Документ подписан простой электронной подписью
Информация о владельце:
ФИО: Макаренко Елена Николаевна
Должность: ректор
Дата подписания: 24.04.2023 09:38:51
Уникальный программный ключ:
c098bc0c1041cb2a4cf926cf171d6715d99a6ae00adc8e27b55cbe1e2dbd7c78

Министерство науки и высшего образования Российской Федерации
Федеральное государственное бюджетное образовательное учреждение высшего образования «Ростовский государственный экономический университет (РИНХ)»

УТВЕРЖДАЮ
Директор Института магистратуры
_____ Иванова Е.А.
«29» 08 2022 г.

Рабочая программа дисциплины
Фундаментальные методы интеллектуального анализа данных мониторинга безопасности

Направление 10.04.01 Информационная безопасность
магистерская программа 10.04.01.02 "Программно-аппаратные методы расследования компьютерных преступлений"

Для набора 2022 года

Квалификация
магистр

КАФЕДРА **Фундаментальная и прикладная математика**

Распределение часов дисциплины по семестрам

Семестр (<Курс>.<Семестр на курсе>)	**2 (1.2)**		Итого	
Недель	15 2/6			
Вид занятий	УП	РП	УП	РП
Лекции	16	16	16	16
Лабораторные	32	32	32	32
Итого ауд.	48	48	48	48
Контактная работа	48	48	48	48
Сам. работа	60	60	60	60
Часы на контроль	36	36	36	36
Итого	144	144	144	144

ОСНОВАНИЕ

Учебный план утвержден учёным советом вуза от 22.02.2022 протокол № 7.

Программу составил(и): д.ф.-м.н, проф., Сахарова Л.В. _____

Зав. кафедрой: к.э.н. Рутта Н.А. _____

Методическим советом направления: д.э.н., проф., Тищенко Е.Н. _____

1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

1.1	получение обучающимися систематизированных теоретических знаний о базовых принципах и методах построения интеллектуальных систем защиты информации, освоение ими типовых приемов решения практических задач защиты информации с использованием методов искусственного интеллекта, привитие базовых навыков анализа и проектирования интеллектуальных систем защиты информации с применением современных технологий интеллектуального анализа данных.

2. ТРЕБОВАНИЯ К РЕЗУЛЬТАТАМ ОСВОЕНИЯ ДИСЦИПЛИНЫ

ПК-4:Способен осуществлять анализ результатов экспериментальных исследований с применением математических и физических методов, выбор технических средств инструментального мониторинга защищенности объектов информатизации

В результате освоения дисциплины обучающийся должен:

Знать:

основные принципы, походы и новые методы экспериментальных исследования в профессиональной сфере, технические средства инструментального мониторинга защищенности объектов информатизации (соотнесено с индикатором ПК 4.1)

Уметь:

применять математические методы и технологии искусственного интеллекта в исследованиях процессов управления информационной безопасностью; анализировать различные подходы при решении задач обеспечения информационной безопасности (соотнесено с индикатором ПК 4.2)

Владеть:

навыками применения различных математических методов и технологий искусственного интеллекта в исследованиях процессов управления информационной безопасностью; методами анализа различных подходов при решении задач обеспечения информационной безопасности (соотнесено с индикатором ПК 4.3)

3. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

Код занятия	Наименование разделов и тем /вид занятия/	Семестр / Курс	Часов	Компетен-ции	Литература
	Раздел 1. Алгоритмы интеллектуального анализа данных: основные методы и понятия				
1.1	Общие сведения о методах анализа данных. Автоматическое извлечение знаний из больших наборов данных. Анализ данных в системах управления безопасностью. Изучение базовых методов: кластеризация, классификация, ассоциативные правила, дерево решений, линейная регрессия, наивный баессовский классификатор. Выбор подходящих атрибутов для анализа и методы снижения размерности задачи. /Лек/	2	2	ПК-4	Л1.1 Л1.2 Л1.3 Л1.9Л2.4 Л2.5 Л2.6
1.2	Общие сведения об алгоритмах нечеткой логики. Системы обнаружения вторжений, построенные с использование алгоритмов нечеткой логики. Общие сведения об экспертных системах ИБ. Построение экспертных систем с использованием модели нечеткой логики. Обучение экспертных систем на основе алгоритмов с учителем и без. /Лек/	2	2	ПК-4	Л1.8 Л1.9Л2.2 Л2.3 Л2.4 Л2.7
1.3	Общие сведения о биометрических системах. Идентификация пользователей на основе лица, голоса, отпечатка. Методика идентификации по цифровому отпечатку (fingerprint). Интеллектуальные алгоритмы идентификации пользователя по распознаванию контрольного изображения (CAPTHCHA). /Лек/	2	4	ПК-4	Л1.1 Л1.9Л2.4 Л2.5 Л2.6
1.4	Изучение алгоритма обратного распространения ошибки (метод Back Propagation) /Лаб/	2	2	ПК-4	Л1.5Л2.5 Л2.9
1.5	Алгоритмы классификации и кластеризации методами машинного обучения. /Лаб/	2	2	ПК-4	Л1.6Л2.5 Л2.8
1.6	Исследование рекуррентной нейронной сети Хопфилда на примере задачи распознавания образов /Лаб/	2	2	ПК-4	Л1.5 Л1.7 Л1.9Л2.1 Л2.5 Л2.6

