим доступа: по подписке. - Текст : электронный.

8.2 Дополнительная учебная литература

5. Грибунин, В. Г. Комплексная система защиты информации на предприятии : учебное пособие / В. Г. Грибунин, В. В. Чудовский. – М.: Академия, 2009. - 416 с. - Текст : непосредственный.

6. Мельников, В. П. Информационная безопасность и защита информации : учебное пособие / В. П. Мельников, С. А. Клейменов, А. М. Петраков. – М. : Академия, 2006. – 336 с. - Текст : непосредственный.

7. Пархимович, М. Н. Основы интернет-технологий : учебное пособие / М. Н. Пархимович, А. А. Липницкий, В. А. Некрасова - Архангельск : ИПЦ САФУ, 2013. - 366 с. - URL: http://biblioclub.ru/index.php?page=book&id=436379 (дата обращения 01.09.2021) . - Режим доступа: по подписке. - Текст : электронный.

8. Громов, Ю. Ю. Основы Web-инжиниринга: разработка клиентских приложений : учебное пособие / Ю. Ю. Громов, О. Г. Иванова, С. В. Данилкин . - Тамбов :Изд -во ФГБОУ ВПО «ТГТУ», 2012. - 240 с. - URL: http://biblioclub.ru/index.php?page=book&id=277648 (дата обращения 04.03.2022) . - Режим доступа: по подписке. - Текст : электронный.

9. Безбогов, А. А. Методы и средства защиты компьютерной информации : учебное пособие / А. А. Безбогов, А. Я. Яковлев, В. Н. Шамкин. - Тамбов : ТГТУ, 2006. - 196 с. - URL: http://window.edu.ru/resource/546/38546 (дата обращения 31.08.2021) . - Режим доступа: по подписке. - Текст : электронный.

8.3 Перечень методических указаний

1. Безопасность систем искусственного интеллекта : учеб. пособие / Д.В. Быков; ВолгГТУ. – Волгоград, 2021. – 35 с.

2. Безопасность систем искусственного интеллекта : методические указания по выполнению самостоятельной работы для студентов направления подготовки 09.04.01 / Юго-Зап. гос. ун-т ; сост. И. Е. Чернецкая. - Электрон. текстовые дан. (316 КБ). - Курск : ЮЗГУ, 2022. - 13 с.

8.4 Другие учебно-методические материалы

1. «Защита информации. Инсайд» [Текст] : информ.-метод. журн./ учредитель ООО "Издательский дом "Афина". - Санкт- Петербург : Афина. - Выходит раз в два месяца
2. Журнал «InformationSecurity/Информационная безопасность.» - http://window.edu.ru/

3. Журнал «Проблемы информационной безопасности. Компью терные системы» - http://window.edu.ru/
4. Журнал «Вестник УрФО. Безопасность в информационной сфере»
5. Журнал «Вопросы защиты информации»
6. Журнал «БДИ (Безопасность. Достоверность. Информация.)»
7. Журнал «Информация и безопасность.»

9 Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины

1. http://school-collection.edu.ru/ - федеральное хранилище Единая коллекция цифровых образовательных ресурсов.
2. http://www.edu.ru/ - федеральный портал Российское образование.
3. www.edu.ru – сайт Министерства образования РФ.
4. http://elibrary.ru/defaultx.asp - научная электронная библиотека «Elibrary».
5. http://fictionbook.ru – электронная библиотека.
6. http://www.rsl.ru/ - Российская Государственная Библиотека.
7. http://e.lanbook.com/ - Электронно-библиотечная «Лань» учебной литературы, периодических изданий по естественным, техническим и гуманитарным наукам.
8. http://www.iqlib.ru - Электронно-библиотечная образовательных и просветительных изданий.
9. http://window.edu.ru/ - Электронная библиотека «Единое окно доступа к образовательным ресурсам».
10. Национальный Открытый Университет «ИНТУИТ» [Электронный ресурс] – Режим доступа: www.intuit.ru.
11. http://www.fsb.ru - Федеральная служба безопасности [официальный сайт].
12. http://fstec.ru - Федеральная служба по техническому и экспортному контролю [официальный сайт].
13. http://microsoft.com - Корпорация Microsoft [официальный сайт].
14. http://www.consultant.ru Компания «Консультант Плюс» [официальный сайт].

10 Методические указания для обучающихся по освоению дисциплины

Основными видами аудиторной работы студента при изучении дисциплины «Безопасность систем искусственного интеллекта» являются практические и лабораторные занятия. Студент не имеет права пропускать занятия без уважительных причин.

