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

Методы и средства криптографической защиты информации

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
2025

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-10 Способен анализировать тенденции развития методов и средств криптографической защиты информации, использовать средства криптографической защиты информации при решении задач профессиональной деятельности.

ОПК-13 Способен разрабатывать компоненты программных и программно-аппаратных средств защиты информации в компьютерных системах и проводить анализ их безопасности.

ОПК-2 Способен применять программные средства системного и прикладного назначений, в том числе отечественного производства, для решения задач профессиональной деятельности.

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

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

Результатами освоения дисциплины являются следующие индикаторы достижения компетенций:

ИОПК-10.1 Осуществляет анализ тенденций развития методов и средств криптографической защиты информации

ИОПК-10.2 Применяет средства криптографической защиты информации при решении задач профессиональной деятельности

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-2.2 Определяет порядок настройки и эксплуатации программных средств системного и прикладного назначений, в том числе отечественного производства, используемых для решения задач профессиональной деятельности

ИОПК-2.3 Формулирует предложения по применению программных средств системного и прикладного назначений, в том числе отечественного производства, используемых для решения задач профессиональной деятельности

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

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

ИПК-2.3 Проводит исследования с целью нахождения наиболее целесообразных практических решений по обеспечению защиты информации

ИПК-3.2 Разработка проектов программных и аппаратных средств защиты информации в соответствии с техническим заданием

2. Задачи освоения дисциплины

– Сформировать у студентов способность анализировать тенденции развития методов и средств криптографической защиты информации, в частности дать представление о базовых понятиях и задачах криптографии, методах криптографического анализа, ознакомить с современными стандартами в области криптографии.

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

Седьмой семестр, экзамен
Восьмой семестр, экзамен

5. Входные требования для освоения дисциплины

Для успешного освоения дисциплины требуются результаты обучения по следующим дисциплинам: Языки программирования, Информатика, Введение в математику, Дискретная математика, Теория вероятностей и математическая статистика, Математическая логика и теория алгоритмов, Дискретная математика, Теория автоматов, Теория информации, Теория чисел, Общая алгебра, Теория вычислительной сложности, Профессиональный перевод специальной литературы.

6. Язык реализации

Русский

7. Объем дисциплины

Общая трудоемкость дисциплины составляет 10 з.е., 360 часов, из которых:
-лекции: 64 ч.
-лабораторные: 16 ч.
в том числе практическая подготовка: 16 ч.
-практические занятия: 48 ч.
в том числе практическая подготовка: 32 ч.
Объем самостоятельной работы студента определен учебным планом.

8. Содержание дисциплины, структурированное по темам

Тема 1. Введение в криптографию
Основные понятия и задачи криптографии.
Криптографический анализ. История криптографии.

Тема 2. Шифры замены и перестановки
Шифры замены. Криптоанализ шифров замены.
Шифры перестановки. Криптоанализ шифров перестановки.
Шифры замены и перестановки. Роторные шифры.

Тема 3. Абсолютно стойкие шифры
Вероятностная модель шифра по К.Шеннону.
Необходимые и достаточные условия абсолютной стойкости шифра.
Атака на основе шифртекста.

Тема 4. Блочные шифры
Принципы построения. Базовые операции. Сеть Фейстеля. SP-сеть.
Шифр DES. Шифр ГОСТ 28147-89 («Магма»). Шифр AES.
Упрощенные шифры DES и AES. Шифр «Кузнечик».

Тема 5. Поточные шифры

Схема поточного шифра. Генераторы псевдослучайных чисел.
Комбинирующий и фильтрующий генераторы. Шифр A5. Шифр RC4.
Тема 6. Ассиметричные шифры
Односторонняя функция с лазейкой. Шифр RSA.
Шифр Эль-Гамаля. Свойства шифра Эль-Гамаля.
Шифр Шамира. Атаки на RSA.

Тема 7. Цифровая подпись
Цифровая подпись RSA, Эль-Гамаля, DSS.
Атаки на цифровые подписи.
Инфраструктура открытых ключей.

Тема 8. Криптографические функции хеширования.
Имитовставка. Бесключевые и ключевые хэш-функции.
Конструкция Меркла-Дамгарда. Конструкция Губка. Стрибог.
SHA. MD4. HMAC. Атаки на хэш-функции.