1.7	Нейросетевые методы. /Лаб/	2	2	ПК-4	Л1.2Л2.4 Л2.5
1.8	Нечеткие алгоритмы контроля. /Лаб/	2	2	ПК-4	Л1.1 Л1.5 Л1.8Л2.2 Л2.10
1.9	Исследование рекуррентной нейронной сети Коско (BAM) на примере задачи распознавания образов /Лаб/	2	2	ПК-4	Л1.3 Л1.5Л2.1 Л2.3 Л2.8
1.10	Иммунные и генетические методы и алгоритмы ИБ /Лаб/	2	2	ПК-4	Л1.1 Л1.4Л2.7 Л2.8
1.11	Гибридные методы и алгоритмы ИБ. /Лаб/	2	2	ПК-4	Л1.4 Л1.5 Л1.6 Л1.7Л2.1 Л2.5 Л2.8
1.12	Общие сведения о методах анализа данных. Автоматическое извлечение знаний из больших наборов данных. Анализ данных в системах управления безопасностью. Изучение базовых методов: кластеризация, классификация, ассоциативные правила, дерево решений, линейная регрессия, наивный баессовский классификатор. Выбор подходящих атрибутов для анализа и методы снижения размерности задачи. /Ср/	2	10	ПК-4	Л1.1 Л1.3 Л1.9Л2.2 Л2.7 Л2.10
1.13	Общие сведения о биометрических системах. Идентификация пользователей на основе лица, голоса, отпечатка. Методика идентификации по цифровому отпечатку (fingerprint). Интеллектуальные алгоритмы идентификации пользователя по распознаванию контрольного изображения (CAPTHCHA). /Ср/	2	10	ПК-4	Л1.1 Л1.3 Л1.9Л2.2 Л2.7
1.14	Общие сведения об алгоритмах нечеткой логики. Системы обнаружения вторжений, построенные с использование алгоритмов нечеткой логики. Общие сведения об экспертных системах ИБ. Построение экспертных систем с использованием модели нечеткой логики. Обучение экспертных систем на основе алгоритмов с учителем и без. /Ср/	2	10	ПК-4	Л1.1 Л1.7Л2.2 Л2.7
	Раздел 2. Методы машинного обучения в информационной безопасности				
2.1	Нейронные сети. Классификация задач машинного обучения. Особенности применения методов машинного обучения в системах ИБ. Иерархические и неиерархические методы кластеризации. Методы поиска аномалий, основанные на кластеризации. Методы и системы на основе кластеризации и выбросов. Методы и системы на основе баз знаний и экспертные системы Применение технологий машинного обучения для решения задачи обнаружения вредоносных интернет-страниц /Лек/	2	2	ПК-4	Л1.1 Л1.5 Л1.6 Л1.7Л2.5 Л2.6 Л2.7 Л2.10
2.2	Нейросетевые методы. Нечеткие алгоритмы контроля. Искусственные нейронные сети (ИНС) в системах обнаружения атак. Принципы нейросетевого мониторинга безопасности. Применение ИНС в задачах классификации и кластеризации. Программные средство обнаружения сетевых атак с помощью ИНС. Комбинирование нейронных сетей для обнаружения атак на компьютерные системы. Системы обнаружения атак (СОА), основные способы построения. СОА на основе сигнатурного анализа. Обнаружение аномалий на основе нейронных сетей Гибридные средства классификации в СЗИ. Методы и системы на основе мягких вычислений /Лек/	2	2	ПК-4	Л1.1 Л1.3 Л1.5 Л1.7 Л1.8 Л1.9Л2.4 Л2.5 Л2.6 Л2.8 Л2.9

