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_» _июня_ 2021 г.

Фонд оценочных средств по дисциплине

Аппаратная реализация криптоалгоритмов

Специальность
10.05.01 Компьютерная безопасность
код и наименование специальности

Анализ безопасности компьютерных систем
наименование специализации

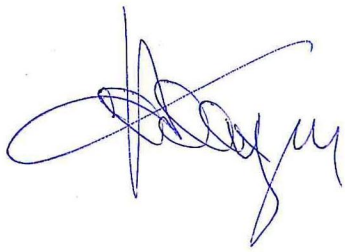
Томск–2021

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

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

Фонд оценочных средств одобрен 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

Фонд оценочных средств (ФОС) является элементом системы оценивания сформированности компетенций у обучающихся в целом или на определенном этапе ее формирования.

ФОС разрабатывается в соответствии с рабочей программой (РП) дисциплины и включает в себя набор оценочных материалов для проведения текущего контроля успеваемости и промежуточной аттестации по дисциплине.

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

Компетенция	**Индикатор компетенции**	**Код и наименование результатов обучения** (планируемые результаты обучения, характеризующие этапы формирования компетенций)	**Критерии оценивания результатов обучения**			
			Отлично	Хорошо	Удовлетворительно	Неудовлетворительно
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.	Высокий уровень знаний и умений; способность самостоятельного анализа проблем предметной области.	В целом успешные, но содержащие отдельные пробелы знания и умения.	Фрагментарные, неполные знания и умения без грубых ошибок.	Не имеет четкого представления об изучаемом материале, допускает грубые ошибки.
ОПК-13. Способен разрабатывать компоненты программных и программно-аппаратных средств защиты информации в	ИОПК-13.1 Предпринимает необходимые действия по сбору и анализу исходных данных для проектирования компонент программных и программно-аппаратных	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.	Высокий уровень знаний и умений; способность самостоятельного анализа проблем предметной области.	В целом успешные, но содержащие отдельные пробелы знания и умения.	Фрагментарные, неполные знания и умения без грубых ошибок.	Не имеет четкого представления об изучаемом материале, допускает грубые ошибки.

компьютерных системах и проводить анализ их безопасности	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.	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.				
ПК-2. Способен проектировать и разрабатывать средства защиты информации компьютерных систем и сетей.	ИПК-2.3 Осуществляет разработку требований, проектирует и разрабатывает средства защиты информации в соответствии с техническим заданием	ОР-2.3.1 Владеть: навыками использования языка описания аппаратуры VHDL при проектировании программно-аппаратных средств защиты информации	Высокий уровень владения навыками использования языка описания аппаратуры VHDL при проектировании программно-аппаратных средств защиты информации.	В целом успешные, но содержащие отдельные пробелы навыки использования языка описания аппаратуры VHDL при проектировании программно-	Фрагментарные, неполные, но без грубых ошибок навыки использования языка описания аппаратуры VHDL при проектировании программно-аппаратных средств защиты	Фрагментарные, неполные, с грубыми ошибками навыки использования языка описания аппаратуры VHDL при проектировании программно-аппаратных средств защиты информации умения использовать

				аппаратных средств защиты информации.	информации.	

2. Этапы формирования компетенций и виды оценочных средств

№	Этапы формирования компетенций (разделы дисциплины)	Код и наименование результатов обучения	Вид оценочного средства (тесты, задания, кейсы, вопросы и др.)
1.	Основы технологии ПЛИС	ОР-10.1.1 Знать: основы проектирования средств криптографической защиты информации на базе технологии ПЛИС.	лабораторные работы, контрольные задания, тесты, опросы на занятиях.
2.	Основы проектирования цифровых устройств	ОР-13.1.1 Знать: этапы проектирования цифровых устройств на базе ПЛИС.	лабораторные работы, контрольные задания, тесты, опросы на занятиях.
3.	Язык описания аппаратуры VHDL	ОР-2.3.1 Владеть: навыками использования языка описания аппаратуры VHDL при проектировании программно-аппаратных средств защиты информации	лабораторные работы, контрольные задания, тесты, опросы на занятиях.
4.	САПР Xilinx WebPack ISE	ОР-13.2.1 Уметь: применять САПР при проектировании программно-аппаратных средств защиты информации.	лабораторные работы, контрольные задания, тесты, опросы на занятиях.
5.	Криптография на ПЛИС	ОР-10.1.1 Знать: основы проектирования средств криптографической защиты информации на базе технологии ПЛИС. ОР-2.3.1 Владеть: навыками использования языка описания аппаратуры VHDL при проектировании программно-аппаратных средств защиты информации	лабораторные работы, контрольные задания, тесты, опросы на занятиях.
6.	Средства защиты информации на ПЛИС	ОР-10.2.1 Уметь: применять средства криптографической защиты информации, разработанные на базе ПЛИС. 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.	лабораторные работы, контрольные задания, тесты, опросы на занятиях.

3. Типовые контрольные задания или иные материалы, необходимые для оценки образовательных результатов обучения

3.1. Типовые задания для проведения текущего контроля успеваемости по дисциплине

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.

3.2. Типовые задания для проведения промежуточной аттестации по дисциплине

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.

4. Методические материалы, определяющие процедуры оценивания образовательных результатов обучения

4.1. Методические материалы для оценки текущего контроля успеваемости по дисциплине.

Текущий контроль подразумевает выполнение лабораторных работ/контрольных заданий. 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 80 баллов.

4.2. Методические материалы для проведения промежуточной аттестации по дисциплине.

Промежуточный контроль знаний по дисциплине осуществляется в форме зачета с оценкой, который подразумевает подготовку студента и ответов в устной/письменной форме на несколько контрольных вопросов по всему курсу. 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.