МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное бюджетное образовательное учреждение высшего образования "Российский государственный геологоразведочный университет имени Серго Орджоникидзе"

(МГРИ)

СПЕЦИАЛИЗАЦИЯ
Методы интеллектуального анализа данных в обеспечении информационной безопасности

рабочая программа дисциплины (модуля)

Закреплена за кафедрой **Промышленной кибербезопасности и защиты геоданных**

Учебный план s100503_25_BZO25.plx
Специальность 10.05.03 Информационная безопасность автоматизированных систем

Квалификация **Специалист по защите информации**

Форма обучения **очная**

Общая трудоемкость **4 ЗЕТ**

Часов по учебному плану	144	Виды контроля в семестрах:
в том числе:		экзамены 11
аудиторные занятия	58,35	
самостоятельная работа	58,65	
часов на контроль	27	

Распределение часов дисциплины по семестрам

Семестр (<Курс>.<Семестр на курсе>)	**11 (6.1)**		Итого	
Недель	14			
Вид занятий	УП	РП	УП	РП
Лекции	28	28	28	28
Практические	28	28	28	28
Иные виды контактной работы	2,35	2,35	2,35	2,35
В том числе инт.	4	4	4	4
Итого ауд.	58,35	58,35	58,35	58,35
Контактная работа	58,35	58,35	58,35	58,35
Сам. работа	58,65	58,65	58,65	58,65
Часы на контроль	27	27	27	27
Итого	144	144	144	144

Москва 2025

1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)	
1.1	Глобальной целью изучения дисциплины «Методы интеллектуального анализа данных в обеспечении информационной безопасности» является углубление общего информационного образования и информационной культуры студентов, а также формирование базовых практических знаний и навыков для проведения исследований, разработок и применение технологий , направленных на обеспечении информационной безопасности автоматизированных систем и значимых объектов критической информационной инфраструктуры,
1.2	Основная задача
1.3	– изучение и освоение навыков разработки алгоритмов анализа данных в системах информационной безопасности, решения основных задач интеллектуального анализа данных
1.4	– классификации, регрессии, прогнозирования, кластеризации, определения взаимосвязей, анализа отклонений, выбора архитектуры нечётких моделей и сетей для задач анализа и моделирования информационных процессов, выбора методов проведения и обработки экспериментальных исследований для создания математических моделей адекватных окружающему миру и решения прикладных задач.

2. МЕСТО ДИСЦИПЛИНЫ (МОДУЛЯ) В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ	
Цикл (раздел) ОП:	Б1.В.10
2.1	**Требования к предварительной подготовке обучающегося:**
2.1.1	Электродинамика и распространение радиоволн
2.1.2	Современные киберугрозы в промышленных и корпоративных системах автоматизации
2.1.3	Электромагнитные поля и волны
2.1.4	Автоматизированные системы управления
2.1.5	Практикум по решению проектных задач профессиональной деятельности
2.1.6	Инженерно-техническая защита информации и технические средства охраны
2.1.7	Цифровая обработка сигналов в системах обеспечения информационной безопасности автоматизированных систем управления
2.1.8	Производственная практика (научно-исследовательская работа)
2.1.9	Основы радиотехники
2.1.10	Практикум по решению научно-исследовательских задач профессиональной деятельности
2.1.11	Прикладные виды спорта
2.1.12	Практикум по решению эксплуатационных задач профессиональной деятельности
2.2	**Дисциплины (модули) и практики, для которых освоение данной дисциплины (модуля) необходимо как предшествующее:**

3. КОМПЕТЕНЦИИ ОБУЧАЮЩЕГОСЯ, ФОРМИРУЕМЫЕ В РЕЗУЛЬТАТЕ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)	
ПК-1: Способен моделировать защищенные автоматизированные системы с целью анализа их уязвимостей и эффективности средств и способов защиты информации	
Знать:	
Уровень 1	методы проведения физических исследований, технические и программные средства, применяемые при анализе электромагнитных полей и волн; уравнения и законы электродинамики и распространения радиоволн; модели элементарных излучателей; основные типы антенн, применяемых при анализе электромагнитных полей; принципы построения и функционирования, примеры реализаций современных локальных и глобальных компьютерных сетей и их компонентов;
Уровень 2	назначение, функции и структуру информационных и библиографических систем; методы поиска, изучения и обобщения научно-технической литературы, нормативных и методических материалов; основные методы исследования по теме своей научно- исследовательской работы; основы теории цифровой обработки сигналов как теоретической базы для разработки и исследования методов обработки, приема и передачи данных в системах обеспечения информационной безопасности автоматизированных систем управления; актуальные угрозы информационной безопасности промышленных компаний, текущее состояние и эволюцию киберугроз как ответную реакцию на внедрение средств и мер информационной безопасности; цели и задачи автоматизации управления, общие понятия автоматизированных систем управления (АСУ), жизненный цикл, функции и виды АСУ
Уровень 3	состав автоматизированных систем управления технологическим процессом (АСУ ТП), виды обеспечения, классификацию и уровни управления АСУ ТП, место АСУ ТП в интегрированных системах управления; области задач организации информационных технологий и современные инструменты построения интеллектуальных систем, обеспечивающих информационную безопасность; основные принципы и проблематику теории обучения машин, основные современные методы обучении по