2.3	ИСЗИ на основе искусственных иммунных систем (ИИС). Иммунная система человека, механизмы функционирования. Обнаружение аномалий процессов с помощью механизмов иммунной системы. Системы антивирусной защиты на основе ИИС Алгоритмы построения и функционирования нейросетевой искусственной иммунной системы для обнаружения вредоносных программ. Интеграция искусственных иммунных и нейронных сетей для обнаружения вредоносных программ. Примеры работы иммунных систем ИБ. Использование генетических алгоритмов для обнаружения вторжений в сети. /Лек/	2	2	ПК-4	Л1.1 Л1.2 Л1.5 Л1.7Л2.2 Л2.3 Л2.4
2.4	Гибридные схемы обнаружения и классификации сетевых атак на основе комбинирования адаптивных классификаторов. /Лек/	2	2	ПК-4	Л1.2 Л1.7Л2.2 Л2.7
2.5	Разведочный анализ данных. /Лаб/	2	2	ПК-4	Л1.1 Л1.2 Л1.7Л2.2 Л2.7
2.6	Обработка пропусков в данных, кодирование категориальных признаков, масштабирование данных /Лаб/	2	2	ПК-4	Л1.1 Л1.7Л2.3 Л2.4
2.7	Подготовка обучающей и тестовой выборки, кросс-валидация и подбор гиперпараметров на примере метода ближайших соседей /Лаб/	2	2	ПК-4	Л1.1 Л1.2Л2.3 Л2.4 Л2.5
2.8	Линейные модели, SVM и деревья решений /Лаб/	2	2	ПК-4	Л1.1 Л1.9Л2.1 Л2.9
2.9	Исследование однослойных нейронных сетей на примере моделирования булевых выражений /Лаб/	2	2	ПК-4	Л1.5 Л1.6Л2.1 Л2.6
2.10	Применение однослойной нейронной сети для решения задач регрессии экспериментальных данных /Лаб/	2	2	ПК-4	Л1.6 Л1.7Л2.1 Л2.5
2.11	Применение однослойной нейронной сети с линейной функцией активации для прогнозирования временных рядов /Лаб/	2	2	ПК-4	Л1.5Л2.1 Л2.9
2.12	Исследование нейронных сетей с радиальными базисными функциями (RBF) на примере моделирования булевых выражений /Лаб/	2	2	ПК-4	Л1.6 Л1.7Л2.3 Л2.4
2.13	Нейронные сети. Классификация задач машинного обучения. Особенности применения методов машинного обучения в системах ИБ. Иерархические и неиерархические методы кластеризации. Методы поиска аномалий, основанные на кластеризации. Методы и системы на основе кластеризации и выбросов. Методы и системы на основе баз знаний и экспертные системы Применение технологий машинного обучения для решения задачи обнаружения вредоносных интернет-страниц /Ср/	2	8	ПК-4	Л1.2 Л1.3 Л1.8 Л1.9
2.14	Нейросетевые методы. Нечеткие алгоритмы контроля. Искусственные нейронные сети (ИНС) в системах обнаружения атак. Принципы нейросетевого мониторинга безопасности. Применение ИНС в задачах классификации и кластеризации. Программные средство обнаружения сетевых атак с помощью ИНС. Комбинирование нейронных сетей для обнаружения атак на компьютерные системы. Системы обнаружения атак (СОА), основные способы построения. СОА на основе сигнатурного анализа. Обнаружение аномалий на основе нейронных сетей Гибридные средства классификации в СЗИ. Методы и системы на основе мягких вычислений /Ср/	2	8	ПК-4	Л1.1 Л1.2 Л1.3 Л1.9Л2.1 Л2.2 Л2.5 Л2.7 Л2.8 Л2.10

2.15	ИСЗИ на основе искусственных иммунных систем (ИИС). Иммунная система человека, механизмы функционирования. Обнаружение аномалий процессов с помощью механизмов иммунной системы. Системы антивирусной защиты на основе ИИС Алгоритмы построения и функционирования нейросетевой искусственной иммунной системы для обнаружения вредоносных программ. Интеграция искусственных иммунных и нейронных сетей для обнаружения вредоносных программ. Примеры работы иммунных систем ИБ. Использование генетических алгоритмов для обнаружения вторжений в сети. /Ср/	2	8	ПК-4	Л1.1 Л1.2 Л1.8 Л1.9Л2.1 Л2.8 Л2.9
2.16	Гибридные схемы обнаружения и классификации сетевых атак на основе комбинирования адаптивных классификаторов. /Ср/	2	6	ПК-4	Л1.1 Л1.2 Л1.3Л2.1 Л2.5
2.17	/Экзамен/	2	36	ПК-4	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6 Л1.7 Л1.8 Л1.9Л2.1 Л2.2 Л2.3 Л2.4 Л2.5 Л2.6 Л2.7 Л2.8 Л2.9 Л2.10

4. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

Структура и содержание фонда оценочных средств для проведения текущей и промежуточной аттестации представлены в Приложении 1 к рабочей программе дисциплины.

5. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

5.1. Основная литература

	Авторы, составители	Заглавие	Издательство, год	Колич-во
Л1.1	Руденков Н. А., Пролетарский А. В., Смирнова Е. В., Суровов А. М.	Технологии защиты информации в компьютерных сетях	Москва: Национальный Открытый Университет «ИНТУИТ», 2016	https://biblioclub.ru/index.php?page=book&id=428820 неограниченный доступ для зарегистрированных пользователей
Л1.2		Вестник Института законодательства и правовой информации имени М.М. Сперанского: журнал	Иркутск: Институт законодательства и правовой информации, 2017	https://biblioclub.ru/index.php?page=book&id=457912 неограниченный доступ для зарегистрированных пользователей
Л1.3		Основы информационной безопасности	Москва: Интернет-Университет Информационных Технологий (ИНТУИТ), 2016	http://www.iprbookshop.ru/52209.html неограниченный доступ для зарегистрированных пользователей
Л1.4	Пальмов, С. В.	Интеллектуальный анализ данных: учебное пособие	Самара: Поволжский государственный университет телекоммуникаций и информатики, 2017	http://www.iprbookshop.ru/75376.html неограниченный доступ для зарегистрированных пользователей
Л1.5		Анализ данных. Часть 1. Подготовка данных к анализу: Учебное пособие	Москва: Московский городской педагогический университет, 2012	http://www.iprbookshop.ru/26444.html неограниченный доступ для зарегистрированных пользователей

	Авторы, составители	Заглавие	Издательство, год	Колич-во
Л1.6	Суворова, Г. М.	Информационная безопасность: учебное пособие	Саратов: Вузовское образование, 2019	http://www.iprbookshop.ru/86938.html неограниченный доступ для зарегистрированных пользователей
Л1.7	Шаньгин, В. Ф.	Информационная безопасность и защита информации	Саратов: Профобразование, 2019	http://www.iprbookshop.ru/87995.html неограниченный доступ для зарегистрированных пользователей
Л1.8	Яхъяева, Г. Э.	Нечеткие множества и нейронные сети: учебное пособие	Москва: Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2020	http://www.iprbookshop.ru/97552.html неограниченный доступ для зарегистрированных пользователей
Л1.9	Павлова, А. И.	Искусственные нейронные сети: учебное пособие	Москва: Ай Пи Ар Медиа, 2021	http://www.iprbookshop.ru/108228.html неограниченный доступ для зарегистрированных пользователей
5.2. Дополнительная литература				
	Авторы, составители	Заглавие	Издательство, год	Колич-во
Л2.1		Программные продукты и системы: журнал	Тверь: Центрпрограммсистем, 2017	https://biblioclub.ru/index.php?page=book&id=459225 неограниченный доступ для зарегистрированных пользователей
Л2.2	Башлы, П. Н., Бабаш, А. В., Баранова, Е. К.	Информационная безопасность и защита информации: учебное пособие	Москва: Евразийский открытый институт, 2012	http://www.iprbookshop.ru/10677.html неограниченный доступ для зарегистрированных пользователей
Л2.3	Артемов, А. В.	Информационная безопасность: курс лекций	Орел: Межрегиональная Академия безопасности и выживания (МАБИВ), 2014	http://www.iprbookshop.ru/33430.html неограниченный доступ для зарегистрированных пользователей
Л2.4		Основы информационной безопасности при работе на компьютере	Москва: Интернет-Университет Информационных Технологий (ИНТУИТ), 2016	http://www.iprbookshop.ru/52160.html неограниченный доступ для зарегистрированных пользователей
Л2.5	Шаньгин В. Ф.	Информационная безопасность и защита информации	Саратов: Профобразование, 2017	http://www.iprbookshop.ru/63594.html неограниченный доступ для зарегистрированных пользователей
Л2.6	Рогозин, В. Ю., Галушкин, И. Б., Новиков, В. К., Вепрев, С. Б.	Основы информационной безопасности: учебник для студентов вузов, обучающихся по направлению подготовки «правовое обеспечение национальной безопасности»	Москва: ЮНИТИ-ДАНА, 2017	http://www.iprbookshop.ru/72444.html неограниченный доступ для зарегистрированных пользователей

