

Методические рекомендации к курсу «Программирование
защищенных интеллектуальных систем» для
специальности 09.03.04 «Программная инженерия»

Никольская Ксения Юрьевна

2022

Цель дисциплины: Целью дисциплины является получение теоретических и практических знаний в области информационной безопасности.

Задачи дисциплины: Цель изучения дисциплины достигается путем решения следующих задач: изучение теоретических основ правового регулирования систем искусственного интеллекта в сфере информационной безопасности; повышения уровня профессиональной культуры и исполнительской дисциплины бакалавров, понимание необходимости использования средств и методов информационной безопасности, в профессиональной деятельности по специальности; освоения основные средств и методов обеспечения информационной безопасности, методик их результативного использования.

Основная литература по курсу:

1. Леонтьев, А.С. Защита информации: учебное пособие / А.С. Леонтьев. – Москва: РТУ МИРЭА, 2021. – 79 с. – Текст: электронный // Лань: электронно-библиотечная система. Режим доступа: для авториз. пользователей.
2. Краковский, Ю.М. Методы защиты информации: учебное пособие для вузов / Ю.М. Краковский. – 3-е изд., перераб. – Санкт-Петербург: Лань, 2021. – 236 с. – ISBN 978-5-8114-5632-1. – Текст: электронный // Лань: электронно-библиотечная система. Режим доступа: для авториз. пользователей.
3. Тумбинская, М.В. Защита информации на предприятии: учебное пособие / М.В. Тумбинская, М.В. Петровский. – Санкт-Петербург: Лань, 2020. – 184 с. – ISBN 978-5-8114-4291-1. – Текст: электронный // Лань: электронно-библиотечная система. Режим доступа: для авториз. пользователей.

Дополнительная литература по курсу:

1. Чيو, К. Машинное обучение и безопасность: руководство / К. Чيو, Д. Фримэн; перевод с английского А. В. Снастина. – Москва: ДМК Пресс, 2020. – 388 с. – ISBN 978-5-97060-713-8. – Текст: электронный // Лань: электронно-библиотечная система. Режим доступа: для авториз. пользователей.

Объем и виды учебной работы:

- Семестр: 7.
- Общая трудоёмкость дисциплины: 144 часа.
- Лекции: 16 часов.
- Практические занятия: 32 часа.

Компетенции:

1. УК-91 Способен планировать и организовывать свою деятельность в цифровом пространстве с учетом правовых и этических норм взаимодействия человека и искусственного интеллекта и требований информационной безопасности:

Знает: цели, задачи и предмет, основные понятия информационной безопасности, информационные угрозы, их классификацию, возможные последствия для организаций различных форм собственности и критерии оценки защищенности информационных систем и систем искусственного интеллекта.

Умеет: работать с информацией с учетом требований информационной безопасности.

Имеет практический опыт: создания доверенных систем искусственного интеллекта в задачах информационной безопасности.

2. ОПК-3 Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности :

Знает: основные нормативно-правовую базу в области информационной безопасности.

Умеет: создавать доверенные обучающие наборы данных для обучения алгоритмов машинного обучения в задачах информационной безопасности.

Имеет практический опыт: тестирования обучающих наборов данных в задачах информационной безопасности.

3. ОПК-4 Способен участвовать в разработке стандартов, норм и правил, а также технической документации, связанной с профессиональной деятельностью:

Знает: основные стандарты в области информационной безопасности и искусственного интеллекта.

Умеет: разрабатывать подходы, согласно действующих норм, для создания доверенных обучающих наборов данных и доверенных систем искусственного интеллекта в задачах информационной безопасности.

Имеет практический опыт: создания доверенных обучающих наборов данных.

4. ОПК-6 Способен разрабатывать алгоритмы и программы, пригодные для практического использования, применять основы информатики и

программирования к проектированию, конструированию и тестированию программных продуктов:

Знает: основы разработки доверенных систем информационной безопасности.

Умеет: разрабатывать алгоритмы машинного обучения для задач информационной безопасности.

Имеет практический опыт: тестирования алгоритмов машинного обучения в задачах информационной безопасности.