	прецедентам — классификации, кластеризации и регрессии; принципы организации информационных систем в соответствии с требованиями по защите информации; основные способы кодирования информации в автоматизированных системах управления (АСУ), обеспечивающие максимальную надежность и высокую скорость при ее передаче по каналам связи (коды: линейные, циклические, БЧХ, Хэмминга, Шеннона - Фано и Хаффмана); уязвимости современных АСУ ТП, подходы к устранению уязвимостей и построению системы защиты современных АСУ ТП; основные виды математических моделей информационных потоков и систем защиты информации и методы их построения
Уметь:	
Уровень 1	использовать методы проведения физических исследований, технические и программные средства для анализа электромагнитных полей технических средств автоматизированных систем; использовать методы исследования электромагнитных полей для оценки физических характеристик технических средств автоматизированных систем; определять типы субъектов доступа и объектов доступа, являющихся объектами защиты; определять методы управления доступом, типы доступа и правила разграничения доступа к объектам доступа, подлежащим реализации в автоматизированной системе; определять параметры информационной системы и ее структуру в соответствии с заданными функциями;
Уровень 2	составлять обзоры по вопросам обеспечения информационной безопасности по теме своей научно-исследовательской работы; применять методы исследования по теме своей научно-исследовательской работы; формировать математическое описание дискретных систем в виде алгоритмов; выполнять компьютерное моделирование дискретных систем на основе их математического описания; анализировать и оценивать риски информационной безопасности в промышленных и корпоративных системах автоматизации; анализировать и моделировать информационные процессы, протекающие в системах промышленной автоматизации; формулировать основные задачи, возникающие при анализе данных, пути их решения, выбирать адекватные алгоритмы решения задачи анализа данных, оценивать качество получаемых решений, обеспечивающих информационную безопасность;
Уровень 3	формализовать постановки прикладных задач анализа данных, применять основные методы создания алгоритмов интеллектуального анализа данных в системах информационной безопасности, такие как классификация, кластеризация и прогнозирование; оценивать информационные риски в информационных системах; решать типовые задачи кодирования и декодирования информации с использованием математических методов и моделей; анализировать структуры АСУ ТП, строить их модели, оценивать риски функциональной безопасности, распознавать атаки социальной инженерии; на основе опытных данных и технических характеристик автоматизированной системы управления (АСУ) строить адекватную математическую модель, связанную с системой защиты информации в АСУ
Владеть:	
Уровень 1	навыком применения методик исследования электромагнитных полей; навыком применения исследовательских методов электродинамики и распространения радиоволн; навыками поиска и изучения научно-технической литературы, а также изложения и оформления результатов своей научно- исследовательской работы; навыком составления математических моделей дискретных систем и сигналов;
Уровень 2	навыком разработки алгоритмов цифровой обработки сигналов в системах информационной безопасности; навыком выбора методов проведения и обработки экспериментальных исследований, оформления научно-технических отчётов, обзоров, докладов, статей; навыком выбора и обоснованием критериев эффективности функционирования защищенных информационных систем
Уровень 3	навыком применения помехоустойчивых шифров и кодов, повышающих скорость передачи информации в АСУ; навыком разработки политик безопасности современных промышленных систем автоматизации, исследования сетевых пакетов в промышленной сети; навыком применения математических моделей для построения системы защиты информации в АСУ и оценки ее эффективности

ПК-2: Способен разрабатывать проектные решения по защите информации в автоматизированных системах	
Знать:	
Уровень 1	навыком применения помехоустойчивых шифров и кодов, повышающих скорость передачи информации в АСУ; навыком разработки политик безопасности современных промышленных систем автоматизации, исследования сетевых пакетов в промышленной сети; навыком применения математических моделей для построения системы защиты информации в АСУ и оценки ее эффективности

