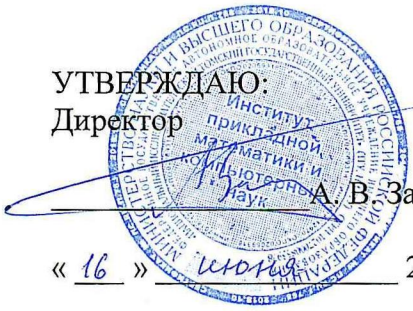
Министерство науки и высшего образования Российской Федерации
НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ
ТОМСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ (НИ ТГУ)

Институт прикладной математики и компьютерных наук



УТВЕРЖДАЮ:
Директор
_____ А. В. Замятин
« 16 » июня 2023 г.

Рабочая программа дисциплины

Модели безопасности компьютерных систем

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.06.09

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-8 – Способен применять методы научных исследований при проведении разработок в области обеспечения безопасности компьютерных систем и сетей.

– ОПК-11 – Способен разрабатывать политики безопасности, политики управления доступом и информационными потоками в компьютерных системах с учетом угроз безопасности информации и требований по защите информации.

– ПК-2 – Способен разрабатывать требования к программно-аппаратным средствам защиты информации компьютерных систем и сетей.

Результатами освоения дисциплины являются следующие индикаторы достижения компетенций:

ИОПК-8.3 Проводит анализ и формализацию поставленных задач, участвует в разработке математических моделей в области обеспечения безопасности компьютерных систем и сетей.

ИОПК-11.1 Понимает основные формальные модели политик управления доступом и информационными потоками в компьютерных системах.

ИОПК-11.2 Владеет необходимым аппаратом формального определения требований политики безопасности, построения и анализа политик управления доступом и информационными потоками в компьютерных системах.

ИОПК-11.3 Формулирует политики безопасности, политики управления доступом и информационными потоками в компьютерных системах с учетом угроз безопасности информации и требований по защите информации.

ИПК-2.1 Определяет угрозы безопасности и их возможные источники, каналы утечки информации.

ИПК-2.2 Разрабатывает математические модели, реализуемые в средствах защиты информации.

Каждая из заявленных компетенций отражает несколько образовательных результатов:

ОР-8.3.1. Знать: назначение и формальное описание классических моделей безопасности (ХРУ, Белла-ЛаПадулы, Take-Grant).

ОР-8.3.2. Уметь: разрабатывать подходящую модель для обеспечения безопасности компьютерных систем и сетей.

ОР-8.3.3. Владеть: математическим аппаратом классических моделей управления доступом.

ОР-11.1.1. Знать: основные формальные модели дискреционного, мандатного, ролевого управления доступом.

ОР-11.1.2. Знать: основные виды политик управления доступом и информационными потоками в компьютерных системах.

ОР-11.2.1. Владеть: аппаратом формального определения требований политики безопасности, построения и анализа политик управления доступом и информационными потоками в компьютерных системах

ОР-11.2.2. Владеть: классическими политиками управления доступом, аппаратом их анализа и разработки.

ОР-11.3.1. Уметь: формулировать свойства безопасности в соответствии с требованиями заданной политики.

ОР-11.3.2. Уметь: разрабатывать политики безопасности компьютерных систем с учетом требований по защите информации.

ОР-2.1.1. Знать: модели изолированной программной среды и безопасности информационных потоков.

ОР-2.1.2. Владеть: математическим аппаратом для анализа безопасности систем управления доступом.

ОР-2.2.1. Уметь: разрабатывать модели угроз и модели нарушителя безопасности компьютерных систем.

ОР-2.2.2. Уметь: разрабатывать механизмы управления доступом для современных компьютерных систем.

2. Задачи освоения дисциплины

- Изучить основные модели дискреционного, мандатного и ролевого управления доступом.
- Изучить модели безопасности информационных потоков и изолированной программной среды.
- Овладеть математическим аппаратом для разработки и анализа безопасности моделей управления доступом
- Овладеть навыками разработки и реализации механизмов управления доступом.