В процессе обучения используются активные формы работы со студентами: работа на практических занятиях, привлечение студентов к творческому процессу на практических занятиях, промежуточный контроль путем отработки студентами пропущенных занятий, участие в групповых и индивидуальных консультациях (собеседовании). Эти формы способствуют выработке у студентов умения работать с

учебником и литературой. Изучение литературы составляет значительную часть самостоятельной работы студента. Это большой труд, требующий усилий и желания студента. В самом начале работы над книгой важно определить цель и направление этой работы. Прочитанное следует закрепить в памяти. Одним из приемов закрепление освоенного материала является конспектирование, без которого немыслима серьезная работа над литературой. Систематическое конспектирование помогает научиться правильно, кратко и четко излагать своими словами прочитанный материал.

Содержание дисциплины изучается на практических занятиях и лабораторных работах, порядок проведения которых излагается в соответствующих планах и методических указаниях, а также в процессе самостоятельной работы обучаемых в объеме отведенного времени для подготовки к выполнению заданий лабораторных работ и промежуточному контролю.

Лабораторные работы необходимы для контроля преподавателем подготовленности студентов; исследования возможностей изучаемых систем и сетей мобильной связи; закрепления изученного материала; развития умений и навыков подготовки докладов, сообщений по заданной тематике; приобретения опыта устных публичных выступлений, ведения дискуссии, в том числе аргументации и защиты выдвигаемых положений и тезисов.

На лабораторных занятиях детально изучаются вопросы, указанные в программе. Лабораторным занятиям предшествует самостоятельная работа студентов, связанная с освоением лекционного материала и материалов, изложенных в учебниках и учебных пособиях, а также литературе, рекомендованной преподавателем.

Самостоятельная работа – это работа студентов по освоению определенной темы курса, которая предполагает: изучение лекционного материала, учебников и учебных пособий, первоисточников, выполнение дополнительных заданий преподавателя. Также предполагает решение тестовых заданий с последующей самопроверкой, осуществляемой путём поиска ответов на тестовые вопросы в учебной и иной литературе. Такая деятельность позволяет выявить и восполнить пробелы в понимании материала, лучше подготовиться к итоговой аттестации.

Перед практическими занятиями следует повторить материал предыдущего занятия. Это поможет в усвоении нового материала, позволит быть готовыми к экспресс-опросу на практическом занятии. Систематическое повторение отнимает незначительное время и существенно экономит его при подготовке к занятиям и зачету. При повторении изученного материала рекомендуется просматривать основную литературу по данному курсу, в которой материал рассматривается в более широком аспекте. Рекомендуемое время на подготовку к занятиям – не более 30 мин.

Перед лабораторной работой следует ознакомиться с методическими рекомендациями по выполнению лабораторной работы. Это позволит быстро выполнить эту работу. Оформление отчета следует выполнять дома. В процессе оформления необходимо прочитать теоретический материал, приведенный в методических указаниях или в учебнике. Сдавать работу следует сразу по ее

оформлению, не затягивая и не накапливая долги. Рекомендуемое время на оформление отчета – 1час.

Контрольная работа представляет собой законченную работу, заключающуюся в выборе и описании технического решения по применению технологии (или нескольких технологий) беспроводной связи в конкретной системе искусственного интеллекта.

Для успешной подготовки к зачету необходимо иметь конспект. Подготовка по основной и дополнительной литературе, где материал дан в значительно большем объеме, потребует от студента существенных временных затрат. Целесообразно эту литературу использовать для уточнения неясных вопросов и углубленного изучения материала.

Самостоятельная работа студентов включает в себя изучение материалов дисциплины по учебникам, выполнение домашних заданий, оформление отчетов по лабораторным работам и практическим занятиям, а также подготовку к зачету. Вся эта работа планируется самим студентом по рекомендациям преподавателя.

Студенты, не имеющие опыта и считающие, что можно работать без плана, запускают занятия и, будучи не в состоянии нагнать пропущенное, перестают понимать материал, не справляются с решением задач на лабораторных и практических занятиях.

Оценка результативности самостоятельной работы студентов обеспечивается контрольными опросами и собеседованиями со студентами и проверкой выполнения заданий по преподавателя.

Наилучшего результата достигают те студенты, которые предварительно знакомятся с материалом по теме предстоящих занятий. Благодаря этому студенты будут осознанно и критически относиться к изложению лекции и воспримут ее с большим “коэффициентом полезного действия”.

