**Программа учебной дисциплины «**Формальные методы верификации и тестирования телекоммуникационных протоколов и сервисов**»**

Утверждена

Академическим советом ООП

Протокол № от «\_\_»\_\_\_\_\_20\_\_ г.

|  |  |
| --- | --- |
| Автор  | Евтушенко Нина Владимировна |
| Число кредитов  | 7 |
| Контактная работа (час.)  | 60 |
| Самостоятельная работа (час.)  | 206 |
| Курс  | 2 |
| Формат изучения дисциплины | Без использования онлайн курса |

1. **ЦЕЛЬ, РЕЗУЛЬТАТЫ ОСВОЕНИЯ ДИСЦИПЛИНЫ И ПРЕРЕКВИЗИТЫ**

Целями освоения дисциплины «Формальные методы верификации и тестирования телекоммуникационных протоколов и сервисов» являются 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

.

В результате освоения дисциплины студент должен:

**знать:**

− основные математические модели и методы их анализа, используемые для тестирования и верификации телекоммуникационных протоколов и сервисов;

− основные достоинства и недостатки известных формальных методов, используемых для анализа качества программных реализаций телекоммуникационных протоколов и сервисов;

 **уметь:**

− применять известные формальные методы при верификации и тестировании телекоммуникационных протоколов и сервисов;

− адаптировать известные методы и разрабатывать новые для качественной верификации и тестирования телекоммуникационных протоколов и сервисов относительно различных критериев;

**владеть:**

− навыками верификации и тестирования телекоммуникационных протоколов и сервисов, в том числе, на основе формальных моделей.

Изучение дисциплины «Формальные методы верификации и тестирования телекоммуникационных протоколов и сервисов» базируется на следующих дисциплинах:

• «Дискретная математика»,

• «Программирование»,

• «Информатика, математическая логика и теория алгоритмов»,

• «Построение и анализ алгоритмов»,

• «Архитектура вычислительных систем»,

• «Формальные методы в программной инженерии»,

• «Верификация программного обеспечения»

.

Для освоения учебной дисциплины студенты должны владеть следующими знаниями и компетенциями:

* знать основные законы разработки алгоритмов;
* знать формальные методы в программной инженерии;
* обладать навыками разработки программ в языках высокого уровня.

Основные положения дисциплины должны быть использованы в дальнейшем при изучении следующих дисциплин:

Подготовка ВКР.

.

1. **СОДЕРЖАНИЕ УЧЕБНОЙ 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.**

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.**

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; криптографические атаки на протокол TLS; тестирование криптографических протоколов.

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. Формальные модели для анализа телекоммуникационных сервисов.**

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.

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.

1. **ОЦЕНИВАНИЕ**

# **Оценочные средства** для текущего контроля студента.

1. Домашнее задание. Изучение одного из протоколов по выбору преподавателя, его особенностей, подготовка презентации и реферата.
2. Выполнение лабораторной работы по верификация протоколов с использованием верификаторов и подготовка отчета по лабораторной работе.

Оценка за первый семестр (итоговая оценка Оитог.1 складывается из накопленной оценки 1 семестра (Онакопл.1) и оценки за устный экзамен в конце 2-го модуля

(Оэкз.1): Онакопл.1 = Одом.зад.; Оитог.1= 0.5⋅Онакопл.1 + 0.5⋅Оэкз.1;

Оценка (Оитог.1) является результирующей

.

Способ округления оценок – арифметический

1. **ПРИМЕРЫ ОЦЕНОЧНЫХ СРЕДСТВ**

# **Примеры тем рефератов и презентации**

1. Протокол TLS и его свойства.
2. Криптографичекие атаки на протокол TLS.
3. Верификатор SPIN; язык Promela.
4. Верификатор Tаmarin, его свойства, достоинства, недостатки.
5. Формальные методы оценки качества телекоммуникационных сервисов.
6. Самообучающиеся модели для оценки качества телекоммуникационных сервисов; нейронные сети с учителем и без учителя, векторные машины, линейная регрессия.
7. Верификация (компонентов) программно-конфигурируемых сетей.
8. Синтез тестов для (компонентов) программно-конфигурируемых сетей.

**Пример лабораторной работы** «Верификация протокола Open-Flow» с использованием верификатора SPIN и подготовка отчета по лабораторной работе.

**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. Криптографические атаки на протокол TLS.
9. Какие существуют этапы проектирования сетевых сервисов?
10. Использование формальных моделей, в том числе моделей с конечным числом состояний для анализа компонентов программно-конфигурируемых сетей.
11. **РЕСУРСЫ**
	1. **Основная литература**
12. Б. Шнайер Прикладная криптография. Протоколы, алгоритмы и исходные текста на языке С, ч. 1., 1995.
13. А.С. Камкин. Верификация программного обеспечения. Изд-во МГУ, 2018, 272 с.
14. 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.:
15. TLS 1.2 [Электронный ресурс] - Режим доступа:

https://tools.ietf.org/html/rfc5246

1. TLS 1.3 [Электронный ресурс] - Режим доступа:

https://tools.ietf.org/html/rfc8446

1. Р. Смелянский. Программно-конфигурируемые сети [Электронный ресурс] – Режим доступа:

http://www.webcitation.org/6DyOwYRyU

* 1. **Дополнительная литература**
1. А.К.Петренко, А.В.Хорошилов, Е.В.Корныхин. Лекция 8. Тестирование на основе формальных моделей [Электронный ресурс] / F.К.Петренко, А.В.Хорошилов, Е.В.Корныхин. Лекция 8, 2012. – Режим доступа:

http://sp.cmc.msu.ru/courses/fmsp/2012/slides/lecture8.pdf (дата обращения: 03.10.2016).

2. SPIN [Электронный ресурс] / Режим доступа

https:// spinroot.com

1. Р. Смелянский. Программно-реконфигурируемые сети. Открытые системы, № 9, 2012.
2. 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.
3. Proccedings of Intern Conf. on Software Testing, ICST, 2008 -2015, and Testing Systems and Software, ICTSS, 1991 – 2018 (ранее: on Protocol Testing)
	1. **Программное обеспечение**

|  |  |  |
| --- | --- | --- |
| **№ п/п** | **Наименование** | **Условия доступа** |
|   1. |  Microsoft Windows 7 Professional RUSMicrosoft Windows 10Microsoft Windows 8.1 Professional RUS | *Из внутренней сети университета (договор)* |
| 2. | Microsoft Office Professional Plus 2010 | *Из внутренней сети университета (договор)* |

* 1. **Материально-техническое обеспечение дисциплины**

Учебные аудитории для лекционных занятий по дисциплине обеспечивают использование и демонстрацию тематических иллюстраций, соответствующих программе дисциплины в составе:

ПЭВМ с доступом в Интернет (операционная система, офисные программы, антивирусные программы);

мультимедийный проектор с дистанционным управлением.

Учебные аудитории для лабораторных и самостоятельных занятий по дисциплине оснащены ­­­­­­­­­­­­­­­­­­­­­­­­ персональными компьютерами, с возможностью подключения к сети Интернет и доступом к электронной информационно-образовательной среде НИУ ВШЭ.