3. Место дисциплины в структуре образовательной программы

Дисциплина «Модели безопасности компьютерных систем» относится к обязательной части Блока 1 «Дисциплины», входит в модуль «Специализация».

Постреквизиты дисциплины: Защита в операционных системах, Безопасность веб-приложений.

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

Девятый семестр, зачет с оценкой

5. Входные требования для освоения дисциплины

Для освоения дисциплины необходимо знать основы дискретной математики и алгебры, иметь базовые представления об операционных системах и компьютерных сетях.

Пререквизиты дисциплины: Дискретная математика, Информатика, Операционные системы, Дискретная математика. Теория автоматов, Алгебра, Компьютерные сети

6. Язык реализации

Русский

7. Объем дисциплины

Общая трудоемкость дисциплины составляет 3 з.е., 108 часов, из которых:
-лекции: 32 ч.
-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. Основные элементы и виды управления доступом

Базовая терминология в области моделей контроля доступа. Субъекты и объекты, права доступа, информационные потоки. Политика, модель, правила и механизм управления доступом. Три аксиомы компьютерной безопасности. Дискреционная и мандатная политики.

Тема 2. Ролевая модель

Базовая ролевая модель контроля доступа. Иерархия ролей и критерии безопасности. Механизмы ограничений в ролевых моделях.

Тема 3. Take-Grant модель

Базовая Take-Grant модель. Де-юре правила, условия передачи прав доступа для графа доступов, включающего только субъекты. Условия передачи прав доступа для произвольного графа доступов в базовой модели take-grant (мосты и острова), условия похищения прав доступа. Расширенная Take-Grant модель. Скрытые (неявные) информационные потоки. Условия информационного потока в расширенной take-grant модели. Замыкание расширенной take-grant модели.

Тема 4. Модель изолированной программной среды и основы ДП моделей

Модель изолированной программной среды. МБО и МБС, Базовая теорема ИПС, Ядро безопасности и создание гарантированно защищенной КС. Основы ДП моделей. Формальное определение и основные элементы базовой ДП модели, условия передачи прав доступа. Мандатная ДП-модель и автоматные модели.

Тема 5. Модели Белла-ЛаПадулы и Биба

Модель Белла-ЛаПадулы, виды запросов. Свойства безопасности модели BLP (simple security-свойство, *-свойство, ds-свойство). Теоремы безопасности и их доказательства. Модель Low-Watermark. Модель целостности Биба.

Тема 6. Разработка механизмов управления доступом для современных компьютерных систем

Списки доступа. Решётки как механизм контроля доступа. Разграничение доступа на основе атрибутов. IBAC и её реализации, LBAC и MLS, TBAC.

9. Текущий контроль по дисциплине

Текущий контроль по дисциплине проводится путем решения задач на практических занятиях прохождения тестов в системе moodle, представления доклада, выполнения группового проекта и фиксируется в форме контрольной точки не менее одного раза в семестр.

Типовые задания и иные необходимые для текущего контроля материалы приведены в Приложении 1 к рабочей программе «Фонд оценочных средств».

10. Порядок проведения и критерии оценивания промежуточной аттестации

Промежуточная аттестация по дисциплине проводится в форме устного зачёта с оценкой по теоретическому материалу. Каждый билет для устного зачёта состоит из двух теоретических вопросов по двум темам дисциплины, а также сопровождается дополнительными вопросами по темам дисциплины.

Практическая подготовка оценивается по результатам выполненных практических работ.

Примеры вопросов к зачёту

Билет 1

1. Базовая терминология (сущность, объект, субъект, контейнер), доступы, информационные потоки по памяти и времени.
2. Свойства безопасности модели BLP (simple security-свойство, *-свойство, ds-свойство). Теоремы безопасности и их доказательства.

Билет 2

1. Три аксиомы компьютерной безопасности.
2. Замыкание расширенной take-grant модели.

