

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

Анализ уязвимостей программного обеспечения

по направлению подготовки / специальности

10.05.01 Компьютерная безопасность

Направленность (профиль) подготовки/ специализация:
Анализ безопасности компьютерных систем

Форма обучения
Очная

Квалификация
Специалист по защите информации

Год приема
2025

СОГЛАСОВАНО:
Руководитель ОП
В.Н. Тренькаев

Председатель УМК
С.П. Сущенко

Томск – 2025

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

Целью освоения дисциплины является формирование следующих компетенций:

ОПК-13 Способен разрабатывать компоненты программных и программно-аппаратных средств защиты информации в компьютерных системах и проводить анализ их безопасности.

ОПК-20 Способен проводить тестирование и использовать средства верификации механизмов защиты информации.

ПК-3 Способен проектировать программно-аппаратные средств защиты информации компьютерных систем и сетей.

Результатами освоения дисциплины являются следующие индикаторы достижения компетенций:

ИОПК-13.1 Предпринимает необходимые действия по сбору и анализу исходных данных для проектирования компонент программных и программно-аппаратных средств защиты информации в компьютерных системах

ИОПК-13.2 Определяет параметры функционирования, архитектуру и интерфейсы компонент программных и программно-аппаратных средств защиты информации в компьютерных системах

ИОПК-13.3 Проводит анализ компонент программных и программно-аппаратных средств защиты информации в компьютерных системах с целью определения уровня обеспечиваемой ими защищенности и доверия

ИОПК-20.1 Понимает принципы организации, состав и алгоритмы работы механизмов защиты информации, стандарты оценивания защищенности компьютерных систем

ИОПК-20.2 Проводит исследование механизмов защиты информации, в том числе с использованием средств верификации, и делает выводы по оценке защищенности и доверия

ИПК-3.3 Проведение аттестации программ и алгоритмов на предмет соответствия требованиям защиты информации

2. Оценочные материалы текущего контроля и критерии оценивания

Элементы текущего контроля:

– лабораторные работы.

Примеры лабораторных работ (ИОПК-13.1, ИОПК-13.2, ИОПК-13.3, ИОПК-20.2, ИПК-3.3)

1. Выданное приложение уязвимо к атаке типа off-by-one. Произвести атаку и получить права администратора в тестовом приложении, доступном по адресу host:port.
2. Выданное приложение уязвимо к атаке переполнения стекового буфера. Произвести атаку и получить возможность выполнения произвольного кода в тестовом приложении, доступном по адресу host:port.
3. Выданное приложение уязвимо к атаке типа Return Oriented Programming. Произвести атаку и получить возможность выполнения произвольного кода в тестовом приложении, доступном по адресу host:port.
4. Выданное приложение уязвимо к атаке типа Return to libc. Произвести атаку и получить возможность выполнения произвольного кода в тестовом приложении, доступном по адресу host:port.

Критерием выполнения студентом лабораторной работы является:

- наличие у студента программной реализации атаки на рассматриваемое в рамках лабораторной работы приложение;
- способность студента объяснить суть атаки, уязвимость, приводящую к возможности осуществления атаки, и причины ее возникновения, а также меры, которые необходимо предпринять чтобы сделать произведенную атаку невозможной для воспроизведения злоумышленником.

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

Промежуточная аттестация по дисциплине проводится в форме устного зачета по теоретическому материалу.

Обучающийся должен знать способы выявления основных уязвимостей ПО, и продемонстрировать навыки выявления уязвимостей в различных приложениях.

Каждый билет для устного зачёта состоит из двух теоретических вопросов по двум темам дисциплины.

Примеры теоретических вопросов в устном зачёте (ИОПК-13.3, ИОПК-20.1, ИПК-3.3):

- Атаки на бинарные приложения типа переполнения локального буфера. Методы обнаружения. Способы предотвращения.
- Атаки на бинарные приложения типа переполнения буфера на куче. Методы обнаружения. Способы предотвращения.
- Атаки на бинарные приложения типа Return Oriented Programming. Методы обнаружения. Способы предотвращения.
- Атаки на бинарные приложения типа Return to libc. Методы обнаружения. Способы предотвращения.
- Атаки на бинарные приложения при помощи контроля форматной строки. Методы обнаружения. Способы предотвращения.
- Атаки на бинарные приложения типа arbitrary read. Методы обнаружения. Способы предотвращения.
- Атаки на бинарные приложения типа arbitrary write. Методы обнаружения. Способы предотвращения.
- Атаки на бинарные приложения типа off-by-one. Методы обнаружения. Способы предотвращения.
- Атаки на бинарные приложения типа type confusion. Методы обнаружения. Способы предотвращения.

Оценка «зачтено» ставится, если студент выполнил лабораторные работы и владеет большей частью теоретического материала. Оценка «не зачтено» – студент не выполнил лабораторные работы и/или не освоил большую часть теоретического материала.

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

Теоретические вопросы (ИОПК-13.2, ИОПК-13.3, ИОПК-20.1, ИПК-3.3):

1. Понятие уязвимостей программного обеспечения
2. Классификация уязвимостей программного обеспечения

3. Техники борьбы с уязвимостями этапа проектирования программного обеспечения.
4. Техники предотвращения уязвимостей на этапе реализации программного обеспечения.
5. Техники анализа бинарных уязвимостей программного обеспечения.

Теоретические вопросы для проверки остаточных знаний предполагают краткое раскрытие основного содержания соответствующего вопроса.

Информация о разработчиках

Останин Сергей Александрович, канд. техн. наук, доцент кафедры компьютерной безопасности.