ГОУ ВПО Российско-Армянский (Славянский) университет

Утверждено
Директор Института
Математики и Информатики
_____ Дарбинян А.А.
«18» июня 2024, протокол №15

УЧЕБНО-МЕТОДИЧЕСКИЙ КОМПЛЕКС ДИСЦИПЛИНЫ

Наименование дисциплины: Практические методы анализа ПО

Авторы: *канд.физ.-мат.наук Асланян Айк Каренович*

Направление подготовки: 01.04.02 Прикладная математика и информатика

1. АННОТАЦИЯ

1.1. Краткое описание содержания данной дисциплины;

Этот курс предоставляет комплексное понимание практических методов обеспечения безопасности программного обеспечения, с акцентом на интеграцию мер безопасности в жизненный цикл разработки программного обеспечения. Курс охватывает такие темы, как конвейеры непрерывной интеграции/непрерывной доставки (CI/CD), GitLab, Jenkins, статический анализ и инструменты для фаззинга.

1.2. Трудоемкость в академических кредитах и часах, формы итогового контроля (экзамен/зачет);

2-ой семестр - 6 ЗЕТ- экзамен,

1.3. Взаимосвязь дисциплины с другими дисциплинами учебного плана специальности (направления)

Для прохождения этого курса изучение других дисциплин не требуются.

1.4. Результаты освоения программы дисциплины:

Код компетенции	**Наименование компетенции**	**Код индикатора достижения компетенций**	**Наименование индикатора достижений компетенций**
ОПК-3	Способен разрабатывать математические модели и проводить их анализ при решении задач в области профессиональной деятельности	**ОПК-3.1**	Формулирует основные теоретические положения в области математического моделирования.
		ОПК-3.2	Демонстрирует умения давать содержательную интерпретацию полученных результатов при проведении анализа математических моделей.
		ОПК-3.3	Имеет практический опыт разработки и проведения анализа математических моделей при решении задач

ОПК-4	Способен комбинировать и адаптировать существующие информационно-коммуникационные технологии для решения задач в области профессиональной деятельности с учетом требований информационной безопасности	**ОПК-4.1**	Обладает знаниями о существующих информационно коммуникационных технологиях и основных требованиях информационной безопасности.
		ОПК-4.2	Демонстрирует умения комбинировать и адаптировать существующие информационно коммуникационные технологии, а также умение учитывать основные требования информационной безопасности при решении прикладных задач
		ОПК-4.3	Имеет практический опыт комбинирования и адаптирования существующих информационно коммуникационных технологий и учета основных требований информационной безопасности при решении прикладных задач
ПК-11	способностью разрабатывать аналитические обзоры состояния	**ПК-11.1**	Знает методологические принципы современной науки, направления,

	области прикладной математики и информационных технологий		концепции, источники знания и приемы работы с ними
		ПК-11.2	Умеет применять логические методы и приемы научного исследования
		ПК-11.3	Может проводить методологическое обоснование научного исследования
ПК-12	способностью к взаимодействию в рамках международных проектов и сетевых сообществ в области прикладной математики и информационных технологий	**ПК-12.1**	Знает новые научные принципы и методы реинжиниринга
		ПК-12.2	Умеет модернизировать программное и аппаратное обеспечение информационных и автоматизированных систем по международные стандартам
		ПК-12.3	Владеет необходимым инструментарием для выведения продукта на международный уровень

2. УЧЕБНАЯ ПРОГРАММА

2.1. Цели и задачи дисциплины

- Понять важность безопасности в жизненном цикле разработки программного обеспечения.
- Реализовать безопасные конвейеры CI/CD с использованием инструментов, таких как GitLab и Jenkins.
- Выполнять статический анализ для обнаружения уязвимостей в исходном коде.
- Использовать инструменты фаззинга для выявления недостатков безопасности.

- Применять лучшие практики безопасности программного обеспечения в реальных проектах.

