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

Институт прикладной математики и компьютерных наук

УТВЕРЖДАЮ:
Директор
_____А. В. Замятин
« 16 » _____ 20 23 г.

Рабочая программа дисциплины

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
2023

Код дисциплины в учебном плане: Б1.О.06.07

СОГЛАСОВАНО:
Руководитель ОП
_____В.Н. Тренькаев

Председатель УМК
_____С.П. Сущенко

Томск – 2023

1. Цель и планируемые результаты освоения дисциплины

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 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-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. Задачи освоения дисциплины

– Освоить сбор, обработку, анализ и систематизацию научно-технической информации, отечественного и зарубежного опыта по проблемам компьютерной безопасности;

– Поучаствовать в теоретических и экспериментальных научно-исследовательских работах по оценке защищенности информации в компьютерных системах;

– Изучить и обобщить опыты работы других учреждений, организаций и предприятий по способам использования методов и средств обеспечения информационной безопасности с целью повышения эффективности и совершенствования работ по защите информации на конкретном объекте;
– Освоить разработку математических моделей защищаемых процессов и средств защиты информации и систем, обеспечивающих информационную безопасность объектов; установку наладку, тестирование и обслуживание аппаратно-программных средств обеспечения информационной безопасности компьютерных систем;
– Научиться проводить аттестацию технических средств, программ, алгоритмов на предмет соответствия требованиям защиты информации по соответствующим классам безопасности или профилям защиты.

3. Место дисциплины в структуре образовательной программы

Дисциплина относится к обязательной части образовательной программы. Дисциплина входит в модуль "Специализация".

4. Семестр(ы) освоения и форма(ы) промежуточной аттестации по дисциплине

Девятый семестр, зачет

5. Входные требования для освоения дисциплины

Для успешного освоения дисциплины требуются результаты обучения по следующим дисциплинам: Языки программирования, Операционные системы.

6. Язык реализации

Русский

7. Объем дисциплины

Общая трудоемкость дисциплины составляет 2 з.е., 72 часов, из которых:
-практические занятия: 32 ч.
в том числе практическая подготовка: 32 ч.
Объем самостоятельной работы студента определен учебным планом.

8. Содержание дисциплины, структурированное по темам

Тема 1. Анализ программных реализаций
Постановка задачи анализа программных реализаций. Метод экспериментов с “черным ящиком”. Статический метод. Динамический метод.

Тема 2. Защита программ от изучения
Искусственное усложнение структуры программы. Нестандартные обращения к функциям операционной системы. Искусственное усложнение алгоритмов обработки данных.

Тема 3. Программные закладки
Программные закладки и формальные модели их взаимодействия с атакуемой системой.

Тема 4. Внедрение программных закладок
Формальная модель “наблюдатель”. Формальная модель “перехват”. Формальная модель “искажение”.

Тема 5. Противодействие программным закладкам

Средства и методы защиты от программных закладок. Основные принципы компьютерной системы в отношении программных закладок. Принцип минимизации ПО.

9. Текущий контроль по дисциплине

Текущий контроль по дисциплине проводится путем контроля качества выполнения лабораторных работ и проведения контрольных точек, и фиксируется в форме контрольной точки не менее одного раза в семестр.

Практическая подготовка оценивается по результатам выполненных практических работ.

10. Порядок проведения и критерии оценивания промежуточной аттестации

Форма промежуточной аттестации – зачет. Обучающийся должен знать общепринятые методы защиты приложений и данных от статического и динамического анализа. При этом оценка «Зачтено» ставится, если студент выполнил практические задания и владеет большей частью теоретического материала. Оценка «Не зачтено» – студент не выполнил практические задания и не освоил большую часть теоретического материала.

11. Учебно-методическое обеспечение

а) Электронный учебный курс по дисциплине в электронном университете «Moodle»

б) Оценочные материалы текущего контроля и промежуточной аттестации по дисциплине (Приложение 1).

12. Перечень учебной литературы и ресурсов сети Интернет

а) основная литература:

– Защита программ и данных, Учебное пособие, Проскурин, В. Г., 2011

– Программирование на языке ассемблера NASM для ОС Unix, Учебное пособие, Столяров А.В., 2011

б) дополнительная литература:

– Reverse Engineering для начинающих, Юричев, Д., Электронный ресурс https://beginners.re/main.html

13. Перечень информационных технологий

а) лицензионное и свободно распространяемое программное обеспечение:

– Oracle VM VirtualBox / VMware Workstation Player или аналогичная система виртуализации.

– Дизассемблер IDA Freeware, Binary Ninja или аналогичный

б) информационные справочные системы:

– Электронный каталог Научной библиотеки ТГУ – http://chamo.lib.tsu.ru/search/query?locale=ru&theme=system

– Электронная библиотека (репозиторий) ТГУ – http://vital.lib.tsu.ru/vital/access/manager/Index

– ЭБС Лань – http://e.lanbook.com/

– ЭБС Консультант студента – http://www.studentlibrary.ru/

– Образовательная платформа Юрайт – https://urait.ru/

– ЭБС ZNANIUM.com – https://znanium.com/
– ЭБС IPRbooks – http://www.iprbookshop.ru/

14. Материально-техническое обеспечение

Аудитории для проведения практических занятий, индивидуальных и групповых консультаций, текущего контроля и промежуточной аттестации.

Помещения для самостоятельной работы, оснащенные компьютерной техникой и доступом к сети Интернет, в электронную информационно-образовательную среду и к информационным справочным системам.

15. Информация о разработчиках

Брославский Олег Викторович, ассистент кафедры компьютерной безопасности ТГУ.