Документ подписан простой электронной подписью
Информация о владельце:
ФИО: Романчук Иван Сергеевич
Должность: Ректор
Дата подписания: 20.01.2025 17:29:21
Уникальный программный ключ:
6319edc2b582ffdacea443f01d5779368d0957ac34f5cd074d81181530452479

Приложение к рабочей программе дисциплины

# МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ ПО ОРГАНИЗАЦИИ САМОСТОЯТЕЛЬНОЙ РАБОТЫ ОБУЧАЮЩИХСЯ

| | |
|---|---|
| Наименование дисциплины | Криптографические протоколы |
| Специальность | 10.05.01 Компьютерная безопасность |
| Специализация | Безопасность распределенных компьютерных систем |
| Форма обучения | очная |
| Разработчик(и) | Сергеев В.В., 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. Понятие о криптографических протоколах. Основные виды протоколов. Примитивные и прикладные протоколы.
2. Понятие о криптографических протоколах. Полнота и корректность.
3. Цифровые подписи общего назначения. Математическая модель. Атаки и угрозы.
4. Цифровые подписи RSA и Рабина.
5. Цифровая подпись Эль-Гамаля и связанные с ней схемы.
6. Стандарты DSA и ГОСТ Р 34.10-94.
7. Эллиптическая кривая над полем вещественных чисел.
8. Эллиптическая кривая над полем GF(p). Задача дискретного логарифмирования на эллиптической кривой.
9. Подпись Эль-Гамаля на эллиптической кривой.
10. Стандарты ECDSA и ГОСТ Р 34.10-2012.
11. Цифровые подписи специального назначения. Коллективная подпись.
12. Неотрицаемая подпись.
13. Слепая подпись.
14. Подписи со скрытым каналом.
15. Протоколы подбрасывания монеты. Применение протоколов подбрасывания монеты для выработки сеансовых ключей.
16. Связанность и секретность протокола электронной жеребьевки. Пример протокола с безусловной связанностью.
17. Связанность и секретность протокола электронной жеребьевки. Пример протокола с безусловной секретностью.
18. Протоколы привязки к биту. Блоб.
19. Понятие о разделении секрета. Группа доступа, структура доступа. Требования к ним. Минимальная группа доступа.
20. Совершенная СРС (система разделения доступа), идеальная СРС.

21. Пороговые схемы разделения секрета. Схема Шамира, ее совершенность и идеальность.

22. Схема Блэкли. Вопрос о ее совершенности и идеальности.

23. СРС на основе Китайской теоремы об остатках. Вопрос о ее совершенности и идеальности.

24. СРС для произвольной структуры доступа. Вопрос о ее совершенности и идеальности.

25. Протоколы конфиденциальных вычислений. Задача миллионеров и протокол Яо.

26. Конфиденциальные вычисления. Логический контур. Протокол GMW.

27. Протоколы идентификации. Классификация. Требования.

28. Парольные схемы. Разновидности. Область применения.

29. Схемы рукопожатия.

30. Интерактивные системы доказательств. Полнота, корректность. Пример интерактивной системы доказательств для языка «Квадратичные невычеты».

31. Доказательства с нулевым разглашением. Статистическая неразличимость, вероятностная неразличимость. Пример интерактивного доказательства с нулевым разглашением для языка «Изоморфизм графов».

32. Протоколы идентификации на основе теории ИСД с нулевым разглашением. Схема Фиата-Шамира. Схема Файге-Фиата-Шамира. Их полнота и корректность.

33. Схема идентификации Шнорра. Схема Брикелла-МакКарли. Их полнота и корректность.

34. Схема идентификации Окамото и теорема о ее условной стойкости.

35. Схема Гиллу-Кискатр. Ее полнота и корректность.

36. Протокол «Покер по телефону».

37. Электронная монета. Электронные деньги. Требования к схемам электронных денег. Схема Шаума.

38. Протоколы голосования.

39. Управление ключами. Этапы жизненного цикла ключей. Задачи управления ключами, решаемые криптографическими средствами.

40. Централизованная выработка ключа. Совместная выработка ключа. Требования к секретному ключу. Алгоритм фон Неймана.

41. Распределение ключа при наличии доверенного центра. Распределение секретного ключа без участия доверенного центра.

42. Схемы Wide-Mouth Frog, Yahalom. Их анализ.

43. Протокол Нидхема-Шредера. Его анализ.

44. Протокол Отвея-Рииса. Его анализ.

45. Бесключевой протокол Шамира, протокол Диффи-Хэллмана и атака «Человек посередине». Противодействие этой атаке.

46. Протокол Нидхема-Шредера на основе шифра с открытым ключом.

47. Широковещательное распределение ключей.

48. Стандарт x.509.

49. Инфраструктура открытых ключей. Сертификаты и справочники открытых ключей. Многоуровневая система удостоверяющих центров

**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.