Перечень экзаменационных вопросов по курсу Теория автоматов и шифров, 2025/2026 уч год

В каждом билете четыре вопроса – два теоретических и два практических. Практические задания выполняются письменно, по первой части курса будет задана таблица переходов конечного автомата/ граф переходов/ матрица переходов, необходимо методом таблиц Рк или таблиц пар определить классы эквивалентности. По второй части курса будет задан текст/ тип шифра, необходимо провести зашифрование/ расшифрование данного фрагмента указанным методом.

1. Модель многополюсного черного ящика, пример

2. Понятие состояния, пример

3. Понятие основной модели, пример

4. Таблица переходов, граф переходов, матрица переходов, пример

5. Классификация состояний и подавтоматов. Изоморфные автоматы, пример (с доказательством)

6. Эквивалентность состояний, понятие, свойства (с доказательством)

7. К- эквивалентность, понятие, свойства (с доказательством, включая Лемму 5)

8.Разбиение автомата методом таблиц Рк (алгоритм)

9. Разбиение автомата методом таблицы пар (алгоритм)

10. Что такое шифр перестановки? На чем основан шифр перестановки?

11. Что такое шифр сцитала? На чем основывается шифр сцитала? Какой максимальный диаметр жезла мог быть использован для шифра сцитала? Каким образом предполагается расшифровывать шифр сцитала?

12. Что такое шифр магического квадрата, и каков принцип его действия?

13. На чем основывается принцип работы шифра Виженера? Что лежит в основе шифра Виженера?

14. Что такое шифр гаммирования? Кто предложил шифр гаммирования?

15. Что выбирается в качестве ключа в шифре гаммирования?

16. В чем отличие шифра Виженера от шифра гаммирования?

17. Что такое шифр Чейза? Опишите принцип работы шифра Чейза.

18. Каковы функции центра сертификации ключей?

19. В чем суть предварительного распределения ключей?

20. Какими методами обеспечивается конфиденциальность информации.

21. Что такое целостность информации.

22. Алгебраическая модель шифра.

23. Вероятностная модель шифра.

24. Математические модели открытого текста

25. С какими целями в криптографии вводят модели открытых текстов?

26. Какие подходы используются для распознавания открытых текстов?

27. Математическое понятие шифров замены и перестановки