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

Институт прикладной математики и компьютерных наук

УТВЕРЖДАЮ:
Проректор по ОД

_____Е.В. Луков

«__» _____ 2025 г.

Рабочая программа дисциплины

Модели безопасности компьютерных систем

по направлению подготовки

10.03.01 Информационная безопасность

Направленность (профиль) подготовки:
Безопасность компьютерных систем

Форма обучения
Очная

Квалификация
Бакалавр

Год приема
2026

СОГЛАСОВАНО:
Руководитель ОП
В.Н. Тренькаев

Председатель УМК
С.П. Сущенко

Томск – 2025

1. Цель и планируемые результаты освоения дисциплины

Целью освоения дисциплины является формирование следующих компетенций:

ОПК-1.1. Способен разрабатывать и реализовывать политики управления доступом в компьютерных системах.

Результатами освоения дисциплины являются следующие индикаторы достижения компетенций:

ИОПК-1.1.1. Понимает основные формальные модели политик управления доступом в компьютерных системах.

ИОПК-1.1.2. Формулирует политики управления доступом в компьютерных системах с учетом угроз безопасности информации и требований по защите информации.

ИОПК-1.1.3. Демонстрирует навыки реализации политик управления доступом в компьютерных системах.

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 относится к Блоку 1 «Дисциплины (модули)».

Дисциплина относится к части образовательной программы, формируемой участниками образовательных отношений, предлагается обучающимся на выбор. Дисциплина входит в модуль «Специализация».

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

Шестой 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.

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 LMS IDO, представления доклада, выполнения группового проекта и фиксируется в форме контрольной точки не менее одного раза в семестр.

Практическая подготовка оценивается по результатам выполненных практических 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

Зачет с оценкой в шестом семестре проводится в устной форме по билетам. Билет состоит из двух теоретических вопросов по двум темам дисциплины, а также сопровождается дополнительными вопросами по темам дисциплины. Продолжительность зачета с оценкой 1 час.

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.

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

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

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 LMS IDO

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

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);

– 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).

Наименование оборудованных учебных кабинетов, объектов для проведения практических занятий, объектов физической культуры и спорта с перечнем основного оборудования	Адрес (местоположение) учебных кабинетов, объектов для проведения практических занятий, объектов физической культуры и спорта (с указанием площади и номера помещения в соответствии с документами бюро технической инвентаризации)
Учебная аудитория для проведения занятий	634050,Томская область, г. Томск, пр-т

лекционного и семинарского типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации. Аудитория № 118. Учебная мебель, оборудование, программное обеспечение: 45 столов по 2 места; 90 стульев; 1 интерактивная доска; Microsoft Windows 10, Microsoft Office 2010. (Лицензия №47729022 от 26.11.2010).	Ленина, 36, стр.7 (78 по паспорту БТИ) Площадь 61,1 м^2.
Учебная аудитория для проведения практических занятий и занятий семинарского типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации. Аудитория № 115. Учебная мебель, оборудование, программное обеспечение: 13 столов по 2 места; 26 стульев; 1 меловая доска; 1 интерактивная доска; 1 проектор; 1 системный блок (Intel Core i7-12700K, AsusTek B660M-K D4, 16Гб DDR4); 1 монитор; Microsoft Windows 10 Professional x64, Microsoft Office 2010 Standart, Dr.Web Desktop Security Suite, Aktru recorder, Aktru Meet, WinRar. (Лицензия №47729022 от 26.11.2010, договор №7193 от 14.10.2015, договор № 2016 от 16.04.2018).	634050,Томская область, г. Томск, пр-т Ленина, 36, стр.7 (29 по паспорту БТИ) Площадь 40,9 м^2.
Учебная аудитория для самостоятельной работы Аудитория № 103А. Учебная мебель, оборудование, программное обеспечение: 13 столов по 1 месту; 13 стульев; 1 меловая доска; 1 интерактивная доска; 1 проектор; 13 системных блоков (Intel Core i7-4790/Ga H97 HD 3/2x 8Gb DDR 3); 13 мониторов; Microsoft Windows 10 Professional x64, Microsoft Office 2010 Standart, Microsoft Office 2003 Professional (only for MS Access), Microsoft Visual Studio 2022 Community, Visual Studio Code, Dr.Web Desktop Security Suite, 1С:Предприятие учебная версия, 7-Zip, Adobe Reader, Android Studio, Far Manager, FreeCommander, Google Chrome, Яндекс Браузер, GPL Ghostscript, Gsview, IntelliJ IDEA Community Edition, Java SDK, Lazarus, Mathsoft Mathcad 13, 15, Mathsoft Prime 3.1, StatSoft Statistica 13, FreeMat, Scilab, NetBeans IDE 22, Eclipse IDE 2024, PyCharm Community 2024, R Project, RapidMiner Studio, Rstudio, Anaconda, JASP (Лицензия №47729022 от 26.11.2010, договор №7193 от 14.10.2015, договор № 2016 от 16.04.2018).	634050,Томская область, г. Томск, пр-т Ленина, 36, стр.7 (72 по паспорту БТИ) Площадь 43 м^2.

15. Информация о разработчиках

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