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
Интеллектуальные методы форензики

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 **Информационные технологии и защита информации**

Распределение часов дисциплины по семестрам

Семестр (<Курс>.<Семестр на курсе>)	3 (2.1)		Итого	
Недель	15 2/6			
Вид занятий	УП	РП	УП	РП
Лекции	6	6	6	6
Практические	8	8	8	8
Итого ауд.	14	14	14	14
Контактная работа	14	14	14	14
Сам. работа	54	54	54	54
Часы на контроль	4	4	4	4
Итого	72	72	72	72

ОСНОВАНИЕ

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

Программу составил(и): к.ф.-м.н., доцент, Карнаухов С.Н. _____

Зав. кафедрой: к.э.н., доцент Ефимова Е.В. _____

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

1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

1.1	получение обучающимися теоретических представлений о принципах создания интеллектуальных информационных систем на основе использования математических методов и компьютерного моделирования, а также выработка практических навыков использования современных инструментальных средств для решения задач искусственного интеллекта в области информационной безопасности.

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:

- вопросы информационной безопасности, процедуру проведения научных исследований и технических разработок с использованием интеллектуальных информационных систем (соотнесено с индикатором ПК-4.1)

Уметь:

- приобретать новые знания и умения, использовать информационные технологии в области информационной безопасности, прогнозировать эффективность и оценивать затраты и риски при формировании политики безопасности, выбирать методы и средства решения профессиональных задач с использованием интеллектуальных информационных систем(соотнесено с индикатором ПК-4.2)

Владеть:

- навыками применения новых знаний и умений для решения профессиональных задач, навыками разработки систем и средств обеспечения информационной безопасности, практическими навыками разработки планов и программ проведения научных и технических разработок в сфере информационной безопасности с использованием интеллектуальных информационных систем(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. Интеллектуальный анализ				
1.1	История форензики.Сферы применения форензики. Классификация компьютерной криминалистики /Лек/	3	2	ПК-4	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3
1.2	"Алгоритм отжига" Суть алгоритма. Основные этапы. Применение алгоритма в экономике и в сфере информационной безопасности. Использование Deductor, Mathlab и Statistika для реализации алгоритма. /Пр/	3	4	ПК-4	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3
1.3	"Алгоритм муравья" Суть алгоритма. Связь алгоритма с теорией графов. Основные этапы алгоритма. Использование Deductor, Mathlab и Statistika для реализации алгоритма в сфере информационной безопасности. /Пр/	3	2	ПК-4	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3
1.4	Основные инструменты форензики. Этапы криминалистического процесса. Инструментарий и тренировочные площадки /Лек/	3	2	ПК-4	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3
1.5	Тема "Основные задачи в проблеме распознавания образов". Задачи распознавания. Алгоритмы распознавания образов. /Ср/	3	14	ПК-4	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3
1.6	Тема "EM-алгоритм в задачах автоматической классификации". Автоматическая классификация. Задачи автоматической классификации. EM-алгоритм. /Ср/	3	14	ПК-4	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3
	Раздел 2. Нейронные сети и генетические алгоритмы				

2.1	"Нейронная сеть Хопфилда" Принципы построения нейронной сети Хопфилда. Применение нейронной сети Хопфилда (в том числе в области информационной безопасности). Использование Deductor и Mathlab для построения нейронной сети. /Лек/	3	2	ПК-4	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3
2.2	"Нейронная сеть Хэмминга" Принципы построения нейронной сети Хэмминга. Применение нейронной сети Хэмминга (в том числе в области информационной безопасности). Использование Mathlab для построения нейронной сети. /Пр/	3	2	ПК-4	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3
2.3	"Нейронная сеть Кохонена" Принципы построения нейронной сети Коханена. Методы классификации на основе нейронной сети Коханена. Алгоритм функционирования нейронной сети Коханена. Принципы построения самоорганизующихся карт Коханена в области информационной безопасности. Использование Mathlab для построения нейронной сети. /Ср/	3	16	ПК-4	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3
2.4	"Генетические алгоритмы" Генетические алгоритмы. Применение генетических алгоритмов при создании ИИС. /Ср/	3	10	ПК-4	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3
2.5	/Зачёт/	3	4	ПК-4	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3

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	Абросимов В. К.	Интеллектуальные методы решения конфликтных задач (нейросетевое измерение дипломатии): монография	Москва: Креативная экономика, 2012	https://biblioclub.ru/index.php?page=book&id=132661 неограниченный доступ для зарегистрированных пользователей
Л1.2	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
Л1.3	Моргунов, А. В.	Информационная безопасность: учебно-методическое пособие	Новосибирск: Новосибирский государственный технический университет, 2019	http://www.iprbookshop.ru/98708.html неограниченный доступ для зарегистрированных пользователей