	Авторы, составители	Заглавие	Издательство, год	Колич-во
Л2.7	Бовырин, А. В., Дружков, П. Н., Ерухимов, В. Л., Золотых, Н. Ю., Кустикова, В. Д., Лысенков, И. Д., Мееров, И. Б., Писаревский, В. Н., Половинкин, А. Н., Сысоев, А. В.	Разработка мультимедийных приложений с использованием библиотек OpenCV и IPP	Москва: Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Эр Медиа, 2019	http://www.iprbookshop.ru/79718.html неограниченный доступ для зарегистрированных пользователей
Л2.8	Кубашева Е. С., Малашкевич И. А., Чекулаева Е. Н.	Информатика и вычислительная техника. Информационная безопасность автоматизированных систем: учебно-методическое пособие к прохождению производственной практики: учебно-методическое пособие	Йошкар-Ола: Поволжский государственный технологический университет, 2019	https://biblioclub.ru/index.php?page=book&id=562246 неограниченный доступ для зарегистрированных пользователей
Л2.9		БИТ. Бизнес & Информационные технологии: журнал	Москва: Положевец и партнеры, 2019	https://biblioclub.ru/index.php?page=book&id=562409 неограниченный доступ для зарегистрированных пользователей
Л2.10	Белозерова Г. И., Скуднев Д. М., Кононова З. А.	Нечеткая логика и нейронные сети: учебное пособие	Липецк: Липецкий государственный педагогический университет имени П.П. Семенова-Тян-Шанского, 2017	https://biblioclub.ru/index.php?page=book&id=576909 неограниченный доступ для зарегистрированных пользователей

5.3 Профессиональные базы данных и информационные справочные системы

ПСС Техэксперт http://www.cntd.ru,

Консультант +

Образовательная платформа по Phyton https://pythonist.ru/

Документация https://pytorch.org/

Документация библиотеки tensorflow - https://www.tensorflow.org/lite?hl=ru

5.4. Перечень программного обеспечения

Python

5.5. Учебно-методические материалы для студентов с ограниченными возможностями здоровья

При необходимости по заявлению обучающегося с ограниченными возможностями здоровья учебно-методические материалы предоставляются в формах, адаптированных к ограничениям здоровья и восприятия информации. Для лиц с нарушениями зрения: в форме аудиофайла; в печатной форме увеличенным шрифтом. Для лиц с нарушениями слуха: в форме электронного документа; в печатной форме. Для лиц с нарушениями опорно-двигательного аппарата: в форме электронного документа; в печатной форме.

6. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

Помещения для всех видов работ, предусмотренных учебным планом, укомплектованы необходимой специализированной учебной мебелью и техническими средствами обучения:

- столы, стулья;

- персональный компьютер / ноутбук (переносной);

- проектор;

- экран / интерактивная доска.

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

Методические указания по освоению дисциплины представлены в Приложении 2 к рабочей программе дисциплины.

Приложение 1

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

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

1.1 Показатели и критерии оценивания компетенций:

ЗУН, составляющие компетенцию	Показатели оценивания	Критерии оценивания	Средства оценивания
ПК-4:Способен осуществлять анализ результатов экспериментальных исследований с применением математических и физических методов, выбор технических средств инструментального мониторинга защищенности объектов информатизации			
З. основные принципы, походы и новые методы экспериментальных исследования в профессиональной сфере, технические средства инструментального мониторинга защищенности объектов информатизации	изучает основную и дополнительную литературу, содержащую материал об основных понятиях инструментальных средствах и математических методах, используемых при решении профессиональных задач, для подготовки к экзамену, и устному опросу	полнота и содержательность ответа на экзамене, устном опросе, соответствие ответов материалу, содержащемся в изученной литературе	УО (Раздел 1 в. 1-11 Раздел 2 в. 1-24) Э (1-32)
У. применять математические методы и технологии искусственного интеллекта в исследованиях процессов управления информационной безопасностью; анализировать различные подходы при решении задач обеспечения информационной безопасности	решение лабораторных заданий: составление программ на Python с использованием библиотек	правильность решения заданий на составление программ на Python с использованием с использованием библиотек	Раздел 1. ПЗ 1-8 Раздел 2. ПЗ 1-8
В. Навыками применения различных математических методов и технологий	решение лабораторных заданий: составление программ на Python с использованием библиотек	обоснованность применения методов для: решения заданий на составление программ на Python с использованием	Раздел 1. ПЗ 1-8 Раздел 2. ПЗ 1-8

