Аннотация к рабочей программе дисциплины «Прикладные математические задачи информационной безопасности»

Цель преподавания дисциплины

Цель дисциплины – формирование у будущего специалиста представления о роли и значимости нейросетевого моделирования в современном мире, ознакомление с математическим обоснованием обучения и функционирования нейронных сетей, выработка методики нейросетевого моделирования процессов в человеческой деятельности, познакомиться с использованием нейронных сетей в различных областях – распознавание образов, прогнозирование и принятие решений для решения задач профессиональной деятельности научно-исследовательского типа.

Задачи изучения дисциплины

Задачами дисциплины являются:

1. Изучение моделирования как одного из основных методов познания в различных областях человеческой деятельности.
2. Усвоение основных методов обучения нейронных сетей.
3. Понимание основных принципов моделирования.
4. Выработка практических навыков работы по моделированию объекта исследования в нейросеревой структуре, построению компьютерной реализации такой модели, планированию нейросетевого эксперимента и анализу полученных результатов.
5. Обеспечить совместно с другими дисциплинами семестра теоретическую подготовку обучающихся к производственной практике (исследовательской работе) на предприятии-заказчике.

Индикаторы компетенций, формируемые в результате освоения дисциплины

УК-1.2 Определяет пробелы в информации, необходимой для решения проблемной ситуации, и проектирует процессы по их устранению

ПК-3.2 Формулирует целевые критерии для оценивания эффективности исследуемых систем

ПК-3.3 Определяет в результате натурных или математических экспериментов характеристики защищённых информационных систем

Разделы дисциплины

Введение. Искусственные нейронные сети. Алгоритмы обучения нейронных сетей. Многослойные сети с обратным распространением информации. Нейронные сети в защите информации.

МИНОБРНАУКИ РОССИИ

Юго-Западный государственный университет

УТВЕРЖДАЮ:
Декан факультета ФиПИ
_____ Таныгин М.О.
(подпись, инициалы, фамилия)
«30» мая 2023г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Прикладные математические задачи информационной безопасности
(наименование дисциплины)

ОПОП ВО 10.04.01 Информационная безопасность,
(шифр и наименование направления подготовки)

направленность (профиль) «Защищенные информационные системы»
(наименование направленности (профиля))

форма обучения очная

ОПОП ВО реализуется по модели дуального обучения

Курск – 2023

Рабочая программа дисциплины составлена:

– в соответствии с ФГОС ВО – магистратура по направлению подготовки 10.04.01 Информационная безопасность, утвержденным приказом Минобрнауки России от 26.11.2020 г. № 1455;

– на основании учебного плана ОПОП ВО 10.04.01 Информационная безопасность, направленность (профиль) «Защищенные информационные системы», одобренного Ученым советом университета (протокол №12 от 29.05.2023).

– с учетом заказа-требования от 28.04.2023 на результаты освоения ОПОП ВО – программы магистратуры 10.04.01 Информационная безопасность, направленность (профиль) «Защищенные информационные системы», реализуемой по модели дуального обучения в ФГБОУ ВО «Юго-Западный государственный университет», от ООО ЦСБ «ЩИТ-ИНФОРМ»
(наименование предприятия (организации))
(приложение к общей характеристике ОПОП ВО).

Рабочая программа дисциплины обсуждена и рекомендована к реализации в образовательном процессе для дуального обучения студентов по ОПОП ВО 10.04.01 Информационная безопасность, направленность (профиль) «Защищенные информационные системы» на совместном заседании кафедры информационной безопасности
(наименование кафедры)
с представителями ООО ЦСБ «ЩИТ-ИНФОРМ»
(наименование предприятия (организации))
(протокол № 8 от 29.05.2023).

Зав. кафедрой _____ А.Л. Марухленко

Разработчик программы
д.ф.-м.н., профессор _____ В.П. Добрица

Директор научной библиотеки _____ В.Г. Макаровская

Рабочая программа дисциплины пересмотрена, обсуждена и рекомендована к реализации в образовательном процессе на основании учебного плана ОПОП ВО дуального обучения 10.04.01 Информационная безопасность, направленность (профиль) «Защищенные информационные системы», одобренного Ученым советом университета (протокол № __ от __. __. 20__), на совместном заседании кафедры информационной безопасности
(наименование кафедры)
с представителями ООО ЦСБ «ЩИТ-ИНФОРМ»
(наименование предприятия (организации))
(протокол № __ от __. __. 20__).