Уровень 2	основные принципы проектирования систем инженерно-технической защиты объектов; принципы построения и функционирования, примеры реализаций современных локальных и глобальных компьютерных сетей и их компонентов; основные методы создания алгоритмов интеллектуального анализа данных в системах информационной безопасности, такие как классификация, кластеризация и прогнозирование
Уровень 3	базовые алгоритмы анализа данных: k-средних, метод опорных векторов, линейная регрессия, ассоциативные правила, деревья решений, анализ выбросов или анализ аномалий, искусственные нейронные сети; меры, операции и приемы, направленные на предотвращение утечки защищаемой информации, несанкционированного и непреднамеренного воздействия на защищаемую информацию в сферах федерального, регионального управления и электронной коммерции; основные этапы реализации проектных решений в области автоматизированных систем электронного документооборота
Уметь:	
Уровень 1	определять параметры настройки программного обеспечения системы защиты информации автоматизированной системы; обоснованно оценивать необходимые параметры дискретизации и квантования, интерполяции и децимации сигналов; объяснять принцип методов оценки параметров сигналов, используемых в системах обеспечения информационной безопасности автоматизированных систем управления; изучать научно-техническую информацию, отечественный и зарубежный опыт и организовывать работы по практическому использованию новых технологий в области цифровой обработки сигналов
Уровень 2	проводить анализ вероятных угроз охраняемому объекту; выбирать наиболее рациональные методы противодействия угрозам охраняемому объекту; выбирать технические средства для решения задачи охраны объекта; определять виды и типы средств защиты информации, обеспечивающих реализацию технических мер защиты информации; реализовывать в виде программного кода базовые алгоритмы анализа данных: k- средних, метод опорных векторов, линейная регрессия, ассоциативные правила, искусственные нейронные сети
Уровень 3	способы построения систем с нечеткой логикой; изучать научно-техническую информацию, отечественный и зарубежный опыт и организовывать работы по практическому использованию новых технологий в области интеллектуального анализа данных; вырабатывать и принимать организационно- технические решения, адекватные степени угроз, в различных отраслях деятельности; разрабатывать защищенные системы электронного документооборота
Владеть:	
Уровень 1	навыком применения типовых прикладных пакетов для синтеза алгоритмов цифровой обработки сигналов, используемых в системах обеспечения информационной безопасности автоматизированных систем управления; навыком разработки проектов нормативных документов, регламентирующих работу по защите информации
Уровень 2	навыком разработки алгоритмов интеллектуального анализа данных в системах информационной безопасности; навыком разработки предложений по совершенствованию систем информационной безопасности предприятий и организаций, комплексно обеспечивающих повышение ее уровня
Уровень 3	навыком разработки и анализом проектных решений в области автоматизированных систем электронного документооборота

В результате освоения дисциплины (модуля) обучающийся должен

3.1	**Знать:**
3.1.1	методы проведения физических исследований, технические и программные средства, применяемые при анализе электромагнитных полей и волн;
3.1.2	цели и задачи автоматизации управления, общие понятия автоматизированных систем управления (АСУ), жизненный цикл, функции и виды АСУ;состав автоматизированных систем
3.1.3	управления технологическим процессом (АСУ ТП), виды обеспечения, классификацию и уровни управления АСУ ТП, место АСУ ТП в интегрированных системах управления, архитектуру промышленных сетей АСУ ТП;
3.1.4	основные криптографические методы, алгоритмы, протоколы, используемые для защиты информации в автоматизированных системах;
3.1.5	актуальные угрозы информационной безопасности промышленных компаний, текущее состояние и эволюцию киберугроз как ответную реакцию на внедрение средств и мер информационной безопасности, типы современных киберугроз в промышленных и корпоративных системах автоматизации, актуальные векторы атак на промышленные сети АСУ ТП;средства и меры информационной безопасности, применяемые в промышленных и корпоративных системах автоматизации;
3.1.6	принципы построения и функционирования, примеры реализаций современных локальных и глобальных компьютерных сетей и их компонентов;

