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 20 23 г.

Рабочая программа дисциплины

Аппаратная реализация криптоалгоритмов

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.В.04.02

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-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.

– 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.

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

2. Задачи освоения дисциплины

- Сформировать компетенции в области проектирования, применения и анализа безопасности программно-аппаратных средств криптографической защиты информации: 1) сформировать навыки использования инструментов автоматизированного проектирования цифровых устройств на основе программируемых логических интегральных схем; 2) сформировать навыки использования языка VHDL при проектировании средств защиты информации и аппаратной реализации криптографических алгоритмов.

3. Место дисциплины в структуре образовательной программы

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

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

Девятый семестр, зачет с оценкой

5. Входные требования для освоения дисциплины

Для успешного освоения дисциплины требуются результаты обучения по следующим дисциплинам: Дискретная математика, Теория автоматов, Электроника и схемотехника, Методы и средства криптографической защиты информации.

6. Язык реализации

Русский

7. Объем дисциплины

Общая трудоемкость дисциплины составляет 3 з.е., 108 часов, из которых:
-лекции: 32 ч.
-лабораторные: 32 ч.
в том числе практическая подготовка: 32 ч.
Объем самостоятельной работы студента определен учебным планом.

8. Содержание дисциплины, структурированное по темам

Тема 1. Основы технологии ПЛИС
- Классификация и архитектура ПЛИС.
- Производители и области применения ПЛИС.
- Обзор характеристик ПЛИС разных производителей.

Тема 2. Основы проектирования цифровых устройств
- Базовые элементы цифровых устройств
- Проектирование комбинационных схем.
- Проектирование последовательных схем.
- Реализация конечных автоматов на ПЛИС

Тема 3. Язык описания аппаратуры VHDL
- Структурное и поведенческое описание цифрового устройства.
- Интерфейс и архитектура. Операторы. Функции. Процедуры.
- Последовательные операторы.
- Параллельные операторы.
- Оптимизация параметров проекта.

Тема 4. САПР Xilinx WebPack ISE
- Создание проекта.
- Поведенческое описание проекта.
- Структурное описание проекта.
- Функциональное моделирование проекта.

Тема 5. Криптография на ПЛИС
- Основы аппаратной реализации блочных и поточных шифров
- Аппаратная реализации элементов блочных и поточных шифров на ПЛИС
- Архитектура криптографического сопроцессора на ПЛИС.

Тема 6. Средства защиты информации на ПЛИС
- Доверенная загрузка ОС на базе ПЛИС. Электронные замки.
- Защита информации на базе аппаратных шифраторов

9. Текущий контроль по дисциплине

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

Практическая подготовка оценивается по результатам выполненных лабораторных работ.

Типовые варианты заданий для лабораторных работ:

1. Основы работы в САПР WebPack ISE. Изучить этапы проектирования цифровых устройств на базе ПЛИС и возможности пользовательского интерфейса САПР WebPack ISE.
2. Реализация на ПЛИС компонент современных блочных шифров. Отработать навыки структурного (в виде логической схемы) и поведенческого (на языке VHDL) описания компонент современных блочных шифров: P-блоков, S-блоков и др., а также отработать навыки функционального моделирования проектов в САПР WebPack ISE.
3. Реализация на ПЛИС компонент современных поточных шифров. Изучить основы проектирования поточных шифров на базе регистров сдвига с линейной обратной связью, отработать навыки структурного и поведенческого описания компонент современных поточных шифров
4. Разработка аппаратного антивируса на базе циклического избыточного кода. Получить навыки проектирования аппаратных средств защиты информации, отработать навыки описания и моделирования проектов в САПР WebPack ISE.
5. Реализация на ПЛИС автоматного шифратора. Изучить основные понятия теории автоматных шифров, способы описания цифровых автоматов на языке VHDL, способы кодирования состояний цифрового автомата, получить навыки проектирования цифровых автоматов, отработать навыки описания и моделирования проектов в САПР WebPack ISE.

Типовые контрольные задания для текущего контроля:

1. Архитектура ПЛИС. Выбрать ПЛИС конкретного производителя и конкретного семейства (линейки). Используя предоставленные источники информации (сайты производителей ПЛИС, обзорные статьи и др.), изучить архитектуру и характеристики ПЛИС, написать мини-реферат и “защитить” его преподавателю.
2. Синтез устройства управления кофе-машиной. Описать на неформальном языке поведение устройства управления кофе-машиной, которая выдает два/три вида напитков (кофе, чай, квас) разной стоимости, затем построить модель устройства на основе конечного автомата, далее синтезировать структурный автомат кофе-машины и “защитить” проект.
3. Современные исследования в области аппаратных реализаций криптографических алгоритмов. Используя предоставленный банк научных статей, выбрать несколько статей по интересующей тематике, изучить и провести критический анализ материала, разработать презентацию доклада, выступить с докладом, ответить на вопросы, выслушать и оценить выступления других участников научного семинара.

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 зачета с оценкой является выполнение 80% лабораторных работ и контрольных заданий, с оценкой за каждую не менее 55 баллов.

10. Порядок проведения и критерии оценивания промежуточной аттестации

Промежуточная аттестация осуществляется на основе выполнения контрольных заданий и лабораторных работ, а также по результатам ответов студента в устной/письменной форме на несколько контрольных вопросов по всему курсу.

