МИНОБРНАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ
НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ
ТОМСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

Институт прикладной математики и компьютерных наук

УТВЕРЖДАЮ
Директор института прикладной
математики и компьютерных наук
_____ А.В. Замятин
«_02_» _____июля_____ 2021 г.

Аппаратная реализация криптоалгоритмов

рабочая программа дисциплины

Закреплена за кафедрой	*компьютерной безопасности*
Учебный план	*10.05.01 Компьютерная безопасность,* *профиль «Анализ безопасности компьютерных систем»*
Форма обучения	*очная*
Общая трудоёмкость	*3 з.е.*
Часов по учебному плану	*108*
в том числе:	
аудиторная контактная работа	*69,45*
самостоятельная работа	*38,55*
Вид(ы) контроля в семестрах *экзамен/зачет/зачет с оценкой*	*Семестр 9 – зачет с оценкой*

Томск-2021

Программу составил:
канд. техн. наук,
доцент кафедры компьютерной безопасности В.Н. Тренькаев

Рецензент:
канд. техн. наук,
заведующий кафедрой компьютерной безопасности С.А.Останин

Рабочая программа дисциплины «Аппаратная реализация криптоалгоритмов» разработана в соответствии с образовательным стандартом высшего образования – специалитет, самостоятельно устанавливаемым федеральным государственным автономным образовательным учреждением высшего образования «Национальный исследовательский Томский государственный университет» по специальности 10.05.01 Компьютерная безопасность (Утвержден Ученым советом НИ ТГУ, протокол от 30.06.2021 г. № 06).

Рабочая программа одобрена на заседании кафедры компьютерной безопасности

Протокол от 02 июня 2021 г. № 06

Заведующий кафедрой компьютерной безопасности,
канд. техн. наук, доцент С.А. Останин

Рабочая программа одобрена на заседании учебно-методической комиссии института прикладной математики и компьютерных наук (УМК ИПМКН)

Протокол от 17 июня 2021 г. № 05

Председатель УМК ИПМКН,
д-р техн. наук, профессор С.П. Сущенко

Цель освоения дисциплины – формирование у студентов компетенций в области проектирования, применения и анализа безопасности программно-аппаратных средств криптографической защиты информации

1. Место дисциплины в структуре ОПОП

Дисциплина «Аппаратная реализация криптоалгоритмов» относится к части, формируемой участниками образовательных отношений Блока 1 «Дисциплины», входит в модуль «Специализация».

Для освоения дисциплины необходимо знать основы теории булевых функций и структурной теории автоматов, элементы схемотехники, современные криптографические стандарты.

Пререквизиты дисциплины: Дискретная математика, Теория автоматов, Электроника и схемотехника, Методы и средства криптографической защиты информации

Постреквизиты дисциплины: Методы верификации, Криптографические протоколы, Производственная практика

2. Компетенции и результаты обучения, формируемые в результате освоения дисциплины

Таблица 1.

Компетенция	**Индикатор компетенции**	**Код и наименование результатов обучения** (планируемые результаты обучения по дисциплине, характеризующие этапы формирования компетенций)
ОПК-10. Способен анализировать тенденции развития методов и средств криптографической защиты информации, использовать средства криптографической защиты информации при решении задач профессиональной деятельности	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.	ОР-10.1.1 **Знать:** основы проектирования средств криптографической защиты информации на базе технологии ПЛИС. ОР-10.2.1 **Уметь**: применять средства криптографической защиты информации, разработанные на базе ПЛИС.
ОПК-13. Способен разрабатывать компоненты программных и программно-аппаратных средств защиты информации в компьютерных системах и проводить анализ их безопасности	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	ОР-13.1.1 **Знать:** этапы проектирования цифровых устройств на базе ПЛИС. ОР-13.2.1 **Уметь**: применять САПР при проектировании программно-аппаратных средств защиты информации. ОР-13.3.1 **Уметь**: проводить анализ компонент программно-аппаратных средств защиты информации на базе ПЛИС с целью определения уровня обеспечиваемой ими защищенности и доверия.

