1. Цели освоения дисциплины

Цель курса – Целью освоения дисциплины является изучение основных принципов использования формальных методов для верификации и тестирования телекоммуникационных протоколов и сервисов, в том числе, изучение основных математических моделей и методов их анализа, для получения навыков анализа телекоммуникационных протоколов и сервисов и их реализаций с использованием формальных методов.

Задачами данного курса являются:

- освоение студентами базовых современных достижений в области использования формальных методов для тестирования и верификации телекоммуникационных протоколов и сервисов и их реализаций;
- формирование практических навыков тестирования и верификации телекоммуникационных протоколов и сервисов на основе формальных методов.

2. Место дисциплины в структуре образовательной программы

Данная дисциплина относится к вариативной части Цикла дисциплин программы (М2).

Изучение данной дисциплины базируется на знаниях, полученных студентами при освоении учебных дисциплин:

- «Дискретная математика»,
- «Программирование»,
- «Информатика, математическая логика и теория алгоритмов»,
- «Построение и анализ алгоритмов»,
- «Архитектура вычислительных систем»,
- «Формальные методы в программной инженерии»,
- «Верификация программного обеспечения».

1 Тематический план учебной дисциплины

№	Название раздела	Всего часов	Аудиторные часы		Самостоя-тельная работа
			Лекции	Практические занятия	
1.	Введение. Использование формальных методов при верификации и тестировании телекоммуникационных протоколов	41	1	0	40
2.	Использование автоматных моделей при тестировании телекоммуникационных протоколов; тестирование	59	6	11	42

	конформности; верификация многокомпонентных систем				
3.	Криптографические протоколы; безопасность протокольных реализаций	60	8	10	42
4.	Использование формальных моделей для анализа функциональных и нефункциональных свойств сетевых сервисов	54	6	6	42
5	Использование формальных моделей для анализа компонентов программно-конфигурируемых сетей	52	4	8	40
Итого:		**266**	**25**	**35**	**206**

2 Формы контроля знаний студентов

Тип контроля	Форма контроля	2 год		Параметры
		1 модуль	2 модуль	
Текущий	Домашнее задание		*	
				Сдача не позднее, чем за 15 дней до экзамена
Итоговый	Экзамен		*	Устный экзамен

3 Критерии оценки знаний, навыков

В рамках курса слушателям предлагается выполнить домашнее задание в виде реферата и сдать итоговый экзамен. Оценки за домашнее задание и экзамен выставляются по 10-ти балльной шкале.

4 Порядок формирования оценок по дисциплине

Оценка за первый семестр (итоговая оценка $О_{итог.1}$) складывается из накопленной оценки 1 семестра ($О_{накопл.1}$) и оценки за устный экзамен в конце 2-го модуля ($О_{экз.1}$):

$О_{накопл.1} = О_{дом.зад.}$;

$О_{итог.1} = 0.5 \cdot О_{накопл.1} + 0.5 \cdot О_{экз.1}$;

Оценка ($О_{итог.1)}$ является результирующей.

Способ округления оценок – арифметический.

5 Содержание дисциплины

Тема 1. Введение. Использование формальных методов при верификации и тестировании телекоммуникационных протоколов. Эволюция формальных методов и средств и оценки эффективности их использования. Обоснование необходимости использования формальных методов при верификации и тестировании сетевых сервисов.

Тема 2. Использование моделей с конечным числом переходов при тестировании телекоммуникационных протоколов, в частности, конечных автоматов и полуавтоматов, входо-выходных полуавтоматов (трансдьюсеров), расширенных и временных автоматов и полуавтоматов; использование автоматных моделей с бесконечным числом переходов при символьном тестировании (symbolic testing). Построение проверяющих тестов с гарантированной полнотой на основе классических и неклассических автоматных моделей для тестирования протокольных реализаций; полнота проверяющих тестов. Верификация многокомпонентных программных систем с использованием композиций автоматных моделей; использование верификаторов и решателей (SPIN, z3 и др.) при проверке свойств безопасности, в том числе, проверке наличия тупиков и зацикливаний.

