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

Институт прикладной математики и компьютерных наук

УТВЕРЖДАЮ:
Директор
_____ А. В. Замятин
« 19 » мая 20 22 г.

Рабочая программа дисциплины

Методы верификации

по направлению подготовки / специальности

10.05.01 Компьютерная безопасность

Направленность (профиль) подготовки / специализация:
Анализ безопасности компьютерных систем

Форма обучения
Очная

Квалификация
Специалист по защите информации

Год приема
2022

Код дисциплины в учебном плане: Б1.В.04.06

СОГЛАСОВАНО:
Руководитель ОП
_____В.Н. Тренькаев

Председатель УМК
_____С.П. Сущенко

Томск – 2022

1. Цель и планируемые результаты освоения дисциплины

Целью освоения дисциплины является формирование следующих компетенций:

– ОПК-19 – Способен оценивать корректность программных реализаций алгоритмов защиты информации.

– ПК-3 – Способен проектировать программно-аппаратные средства защиты информации компьютерных систем и сетей.

Результатами освоения дисциплины являются следующие индикаторы достижения компетенций:

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 результатов проверки работоспособности программного обеспечения, оценку соответствия программного обеспечения требуемым характеристикам.

ИПК-3.2 Разработка проектов программных и аппаратных средств защиты информации в соответствии с техническим заданием.

2. Задачи освоения дисциплины

– Освоить математический аппарат методов верификации;

– Освоить работу с программным обеспечением, используемым для верификации (инструмент SPIN в режиме симуляции и верификации, инструмент fsmtestonline для построения полных проверяющих тестов);

– Научиться осуществлять верификацию программ, в том числе, анализировать корректность реализаций алгоритмов защиты информации.

3. Место дисциплины в структуре образовательной программы

Дисциплина относится к части образовательной программы, формируемой участниками образовательных отношений. Дисциплина входит в модуль «Специализация».

4. Семестр(ы) освоения и форма(ы) промежуточной аттестации по дисциплине

Девятый семестр, экзамен

5. Входные требования для освоения дисциплины

Для успешного освоения дисциплины требуются результаты обучения по следующим дисциплинам: Б1.О.02.02 «Математическая логика и теория алгоритмов», Б1.О.02.03 «Дискретная математика», Б1.О.02.10 «Теория автоматов», Б1.О.05.03 «Алгоритмы и структуры данных».

6. Язык реализации

Русский

7. Объем дисциплины

Общая трудоемкость дисциплины составляет 4 з.е., 144 часов, из которых:
-лекции: 32 ч.
-лабораторные: 32 ч.
Объем самостоятельной работы студента определен учебным планом.

8. Содержание дисциплины, структурированное по темам

Тема 1. Введение в формальные методы верификации
Вводная лекция. Основные понятия, определения, цель, задачи, структура курса.

Тема 2. Верификация на основе конечно-автоматной модели
Эксперименты с конечными детерминированными автоматами. Распознавание неисправности из заданного класса. Построение множества достижимости и множества различимости для детерминированного конечного автомата. Недетерминированные конечные автоматы и отношения между ними. Расширенные и временные автоматы. Тестирование протокольных реализаций (с применением инструмента fsmtestonline)

Тема 3. Верификация моделей программ (model checking)
Структура Крипке. Автомат Бюхи. Темпоральная (временная) логика линейного времени (LTL). Темпоральная (временная) логика ветвящегося времени (CTL). Применение темпоральных логик для задания свойств системы.

Тема 4. Язык Promela и верификатор Spin.
Синтаксис языка Promela. Работа с верификатором SPIN в режиме верификации (проверка заданного свойства) и в режиме симуляции.

9. Текущий контроль по дисциплине

Текущий контроль по дисциплине проводится путем устных опросов и проверки лабораторных работ и фиксируется в форме контрольной точки не менее одного раза в семестр.

10. Порядок проведения и критерии оценивания промежуточной аттестации

Экзамен проводится в девятом семестре. Допуском к экзамену служит выполнение всех лабораторных работ. Экзаменационный билет состоит из двух вопросов. Время подготовки к ответу на вопросы в билете составляет 40 минут.

Важность выполнения лабораторных работ в семестре и допуск к экзамену на основе того факта, что лабораторные работы выполнены, обусловлена тем, что именно при сдаче лабораторных работ проверяется освоение компетенций ИОПК-19.2, ИОПК-19.3, ИПК-3.2. Также при выполнении лабораторных работ студенты применяют знания, приобретенные во время лекций и самостоятельной работы и предусмотренные практике компетенцией ИОПК-19.1. В ходе самого устного экзамена более глубоко и тщательно проверяется компетенция ИОПК-19.1.