5.2. Дополнительная литература

	Авторы, составители	Заглавие	Издательство, год	Колич-во
Л2.1	Рытенкова О.	Информационная безопасность: журнал	Москва: ГРОТЕК, 2012	https://biblioclub.ru/index.php?page=book&id=211298 неограниченный доступ для зарегистрированных пользователей

	Авторы, составители	Заглавие	Издательство, год	Колич-во
Л2.2		Введение в нейронные сети	Москва: Интернет-Университет Информационных Технологий (ИНТУИТ), 2016	http://www.iprbookshop.ru/52144.html неограниченный доступ для зарегистрированных пользователей
Л2.3	Белозерова Г. И., Скуднев Д. М., Кононова З. А.	Нечеткая логика и нейронные сети: учебное пособие	Липецк: Липецкий государственный педагогический университет им. 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

Национальная электронная библиотека (НЭБ) https://rusneb.ru/

База статистических данных Росстата http://www.gks.ru/

Консультант+

Гарант

5.4. Перечень программного обеспечения

Deductor

LibreOffice

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. вопросы информационной безопасности, процедуру проведения научных исследований и технических разработок с использованием интеллектуальных информационных систем (соотнесено с индикатором ПК-4.1)	Многослойные сети. Методы обучения персептрона и многослойной сети. Примеры применения многослойной сети в экономических задачах.	полнота и содержательность ответа умение приводить примеры	О – опрос (1-32), З – вопросы к зачету (1-32)
У. приобретать новые знания и умения, использовать информационные технологии в области информационной безопасности, прогнозировать эффективность и оценивать затраты и риски при формировании политики безопасности, выбирать методы и средства решения профессиональных задач с использованием интеллектуальных информационных систем(соотнесено с индикатором ПК-4.2)	Нейронные сети. Принципы построения нейронной сети.	полнота и содержательность ответа умение приводить примеры умение самостоятельно находить решение поставленных задач	ЛЗ – лабораторные задания (1-6) ПОЗЗ практико-ориентированные задания к зачету (1-5)
В. навыками применения новых знаний и умений для решения профессиональных задач, навыками разработки систем и средств обеспечения информационной безопасности, практическими навыками разработки планов и программ проведения научных и технических разработок в сфере информационной безопасности с использованием интеллектуальных информационных систем(соотнесено с индикатором ПК-4.3)	Основные задачи в проблеме распознавания образов. EM-алгоритм в задачах автоматической классификации.	полнота и содержательность ответа умение приводить примеры умение самостоятельно находить решение поставленных задач	ЛЗ – лабораторные задания (1-6) ПОЗЗ практико-ориентированные задания к зачету (1-5)

1.2 Шкалы оценивания:

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

50-100 баллов (зачет)

0-49 баллов (незачет)

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

Вопросы к зачету

1) Машинное обучение.
2) Основные алгоритмы ИИС.
3) Алгоритм отжига.
4) Суть алгоритма отжига.
5) Основные этапы алгоритма отжига.
6) Применение алгоритма отжига в экономике.
7) Алгоритм муравья.
8) Суть алгоритма муравья.
9) Связь алгоритма муравья с теорией графов.
10) Основные этапы алгоритма муравья.
11) Понятие персептрона.
12) Многослойные сети.
13) Методы обучения персептрона и многослойной сети.
14) Примеры применения многослойной сети в экономических задачах.
15) Нейронные сети.
16) Принципы построения нейронной сети.
17) Основные задачи в проблеме распознавания образов.
18) EM-алгоритм в задачах автоматической классификации.
19) Нейронная сеть Хопфилда.
20) Принципы построения нейронной сети Хопфилда.
21) Применение нейронной сети Хопфилда.
22) Нейронная сеть Хэмминга.
23) Принципы построения нейронной сети Хэмминга.
24) Применение нейронной сети Хэмминга.
25) Нейронная сеть Кохонена.
26) Принципы построения нейронной сети Коханена.
27) Методы классификации на основе нейронной сети Коханена.
28) Алгоритм функционирования нейронной сети Коханена.
29) Принципы построения самоорганизующихся карт Коханена.
30) Генетические алгоритмы.
31) Применение генетических алгоритмов при создании ИИС.
32) Алгоритмы работы системы обучения с подкреплением.