Рекомендации по подготовке к тестированиям по усвоению материалов лекций:

Рекомендации по подготовке к тестированию по усвоению материалов 1 раздела «Правовое регулирование систем искусственного интеллекта в сфере информационной безопасности»:

1. Дайте определение искусственного интеллекта.
2. Дайте определение технологии искусственного интеллекта.
3. Перечислите виды искусственного интеллекта.
4. Перечислите формы искусственного интеллекта.
5. Перечислите этапы развития искусственного интеллекта.
6. Перечислите подходы к регулированию искусственного интеллекта.

Рекомендации по подготовке к тестированию по усвоению материалов 2 раздела «Этические аспекты применения искусственного интеллекта в сфере информационной безопасности»:

1. Дайте определение этики искусственного интеллекта.
2. Перечислите какой потенциальный вред могут нанести системы искусственного интеллекта.
3. Является ли усложняющим фактором то, что существует множество различных типов искусственного интеллекта.
4. Дайте определение сильному и слабому искусственному интеллекту.
5. Является ли технология искусственного интеллекта этичной или не этичной.

Рекомендации по подготовке к тестированию по усвоению материалов 3 раздела «Искусственный интеллект в механизмах идентификации и аутентификации»:

1. Перечислите методы статической биометрической идентификации.
2. Дайте определение авторизации.
3. Дайте определение аутентификации.
4. Дайте определение администрированию.
5. Дайте определение идентификации.
6. Перечислите методы идентификации с использованием искусственного интеллекта.
7. Перечислите методы аутентификации с использованием искусственного интеллекта.
8. Перечислите методы администрирования с использованием искусственного интеллекта.

Рекомендации по подготовке к тестированию по усвоению материалов 4 раздела «Проектирование интеллектуальных защищенных информационных систем»:

1. Как искусственный интеллект помогает в решении задачи анализа возможных угроз.

2. Как искусственный интеллект помогает в решении задачи сетевой безопасности.

3. Как искусственный интеллект помогает в решении задачи моделирования угроз безопасности.

4. Какие существуют правила для формирования доверенного обучающего набора данных.

5. Какие требования должны быть выполнены при проектировании систем искусственного интеллекта.

Рекомендации по подготовке к тестированию по усвоению материалов **5 раздела «Компьютерные вирусы и антивирусное программное обеспечение с искусственным интеллектом»:**

1. Дайте определение вредоносным компьютерным программам.

2. Дайте определение загрузочным вирусам.

3. В чем заключается косвенный способ заражения.

4. Дайте определение макровирусам.

5. В чем заключается суть непосредственного способа размножения.

6. В чем отличия антивирусов с применением алгоритмов искусственного интеллекта.

7. В чем отличия вирусов с применением алгоритмов искусственного интеллекта.

Рекомендации по подготовке к тестированию по усвоению материалов **6 раздела «Искусственный интеллект и защита информации в компьютерных сетях»:**

1. Перечислите инструменты для интеллектуального анализа данных.

2. Перечислите проблемы искусственного интеллекта в задаче классификации сетевого трафика.

3. Какое влияние на модель оказывает фоновый трафик.

4. Классификация трафика в режиме реального времени.

5. Классификация зашифрованного трафика.

Рекомендации по подготовке к тестированию по усвоению материалов **7 раздела «Искусственный интеллект в биометрических системах защиты информации»:**

1. Что может выступать в качестве биометрического идентификатора.

2. На чем основаны динамические методы идентификации.

3. Перечислите динамические методы идентификации.

4. Перечислите статические методы идентификации.

5. На чем основаны статические методы идентификации.

Рекомендации по подготовке к тестированию по усвоению материалов **8 раздела «Криптография и искусственный интеллект»:**

1. Дайте определение криптографии.

2. Дайте определение шифрованию.

3. Дайте определение интеллектуальной криптографической системе.

4. Перечислите криптографические технологии обработки данных с использованием технологий искусственного интеллекта.

5. В чем заключается суть механизма безопасной коммуникации на базе алгоритмов искусственного интеллекта.

Рекомендации по подготовке к тестированиям по усвоению материалов практических занятий:

Рекомендации по подготовке к сдаче 1 практического задания «Этические аспекты применения искусственного интеллекта в сфере информационной безопасности»:

1. Перечислите основные виды нормативно-правовых актов, которые существуют на данный момент в мире в области этики искусственного интеллекта.

2. Перечислите и раскройте основные пункты закона о робототехнике России.

3. Перечислите и раскройте основные рекомендации Евросоюза по гражданско-правовым нормам в робототехнике.