Тема 9. Теория секретных систем Шеннона.
Алгебра секретных систем. Виды секретных систем.
Примеры секретных систем. Свойства секретных систем.

Тема 10. Методы криптоанализа.
Обзор методов криптоанализа. Линейный криптоанализ.
Дифференциальный криптоанализ. Слайдовая атака.
Корреляционная атака. Алгебраическая атака.
Атаки по побочным каналам.

Тема 11. Автоматная криптография.
Автоматы как компоненты криптосистем. Автоматные шифрсистемы.
Конечно-автоматная криптосистема с открытым ключом (FAPKC).
Поточные и автоматные шифрсистемы.

Тема 12. Средства криптографической защиты информации.
Обзор средств криптографической защиты информации.
Криптоконтейнеры. Криптопровайдеры. VPN-шлюзы.

9. Текущий контроль по дисциплине

Текущий контроль по дисциплине проводится путем контроля посещаемости, выполнения лабораторных работ/контрольных заданий и фиксируется в форме контрольной точки не менее одного раза в семестр.

Практическая подготовка оценивается по результатам выполненных практических и лабораторных работ.

Выполнение лабораторной работы/контрольного задания оценивается в 100 баллов:

0-20 Студент не разбирается в задаче, не знает методов решения, не отвечает, либо отвечает, но с грубыми ошибками на вопросы преподавателя.

21-40 Студент слабо разбирается в задаче, плохо знает методы решения, не отвечает, либо отвечает, но с ошибками на вопросы преподавателя.

41-60 Студент в целом удовлетворительно разбирается в задаче, использует методы решения при подсказке преподавателя, отвечает на вопросы неуверенно, но с негрубыми ошибками. Представляет работу на защите удовлетворительно.

61-80 Студент в целом уверенно разбирается в задаче, знает и использует методы решения практически самостоятельно, отвечает на вопросы с замечаниями. Представляет работу на защите в целом хорошо, с замечаниями.

81-100 Студент отлично разбирается в задаче, знает и использует методы решения самостоятельно, отвечает на вопросы уверенно. Представляет работу на защите отлично, уверенно.

Допуском до экзамена является выполнение 80% лабораторных работ/контрольных заданий, с оценкой за каждую не менее 50 баллов.

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 в седьмом и восьмом семестрах проводится в устной/письменной форме с использованием перечня контрольных вопросов/билетов по курсу. Схема вопросов экзамена соответствует компетентностной структуре дисциплины. Результаты экзамена определяются оценками «отлично», «хорошо», «удовлетворительно», «неудовлетворительно». Продолжительность экзамена 1,5 часа.

Критерии выставления оценок:

Отлично - студент в совершенстве овладел всеми теоретическими вопросами обязательного материала по разделам лекционного курса, показал все требуемые умения и навыки при выполнении заданий на лабораторных/практических занятиях.

Хорошо - студент овладел обязательным материалом по разделам лекционного курса, возможно с некоторыми недостатками, а также показал все требуемые умения и навыки при выполнении заданий на лабораторных/практических занятиях.

Удовлетворительно - студент имеет недостаточно глубокие знания по теоретическим разделам обязательного материала дисциплины, но показал все требуемые умения и навыки при выполнении заданий на лабораторных/практических занятиях.

Неудовлетворительно - студент имеет существенные пробелы по отдельным теоретическим разделам специальной дисциплины или не показал требуемые умения и навыки при выполнении заданий на лабораторных/практических занятиях.

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=8568

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

в) План практических занятий по дисциплине.

1. Разбор примеров и решение задач по теме шифры замены
2. Разбор примеров и решение задач по теме шифры перестановки.
3. Разбор примеров и решение задач по теме абсолютно стойкие шифры.
4. Разбор примеров и решение задач по теме блочные шифры.
5. Разбор примеров и решение задач по теме поточные шифры.
6. Разбор примеров и решение задач по теме ассиметричные шифры.
7. Разбор примеров и решение задач по теме цифровая подпись.
8. Разбор примеров и решение задач по теме криптографические функции хеширования.

г) Методические указания по проведению лабораторных работ.

