МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
(МИНОБРНАУКИ РОССИИ)

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«ДОНБАССКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»
(ФГБОУ ВО «ДонГТУ»)

Факультет информационных технологий и автоматизации производственных процессов

Кафедра интеллектуальных систем и информационной безопасности

УТВЕРЖДАЮ
И.о. проректора
по учебной работе
Д.В. Мулов

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Интеллектуальные системы информационной безопасности
(наименование дисциплины)

10.05.03 Информационная безопасность автоматизированных систем
(код, наименование специальности)

Безопасность открытых информационных систем
(специализация)

Квалификация специалист по защите информации
(бакалавр/специалист/магистр)

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

Алчевск, 2024

1 Цели и задачи изучения дисциплины

Цели дисциплины. Целью изучения дисциплины «Интеллектуальные системы информационной безопасности» предоставить студентам теоретические знания и практические навыки в области обеспечения информационной безопасности с использованием интеллектуальных технологий.

Задачи изучения дисциплины:

– приобретения студентами навыков формального представления знаний средствами различных моделей и программной реализации элементов систем хранения и обработки знаний и экспертных систем (ЭС);

– изучение основных принципов создания интеллектуальных систем безопасности для информационных систем.

Дисциплина направлена на формирование общепрофессиональных (ПК-2) компетенций выпускника.

2 Место дисциплины в структуре образовательной программы

Логико-структурный анализ дисциплины – курс входит в часть, формируемую участниками образовательных отношений БЛОКА 1 «Дисциплины (модули)» подготовки студентов по специальности 10.05.03 Информационная безопасность автоматизированных систем (10.05.03-05 Безопасность открытых информационных систем).

Дисциплина реализуется кафедрой интеллектуальных систем и информационной безопасности. Основывается на базе дисциплин: «Математическая логика и теория алгоритмов», «Средства защиты от разрушающих программных компонентов», «Технологии и методы программирования».

Является основой для изучения следующих дисциплин: «Информационная безопасность открытых информационных систем», «Технология построения защищенных распределенных приложений».

Для изучения дисциплины необходимы компетенции, сформированные у студента для решения профессиональных задач деятельности, связанных с применением интеллектуальных вычислительных систем.

Курс является фундаментом для ориентации студентов в сфере разработки интеллектуальных информационных систем.

Общая трудоемкость освоения дисциплины составляет 4 зачетных единицы, 144 ак.ч. Программой дисциплины предусмотрены лекционные (36 ак.ч.), лабораторные (36 ак.ч.) занятия и самостоятельная работа студента (72 ак.ч.).

Дисциплина изучается на 5 курсе в 10 семестре. Форма промежуточной аттестации – экзамен.

3 Перечень результатов обучения по дисциплине, соотнесённых с планируемыми результатами освоения образовательной программы

Процесс изучения дисциплины «Интеллектуальные системы информационной безопасности» направлен на формирование компетенции, представленной в таблице 1.

Таблица 1 – Компетенции, обязательные к освоению

Содержание компетенции	Код компетенции	Код и наименование индикатора достижения компетенции
Способен использовать интеллектуальные методы и технологии при разработке программного обеспечения средств защиты информации автоматизированных систем	ПК-2	ПК-2.2 Применяет интеллектуальные методы и технологии при разработке программного обеспечения средств защиты информации автоматизированных систем

4 Объём и виды занятий по дисциплине

Общая трудоёмкость учебной дисциплины составляет 4 зачётных единицы, 144 ак.ч.

Самостоятельная работа студента (СРС) включает проработку материалов лекций, подготовку к практическим занятиям, текущему контролю, выполнение индивидуального задания, самостоятельное изучение материала и подготовку к экзамену.

При организации внеаудиторной самостоятельной работы по данной дисциплине используются формы и распределение бюджета времени на СРС для очной формы обучения в соответствии с таблицей 2.