4. Перечислите и раскройте основные нормы в законе о робототехнике в США.

5. Перечислите и раскройте основные нормы в законе о робототехнике в Китае.

6. Перечислите и раскройте основные нормы в законе о робототехнике в Канаде.

Рекомендации по подготовке к сдаче 2 практического задания «Искусственный интеллект в механизмах идентификации и аутентификации»:

1. Дайте определение взаимной аутентификации.

2. Имеет ли значение авторизация без аутентификации, и почему.

3. Имеет ли значение авторизация без идентификации, и почему.

4. Имеет ли значение аутентификация без предварительной идентификации, и почему.

5. Имеет ли значение идентификация без аутентификации, и почему.

6. Перечислите и дайте краткую характеристику методам биометрической идентификации.

Рекомендации по подготовке к сдаче 3 практического задания «Проектирование интеллектуальных защищенных информационных систем»:

1. Перечислите требования к используемым алгоритмам искусственного интеллекта в системах информационной безопасности.

2. Каким нормативным документам следует руководствоваться при создании систем искусственного интеллекта, которые работают с персональными данными.

3. Каким нормативным документам следует руководствоваться при создании систем искусственного интеллекта, которые работают с медицинскими данными.

4. Какова роль стандартов информационной безопасности.
5. Перечислите единые критерии безопасности информационных технологий.
6. Перескажите 5 международных стандартов информационной безопасности, и дайте им краткое пояснение.

Рекомендации по подготовке к сдаче **4 практического задания «Искусственный интеллект и защита информации в компьютерных сетях»:**

1. Какие алгоритмы искусственного интеллекта используются для классификации сетевого трафика.
2. Какие алгоритмы искусственного интеллекта используются для сетевых атак.
3. Какие алгоритмы искусственного интеллекта применяют для анализа журналов СЗИ.
4. Перечислите основные правила создания наборов данных для обучения алгоритмов искусственного интеллекта в задаче сетевого трафика.
5. Перечислите методы захвата трафика.
6. Перечислите сетевые анализаторы трафика и принцип их работы.

Рекомендации по подготовке к сдаче **5 практического задания «Искусственный интеллект в биометрических системах защиты информации»:**

1. Перечислите основные правила для создания безопасного обучающего набора данных для систем искусственного интеллекта.
2. Перечислите примеры применения искусственного интеллекта в биометрических системах.
3. Перечислите риски при использовании алгоритмов искусственного интеллекта в биометрических системах.
4. Перечислите стандарты создания биометрических систем с использованием алгоритмов искусственного интеллекта.
5. Перечислите алгоритмы искусственного интеллекта для работы с биометрическими данными и приведите примеры.
6. В чем заключается суть биометрической идентификации на основе алгоритмов машинного обучения.

Рекомендации по подготовке к сдаче **6 практического задания «Криптография и искусственный интеллект»:**

1. Симметричное шифрование.
2. Аутентификация сообщений.
3. Функция хеширования.
4. Дайте определение ключу шифрования.
5. Дайте определение алгоритму шифрования.
6. Как взламывают алгоритмы шифрования?

Вопросы к экзамену:

7. Дайте определение искусственного интеллекта.
8. Дайте определение технологии искусственного интеллекта.
9. Перечислите виды искусственного интеллекта.
10. Перечислите формы искусственного интеллекта.
11. Перечислите этапы развития искусственного интеллекта.
12. Перечислите подходы к регулированию искусственного интеллекта.
13. Дайте определение этики искусственного интеллекта.
14. Перечислите какой потенциальный вред могут нанести системы искусственного интеллекта.
15. Является ли усложняющим фактором то, что существует множество различных типов искусственного интеллекта.
16. Дайте определение сильному и слабому искусственному интеллекту.
17. Является ли технология искусственного интеллекта этичной или не этичной.
18. Перечислите методы статической биометрической идентификации.
19. Дайте определение авторизации.
20. Дайте определение аутентификации.
21. Дайте определение администрированию.
22. Дайте определение идентификации.
23. Перечислите методы идентификации с использованием искусственного интеллекта.
24. Перечислите методы аутентификации с использованием искусственного интеллекта.
25. Перечислите методы администрирования с использованием искусственного интеллекта.
26. Как искусственный интеллект помогает в решении задачи анализа возможных угроз.
27. Как искусственный интеллект помогает в решении задачи сетевой безопасности.
28. Как искусственный интеллект помогает в решении задачи моделирования угроз безопасности.
29. Какие существуют правила для формирования доверенного обучающего набора данных.
30. Какие требования должны быть выполнены при проектировании систем искусственного интеллекта.
31. Дайте определение вредоносным компьютерным программам.
32. Дайте определение загрузочным вирусам.
33. В чем заключается косвенный способ заражения.
34. Дайте определение макровирусам.
35. В чем заключается суть непосредственного способа размножения.
36. В чем отличия антивирусов с применением алгоритмов искусственного интеллекта.

