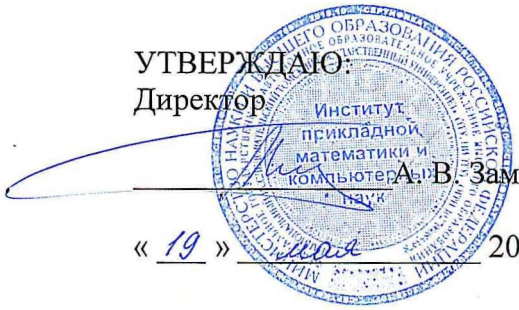
Министерство науки и высшего образования Российской Федерации
НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ
ТОМСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ (НИ ТГУ)

Институт прикладной математики и компьютерных наук

УТВЕРЖДАЮ:
Директор



_____ А. В. Замятин

« 19 » мая 20 22 г.

Рабочая программа дисциплины

Защита в операционных системах

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.О.06.02

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-9 – Способен решать задачи профессиональной деятельности с учетом текущего состояния и тенденций развития методов защиты информации в операционных системах, компьютерных сетях и системах управления базами данных, а также методов и средств защиты информации от утечки по техническим каналам, сетей и систем передачи информации.

– ОПК-16 – Способен проводить мониторинг работоспособности и анализ эффективности средств защиты информации в компьютерных системах и сетях.

– ОПК-18 – Способен проводить анализ защищенности и осуществлять поиск уязвимости компьютерной системы.

– ПК-3 – Способен проектировать программно-аппаратные средств защиты информации компьютерных систем и сетей.

Результатами освоения дисциплины являются следующие индикаторы достижения компетенций:

ИОПК-9.1 Учитывает современные тенденции развития методов защиты информации в операционных системах, компьютерных сетях и системах управления базами данных при решении задач своей профессиональной деятельности.

ИОПК-9.2 Обладает знанием и демонстрирует навыки применения базовых методов защиты информации в операционных системах, компьютерных сетях и системах управления базами данных.

ИОПК-16.1 Осуществляет оценку работоспособности применяемых средств защиты информации в компьютерных системах и сетях с использованием штатных средств и методик.

ИОПК-16.2 Осуществляет оценку эффективности применяемых средств защиты информации в компьютерных системах и сетях с использованием штатных средств и методик.

ИОПК-16.3 Определяет уровень защищенности и доверия средств защиты информации в компьютерных системах и сетях.

ИОПК-18.1 Определяет уровень защищенности и доверия в компьютерных системах и прогнозирует возможные пути развития действий нарушителя информационной безопасности.

ИОПК-18.2 Оценивает соответствие механизмов безопасности компьютерной системы требованиям существующих нормативных документов, а также их адекватности существующим рискам.

ИОПК-18.3 Составляет и оформляет аналитический отчет по результатам проведенного анализа, разрабатывает предложения по устранению выявленных уязвимостей.

ИПК-3.1 Разработка технических заданий, эскизных, технических и рабочих проектов работ по защите информации.

2. Задачи освоения дисциплины

– Изучить понятийный аппарат и общие подходы к обеспечению ИБ операционных систем;
– изучить средства и методы управления доступом в защищенных ОС;
– изучить средства и методы интеграции защищенных ОС в защищенную сеть.

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

Десятый семестр, зачет с оценкой

5. Входные требования для освоения дисциплины

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

6. Язык реализации

Русский

7. Объем дисциплины

Общая трудоемкость дисциплины составляет 4 з.е., 144 часов, из которых:
-лабораторные: 16 ч.
-практические занятия: 32 ч.
Объем самостоятельной работы студента определен учебным планом.

8. Содержание дисциплины, структурированное по темам

Тема 1. Понятие защищенной операционной системы
Предмет защиты информации. Основные положения безопасности информационных систем. Основные принципы обеспечения информационной безопасности в информационных системах.

Тема 2. Управление доступом
Субъекты, объекты, методы и права доступа. Привилегии субъектов доступа. Избирательное и полномочное разграничение доступа, изолированная программная среда. Примеры реализации разграничения доступа в современных ОС.

Тема 3. Идентификация, аутентификация и авторизация
Понятия идентификации и аутентификации пользователей. Аутентификация на основе паролей, методы подбора паролей, средства и методы повышения защищенности ОС от подбора паролей. Аутентификация на основе внешних носителей ключа, биометрических характеристик пользователя. Примеры реализации идентификации и аутентификации в современных ОС.

Тема 4. Аудит в ОС
Необходимость аудита. Требования к подсистеме аудита. Примеры реализации аудита в современных ОС.

Тема 5. Интеграция защищенных операционных систем в защищенную сеть
Классификация методов и их сравнительная статистика.

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 методы защиты информации в современных операционных системах. Уметь продемонстрировать на практике способы обеспечения различных аспектов безопасности ОС на примере выполненных за время семестра лабораторных работ. 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:

– Бэндл Дэвид. Защита и безопасность в сетях Linux. Питер, 2002.

– Проскурин В.Г. Защита в операционных система. Учебное пособие. Горячая линия Телеком, 2016

б) дополнительная литература:

– Девянин П.Н. Модели безопасности компьютерных систем. Управление доступом и информационными потоками. Учебное пособие. Горячая линия Телеком, 2016

– Furgel, I., & Saftig, V. (2016). Common Criteria Protection Profile “Multiple Independent Levels Of Security: Operating System” [V2.03]. https://doi.org/10.5281/zenodo.51582

13. Перечень информационных технологий

а) лицензионное и свободно распространяемое программное обеспечение:

– 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.