Таблица 2 – Распределение бюджета времени на СРС

Вид учебной работы	Всего ак.ч.	Ак.ч. по семестрам
		10
Аудиторная работа, в том числе:	72	72
Лекции (Л)	36	36
Практические занятия (ПЗ)	36	36
Лабораторные работы (ЛР)	-	-
Курсовая работа/курсовой проект	-	-
Самостоятельная работа студентов (СРС), в том числе:	72	72
Подготовка к лекциям	9	9
Подготовка к лабораторным работам	18	18
Подготовка к практическим занятиям / семинарам	-	-
Выполнение курсовой работы / проекта	-	-
Расчетно-графическая работа (РГР)	-	-
Реферат (индивидуальное задание)	–	–
Домашнее задание	-	-
Подготовка к контрольным работам	-	-
Подготовка к коллоквиуму	-	-
Аналитический информационный поиск	-	-
Работа в библиотеке	9	9
Подготовка к экзамену	36	36
Промежуточная аттестация – экзамен (Э)	Э	Э
Общая трудоемкость дисциплины		
ак.ч.	144	144
з.е.	4	4

5 Содержание дисциплины

С целью освоения компетенций, приведенных в п.3 дисциплина разбита на 5 тем:

– тема 1 (Введение. Основные понятия и история развития направления. Экспертные системы и их структура);

– тема 2 (Методы ИИ в системах информационной безопасности.. Модели представления знаний);

– тема 3 (Нечеткие логические модели представления знаний в системах информационной безопасности);

– тема 4 (Искусственные нейронные сети в системах информационной безопасности);

– тема 5 (Генетические алгоритмы в системах информационной безопасности).

Виды занятий по дисциплине и распределение аудиторных часов для очной формы приведены в таблице 3.

Таблица 3 – Виды занятий по дисциплине и распределение аудиторных часов (очная форма обучения)

№ п/п	Наименование темы (раздела) дисциплины	Содержание лекционных занятий	Трудоемкость в ак.ч.	Темы практических занятий	Трудоемкость в ак.ч.	Тема лабораторных занятий	Трудоемкость в ак.ч.
1	2	3	4	5	6	7	8
1	Введение. Основные понятия и история развития направления. Экспертные системы и их структура	Понятие искусственного интеллекта (ИИ) и интеллектуальной информационной системы. История развития ИИ. Экспертные системы. Назначение. Структура. Классификация.	4	–	–	–	–
	Методы ИИ в системах информационной безопасности.. Модели представления знаний	Методы представления знаний в интеллектуальных информационных системах. Классификация. Представление знаний в виде семантических сетей. Преимущества и недостатки. Представление знаний на основе фреймов. Преимущества и недостатки. Представление знаний на основе продукционной модели. Преимущества и недостатки.	8			Представление знаний в виде семантических сетей. Представление знаний на основе фреймов.	6 6

Завершение таблицы 3

1	2	3	4	5	6	7	8
3	Нечеткие логические модели представления знаний в системах информационной безопасности	Основы теории нечетких множеств. Понятие лингвистической переменной. Нечеткий логический вывод в продукционных системах.	8	–	–	Лингвистические переменные – создание и обработка Продукционная модель вывода	6 6
4	Искусственные нейронные сети в системах информационной безопасности	Определение. Основные понятия. Виды искусственных нейронных сетей (ИНС). Алгоритмы обучения ИНС с учителем и без. Практическое применение в распознавании образов.	8			Создание, обучение и тестирование	6
5	Генетические алгоритмы в системах информационной безопасности	Основные понятия. Этапы генетического алгоритма Применение генетических алгоритмов в решении оптимизационных задач	8			Разработка генетического алгоритма	6
Всего аудиторных часов		36		-		36	

6 Фонд оценочных средств для проведения текущего контроля успеваемости и промежуточной аттестации студентов по дисциплине

6.1 Критерии оценивания

В соответствии с Положением о кредитно-модульной системе организации образовательного процесса ФГБОУ ВО «ДонГТУ» (https://www.dstu.education/images/structure/license_certificate/polog_kred_modul.pdf) при оценивании сформированности компетенций по дисциплине используется 100-балльная шкала.

Перечень компетенций по дисциплине и способы оценивания знаний приведены в таблице 4.

