МИНИСТЕРСТВО ЦИФРОВОГО РАЗВИТИЯ, СВЯЗИ И МАССОВЫХ КОММУНИКАЦИЙ РОССИЙСКОЙ ФЕДЕРАЦИИ
Ордена Трудового Красного Знамени
федеральное государственное бюджетное образовательное
учреждение высшего образования
«Московский технический университет связи и информатики»



УТВЕРЖДАЮ:
Проректор по научной работе
_____Ю.Л. Леохин
"12" апреля 2023 г.

ПРОГРАММА ПОДГОТОВКИ
К СДАЧЕ КАНДИДАТСКОГО МИНИМУМА
по научной специальности

2.3.6. МЕТОДЫ И СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ, ИНФОРМАЦИОННАЯБЕЗОПАСНОСТЬ

Отрасль науки: **технические науки**

Москва, 2023

Рабочая программа дисциплины «Технологии искусственного интеллекта в информационной безопасности» составлена в соответствии с Федеральными государственными требованиями к структуре программ подготовки научных и научно-педагогических кадров в аспирантуре, условиям их реализации, срокам освоения этих программ с учетом различных форм обучения, образовательных технологий и особенностей отдельных категорий аспирантов, утвержденными приказом Министерства образования и науки Российской Федерации от 20 октября 2021 г. № 951.

Разработчик(и) программы:_
Зав. кафедрой « Информационная безопасность»_____ Шелухин О.И.
подпись

Рабочая программа утверждена на заседании кафедры ИБ

Протокол №_____ от «___»_____ 20__г.

Заведующий кафедрой « Информационная безопасность»
Шелухин О.И. _____
подпись

«__» _____ 2023г.

Рабочая программа хранится на кафедре ИБ и в отделе аспирантуры.

1. Цели освоения дисциплины

Цель программы — подготовка исследователей в области анализа современных фундаментальных и прикладных проблем компьютерной безопасности, владеющих как современным математическим аппаратом, необходимым для создания современных информационных систем и для доказательной оценки безопасности программного обеспечения, так и знаниями в области системного программного обеспечения и архитектуры современных распределенных вычислительных систем.

2.Место дисциплины в структуре программы аспирантуры

Дисциплина «**Технологии искусственного интеллекта в информационной безопасности**» (ТИИвИБ) включена в образовательный блок дисциплин учебного плана. Дисциплина ТИИвИБ реализуется в соответствии с требованиями ФГТ, ОП и Учебного плана по Программе подготовки научных и научно-педагогических кадров 2.3.6 Методы и системы защиты информации, информационная безопасность в аспирантуре).

Для освоения дисциплины требуются знания и умения, приобретенные обучающимися в результате освоения ряда дисциплин (разделов дисциплин), таких как:

Системы управления базами данных;

Основы информационной безопасности;

Модели безопасности компьютерных систем;

Защита в операционных системах;

Основы построения защищенных компьютерных сетей;

Защита программ и данных;

Сети и системы передачи информации;

Техническая защита информации;

Криптографические методы защиты информации и криптографические протоколы;

Теоретико-числовые методы в криптографии;

Теория кодирования, сжатия и восстановления информации.

Рабочая программа дисциплины ТИИвИБ для инвалидов и лиц с ограниченными возможностями здоровья разрабатывается индивидуально с учетом особенностей психофизического развития, индивидуальных возможностей и состояния здоровья таких обучающихся.

3. Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения образовательной программы.

В результате изучения дисциплины ТИИвИБ аспирант должен:

✓ ***Знать:***

- современные достижения науки и передовые технологии в области защиты информации;

- требования к содержанию нормативно-методических документов по защите информации;
- основы применения криптосистем для защиты компьютерной информации в информационных системах;
- методы идентификации и проверки подлинности пользователей компьютерных систем;
- методы комплексной защиты процесса обработки информации в компьютерных системах.

Уметь:

- оценивать перспективные направления развития методов защиты информации с учетом мирового опыта;
- проводить работы по выбору и настройке аппаратно-программных средств криптографической защиты компьютерной информации;
- применять современные методы и средства исследования для решения конкретных задач развития средств защиты информации;
- оценивать эффективность защиты компьютерных систем от удаленных атак через сеть Internet;
- проводить работы по моделированию объектов защиты информации;

Иметь опыт:

- планирования процессов решения научно-технических задач;
- анализа работы технических средств идентификации и проверки подлинности пользователей компьютерных систем;
- работы с системами автоматизированного встраивания защитных механизмов в программное обеспечение;
- разработки мероприятий по защите от компьютерных вирусов;
- работы с программно-аппаратными средствами моделирования объектов защиты информации.