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)).

Вопросы к 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).

Результаты экзамена определяются оценками «отлично», «хорошо», «удовлетворительно», «неудовлетворительно».

Оценки «неудовлетворительно» выставляется в случае, если студент не получил допуск к экзамену, т.е. не сдал в течение семестра лабораторные работы. Оценка «удовлетворительно» может быть выставлена автоматически без сдачи экзамена по билетам в случае, если студент сдал лабораторные работы в срок. Оценка «хорошо» выставляется в случае, если студент допущен к экзамену и предоставил развернутый аргументированный ответ на один из двух вопросов в билете. Оценка «отлично» проставляется в случае, если студент допущен к экзамену и предоставил развернутый аргументированный ответ на оба вопроса в билете.

11. Учебно-методическое обеспечение

а) Электронный учебный курс по дисциплине в электронном университете «Moodle» - https://moodle.tsu.ru/course/view.php?id=12367

12. Перечень учебной литературы и ресурсов сети Интернет

а) основная литература:

– Кудрявцев В. Б. Теория автоматов : Учебник для бакалавриата и магистратуры / Кудрявцев В. Б., Алешин С. В., Подколзин А. С.. - Москва : Юрайт, 2019. - 320 с.

– Старолетов С. М. Основы тестирования и верификации программного обеспечения / Старолетов С. М.. - Санкт-Петербург : Лань, 2020. - 344 с.. URL: https://e.lanbook.com/book/138181.

– Камкин А.С. Введение в формальные методы верификации программ: учебное пособие /. А. С. Камкин. – Москва: МАКС Пресс, 2018. – 272 с.

б) дополнительная литература:

– Шошмина И. В., Карпов Ю. Г. Введение в язык Promela и систему комплексной верификации Spin. Учебное пособие – СПб.: СПбГПУ, 2010. – 111 с.

– Евтушенко Н.В. Недетерминированные автоматы: анализ и синтез: учебное пособие, ч.1 / Н. В. Евтушенко, А.Ф. Петренко, М. В.Ветрова. Томск: Том. гос. ун-т, 2006. – 142 с.

– Евтушенко Н.В. Недетерминированные автоматы: анализ и синтез: учебное пособие, ч.3 / Н. В. Евтушенко, М. Л. Громов, Н. В. Шабалдина. Томск: Том. гос. ун-т, 2013. – 57 с.

– Гилл А. Введение в теорию конечных автоматов / А. Гилл; под ред. П.П. Пархоменко. М. : Наука, Физматлит, 1966, 272 с.

в) ресурсы сети Интернет:

– Электронная библиотека (репозиторий) ТГУ [Электронный ресурс] / Электронная библиотека (репозиторий) ТГУ. – URL: http://vital.lib.tsu.ru/vital/access/manager/Index.

– Шабалдина Н.В., Прокопенко С.А., Торгаев С.Н., Громов М.Л., Лапутенко А.В. Математика в тестировании дискретных систем [Электронный ресурс]. – URL: https://stepik.org/course/73866.

– Test Generation for Finite State Machine [Электронный ресурс]. – URL: http://www.fsmtestonline.ru/

– Карпов Ю.Г., Шошмина И.В. Математическая логика [Электронный ресурс].– URL: https://openedu.ru/course/spbstu/MATLOG/.

– Verifying Multi-threaded Software with SPIN. – URL: http://spinroot.com/

13. Перечень информационных технологий

а) лицензионное и свободно распространяемое программное обеспечение:

– Верификатор SPIN. – URL: http://spinroot.com/

– Инструмент для построения тестов Test Generation for Finite State Machine. – URL: http://www.fsmtestonline.ru/

б) информационные справочные системы:

– Электронный каталог Научной библиотеки ТГУ – http://chamo.lib.tsu.ru/search/query?locale=ru&theme=system

– Электронная библиотека (репозиторий) ТГУ – http://vital.lib.tsu.ru/vital/access/manager/Index

– ЭБС Лань – http://e.lanbook.com/

– Образовательная платформа Юрайт – https://urait.ru/

14. Материально-техническое обеспечение

Аудитории для проведения занятий лекционного типа.

Аудитории для проведения занятий индивидуальных и групповых консультаций, текущего контроля и промежуточной аттестации.

Аудитории для проведения лабораторных занятий, оснащенные компьютерной техникой и доступом к сети Интернет, с установленным на компьютеры верификатором SPIN.

Помещения для самостоятельной работы, оснащенные компьютерной техникой и доступом к сети Интернет, в электронную информационно-образовательную среду и к информационным справочным системам.

15. Информация о разработчиках

Шабалдина Наталия Владимировна, к.т.н., доцент