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

Цель дисциплины – формирование у будущего специалиста представления о роли и значимости нейросетевого моделирования в современном мире, ознакомление с математическим обоснованием обучения и функционирования нейронных сетей, выработка методики нейросетевого моделирования процессов в человеческой деятельности, познакомиться с использованием нейронных сетей в различных областях – распознавание образов, прогнозирование и принятие решений для решения задач профессиональной деятельности научно-исследовательского типа.

1.2 Задачи дисциплины

Задачами дисциплины являются:

1. Изучение моделирования как одного из основных методов познания в различных областях человеческой деятельности.
2. Усвоение основных методов обучения нейронных сетей.
3. Понимание основных принципов моделирования.
4. Выработка практических навыков работы по моделированию объекта исследования в нейросеревой структуре, построению компьютерной реализации такой модели, планированию нейросетевого эксперимента и анализу полученных результатов.
5. Обеспечить совместно с другими дисциплинами семестра теоретическую подготовку обучающихся к производственной практике (исследовательской работе) на предприятии-заказчике.

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*		
УК-1	Способен осуществлять критический анализ проблемных ситуаций на основе	УК-1.2 Определяет пробелы в информации, необходимой для	***Знать:*** ряд проблемных ситуаций, которые могут возникать на предприятии

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*		
	системного подхода, вырабатывать стратегию действий	решения проблемной ситуации, и проектирует процессы по их устранению	***Уметь:*** находить выход из сложившейся ситуации путём анализа опыта предыдущих проблем и конкурирующих организаций ***Владеть (****или* ***Иметь опыт деятельности):*** проектирования процессов исправления возникающего ряда трудностей в управлении
ПК-3	Способен проводить теоретические и экспериментальные исследования	ПК-3.2 Формулирует целевые критерии для оценивания эффективности исследуемых систем	***Знать:*** критерии и показатели эффективности технологий АИАД, методы и средства повышения эффективности технологий АИАД ***Уметь:*** применять научные методы оценки эффективности технологий АИАД ***Владеть (****или* ***Иметь опыт деятельности):*** оценки эффективности полученных научных результатов
		ПК-3.3 Определяет в результате натурных или математических экспериментов характеристики защищённых информационных систем	***Знать:*** методы апробации и внедрения результатов научных исследований, требования нормативных документов по оформлению научно-технической продукции, нормативные правовые акты в области защиты информации ***Уметь:*** разрабатывать научно-техническую документацию по результатам выполненных исследований в области АИАД, производить апробацию результатов выполненных исследований в области

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*		
			АИАД ***Владеть (****или* ***Иметь опыт деятельности):*** апробации и внедрения разработанных эффективных технологий АИАД

2 Указание места дисциплины в структуре основной профессиональной образовательной программы

Дисциплина «Прикладные математические задачи информационной безопасности» входит в часть, формируемую участниками образовательных отношений, блока 1 «Дисциплины (модули)» основной профессиональной образовательной программы – программы магистратуры 10.04.01 Информационная безопасность, направленность (профиль) «Защищенные информационные системы», реализуемой по модели дуального обучения.

Дисциплина изучается на 1 курсе в 1 семестре.

Дисциплина имеет практико-ориентированный характер и изучается до прохождения обучающимися производственной практики (исследовательской работы), завершающей данный семестр.

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)	72
в том числе:	
лекции	36
лабораторные занятия	-
практические занятия	36, из них практическая подготовка обучающихся – 4
Самостоятельная работа обучающихся (всего)	34,85

Контроль (подготовка к экзамену)	36
Контактная работа по промежуточной аттестации (всего АттКР)	1,15
в том числе:	
зачет	не предусмотрен
зачет с оценкой	не предусмотрен
курсовая работа (проект)	не предусмотрен(-а)
экзамен (включая консультацию перед экзаменом)	1,15

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	2	3
1	Введение	Искусственный интеллект. Первые шаги в области искусственных нейронных сетей. Инструменты для расчета и проектирования нейронных сетей на примере ООО ЦСБ «ЩИТ-ИНФОРМ». Особенности 6-й версии системы MATLAB.
2	Искусственные нейронные сети	Нейронный элемент. Функции активации нейронных элементов. Однослойные нейронные сети. Классификация нейронных сетей.
3	Алгоритмы обучения нейронных сетей	Правила обучения Хебба. Правила обучения персептрона. Правило обучения Видроу – Хоффа. Метод обратного распространения ошибки.
4	Многослойные сети с обратным распространением информации	Многослойные сети с обратным распространением информации. Обобщенное правило обучения Хебба. Радиальные базисные сети и их обучение на примере ООО ЦСБ «ЩИТ-ИНФОРМ».
5	Нейронные сети в защите информации	Подходы к использованию нейронных сетей в шифровании на примере ООО ЦСБ «ЩИТ-ИНФОРМ». Нейросетевой блок выработки ключа симметричного шифрования по короткому коду. Нейросетевой блок выработки ключа симметричного шифрования для каждого блока по предыдущему блоку.

