Приложение к рабочей программе дисциплины

МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ ПО ОРГАНИЗАЦИИ САМОСТОЯТЕЛЬНОЙ РАБОТЫ ОБУЧАЮЩИХСЯ

Наименование дисциплины	Теоретико-числовые методы в криптографии
Специальность	10.05.03 Информационная безопасность автоматизированных систем
Специализация	Безопасность открытых информационных систем
Форма обучения	очная
Разработчик(и)	Захаров С.Д., доцент кафедры информационной безопасности

1.Темы дисциплины для самостоятельного освоения обучающимися
Отсутствуют

2. План самостоятельной работы

п/п	Учебные встречи	Виды самостоятельной работы	Форма отчетности/ контроля	Количество баллов	Рекомендуемый бюджет времени на выполнение (ак.ч.)*
1.	УВ №4. Практическое занятие 1-2. «Введение в криптографические протоколы. Цифровые подписи общего назначения.».	Проработка лекций. Чтение обязательной и дополнительной литературы, выполнение практических заданий	Отчет в форме Пояснительной записки. Код программы	2	10
2.	УВ №8. Практическое занятие 3-4. «Эллиптические кривые. Цифровые подписи на эллиптической кривой.»	Проработка лекций. Чтение обязательной и дополнительной литературы, выполнение практических заданий	Отчет в форме Пояснительной записки. Код программы	2	10
3.	УВ №12. Практическое занятие 5-6. «Цифровые подписи специального назначения. Свойства цифровых подписей.»	Проработка лекций. Чтение обязательной и дополнительной литературы, выполнение практических заданий	Отчет в форме Пояснительной записки. Код программы	2	10
4.	УВ №16. Практическое занятие 7-8. «Электронная жеребьевка. Разделение секрета.»	Проработка лекций. Чтение обязательной и дополнительной литературы, выполнение практических заданий	Отчет в форме Пояснительной записки. Код программы	2	10
5.	УВ № 20. Практическое занятие 9-10. «Конфиденциальные вычисления. Покер по телефону.»	Проработка лекций. Чтение обязательной и дополнительной литературы, выполнение практических заданий	Отчет в форме Пояснительной записки. Код программы	2	10
6.	УВ № 24. Практическое занятие 11-12. «Идентификация и аутентификация. Управление ключами.»	Проработка лекций. Чтение обязательной и дополнительной литературы, выполнение практических заданий	Отчет в форме Пояснительной записки. Код программы	2	10

7.	УВ № 28. Практическое занятие 13-14. «Электронная монета. Электронные выборы.»	Проработка лекций. Чтение обязательной и дополнительной литературы, выполнение практических заданий	Отчет в форме Пояснительной записки. Код программы	2	10
8.	УВ № 32. Практическое занятие 15-16. «Прикладные сетевые протоколы»	Проработка лекций. Чтение обязательной и дополнительной литературы, выполнение практических заданий	Отчет в форме Пояснительной записки. Код программы	2	10
	ИТОГО: часов самостоятельной работы				80

3. Требования и рекомендации по выполнению самостоятельных работ обучающихся, критерии оценивания

3.1. Оформление работы

Отчет о самостоятельной работе оформляется в виде пояснительной записки в электронном или рукописном виде.

ПРИМЕРНЫЙ ШАБЛОН оформления пояснительной записки к практическому занятию

Иванов Петр, КБ-20.01

Практическое занятие № *N*

Тема «Название темы»

1. Постановка задачи

Формулировка задачи в общей постановке, номер варианта задания и свои исходные данные. Можно привести список выполняемых заданий.

2. Метод решения (название метода)

Описание метода: краткие теоретические сведения, структура, алгоритм, реализация.

3. Анализ результатов

Привести скриншоты основных этапов алгоритма и полученных результатов.

Шрифт 14 Times New Roman, выравнивание по ширине, междустрочный интервал «одинарный».

Отчет в рукописной форме должен содержать подробное выполнение решения поставленной задачи.

3.2. Сроки выполнения, требования к объему.

Задания для самостоятельной работы выполняются в течение семестра, в котором читается

данная дисциплина. Объем не превышает 10 стр. текста.

3.3. Критерии оценивания

При проведении текущего контроля для оценки заданий применяется система оценивания:

- 2 балла. Студент имеет четкое представление о видах математических моделей, о способах построения и реализации алгоритма применяемого метода решения; анализа полученных результатов. Предоставлен код работающей программы.
- 1 балл. Задание в основном соответствует требованиям. Студент продемонстрировал самостоятельную реализацию алгоритмов решения практических задач, умение давать анализ результатов решения. Предоставлен код программы.
- 0 баллов - Задание выполнено на низком уровне, студент не владеет терминологией, не ориентируется в теоретических вопросах и не способен использовать знания для решения практических задач.