Тема 3. Криптографические протоколы; безопасность протокольных реализаций как цепочки «стойкость алгоритма – верификация модели - обнаружение уязвимостей в реализации». Анализ безопасности протокола TLS, в том числе, анализ обнаруженных угроз и уязвимостей в протоколе и, соответственно, в его реализациях.

Тема 4. Использование формальных моделей для анализа функциональных и нефункциональных свойств сетевых сервисов; использование моделей с конечным числом переходов на различных этапах их жизненного цикла. Формальные методы при анализе качества сервиса с точки зрения конечного пользователя.

Тема 5. Использование формальных моделей для анализа компонентов программно-конфигурируемых сетей: формальные методы при анализе запросов, верификация композиций на наличие тупиков и зацикливаний, совместимость правил в коммутаторах, тестирование SDN контроллеров в контексте приложений и/или панели данных.

6 Оценочные средства для текущего контроля и аттестации студента

6.1 Тематика заданий текущего контроля

Домашнее задание. Изучение одного из протоколов по выбору преподавателя, его особенностей, подготовка презентации и реферата.

6.2 **Примеры контрольных вопросов для экзамена**

1. Какие модели с конечным числом переходов Вы знаете? Какова семантика входных и выходных символов при описании телекоммуникационного протокола автоматной моделью? Какими особенностями обладают входо-выходные полуавтоматы и тесты, построенные на их основе?
2. Что такое тестирование протокольной реализации на соответствие спецификации? На безопасность?
3. Какие Вам известны методы построения тестов по входо-выходным полуавтоматам?
4. Композиции автоматных моделей и тестирование на совместимость.
5. Тестирование протокольных реализаций: когда удобно использовать активное и/или пассивное тестирование?
6. Верификатор SPIN и его свойства.
7. Анализ безопасности криптографических протоколов.
8. Какие существуют этапы проектирования сетевых сервисов?
9. Использование формальных моделей, в том числе моделей с конечным числом состояний, для анализа компонентов программно-конфигурируемых сетей.

7 Учебно-методическое и информационное обеспечение дисциплины

7.1 **Основная литература**

1. C. Kaner, R. L. Fiedler. Foundations of Software Testing. Context-Driven Press, 2013.
2. Б. Шнайер Прикладная криптография. Протоколы, алгоритмы и исходные текста на языке С, ч. 1., 1995.
3. Крупский В. Н. Математическая логика и теория алгоритмов: [учебное пособие для бакалавров, обучающихся по направлениям подготовки "Информатика и вычислительная техника", "Информационные системы"] / В. Н. Крупский, В. Е. Плиско. - Москва : Академия, 2013. – 415 с.
4. А.С. Камкин. Верификация программного обеспечения. Изд-во МГУ, 2018, 272 с.
5. Олифер В. Г. Компьютерные сети. Принципы, технологии, протоколы: [учебное пособие для вузов по направлению 552800 "Информатика и вычислительная техника" и по специальностям 220100 "Вычислительные машины, комплексы, системы и сети", 220400 "Программное обеспечение вычислительной техники и автоматизированных систем"] / В. Г. Олифер, Н. А. Олифер. - 5-е изд. - Санкт-Петербург [и др.] : Питер, 2016. - 991 с.: ил., табл.- (Учебник для вузов) - (Стандарт третьего поколения).
6. Р. Смелянский. Программно-реконфигурируемые сети. Открытые системы, № 9, 2012.

7.2 **Дополнительная литература**

1. Ю.Г. Карпов. Верификация параллельных и распределенных программных систем. Санкт-Петербург, БХВ-Петербург, 2010.
2. Д. Месарош. Шаблоны тестирования xUnit. М.: Вильямс, 2008.
3. A. P. Mathur. Foundations of Software Testing. Copymat Services, 2006.
4. Евтушенко Н.В. Недетерминированные автоматы: анализ и синтез: учебное пособие, ч.1, 3 / Н. В. Евтушенко, и др. - Томск: Том. гос. ун-т, 2006 - 2013.