Таблица 4 – Перечень компетенций по дисциплине и способы оценивания знаний

Код и наименование компетенции	Способ оценивания	Оценочное средство
ПК-2	Экзамен	Комплект контролирующих материалов для экзамена

Всего по текущей работе в семестре студент может набрать 100 баллов, в том числе:

– реферат – всего 20 баллов;

- лабораторные работы – всего 80 баллов.

Оценка по экзамену проставляется автоматически, если студент набрал в течении семестра не менее 60 баллов и отчитался за каждую контрольную точку. Минимальное количество баллов по каждому из видов текущей работы составляет 60% от максимального.

Экзамен по дисциплине «Интеллектуальные системы информационной безопасности» проводится по результатам работы в семестре. В случае, если полученная в семестре сумма баллов не устраивает студента, во время сессии студент имеет право повысить итоговую оценку в форме устного собеседования по приведенным ниже вопросам.

Шкала оценивания знаний при проведении промежуточной аттестации приведена в таблице 5.

Таблица 5 – Шкала оценивания знаний

Сумма баллов за все виды учебной деятельности	Оценка по национальной шкале зачёт/экзамен
0-59	Не зачтено/неудовлетворительно
60-73	Зачтено/удовлетворительно
74-89	Зачтено/хорошо
90-100	Зачтено/отлично

6.2 Домашнее задание

Домашнее задание не предусмотрено.

6.3 Темы для рефератов (презентаций) – индивидуальное задание

Рефераты (индивидуальные задания) не предусмотрены.

6.4 Оценочные средства для самостоятельной работы и текущего контроля успеваемости

Тема 1 Введение. Основные понятия и история развития направления. Экспертные системы и их структура.

1. Вывод, строящийся по принципу движения мысли от общего к частному – это …

а) индуктивный вывод;

б) дедуктивный вывод.

Ответ: б

2. .... – это закономерности предметной области (принципы, связи, законы), полученные в результате практической деятельности и профессионального опыта, позволяющие специалистам ставить и решать задачи в этой предметной области.

Ответ: знания.

3. Модель знаний, представленная в виде ориентированного графа, вершины которого – понятия, а дуги – отношения между ними – это ... сеть.

Ответ: семантическая.

4. Экспертные системы по своей сути – это:

а) авторские системы;

б) операционные системы;

в) системы программирования;

г) системы искусственного интеллекта.

Ответ: г

5. ..... – это структура данных, компоненты которой называются слотами.

Ответ: фреймы.

Тема 2 Методы ИИ в системах информационной безопасности.. Модели представления знаний.

1. Что такое модель представления знаний? Выберите один правильный ответ.

а) Зафиксированная и проверенная практикой обработанная информация, которая использовалась и может многократно использоваться для принятия решений.

б) Совокупность структур представления знаний и механизма вывода на их основе содержащихся либо новых знаний.

в) Совокупность сведений, зафиксированных на определенном носителе в форме, пригодной для постоянного хранения, передачи и обработки.

г) Закономерности предметной области (принципы, связи, законы), полученные в результате практической деятельности и профессионального опыта.

д) Отдельные факты, характеризующие объекты, процессы и явления предметной области, а также их свойства.

Ответ: б

2. Продукционная модель - это... Выберите один правильный ответ

а) Способ представления знаний, представляющий собой схему действий в реальной ситуации.

б) Раздел искусственного интеллекта, изучающий базы знаний и методы работы со знаниями

в) Сведения об объектах и явлениях окружающей среды, их параметрах, свойствах и состоянии.

г) Основанная на правилах модель, позволяющая представить знание в виде предложений типа «Если (условие), то (действие)».

д) Выбор наилучшего варианта решения из множества допустимых на основании имеющейся информации.