искусственного интеллекта в исследованиях процессов управления информационной безопасностью; методами анализа различных подходов при решении задач обеспечения информационной безопасности	(NumPy,Pandas, matplotlib, PyBrian)	библиотек (NumPy,Pandas, matplotlib, PyBrian)	

Э – вопросы к экзамену, ЛЗ-практическое задание, УО- устный опрос

1.2 Шкалы оценивания:

Текущий контроль успеваемости и промежуточная аттестация осуществляется в рамках накопительной балльно-рейтинговой системы в 100-балльной шкале:

84-100 баллов (оценка «отлично»)
67-83 баллов (оценка «хорошо»)
50-66 баллов (оценка «удовлетворительно»)
0-49 баллов (оценка «неудовлетворительно»)

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

В разделе приводятся типовые варианты оценочных средств: вопросы к экзамену, практические задания, вопросы для устного опроса

Вопросы к экзамену

1. Методы анализа данных: кластеризация, классификация, ассоциативные правила, дерево решений, линейная регрессия, баессовский классификатор.
2. Выбор подходящих атрибутов для анализа и методы снижения размерности задачи.
3. Общие сведения о биометрических системах. Идентификация пользователей на основе лица, голоса, отпечатка.
4. Методика идентификации по цифровому отпечатку (fingerprint).
5. Интеллектуальные алгоритмы идентификации пользователя по распознаванию контрольного изображения (CAPTHCHA).
6. Системы обнаружения вторжений, построенные с использование алгоритмов нечеткой логики.
7. Построение экспертных систем с использованием модели нечеткой логики.
8. Обучение экспертных систем на основе алгоритмов с учителем и без.
9. Нейронные сети. Классификация задач машинного обучения.
10. Алгоритмы классификации и кластеризации методами машинного обучения. Классификация. Основы обучения с учителем. Классификация на основе ассоциативных правил.
11. Особенности применения методов машинного обучения в системах ИБ. Иерархические и неиерархические методы кластеризации.
12. Методы поиска аномалий, основанные на кластеризации.
13. Методы и системы на основе кластеризации и выбросов.
14. Методы и системы на основе баз знаний и экспертные системы
15. Применение технологий машинного обучения для решения задачи обнаружения вредоносных интернет- страниц
16. Нейросетевые методы. Нечеткие алгоритмы контроля.
17. Искусственные нейронные сети (ИНС) в системах обнаружения атак.

18. Принципы нейросетевого мониторинга безопасности.
19. Применение ИНС в задачах классификации и кластеризации.
20. Программные средство обнаружения сетевых атак с помощью ИНС.
21. Комбинирование нейронных сетей для обнаружения атак на компьютерные системы.
22. Системы обнаружения атак (СОА), основные способы построения.
23. СОА на основе сигнатурного анализа.
24. Обнаружение аномалий на основе нейронных сетей
25. Гибридные средства классификации в СЗИ.
26. Методы и системы на основе мягких вычислений
27. ИСЗИ на основе искусственных иммунных систем (ИИС).
28. Системы антивирусной защиты на основе ИИС
29. Алгоритмы построения и функционирования нейросетевой искусственной иммунной системы для обнаружения вредоносных программ.
30. Интеграция искусственных иммунных и нейронных сетей для обнаружения вредоносных программ.
31. Примеры работы иммунных систем ИБ. Использование генетических алгоритмов для обнаружения вторжений в сети.
32. Гибридные схемы обнаружения и классификации сетевых атак на основе комбинирования адаптивных классификаторов.