4. Структура и содержание дисциплины

Общая трудоемкость дисциплины составляет **5** зачетных единиц (180 часов). Процесс изучения дисциплины реализуется при очной форме обучения в 4-ом семестре. Промежуточная аттестация предусматривает **экзамен** в 4-ом семестре.

4.1 Распределение трудоёмкости дисциплины по видам работ по семестрам

Общая трудоёмкость дисциплины составляет 5 зач.ед. (180 часов), их распределение по видам работ, семестрам представлено в таблице 1.

Таблица 1

Распределение трудоёмкости дисциплины по видам работ по семестрам

Виды учебной работы	Трудоемкость (часы)		4-ый семестр (указание часов по семестрам)
Аудиторные занятия (всего)	108		108
В том числе:			
Лекции	72		72
Практические занятия	36		36
Самостоятельная работа (всего)	36		36
Формы аттестации по дисциплине (зачет, экзамен)			Экзамен 36
Общая трудоемкость дисциплины	Часы 180	ЗЕТ 5	

4.2 Содержание дисциплины

Тематический план учебной дисциплины Таблица 2

Наименование разделов и тем дисциплин (укрупнённо)	**Всего**	**Аудиторная работа**		**Внеаудиторная работа СР**
		Л	**ПЗ/С**	
Раздел 1 Основные понятия интеллектуальных систем защиты информации (ИСЗИ)..	24	12	6	6
Раздел 2 **.** Алгоритмы интеллектуального анализа данных: основные методы и понятия	24	12	6	6
Раздел 3. Использование искусственных нейронных сетей в ИБ	24	12	6	6
Раздел 4. Методы анализа данных в системах ИБ	24	12	6	6
Раздел 5. Нечеткая логика и экспертные системы ИБ	24	12	6	6
Раздел 6. Иммунные , генетические и гибридные методы и алгоритмы ИБ	28	12	6	6
Всего за _4 семестр	144	**72**	**36**	**36**
Экзамен (при наличии)	36			
Итого по дисциплине	**180**			

4.3 Лекции /практические/ занятия

Таблица 3

Содержание лекций /практических занятий

№ п/п	Название раздела, темы	№ и название лекций/ лабораторных/ практических/ семинарских занятий	Формируемые компетенции	Кол-во часов
1.	**Раздел 1.** Основные понятия интеллектуальных систем защиты информации (ИСЗИ)			
	Тема 1. алмиза данных- Основные понятия интеллектуальных систем защиты информации (ИСЗИ)	**Лекция№1** Тенденции развития и использования искусственного интеллекта в информационной безопасности		2
		Лекция №2 Подходы и направления развития искусственного интеллекта		2
		Лекция №3 Классификация текстов		2
		Практическая работа №1.Классификация текстов. Этапы классификации. Индексация и предобработка документа. Извлечение термов. Методы перевода текста в пространство признаков.		2
		Практическая работа№2. Построение и обучение классификаторов текста с помощью методов машинного обучения		2
	Тема 2. Методы искусственного интеллекта в задачах обеспечения безопасности компьютерных сетей.	**Лекция №3.** Основные понятия. Классификация. Основы обучения с учителем. Классификация на основе ассоциативных правил.		2
		Лекция №4.Методы кластерного анализа данных. Сравнительный анализ методов кластеризации.		2
		Практическая работа№4.Метрики оценки качества алгоритмов кластеризации		2
		Лекция № 5. Методы и системы на основе баз знаний и экспертные системы		2
		Лекция № 6.Потоковая классификация. Сценарии обработки потоковых данных. Дрейф концепта при потоковой классификации		2