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	Введение	4	-	1-2	У 1-4 МУ-1,2	УО, ЗПР 1-2	УК-1 ПК-3

2	Искусственные нейронные сети	6	-	3-4	У 1-4 МУ-1,2	УО, ЗПР 3-5	УК-1 ПК-3
3	Алгоритмы обучения нейронных сетей	6	-	5	У 1-4 МУ-1,2	УО, ЗПР 6-8	УК-1 ПК-3
4	Многослойные сети с обратным распространением информации	8	-	6-7	У 1-4 МУ-1,2	УО, ЗПР 9-11	УК-1 ПК-3
5	Нейронные сети в защите информации	6	-	8	У 1-4 МУ-1,2	УО, ЗПР, КЗ, ПЗ 12-14	УК-1 ПК-3

УО – устный опрос, ЗПР – защита практической работы, КЗ – кейс, ПЗ - производственная задача

4.2 Лабораторные работы и (или) практические занятия

4.2.1 Практические занятия

Таблица 4.2.1 – Практические занятия

№	Наименование практического занятия	Объем, час.
1	2	3
1	Функции активации нейронных сетей.	4
2	Геометрический метод обучения нейронных сетей.	4
3	Правило Хебба обучения нейронных сетей.	4
4	Правило Розеблатта. Псевдо обратные матрицы.	4
5	Алгоритм Видроу-Хоффа.	4
6	Обучение ассоциативной памяти.	4
7	Алгоритм обратного распространения ошибок.	6
8	Нейросети в прогнозировании временных рядов.	6, из них практическая подготовка обучающихся – 4
Итого		36, из них практическая подготовка обучающихся – 4

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	2	3	4
1.	Введение	1-2 недели	4
2.	Искусственные нейронные сети	3-5 недели	6
3.	Алгоритмы обучения нейронных сетей	6-8 недели	10
4.	Многослойные сети с обратным распространением информации	9-11 недели	8
5.	Нейронные сети в защите информации	12-14 недели	6,85
Итого			34,85

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

При самостоятельном изучении отдельных тем и вопросов дисциплины студенты могут пользоваться учебно-наглядными пособиями, учебным оборудованием и методическими разработками кафедры *информационной безопасности* в рабочее время, установленное Правилами внутреннего распорядка работников университета.

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

библиотекой университета:

- библиотечный фонд укомплектован учебной, методической, научной, периодической, справочной и художественной литературой в соответствии с учебным планом 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;

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

типографией университета:

– посредством оказания помощи авторам в подготовке и издании научной, учебной и методической литературы;

– посредством удовлетворения потребности в тиражировании научной, учебной и методической литературы.

6 Образовательные технологии. Практическая подготовка обучающихся

Реализация программы магистратуры по модели дуального обучения и компетентностного подхода предусматривают широкое использование в образовательном процессе активных и интерактивных форм проведения занятий в сочетании с внеаудиторной работой с целью формирования универсальных и профессиональных компетенций обучающихся.

Таблица 6.1 – Интерактивные образовательные технологии, используемые при проведении аудиторных занятий

№	Наименование раздела (темы лекции, практического или лабораторного занятия)	Используемые интерактивные образовательные технологии	Объем, час.
1	2	3	4
1	Нейронные сети в защите информации	Кейс-технология	4
2	Нейросети в прогнозировании временных рядов	Кейс-технология	6
Итого:			10

Практическая подготовка обучающихся при реализации дисциплины осуществляется путем проведения практических занятий, предусматривающих участие обучающихся в выполнении отдельных элементов работ, связанных с будущей профессиональной деятельностью и направленных на формирование, закрепление, развитие практических навыков и компетенций по направленности (профилю) программы магистратуры.

Практическая подготовка обучающихся при реализации дисциплины организуется в модельных условиях.

Практическая подготовка обучающихся проводится в соответствии с положением П 02.181.

