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
«_02_» _июля_ 2021 г.

Методы верификации

рабочая программа дисциплины

Закреплена за кафедрой	*компьютерной безопасности*
Учебный план	*10.05.01 Компьютерная безопасность,* *профиль «Анализ безопасности компьютерных систем»*
Форма обучения	*очная*
Общая трудоёмкость	*4 з.е.*
Часов по учебному плану	*144*
в том числе:	
аудиторная контактная работа	*71.5*
самостоятельная работа	*72.5*
Вид(ы) контроля в семестрах *экзамен/зачет/зачет с оценкой*	*Семестр 9 – экзамен*

Томск-2021

Программу составила:
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

Рабочая программа дисциплины «Методы верификации» разработана в соответствии с образовательным стандартом высшего образования – специалитет, самостоятельно устанавливаемым федеральным государственным автономным образовательным учреждением высшего образования «Национальный исследовательский Томский государственный университет» по специальности 10.05.01 Компьютерная безопасность (Утвержден Ученым советом НИ ТГУ, протокол от 30.06.2021 г. № 06).

Рабочая программа одобрена на заседании кафедры компьютерной безопасности

Протокол от 02 июня 2021 г. № 06

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

Рабочая программа одобрена 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

Цель освоения дисциплины

Цель – научить студентов осуществлять верификацию программ, в том числе, анализировать корректность реализаций алгоритмов защиты информации.

1. Место дисциплины в структуре ОПОП

Дисциплина «Методы верификации» относится к части, формируемой участниками образовательных отношений, Блока 1 «Дисциплины», входит в модуль «Специализация».

Для освоения дисциплины необходимо знать основы математической логики, теории алгоритмов, дискретной математики, в том числе, теории автоматов.

Пререквизиты дисциплины: 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».

Постреквизиты дисциплины: нет.

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

Таблица 1.

Компетенция	**Индикатор компетенции**	**Код и наименование результатов обучения** (планируемые результаты обучения по дисциплине, характеризующие этапы формирования компетенций)
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 результатов проверки работоспособности программного обеспечения, оценку соответствия программного обеспечения требуемым характеристикам.	**ОР-1** Понимает важность формальной верификации программ **ОР-2** Умеет применять формальные модели для описания поведения дискретных систем и взаимодействующих процессов (компонент), подбирать подходящую модель в зависимости от особенностей дискретной системы. **ОР-3** Умеет выбирать подходящую модель неисправности для тестирования дискретной системы **ОР-4** Умеет применять инструмент fsmtestonline для построения полных проверяющих тестов **ОР-5** Умеет применять инструмент SPIN в режиме симуляции и верификации **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 **ПР-2** Умеет описывать модели распределенных систем на языке Promela

		ПР-3 Умеет задавать верифицируемые свойства на языке Promela

3. Структура и содержание дисциплины

3.1. Структура и трудоемкость видов учебной работы по дисциплине

Общая трудоемкость дисциплины составляет 4 зачетные единицы, 144 часа.

Таблица 2.

Вид учебной работы	Трудоемкость в академических часах	
	9 семестр	всего
Общая трудоемкость	144	144
Контактная работа:	71,5	71,5
Лекции (Л):	32	32
Практики (ПЗ)		
Лабораторные работы (ЛР)	32	32
Семинары (СЗ)		
Групповые консультации	2	2
Индивидуальные консультации	3,2	3,2
Промежуточная аттестация	2,3	2,3
Самостоятельная работа обучающегося:	40,8	40,8
- подготовка к лабораторным занятиям	15,8	15,8
- изучение учебного материала	15	15
- другие формы самостоятельной работы	10	10
Подготовка к рубежному контролю по теме/разделу	31,7	31,7
Вид промежуточной аттестации (зачет, зачет с оценкой, экзамен)	**Экзамен**	**Экзамен**

3.2. Содержание и трудоемкость разделов дисциплины

Таблица 3.

Код занятия	Наименование разделов и тем и их содержание	Вид учебной работы, занятий, контроля	Семестр	Часы в электронной форме	Всего (час.)	Литература	Код (ы) результата(ов) обучения
	Раздел 1. Введение в формальные методы верификации		9		**4**	**2, 3, 4**	ОР-1
1.1.	Вводная лекция. Основные понятия, определения, цель, задачи, структура курса	Лекции	9		2		
1.2.	Изучение учебного материала	СРС	9		2		
	Раздел 2. Верификация на основе конечно-автоматной модели		9		**50**	**1, 3, 5-7**	ОР-2, ОР-3, ОР-4
2.1.	Эксперименты с конечными детерминированными автоматами	Лекции	9		8		
2.2.	Работа в МООК «Математика в тестировании дискретных систем», подготовка к лабораторным работам, изучение учебного материала	СРС	9		16		
2.3.	Распознавание неисправности из заданного класса	ЛР	9		2		
2.4.	Построение множества достижимости и множества различимости для детерминированного конечного автомата	ЛР	9		4		
2.5.	Недетерминированные конечные автоматы и отношения между ними. Расширенные и временные автоматы	Лекции	9		6		
2.6.	Тестирование протокольных реализаций (с применением инструмента fsmtestonline)	ЛР			10		
	Раздел 3. Верификация моделей программ (model checking)		9		**13**	**2-4**	ОР-6, ПР-1, ПР-2, ПР-3
3.1.	Структура Крипке. Автомат Бюхи	Лекции	9		2		
3.2.	Темпоральная (временная) логика линейного времени (LTL). Темпоральная (временная) логика ветвящегося времени (CTL)	Лекции	9		4		
3.3.	Применение темпоральных логик для задания свойств системы	Лекции	9		2		
3.4.	Изучение учебного материала	СРС	9		5		
	Раздел 4. Язык Promela и верификатор Spin		9		**34**	**2-4**	ОР-5, ОР-6, ПР-1, ПР-2, ПР-3
4.1.	Синтаксис языка Promela	Лекции	9		8		
4.2.	Работа с верификатором SPIN в режиме верификации (проверка заданного свойства) и в режиме симуляции	ЛР	9		16		
4.3.	Изучение учебного материала. Подготовка к лабораторным работам	СРС			10		
	Подготовка к промежуточной аттестации в форме экзамена	СРС	9		**31,7**	**1, 2, 3, 4, 5, 6, 7**	ОР-1, ОР-2, ОР-3, ОР-4, ОР-5, ОР-6,