3.1.7	цели и задачи проектирования систем инженерно-технической защиты объектов;основные понятия и терминологию, принятые в проектировании систем инженерно- технической защиты объектов;основные принципы проектирования систем инженерно- технической защиты объектов, физические принципы, на которых строятся системы инженерно-технической защиты объектов;
3.1.8	основы теории цифровой обработки сигналов как теоретической базы для разработки и исследования методов обработки, приема и передачи данных в системах обеспечения
3.1.9	информационной безопасности автоматизированных систем управления, основные алгоритмы при цифровой обработке сигналов, факторы, определяющие связь эксплуатационных свойств систем цифровой обработки сигналов с их техническими характеристиками;
3.1.10	уравнения и законы электродинамики и распространения радиоволн; модели элементарных излучателей; основные типы антенн, применяемых при анализе электромагнитных полей;
3.1.11	назначение, функции и структуру информационных и библиографических систем;методы поиска, изучения и обобщения научно-технической литературы, нормативных и методических материалов;основные методы исследования по теме своей научно- исследовательской работы;
3.2	**Уметь:**
3.2.1	использовать методы проведения физических исследований, технические и программные средства для анализа электромагнитных полей технических средств автоматизированных систем;
3.2.2	анализировать и моделировать информационные процессы, протекающие в системах промышленной автоматизации, применять методы и средства регистрации, записи и хранения значимых параметров потоков данных АСУ ТП;
3.2.3	определять параметры настройки программного обеспечения системы защиты информации автоматизированной системы;
3.2.4	анализировать и оценивать риски информационной безопасности в промышленных и корпоративных системах автоматизации, проводить аналитику современных киберугроз в
3.2.5	промышленных и корпоративных системах автоматизации, актуальные векторы атак на промышленные сети АСУ ТП;
3.2.6	определять типы субъектов доступа и объектов доступа, являющихся объектами защиты;определять методы управления доступом, типы доступа и правила разграничения доступа к объектам доступа, подлежащим реализации в автоматизированной системе;
3.2.7	проводить анализ вероятных угроз охраняемому объекту;выбирать наиболее рациональные методы противодействия угрозам охраняемому объекту;выбирать технические средства для
3.2.8	решения задачи охраны объекта, проводить оптимизацию структуры комплексов инженерно- технической защиты объектов;
3.2.9	формировать математическое описание дискретных систем в виде алгоритмов; выполнять компьютерное моделирование дискретных систем на основе их математического описания, обоснованно оценивать необходимые параметры дискретизации и квантования, интерполяции и децимации сигналов;объяснять принцип методов оценки параметров сигналов, используемых в системах обеспечения информационной безопасности автоматизированных систем управления;изучать научно-техническую информацию, отечественный и зарубежный опыт и организовывать работы по практическому использованию новых технологий в области цифровой обработки сигналов;
3.2.10	использовать методы исследования электромагнитных полей для оценки физических характеристик технических средств автоматизированных систем;
3.2.11	определять параметры информационной системы и ее структуру в соответствии с заданными функциями;составлять обзоры по вопросам обеспечения информационной безопасности по
3.2.12	теме своей научно-исследовательской работы;применять методы исследования по теме своей научно-исследовательской работы;
3.3	**Владеть:**
3.3.1	применения методик исследования электромагнитных полей;
3.3.2	определения ключевых точек мониторинга значимых параметров потоков данных, распределенных в информационной системе промышленных сетей АСУ ТП;
3.3.3	идентификации и моделирования каналов возможного деструктивного информационно-технического воздействия в промышленных и корпоративных системах автоматизации, оценки уязвимостей по отношению к современным киберугрозам промышленных сетей АСУ ТП;
3.3.4	анализа критериев оценки параметров технических средств охраны объектов;составления программы испытаний систем инженерно-технической защиты объектов;
3.3.5	составления математических моделей дискретных систем и сигналов;разработки алгоритмов цифровой обработки сигналов в системах информационной безопасности;выбора методов проведения и обработки экспериментальных исследований, оформления научно-технических отчётов, обзоров, докладов, статей, применения типовых прикладных пакетов для синтеза алгоритмов цифровой обработки сигналов, используемых в системах обеспечения информационной безопасности автоматизированных систем управления;

3.3.6	применения исследовательских методов электродинамики и распространения радиоволн;
3.3.7	навыками поиска и изучения научно-технической литературы, а также изложения и оформления результатов своей научно-исследовательской работы;

4. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

Код занятия	Наименование разделов и тем /вид занятия/	Семестр / Курс	Часов	Компетен-ции	Литература	Инте ракт.	Примечание
	Раздел 1. Введение в интеллектуальный анализ данных в обеспечении информационной безопасности.						
1.1	Введение в интеллектуальный анализ данных в обеспечении информационной безопасности. Предмет дисциплины: основные цели и задачи, средства и методы ИАД. Сведения о развитии теории анализа и интерпретации данных. /Лек/	11	1	ПК-1 ПК-2	Л1.1 Л1.2Л2.1	0	
	Раздел 2. Классификация и кластерный анализ данных						
2.1	Задачи и методы классификации данных. Методы ближайшего соседа и k-ближайшего соседа. Метод опорных векторов. Байесовская классификация . Линейная регрессия. /Лек/	11	1	ПК-1 ПК-2	Л1.1 Л1.2Л2.1	0	
2.2	Задачи и методы кластерного анализа данных. Иерархические методы кластерного анализа. Не иерархические методы кластерного анализа, /Лек/	11	1	ПК-1 ПК-2	Л1.1 Л1.2Л2.1	0	
2.3	Построение линейной регрессия данных. Решение задачи двух классовой классификации данных. /Пр/	11	4	ПК-1 ПК-2	Л1.1 Л1.2Л2.1	0	
2.4	Исследование метода иерархического агломеративного кластерного анализа данных. /Пр/	11	4	ПК-1 ПК-2	Л1.1 Л1.2Л2.1	2	
	Раздел 3. Обнаружение логических закономерностей и деревья решений. Случайный лес						
3.1	Обнаружение логических закономерностей. Линейная регрессия. Корреляционно-регрессионный анализ Методы поиска ассоциативных правил, в том числе алгоритм Apriori. /Лек/	11	2	ПК-1 ПК-2	Л1.1 Л1.2Л2.1	0	
3.2	Деревья решений, деревья решающих правил, деревья классификации и регрессии.. Случайный лес. /Лек/	11	3	ПК-1 ПК-2	Л1.1 Л1.2Л2.1	0	
3.3	Исследование метода поиска ассоциативных правил с использованием алгоритма Apriori. /Пр/	11	2	ПК-1 ПК-2	Л1.1 Л1.2Л2.1	0	
3.4	Исследование алгоритма "случайного леса" на множестве решающих деревьев. /Пр/	11	2	ПК-1 ПК-2	Л1.1 Л1.2Л2.1	0	
3.5	Подготовка к практическим занятиям /Ср/	11	30	ПК-1 ПК-2	Л1.1 Л1.2Л2.1	0	
	Раздел 4. Методы прогнозирования временных рядов.						
4.1	Обзор методов прогнозирования временных рядов. Анализ временных рядов (динамические модели и прогнозирование). /Лек/	11	2	ПК-1 ПК-2	Л1.1 Л1.2Л2.1	0	

4.2	Применение методов прогнозирования временных рядов данных в задачах обнаружения аномалий функционирования автоматизированных систем управления техническими процессами. /Лек/	11	2	ПК-1 ПК-2	Л1.1 Л1.2Л2.1	0	
4.3	Построение параметрических моделей прогнозирования временных рядов. /Пр/	11	2	ПК-1 ПК-2	Л1.1 Л1.2Л2.1	0	
4.4	Исследование параметрических моделей прогнозирования временных рядов для обнаружения аномалий в рядах данных. /Пр/	11	2	ПК-1 ПК-2	Л1.1 Л1.2Л2.1	0	
	Раздел 5. Искусственные нейронные сети в интеллектуальном анализе данных в задачах обеспечения информационной безопасности.						
5.1	Искусственные нейронные сети в задачах обеспечении информационной безопасности. Этапы решения практических задач с использованием нейронных сетей. Решение задач идентификации, прогнозирования и других с помощью искусственных нейронных сетей /Лек/	11	2	ПК-1 ПК-2	Л1.1 Л1.2Л2.1	0	
5.2	Формальная модель нейрона. Рекуррентные нейронные сети. Сеть Элмана. Нейронные сети - радиальные базисные сети (РБС). Архитектура сети РБФ. Нейронные сети - сети регрессии, вероятностные НС. /Лек/	11	2	ПК-1 ПК-2	Л1.1 Л1.2Л2.1	0	
5.3	Архитектура сети Кохонена. Самоорганизующаяся карта Кохонена /Лек/	11	2	ПК-1 ПК-2	Л1.1 Л1.2Л2.1	0	
5.4	Сверточная нейронная сеть. Генеративные состязательные сети. Автоэнкодер (автокодировщик). Глубокие нейронные сети. /Лек/	11	2	ПК-1 ПК-2	Л1.1 Л1.2Л2.1	0	
5.5	Исследование работы нейронной сети - Персептрона. /Пр/	11	2	ПК-1 ПК-2	Л1.1 Л1.2Л2.1	1	
5.6	Исследование работы рекуррентной нейронной сети Элмана. /Пр/	11	2	ПК-1 ПК-2	Л1.1 Л1.2Л2.1	0	
5.7	Исследование работы нейронной сети самоорганизующейся карты Кохонена. /Пр/	11	2	ПК-1 ПК-2	Л1.1 Л1.2Л2.1	1	
5.8	Исследование работы нейронной сети автоэнкодера (автокодировщика). /Пр/	11	2	ПК-1 ПК-2	Л1.1 Л1.2Л2.1	0	
	Раздел 6. Системы на основе нечёткой логики в интеллектуальном анализе данных в задачах обеспечения информационной безопасности.						
6.1	Базовые понятия нечеткой логики. /Лек/	11	2	ПК-1 ПК-2	Л1.1 Л1.2Л2.1	0	
6.2	Логико-лингвистические модели. /Лек/	11	2	ПК-1 ПК-2	Л1.1 Л1.2Л2.1	0	
6.3	Типовые структуры систем нечеткой логики. /Лек/	11	2	ПК-1 ПК-2	Л1.1 Л1.2Л2.1	0	