7 Фонд 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, при изучении которых формируется данная компетенция		
	начальный	основной	завершающий
1	2	3	4
УК-1 Способен осуществлять критический анализ проблемных ситуаций на основе системного подхода, вырабатывать стратегию действий	Современная философия и методология науки Прикладные математические задачи информационной безопасности Организация работ по обеспечению безопасности в информационных системах		
ПК-3 Способен проводить теоретические и экспериментальные исследования защищённости информационных систем	Прикладные математические задачи информационной безопасности	Моделирование технических объектов и систем управления Производственная практика по получению умений и навыков управленческой деятельности	Оценка защищённости информационных систем Теоретические основы компьютерной безопасности Производственная преддипломная практика

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 *(наименование этапа по таблице 6.1)*	Показатели оценивания компетенций *(индикаторы достижения компетенций, закрепленные за практикой)*	Критерии и шкала оценивания компетенций			
		Недостаточный уровень («неудовл.»)	Пороговый уровень («удовл.»)	Продвинутый уровень («хорошо»)	Высокий уровень («отлично»)
1	2	3	4	5	6

УК-1/ начальный	УК-1.2 Определяет пробелы в информации, необходимой для решения проблемной ситуации, и проектирует процессы по их устранению	**Знать:** демонстрирует менее 60% знаний, указанных в таблице 1.3 для УК-1. Обучающийся нуждается в постоянных подсказках; допускает грубые ошибки, которые не может исправить самостоятельно.	**Знать:** демонстрирует 60-74% знаний, указанных в таблице 1.3 для УК-1. Знания обучающегося имеют поверхностный характер, имеют место неточности и ошибки.	**Знать:** демонстрирует 75-89% знаний, указанных в таблице 1.3 для УК-1. Обучающийся имеет хорошие, но не исчерпывающие знания; допускает неточности.	**Знать:** демонстрирует 90-100% знаний, указанных в таблице 1.3 для УК-1. Знания обучающегося являются прочными и глубокими, имеют системный характер. Обучающийся свободно оперирует знаниями.
		Уметь: демонстрирует менее 60% умений, установленных в таблице 1.3 для УК-1.	**Уметь:** в целом сформированные, но вызывающие затруднения при самостоятельном применении умения, указанные в таблице 1.3 для УК-1.	**Уметь:** сформированные и самостоятельно применяемые умения, указанные в таблице 1.3 для УК-1.	**Уметь:** хорошо развитые, уверенно и успешно применяемые умения, указанные в таблице 1.3 для УК-1.
		Владеть (*или* ***Иметь опыт деятельности):*** навыки, указанные в таблице 1.3 для УК-1, не развиты.	***Владеть (****или* ***Иметь опыт деятельности):*** навыки, указанные в таблице 1.3 для УК-1, развиты на элементарном уровне.	***Владеть (****или* ***Иметь опыт деятельности):*** навыки, указанные в таблице 1.3 для УК-1, хорошо развиты.	***Владеть (****или* ***Иметь опыт деятельности):*** навыки, указанные в таблице 1.3 для УК-1, доведены до автоматизма.

ПК-3/ начальный	ПК-3.2 Формулирует целевые критерии для оценивания эффективности исследуемых систем ПК-3.3 Определяет в результате натурных или математических экспериментов характеристики защищённых информационных систем	**Знать:** демонстрирует менее 60% знаний, указанных в таблице 1.3 для ПК-3. Обучающийся нуждается в постоянных подсказках; допускает грубые ошибки, которые не может исправить самостоятельно.	**Знать:** демонстрирует 60-74% знаний, указанных в таблице 1.3 для ПК-3. Знания обучающегося имеют поверхностный характер, имеют место неточности и ошибки.	**Знать:** демонстрирует 75-89% знаний, указанных в таблице 1.3 для ПК-3. Обучающийся имеет хорошие, но не исчерпывающие знания; допускает неточности.	**Знать:** демонстрирует 90-100% знаний, указанных в таблице 1.3 для ПК-3. Знания обучающегося являются прочными и глубокими, имеют системный характер. Обучающийся свободно оперирует знаниями.
		Уметь: демонстрирует менее 60% умений, установленных в таблице 1.3 для ПК-3.	**Уметь:** в целом сформированные, но вызывающие затруднения при самостоятельном применении умения, указанные в таблице 1.3 для ПК-3.	**Уметь:** сформированные и самостоятельно применяемые умения, указанные в таблице 1.3 для ПК-3.	**Уметь:** хорошо развитые, уверенно и успешно применяемые умения, указанные в таблице 1.3 для ПК-3.
		Владеть (*или* ***Иметь опыт деятельности):*** навыки, указанные в таблице 1.3 для ПК-3, не развиты.	***Владеть (****или* ***Иметь опыт деятельности):*** навыки, указанные в таблице 1.3 для ПК-3, развиты на элементарном уровне.	***Владеть (****или* ***Иметь опыт деятельности):*** навыки, указанные в таблице 1.3 для ПК-3, хорошо развиты.	***Владеть (****или* ***Иметь опыт деятельности):*** навыки, указанные в таблице 1.3 для ПК-3, доведены до автоматизма.