37. В чем отличия вирусов с применением алгоритмов искусственного интеллекта.
38. Перечислите инструменты для интеллектуального анализа данных.
39. Перечислите проблемы искусственного интеллекта в задаче классификации сетевого трафика.
40. Какое влияние на модель оказывает фоновый трафик.
41. Классификация трафика в режиме реального времени.
42. Классификация шифрованного трафика.
43. Что может выступать в качестве биометрического идентификатора.
44. На чем основаны динамические методы идентификации.
45. Перечислите динамические методы идентификации.
46. Перечислите статические методы идентификации.
47. На чем основаны статические методы идентификации.
48. Дайте определение криптографии.
49. Дайте определение шифрованию.
50. Дайте определение интеллектуальной криптографической системе.
51. Перечислите криптографические технологии обработки данных с использованием технологий искусственного интеллекта.
52. В чем заключается суть механизма безопасной коммуникации на базе алгоритмов искусственного интеллекта.
53. Перечислите основные виды нормативно-правовых актов, которые существуют на данный момент в мире в области этики искусственного интеллекта.
54. Перечислите и раскройте основные пункты закона о робототехнике России.
55. Перечислите и раскройте основные рекомендации Евросоюза по гражданско-правовым нормам в робототехнике.
56. Перечислите и раскройте основные нормы в законе о робототехнике в США.
57. Перечислите и раскройте основные нормы в законе о робототехнике в Китае.
58. Перечислите и раскройте основные нормы в законе о робототехнике в Канаде.
59. Дайте определение взаимной аутентификации.
60. Имеет ли значение авторизация без аутентификации, и почему.
61. Имеет ли значение авторизация без идентификации, и почему.
62. Имеет ли значение аутентификация без предварительной идентификации, и почему.
63. Имеет ли значение идентификация без аутентификации, и почему.
64. Перечислите и дайте краткую характеристику методам биометрической идентификации.

65. Перечислите требования к используемым алгоритмам искусственного интеллекта в системах информационной безопасности.

66. Каким нормативным документам следует руководствоваться при создании систем искусственного интеллекта, которые работают с персональными данными.

67. Каким нормативным документам следует руководствоваться при создании систем искусственного интеллекта, которые работают с медицинскими данными.

68. Какова роль стандартов информационной безопасности.

69. Перечислите единые критерии безопасности информационных технологий.

70. Пересилите 5 международных стандартов информационной безопасности, и дайте им краткое пояснение.

71. Какие алгоритмы искусственного интеллекта используются для классификации сетевого трафика.

72. Какие алгоритмы искусственного интеллекта используются для сетевых атак.

73. Какие алгоритмы искусственного интеллекта применяют для анализа журналов СЗИ.

74. Перечислите основные правила создания наборов данных для обучения алгоритмов искусственного интеллекта в задаче сетевого трафика.

75. Перечислите методы захвата трафика.

76. Перечислите сетевые анализаторы трафика и принцип их работы.

77. Перечислите основные правила для создания безопасного обучающего набора данных для систем искусственного интеллекта.

78. Перечислите примеры применения искусственного интеллекта в биометрических системах.

79. Перечислите риски при использовании алгоритмов искусственного интеллекта в биометрических системах.

80. Перечислите стандарты создания биометрических систем с использованием алгоритмов искусственного интеллекта.

81. Перечислите алгоритмы искусственного интеллекта для работы с биометрическими данными и приведите примеры.

82. В чем заключается суть биометрической идентификации на основе алгоритмов машинного обучения.

83. Симметричное шифрование.

84. Аутентификация сообщений.

85. Функция хеширования.

86. Дайте определение ключу шифрования.

87. Дайте определение алгоритму шифрования.

88. Как взламывают алгоритмы шифрования?