2.2. Трудоемкость дисциплины и виды учебной работы (в академических часах и зачетных единицах)

Виды учебной работы	Всего, в акад. часах	Распределение по семестрам					
		I сем	II сем	___ сем	___ сем.	___ сем	____ сем.
1	2	3	4	5	6	7	8
1. Общая трудоемкость изучения дисциплины по семестрам, в т. ч.:	**324**						
1.1. Аудиторные занятия, в т. ч.:	**154**						
1.1.1. Лекции	**58**	**34**					
1.1.2. Практические занятия, в т. ч.	**96**	**72**					
1.2. Самостоятельная работа, в т. ч.:	**107**	**74**					
1.3. Другие методы и формы занятий	**63**	**36**					
Итоговый контроль (Экзамен, Зачет, диф. зачет - указать)		**Экзамен**	**Диф.зачет**				

2.3. Содержание дисциплины

2.3.1. Тематический план и трудоемкость аудиторных занятий (модули, разделы дисциплины и виды занятий) по рабочему учебному плану

Разделы и темы дисциплины	Всего (ак. часов)	Лекции (ак. часов)	Практ. занятия (ак. часов)	Семина-ры (ак. часов)	Лабор. (ак. часов)	Другие виды занятий (ак. часов)
1	2=3+4+5+6+7	3	4	5	6	7
Модуль 1.						
Тема 1. Введение в безопасность программного обеспечения	**4**	**2**	**2**			
Тема 2. GitLab и Jenkins для CI/CD	**4**	**2**	**2**			
Тема 3. Статический анализ	**4**	**2**	**2**			
Тема 4. Инструменты фаззинга	**4**	**2**	**2**			
Тема 5. Санитайзеры	**4**	**2**	**2**			

Тема 6. Практики безопасного кодирования	**4**	**2**	**2**			
Тема 7. Тестирование безопасности и QA	**4**	**2**	**2**			
Тема 8. Финальный проект	**4**	**2**	**2**			
ИТОГО	**32**	**16**	**16**			

2.3.2. Краткое содержание разделов дисциплины в виде тематического плана

Тема 1: Введение в безопасность программного обеспечения

- Обзор безопасности программного обеспечения
- Общие угрозы и уязвимости безопасности
- Важность интеграции безопасности в жизненный цикл разработки программного обеспечения
- Введение в концепции CI/CD
- Преимущества CI/CD в обеспечении безопасности программного обеспечения

Тема 2: GitLab и Jenkins для CI/CD

- Введение в GitLab и Jenkins
- Создание и конфигурирование конвейеров GitLab и Jenkins
- Интеграция проверок безопасности в конвейеры GitLab и Jenkins

Тема 3: Статический анализ

- Обзор статического анализа
- Инструменты для статического анализа (например, SonarQube, Coverity)
- Интеграция статического анализа в конвейеры CI/CD
- Анализ и интерпретация результатов статического анализа
- Лучшие практики статического анализа

Тема 4: Инструменты фаззинга

- Введение в фаззинг
- Типы фаззинга (например, black-box, white-box, grey-box)
- Инструменты для фаззинга (например, AFL, LibFuzzer)
- Интеграция инструментов фаззинга в конвейеры CI/CD

Тема 5: Санитайзеры

- Введение в санитайзеры
- Типы санитайзеров (например, AddressSanitizer, ThreadSanitizer, MemorySanitizer)

- Применение санитайзеров для выявления ошибок в программах

Тема 6: Практики безопасного кодирования

- Принципы безопасного кодирования
- Общие руководства по безопасному кодированию (например, OWASP, CERT)
- Стандарты безопасного кодирования

Тема 7: Тестирование безопасности и QA

- Методы тестирования безопасности (например, тестирование на проникновение, рецензия кода)
- Инструменты для тестирования безопасности
- Интеграция тестирования безопасности в процессы QA

Тема 8: Финальный проект

- Проектирование безопасного конвейера CI/CD
- Интеграция инструментов статического анализа и фаззинга

- Реализация и демонстрация безопасного программного проекта

2.3.3. Краткое содержание семинарских/практических занятий/лабораторного практикума

Решение задач согласно пройденной на лекционном занятии темы.

2.3.4. Материально-техническое обеспечение дисциплины

Компьютеры с интернет-браузером.