Критерии оценивания:

Основой для определения баллов, набранных при промежуточной аттестации, служит объём и уровень усвоения материала, предусмотренного рабочей программой дисциплины. При этом необходимо руководствоваться следующим:

- 84-100 баллов (оценка **«отлично»**) - изложенный материал фактически верен, наличие глубоких исчерпывающих знаний в объеме пройденной программы дисциплины в соответствии с поставленными программой курса целями и задачами обучения; правильные, уверенные действия по применению полученных знаний на практике, грамотное и логически стройное изложение материала при ответе, усвоение основной и знакомство с дополнительной литературой;
- 67-83 баллов (оценка **«хорошо»**) - наличие твердых и достаточно полных знаний в объеме пройденной программы дисциплины в соответствии с целями обучения, правильные действия по применению знаний на практике, четкое изложение материала, допускаются отдельные логические и стилистические погрешности, обучающийся усвоил основную литературу, рекомендованную в рабочей программе дисциплины;
- 50-66 баллов (оценка **«удовлетворительно»**) - наличие твердых знаний в объеме пройденного курса в соответствии с целями обучения, изложение ответов с отдельными ошибками, уверенно исправленными после дополнительных вопросов; правильные в целом действия по применению знаний на практике;
- 0-49 баллов (оценка **«неудовлетворительно»**) - ответы не связаны с вопросами, наличие грубых ошибок в ответе, непонимание сущности излагаемого вопроса, неумение применять знания на практике, неуверенность и неточность ответов на дополнительные и «наводящие» вопросы.

Лабораторные задания

Раздел 1. Алгоритмы интеллектуального анализа данных: основные методы и понятия

Тема 1.
Изучение алгоритма обратного распространения ошибки (метод Back Propagation

Тема 2.
Алгоритмы классификации и кластеризации методами машинного обучения

Тема 3.
Исследование рекуррентной нейронной сети Хопфилда на примере задачи распознавания образов

Тема 4.

Нейросетевые методы

Тема 5.
Нечеткие алгоритмы контроля

Тема 6.
Исследование рекуррентной нейронной сети Коско (BAM) на примере задачи распознавания образов

Тема 7.
Иммунные и генетические методы и алгоритмы ИБ

Тема 8.
Гибридные методы и алгоритмы ИБ

Каждое задание оценивается в 5 баллов

Критерии оценивания:
5 б. – задание выполнено верно;
4 б. – при выполнении задания были допущены неточности, не влияющие на результат;
3 б. – при выполнении задания были допущены ошибки;
2-1 б. – при выполнении задания были допущены существенные ошибки.
0 б. – задание не выполнено.

Максимальное количество баллов по лабораторным заданиям раздела 1 – 40 б.

Раздел 2. Методы машинного обучения в информационной безопасности

Тема 1.
Разведочный анализ данных

Тема 2.
Обработка пропусков в данных, кодирование категориальных признаков, масштабирование данных

Тема 3.
Подготовка обучающей и тестовой выборки, кросс- валидация и подбор гиперпараметров на примере метода ближайших соседей

Тема 4.
Линейные модели, SVM и деревья решений

Тема 5.
Исследование однослойных нейронных сетей на примере моделирования булевых выражений

Тема 6.
Применение однослойной нейронной сети для решения задач регрессии экспериментальных данных

Тема 7.
Применение однослойной нейронной сети с линейной функцией активации для прогнозирования временных рядов

Тема 8.
Исследование нейронных сетей с радиальными базисными функциями (RBF) на примере моделирования булевых выражений

Каждое задание оценивается в 5 баллов

Критерии оценивания:
5 б. – задание выполнено верно;
4 б. – при выполнении задания были допущены неточности, не влияющие на результат;
3 б. – при выполнении задания были допущены ошибки;

2-1 б. – при выполнении задания были допущены существенные ошибки.
0 б. – задание не выполнено.

Максимальное количество баллов по лабораторным заданиям раздела 2 – 40 б.

Максимальное количество баллов по лабораторным заданиям - 80

Перечень вопросов для устного опроса

Раздел 1. Алгоритмы интеллектуального анализа данных: основные методы и понятия

1. Методы анализа данных: кластеризация, классификация,
2. Методы анализа данных: ассоциативные правила, дерево решений
3. Методы анализа данных: линейная регрессия, баессовский классификатор.
4. Выбор подходящих атрибутов для анализа и методы снижения размерности задачи.
5. Общие сведения о биометрических системах.
6. Идентификация пользователей на основе лица, голоса, отпечатка.
7. Методика идентификации по цифровому отпечатку (fingerprint).
8. Интеллектуальные алгоритмы идентификации пользователя по распознаванию контрольного изображения (CAPTHCHA).
9. Системы обнаружения вторжений, построенные с использование алгоритмов нечеткой логики.
10. Построение экспертных систем с использованием модели нечеткой логики.
11. Обучение экспертных систем на основе алгоритмов с учителем и без.

