МИНОБРНАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ
НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ
ТОМСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

Институт прикладной математики и компьютерных наук

УТВЕРЖДАЮ
Директор института прикладной
математики и компьютерных наук
_____ А.В. Замятин
«_____» _____ 2021 г.

**Фонд оценочных средств по дисциплине**

Методы верификации

Специальность
**10.05.01 Компьютерная безопасность**
*код и наименование специальности*

**Анализ безопасности компьютерных систем**
*наименование специализации*

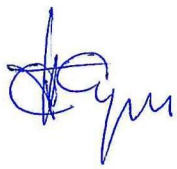
Томск–2021

ФОС составил(и):
канд. техн. наук, доцент
доцент каф. информационных технологий
в исследовании дискретных структур  Н.В. Шабалдина

Рецензент:
Заведующий кафедрой компьютерной безопасности,
канд. техн. наук, доцент  С.А. Останин

Фонд оценочных средств одобрен на заседании учебно-методической комиссии института прикладной математики и компьютерных наук (УМК ИПМКН)

Протокол от 17 июня 2021 г. № 05

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

**Фонд оценочных средств (ФОС)** является элементом системы оценивания сформированности компетенций у обучающихся в целом или на определенном этапе ее формирования.

ФОС разрабатывается в соответствии с рабочей программой (РП) дисциплины и включает в себя набор оценочных материалов для проведения текущего контроля успеваемости и промежуточной аттестации по дисциплине.

## 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-19. Способен оценивать корректность программных реализаций алгоритмов защиты информации | ИОПК-19.1 Обладает знанием формальных приемов, правил, алгоритмов, технологий создания и документирования контрольных примеров и тестовых наборов данных; ИОПК-19.2 Осуществляет подготовку тестовых наборов данных в соответствии с выбранной методикой, а также проверку работоспособности программного обеспечения на основе разработанных тестовых наборов данных; ИОПК-19.3 Осуществляет сбор и анализ полученных | **ОР-1** Понимает важность формальной верификации программ<br><br>**ОР-2** Умеет применять формальные модели для описания поведения дискретных систем и взаимодействующих процессов (компонент), подбирать подходящую модель в зависимости от особенностей дискретной системы.<br><br>**ОР-3** Умеет выбирать подходящую модель неисправности для тестирования дискретной системы<br><br>**ОР-4** Умеет применять инструмент fsmtestonline для | Сформированные системные знания; успешно применяемые навыки и умения | Сформированные, но содержащие отдельные пробелы знания; в целом успешно применяемые навыки и умения | Общие, но не структурированные знания; частично освоенные навыки и умения | Отсутствие либо фрагментарность знаний/навыков |

| | | | | | | |
|---|---|---|---|---|---|---|
| | результатов проверки работоспособности программного обеспечения, оценку соответствия программного обеспечения требуемым характеристикам. | построения полных проверяющих тестов<br><br>**ОР-5** Умеет применять инструмент SPIN в режиме симуляции и верификации<br><br>**ОР-6** Умеет проверять свойства распределенных систем, в том числе, свойство безопасности | | | | |
| ПК-3. Способен проектировать программно-аппаратные средств защиты информации компьютерных систем и сетей | ИПК-3.2 Разработка проектов программных и аппаратных средств защиты информации в соответствии с техническим заданием. | **ПР-1** Знает о различных критериях безопасного взаимодействия процессов/программ<br><br>**ПР-2** Умеет описывать модели распределенных систем на языке Promela<br><br>**ПР-3** Умеет задавать верифицируемые свойства на языке Promela | Сформированные системные знания; успешно применяемые навыки и умения | Сформированные, но содержащие отдельные пробелы знания; в целом успешно применяемые навыки и умения | Общие, но не структурированные знания; частично освоенные навыки и умения | Отсутствие либо фрагментарность знаний/навыков |

## 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 | ОР-1 | Лабораторные задания<br>Устные опросы<br>Устный экзамен |
| 2. | Верификация на основе конечно-автоматной модели | ОР-2, ОР-3, ОР-4 | Лабораторные задания<br>Устные опросы<br>Устный экзамен |
| 3. | Верификация моделей программ (model checking) | ОР-6, ПР-1, ПР-2, ПР-3 | Лабораторные задания<br>Устные опросы<br>Устный экзамен |
| 4. | Язык Promela и верификатор Spin | ОР-5, ОР-6, ПР-1, ПР-2, ПР-3 | Лабораторные задания<br>Устные опросы<br>Устный экзамен |

## 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 пригодится 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.** Построение множества достижимости и множества различимости для детерминированного конечного автомата. **Задание:** Для заданного детерминированного полностью определенного конечного автомата построить множество достижимости. Для заданного детерминированного полностью определенного приведенного конечного автомата построить множество различимости.

**Лабораторная работа 3.** 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 экзамену**

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 экзамену необходимо выполнение всех лабораторных работ, проверочной работы в электронном курсе и заданий в МООК.

4.2. Методические материалы для проведения промежуточной аттестации по дисциплине.

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

Каждый билет для устного экзамена состоит из двух теоретических вопросов по

двум темам дисциплины. В качестве дополнительных вопросов на устном экзамене используются контрольные вопросы по дисциплине.