5. Gerald J. Holzman The Spin Model Checker: Primer and Reference Manual – Addison-Wesley, 2004.
6. Omer Nguena Timo1, Alexandre Petrenko1, and S. Ramesh. Multiple Mutation Testing from Finite State Machines with Symbolic Inputs. In Proc. of ICTSS'2017.
7. Petrenko, A., Boroday S., Groz, R.: Confirming Configurations in EFSM Testing. IEEE Trans. Software Eng., 2004, 30(1), pp. 29-42.
8. El-Fakih, K., Salameh, T., Yevtushenko, N. On Code Coverage of Extended FSM Based Test Suites: An Initial Assessment. LNCS, 2014, 8763, pp. 198-204.
9. Proccedings of Intern Conf. on Software Testing, ICST, 2008 - 2015, and Testing Systems and Software, ICTSS, 1991 – 2018 (ранее: on Protocol Testing).
7. J. Tretmans Model based testing with labeled transition systems // Formal Methods and Testing. — 2008, pp. 1–38.
8. Dimitris E. Simos, Josip Bozic, Feng Duan, Bernhard Garn, Kristo ffer Klei
Franz Wotawa. Testing TLS Using Combinatorial Methods and Execution Framework. In Proc. of ICTSS'2017.
9. Kondratyeva O., Kushik N., Cavalli A., Yevtushenko N. Using Finite State Models for Quality Evaluation at Web Service Development Steps. International Journal on Service Computing (IJSC), ISSN 2330-4472, 1(2), pp. 1-12.
10. Jay Beale, Renaud Deraison, Haroon Meer, Roelof Temmingh, and Charl Van Der Walt. 2004. Nessus Network Auditing. Syngress Publishing.
11. Stallings, William. Cryptography and Network Security, 4/E. Pearson Education India, 2006.
12. Proceedings of International Conferences and Workshops of the IEEE World Congress on Services, 2012 – 2018.
13. Р. Смелянский. Программно-конфигурируемые сети. Открытые системы, № 9, 2012.
14. Opennetworking. Software-defined networking: The new norm for networks. ONF White Paper, 2012.
15. В. А. Захаров, Р. Л. Смелянский, Е. В. Чемерицкий. Формальная модель и задачи верификации программно-конфигурируемых сетей. *Модел. и анализ информ. систем*, **20**:6 (2013), 36–51.
16. Canini, M., Kostic, D., Rexford, J.,and Venzano, D. Automating the testing of openflow applications. In Proceedings of the 1st International Workshop on Rigorous Protocol Engineering (WRiPE), 2011.
17. Canini, M., Venzano, D., Peresini, P., Kostic, D., Rexford, J., et al. (2012). A nice way to test openflow applications. In NSDI'2012, volume 12, pages 127–140.
18. David, L., Stefano, V., and Olivier, B. (2014). Towards test-driven software defined networking. In 2014 IEEE Network Operations and Management Symposium, pages 1–9.
19. Fayaz, S. K., Yu, T., Tobioka, Y., Chaki, S., and Sekar, V. (2016). BUZZ: testing context-dependent policies in stateful networks. In 13th USENIX Symposium on Networked Systems Design and Implementation, pages 275–289.

7.3 **Ресурсы информационно-телекоммуникационной сети Интернет**

1. А.К.Петренко, А.В.Хорошилов, Е.В.Корныхин. Лекция 8. Тестирование на основе формальных моделей, 2012. – URL: http://sp.cmc.msu.ru/courses/fmsp/2012/slides/lecture8.pdf (дата обращения: 03.10.2016).
2. Верификация программного обеспечения : курс лекций: [Электронный ресурс] / С.В. Синицын, Н.Ю. Налютин. – Московский инженерно-физический институт

(государственный университет). – ФГАУ ГНИИ ИТТ «Информика» . – М., 2005 – 2016. – URL: http://window.edu.ru/window/library/pdf2txt?p_id=18858&p_page=1.
3. SPIN [Электронный ресурс] https://spinroot.com
4. TLS1.2 [Электронный ресурс] https://tools.ietf.org/html/rfc5246
5. TLS1.3 [Электронный ресурс] https://tools.ietf.org/html/rfc8446
6. Р. Смелянский. Программно-конфигурируемые сети [Электронный ресурс] http://www.webcitation.org/6DyOwYRyU