Примерный перечень вопросов к зачету с оценкой:

1. Общие сведения об интегральных схемах.
2. Предшественники микросхем программируемой логики.
3. Простые программируемые логические устройства.
4. Сложные программируемые логические устройства.
5. Классификация интегральных схем программируемой логики.
6. Архитектура ПЛИС.
7. Конфигурируемый логический блок
8. Общие сведения о проектировании комбинационных схем.
9. Общие сведения о проектировании последовательных схем.
10. Типовые функциональные узлы цифровых устройств.
11. Этапы разработки цифровых устройств на ПЛИС.
12. Основные производители ПЛИС (базовые характеристики).
13. Области применения ПЛИС.
14. Язык VHDL. Структурное описание цифрового устройства.
15. Язык VHDL. Поведенческое описание цифрового устройства.
16. Язык VHDL. Типы данных.
17. Язык VHDL. Интерфейс и архитектура объекта.
18. Язык VHDL. Понятие сигнала.
19. Язык VHDL. Последовательные операторы.
20. Язык VHDL. Параллельные операторы.
21. Язык VHDL. Функции.
22. Язык VHDL. Процедуры.
23. Язык VHDL. Компоненты.
24. САПР Xilinx WebPack ISE. Создание проекта.
25. САПР Xilinx WebPack ISE. Поведенческое описание проекта.
26. САПР Xilinx WebPack ISE. Структурное описание проекта.
27. САПР Xilinx WebPack ISE. Функциональное моделирование проекта.
28. Достоинства и недостатки аппаратной реализация криптографических алгоритмов.
29. Основы аппаратной реализации шифров на примере DES.
30. Аппаратная реализация поточных шифров на базе LFRS.

31. Аппаратные шифраторы и электронные замки.
32. Отечественные аппаратные средства защиты информации.

Результаты зачета с оценкой определяются оценками «отлично», «хорошо», «удовлетворительно», «неудовлетворительно». 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 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 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 занятиях.

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

11. Учебно-методическое обеспечение

а) Электронный учебный курс по дисциплине в электронном университете «Moodle» - https://moodle.tsu.ru/course/view.php?id=1444

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

в) Семинарских / практических занятий по дисциплине нет.

г) Методические указания по проведению лабораторных работ.

Для выполнения лабораторной работы необходимо:

1. Изучить методические указания по выполнению лабораторной работы.
2. Реализовать на ПЛИС необходимый компонент современного шифра.
3. Прокомментировать преподавателю описание компонента на языке VHDL.

д) 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.

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.

12. Перечень учебной литературы и ресурсов сети Интернет

а) основная литература:

– Пухальский Г.И., Новосельцева Т.Я. Проектирование цифровых устройств: учебное пособие. - Санкт-Петербург: Лань, 2021, 896 с.

– Бибило П.Н. Основы языка VHDL: Учебное пособие, М.: СОЛОН-Р, 2016 , 200 с.

– Соловьев В.В. Архитектуры ПЛИС фирмы Xilinx: CPLD и FPGA 7-й серии. - М.: Горячая линия – Телеком, 2016, 392 с.

– Кнышев Д. А., Кузелин М. О. ПЛИС фирмы Xilinx. Описание структуры основных семейств.- М.: ДМК Пресс, 2017, 238 с.

б) дополнительная литература:

– Тарасов И.Е. Разработка цифровых устройств на основе ПЛИС Xilinx с применением языка VHDL.-М.: Горячая линия – Телеком, 2005, 253 с.

– Угрюмов Е.П. Цифровая схемотехника: учеб. пособие для вузов.-СПб.: БХВ-Петербург, 2010, 800 с.

– Поляков А.К. Языки VHDL и VERILOG в проектировании цифровой аппаратуры.- М.: СОЛОН-Пресс, 2003, 305 с.

– T. Huffmire et al. Handbook of FPGA Design Security.-Springer, 2010, 177 с.

– Клайв Максфилд Проектирование на ПЛИС. Архитектура, средства и методы. Курс молодого бойца.-М.: ДМК Пресс, 2015, 408 с.

– Дэвида М. Харрис и Сары Л. Харрис Цифровая схемотехника и архитектура компьютера.- М.:ДМК Пресс, 2018, 792 с.

– Панасенко С.П. Алгоритмы шифрования. Специальный справочник.-СПб.: БХВ-Петербург, 2009, 576 с.

в) ресурсы сети Интернет:

– Курс "Введение в цифровую схемотехнику" [Электронный ресурс] // Национальный Открытый Университет "ИНТУИТ"
URL: http://www.intuit.ru/studies/courses/104/104/info

– Тренькаев В. Н. Аппаратная реализация криптографических алгоритмов : учебно-методический комплекс : [для студентов высших учебных заведений, обучающихся по направлению 10.05.01 «Компьютерная безопасность»] / Тренькаев В. Н. ; Том. гос. ун-т, [Ин-т дистанционного образования]. - Томск : [ИДО ТГУ], 2015. URL: http://vital.lib.tsu.ru/vital/access/manager/Repository/vtls:000516087

– Пономарев О.Г. Плис-технологии в радиофизике : лабораторный практикум / Пономарев О.Г. ; Том. гос. ун-т, Радиофиз. фак. - Томск : [б. и.], 2011. URL: http://vital.lib.tsu.ru/vital/access/manager/Repository/vtls:000421575

– Буркатовская Л.И. Логическое проектирование дискретных устройств : учебное пособие : [для студентов, изучающих историю автоматов] / Л.И. Буркатовская, Ю.Б. Буркатовская ; Том. гос. ун-т, Фак. прикладной мат. и кибернетики. - Томск : Том. гос. ун-т, 2011. URL: http://vital.lib.tsu.ru/vital/access/manager/Repository/vtls:000418985

13. Перечень информационных технологий

а) лицензионное и свободно распространяемое программное обеспечение:

– Операционная система Windows/Linux

– Браузер Firefox/Яндекс

– САПР ISE Xilinx ISE WebPACK.

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, лабораторных занятий, 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