Остальные вопросы и также критерии оценивания приведены в Приложении 1 к рабочей программе «Фонд оценочных средств»

Для допуска к устному зачёту с оценкой необходимо прохождение текущей аттестации, которая включает следующие пункты.

1. Выполнение группового проекта
2. Прохождение итогового теста в системе moodle. Тест считается пройденным, если обучающийся верно ответил на 70% вопросов или более. В случае неудачи – предоставляется дополнительная попытка.
3. Выступление с докладом

11. Учебно-методическое обеспечение

а) Электронный учебный курс по дисциплине в электронном университете «Moodle» - https://moodle.tsu.ru/course/view.php?id=9420

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

в) Самостоятельная работа студентов при изучении дисциплины предусмотрена в следующих видах и формах:

- изучение теоретического материала на основе курса лекций, предложенной литературы и учебно-методического обеспечения (перечень литературы проведён ниже);
- прохождение теста в системе moodle;
- подготовка доклада
- выполнение группового проекта.

12. Перечень учебной литературы и ресурсов сети Интернет

а) основная литература:

- Девянин, П. Н. Модели безопасности компьютерных систем. Управление доступом и информационными потоками: Учебное пособие для вузов / П.Н. Девянин. - Москва : Гор. линия-Телеком, 2012. – 320 с.
- Щербаков А.Ю. Современная компьютерная безопасность. Теоретические основы. Практические аспекты. Учебное пособие. – М.: Книжный мир, 2009. – 352 с.
- Bishop, M. Computer security: Art and science, 2002. – 1084 p.
- Гайдамакин Н.А. Теоретические основы компьютерной безопасности. Учебное пособие. Екатеринбург: изд-во Урал. Ун-та, 2008. – 212 с.

б) дополнительная литература:

- Девянин П. Н. Анализ безопасности управления доступом и информационными потоками в компьютерных системах. М.: Радио и связь, 2006. – 176 с.
- Богульская Н. Модели безопасности компьютерных систем : Учебное пособие / Сибирский федеральный университет. - Красноярск : Сибирский федеральный университет, 2019. - 206 с.
- Бондарев В. В. Введение в информационную безопасность автоматизированных систем : учебное пособие / Москва : Издательство МГТУ им. Н. Э. Баумана, 2021. - 250 с.

в) ресурсы сети Интернет:

- Электронная библиотека (репозиторий) ТГУ [Электронный ресурс] / Электронная библиотека (репозиторий) ТГУ : [сайт]. – [Томск, 2011–2016]. – URL: http://vital.lib.tsu.ru/vital/access/manager/Index.

- Владимир Кочетков. Философия Application Security. – URL: https://www.youtube.com/watch?v=mb7tcT-9VXk
- Maarten Decat. Access Control. – URL: https://www.youtube.com/watch?v=7e0fMbnovMc
- George Danezis. Access Control. – URL: https://www.youtube.com/watch?v=QaS_UBuPVWA
- Колегов Д.Н. Моделирование безопасности управления доступом и информационными потоками на основе ДП-моделей. – URL: https://vimeo.com/97906604

13. Перечень информационных технологий

а) лицензионное и свободно распространяемое программное обеспечение:

Программное обеспечение для показа презентаций с лекциями и докладами обучающихся (напр. Adobe Acrobat Reader или Microsoft PowerPoint или их аналоги). Проекты выполняются студентами с использованием свободно-распространяемого программного обеспечения.

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

Для реализации дисциплины необходимы лекционные аудитории и аудитории для проведения практических занятий. Проектор требуются для демонстрации материала в рамках изучаемых разделов, проведения защиты проектов в конце семестра и представления докладов.

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

Для совместной работы над групповым проектом рекомендуется использовать соответствующие информационные технологии (например, discord, github и их аналоги).

15. Информация о разработчиках

Твардовский Александр Сергеевич, канд. физ.-мат. наук, старший преподаватель кафедры компьютерной безопасности.