Приложение 1

Министерство науки и высшего образования Российской Федерации
НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ
ТОМСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ (НИ ТГУ)

Институт прикладной математики и компьютерных наук

УТВЕРЖДАЮ:
Директор института прикладной
математики и компьютерных наук
_____ А. В. Замятин
«19» мая 2022 г.

Оценочные материалы текущего контроля и промежуточной аттестации по дисциплине
(Оценочные средства по дисциплине)

Математические модели и методы решения задач информационной безопасности-1*BDD-representations of Boolean functions

по направлению подготовки

01.04.02 Прикладная математика и информатика

Направленность (профиль) подготовки:
Информационная безопасность

Томск – 2022

ОМ составил(и):
канд. техн. наук, доцент,
зав. кафедры компьютерной безопасности С.А. Останин

Рецензент:
канд. техн, доцент,
доцент кафедры компьютерной безопасности В.В. Андреева

Оценочные средства одобрены на заседании учебно-методической комиссии института прикладной математики и компьютерных наук (УМК ИПМКН)

Протокол от 12 мая 2022 г. № 4

Председатель УМК ИПМКН,
д-р техн. наук, профессор С.П. Сущенко

Оценочные средства (ОС) являются элементом оценивания сформированности компетенций у обучающихся в целом или на определенном этапе ее формирования.

ОС разрабатываются в соответствии с рабочей программой (РП).

1. Компетенции и результаты обучения, формируемые в результате освоения дисциплины

Компетенция	**Индикатор компетенции**	**Код и наименование результатов обучения** (планируемые результаты обучения, характеризующие этапы формирования компетенций)	**Критерии оценивания результатов обучения**			
			Отлично	Хорошо	Удовлетворительно	Неудовлетворительно
ОПК-4 – Способен комбинировать и адаптировать существующие информационно-коммуникационные технологии для решения задач в области профессиональной деятельности с учетом требований информационной безопасности.	ИОПК-4.1 Анализирует задачи прикладной математики и информатики средствами информационных технологий. ИОПК-4.2 Учитывает основные требования информационной безопасности.	ОР-4.1.1. Обучающийся сможет: - выполнять анализ задач с помощью аппарата, использующего представления булевых функций в виде графов. - искать решения практических задач с использованием специализированного программного обеспечения. ОР-4.1.2 Обучающийся сможет: - комбинировать и адаптировать существующие технологии для решения задач с учетом информационной безопасности. - при решении практических задач учитывать основные требования информационной безопасности.	Обучающийся полностью владеет материалом. Умеет объяснить изученные алгоритмы и применить их на практике. Способен программно реализовать изученные алгоритмы, а также искать решения применяя специализированное программное обеспечение. Комбинировать и адаптировать существующие	В целом успешные, но содержащие отдельные пробелы в знании материала и применении алгоритмов на практике. Способен искать решения применяя специализированное программное обеспечение. Адаптировать существующие технологии для решения задач с учетом информационной безопасности.	Фрагментарно, неполное без грубых ошибок знание материала. умение применять алгоритмы на практике. Не способен использовать существующие технологии для решения задач с учетом информационной безопасности.	Не имеет четкого представления об изучаемом материале, допускает грубые ошибки при выборе алгоритмов. Не способен искать решения применяя специализированное программное обеспечение. Не способен использовать существующие технологии для решения задач с учетом информационной безопасности.

			технологии для решения задач с учетом информационной безопасности.			
ПК-2 – Способен оценить уровень безопасности компьютерных систем и разработать программно-аппаратные средства защиты информации.	ИПК-2.1 Осуществляет проведение контрольных проверок работоспособности и эффективности применяемых программно-аппаратных средств защиты информации, разработку требований к программно-аппаратным средствам защиты информации компьютерных систем. ИПК-2.2 Осуществляет разработку требований по защите, формирование политик безопасности компьютерных систем и сетей, проектирование программно-аппаратных средств защиты информации компьютерных систем. ИПК-2.3 Осуществляет проведение анализа безопасности компьютерных систем, проведение сертификации программно-аппаратных средств защиты информации и анализ результатов, разработку и тестирование средств защиты информации компьютерных систем.	ОР-2.1.1 Владеть: навыками проведения контрольных проверок работоспособности и эффективности примитивов разработки систем контроля доступа и механизмов их реализации для разработки безопасных компьютерных систем; ОР-2.1.2 Уметь: разрабатывать требования к безопасному функционированию телекоммуникационных систем и оценивать их работоспособность и эффективность; ОР-2.1.3 Уметь: разрабатывать требования к программно-аппаратным реализациям криптографических алгоритмов и оценивать их работоспособность и эффективность в рамках поставленной задачи.	Демонстрация высокого уровня знаний; способность учитывать основные требования информационной безопасности при решении задач в области профессиональной деятельности.	В целом успешные, но содержащие отдельные пробелы знания в процессе анализа основных требований информационной безопасности при решении задач в области профессиональной деятельности.	Фрагментарное, неполное знание без грубых ошибок при анализе основных требований информационной безопасности при решении задач в области профессиональной деятельности.	Не имеет четкого представления об изучаемом материале, допускает грубые ошибки при анализе основных требований информационной безопасности при решении задач в области профессиональной деятельности.

