

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

« 13 » мая 20 22 г.

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

Формальная верификация программ

по направлению подготовки

01.04.02 Прикладная математика и информатика

Направленность (профиль) подготовки:

Информационная безопасность

ОМ составил(и):
канд. техн. наук, доцент



Н.В. Шабалдина

Рецензент:
зав. кафедрой компьютерной безопасности,
канд. техн. наук, доцент



С.А. Останин

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	
			Зачтено	Не зачтено
ПК-1. Способен формализовать требования к программному обеспечению, спроектировать программное обеспечение, написать программный код, а также проверить работоспособность программного обеспечения и исправить дефекты.	ИПК-1.1 Осуществляет анализ требований к программному обеспечению, построение формальной модели, проверку работоспособности программного обеспечения и исправление дефектов; ИПК-1.2 Осуществляет разработку технических спецификаций на программные компоненты и их взаимодействие, разработку процедур проверки работоспособности и измерения характеристик программного обеспечения, разработку тестовых наборов данных; ИПК-1.3 Осуществляет проектирование	ПР-1.1 Понимает важность формальной верификации программ ПР-1.2 Умеет применять формальные модели для описания поведения дискретных систем и взаимодействующих процессов (компонент), подбирать подходящую модель в зависимости от особенностей дискретной системы. ПР-1.3 Умеет выбирать подходящую модель неисправности для тестирования дискретной системы	Сформированные системные знания; успешно применяемые навыки и умения	Отсутствие либо фрагментарность знаний/навыков

	<p>программного обеспечения, работу с системой контроля версий, рефакторинг и оптимизацию программного кода.</p>	<p>ПР-1.4</p> <p>Умеет применять инструмент fsmtestonline для построения полных проверяющих тестов</p> <p>ПР-1.5</p> <p>Умеет применять инструмент SPIN в режиме симуляции и верификации</p> <p>ПР-1.6</p> <p>Умеет проверять свойства распределенных систем, в том числе, свойство безопасности</p>		
<p>ПК-2. Способен оценить уровень безопасности компьютерных систем и разработать программно-аппаратные средства защиты информации.</p>	<p>ИПК-2.2 Осуществляет разработку требований по защите, формирование политик безопасности компьютерных систем и сетей, проектирование программно-аппаратных средств защиты информации компьютерных систем.</p>	<p>ПР-2.1</p> <p>Знает о различных критериях безопасного взаимодействия процессов/программ</p> <p>ПР-2.2</p> <p>Умеет описывать модели распределенных систем на языке Promela</p> <p>ПР-2.3</p> <p>Умеет задавать верифицируемые свойства на языке Promela</p>	<p>Сформированные системные знания; успешно применяемые навыки и умения</p>	<p>Отсутствие либо фрагментарность знаний/навыков</p>

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.	Введение в формальные методы верификации	ПР-1.1	Устные опросы Устный зачет
2.	Верификация на основе конечно-автоматной модели	ПР-1.2, ПР-1.3, ПР-1.4	Лабораторные задания Устные опросы Устный зачет
3.	Верификация моделей программ (model checking)	ПР-1.6, ПР-2.1, ПР-2.2, ПР-2.3	Устные опросы Устный зачет
4.	Язык Promela и верификатор Spin	ПР-1.5, ПР-1.6, ПР-2.1, ПР-2.2, ПР-2.3	Лабораторные задания Устные опросы Устный зачет

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

3.1. Типовые задания для проведения текущего контроля успеваемости по дисциплине

Контрольные вопросы по дисциплине для устных опросов

1. Для чего нужны формальные модели в тестировании?
2. Всегда ли разрешима установочная задача? А диагностическая задача?
3. Что такое исключительный класс автоматов? (в контексте разрешимости задачи идентификации).
4. Приведите пример возникновения частичности и недетерминизма в описании поведения дискретной системы при помощи конечного автомата.
5. Всегда ли установочная последовательность будет являться диагностической? А диагностическая – установочной?
6. Приведите пример использования процесса never.
7. Для решения каких практических задач можно использовать верификатор SPIN в режиме симуляции?
8. Приведите пример задания какого-либо требования в логике LTL.
9. В каких случаях может пригодиться метка заключительного состояния end?
10. В чем особенность выбора по условию в языке Promela?

Задания для лабораторных работ

Лабораторная работа 1. Распознавание неисправности из заданного класса. **Задание:** Дан эталонный автомат. Также предъявлен для экспериментов «черный ящик» – про него известно, что это неисправная реализация эталонного автомата и явно задан тип ошибки. Путем эксперимента требуется определить таблицу переходов-выходов предъявленного автомата.

Лабораторная работа 2. Тестирование протокольных реализаций (с применением инструмента fsmtestonline). **Задание:** по спецификации выбранного протокола построить формальную модель (конечный автомат). Построить тест на основе формальной модели при помощи инструмента fsmtestonline.ru. Подать тест на реализацию протокола. Написать краткий отчет, содержащий модель, тест, описание процесса тестирования, выводы.

Лабораторная работа 4. Работа с верификатором SPIN в режиме верификации (проверка заданного свойства) и в режиме симуляции (взаимодействие процессов; протокол выбора лидера в однонаправленном кольце; решение задачи о волке, козе и капусте; криптографический протокол Нидхама-Шредера (поиск атаки)).

3.2. Типовые задания для проведения промежуточной аттестации по дисциплине

Вопросы с устному зачету

1. Что такое верификация.
2. Этапы формальной верификации.
3. Разновидности методов формальной верификации.
4. Проверка эквивалентности.
5. Диагностические и установочные эксперименты с детерминированными конечными автоматами.
6. Отношения соответствие для недетерминированных конечных автоматов.
7. Структура Крипке.
8. Отличие темпоральной логики линейного времени (LTL) от классической математической логики.
9. Верификатор SPIN: основные возможности.
10. Язык Promela. Типы данных.
11. Запись LTL-формул в языке Promela.
12. Язык Promela. Процессы.
13. Язык Promela. Условия, циклы.
14. Язык Promela. Каналы. Взаимодействие рандеву.
15. Семантика выполнимости в Promela.
16. Классы свойств распределенных систем.
17. Язык Promela. Оператор assert.
18. Язык Promela. Блок atomic.
19. Язык Promela. Особый процесс never.
20. Метки состояний (активного, заключительного, принимающего).

4. Методические материалы, определяющие процедуры оценивания образовательных результатов обучения

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

Для допуска к устному зачету необходимо выполнение всех лабораторных работ.

4.2. Методические материалы для проведения промежуточной аттестации по дисциплине.

Промежуточная аттестация по дисциплине проводится в форме устного зачета по теоретическому материалу. К зачету допускаются только студенты, успешно прошедшие текущие аттестации.

Каждый билет для устного зачета состоит из двух теоретических вопросов по двум темам дисциплины. В качестве дополнительных вопросов на устном зачете используются контрольные вопросы по дисциплине.