

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 программ и данных

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. Треньяев

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-19 Способен оценивать корректность программных реализаций алгоритмов защиты информации.

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

ПК-2 Способен разрабатывать требования к программно-аппаратным средствам защиты информации компьютерных систем и сетей.

ПК-3 Способен проектировать программно-аппаратные средства 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-19.1 Обладает знанием формальных приемов, правил, алгоритмов, технологий создания и документирования контрольных примеров и тестовых наборов данных

ИОПК-19.2 Осуществляет подготовку тестовых наборов данных в соответствии с выбранной методикой, а также проверку работоспособности программного обеспечения на основе разработанных тестовых наборов данных

ИОПК-19.3 Осуществляет сбор и анализ полученных результатов проверки работоспособности программного обеспечения, оценку соответствия программного обеспечения требуемым характеристикам

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-2.3 Проводит исследования с целью нахождения наиболее целесообразных практических решений по обеспечению защиты информации

ИПК-3.2 Разработка проектов программных и аппаратных средств защиты информации в соответствии с техническим заданием

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:

– практические задания;

Примеры практических работ (ОПК-13, ОПК-19, ОПК-20, ИПК-2)

1. Исследование бинарных приложений, имеющих архитектуру x86
2. Исследование бинарных приложений, имеющих архитектуру AMD64
3. Исследование бинарных приложений, имеющих архитектуру ARM
4. Исследование приложений, использующих методы запутывания потока исполнения
5. Исследование приложений, использующих методы сокрытия данных
6. Применение SAT/SMT решателей при исследовании бинарных приложений

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

Контрольные вопросы для проведения зачета (ИОПК-19.1, ИОПК-20.1, ИПК-2.3, ИПК-3.3):

- 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 вариadicеских функций в 32-битных СС
- Принципы работы вариadicеских 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.
- Защита программ от изучения
- Понятие программной закладки
- Классификация программных закладок
- Модель наблюдатель
- Модель перехват
- Методы внедрения программных закладок
- Принципы построения политики безопасности, обеспечивающей высокую защищенность от программных закладок

Оценка «зачтено» ставится если студент выполнил все практические задания и владеет большей частью теоретического материала. Оценка «не зачтено» ставится, если студент не выполнил все практические задания и не освоил большую часть теоретического материала.

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

Теоретические вопросы (ИОПК-19.1, ИОПК-20.1)

1. Принципы функционирования отладчиков
2. Методы поиска функций защиты в машинном коде
3. Защита от дизассемблирования
4. Защита от отладки
5. Методы встраивания защиты в программное обеспечение
6. Понятие программной закладки

7. Классификация программных закладок
8. Методы внедрения программных закладок
9. Компьютерные вирусы как особый класс программных закладок
10. Средства и методы маскировки вирусов и противодействия антивирусному программному обеспечению

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.