№ п/п	Название раздела, темы	№ и название лекций/ лабораторных/ практических/ семинарских занятий	Формируемые компетенции	Кол-во часов
2.	**Раздел 2** Алгоритмы интеллектуального анализа данных: основные методы и понятия			
	Тема 3. Алгоритмы интеллектуального анализа данных: основные методы и понятия	**Лекция №7** Методы обнаружения и классификации компьютерных атак и сетевых аномалий методами ИИ	.	4
		Лекция №8. Особенности применения методов машинного обучения в системах ИБ. Иерархические и не иерархически методы кластеризации. Методы поиска аномалий, основанные на кластеризации. Методы и системы на основе кластеризации и выбросов.		4
		Лекция №9. Применение технологий машинного обучения для решения задачи обнаружения вредоносных интернет-страниц		2
		Практическое занятие №5. Алгоритмы классификации и кластеризации методами машинного обучения		4
		Практическое занятие №6. Методы и системы на основе кластеризации и выбросов.		2
		Лекция №10. Особенности применения методов машинного обучения в системах ИБ. Иерархические и не иерархически методы кластеризации. Методы поиска аномалий, основанные на кластеризации.		2
3.	**Раздел 3.** Использование искусственных нейронных сетей в ИБ			
	Тема 4. Нейросетевые методы и алгоритмы	**Лекция №11.** Общие сведения об ИНС. Алгоритм обратного распространения ошибок. Использование ИНС в системах обнаружения вторжений.	.	4
		Лекция №12 Принципы нейросетевого мониторинга безопасности. Применение ИНС в задачах классификации и кластеризации.		4
		Лекция №13. Программные средство		4

№ п/п	Название раздела, темы	№ и название лекций/ лабораторных/ практических/ семинарских занятий	Формируемые компетенции	Кол-во часов
		обнаружения сетевых атак с помощью ИНС. Комбинирование нейронных сетей для обнаружения атак на компьютерные системы.		
		Практическое занятие №7. Искусственная нейронная сеть с алгоритмом обратного распространения ошибки		2
		Практическое занятие №8. Исследование алгоритмов кластеризации с помощью методов нечеткой логики.		4
4.	**Раздел 4..** Методы анализа данных в системах ИБ			
	Тема 5. Методы анализа данных в системах ИБ	**Лекция №14.** Общие сведения о методах анализа данных. Автоматическое извлечение знаний из больших наборов данных.	.	4.
		Лекция №15. Анализ данных в системах управления безопасностью.		2
		Лекция №16. Базовые методы анализа данных. Кластеризация, классификация, ассоциативные правила, дерево решений, линейная регрессия, наивный баессовский классификатор.		4
		Лекция №17. Выбор подходящих атрибутов для анализа и методы снижения размерности задачи.		2
		Практическое занятие №9. Методы анализа данных в ИБ : ассоциативные правила, дерево решений, линейная регрессия, наивный баессовский классификатор		6
5	**Раздел 5.** Нечеткая логика и экспертные системы ИБ.			
	Тема 6. Нечеткая логика и экспертные системы ИБ	**Лекция №18.** Общие сведения об алгоритмах нечеткой логики.		2
		Лекция №19. Системы обнаружения вторжений, построенные с использование алгоритмов нечеткой логики.		4
		Лекция №20. Общие сведения об экспертных системах ИБ. Построение экс-		2

№ п/п	Название раздела, темы	№ и название лекций/ лабораторных/ практических/ семинарских занятий	Формируемые компетенции	Кол-во часов
		пертых систем с использованием модели нечеткой логики.		
		Лекция №21. Обучение экспертных систем на основе алгоритмов с учителем и без.		4
		Практическое занятие №10. Примеры экспертных систем и алгоритмов ИБ, построенных по принципу нечеткой логики		4
		Практическое занятие №11. Построение модели алгоритма обнаружения вторжений на основе подходов нечёткой логики		2
	Раздел 6. Иммунные , генетические и гибридные методы и алгоритмы ИБ			
	Тема 7. Иммунные и генетические методы и алгоритмы ИБ	**Лекция №22** ИСЗИ на основе искусственных иммунных систем (ИИС). Системы антивирусной защиты на основе ИИС		2
		Лекция №23 Алгоритмы построения и функционирования нейросетевой искусственной иммунной системы для обнаружения вредоносных программ.		4
		Практическое занятие №12 Иммунные методы и алгоритмы ИБ		2
		Практическое занятие №13 Генетические методы и алгоритмы ИБ		2
	Тема 8. Гибридные методы и алгоритмы ИБ	**Лекция №24** Гибридные схемы обнаружения и классификации сетевых атак на основе комбинирования адаптивных классификаторов.		2
		Практическое занятие №14 Гибридные методы и алгоритмы ИБ		2