2. Этапы формирования компетенций и виды оценочных средств

№	Этапы формирования компетенций (разделы дисциплины)	Код и наименование результатов обучения	Вид оценочного средства (тесты, задания, кейсы, вопросы и др.)
1.	Тема 1. Различные способы представления булевых функций.	ОР-4.1.1, ОР-4.1.2, ОР-2.1.1, ОР-2.1.3, ОР-2.1.3	Лабораторные работы, контрольные работы, зачет с оценкой
2.	Тема 2. Реализация основных операций над ROBDD-графами.	ОР-4.1.1, ОР-4.1.2, ОР-2.1.1, ОР-2.1.3, ОР-2.1.3	Лабораторные работы, контрольные работы, зачет с оценкой
3.	Тема 3. Примеры использования ROBDD-графов.	ОР-4.1.1, ОР-4.1.2, ОР-2.1.1, ОР-2.1.3, ОР-2.1.3	Лабораторные работы, контрольные работы, зачет с оценкой
4.	Тема 4. Представление систем булевых функций.	ОР-4.1.1, ОР-4.1.2, ОР-2.1.1, ОР-2.1.3, ОР-2.1.3	Лабораторные работы, контрольные работы, зачет с оценкой
5.	Тема 5. Новые типы декомпозиций и соответствующие типы диаграмм – PPRDDD (FDD), NPRMDD.	ОР-4.1.1, ОР-4.1.2, ОР-2.1.1, ОР-2.1.3, ОР-2.1.3	Лабораторные работы, контрольные работы, зачет с оценкой
6.	Тема 6. BDD с помеченными ребрами.	ОР-4.1.1, ОР-4.1.2, ОР-2.1.1, ОР-2.1.3, ОР-2.1.3	Лабораторные работы, контрольные работы, зачет с оценкой
7.	Тема 7. Zero suppressed Decision Diagram (ZDD).	ОР-4.1.1, ОР-4.1.2, ОР-2.1.1, ОР-2.1.3, ОР-2.1.3	Лабораторные работы, контрольные работы, зачет с оценкой
8.	Тема 8. Троичные решающие диаграммы (Ternary Decision Diagram - TDD).	ОР-4.1.1, ОР-4.1.2, ОР-2.1.1, ОР-2.1.3, ОР-2.1.3	Лабораторные работы, контрольные работы, зачет с оценкой

3. Типовые контрольные задания или иные материалы, необходимые для оценки образовательных результатов обучения

3.1. Типовые задания для проведения текущего контроля успеваемости по дисциплине.

Задание на лабораторную работу:

Реализовать ROBDD:

1. Внутреннее представление (например, в виде таблицы).
2. Основные операции (MakeNode, Build, Apply и др.).
3. Входные данные: из файла в формате PLA, с формы в виде формулы над множеством элементарных булевых функций (например, &, | и !). Для задания приоритета операций в формуле используем скобки.
4. Выходные данные: сохраните в текстовом файле таблицу с внутренним представлением диаграммы (формат разработайте сами), графическое отображение диаграммы произвольным способом (например, с помощью приложения Graphviz (https://ru.wikipedia.org/wiki/Graphviz), GLEE Microsoft Automatic Graph Layout или что-то еще на Ваше усмотрение).
5. Продемонстрировать использование диаграммы при решении практической задачи (не обязательно, но приветствуется!).

Контрольная работа:

1) Для булевых функций построить диаграммы заданного типа:

A) SBDD(f_1, f_2).
B) MTBDD(f_1, f_2).
C) FDD(f_1).
D) NPRMDD(f_1).
E) BDD с инверсными ребрами (f_1).
F) Kleene_TDD(f_1).
G) ZDD(f_1).

2) Проверьте корректность, построенной диаграммы.

Варианты:

1. $f_1 = xy \oplus z$; $f_2 = (x \vee y) \to z$.
2. $f_1 = xy \square z$; $f_2 = (x \vee y) \square z$.

3.2. Типовые задания для проведения промежуточной аттестации по дисциплине.

Вопросы к экзамену:

1. Способы представления булевых функций (БФ). Задача выполнимости и задача определения тавтологии БФ.
2. Условный оператор (if-then-else). Представление БФ в виде INF.
3. Определить BDT (binary decision tree) и BDD (binary decision diagram) используя INF представление булевой функции.
4. Дать определение ROBDD, сформулировать правила сокращения и свойства.
5. Доказать лемму о каноническом представлении БФ в виде ROBDD.
6. Каким образом порядок разложения по переменным влияет на ROBDD. Продемонстрировать на примере.
7. Способы хранения ROBDD в памяти. Функции: MK[T,h}(I,l,h) и Build[T,H](t).
8. Способы хранения ROBDD в памяти. Функции: Apply[T,H](op,u1,u2) и Restrict[T,H](u,j,b).
9. Функции: SatCount[T](u), AnySat(u), AllSat(u).
10. Функции: Simplify(d,u). Оценки времени работы основных алгоритмов оперирующих ROBDD.
11. Примеры практических задач решаемых с помощью ROBDD.
12. Представления систем БФ в виде BDD (SBDD, MTBDD).
13. Представление конечных автоматов в виде BDD, характеристические функции и отношения.
14. Троичные диаграммы (Ternary DD) общий случай и вариации.
15. BDD с помеченными ребрами (Attributed Edges BDD). Общий случай (произвольное отображение) и частный случай (с инверсными ребрами). Основные свойства, пример построения.
16. Декомпозиция Шеннона, Давио (позитивная и негативная) их представления в виде INF. Примеры построения деревьев разложения БФ для заданных декомпозиций.
17. Функциональные диаграммы (FDD~PPRMDD) и NPRMDT. Пример построения и правила сокращения.
18. Кронекеровские и псевдо-кронекеровские диаграммы. Примеры построения.

4. Методические материалы, определяющие процедуры оценивания образовательных результатов обучения

4.1. Методические материалы для оценки текущего контроля успеваемости по дисциплине.

В течение семестра необходимо выполнение всех обязательных практических заданий, лабораторных и контрольных работ.

4.2. Методические материалы для проведения промежуточной аттестации по дисциплине.

Промежуточная аттестация по дисциплине проводится в форме зачета с оценкой по теоретическому материалу.