Ответ: г

3. Как выглядит общий вид продукционной модели? Выберите один правильный ответ

а) Описание класса ситуаций, условие для активации продукции, ядро продукции, постусловие

б) Протоколы вышестоящего уровня используют протоколы нижестоящего уровня

в) Множество вершин и множество отношений между ними

г) Определенная структура, состоит из имени и отдельных единиц

Ответ: г

4. Моделью представления знаний в ИС может быть (несколько вариантов ответа):

а) фреймовая

б) логическая

в) семантическая сеть

г) любая из перечисленных

д) продукционная

Ответ: г

5. Знания – это:

а) отдельные факты, характеризующие объекты;

б) закономерности предметной области (принципы, связи, законы);

в) сведения о процессах и явлениях предметной области, а также их свойствах.

Ответ: в

Тема 3 Нечеткие логические модели представления знаний в системах информационной безопасности.

1. Что такое нечеткая логика?

a) Метод работы с неопределенностью и приближенными значениями

b) Метод оптимизации

c) Метод визуализации данных

d) Метод генерации данных

Ответ: а

2. Что такое нечеткое множество?

a) Множество, где элементы имеют степень принадлежности

b) Метод оптимизации

c) Метод визуализации данных

d) Метод генерации данных

Ответ: а

3. В нечеткой логике _____ определяет степень принадлежности элемента множеству.

Ответ: функция принадлежности

4. _____ — это процесс получения решений на основе нечетких правил.

Ответ: нечеткий вывод

5. Напишите формулу для центроидного метода дефаззификации.

Ответ: $y = (\Sigma\mu(x_i) * x_i) / \Sigma\mu(x_i)$

Тема 4 Искусственные нейронные сети в системах информационной безопасности.

1. Что такое нейрон в нейронной сети?

a) Математическая функция

b) Элемент, который принимает входные данные, обрабатывает их и передает выход

c) Тип алгоритма оптимизации

d) Графическое представление данных

Ответ: b

2. Какая функция активации чаще всего используется в скрытых слоях нейронных сетей?

a) Сигмоида

b) ReLU

c) Тангенс

d) Линейная

Ответ: b

3. Что такое градиентный спуск?

a) Метод оптимизации, который минимизирует функцию потерь

b) Метод генерации данных

c) Метод визуализации данных

d) Метод кластеризации

Ответ: a

4. Метод _____ используется для минимизации функции потерь в нейронных сетях.

Ответ: градиентный спуск

5. Дайте определение обратного распространения ошибки. **Ответ: Метод, который вычисляет градиент функции потерь по весам сети для их обновления.**

Тема 5 Генетические алгоритмы в системах информационной безопасности.

1. Что такое генетический алгоритм?

a) Метод оптимизации, основанный на принципах естественного отбора

b) Метод кластеризации данных

c) Метод визуализации данных

d) Метод генерации данных

Ответ: a

2. Что такое хромосома в генетическом алгоритме?

a) Набор параметров, представляющих решение

b) Тип функции активации

c) Метод оптимизации

d) Метод визуализации данных

Ответ: а

3. Что такое фитнес-функция?

a) Функция, которая оценивает качество решения

b) Функция, которая генерирует данные

c) Функция, которая визуализирует данные

d) Функция, которая оптимизирует данные

Ответ: а

4. Что такое мутация в генетическом алгоритме?

a) Случайное изменение параметров хромосомы

b) Метод оптимизации

c) Метод визуализации данных

d) Метод генерации данных

Ответ: а

5. Что такое скрещивание (кроссовер)?

a) Обмен частями хромосом между двумя родителями

b) Метод оптимизации

c) Метод визуализации данных

d) Метод генерации данных

Ответ: а

6.5 Вопросы для подготовки к экзамену

1) Какие Вы знаете основные направления исследований в области искусственного интеллекта?

2) Какие Вы знаете основные понятия, определение и классификация интеллектуальных систем?

3) Что Вы знаете об истории развития методов и технологий искусственного интеллекта?

4) Что такое экспертные системы, основные понятия и определения? классификация?

5) Что Вы знаете о назначении и принципах построения экспертных систем?

6) Что Вы знаете о представлении знаний в интеллектуальных системах: последовательное развитие структур данных, переход от данных к знаниям, отличительные особенности знаний, типы знаний?