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	Введение	УК-1 ПК-3	Лекция, СРС, практическое занятие	Вопросы для УО КВЗПР 1-2	1-10 1-20	Согласно табл.7.2
2	Искусственные нейронные сети	УК-1 ПК-3	Лекция, СРС, практическое занятие	Вопросы для УО КВЗПР 3-4	1-10 1-20	Согласно табл.7.2
3	Алгоритмы обучения нейронных сетей	УК-1 ПК-3	Лекция, СРС, практическое занятие	Вопросы для УО КВЗПР 5	1-10 1-10	Согласно табл.7.2
4	Многослойные сети с обратным распространением информации	УК-1 ПК-3	Лекция, СРС, практическое занятие	Вопросы для УО КВЗПР 6-7	1-10 1-20	Согласно табл.7.2
5	Нейронные сети в защите информации	УК-1 ПК-3	Лекция, СРС, практическое занятие	Вопросы для УО КВЗПР 8 Кейс Производственная задача	1-10 1-10 1-4 1-10	Согласно табл.7.2

КВЗПР – контрольные вопросы для защиты практических работ

7.3.1 Примеры типовых контрольных заданий для проведения текущего контроля успеваемости

Вопросы для устного опроса по разделу (теме) № 1 «Введение»

1. Интеллект и искусственный интеллект.
2. Предмет, цели и задачи искусственного интеллекта.
3. Основные направления исследований по искусственному интеллекту.

4. Работа мозга человека.
5. Механизмы обучения нейронных систем.

Контрольные вопросы для защиты практической работы №1
1. Нахождение уравнения прямой, проходящей через две данные точки.
2. Нахождение уравнения плоскости по координатам трех точек.
3. Виды различных функций активации и их графики.

Производственная задача

Определение оптимального размера ключа: компания использует криптографические алгоритмы для защиты данных. Задача состоит в математическом анализе стойкости алгоритмов в зависимости от размера ключа и определении оптимального размера ключа для обеспечения требуемого уровня безопасности при минимальных вычислительных ресурсах.

Кейс

Компания занимается разработкой информационной безопасности и получила заказ от клиента на разработку криптографической системы для безопасной передачи конфиденциальной информации. Клиент работает с чувствительными данными, которые требуют высокого уровня защиты от несанкционированного доступа. Ваша задача - разработать и реализовать криптографическую систему, которая будет обеспечивать конфиденциальность и целостность передаваемых данных.

Вам предстоит выполнить следующие задачи:

Выбор криптографических алгоритмов: Проанализируйте различные криптографические алгоритмы, такие как блочные шифры, поточные шифры, асимметричные шифры и хэш-функции. Выберите подходящие алгоритмы, которые обеспечат необходимый уровень безопасности для передаваемой информации.

Разработка протокола обмена ключами: Разработайте протокол обмена ключами, который будет использовать математические методы, такие как диффи-хеллмановский обмен ключами или эллиптическая криптография. Протокол должен обеспечивать безопасность передаваемых ключей и защиту от атак по перехвату.

Реализация шифрования данных: Разработайте алгоритм шифрования данных с использованием выбранных криптографических алгоритмов. Обеспечьте конфиденциальность и целостность данных при передаче и хранении. Учтите требования клиента относительно скорости и эффективности шифрования.

Разработка системы цифровой подписи: Разработайте систему цифровой подписи, которая позволит клиенту подтверждать подлинность и целостность передаваемых данных. Используйте асимметричные криптографические методы, такие как RSA или эллиптическая криптография, для создания и проверки цифровых подписей.

Тестирование и анализ безопасности: Проведите тестирование разрабо-

танной криптографической системы на наличие уязвимостей и атак.

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

7.3.2 Типовые задания для проведения промежуточной аттестации обучающихся

Промежуточная аттестация по дисциплине проводится в форме экзамена. На промежуточной аттестации по дисциплине применяется механизм квалификационного экзамена. Экзамен имеет структуру квалификационного экзамена и состоит из 2 частей:

– теоретической (компьютерное тестирование);

– практической (решение компетентностно-ориентированной задачи).

На теоретической части экзамена (тестировании) проверяются знания и частично – умения и навыки обучающихся. 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.

*«*На практической части экзамена проверяются результаты практической подготовки: *компетенции, включая умения, навыки (или опыт деятельности)*). Результаты практической подготовки *(компетенции, включая умения, навыки (или опыт деятельности))* проверяются с помощью компетентностно-ориентированных задач (ситуационных, производственных, кейс-задач или кейсов) 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 ка-

чество освоения обучающимися основных элементов содержания дисциплины и уровень сформированности компетенций.

а) Примеры типовых заданий для теоретической части экзамена (тестирования)

Задание в закрытой форме:

Среди данных функций указать пороговую в биполярном случае.

1) th(x);
2) sign(x);
3) $\underline{\text{sgn}}(x)$;
4) $\overline{\text{sgn}}(x)$;
5) $f(x) = 1/1+e^x$.

Задание в открытой форме:

Постройте графики функций: sign(x), sgn(x), $\overline{\text{sgn}}(x)$.

Задание на установление правильной последовательности:

Расположите следующие этапы обучения нейронной сети в правильной последовательности:

1. Инициализация весов
2. Прямой проход (forward propagation)
3. Обратный проход (backpropagation)
4. Оценка ошибки (loss evaluation)
5. Обновление весов

Задание на установление соответствия:

функция	Название функции
th(x)	Функция знака
sign(x)	Сигмоидная функция в биполярном случае
$\underline{\text{sgn}}(x)$	Сигмоидная функция
$\overline{\text{sgn}}(x)$	Гиперболический тангенс
$f(x) = 1/1+e^x$	Пороговая функция в полярном случае
	Пороговая функция в биполярном случае

б) Примеры типовых заданий для практической части экзамена

Компетентностно-ориентированная задача:

Разработайте криптографический протокол для безопасной передачи данных между клиентами и сервером. Ваша задача состоит в математическом моделировании и анализе протокола для обеспечения его надежности, конфиденциальности и целостности данных.

Полностью оценочные материалы и оценочные средства для проведения промежуточной аттестации обучающихся представлены в УММ по дисциплине.

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

– положение П 02.207 «Проектирование и реализация основных профессиональных программ высшего образования – программ магистратуры по модели дуального обучения»;

– 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
Устный опрос по темам 1-5	6	Не ответил или неполно ответил на какой-либо вопрос	12	Правильно и полно ответил на все вопросы
Практические работы № 1-8	12	Выполнил, но не ответил или неполно ответил на какой-либо вопрос	24	Выполнил, правильно и полно ответил на все вопросы
Кейс	4	Выполнил, но не ответил или	8	Выполнил, правильно и полно от-

Форма контроля	Минимальный балл		Максимальный балл	
	балл	примечание	балл	примечание
1	2	3	4	5
		неполно ответил на какой-либо вопрос		ветил на все вопросы
Производственная задача	2	Выполнил, но не ответил или неполно ответил на какой-либо вопрос	4	Выполнил, правильно и полно ответил на все вопросы
Итого	24		48	
Посещаемость	0		16	
Экзамен	0		36	
Итого	24		100	

Для проведения промежуточной аттестации обучающихся (теоретической части и практической части) используется следующая методика оценивания знаний, умений, навыков и (или) опыта деятельности. В каждом варианте КИМ –16 заданий (15 вопросов для тестирования и одна компетентностно-ориентированная задача).

Каждый верный ответ оценивается следующим образом:

– задание в закрытой форме –2 балла,
– 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 по промежуточной аттестации – 36.

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

8.1 Основная литература

1. Яхъяева, Г. Э. Нечеткие множества и нейронные сети : учебное пособие / Г. Э. Яхъяева. — 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: 09.10.2023). — Режим доступа: для авторизир. пользователей

2. Епишкина, А. В. Теория алгоритмов в задачах информационной безопасности: конспект лекций : учебное пособие / А. В. Епишкина, К. Г. Когос. — Москва : Национальный исследовательский ядерный университет «МИФИ», 2022. — 96 с. — ISBN 978-5-7262-2897-6. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: https://www.iprbookshop.ru/132697.html (дата обращения: 09.10.2023). — Режим доступа: для авторизир. пользователей

8.2 Дополнительная литература

3. Пенькова, Т. Г. Модели и методы искусственного интеллекта : учебное пособие / Т. Г. Пенькова, Ю. В. Вайнштейн. — Красноярск : Сибирский федеральный университет, 2019. — 116 с. — ISBN 978-5-7638-4043-8. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: https://www.iprbookshop.ru/100056.html (дата обращения: 09.10.2023). — Режим доступа: для авторизир. пользователей

4. Белозерова, Г. И. Нечеткая логика и нейронные сети : учебное пособие / Г. И. Белозерова, Д. М. Скуднев, З. А. Кононова. — Липецк : Липецкий государственный педагогический университет имени П.П. Семёнова-Тян-Шанского, 2017. — 63 с. — ISBN 978-5-88526-875-2 (Ч. 1), 978-5-88526-874-5. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: https://www.iprbookshop.ru/101639.html (дата обращения: 09.10.2023). — Режим доступа: для авторизир. пользователей

5. Павлов, С. Н. Системы искусственного интеллекта. Часть 1 : учебное пособие / С. Н. Павлов. — Томск : Томский государственный университет систем управления и радиоэлектроники, Эль Контент, 2011. — 176 с. — ISBN 978-5-4332-0013-5. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: https://www.iprbookshop.ru/13974.html (дата обращения: 09.10.2023). — Режим доступа: для авторизир. пользователей

8.3 Перечень методических указаний

1. Прикладные математические задачи информационной безопасности: методические указания по выполнению практических работ / Юго-Зап. гос. ун-т; сост.: В.П. Добрица. – Курск, 2023. – 18 с.: Библиогр.: с. 18. - Текст : электронный.
2. Прикладные математические задачи информационной безопасности: методические указания для самостоятельной работы / Юго-Зап. гос. ун-т; сост.: Е.А. Кулешова. – Курск, 2023. – 13 с.: Библиогр.: с. 13. - Текст : электронный.

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

1. Федеральная служба безопасности [официальный сайт]. Режим доступа: http://www.fsb.ru/
2. Федеральная служба по техническому и экспортному контролю [официальный сайт]. Режим доступа: http://fstec.ru/
3. Электронно-библиотечная система «Лань» - http://e.lanbook.com/
4. Электронно-библиотечная система IQLib – http://www.iqlib.ru
5. Электронная библиотека «Единое окно доступа к образовательным ресурсам» - http://window.edu.ru/

10 Методические указания для обучающихся по освоению дисциплины

Основными видами аудиторной работы студента при изучении дисциплины являются лекции и практические занятия.

На лекциях излагаются и разъясняются основные понятия и положения каждой новой темы; важные положения аргументируются и иллюстрируются примерами из практики; объясняется практическая значимость изучаемой темы; делаются выводы; даются рекомендации для самостоятельной работы по данной теме. На лекциях необходимо задавать преподавателю уточняющие вопросы с целью уяснения теоретических положений, разрешения спорных вопросов. В ходе лекции студент должен конспектировать учебный материал. Конспектирование лекций – сложный вид работы, предполагающий интенсивную умственную деятельность студента. Конспект является полезным тогда, когда записано самое существенное и сделано это лично студентом в режиме реального времени в течение лекции. Не следует стремиться записать лекцию дословно. Целесообразно вначале понять основную мысль, излагаемую лектором, а затем кратко записать ее. Желательно заранее оставлять в тетради пробелы, куда позднее, при самостоятельной работе с конспектом, можно внести дополнительные записи. Конспект лекции лучше подразделять на пункты, соблюдая красную строку. Этому в большой степени будут способствовать вопросы плана лекции, который преподаватель дает

в начале лекционного занятия. Следует обращать внимание на акценты, выводы, которые делает лектор, отмечая наиболее важные моменты в лекционном материале.

Необходимым является глубокое освоение содержания лекции и свободное владение им, в том числе использованной в ней терминологией. Работу с конспектом лекции целесообразно проводить непосредственно после ее прослушивания, что способствует лучшему усвоению материала, позволяет своевременно выявить и устранить «пробелы» в знаниях. Работа с конспектом лекции предполагает перечитывание конспекта, внесение в него, по необходимости, уточнений, дополнений, разъяснений и изменений. Некоторые вопросы выносятся за рамки лекций. Изучение вопросов, выносимых за рамки лекционных занятий, предполагает самостоятельное изучение студентами дополнительной литературы, указанной в п.8.2.

Изучение наиболее важных тем или разделов дисциплины продолжается на практических занятиях, которые обеспечивают контроль подготовленности студента; закрепление учебного материала; приобретение опыта устных публичных выступлений, ведения дискуссии, в том числе аргументации и защиты выдвигаемых положений и тезисов.