	определения уровня обеспечиваемой ими защищенности и доверия.	
ПК-3. Способен проектировать программно-аппаратные средств защиты информации компьютерных систем и сетей	ИПК-3.2 Разработка проектов программных и аппаратных средств защиты информации в соответствии с техническим заданием	ОР-3.2.1 **Владеть:** навыками использования языка описания аппаратуры VHDL при проектировании программно-аппаратных средств защиты информации

3. Структура и содержание дисциплины

3.1. Структура и трудоемкость видов учебной работы по дисциплине

Общая трудоемкость дисциплины составляет 3 зачетных единицы, 108 часов.

Таблица 2.

Вид учебной работы	Трудоемкость в академических часах	
	9 семестр	всего
Общая трудоемкость	108	108
Контактная работа:	69,45	69,45
Лекции (Л):	32	32
Практики (ПЗ)		
Лабораторные работы (ЛР)	32	32
Семинары (СЗ)		
Групповые консультации	2	2
Индивидуальные консультации	3,2	3,2
Промежуточная аттестация	0,25	0,25
Самостоятельная работа обучающегося:	38,55	38,55
- выполнение контрольных заданий	6,8	6,8
- подготовка к лабораторным занятиям	14	14
- прохождение тестирования	2	2
- подготовка к рубежному контролю по теме/разделу	15,75	15,75
Вид промежуточной аттестации (зачет, зачет с оценкой, экзамен)	**Зачет с оценкой**	**Зачет с оценкой**

3.2. Содержание и трудоемкость разделов дисциплины

Таблица 3.

Код занятия	Наименование разделов и тем и их содержание	Вид учебной работы, занятий, контроля	Семестр	Часы в электронной форме	Всего (час.)	Литература	Код (ы) результата(ов) обучения
	Раздел 1. Основы технологии ПЛИС		9		**10**	3,4,5,9	ОР-10.1.1
1.1.	Классификация и архитектура ПЛИС.	Лекции	9		4		
1.2.	Производители и области применения ПЛИС.	ЛР	9		4		
1.3.	Обзор характеристик ПЛИС компания Xilinx.	СРС	9		2		
	Раздел 2. Основы проектирования цифровых устройств		9		**12**	1,6,10	ОР-13.1.1
2.1.	Проектирование комбинационных и последовательных схем.	Лекция	9		4		
2.2.	Примеры проектирования комбинационных и последовательных схем.	ЛР	9		4		
2.3.	Реализация конечных автоматов на ПЛИС	СРС	9		4		
	Раздел 3. Язык описания аппаратуры VHDL		9		**20**	2,7	ОР-2.3.1
3.1.	Структурное и поведенческое описание цифрового устройства.	Лекция	9		4		
3.2.	Интерфейс и архитектура. Операторы. Функции. Процедуры.	Лекция	9		4		
3.3.	Последовательные операторы.	ЛР	9		4		
3.4.	Параллельные операторы.	ЛР	9		4		
3.5.	Оптимизация параметров проекта.	СРС	9		4		
	Раздел 4. САПР Xilinx WebPack ISE		9		**12**	5	ОР-13.2.1
4.1.	Этапы разработки цифрового устройства в САПР Xilinx WebPack ISE.	Лекции	9		4		
4.2.	Этапы разработки цифрового устройства в САПР Xilinx WebPack ISE.	ЛР	9		4		
4.3.	Испытательный стенд (test bench).	СРС	9		4		
	Раздел 5. Криптография на ПЛИС		9		**20**	8,11	ОР-10.1.1, ОР-2.3.1
5.1.	Основы аппаратной реализации блочных и поточных шифров	Лекции	9		8		
5.2.	Аппаратная реализации элементов блочных и поточных шифров	ЛР	9		8		
5.3.	Архитектура криптографического сопроцессора на ПЛИС.	СРС	9		4		
	Раздел 6. Средства защиты информации на ПЛИС		9		**12,8**	8	ОР-10.2.1, ОР-13.3.1
6.1.	Доверенная загрузка ОС на базе ПЛИС. Электронные замки.	Лекции	9		4		
6.2.	Аппаратный антивирус и аппаратные шифратор	ЛР	9		4		
6.3.	Комплексная защита информации на базе аппаратных шифраторов	СРС	9		4,8		

	Подготовка к промежуточной аттестации в форме зачета с оценкой	СРС	**9**		**15,75**	1-11	
	Прохождение промежуточной аттестации в форме зачета с оценкой	Э	**9**		**2,25**		

