

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  
« 19 » мая 20 22 г.

Рабочая программа дисциплины

**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

**2022**

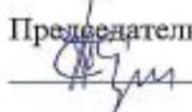
Код дисциплины в учебном плане: Б1.В.04.07

СОГЛАСОВАНО:

Руководитель ОП

 В.Н. Тренькаев

Председатель УМК

 С.П. Сущенко

Томск – 2022

## **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-20 – Способен проводить тестирование и использовать средства верификации механизмов защиты информации.

– 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-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. Задачи освоения дисциплины**

– Сформировать навыки экспертизы качества и надежности реализаций программных и программно-аппаратных средств обеспечения информационной безопасности;

– Сформировать навыки анализа программных реализаций на предмет наличия уязвимостей

## **3. Место дисциплины в структуре образовательной программы**

Дисциплина относится к части образовательной программы, формируемой участниками образовательных отношений. 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 3 з.е., 108 часов, из которых:

-лабораторные: 48 ч.

-практические занятия: 16 ч.

Объем самостоятельной работы студента определен учебным планом.

## **8. Содержание дисциплины, структурированное по темам**

Тема 1. Понятие и классификация уязвимостей программного обеспечения

Основные понятия курса анализ уязвимости программного обеспечения. Основные положения классификации уязвимостей программного обеспечения

Тема 2. Актуальные уязвимости современного программного обеспечения

Понятия угрозы, уязвимости и атаки. Краткий обзор актуальных уязвимостей современного программного обеспечения.

Тема 3. Уязвимости этапа проектирования программного обеспечения

Обзор широко используемых техник борьбы с уязвимостями этап проектирования программного обеспечения. И подходов по уменьшению рисков.

Тема 4. Предотвращение уязвимостей на этапе реализации

Обзор современных техник предотвращения уязвимостей на этапе реализации и методологий по их применению.

Тема 5. Анализ бинарных уязвимостей программного обеспечения

Рассматриваются основные бинарные уязвимости и различные техники их анализа.

## **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.

## **10. Порядок проведения и критерии оценивания промежуточной аттестации**

Форма промежуточной аттестации – зачет. Обучающийся должен знать способы выявления основных уязвимостей ПО, и продемонстрировать навыки выявления уязвимостей в различных приложениях. При этом оценка «Зачтено» ставится, если студент выполнил лабораторные работы и владеет большей частью теоретического материала. Оценка «Не зачтено» – студент не выполнил лабораторные работы и не освоил большую часть теоретического материала.

## **11. Учебно-методическое обеспечение**

а) Электронный учебный курс по дисциплине в электронном университете «Moodle» - <https://moodle.tsu.ru/course/view.php?id=00000>

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

## **12. Перечень учебной литературы и ресурсов сети Интернет**

а) основная литература:

– Linux глазами хакера. - 6-е изд. М. Е. Фленов, 2021

– Penetration Testing: A Hands-On Introduction to Hacking. Georgia Weidman. 2014

б) дополнительная литература:

- The Web Application Hacker's Handbook: Finding and Exploiting Security Flaws. Dafydd Stuttard, Marcus Pinto. Wiley; 2nd edition (September 27, 2011)
- Hacking: The Art of Exploitation, 2nd Edition. Jon Erickson. No Starch Press; 2nd edition (February 4, 2008)

### **13. Перечень информационных технологий**

а) лицензионное и свободно распространяемое программное обеспечение:

- Burp Suite
- Kali Linux
- Oracle VM VirtualBox / VMware Workstation Player или аналогичная система виртуализации.

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 занятий лекционного типа.

Аудитории для проведения занятий семинарского типа, 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.