							ПР-1, ПР-2, ПР-3
	Прохождение промежуточной аттестации в форме экзамена	Э	9		**4,3**		

4. Образовательные технологии, учебно-методическое и информационное обеспечение для освоения дисциплины

В основе подготовки по данному курсу лежит лекционный материал, который читается студентам на лекционных занятиях и представлен в LMS MOODLE. Лекционный материал подкреплён лабораторными занятиями.

Промежуточная аттестация проводится в форме экзамена при условии выполнения студентами лабораторных работ.

Самостоятельная работа студентов при изучении дисциплины (модуля) предусмотрена в следующих видах и формах:

- Работа с лекционным материалом, поиск и обзор литературы и электронных источников информации по индивидуально заданной проблеме курса;
- Работа в электронном курсе и в МООК (изучение теоретического материала, выполнение индивидуальных заданий и контролирующих мероприятий и др.);
- Изучение тем, вынесенных на самостоятельную проработку;
- Подготовка к лабораторным занятиям;
- Подготовка к оценивающим мероприятиям, в том числе, к промежуточной аттестации.

4.1. Рекомендуемая литература и учебно-методическое обеспечение

№ п/п	Авторы / составители	Заглавие	Издательство	Год издания, количество страниц
Основная литература				
1.	Кудрявцев В. Б., Алешин С. В., Подколзин А. С.	Теория автоматов : Учебник для бакалавриата и магистратуры	М. : Юрайт	2019 г., 320 с.
2.	Старолетов С. М.	Основы тестирования и верификации программного обеспечения	СПб. : Лань	2020 г., 320 с.
3.	Камкин А.С.	Введение в формальные методы верификации программ: учебное пособие	М. : МАКС Пресс	2018 г., 272 с.
Дополнительная литература				
4.	Шошмина И. В., Карпов Ю. Г.	Введение в язык Promela и систему комплексной верификации Spin. Учебное пособие	СПб.: СПбГПУ	2010 г., 111 с.
5.	Евтушенко Н. В., Петренко А.Ф., Ветрова М. В.	Недетерминированные автоматы: анализ и синтез: учебное пособие, ч.1	Томск: Том. гос. ун-т	2006 г., 142 с.
6.	Евтушенко Н. В., Громов М. Л., Шабалдина Н. В.	Недетерминированные автоматы: анализ и синтез: учебное пособие, ч.3	Томск: Том. гос. ун-т	2013 г., 57 с.
7.	Гилл А.	Введение в теорию конечных автоматов	М. : Наука	1966 г., 272 с.

4.2. Базы данных и информационно-справочные системы, в том числе зарубежные

1. Электронная библиотека (репозиторий) ТГУ [Электронный ресурс] / Электронная

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

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

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

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

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

4.3. Перечень лицензионного и программного обеспечения

1. Верификатор SPIN. – URL: http://spinroot.com/
2. Инструмент для построения тестов Test Generation for Finite State Machine. – URL: http://www.fsmtestonline.ru/

4.4. Оборудование и технические средства обучения

Для реализации дисциплины необходимы лекционные аудитории и аудитории для проведения лабораторных занятий. Специальные технические средства (проектор, компьютер и т.д.) требуются для демонстрации материала в рамках изучаемых разделов, проведения защиты проектов в конце семестра. Вся основная и дополнительная литература, необходимая для самостоятельной работы и подготовки к экзамену, имеется в научной библиотеке ТГУ.

5. Методические указания обучающимся по освоению дисциплины

Основой обучения является курс лекций, читаемый преподавателем. Практические навыки формируются лабораторными работами. Для самостоятельной работы и дополнительного расширения круга знаний желательно использовать литературу, приведенную в разделе 4.1, а также информационные системы, приведенные в разделе 4.2. Промежуточная аттестация осуществляется в виде устного зачёта при условии выполнения лабораторных работ.

6. Преподавательский состав, реализующий дисциплину

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

7. Язык преподавания – русский язык.