Типовые практико-ориентированные задания к зачету

Задание 1. Добавить пользователей в компьютер.
Задание 2. Создать учетную запись локального пользователя.
Задание 3. Измените учетную запись локального пользователя на учетную запись администратора.
Задание 4.Выполнить настройку учетной записи с ограниченными правами.
Задание 5. Выполнить добавление учетных записей, используемых приложениями.

Ключ для контроля правильности выполнения практико-ориентированные задания к зачету

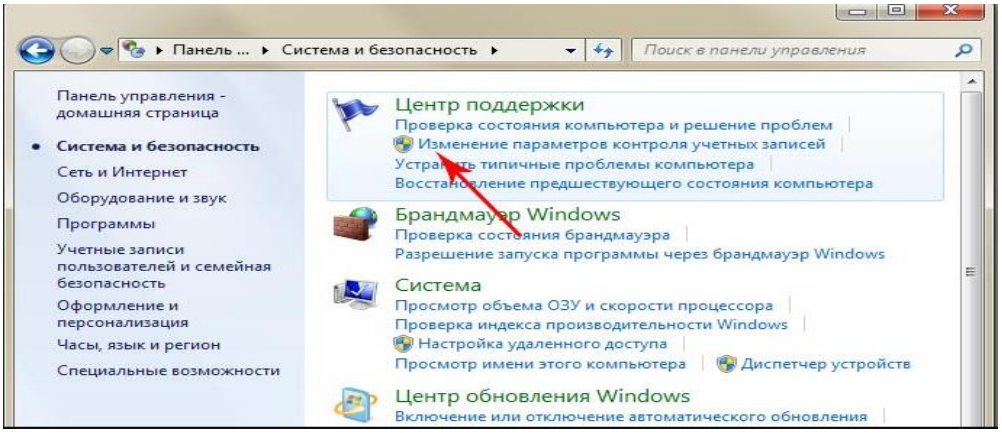
1. Добавление пользователей в рабочий или учебный компьютер. Выберите параметры > "Пуск" > " Учетные записи > Другие пользователи". В разделе "Рабочие или учебные > добавить рабочую или учебную учетную запись" выберите " Добавить учетную запись". Введите учетную запись этого пользователя, выберите тип учетной записи и нажмите Добавить.

2. Создание учетной записи локального пользователя. Выберите Пуск > Параметры > Учетные записи, а затем Семья и другие пользователи. Рядом с пунктом Добавить другого пользователя выберите Добавить учетную запись. Выберите пункт У меня нет учетных данных этого пользователя и на следующей странице нажмите Добавить пользователя без учетной записи Майкрософт. Введите имя пользователя, пароль, подсказку о пароле или выберите секретные вопросы, а затем нажмите Далее.

3. Изменение учетной записи локального пользователя на учетную запись администратора. Выберите Пуск > Параметры > Учетные записи. В разделе Семья и другие пользователи щелкните имя владельца учетной записи (под ним должно быть указано "Локальная учетная запись") и выберите Изменить

тип учетной записи. В разделе Тип учетной записи выберите Администратор, и нажмите ОК. Войдите в систему с новой учетной записью администратора.

4.



5.Добавление на компьютер учетной записи, используемой приложениями: Выберите **параметры >** параметров > **учетных** записей > **электронной почты & учетных записей**. Добавление учетной записи, используемой по электронной почте. выберите "Добавить учетную запись" в разделе "Учетные записи", используемые электронной почтой**, календарем и** контактами. Для других приложений выберите "Добавить учетную запись Майкрософт " или "Добавить рабочую или учебную учетную запись". Следуйте инструкциям по добавлению учетной записи.

Критерии оценивания:

– 50-100 баллов (зачет) – изложенный материал фактически верен, наличие глубоких исчерпывающих знаний; правильные, уверенные действия по применению полученных знаний на практике, грамотное и логически стройное изложение материала при ответе; практико-ориентированное задание выполнено правильно и прокомментировано; наличие твердых и достаточно полных знаний, правильные действия по применению знаний на практике, четкое изложение материала, допускаются отдельные логические и стилистические погрешности, неуверенность и неточность ответов на дополнительные и наводящие вопросы; практико-ориентированное задание выполнено правильно, но не прокомментировано; при неполном ответе на вопросы; затрудняется ответить на дополнительные вопросы; практико-ориентированное задание выполнено с ошибками и отсутствуют комментарии;

– 0-49 баллов (незачет) – 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; практико-ориентированное задание не выполнено.

