Приложение к рабочей программе дисциплины

МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ ПО ОРГАНИЗАЦИИ САМОСТОЯТЕЛЬНОЙ РАБОТЫ ОБУЧАЮЩИХСЯ

Наименование дисциплины	Модели безопасности компьютерных систем
Специальность	10.05.01 Компьютерная безопасность
Специализация	Безопасность компьютерных систем и сетей (связь, информационные и коммуникационные технологии)
Форма обучения	Очная
Разработчик(и)	Паюсова Т.И., 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 №2, Практическое занятие 1, «Тема 1. Математические основы построения моделей безопасности» (теория автоматов)	Проработка лекций. Чтение обязательной и дополнительной литературы, выполнение практического задания	Отчет в форме пояснительной записки. Исходный код программы	2	5
2.	УВ №5, Практическое занятие 2, «Тема 1. Математические основы построения моделей безопасности» (теория автоматов)	Проработка лекций. Чтение обязательной и дополнительной литературы, выполнение практического задания	Отчет в форме пояснительной записки. Исходный код программы	2	5
3.	УВ №8, Практическое занятие 3, «Тема 2. Математические основы построения моделей безопасности» (теория графов)	Проработка лекций. Чтение обязательной и дополнительной литературы, выполнение практического задания	Отчет в форме пояснительной записки. Исходный код программы	2	5
4.	УВ №11, Практическое занятие 4, «Тема 2. Математические основы построения моделей безопасности»	Проработка лекций. Чтение обязательной и дополнительной литературы, выполнение практического задания	Отчет в форме пояснительной записки. Исходный код программы	2	5

	(теория графов)				
5.	УВ №14, Практическое занятие 5, «Тема 3. Математические основы построения моделей безопасности» (вероятностный подход к обеспечению ИБ)	Проработка лекций. Чтение обязательной и дополнительной литературы, выполнение практического задания	Отчет в форме пояснительной записки. Исходный код программы	2	5
6.	УВ №17, Практическое занятие 6, «Тема 3. Математические основы построения моделей безопасности» (вероятностный подход к обеспечению ИБ)	Проработка лекций. Чтение обязательной и дополнительной литературы, выполнение практического задания	Отчет в форме пояснительной записки. Исходный код программы	2	5
7.	УВ №20, Практическое занятие 7, «Тема 4. Дискреционная модель доступа» (модель Харрисона-Руззо-Ульмана)	Проработка лекций. Чтение обязательной и дополнительной литературы, выполнение практического задания	Отчет в форме пояснительной записки. Исходный код программы	2	5
8.	УВ №23, Практическое занятие 8, «Тема 4. Дискреционная модель доступа» (модель Харрисона-Руззо-Ульмана)	Проработка лекций. Чтение обязательной и дополнительной литературы, выполнение практического задания	Отчет в форме пояснительной записки. Исходный код программы	2	5
9	УВ №26, Практическое занятие 9, «Тема 5. Дискреционная модель доступа» (модель Take-Grant)	Проработка лекций. Чтение обязательной и дополнительной литературы, выполнение практического задания	Отчет в форме пояснительной записки. Исходный код программы	2	5
10.	УВ №29, Практическое занятие 10, «Тема	Проработка лекций. Чтение обязательной и дополнительной литературы,	Отчет в форме пояснительно	2	5

	5. Дискреционная модель доступа» (модель Take-Grant)	выполнение практического задания	й записки. Исходный код программы		
11.	УВ №32, Практическое занятие 11, «Тема 6. Мандатная модель доступа» (модель Белла-Лападулы)	Проработка лекций. Чтение обязательной и дополнительной литературы, выполнение практического задания	Отчет в форме пояснительной записки. Исходный код программы	2	5
12.	УВ №35, Практическое занятие 12, «Тема 6. Мандатная модель доступа» (модель Белла-Лападулы)	Проработка лекций. Чтение обязательной и дополнительной литературы, выполнение практического задания	Отчет в форме пояснительной записки. Исходный код программы	2	5
13.	УВ №38, Практическое занятие 13, «Тема 7. Ролевая модель доступа» (модель RBAC)	Проработка лекций. Чтение обязательной и дополнительной литературы, выполнение практического задания	Отчет в форме пояснительной записки. Исходный код программы	2	5
14.	УВ №41, Практическое занятие 14, «Тема 7. Ролевая модель доступа» (модель RBAC)	Проработка лекций. Чтение обязательной и дополнительной литературы, выполнение практического задания	Отчет в форме пояснительной записки. Исходный код программы	2	5
15.	УВ №44, Практическое занятие 15, «Тема 8. Атрибутивная модель доступа» (модель ABAC)	Проработка лекций. Чтение обязательной и дополнительной литературы, выполнение практического задания	Отчет в форме пояснительной записки. Исходный код программы	2	5
16.	УВ №47, Практическое занятие 16, «Тема 9. Модели безопасности информационных потоков и изолированной программной среды»	Проработка лекций. Чтение обязательной и дополнительной литературы, выполнение практического задания	Отчет в форме пояснительной записки. Исходный код программы	2	5
	ИТОГО: часов самостоятельной				80

	работы				

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 виде.