5. Фонд оценочных средств

5.1. Контрольные вопросы и задания

1. 1. Назовите методы Data Mining, предназначенные для решения задач прогноза.
2. Назовите методы Data Mining, предназначенные для решения задач классификации.
3. Назовите методы Data Mining, предназначенные для решения задач оптимизации.
4. Какие ограничения накладываются на классификационные группы в методе деревьев?
5. Какой из методов Data Mining наиболее чувствителен к выбору меры схожести объектов или ситуаций, находящихся в базе данных?
6. Как называются системы, реализующие модели рынка?
7. Назовите источники знаний для методов Data Mining.
8. Имеется база данных большого объема. Записи образуют непересекающиеся группы. Всем записям группы соответствует одно решение. Требуется по заданной ситуации найти решение. Какой метод выбрать?
9. Существует бесконечное множество ситуаций(решений), каждую можно оценить. Вычисление оценки занимает много времени. Необходимо найти ситуацию, близкую к оптимальной по выбранному критерию оценки за ограниченное время. Какой метод Data Mining использовать?
10. Основное отличие ЭС от методов Data Mining при решении задач.
11. Основное отличие ЭС от методов Data Mining при получении знаний.
12. Основное отличие ЭС от методов Data Mining при интерпретации результата.
13. Отличие источников знаний для ЭС и методов Data Mining.
14. При помощи какого инструментария создаются системы Data Mining
15. Что такое нейросеть?
16. Расскажите про биологический и формальный нейрон.
17. В каком случае нейрон возбуждается?
18. В каком случае поведение формального нейрона меняется?
19. «Пример» для обучения нейросети, и из каких частей он состоит?
20. В чем отличие нейросети прямого распространения от рекуррентной нейросети в процессе обучения?
21. В чем отличие нейросети прямого распространения от рекуррентной нейросети при остановке обучения?
22. В чем отличие обучающих данных для нейросети прямого распространения и для рекуррентной нейросети?
23. Чем определяется преобразование входных сигналов сети в выходные?
24. Перечислите этапы построения и этапы использования нейросети.
25. Что в себя включает процесс обучения нейросети?
26. Как меняется структура сети при обучении?
27. Что определяет архитектура сети?
28. Расскажите про классификацию нейросетей.
29. Как называются сети, имеющие обратные связи?

30. Рекуррентные сети – это сети, в которых сигнал…
31. В каких сетях каждый из нейронов связан со всеми остальными?
32. Как расположены нейроны в сетях прямого распространения?
33. Какие связи между нейронами в слоистых сетях?
34. В чем состоит процесс обучения с учителем?
35. В чем состоит процесс обучения без учителя?
36. При каком виде обучения нейросеть работает несколько тактов до стабилизации сигнала на ее выходе после предъявления примера.
37. Перечислите параметры управления обучением нейросети.
38. Свойства нейросети запоминать и обобщать.
39. Типы данных для обучения нейросети.
40. Критерии остановки обучения нейросети.
41. Когда целесообразно применять нейронные сети?
На каком этапе генетического алгоритма в нескольких случайно выбранных особях нового поколения изменяются некоторые гены?
43. По какому принципу выбирается индивидуум для скрещивания?
44. Какие этапы включает в себя генетический алгоритм?
45. На сколько точные решения получаются в результате работы генетического алгоритма и с чем это связано?
46. На основе какой функции строится функция приспособленности?
47. Приспособленность особи на фенотипическом уровне определяет…
48. Приспособленность особи на генотипическом уровне определяет…
49. Перечислите критерии остановки генетического алгоритма.
50. По какой причине необходимо останавливать генетический алгоритм?
51. В чем заключается принцип критерия остановки генетического алгоритма по ошибке?
52. Назовите3 условия применимости генетического алгоритма для задач, связанных с поиском оптимального решения.
53. Какие методы отбора в генетическом алгоритме вы знаете?
54. При каком методе отбора обязательно будут выживать лучший или лучшие члены популяции?
55. В чем различие между одноточечным и двухточечным кроссовером?
56. Как называется численность популяции в терминологии генетического алгоритма?
57. Назовите параметры скрещивания, которые настраиваются перед началом работы генетического алгоритма.
58. Как называется скрещивание в терминологии генетических алгоритмов?
59. В чем основное различие между целевой функции и функцией приспособленности?
60. Какие типы задач решаются с помощью генетических алгоритмов?
61.Как правило нечеткого логического вывода, сформулированное на естественном языке, преобразуется в строгую математическую модель?
62. Как происходит выполнение правила нечеткого логического вывода?
63. Как происходит нечеткий вывод?
64. Назовите модели представления знаний и перечислите способности человека, которым они соответствуют.