11 Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине, включая перечень программного обеспечения и информационных справочных систем (при необходимости)

При проведении аудиторных занятий используются следующие информационные технологии:

- Программа анализа и управления информационными рисками “Гриф”.(свободное ПО).
- Программа хранения паролей Password Commander(свободное ПО).
- Фаервол Comodo Firewall (свободное ПО).
- Программа анализа защищенности операционной системы GFI LANguard Network Security Scanner.
- Microsoft Office 2016.Лицензионный договор №S0000000722 от 21.12.2015 г. с ООО «АйТи46», лицензионный договор №K0000000117 от 21.12.2015 г. с ООО «СМСКанал»,

– Kaspersky Endpoint Security Russian Edition, лицензия 156A-140624-192234,

– Windows 7, договор IT000012385.

12 Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине

Стандартно оборудованные лекционные аудитории и аудитории для проведения занятий семинарского типа.

Компьютерный класс оснащенный

ПК ВаРИАНт PD2160/I C33/2*512 Mb/HDD 160Gb/DVD-ROM/FDD/ATX 350W/Km/WXP/DFF/17’TFTE 700

или

интерактивная панель JeminiCo. JQ75MW с ОПС модулем и мобильной стойкой; компьютер в сборе (ТИП-2)

или

рабочая станция Core 2 Duo 1863/2*DDR2 1024 Mb/2*HDD 200G/SVGA/DVD-RW/20’LCD*2/Secret Net; ПЭВМ INTEL Gore i3-7100/H110M-R C/SI White Box LGA1151.mATX/8GB/1TB/DVDRW/LCD 21.5”/k+m/

в зависимости от предоставленной аудитории.

13 Особенности реализации дисциплины для инвалидов и лиц с ограниченными возможностями здоровья

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 такжесурдопереводчиков 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).

14Лист дополнений и изменений, внесенных в рабочую программу дисциплины

Номер изменения	Номера страниц				Всего страниц	Дата	Основание для изменения и подпись лица, проводившего изменения
	изме-ненных	замененных	аннулированных	новых			

МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное образовательное учреждение высшего образования
«Волгоградский государственный технический университет»

Факультет электроники и вычислительной техники

МОДУЛЬ "СЕТИ И ЦЕНТРЫ ОБРАБОТКИ ДАННЫХ"
Безопасность систем искусственного интеллекта

рабочая программа дисциплины (модуля, практики)

Закреплена за кафедрой **Электронно-вычислительные машины и системы**

Учебный план Направление 09.04.01 Информатика и вычислительная техника
Программа "Киберфизические системы и искусственный интеллект"

Профиль **Облачная и сетевая инфраструктура систем искусственного интеллекта**

Квалификация **Магистр**

Срок обучения **2**

Форма обучения **очная**

Виды контроля в семестрах: зачеты 4

Семестр(Курс.Номер семестра на курсе)	4(2.2)		Итого	
	УП	ПП	УП	ПП
Практические	12	12	12	12
Лабораторные	12	12	12	12
Итого ауд.	24	24	24	24
Контактная работа	24,25	24,25	24,25	24,25
Сам. работа	119,75	119,75	119,75	119,75
Часы на контроль	0	0	0	0
Практическая подготовка	0	0	0	0
Итого трудоемкость в часах	144	144	0	0

ЛИСТ ОДОБРЕНИЯ И СОГЛАСОВАНИЯ РАБОЧЕЙ ПРОГРАММЫ

Разработчик(и) программы:

доцент Быков Дмитрий Владимирович ктн

Рецензент(ы):
(при наличии)
_____

Рабочая программа дисциплины (модуля, практики)
Безопасность систем искусственного интеллекта

разработана в соответствии с ФГОС ВО:

Федеральный государственный образовательный стандарт высшего образования - магистратура по направлению подготовки 09.04.01 Информатика и вычислительная техника (приказ Минобрнауки России от 19.09.2017 г. № 918)

составлена на основании учебного плана:

Направление 09.04.01 Информатика и вычислительная техника
Программа "Киберфизические системы и искусственный интеллект"

Профиль: Облачная и сетевая инфраструктура систем искусственного интеллекта

утвержденного учёным советом вуза от 29.09.2021 протокол № 2.

Рабочая программа одобрена на заседании кафедры
Электронно-вычислительные машины и системы

Протокол от 16 сентября 2021 г. № 2

Зав. кафедрой Андреев Андрей Евгеньевич

СОГЛАСОВАНО:

Председатель НМС _____ / Авдеюк О.А. /

Протокол заседания НМС от 27 сентября 2021 г. № 2

ЛИСТ АКТУАЛИЗАЦИИ РАБОЧЕЙ ПРОГРАММЫ

№ п/п	Виды дополнений и изменений (или иная информация)	Дата и номер протокола заседания кафедры	Визирование актуализации РПД председателем НМС факультета
1.		Рабочая программа пересмотрена, обсуждена и одобрена для исполнения в 2022-2023 учебном году на заседании кафедры Электронно-вычислительные машины и системы Протокол от __ _____ 2022 г. № __ Зав. кафедрой Андреев Андрей Евгеньевич _____	Председатель НМС _____/_____/ Протокол заседания НМС от __ _____ 2022 г. №__
2.		Рабочая программа пересмотрена, обсуждена и одобрена для исполнения в 2023-2024 учебном году на заседании кафедры Электронно-вычислительные машины и системы Протокол от __ _____ 2023 г. № __ Зав. кафедрой Андреев Андрей Евгеньевич _____	Председатель НМС _____/_____/ Протокол заседания НМС от __ _____ 2023 г. №__
3.		Рабочая программа пересмотрена, обсуждена и одобрена для исполнения в 2024-2025 учебном году на заседании кафедры Электронно-вычислительные машины и системы Протокол от __ _____ 2024 г. № __ Зав. кафедрой Андреев Андрей Евгеньевич _____	Председатель НМС _____/_____/ Протокол заседания НМС от __ _____ 2024 г. №__

1. ЦЕЛИ И ЗАДАЧИ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ, ПРАКТИКИ). ВИД, ТИП ПРАКТИКИ, СПОСОБ И ФОРМА (ФОРМЫ) ЕЕ ПРОВЕДЕНИЯ.
Формирование у студентов знаний и умений связанных с решением задач обеспечения безопасности систем искусственного интеллекта
- изучение способов анализа угроз информационной безопасности систем искусственного интеллекта и основных общеметодологических принципов построения систем обеспечения информационной безопасности;
- получение навыков использования основных методов и средств проектирования систем обеспечения информационной безопасности, методов оценки качества систем и моделей, проведения аттестации защищаемых систем искусственного интеллекта.

2. МЕСТО ДИСЦИПЛИНЫ (МОДУЛЯ, ПРАКТИКИ) В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ		
Цикл (раздел) ОП:		К.М.01.ДВ.01.01
2.1	**Требования к предварительной подготовке обучающегося:**	
2.1.1	Методы и средства защиты облачной и сетевой инфраструктуры	
2.1.2	Методы и средства защиты облачной и сетевой инфраструктуры	
2.1.3	Администрирование операционных систем	
2.2	**Дисциплины (модули) и практики, для которых освоение данной дисциплины (модуля) необходимо как предшествующее:**	
2.2.1	Производственная практика: Преддипломная практика	
2.2.2	Выполнение и защита выпускной квалификационной работы	
2.2.3	Отказоустойчивые и масштабируемые вычислительные системы	

3. КОМПЕТЕНЦИИ ОБУЧАЮЩЕГОСЯ, ФОРМИРУЕМЫЕ В РЕЗУЛЬТАТЕ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ, ПРАКТИКИ)
ПК-6: Способен руководить проектами по созданию комплексных систем на основе аналитики больших данных в различных отраслях
ПК-6.3: Проводит планирование, управление, развертывание, аудит безопасности и защиты персональных данных при работе с большими данными и руководит операционной деятельностью, связанной с безопасностью и защитой персональных данных при работе с большими данными
Результаты обучения: ПК-6.3. З-1. Знает терминологию и последовательность мероприятий по безопасности и защите персональных данных при работе с большими данными ПК-6.3. У-1. Умеет проводить подготовку и планирование действий по верхнеуровневому управлению безопасностью и защитой персональных данных при работе с большими данными ПК-6.3. У-2. Умеет проводить мониторинг, оценку и контроль действий по верхнеуровневому управлению безопасностью и защитой персональных данных при работе с большими данными ПК-6.3. У-3. Умеет определять цели верхнеуровневого управления безопасностью и защитой персональных данных при работе с большими данными
ПК-8: Способен разрабатывать и модернизировать программное и аппаратное обеспечение технологий и систем искусственного интеллекта с учетом требований информационной безопасности в различных предметных областях
ПК-8.1: Разрабатывает программное и аппаратное обеспечение технологий и систем искусственного интеллекта для решения профессиональных задач с учетом требований информационной безопасности в различных предметных областях
Результаты обучения: ПК-8.1. З-1. Знает новые научные принципы и методы разработки программного и аппаратного обеспечения технологий и систем искусственного интеллекта для решения профессиональных задач в различных предметных областях ПК-8.1. У-1. Умеет разрабатывать программное и аппаратное обеспечение технологий и систем искусственного интеллекта с учетом требований информационной безопасности для решения профессиональных задач в различных предметных областях
ПК-8.2: Модернизирует программное и аппаратное обеспечение технологий и систем искусственного интеллекта для решения профессиональных задач с учетом требований информационной безопасности в различных предметных областях
Результаты обучения: ПК-8.2. З-1. Знает особенности модернизации программного и аппаратного обеспечения технологий и систем искусственного интеллекта для решения профессиональных задач в различных предметных областях ПК-8.2. У-1. Умеет модернизировать программное и аппаратное обеспечение технологий и систем искусственного интеллекта с учетом требований информационной безопасности для решения профессиональных задач в различных предметных областях

4. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ, ПРАКТИКИ)

Код занятия	Наименование разделов и тем /вид занятия/	Семестр / Курс	Часов	Форма контроля
1	**Раздел 1. Обучение**			
1.1	Безопасность систем искусственного интеллекта /Тема/	4	0	

1.1.1	Методологические основы комплексной системы защиты информации систем искусственного интеллекта. Определение состава защищаемой информации. /Пр/	4	4	К, З
1.1.2	Источники, способы и результаты дестабилизирующего воздействия на информацию. Каналы и методы несанкционированного доступа к информации. /Пр/	4	4	К, З
1.1.3	Моделирование процессов комплексной системы защиты информации. Нормативно-методическое обеспечение систем защиты информации. Управление комплексной системой защиты информации. /Пр/	4	4	К, З
1.1.4	Предпроектное обследование. Аналитическое обоснование необходимости создания СЗИ. /Лаб/	4	4	Ко, К
1.1.5	Техническое (частное техническое) задание на разработку СЗИ. Проектирование комплексной системы защиты информации. /Лаб/	4	4	Ко, К
1.1.6	Технический проект КСЗИ. Политика информационной безопасности. /Лаб/	4	4	Ко, К
2	**Раздел 2. Самостоятельная работа студентов**			
2.1	в том числе /Тема/	4	0	
2.1.1	Подготовка к отчету лабораторных работ и практическим занятиям /Ср/	4	60	
2.1.2	Выполнение контрольной работы /Ср/	4	59,75	
3	**Раздел 3. Промежуточная аттестация**			
3.1	в том числе /Тема/	4	0	
3.1.1	/Зачет/ /Зачёт/	4	0	З
3.1.2	Контактная работа с ППС /КоРа/	4	0,25	З

Примечание. Формы контроля: Эк – экзамен, К- контрольная работа, Ко- контрольный опрос, Сз- семестровое задание, З-зачет, ОП- отчет по практике.

5. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

Оценочные средства планируемых результатов обучения представлены в виде фондов оценочных средств (ФОС), разработанных в соответствии с локальным нормативным актом университета. ФОС может быть представлен в Приложении к рабочей программе.

ПК-8: Способен разрабатывать и модернизировать программное и аппаратное обеспечение технологий и систем искусственного интеллекта с учетом требований информационной безопасности в различных предметных областях

ПК-8.1: Разрабатывает программное и аппаратное обеспечение технологий и систем искусственного интеллекта для решения профессиональных задач с учетом требований информационной безопасности в различных предметных областях

Студент должен знать новые научные принципы и методы разработки программного и аппаратного обеспечения технологий и систем искусственного интеллекта для решения профессиональных задач в различных предметных областях

Вопросы, задания:
1. Какие основные принципы обеспечения безопасности систем искусственного интеллекта?
2. На какие направления можно декомпозировать задачу обеспечения безопасности систем искусственного интеллекта?
3. Каковы основные участники процесса обеспечения безопасности систем искусственного интеллекта?
4. Каковы основные стадии процесса обеспечения безопасности систем искусственного интеллекта?
5. Какие группы нормативной документации применяются при обеспечении безопасности систем искусственного интеллекта?

Студент должен уметь разрабатывать программное и аппаратное обеспечение технологий и систем искусственного интеллекта с учетом требований информационной безопасности для решения профессиональных задач в различных предметных областях

Вопросы, задания:
1. Опишите построения системы защиты в рамках разработки программного и аппаратного обеспечения технологий и систем искусственного интеллекта
2. Приведите примеры документов, которые формируются при построении системы защиты в рамках разработки программного и аппаратного обеспечения технологий и систем искусственного интеллекта
3. Какие классы СЗИ применяются при проектировании системы защиты в рамках разработки программного и аппаратного обеспечения технологий и систем искусственного интеллекта?
4. Опишите организационные мероприятия, которые должны применяться при внедрении системы защиты в рамках разработки программного и аппаратного обеспечения технологий и систем искусственного интеллекта
5. Опишите виды и методы испытаний, которые должны проводиться после внедрения системы защиты в рамках разработки программного и аппаратного обеспечения технологий и систем искусственного интеллекта

ПК-8.2: Модернизирует программное и аппаратное обеспечение технологий и систем искусственного интеллекта для решения профессиональных задач с учетом требований информационной безопасности в различных предметных областях

Студент должен знать особенности модернизации программного и аппаратного обеспечения технологий и систем искусственного интеллекта для решения профессиональных задач в различных предметных областях

Вопросы, задания:
1. Каков порядок построения системы защиты в рамках модернизации программного и аппаратного обеспечения технологий и систем искусственного интеллекта?
2. Какие основные документы разрабатываются при построении системы защиты?
3. Какие классы СЗИ применяются при проектировании системы защиты в рамках модернизации программного и аппаратного обеспечения технологий и систем искусственного интеллекта?
4. Какой организационные мероприятия должны применяться при внедрении системы защиты?
5. Какие виды и методы испытаний должны проводиться после внедрения системы защиты?