4. Образовательные технологии, учебно-методическое и информационное обеспечение для освоения дисциплины

Образовательная технология – посещение студентом последовательности из набора лекций по разным темам дисциплины с последующим выполнением лабораторных работ и контрольных заданий по пройденным темам. Самостоятельная работа студентов включает выполнение контрольных заданий, подготовку к лабораторным занятиям, прохождение тестов, подготовку к рубежному контролю по разделу. Учебно-методическое обеспечение включает: список основной и дополнительной учебной литературы, список информационные ресурсов в сети Интернет, базу данных статей по вопросам аппаратной реализации криптографических алгоритмов, слайды лекционных занятий, перечень контрольных заданий, методические рекомендации по выполнению лабораторных работ. Промежуточная аттестация осуществляется на основе выполнения контрольных заданий и лабораторных работ, а также по результатам собеседования с использованием перечня контрольных вопросов по курсу.

Типовые контрольные задания или иные материалы, необходимые для оценки результатов обучения, характеризующих этапы формирования компетенций, и методические материалы, определяющие процедуры оценивания результатов обучения, приведены в Приложении 1 к рабочей программе «Фонд оценочных средств».

Типовые контрольные задания или иные материалы, необходимые для текущей аттестации, и методические материалы, определяющие процедуры оценивания результатов текущей аттестации, приведены в Приложении 2 к рабочей программе «Примерные оценочные средства текущей аттестации».

4.1. Рекомендуемая литература и учебно-методическое обеспечение

№ п/п	Авторы / составители	Заглавие	Издательство	Год издания, количество страниц
Основная литература				
1.	Пухальский Г. И., Новосельцева Т. Я.	Проектирование цифровых устройств: учебное пособие	Санкт-Петербург: Лань	2021 г., 896 с.
2.	Бибило П.Н.	Основы языка VHDL: Учебное пособие	М.: СОЛОН-Р	2016 г., 200 с.
3.	Соловьев В.В.	Архитектуры ПЛИС фирмы Xilinx: CPLD и FPGA 7-й серии	М.: Горячая линия - Телеком	2016 г., 392 с.
4.	Кнышев Д. А., Кузелин М. О.	ПЛИС фирмы Xilinx. Описание структуры основных семейств	М.: ДМК Пресс	2017 г., 238 с.
Дополнительная литература				
5.	Тарасов И.Е.	Разработка цифровых устройств на основе ПЛИС Xilinx с применением языка VHDL	М.: Горячая линия - Телеком	2005 г., 253 с.
6.	Угрюмов Е.П.	Цифровая схемотехника: учеб. пособие для вузов	СПб.: БХВ-Петербург	2010 г., 800 с.
7.	Поляков А.К.	Языки VHDL и VERILOG в проектировании цифровой аппаратуры	М.: СОЛОН-Пресс	2003 г., 305 с.
8.	T. Huffmire et al.	Handbook of FPGA Design	Springer	2010 г., 177 с.

		Security		
9.	Клайв Максфилд	Проектирование на ПЛИС. Архитектура, средства и методы. Курс молодого бойца	М.:ДМК Пресс	2015 г., 408 с.
10.	Дэвида М. Харрис и Сары Л. Харрис	Цифровая схемотехника и архитектура компьютера	М.:ДМК Пресс	2018 г., 792 с.
11.	Панасенко С.П.	Алгоритмы шифрования. Специальный справочник	СПб.: БХВ-Петербург	2009 г., 576 с.

4.2. Базы данных и информационно-справочные системы, в том числе зарубежные

1. 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

2. 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

3. 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

4.3. Перечень лицензионного и программного обеспечения

Операционная система Windows/Linux, Браузер Firefox/Яндекс, САПР ISE Xilinx ISE WebPACK.

4.4. Оборудование и технические средства обучения

Для реализации дисциплины необходимы лекционная аудитория и аудитория для проведения лабораторных занятий. Специальные технические средства (проектор, компьютер и т.д.) требуются для демонстрации материала в рамках изучаемых разделов и проведения лабораторных работ (отладочная плата). Вся основная и дополнительная литература, необходимая для самостоятельной работы и подготовки к экзамену, имеется в научной библиотеке ТГУ.

5. 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.

6. Преподавательский состав, реализующий дисциплину

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

7. Язык преподавания – русский язык.