Максимальное количество баллов по разделу 1 – 10 б

Раздел 2. Методы машинного обучения в информационной безопасности

1. Нейронные сети. Классификация задач машинного обучения.
2. Алгоритмы классификации и кластеризации методами машинного обучения. Классификация. Основы обучения с учителем. Классификация на основе ассоциативных правил.
3. Особенности применения методов машинного обучения в системах ИБ. Иерархические и неиерархические методы кластеризации.
4. Методы поиска аномалий, основанные на кластеризации.
5. Методы и системы на основе кластеризации и выбросов.
6. Методы и системы на основе баз знаний и экспертные системы
7. Применение технологий машинного обучения для решения задачи обнаружения вредоносных интернет- страниц
8. Нейросетевые методы. Нечеткие алгоритмы контроля.
9. Искусственные нейронные сети (ИНС) в системах обнаружения атак.
10. Принципы нейросетевого мониторинга безопасности.
11. Применение ИНС в задачах классификации и кластеризации.
12. Программные средство обнаружения сетевых атак с помощью ИНС.
13. Комбинирование нейронных сетей для обнаружения атак на компьютерные системы.
14. Системы обнаружения атак (СОА), основные способы построения.
15. СОА на основе сигнатурного анализа.
16. Обнаружение аномалий на основе нейронных сетей
17. Гибридные средства классификации в СЗИ.
18. Методы и системы на основе мягких вычислений
19. ИСЗИ на основе искусственных иммунных систем (ИИС).
20. Системы антивирусной защиты на основе ИИС
21. Алгоритмы построения и функционирования нейросетевой искусственной иммунной системы для обнаружения вредоносных программ.
22. Интеграция искусственных иммунных и нейронных сетей для обнаружения вредоносных программ.
23. Примеры работы иммунных систем ИБ. Использование генетических алгоритмов для обнаружения вторжений в сети.
24. Гибридные схемы обнаружения и классификации сетевых атак на основе комбинирования адаптивных классификаторов.

Максимальное количество баллов по разделу 2 – 10 б.

Критерии оценивания:
Для каждого вопроса:
2 балла - дан полный, развёрнутый ответ на поставленный вопрос, изложение материала при ответе – грамотное и логически стройное;
1 балл - дан неполный ответ на поставленный вопрос
0 баллов - обучающийся не владеет материалом по заданному вопросу.

Максимальное количество баллов по устному опросу – 20

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

Процедуры оценивания включают в себя текущий контроль и промежуточную аттестацию.

Текущий контроль успеваемости проводится с использованием оценочных средств, представленных в п. 2 данного приложения. Результаты текущего контроля доводятся до сведения студентов до промежуточной аттестации.

Промежуточная аттестация проводится в форме экзамена 2 семестр

Экзамен проводится по окончании теоретического обучения до начала экзаменационной сессии в письменном виде. Количество вопросов в задании – 2. Проверка ответов и объявление результатов производится в день экзамена. Результаты аттестации заносятся в зачетную ведомость и зачетную книжку студента. Студенты, не прошедшие промежуточную аттестацию по графику сессии, должны ликвидировать задолженность в установленном порядке.

Приложение 2

МЕТОДИЧЕСКИЕ УКАЗАНИЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ

Учебным планом предусмотрены следующие виды занятий:

- лекции;
- лабораторные занятия.

В ходе лабораторных работ развиваются навыки применения математических методов, выбора инструментальных средств для обработки и анализа данных в профессиональной деятельности

При подготовке к лабораторным занятиям каждый студент должен:

– изучить рекомендованную учебную литературу;

В процессе подготовки к лабораторным занятиям студенты могут воспользоваться консультациями преподавателя.

Теоретические вопросы должны быть изучены студентами в ходе самостоятельной работы. Контроль самостоятельной работы студентов над учебной программой курса осуществляется методом устного опроса и выполнения лабораторных заданий. В ходе самостоятельной работы каждый студент обязан прочитать основную и по возможности дополнительную литературу по изучаемой теме. Выделить непонятные термины, найти их значение в литературе.

Для подготовки к занятиям, текущему контролю и промежуточной аттестации студенты могут воспользоваться электронно-библиотечными системами. Также обучающиеся могут взять на дом необходимую литературу на абонементе университетской библиотеки или воспользоваться читальными залами.