Студент должен уметь модернизировать программное и аппаратное обеспечение технологий и систем искусственного интеллекта с учетом требований информационной безопасности для решения профессиональных задач в различных предметных областях

Вопросы, задания:
1. Приведите примеры требований, которые должны учитываться при выборе средств защиты
2. Опишите, какие задачи решают и какими возможностями обладают средства защиты информации от несанкционированного доступа
3. Опишите, какие задачи решают и какими возможностями обладают сетевые средства защиты информации
4. Опишите, какие задачи решают и какими возможностями обладают криптографические средства защиты информации
5. Опишите, какие задачи решают и какими возможностями обладают средства антивирусной защиты и анализа защищенности

ПК-6: Способен руководить проектами по созданию комплексных систем на основе аналитики больших данных в различных отраслях

ПК-6.3: Проводит планирование, управление, развертывание, аудит безопасности и защиты персональных данных при работе с большими данными и руководит операционной деятельностью, связанной с безопасностью и защитой персональных данных при работе с большими данными

Студент должен знать терминологию и последовательность мероприятий по безопасности и защите персональных данных при работе с большими данными

Вопросы, задания:
1. Какова нормативная база в вопросах защиты ПДн?
2. Каков основной порядок проведения мероприятий по защите ПДн?
3. Каков порядок определения уровня защищенности ИСПДн?
4. Каковы основные требования к обеспечению ИБ ПДн?
5. Какие основные организационные мероприятия должны быть проведены при защите ПДн?

Студент должен уметь проводить подготовку и планирование действий по верхнеуровневому управлению безопасностью и защитой персональных данных при работе с большими данными, проводить мониторинг, оценку и контроль действий по верхнеуровневому управлению безопасностью и защитой персональных данных при работе с большими данными, определять цели верхнеуровневого управления безопасностью и защитой персональных данных при работе с большими данными

Вопросы, задания:
1. Опишите основные шаги при моделировании угроз ПДн
2. Опишите порядок выбора мер защиты ПДн исходя из состава актуальных угроз и уровня защищенности ИСПДн
3. Опишите, порядок выбора мер защиты для ИСПДн
4. Опишите последовательность утверждения внутренней ОРД в области безопасности ПДн
5. Опишите порядок осуществления периодического контроля состояния защищенности ПДн

6. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ, ПРАКТИКИ)

6.1. Рекомендуемая литература

	Авторы, составители	Заглавие	Издательство, год.	Электронный адрес

	Авторы, составители	Заглавие	Издательство, год.	Электронный адрес
Л.1	Лукьянов В. С., Черковский И. В., Скакунов А. В., Быков Д. В.	Модели компьютерных сетей с удостоверяющими центрами: монография	Волгоград: ВолгГТУ, 2009	
Л.2	Лукьянов В. С., Андреев А. Е., Жариков Д. Н., Островский А. А., Гаевой С. В.	Имитационное моделирование грид-систем: монография	Волгоград: ВолгГТУ, 2012	
Л.3	Лукьянов В. С., Быков Д. В.	Методы обеспечения безопасности в сетях с публичными ключами: учеб. пособие	Волгоград: ВолгГТУ, 2015	
Л.4	Олифер В. Г., Олифер Н. А.	Компьютерные сети. Принципы, технологии, протоколы: учеб. пособие для студ. вузов	СПб.: Питер, 2004	
Л.5	Остроух А. В., Николаев А. Б.	Интеллектуальные информационные системы и технологии: монография	Санкт-Петербург: Лань, 2019	
Л.6	Нестеров С. А.	Основы информационной безопасности: учеб. пособие	Санкт-Петербург: Лань, 2018	
Л.7	Бизяев А. А., Куратов К. А.	Сети связи и системы коммутации: учебное пособие	Новосибирск: НГТУ, 2016	https://e.lanbook.com/book/118257
Л.8	Ли П., Райтман М. А.	Архитектура интернета вещей	Москва: ДМК Пресс, 2019	https://e.lanbook.com/reader/book/112923/#5
Л.9	Эделман Дж., Лоу С. С., Осуолт М.	Автоматизация программируемых сетей	Москва: ДМК Пресс, 2019	https://e.lanbook.com/reader/book/123708/#2

