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

Институт прикладной математики и компьютерных наук

УТВЕРЖДЕНО:
Директор
А. В. Замятин

Оценочные материалы по дисциплине

Защита информации на уровне программ и данных

по направлению подготовки

01.04.02 Прикладная математика и информатика

Направленность (профиль) подготовки:
Информационная безопасность

Форма обучения
Очная

Квалификация
Магистр

Год приема
2024

СОГЛАСОВАНО:
Руководитель ОП
А.Ю. Матросова

Председатель УМК
С.П. Сущенко

Томск – 2024

1. Компетенции и индикаторы их достижения, проверяемые данными оценочными материалами

Целью освоения дисциплины является формирование следующих компетенций:

ОПК-4 Способен комбинировать и адаптировать существующие информационно-коммуникационные технологии для решения задач в области профессиональной деятельности с учетом требований информационной безопасности.

ПК-2 Способен оценить уровень безопасности компьютерных систем и разработать программно-аппаратные средства защиты информации.

Результатами освоения дисциплины являются следующие индикаторы достижения компетенций:

ИОПК-4.3 Использует современные информационно-коммуникационные технологии для решения задач в области прикладной математики и информатики с учетом требований информационной безопасности.

ИПК-2.1 Осуществляет проведение контрольных проверок работоспособности и эффективности применяемых программно-аппаратных средств защиты информации, разработку требований к программно-аппаратным средствам защиты информации компьютерных систем.

ИПК-2.2 Осуществляет разработку требований по защите, формирование политик безопасности компьютерных систем и сетей, проектирование программно-аппаратных средств защиты информации компьютерных систем.

ИПК-2.3 Осуществляет проведение анализа безопасности компьютерных систем, проведение сертификации программно-аппаратных средств защиты информации и анализ результатов, разработку и тестирование средств защиты информации компьютерных систем.

2. Оценочные материалы текущего контроля и критерии оценивания

Элементы текущего контроля:

– лабораторные работы;

Примеры лабораторных работ (ИОПК-4.3, ИПК-2.1, ИПК-2.2, ИПК-2.3):

1. Исследование бинарных приложений, имеющих архитектуру x86.

Цель и задачи: развить навыки анализа и понимания алгоритмов, реализованных в бинарных приложениях для архитектуры x86; углубить знания о низкоуровневых аспектах программирования, специфичных для архитектуры x86; изучить и распознать используемые в приложениях методы запутывания (обфускации). В лабораторной работе студенты анализируют приложение, скомпилированное для архитектуры x86, выясняют реализуемый алгоритм, распознают и исследуют методы обфускации, если они присутствуют.

2. Исследование бинарных приложений, имеющих архитектуру AMD64

Цель: развить навыки анализа и понимания алгоритмов, реализованных в бинарных приложениях для архитектуры AMD64; изучить низкоуровневые детали и специфики программирования для архитектуры AMD64; освоить особенности соглашений о вызовах и анализ структуры стекового кадра для 64-битных приложений. идентифицировать и объяснить применяемые в приложениях методы запутывания (обфускации). Студенты проводят анализ бинарного приложения, написанного для архитектуры AMD64, чтобы объяснить алгоритм, реализованный приложением. Изучают и объясняют низкоуровневые детали, такие как специфические для AMD64 соглашения о вызовах и структура стекового кадра. Также необходимо определить и описать методы обфускации, применяемые в приложении, выделить различия и сходства с архитектурой x86.

Критериями выполнения студентом лабораторной работы являются:

- способность студента объяснить алгоритм, реализуемый приложением, предоставляемом в лабораторной работе;
- понимание и способность объяснить низкоуровневые детали реализации алгоритма, сгенерированные компилятор, такие как: соглашение о вызовах, используемое данной функцией, структура стекового фрейма, используемые в приложении методы запутывания.

3. Оценочные материалы итогового контроля (промежуточной аттестации) и критерии оценивания

Экзамен во втором семестре проводится в устной (или письменной) форме по билетам. Экзаменационный билет содержит два теоретических вопроса.

Теоретические вопросы к экзамену (ИПК-2.1, ИПК-2.2, ИПК-2.3):

- Что такое calling convention? Основные СС для архитектуры i386: ключевые особенности и отличия.
- Что такое calling convention? Основные СС для архитектуры amd64: ключевые особенности и отличия.
- Принципы работы вариадических функций в 32-битных СС
- Принципы работы вариадических функций в 64-битных СС
- Особенности стековых фреймов в 64-битных СС
- Динамическая линковка и загрузка кода.
- Механизм сигналов в Linux. Запутывание потока исполнения на основе сигналов

Результаты экзамена определяются оценками «отлично», «хорошо», «удовлетворительно», «неудовлетворительно». Положительная оценка на экзамене ставится только в случае сдачи студентом всех лабораторных работ.

Оценка «отлично» ставится, если полно раскрыто содержание материала вопроса; материал изложен грамотно, в определенной логической последовательности.

«Хорошо»: вопрос изложен систематизировано и последовательно; продемонстрировано умение анализировать материал, однако в изложении допущены небольшие пробелы, не исказившие содержание ответа.

«Удовлетворительно»: неполно или непоследовательно раскрыто содержание материала, но показано общее понимание вопроса и продемонстрированы умения, достаточные для дальнейшего усвоения материала.

«Неудовлетворительно»: полностью отсутствует ответ; не раскрыто основное содержание вопроса; обнаружено незнание или непонимание большей, или наиболее важной части вопроса.

4. Оценочные материалы для проверки остаточных знаний (сформированности компетенций)

Для проверки остаточных знаний студенту предлагается ответить на один теоретический экзаменационный вопрос (перечень теоретических вопросов и критерии оценивания приведены в п. 3)

Информация о разработчиках

Останин Сергей Александрович, канд. техн. наук, заведующий кафедрой компьютерной безопасности