4. Рекомендации по самоподготовке к промежуточной аттестации по дисциплине

4.1. Вопросы к экзамену для самопроверки:

1. Основные понятия теории чисел. Теорема делимости.
2. Наибольший общий делитель и алгоритм Евклида.
3. Цепные дроби и алгоритм Евклида.
4. Наименьше общее кратное. Простые числа.
5. Теоремы Евклида о простых числах. Решето Эратосфена.
6. Основные свойства простых чисел. Теорема о единственности разложения на простые сомножители.
7. Теорема о делителях числа и ее следствия.
8. Асимптотический закон распределения простых чисел.
9. Функция Эйлера, ее свойства.
10. Сравнения. Свойства сравнений.
11. Полная система вычетов, приведенная система вычетов. Алгебраические свойства, обратный элемент.
12. Теорема Эйлера, теорема Ферма. Следствие.
13. Тест Ферма на простоту. Числа Кармайкла. Теорема Кармайкла.
14. Применение теоремы Ферма в криптосистеме RSA.
15. Сравнения с одним неизвестным 1-й степени.
16. Система сравнений 1-й степени. Китайская теорема об остатках.
17. Применение Китайской теоремы об остатках в RSA
18. Квадратичные сравнения по простому модулю.
19. Символ Лежандра и его свойства.
20. Решение квадратичных сравнений по простому модулю.
21. Число решений квадратичного сравнения по составному модулю.
22. Символ Якоби, его свойства. Тест Соловея-Штрассена.
23. Квадратичные сравнения по модулю RSA. Связь задач извлечения корней и факторизации. Криптосистема Рабина.
24. Квадраты и псевдоквадраты. Числа Блюма.

25. BBS-генератор. Криптосистема Блюма-Гольдвассер, криптосистема ГольдвассерМикали.
26. Тест Миллера-Рабина.
27. Порядок группы. Порядок элемента в группе. Порождающий элемент.
28. Существование порождающего элемента в Z*n
29. Критерий Люка.
30. Теорема Сэлфриджа и тест Миллера.
31. Теорема Поклнгтона и тест на простоту на ее основе.
32. Числа Ферма, теорема Пепина, тест Пепина.
33. Числа Мерсена. Тест Лукаса-Лемера.
34. Теорема Диемитко. Процедура генерации простых чисел ГОСТ Р 34.10-94.
35. Дискретный логарифм. Проблема Диффи-Хелмана. Криптосистема ЭльГамаля.
36. Проблема факторизации. Метод пробных делений.
37. Метод Ферма факторизации.
38. Метод квадратичного решета.
39. Ро-метод Полларда факторизации.
40. р—1 – метод факторизации.
41. Метод Диксона.
42. Задача дискретного логарифмирования. Метод прямого поиска.
43. Ро-метод Полларда дискретного логарифмирования.
44. Алгоритм Полига-Хеллмана.
45. Метод «Шаг младенца-шаг великана».
46. Метод исчисления порядка.

4.2. Система оценивания

По окончании курса по данной дисциплине учебным планом предусмотрен **экзамен**. Студент может получить оценку по результатам работы в течение семестра при условии успешного освоения **61 %** учебного материала (**61 балл**, оценка «удовлетворительно»). По завершению изучения дисциплины студентам, не набравшим необходимое количество баллов для получения финальной оценки, или желающим улучшить свой результат, предлагается сдать экзамен.

Критерии оценки для **экзамена:**

Ниже 61 балла – «неудовлетворительно»,

61-75 баллов – «удовлетворительно»,

76-90 баллов – «хорошо»,

91-100 баллов – «отлично».

Экзамен проводится в устно-письменной форме (на усмотрение преподавателя).

Каждый экзаменационный билет содержит по два вопроса из разных разделов курса. Преподаватель вправе задать уточняющий вопрос по каждому из вопросов билета. Итоговая оценка выводится как средняя арифметическая из оценок по двум вопросам билета.

Ответ на каждый из вопросов оценивается по следующей шкале:

2 («неудовлетворительно») - студент не ответил на вопрос либо содержание ответа

на раскрывает сути вопроса.

3 («удовлетворительно») - студент отвечает по существу, но не демонстрирует целостного представления по вопросу, не может аргументировать свой ответ.

4 («хорошо») - студент отвечает по существу, демонстрирует целостное представление по вопросу; не может аргументировать свой ответ либо аргументация не обоснована.

5 («отлично») - студент дает полный, развернутый, аргументированный ответ на вопрос.

Результаты выполнения самостоятельной работы (Пояснительная записка, рукописный отчет, код программы) загружаются в соответствующий раздел дисциплины «Криптографические протоколы» на образовательной платформе LMS ТюмГУ.