64. Перечислите модели представления знаний, основанные на правилах.
65. Сравните исчисления высказываний и предикатов. Приведите примеры.
66. Перечислите различные виды исчислений.
67. Какие условия определяют суть объектно-ориентированного подхода?
68. В чем состоят преимущества объектного подхода?

6. Учебно-методическое и информационное обеспечение дисциплины

6.1 Основная литература

1. Шелухин О. И., Ерохин С.Д., Полковников М. В. Технологии машинного обучения в сетевой безопасности. / Под ред. О. И. Шелухина. – М.: Горячая линия – Телеком, 2021. – 360 с. Тираж 500 экзISBN 978-5-9912-0913-7

2. Шелухин О. И. Сетевые аномалии. Обнаружение, локализация, прогнозирование. – М.: Горячая линия –Телеком, 2019. – 448 с. ISBN 978-5-9912-0756-0

3. Шелухин О. И., Осин А.В. Безопасность сетевых приложений / Под ред. О. И. Шелухина. – М.: Горячая линия – Телеком, 2021. – 224с. Тираж 500 экз.ISBN 978-5-9912-0911-3

6.2 Дополнительная литература

1. Самуйлов С.В. Алгоритмы и структуры обработки данных [Электронный ресурс]: учебное пособие / С.В. Самуйлов. — Электрон. текстовые данные. — Саратов: Вузовское образование, 2016. — 132 c. — 2227-8397. — Режим доступа: http://www.iprbookshop.ru/47275.html - ЭБС «IPRbooks», по паролюБарсегян, А. А.
2. Анализ данных и процессов: учеб. пособие / А. А. Барсегян, М. С. Куприянов, И. И. Холод, М. Д. Тесс, С. И. Елизаров. — 3-е изд., перераб. и доп. — СПб.: БХВ-Петербург, 2009. — 512 с.: ил. + CD-ROM — (Учебная литература для вузов)

6.3 Периодические издания

1. Журнал « Вопросы кибербезопасности»

7. Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины (модуля)

3. http://google.ru
4. http://www.intuit.ru/
5. https://ru.wikipedia.org/
6. http://all-ib.ru/

8. Перечень программного обеспечения и информационных справочных систем

1. Kaspersky Endpoint Security для бизнеса – Расширенный Russian Edition. Educational Renewal;

2. ОС Astra Linux Common Edition релиз «Орел» (свободное ПО);
3. LibreOffice (свободное ПО);

Кафедра «Информационная безопасность» располагает кадровыми ресурсами, гарантирующими качество подготовки аспиранта по специальности 2.3.6 Методы и системы защиты информации, информационная безопасность **в соответствии с ФГТ.**

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

Учебная аудитория для проведения лекционных занятий, укомплектованная специализированной мебелью и техническими средствами обучения, служащими для представления учебной информации большой аудитории: наборами демонстрационного оборудования и учебно-наглядных пособий, обеспечивающими тематические иллюстрации, соответствующие рабочей программе дисциплины.

2. Учебная аудитория для проведения практических и лабораторных занятий, укомплектованная специализированной мебелью и техническими средствами обучения, служащими для представления учебной информации большой аудитории: наборами демонстрационного оборудования и учебно-наглядных пособий, обеспечивающими тематические иллюстрации, соответствующие рабочей программе дисциплины, оснащенная компьютерной техникой.

10. Методические рекомендации студентам по освоению дисциплины

В процессе изучения дисциплины предусмотрены следующие формы контроля по овладению компетенциями: текущий, промежуточный контроль (экзамен), контроль самостоятельной работы студентов.

Текущий контроль осуществляется в течение семестра в виде устного опроса студентов на практических занятиях, в виде письменных проверочных работ по текущему материалу, а так же в виде сетевого тестирования в рамках контрольных точек, проводимых в соответствии с графиками учебного процесса. Устные ответы и письменные работы студентов оцениваются. Оценки доводятся до сведения студентов. Результаты тестирования суммируются с баллами, полученными по остальным формам контроля, и выставляются в электронные рейтинговые ведомости.

Промежуточный контроль осуществляется в форме экзамена в конце семестра.

Самостоятельная работа студента по дисциплине включает:

- Проработку лекционного материала, а также материала, изучаемого на практических занятиях;
- Подготовку к экзамену.