6.4	Применение нечеткой логики в системах обеспечении информационной безопасности. /Лек/	11	2	ПК-1 ПК-2	Л1.1 Л1.2Л2.1	0	
6.5	4 /Пр/	11	0	ПК-1 ПК-2	Л1.1 Л1.2Л2.1	0	
6.6	Исследование работы гибридной искусственной нечёткой нейронной сети. /Пр/	11	4	ПК-1 ПК-2	Л1.1 Л1.2Л2.1	0	
6.7	Подготовка к экзамену /Ср/	11	28,65	ПК-1 ПК-2	Л1.1 Л1.2Л2.1	0	
6.8	экзамен /ИВКР/	11	2,35	ПК-1 ПК-2	Л1.1 Л1.2Л2.1	0	

5. ОЦЕНОЧНЫЕ СРЕДСТВА

5.1. Контрольные вопросы и задания

Тема 1: Введение в интеллектуальный анализ данных (ИАД) в ИБ
1. Что такое интеллектуальный анализ данных и каково его значение в информационной безопасности?
2. Какие цели и задачи решаются с помощью ИАД в системах защиты информации?
3. Какие основные этапы анализа данных выделяются в практике ИБ?
4. Какие средства и методы используются в ИАД?
5. Как развивались методы анализа и интерпретации данных?
Тема 2: Методы классификации данных
6. Что такое задача классификации в контексте ИБ?
7. Как работает алгоритм ближайшего соседа (kNN)?
8. Что представляет собой метод опорных векторов (SVM) и где он применяется?
9. Как реализуется байесовская классификация в задачах обнаружения угроз?
10. Как используется линейная регрессия для решения задач классификации?
Тема 3: Кластерный анализ и обнаружение закономерностей
11. Что такое кластеризация и как она используется в ИБ?
12. Как работают иерархические методы кластеризации?
13. Как функционируют неиерархические методы (например, k-means)?
14. Что такое обнаружение логических закономерностей и зачем оно нужно?
15. Как корреляционно-регрессионный анализ помогает в выявлении аномалий?
Тема 4: Поиск ассоциативных правил
16. Что такое ассоциативные правила и как они формируются?
17. Как работает алгоритм Apriori и какие метрики использует?
18. Как ассоциативные правила могут использоваться при анализе инцидентов ИБ?
19. Как строить модели поведения на основе ассоциаций событий?
20. Какие ограничения имеют методы поиска ассоциативных правил?
Тема 5: Деревья решений и ансамбли
21. Что такое дерево решений и как оно строится?
22. Чем отличаются деревья классификации от деревьев регрессии?
23. Как происходит выбор разбиения узлов дерева?
24. Что такое случайный лес и почему он эффективен?
25. Как ансамблевые методы повышают точность моделей?
Тема 6: Прогнозирование временных рядов
26. Что такое временной ряд и как он формируется из логов ИС?
27. Какие методы прогнозирования временных рядов наиболее популярны?
28. Как строятся ARIMA и SARIMA модели?
29. Как используются динамические модели для предсказания инцидентов ИБ?
30. Как прогнозирование временных рядов помогает в обнаружении аномалий?
Тема 7: Применение прогнозирования в АСУ ТП
31. Как анализ временных рядов применяется к данным АСУ ТП?
32. Какие особенности имеет прогнозирование в реальном времени?
33. Какие аномалии можно обнаружить с помощью временного анализа?
34. Какие проблемы возникают при работе с промышленными данными?
35. Как обучать модели на потоковых данных АСУ ТП?
Тема 8: Искусственные нейронные сети (ИНС) в ИБ
36. Какие задачи ИБ решаются с помощью нейронных сетей?
37. Какие этапы подготовки данных и обучения модели выделяются?
38. Как используются ИНС для идентификации, прогнозирования и анализа инцидентов?
39. Как организовать сбор и подготовку данных для обучения ИНС?
40. Как оценить качество и обобщающую способность нейросетевой модели?
Тема 9: Архитектуры искусственных нейронных сетей

41. Что такое формальная модель нейрона?
42. Как работают рекуррентные нейронные сети и сеть Элмана?
43. Что представляют собой радиально-базисные сети (RBF)?
44. Как устроена сеть регрессии и вероятностная нейросеть?
45. Какие особенности работы самоорганизующихся карт Кохонена?

Тема 10: Глубокое обучение и специализированные архитектуры

46. Что такое свёрточная нейронная сеть и где она применяется?
47. Как работают генеративно-состязательные сети (GAN) в задачах ИБ?
48. Что такое автоэнкодеры и как они используются для детекции аномалий?
49. Какие задачи решаются с помощью глубоких нейронных сетей?
50. Как использовать нейросети для обработки неструктурированных данных?