Практическому занятию предшествует самостоятельная работа студента, связанная с освоением материала, полученного на лекциях, и материалов, изложенных в учебниках и учебных пособиях, а также литературе, рекомендованной преподавателем. Самостоятельная работа с учебниками, учебными пособиями, научной, справочной литературой, материалами периодических изданий и Интернета является наиболее эффективным методом получения дополнительных знаний, позволяет значительно активизировать процесс овладения информацией, способствует более глубокому усвоению изучаемого материала. При работе с источниками и литературой необходимо:

– сопоставлять, сравнивать, классифицировать, группировать, систематизировать информацию в соответствии с определенной учебной задачей;

– обобщать полученную информацию, оценивать прочитанное;

– фиксировать основное содержание прочитанного текста; формулировать устно и письменно основную идею текста; составлять план, формулировать тезисы.

Самостоятельную работу следует начинать с первых занятий. От занятия к занятию нужно регулярно прочитывать конспект лекций, знакомиться с соответствующими разделами учебника, читать и конспектировать литературу по каждой теме дисциплины. Самостоятельная работа дает студентам возможность равномерно распределить нагрузку, способствует более глубокому и качественному освоению учебного материала. В случае необходимости студенты обращаются за консультацией к преподавателю. Обязательным элементом самостоятельной работы по дисциплине является самоконтроль. Одной из важных задач обучения студентов способам и приемам самообразования является формирование у них умения самостоятельно контролировать и адекватно оценивать результаты своей учебной деятельности и на этой

основе управлять процессом овладения знаниями. Овладение умениями самоконтроля приучает студентов к планированию учебного труда, способствует углублению их внимания, памяти и выступает как важный фактор развития познавательных способностей. Самоконтроль включает:

– оперативный анализ глубины и прочности собственных знаний и умений;

– критическую оценку результатов своей познавательной деятельности.

Самоконтроль учит ценить свое время, позволяет вовремя заметить и исправить свои ошибки. Формы самоконтроля могут быть следующими:

– устный пересказ текста лекции и сравнение его с содержанием конспекта лекции;

– составление плана, тезисов, формулировок ключевых положений текста по памяти;

– пересказ с опорой на иллюстрации, чертежи, схемы, таблицы, опорные положения.

Самоконтроль учебной деятельности позволяет студенту оценивать эффективность и рациональность применяемых методов и форм умственного труда, находить допускаемые недочеты и на этой основе проводить необходимую коррекцию своей познавательной деятельности.

При подготовке к промежуточной аттестации по дисциплине необходимо повторить основные теоретические положения каждой изученной темы и основные термины, самостоятельно решить несколько типовых компетентностно-ориентированных задач.

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

Информационные технологии:

1. Средства для просмотра презентаций;
2. Средства для проведения онлайн-конференций.
3. Электронно-образовательная среда ЮЗГУ

Программное обеспечение:

1. OpenOffice: режим доступа: свободный.
2. Яндекс.Телемост: режим доступа: свободный.

Информационные справочные системы:

1. Научно-информационный портал ВИНИТИ РАН. Режим доступа: свободный.
2. База данных "Патенты России". Режим доступа: свободный.

3. Электронно-библиотечная система «Университетская библиотека онлайн» Режим доступа: по подписке.

4. Электронная библиотека диссертаций и авторефератов РГБ. Режим доступа: свободный.

5. Электронный каталог Научной библиотеки ЮЗГУ. Режим доступа: свободный.

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

Аудиторные занятия по дисциплине проводятся в учебной аудитории для проведения занятий лекционного типа и лаборатории кафедры информационной безопасности, оснащенных стандартной учебной мебелью (столы и стулья для обучающихся; стол и стул для преподавателя; доска).

Для организации образовательного процесса применяются технические средства обучения: Проекционный экран на штативе; Мультимедиа центр: ноутбук ASUS X50VL PMD-T2330/1471024Mb/160Gb/ сумка/ проектор inFocus IN24.

Для осуществления практической подготовки обучающихся при реализации дисциплины используются оборудование и технические средства обучения кафедры информационной безопасности:

1. Класс ПЭВМ - Asus-P7P55LX-/DDR34096Mb/Coree i3-540/SATA-11 500 Gb Hitachi/PCI-E 512Mb, Монитор TFT Wide 23.

2. Мультимедиацентр: ноутбук ASUS X50VL PMD - T2330/14"/1024Mb/ 160Gb/ сумка/проектор inFocus IN24+ .

3. Экран мобильный Draper Diplomat 60x60.

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 также сурдопереводчиков и тифлосурдопереводчиков. Текущий контроль успеваемости осуществляется в письменной форме: обучающийся письменно отвечает на вопросы, письменно выполняет практические задания. 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).

14 Лист дополнений и изменений, внесенных в рабочую программу дисциплины

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