

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

Рабочая программа дисциплины

Защита информации на уровне программ и данных

по направлению подготовки

01.04.02 Прикладная математика и информатика

Направленность (профиль) подготовки:
Информационная безопасность

Форма обучения
Очная

Квалификация
Магистр

Год приема
2024

СОГЛАСОВАНО:
Руководитель ОП
А.Ю. Матросова

Председатель УМК
С.П. Сущенко

Томск – 2024

1. Цель и планируемые результаты освоения дисциплины

Целью освоения дисциплины является формирование следующих компетенций:

ОПК-4 Способен комбинировать и адаптировать существующие информационно-коммуникационные технологии для решения задач в области профессиональной деятельности с учетом требований информационной безопасности.

ПК-2 Способен оценить уровень безопасности компьютерных систем и разработать программно-аппаратные средства защиты информации.

Результатами освоения дисциплины являются следующие индикаторы достижения компетенций:

ИОПК-4.3 Использует современные информационно-коммуникационные технологии для решения задач в области прикладной математики и информатики с учетом требований информационной безопасности.

ИПК-2.1 Осуществляет проведение контрольных проверок работоспособности и эффективности применяемых программно-аппаратных средств защиты информации, разработку требований к программно-аппаратным средствам защиты информации компьютерных систем.

ИПК-2.2 Осуществляет разработку требований по защите, формирование политик безопасности компьютерных систем и сетей, проектирование программно-аппаратных средств защиты информации компьютерных систем.

ИПК-2.3 Осуществляет проведение анализа безопасности компьютерных систем, проведение сертификации программно-аппаратных средств защиты информации и анализ результатов, разработку и тестирование средств защиты информации компьютерных систем.

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 Блоку 1 «Дисциплины (модули)».

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

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

Второй семестр, экзамен

5. Входные требования для освоения дисциплины

Для успешного освоения дисциплины требуются компетенции, сформированные в ходе освоения образовательных программ предшествующего уровня образования.

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 5 з.е., 180 часов, из которых:

-лекции: 32 ч.

-лабораторные: 16 ч.

в том числе практическая подготовка: 16 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 лабораторных работ.

Оценочные материалы текущего контроля размещены на сайте ТГУ в разделе «Информация об образовательной программе» - <https://www.tsu.ru/sveden/education/eduop/>.

10. Порядок проведения и критерии оценивания промежуточной аттестации

Экзамен во втором семестре проводится в устной/письменной форме по билетам. Экзаменационный билет содержит два теоретических вопроса. Продолжительность экзамена 1,5 часа.

Примеры теоретических вопросов:

- 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. Запутьывание потока исполнения на основе сигналов.

Результаты экзамена определяются оценками «отлично», «хорошо», «удовлетворительно», «неудовлетворительно».

Оценка «отлично» ставится, если полно раскрыто содержание материала вопроса; материал изложен грамотно, в определенной логической последовательности, сданы все лабораторные работы.

«Хорошо»: вопрос изложен систематизировано и последовательно; продемонстрировано умение анализировать материал, однако в изложении допущены небольшие пробелы, не искажившие содержание ответа, сданы все лабораторные работы.

«Удовлетворительно»: неполно или непоследовательно раскрыто содержание материала, но показано общее понимание вопроса и продемонстрированы умения, достаточные для дальнейшего усвоения материала, сданы все лабораторные работы.

«Неудовлетворительно»: полностью отсутствует ответ; не раскрыто основное содержание вопроса; обнаружено незнание или непонимание большей или наиболее важной части вопроса, сданы не все лабораторные работы.

Оценочные материалы для проведения промежуточной аттестации размещены на сайте ТГУ в разделе «Информация об образовательной программе» - <https://www.tsu.ru/sveden/education/eduop/>.

11. Учебно-методическое обеспечение

а) Электронный учебный курс по дисциплине в системе электронного обучения iDO - <https://lms.tsu.ru/course/view.php?id=5545>

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

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 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

Останин Сергей Александрович, канд. техн. наук, заведующий кафедрой компьютерной безопасности.