7) Как производится представление знаний семантическими сетями? Что такое формализация семантической сети?

8) Как производится представление знаний фреймами: формализация, основные свойства фреймов, способы управления выводом?

9) Как производится представление знаний в виде нечетких продукций?

10) Что такое теория нечетких множеств?

11) Что Вы знаете о понятии нечеткого множества и операциях над ним?

12) Что Вы знаете о лингвистической переменной?

13) Что такое нечеткие отношения?

14) Какова структура нечеткой системы?

15) Какова структура модели вывода в нечетких системах?

16) Что такое понятие нейронной сети?

17) Какие Вы знаете математические модели нейронов?

18) Что такое однослойные искусственные нейронные сети?

19) Что такое многослойные искусственные нейронные сети?

20) Что такое перцептроны?

21) Какие Вы знаете алгоритмы обучения искусственных нейронных сетей?

22) Что такое алгоритм обратного распространения ошибки?

23) Что Вы знаете о применении нейронных сетей в решении задач классификации?

24) Что такое эволюционные алгоритмы?

25) Каковы общие понятия генетического алгоритма?

26) Как производятся генетические операции: селекция, скрещивание, мутация?

27) Что такое простой генетический алгоритм?

28) Какоыа стратегии, применяемые в генетических алгоритмах?

29) Каково применение генетических алгоритмов в решении оптимизационных задач?

6.6 Тематика и содержание курсового проекта

Курсовой проект не предусмотрен.

7 Учебно-методическое и информационное обеспечение дисциплины

7.1 Рекомендуемая литература

Основная литература

1. Рассел, Стюарт, Норвиг, Питер. Искусственный интеллект: современный подход, 4-е издание, том 3. Обучение, восприятие и действие. : Пер. с англ. - СПб. : ООО "Диалектика", 2022. - 640 с. - Парал. тит. англ. [Электронный ресурс]:. – Режим доступа: https://vk.com/topic-51126445_32505707?offset=80. (Дата обращения 26.08.2024).

2. Боровская, Е. В. Интеллектуальные системы информационной безопасности: учебное пособие / Е. В. Боровская, Н. А. Давыдова. – 4-изд., электрон. - М.: Лаборатория знаний, 2020. - 130 с. // Режим доступа: https://lib.tau-edu.kz/wp-content/uploads/2023/01/Боровская-Е.В.-Основы-искусственногоинтеллекта.pdf. (Дата обращения 26.08.2024).

3. Ватьян, А.С., Гусарова Н.Ф., Добренко Н.В. Системы искусственного интеллекта. – СПб: Университет ИТМО, 2022. – 186 с. – Режим доступа: https://books.ifmo.ru/file/pdf/3142.pdf. (дата обращения: 26.08.2024).

4. Остроух, А.В. Введение в искусственный интеллект: монография / А.В. Остроух. – Красноярск: Научно-инновационный центр, 2020. – 250 с. – Режим доступа: https://nkras.ru/arhiv/2020/ostroukh1.pdf. (Дата обращения 26.08.2024).

Дополнительная литература

1. Таулли, Т. Интеллектуальные системы информационной безопасности: нетехническое введение: Пер. с англ. / Т. Таули – СПб.: БХВ-Петербург, 2021. – 288с.: ил. // Режим доступа: https://psv4.userapi.com/s/v1/d/s6M1hk3LgCR_byMEzuGOXmxLrdKQXHJPo0FnGZnRI3cQoCkOw-sRF6PRSaPvB3uAD4hZfjnvmT6pdTU2EDWVon35vpXdFYwSvkYIjBTOFMNV0CMz/Osnovy_iskusstvennogo_intellekta_netekhnicheskoe_vvedenie_4.pdf. (Дата обращения: 26.08.2024).

2. Постолит, А. В. Интеллектуальные системы информационной безопасности в примерах на Python. Самоучитель. - СПб.: БХВ-Петербург, 2021. -448 с.: ил. - Режим доступа: https://vk.com/doc44301783_616183734?hash=i95rwlLMIwIxkxRWVGcuWib9B2lzm8uKZY7IFTCicqz. (Дата обращения 26.08.2024).