2.4. Модульная структура дисциплины с распределением весов по формам контролей

Формы контролей	Вес формы (форм) текущего контроля в результирующей оценке текущего контроля (по модулям)		Вес формы промежуточного контроля в итоговой оценке промежуточного контроля		Вес итоговой оценки промежуточного контроля в результирующей оценке промежуточных контролей		Вес итоговой оценки промежуточного контроля в результирующей оценке промежуточных контролей (семестровой оценке)	Веса результирующей оценки промежуточных контролей и оценки итогового контроля в результирующей оценке итогового контроля
Вид учебной работы/контроля	**М1**	**М2**	**М1**	**М2**	**М1**	**М2**		
Контрольная работа		1		1				
Письменные домашние задания *(при наличии)*								
Веса результирующих оценок текущих контролей в итоговых оценках промежуточных контролей								
Веса оценок промежуточных контролей в итоговых оценках промежуточных контролей					0.5	0.5		
Вес итоговой оценки 1-го промежуточного контроля в результирующей оценке промежуточных контролей							0	
Вес итоговой оценки 2-го промежуточного контроля в результирующей оценке промежуточных контролей							1	
Вес результирующей оценки промежуточных контролей в результирующей оценке итогового контроля								0.5
Вес итогового контроля (Экзамен/зачет) в результирующей оценке итогового контроля								0.5

	∑ = **1**	∑ = **1**	∑ = **1**	∑ = **1**	∑ = **1**	∑ = **1**	∑ = **1**	∑ = **1**

3. Теоретический блок

3.1. Материалы по теоретической части курса

3.1.1. Брайан Керниган, Деннис Ритчи, Язык программирования Си, 2-е издание

Бьерн Страуструп, Язык программирования C++, 2-е издание

Герберт Шилдт, C++. Базовый курс

3.1.2. Учебное пособие:

«Ալգորիթմներ և ալգորիթմական լեզուներ» Գործնական պարապմունքների մեթոդական ձեռնարկ

https://rau.am/uploads/post/editor_image/C_C++%20practice%20(1)_1717589821.pdf

4. Фонды оценочных средств.

4.1. Материалы по практической части курса

4.1.1. Учебно-методические пособия;

Սարգսյան Ս., Ասլանյան Կ.

4.2. Вопросы и задания для самостоятельной работы студентов

В системе ejudge

4.3. Перечень экзаменационных вопросов

1. Представление целых и вещественных чисел в двоичной форме. Прямой, обратный и дополнительный код. IEEE-754 формат. Порядок представления байтов (big and little endian). Размеры типов в языке C. Знаковые и беззнаковые числа. Приведение типов.

Литература:

- Книга Computer Systems Programmers perspective, вторая глава.
- Книга Зубков С. В, первая глава
- Книга В.И. Юров: глава 4, глава 17

2. Процессор x86, регистры. Формат данных. Пересылка данных (mov). Регистр eflags. Арифметические и логические операции. Сдвиги. Переполнение. Флаги OF, CF, ZF. Отображение из C в ассемблер и наоборот.

Литература:

● Книга Computer Systems Programmers perspective: 3.1 - 3.6

● Книга В.И. Юров: глава 7, 8, 9

3. Флаги OF, CF, ZF, SF. Команды передачи управления. Инструкция jmp и условный переход. Представление операторов условного перехода языка Си в ассемблере. Оператор switch.

Литература:

● Книга Computer Systems Programmers perspective: 3.1 - 3.6

● Intel reference manual

● Книга В.И. Юров: глава 10

4. Организация циклов. Инструкция loop. Представление операторов цикла языка Си в ассемблере: do-while, while, for. Инструкция условной пересылки (Conditional Move Instructions)

Литература:

● Книга Computer Systems Programmers perspective: 3.1 - 3.6

● Книга В.И. Юров: глава 10

5. Представление программы в памяти. Стек и локальные переменные. Расположение глобальных и статических переменных. Организация вызова функций. Передача аргументов, адрес возврата. Фрейм стека. Различные соглашения о вызовах.

Литература:

● Книга Computer Systems Programmers perspective: 3.7

● Книга Зубков С. В, 5.2, 5.3

● Книга В.И. Юров: глава 15

6. Массивы и указатели. Представление одномерных и двумерных массивов. Структуры данных в ассемблере.

Литература:

● Книга Computer Systems Programmers perspective: 3.1 - 3.6

● Книга В.И. Юров: глава 13

7. Процессор x87. Организация процессора и его регистры. Основные команды процессора x87.

Литература:

● Книга В.И. Юров: Глава 17

8. RISC-V

Литература:

- https://riscv.org/wp-content/uploads/2017/05/riscv-spec-v2.2.pdf
- https://github.com/riscv/riscv-bitmanip/releases/download/1.0.0/bitmanip-1.0.0.pd