Задания для опроса

1. Что такое форензика
2. Инструментарий форензики
3. Сферы применения форензики
4. Возникновение, перспективы, проблемы ИИС.
5. Машинное обучение.
6. Основные алгоритмы ИИС.
7. Алгоритм отжига.
8. Суть алгоритма отжига.
9. Основные этапы алгоритма отжига.
10. Применение алгоритма отжига в экономике.
11. Алгоритм муравья.
12. Суть алгоритма муравья.
13. Связь алгоритма муравья с теорией графов.
14. Основные этапы алгоритма муравья.
15. Понятие персептрона.
16. Многослойные сети.
17. Методы обучения персептрона и многослойной сети.

18. Примеры применения многослойной сети в экономических задачах.
19. Нейронные сети.
20. Принципы построения нейронной сети.
21. Основные задачи в проблеме распознавания образов.
22. EM-алгоритм в задачах автоматической классификации.
23. Нейронная сеть Хопфилда.
24. Принципы построения нейронной сети Хопфилда.
25. Применение нейронной сети Хопфилда.
26. Нейронная сеть Хэмминга.
27. Принципы построения нейронной сети Хэмминга.
28. Применение нейронной сети Хэмминга.
29. Нейронная сеть Кохонена.
30. Принципы построения нейронной сети Коханена.
31. Методы классификации на основе нейронной сети Коханена.
32. Алгоритм функционирования нейронной сети Коханена.
33. Принципы построения самоорганизующихся карт Коханена.
34. Генетические алгоритмы.
35. Алгоритмы работы системы обучения с подкреплением.

Критерии оценивания:

Для каждого вопроса:

- 1 балла дан полный ответ на поставленный вопрос, изложение материала при ответе – грамотное и логически стройное;
- 0 баллов – обучающийся не владеет материалом по заданному вопросу.

Максимальное количество баллов – 30

Лабораторные задания

Лабораторная работа №1

Основные инструменты форензики

1) AccessDataForensicToolkit — программное обеспечение для проведения компьютерных экспертиз, для анализа дампа оперативной памяти, использует мощный инструмент поиска, осуществляет архивацию данных и проводит полное исследование компьютера в рамках судебной экспертизы;

2) BrowserForensicTool — инструмент для извлечения информации о действиях пользователя из различных браузеров;

3) TheSleuthKit (TSK) — библиотеку консольных программ, предназначенных для проведения анализа данных на произвольных файловых системах. Используя это программное обеспечение, следователи могут идентифицировать и восстановить удаленные данные из образов, снятых во время расследования или с работающих систем;

4) EncryptedDiskDetector — программа, которая помогает найти на локальном компьютере скрытые зашифрованные тома TrueCrypt, PGP и Bitlocker, используя подпись/сигнатуру шифрования диска в главной загрузочной области

Лабораторная работа №2

Применение методов первичного разведочного анализа данных в решении задач интеллектуального анализа данных средствами интегрированной системы Statistica

Лабораторная работа №3

Решение задач интеллектуального анализа данных: классификация объектов средствами интегрированной системы Statistica

Лабораторная работа №4

Решение задач интеллектуального анализа данных средствами Deductor

Лабораторная работа №5

Решение задач интеллектуального анализа данных: прогнозирование временных рядов средствами интегрированной системы Statistica

Лабораторная работа №6
Распознавание образов на основных инструментальных средств

Лабораторная работа №7
Разработка и обучение нейронной сети

Критерии оценки:
(для каждого лабораторного задания)
10 б. – задание выполнено верно;
8 б. – при выполнении задания были допущены неточности, не влияющие на результат;
5 б. – при выполнении задания были допущены ошибки;
2 б. – при выполнении задания были допущены существенные ошибки.
0 б. – задание не выполнено.

Максимальное количество баллов за семестр 70.

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.

Зачет проводится по расписанию промежуточной аттестации.

Проверка ответов и объявление результатов производится в день зачета. Результаты аттестации заносятся в экзаменационную 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;

- практические занятия.

В ходе лекционных занятий рассматриваются основные теоретические вопросы по дисциплине.

В ходе практических занятий углубляются и закрепляются знания студентов по ряду рассмотренных вопросов, развиваются навыки использования методов форензики.

Вопросы, не рассмотренные на лекционных и практических занятиях, должны быть изучены студентами в ходе самостоятельной работы. Контроль самостоятельной работы студентов над учебной программой курса осуществляется в ходе занятий методом устного опроса или посредством тестирования. В ходе самостоятельной работы каждый студент обязан прочитать основную и по возможности дополнительную литературу по изучаемой теме, дополнить конспекты лекций недостающим материалом, выписками из рекомендованных первоисточников. Выделить непонятные термины, найти их значение в энциклопедических словарях.

Студент должен готовиться к предстоящему лекционному и практическому занятию по всем, обозначенным в рабочей программе дисциплины вопросам.

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.