6.2. Перечень ресурсов информационно-телекоммуникационной сети "Интернет"

Э1	Кутузов, О. И. Инфокоммуникационные системы и сети : учебник для вузов / О. И. Кутузов, Т. М. Татарникова, В. В. Цехановский. — 2-е изд., стер. — Санкт-Петербург : Лань, 2021. — 244 с. — ISBN 978-5-8114-8051-7. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/171410 (дата обращения: 18.09.2021). — Режим доступа: для авториз. пользователей.
Э2	Журавлев, А. Е. Инфокоммуникационные системы. Аппаратное обеспечение : учебник для вузов / А. Е. Журавлев, А. В. Макшанов, А. В. Иванищев. — 2-е изд., стер. — Санкт-Петербург : Лань, 2021. — 392 с. — ISBN 978-5-8114-8514-7. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/176657 (дата обращения: 18.09.2021). — Режим доступа: для авториз. пользователей.
Э3	Журавлев, А. Е. Инфокоммуникационные системы. Программное обеспечение : учебник для вузов / А. Е. Журавлев, А. В. Макшанов, А. В. Иванищев. — 2-е изд., стер. — Санкт-Петербург : Лань, 2021. — 376 с. — ISBN 978-5-8114-8515-4. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/176658 (дата обращения: 18.09.2021). — Режим доступа: для авториз. пользователей.
Э4	Лукша, М. Kubernetes в действии / М. Лукша ; перевод с английского А. В. Логунов. — Москва : ДМК Пресс, 2019. — 672 с. — ISBN 978-5-97060-657-5. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/131688 (дата обращения: 18.09.2021). — Режим доступа: для авториз. пользователей.
Э5	Кутузов, О. И. Инфокоммуникационные системы и сети : учебник для вузов / О. И. Кутузов, Т. М. Татарникова, В. В. Цехановский. — 2-е изд., стер. — Санкт-Петербург : Лань, 2021. — 244 с. — ISBN 978-5-8114-8051-7. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/171410 (дата обращения: 18.09.2021). — Режим доступа: для авториз. пользователей.
Э6	Федеральный портал «Российское образование» [Электронный ресурс] – Режим доступа: www.edu.ru
Э7	Национальный Открытый Университет «ИНТУИТ» [Электронный ресурс] – Режим доступа: www.intuit.ru
Э8	Нестеров, С. А. Основы информационной безопасности : учебник для вузов / С. А. Нестеров. — Санкт-Петербург : Лань, 2021. — 324 с. — ISBN 978-5-8114-6738-9. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/165837 (дата обращения: 09.09.2021). — Режим доступа: для авториз. пользователей.
Э9	Защита информации в центрах обработки данных : учебно-методическое пособие / И. А. Ушаков, В. А. Десницкий, А. А. Чечулин, Т. Е. Захарова. — Санкт-Петербург : СПбГУТ им. М.А. Бонч-Бруевича, 2019. — 44 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/180094 (дата обращения: 09.09.2021). — Режим доступа: для авториз. пользователей.
Э10	Документация по технической защите конфиденциальной информации [Электронный ресурс] – Режим доступа : https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty (дата обращения: 18.09.2021)

6.3 Перечень программного обеспечения

6.3.1.1	OpenOffice, LibreOffice – офисные пакеты
6.3.1.2	Microsoft Visual Studio Community – среда разработки
6.3.1.3	Яндекс.Браузер - веб-браузер.

6.4 Перечень информационных справочных систем

6.3.2.1	Библиотека (НТБ), http://library.vstu.ru/sci-nci

6.3.2.2	Электронная информационно-образовательная среда университета, http://eos2.vstu.ru
6.3.2.3	ЭБС "Лань", https://e.lanbook.com/
6.3.2.4	ЭБС "Book.ru", https://www.book.ru/
6.3.2.5	Электронная библиотека "Grebennikon", https://grebennikon.ru/
6.3.2.6	Библиографическая и реферативная база данных статей, опубликованных в научных изданиях “Scopus”,
6.3.2.7	https://www.scopus.com/
6.3.2.8	Российская научная электронная библиотека, интегрированная с РИНЦ “eLIBRARY.ru”, https://www.elibrary.ru/
6.3.2.9	Поисковая интернет-платформа, объединяющая реферативные базы данных публикаций в научных журналах и
6.3.2.10	патентов “Web of Science”, https://webofknowledge.com/

7. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ, ПРАКТИКИ) /ОБОРУДОВАНИЕ	
7.1	1. Лаборатория сетевых технологий / Мультимедийный класс для проведения занятий лекционного и семинарского
7.2	типа, лабораторных занятий
7.3	1) ПЭВМ Intel DualCore 2ГГц / 2Гб RAM / LCD 19" - 8 шт.; 2) экран EliteScreens; 3) проектор Acer 1200; 4) Коммутаторы CISCO
7.4	2. Учебная лаборатория / комьютерный класс
7.5	1) Ноутбуки HP Elitebook 8460p – 4 шт., 2) Ноутбуки HP EliteBook 8570p - 4 шт. 3) Ноутбук Lenovo ThinkPad T420 – 4 шт. 4) экран EliteScreens; 5) проектор Acer 1203;
7.6	6) доступ в Интернет и к наукометрическим базам данных
7.7	3. Аудитория для самостоятельной работы обучающихся./Учебная мебель, компьютерная техника с возможностью
7.8	подключения к сети "Интернет" и обеспечением доступа в электронную информационно-образовательную среду
7.9	университета (читальный зал информационно-библиотечного центра)

8. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ (МОДУЛЯ, ПРАКТИКИ)

Организация образовательного процесса по данной дисциплине регламентируется учебным планом и расписанием учебных занятий. При формировании своей индивидуальной образовательной траектории обучающийся имеет право на перезачет дисциплины (переаттестации ее части), если она была освоена в процессе предшествующего обучения. Перезачёт (переаттестации ее части) освобождает обучающегося от необходимости повторного освоения дисциплины (полностью или частично).

Учебный процесс при преподавании курса основывается на использовании традиционных, инновационных и информационных образовательных технологий. Традиционные образовательные технологии представлены практическими занятиями. Инновационные образовательные технологии используются в виде широкого применения активных и интерактивных форм проведения занятий. Информационные образовательные технологии реализуются путем активизации самостоятельной работы студентов в электронной информационной образовательной среде.

Практические занятия проводятся в целях рассмотрения основных вопросов курса и охватывают основные разделы дисциплины.

Основной формой проведения практических занятий является решение конкретных задач, аналогичные которым будут выполнять студенты на лабораторных работах.

Лабораторные работы предполагают выполнение и отчет заданий по темам, рассмотренным на практических занятиях. Каждому лабораторному занятию предшествует самостоятельная подготовка студента, включающая: ознакомление с содержанием лабораторной работы по методическим указаниям; проработку теоретической части по учебникам, рекомендованным в методических указаниях;

Самостоятельная работа студентов включает изучение законспектированного материала, дополнение его с учетом рекомендованной по данной теме литературы, самостоятельную подготовку к лабораторным работам, самостоятельное выполнение и оформление заданий контрольной работы, аналогичных выполненным на занятиях.

В течении семестра для студентов проводятся групповые текущие консультации по учебной дисциплине.

Методические рекомендации по обучению лиц с ограниченными возможностями здоровья и инвалидов

Профессорско-педагогический состав знакомится с психолого-физиологическими особенностями обучающихся инвалидов и лиц с ограниченными возможностями здоровья (ОВЗ), индивидуальными программами реабилитации инвалидов (при наличии). При необходимости осуществляется дополнительная поддержка преподавания тьюторами, психологами, социальными работниками, прошедшими подготовку ассистентами.

В соответствии с методическими рекомендациями Минобрнауки РФ (утв. 8 апреля 2014 г. N АК-44/05вн), в курсе предполагается использовать социально-активные и рефлексивные методы обучения, технологии социокультурной реабилитации с целью оказания помощи в установлении полноценных межличностных отношений с другими студентами, создании комфортного психологического климата в студенческой группе. Подбор и разработка учебных материалов производятся с учетом предоставления материала в различных формах: аудиальной, визуальной, с использованием специальных технических средств и информационных систем.

Освоение дисциплины лицами с ОВЗ осуществляется с использованием средств обучения общего и специального

назначения (персонального и коллективного использования). Материально-техническое обеспечение предусматривает приспособление аудиторий к нуждам лиц с ОВЗ (при необходимости).
Форма проведения аттестации для студентов-инвалидов устанавливается с учетом индивидуальных психофизических особенностей. Для студентов с ОВЗ предусматривается доступная форма предоставления заданий оценочных средств. Студентам с инвалидностью увеличивается время на подготовку ответов на контрольные вопросы. Для таких студентов предусматривается доступная форма предоставления ответов на задания.
При необходимости для обучающихся с инвалидностью процедура оценивания результатов обучения может проводиться в несколько этапов.

Учебно-методическое пособие по дисциплине :
Быков Д.В. Безопасность систем искусственного интеллекта : учебно-методическое пособие, Волгоград : ВолгГТУ, 2021