3. Хайкин, Саймон Нейронные сети: полный курс, 2-изд. : Пер. с анг. – М.: ООО И.Д. Вильямс, 2016. – 1104 с. : ил. . - Режим доступа: http://i.uran.ru/webcab/system/files/bookspdf/neyronnye-seti-polnyy-kurs/229022.pdf. (Дата обращения 26.08.2024).

Учебно-методические материалы и пособия

1. Закутный А.С. Интеллектуальные системы информационной безопасности: методические указания к лабораторным работам [Электронный ресурс] – URL: https://3kl.dontu.ru/course/. Режим доступа: для авториз. пользователей. — Текст: электронный. (Дата обращения 26.08.2024).

7.2 Базы данных, электронно-библиотечные системы, информационно-справочные и поисковые системы

1. Научная библиотека ДонГТУ : официальный сайт.— Алчевск. —URL: library.dstu.education. — Текст : электронный.
2. Научно-техническая библиотека БГТУ им. Шухова : официальный сайт. — Белгород. — URL: http://ntb.bstu.ru/jirbis2/. — Текст : электронный.
3. Консультант студента : электронно-библиотечная система.— Москва. — URL: http://www.studentlibrary.ru/cgi-bin/mb4x. — Текст : электронный.
4. Университетская библиотека онлайн: электронно-библиотечная система. – URL: http://biblioclub.ru/index.php?page=main_ub_red. – Текст : электронный.
5. IPR BOOKS : электронно-библиотечная система.—Красногорск. — URL: http://www.iprbookshop.ru/. — Текст : электронный.
6. Сайт кафедры ИСИБ http://scs.dstu.education.

8 Материально-техническое обеспечение дисциплины

Материально-техническая база обеспечивает проведение всех видов деятельности в процессе обучения, соответствует требованиям ФГОС ВО.

Материально-техническое обеспечение представлено в таблице 6.

Таблица 6 – Материально-техническое обеспечение

Наименование оборудованных учебных кабинетов	Адрес (местоположение) учебных кабинетов
Специальные помещения: Аудитории для проведения лекций: *Мультимедийная аудитория. (60 посадочных мест)*, оборудованная специализированной (учебной) мебелью (парта трехместная – 18 шт., парта двухместная – 6 шт, стол– 1 шт., доска аудиторная– 1 шт.), учебное ПК (монитор + системный блок), мультимедийная стойка с оборудованием – 1 шт., широкоформатный экран. *Компьютерные классы (22 посадочных места),* оборудованный учебной мебелью, компьютерами с неограниченным доступом к сети Интернет, включая доступ к ЭБС:	ауд. *207* корп. *4* ауд. *217* корп. *3* ауд. *211* корп. *4*

Лист согласования РПД

Разработал:
ст. преподаватель кафедры
интеллектуальных систем и
информационной безопасности
(должность)

(подпись) А.С. Закутный (Ф.И.О.)

И.о. заведующего кафедрой
интеллектуальных систем и
информационной безопасности
(наименование кафедры)

(подпись) Е.Е. Бизянов (Ф.И.О.)

Протокол № 1 заседания кафедры от 27.08. 2024г.

И.о. декана факультета
информационных технологий
и автоматизации производственных
процессов:
(наименование факультета)

(подпись) В.В. Дьячкова (Ф.И.О.)

Согласовано

Председатель методической
комиссии по специальности 10.05.03
Информационная безопасность
автоматизированных систем

(подпись) Е.Е. Бизянов (Ф.И.О.)

Начальник учебно-методического центра

(подпись) О.А. Коваленко (Ф.И.О.)

Лист изменений и дополнений

Номер изменения, дата внесения изменения, номер страницы для внесения изменений	
ДО ВНЕСЕНИЯ ИЗМЕНЕНИЙ:	ПОСЛЕ ВНЕСЕНИЯ ИЗМЕНЕНИЙ:
Основание:	
Подпись лица, ответственного за внесение изменений	