Для выполнения лабораторной работы студенту необходимо:
1. Изучить методические указания по выполнению лабораторной работы.
2. Реализовать требуемый метод криптоанализа.
3. Прокомментировать преподавателю процесс вычислений.

г) Методические указания по организации самостоятельной работы студентов.

Самостоятельная работа организуется в следующих формах: работа со слайдами лекции; изучение вопросов, выносимых за рамки лекционных занятий; выполнение контрольных заданий; подготовка к лабораторным занятиям; подготовка к рубежному контролю по теме/разделу (аттестации). Работу со слайдами (конспектом) лекции целесообразно проводить непосредственно после ее прослушивания. Необходимым является глубокое освоение содержания лекции и свободное владение им, в том числе использованной в ней терминологии. Изучение вопросов, выносимых за рамки лекционных занятий, предполагает самостоятельное изучение студентами дополнительной литературы. Контрольные задания и лабораторные работы, приведенные в планах занятий, выполняются студентами в обязательном порядке. Методические указания обучающимся по освоению дисциплины: целенаправленно, систематически и планомерно работать со слайдами лекций; изучать рекомендуемую литературу, добывая новые/обобщая полученные знания; тратить не менее часа в день на самостоятельную работу; консультироваться с преподавателем при возникновении вопросов; активно использовать учебно-методический комплекс на базе Moodle ТГУ; работать с тематическими форумами в сети Интернет.

12. Перечень учебной литературы и ресурсов сети Интернет

а) основная литература:

– Запечников С.В., Казарин О.В., Тарасов А.А. Криптографические методы защиты информации - М.: Юрайт, 2016, 308 с.

– Лось А.Б. Криптографические методы защиты информации - М.: Юрайт,2018, 473 с.

– Рябко Б.Я., Фионов А.Н. Криптографические методы защиты информации - М.: Горячая Линия – Телеком, 2014, 229 с.

– Фомичёв В.М., Мельников Д.А. Криптографические методы защиты информации -М.: Юрайт , 2017, 209 с.

– Бабаш А.В. Криптографические методы защиты информации-М.: РИОР,2019, 413 с.

б) дополнительная литература:

– Алферов А.П., Зубов А.Ю., Кузьмин А.С., Черемушкин А.В. Основы криптографии. Учебное пособие. - М.: Гелиос АРВ, 2002, 480 с.

– Бабенко Л.К., Ищукова Е.А. Современные алгоритмы блочного шифрования и методы их анализа -М.: Гелиос АРВ, 2006, 376 с.

– Агибалов Г.П. Конечные автоматы в криптографии // Прикладная дискретная математика, 2009, Приложение № 2, С. 43–73

– Агибалов Г.П. Избранные теоремы начального курса криптографии - Томск: НТЛ, 2005, 116 с.

– Венбо Мао Современная криптография: теория и практика - М.: Вильямс, 2005, 768 с.

– Шнайер Брюс Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си - М.: Триумф, 2002, 816 с.

– Кузьминов Т.В. Криптографические методы защиты информации - Новосибирск: Наука, 1998, 194 с.

в) ресурсы сети Интернет:

– Курс "Основы криптографии" [Электронный ресурс] // Национальный Открытый Университет "ИНТУИТ". URL: http://www.intuit.ru/studies/courses/691/547/info

– Курс "Математика криптографии и теория шифрования» [Электронный ресурс] // Национальный Открытый Университет "ИНТУИТ". URL: http://www.intuit.ru/studies/courses/552/408/info

– Курс "Криптографические основы безопасности" [Электронный ресурс] // Национальный Открытый Университет "ИНТУИТ". URL: http://www.intuit.ru/studies/courses/28/28/info

13. Перечень информационных технологий

а) лицензионное и свободно распространяемое программное обеспечение:
– ОС Windows/Linux, браузер Firefox/Яндекс
– публично доступные облачные технологии (Google Docs, Яндекс диск и т.п.).
– бесплатная интегрированная среда разработки для Python/C++
– криптопровайдер КриптоПро CSP
– USB-токен JaCarta

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 практических и лабораторных занятий, а также занятий лекционного 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

Тренькаев Вадим Николаевич, канд. техн. наук, доцент, доцент кафедры компьютерной безопасности