ПРИМЕРНЫЙ ШАБЛОН оформления пояснительной записки к практическому заданию
ФИО обучающегося, Название и номер группы

Практическое задание № *N*
Тема «Название темы»

1. Постановка задачи

Формулировка задачи в общей постановке (например, реализовать разграничение прав доступа на основе дискреционной модели), номер варианта задания и свои исходные данные. Можно привести список выполняемых заданий.

2. Метод решения (название метода)

Описание метода: краткие теоретические сведения, основные расчетные формулы и блок-схемы.

3. Анализ результатов

Привести скриншоты основных этапов алгоритма и полученных результатов.

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

Отчет в форме пояснительной записки должен содержать подробное выполнение решения поставленной задачи.

1.2. Сроки выполнения, требования к объему.

Задания для самостоятельной работы выполняются в течение семестра, в котором читается данная дисциплина. Объем пояснительной записки для практических заданий 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 методах решения поставленной задачи, о способах построения и реализации алгоритма, уверенно отвечает на вопросы о проделанной работе. Предоставлен код работающей программы.

— 1 балл. Задание в основном соответствует требованиям. Студент продемонстрировал самостоятельную реализацию поставленной задачи, частично ответил на вопросы о проделанной работе. 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.

2. Рекомендации по самоподготовке к промежуточной аттестации по дисциплине

4.1. Вопросы к зачету для самопроверки:

1. Определение информационной и компьютерной безопасности.

2. Классификация угроз информационной безопасности.

3. Определение и структура политики безопасности информационной системы.

4. Закрытые, открытые, гибридные политики информационной безопасности.

5. Аналитический метод описания политик безопасности.

6. Графовый метод описания политик безопасности.

7. Объектный метод описания политик безопасности.

8. Логический метод описания политик безопасности

9. Пример графового метода описания ПБ: визуальный язык объектных ограничений «Language on Objects for Security Constraints» (LaSCO).

10. Определение графа атак. Формальное описание построения модели графа атак.

11. Анализ графа атак. Модель злоумышленника.

12. Определение гарантированной (верифицируемой) защиты.

13. Методы обеспечения гарантированности защиты.

14. Каналы несанкционированного доступа, утечки информации и деструктивных воздействий на информационную среду (НСДУВ).

15. Вероятностная оценка реализации канала НСДУВ.

16. Формальное описание обобщённой модели системы защиты информационной системы.

17. Формальное описание вероятностной модели систем защиты информационной системы.

18. Формальное описание модели безопасности информационной системы, построенной с использованием теории графов.

19. Формальное описание модели безопасности информационной системы, построенной с использованием теории автоматов.

20. Основные понятия защиты информации (субъекты, объекты, информационные потоки).

21. Модель системы безопасности HRU. Основные положения модели.

22. Теорема об алгоритмической неразрешимости проблемы безопасности в произвольной системе HRU.

23. Модель типизированной матрицы доступов. Основные положения модели.

24. Теорема о существовании алгоритма проверки безопасности ациклических систем монотонных ТМД.

25. Модель распространения прав доступа Take-Grant. Теоремы о передаче прав в графе доступов, состоящем из субъектов, и произвольном графе доступов.

26. Расширенная модель Take-Grant и ее применение для анализа информационных потоков в автоматизированной системе (АС).

27. Модель Белла-Лападулы как основа построения систем мандатного разграничения доступа. Основные положения модели.

28. Базовая теорема безопасности (BST). Политика low-watermark в модели Белла-Лападулы.

29. Применения модели Биба для реализации мандатной политики целостности.

30. Применение модели систем военных сообщений для систем приема, передачи и обработки почтовых сообщений, реализующих мандатную политику безопасности.

31. Шесть теоретических принципов политики контроля целостности. Соответствие правил модели Кларка-Вилсона принципам политики целостности.

32. Понятие ролевого управления доступом. Базовая модель ролевого управления доступом.

33. Понятие администрирования ролевого управления доступом. Администрирование иерархии ролей.

34. Понятие мандатного ролевого управления доступом. Требования либерального мандатного управления доступом.

35. Автоматная модель безопасности информационных потоков.

36. Вероятностная модель безопасности информационных потоков.

37. Информационное невлияние. Информационное невлияние с учетом фактора времени.

38. Монитор безопасности объектов. Монитор безопасности субъектов.

39. Теоремы о достаточных условиях гарантированного выполнения политики безопасности в компьютерных системах.

40. Базовая теорема изолированной программной среды.

4.2. Система оценивания

По окончании курса по данной дисциплине учебным планом предусмотрен **дифференцированный зачет**. 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 зачет.

Критерии оценки для дифференцированного зачета:

Ниже 61 балла – «неудовлетворительно»,

61-75 баллов – «удовлетворительно»,

76-90 баллов – «хорошо»,

91-100 баллов – «отлично».

Дифференцированный зачет проводится в устно-письменной форме по билетам.

Каждый 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, код программы) загружаются в соответствующие разделы дисциплины «Модели безопасности компьютерных систем» на образовательной платформе LMS ТюмГУ.