Тема 11: Нечёткая логика в задачах ИБ

51. Что такое нечёткая логика и чем она отличается от классической?
52. Какие базовые понятия нечёткой логики используются?
53. Что такое лингвистическая переменная и как она задаётся?
54. Как строятся логико-лингвистические модели?
55. Какие типовые структуры систем нечёткой логики существуют?

Тема 12: Применение нечёткой логики в ИБ

56. Как нечёткая логика может быть использована для оценки рисков?
57. Как строить системы принятия решений с нечёткой логикой?
58. Как нечёткие модели помогают при анализе неопределённых данных?
59. Как интегрируются нечёткие системы с другими методами анализа?
60. Какие примеры применения нечёткой логики в системах ИБ известны?

Тема 13: Обнаружение аномалий и автоматизация ИБ

61. Как методы ИАД используются для обнаружения аномалий?
62. Как осуществляется мониторинг и выявление нестандартного поведения?
63. Какие модели применяются для анализа поведения пользователей (UEBA)?
64. Как машинное обучение помогает в обнаружении вторжений?
65. Какие подходы к автоматизации реагирования на основе анализа данных?

Тема 14: Практическое применение методов ИАД в системах ИБ

66. Какие практические задачи ИБ решаются с помощью ИАД?
67. Как ИАД используется в системах DLP и SIEM?
68. Как классифицировать вредоносный трафик с помощью ML?
69. Как распознавать фишинг и мошенничество с помощью моделей?
70. Как использовать ИАД для анализа журналов безопасности и выявления инцидентов?

5.2. Темы письменных работ

не предусмотрены

5.3. Оценочные средства

Рабочая программа "Методы интеллектуального анализа данных в обеспечении информационной безопасности" обеспечена оценочными средствами для проведения текущего контроля и промежуточной аттестации, включающими контрольные вопросы для проведения промежуточной аттестации, критерии оценивания учебной деятельности обучающихся по балльно-рейтинговой системе, примеры заданий для практических и лабораторных занятий, билеты для проведения промежуточной аттестации.
Все оценочные средства представлены в Приложении 1.

5.4. Перечень видов оценочных средств

Оценочные средства разработаны для всех видов учебной деятельности студента - лекций, практических занятий, самостоятельной работы и промежуточной аттестации. Оценочные средства представлены в виде:
- средства текущего контроля: проверочных работ по решению задач, дискуссии по теме;
- средств итогового контроля - промежуточной аттестации: экзамена в 11 семестре.

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

6.1. Рекомендуемая литература

6.1.1. Основная литература

	Авторы, составители	Заглавие	Издательство, год
Л1.1	Косников С. Н., Золкин А. Л., Ахмадуллин Ф. Р., Урусова А. Б., Малова Н. Н., Поскряков И. А., Вербицкий Р. А.	Основы анализа данных и интеллектуальные системы: учебное пособие для вузов	Санкт-Петербург: Лань, 2025
Л1.2	Митяков Е. С., Шмелева А. Г., Ладынин А. И.	Искусственный интеллект и машинное обучение: учебное пособие для вузов	Санкт-Петербург: Лань, 2025

6.1.2. Дополнительная литература			
	Авторы, составители	Заглавие	Издательство, год
Л2.1	Затонский А. В., Тугашова Л. Г.	Моделирование объектов управления в MatLab: учебное пособие	Санкт-Петербург: Лань, 2022
6.3.1 Перечень программного обеспечения			
6.3.1.1	Office Professional Plus 2019		
6.3.1.2	Windows 10		
6.3.1.3	МТС-Линк	Комплексная платформа для коммуникаций, обучения и совместной работы, разработанная с использованием современных технологий. Доступны десктопные и мобильные приложения для удобной работы с системой.	
6.3.2 Перечень информационных справочных систем			
6.3.2.1	База данных научных электронных журналов "eLibrary"		
6.3.2.2	Электронно-библиотечная система "Лань" Доступ к коллекциям электронных изданий ЭБС "Издательство "Лань"		
6.3.2.3	Электронно-библиотечная система «Книжный Дом Университета» ("БиблиоТех")		

7. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)			
Аудитория	Назначение	Оснащение	Вид
5	Помещение № 5 для самостоятельной работы обучающихся	Письменный стол обучающегося; Стул обучающегося; Письменный стол обучающегося с ограниченными возможностями здоровья; Стул обучающегося с ограниченными возможностями здоровья; Ноутбук с возможностью подключения к сети «Интернет» и обеспечением доступа к электронной информационно-образовательной среде лицензиата; Моноблок (в том числе, клавиатура, мышь, наушники) с возможностью подключения к сети «Интернет» и обеспечением доступа к электронной информационно-образовательной среде	

