

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

10.03.01 Информационная безопасность

Направленность (профиль) подготовки:
Безопасность компьютерных систем

Форма обучения
Очная

Квалификация
Бакалавр

Год приема
2025

СОГЛАСОВАНО:
Руководитель ОП
В.Н. Тренькаев

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-1.4. Способен оценивать уровень безопасности компьютерных систем и сетей, в том числе в соответствии с нормативными и корпоративными требованиями.

Результатами освоения дисциплины являются следующие индикаторы достижения компетенций:

ИОПК-1.4.1. Понимает принципы организации, состав и алгоритмы работы механизмов защиты информации, стандарты оценивания безопасности компьютерных систем и сетей.

ИОПК-1.4.2. Определяет уровень защищенности компьютерных систем и сетей и прогнозирует возможные пути развития действий нарушителя информационной безопасности.

ИОПК-1.4.3. Оценивает соответствие механизмов безопасности требованиям существующих нормативных документов, а также их адекватности существующим рискам.

2. Оценочные материалы текущего контроля и критерии оценивания

Элементы текущего контроля:

– практические задания.

Примеры практических работ:

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.

Критерии оценки решения задачи:

За решение задачи выставляется оценка «зачтено», если верно указан и использован метод решения задачи; корректно реализован алгоритм решения задачи; получен полный и правильный ответ.

За решение задачи выставляется оценка «не зачтено», если ответ отсутствует полностью или допущены ошибки при использовании выбранного метода решения задачи; некорректно реализован алгоритм решения задачи; ответ не получен или получен неверный.

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

Зачет в 7 семестре проводится в письменной и(или) устной форме. Зачётное задание состоит из двух частей: одного теоретического вопроса и одной задачи. В рамках перечня теоретических вопросов и набора задач задания сопоставимы по сложности и затратам времени на выполнение. Поэтому данные задания не сведены в один билет, а выбираются преподавателем в случайном порядке по каждой позиции зачетного задания.

Перечень теоретических вопросов:

1. Что такое calling convention? Основные СС для архитектуры i386: ключевые особенности и отличия.
2. Что такое calling convention? Основные СС для архитектуры amd64: ключевые особенности и отличия.

3. Принципы работы вариационных функций в 32-битных СС.
4. Принципы работы вариационных функций в 64-битных СС.
5. Особенности стековых фреймов в 64-битных СС.
6. Динамическая линковка и загрузка кода.
7. Механизм сигналов в Linux. Запущивание потока исполнения на основе сигналов.
8. Защита программ от изучения.
9. Понятие программной закладки.
10. Классификация программных закладок.
11. Модель «наблюдатель».
12. Модель «перехват».
13. Методы внедрения программных закладок.
14. Принципы построения политики безопасности, обеспечивающей высокую защищенность от программных закладок.

Пример задач:

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 запущивания потока исполнения.
5. Исследование приложений, использующих методы сокрытия данных.
6. Применение SAT/SMT решателей при исследовании бинарных приложений.

Критерии оценивания:

Оценка «зачтено» по итогам промежуточной аттестации по дисциплине «Защита программ и данных» выставляется, если ответ на теоретический вопрос оценен на оценку «зачтено», решение задачи оценено на оценку «зачтено».

Оценка «не зачтено» по итогам промежуточной аттестации по дисциплине «Защита программ и данных» выставляется, если хотя бы одно из зачетных заданий (теоретический вопрос, задача) оценено на оценку «не зачтено».

Критерии оценки ответа на теоретический вопрос:

За ответ на теоретический вопрос выставляется оценка «зачтено», если полно раскрыто содержание материала вопроса; материал изложен грамотно, в определенной логической последовательности; специальные термины используются правильно; определения и формулы приведены верно; допущены одна–две неточности при освещении вопросов, которые исправляются по замечанию преподавателя.

За ответ на теоретический вопрос выставляется оценка «не зачтено», если полностью отсутствует ответ или неполно или непоследовательно раскрыто содержание материала, обнаружено незнание или непонимание большей или наиболее важной части вопроса, допущены ошибки в определении понятий и записи формул.

Критерии оценки решения задачи:

За решение задачи выставляется оценка «зачтено», если верно указан и использован метод решения задачи; корректно реализован алгоритм решения задачи; получен полный и правильный ответ.

За решение задачи выставляется оценка «не зачтено», если ответ отсутствует полностью или допущены ошибки при использовании выбранного метода решения задачи; некорректно реализован алгоритм решения задачи; ответ не получен или получен неверный.

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

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

Информация о разработчиках

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

Данилюк Елена Юрьевна, канд. физ.-мат. наук, доцент, доцент кафедры прикладной математики НИ ТГУ.