Вопросы к зачету
по дисциплине «Теория псевдослучайных генераторов»
для специальности «Компьютерная безопасность»
составил: к.ф-м.н., доцент Перцева Ирина Анатольевна

8семестр

Дисциплина «Теория псевдослучайных генераторов»
Примерный перечень вопросов к зачету:

1. определения ГСП и ГПСП
2. принципы построения ГПСП
3. требования к ГПСП
4. классификацию ГПСП
5. структурная схема ГПСП
6. приемы и особенности построения ГПСП при использовании блочных шифров
7. достоинства и недостатки криптографических ГПСП с использованием функций блочных шифров
8. приемы и особенности построения ГПСП при использовании поточных шифров
9. достоинства и недостатки криптографических ГПСП с использованием функций поточных шифров
10. приемы и особенности построения ГПСП с использованием односторонних функций
11. достоинства и недостатки криптографических ГПСП с использованием односторонних функций
12. линейный конгруэнтный метод построения ГПСЧ и его вариации
13. достоинства и недостатки линейного конгруэнтного метода
14. построения ГПСЧ и его вариаций
15. основные теоремы о выборе параметров и максимальной
16. длине периода для линейного конгруэнтного метода
17. построения ГПСЧ и его вариаций
18. метод построения ГПСП на регистрах сдвига с линейными
19. обратными связями и его вариации
20. достоинства и недостатки построения ГПСП на регистрах
21. сдвига с линейными обратными связями и его вариаций
22. основные теоремы о выборе параметров и максимальной
23. длине периода для ГПСП на регистрах сдвига с линейными
24. обратными связями и его вариаций
25. достоинства и недостатки графических тестов качества
26. псевдослучайных последовательностей
27. основные графические тесты качества псевдослучайных
28. последовательностей
29. статистические тесты качества псевдослучайных
30. последовательностей Д. Кнута
31. достоинства и недостатки статистических тестов качества
32. псевдослучайных последовательностей Д.Кнута
33. основные статистические тесты качества псевдослучайных
34. последовательностей НИСТ.
35. достоинства и недостатки статистических тестов качества
36. псевдослучайных последовательностей НИСТ