6-25	Специализированная многофункциональная лаборатория № 6-25 для проведения практических и лабораторных занятий, текущего контроля и промежуточной/ итоговой аттестации, в том числе для организации практической подготовки обучающихся	Компьютерные столы; Стулья; Письменный стол педагогического работника; Стул педагогического работника; Магнитно-маркерная доска; Мультимедийный проектор; Экран; ПК с возможностью подключения к сети «Интернет» и обеспечением доступа к электронной информационно-образовательной среде лицензиата; Телекоммуникационные шкафы; Средства отображения информации. Стенды сетей передачи информации с коммутацией пакетов и коммутацией каналов в составе: Учебный стенд "Основы IP-сетей" (маршрутизаторы, коммутаторы L2/L3); Учебный стенд "Виртуальные сети (VLAN, VPN)"; Учебный стенд "Беспроводные сети (Wi-Fi, IoT)"; Учебный стенд "Телефония (ISDN, VoIP)"; Учебный стенд "Оптические сети (PON, DWDM)"; Стенд "Цифровые системы передачи (E1, SDH)". Стенды для изучения проводных и беспроводных компьютерных сетей в составе: абонентские устройства; коммутаторы; маршрутизаторы; точкидоступа, межсетевые экраны; средства обнаружения компьютерных атак; системы углубленной проверки сетевых пакетов; системы защиты от утечки данных; анализаторы кабельных сетей. Учебно-лабораторные комплексы в составе: Учебный лабораторный комплекс контроля сетевой безопасности (системы обнаружения вторжений и анализа защищенности, сетевые сканеры). Учебный лабораторный комплекс проведения анализа защищенности значимого объекта КИИ на соответствие	

		требованиям по обеспечению безопасности. Учебный лабораторный комплекс для обеспечения исследований специального программного обеспечения и аппаратного СЗИ в составе: средства защиты информации от НСД; программно-аппаратный комплекс доверенной нагрузки; антивирусные программные комплексы; межсетевые экраны; средства создания модели разграничения доступа; программа контроля полномочий доступа к информационным ресурсам; программа фиксации и контроля исходного состояния программного комплекса; программа поиска и гарантированного уничтожения информации на дисках; аппаратные средства аутентификации пользователя; системы обнаружения вторжений и анализа защищенности; средства анализа защищенности компьютерных сетей; сканеры безопасности; устройства чтения смарт-карт и радиометок; программно-аппаратные комплексы защиты информации; средства криптографической защиты информации. Учебный лабораторный комплекс для обеспечения исследований типовых сертифицированных программных и программно-технических средств защиты информации от НСД. Учебный лабораторный комплекс для обеспечения исследований сертифицированных средств в которых реализованы средства защиты информации от НСД. УЛК для проведения аттестационных испытаний автоматизированных систем от НСД по требованиям безопасности информации. Аппаратно-программные комплексы в составе: аппаратно-программные средства управления	

		доступом к данным; средства криптографической защиты информации; средства дублирования и восстановления данных; средства мониторинга состояния автоматизированных систем; средства контроля и управления доступом в помещения.	
Ауд. 8	Аудитория для научно-исследовательской работы обучающихся, курсового и дипломного проектирования № 8	Рабочие места на базе вычислительной техники с набором необходимых для проведения и оформления результатов исследований дополнительных аппаратных и/или программных средств; Письменный стол обучающегося; Стул обучающегося; Письменный стол обучающегося с ограниченными возможностями здоровья; Стул обучающегося с ограниченными возможностями здоровья; Ноутбук с возможностью подключения к сети «Интернет» и обеспечением доступа к электронной информационно-образовательной среде лицензиата; Моноблок (в том числе, клавиатура, мышь, наушники) с возможностью подключения к сети «Интернет» и обеспечением доступа к электронной информационно-образовательной среде; Многофункциональное устройство (принтер, сканер, ксерокс).	
1	Специализированная многофункциональная учебная аудитория № 1 для проведения учебных занятий лекционного и семинарского типов, групповых и индивидуальных консультаций, текущего контроля и промежуточной/ итоговой аттестации	Столы обучающихся; Стулья обучающихся; Письменный стол педагогического работника; Стул педагогического работника; Кафедра; Магнитно-маркерная доска; Мультимедийный проектор; Экран; Ноутбук с возможностью подключения к сети «Интернет» и обеспечением доступа к электронной информационно-образовательной среде	

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

Методические указания по изучению дисциплины "Методы интеллектуального анализа данных в обеспечении информационной безопасности" представлены в Приложении 2 и включают в себя:
1. Методические указания для обучающихся по организации учебной деятельности.

2. Методические указания по организации самостоятельной работы обучающихся.
3. Методические указания по организации процедуры оценивания знания, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций.