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

Оценочные материалы по дисциплине

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
2025

СОГЛАСОВАНО:
Руководитель ОП
В.Н. Тренькаев

Председатель УМК
С.П. Сущенко

Томск – 2025

1. Компетенции и индикаторы их достижения, проверяемые данными оценочными материалами

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. Оценочные материалы текущего контроля и критерии оценивания

Элементы текущего контроля:
– контрольные задания;
– лабораторные работы.

Текущий контроль по дисциплине проводится путем контроля посещаемости, проведения лабораторных работ, выполнения контрольных заданий по изученному лекционному материалу.

При оценивании необходимо продемонстрировать достижение всех запланированных индикаторов достижения компетенций: ИОПК-10.1, ИОПК-10.2, ИОПК-13.1, ИОПК-13.2, ИОПК-13.3, ИПК-3.2.

Типовые варианты заданий для лабораторных работ:

1. Лабораторная работа Основы работы в САПР (WebPack ISE, Gowin EDA Education, Icarus Verilog, GTKWave). Цель - изучить этапы проектирования цифровых устройств на базе ПЛИС и возможности пользовательского интерфейса САПР. Задание: изучить этапы проектирования цифровых устройств на базе ПЛИС, реализуя малый проект на базе свободно распространяемой САПР.
2. Лабораторная работа Реализация на ПЛИС компонент современных блочных шифров. Цель - отработать навыки структурного и поведенческого HDL-описания компонент современных блочных шифров: P-блок, S-блок и др., а также отработать

навыки функционального моделирования проектов цифровых схем. Задание 1. Синтезировать упрощенный вариант S-блока (блок замены) с одним управляющим входом, двумя информационными входами и двумя информационными выходами в базисе И, ИЛИ, НЕ. Промоделировать разработанный S-блок, заданный на языке описания аппаратуры. Задание 2. Синтезировать упрощенный вариант S-блока без управляющего входа, но с тремя информационными входами и тремя информационными выходами на базе шифратора и дешифратора. Промоделировать разработанный S-блок, заданный в виде логической схемы. Задание 3. Синтезировать упрощенный вариант P-блока (блока перестановки) с четырьмя входными и выходными сигналами. Промоделировать проект P-блока, заданный с помощью языка описания аппаратуры.

3. Лабораторная работа Реализация на ПЛИС компонент современных поточных шифров. Цель - изучить основы проектирования поточных шифров на базе регистров сдвига с линейной обратной связью, отработать навыки структурного и поведенческого описания компонент современных поточных шифров, в частности генератора псевдослучайной последовательности. Задание: разработать упрощенный вариант поточного шифратора на базе регистра сдвига с линейной обратной связью длины четыре и произвольной функцией обратной связи, провести описание проекта шифратора на структурном и поведенческом уровне, промоделировать проекты шифратора.
4. Лабораторная работа Разработка аппаратного антивируса на базе циклического избыточного кода. Цель - получить навыки проектирования аппаратных средств защиты информации, отработать навыки описания и моделирования проектов цифровых устройств. Задание: разработать упрощенный вариант аппаратного антивируса на базе циклического избыточного кода с использованием регистра сдвига с линейной обратной связью, спроектированного для лабораторной работы №3, провести описание проекта на языке описания аппаратуры, провести функциональное моделирование проекта аппаратного антивируса.
5. Лабораторная работа Реализация на ПЛИС автоматного шифратора. Цель - изучить основные понятия теории автоматных шифров, способы описания цифровых автоматов на языке описания аппаратуры, способы кодирования состояний цифрового автомата, получить навыки проектирования цифровых автоматов, отработать навыки описания и моделирования проектов цифровых автоматов. Задание: разработать автоматный шифратор, провести описание проекта шифратора на языке описания аппаратуры, провести функциональное моделирование проекта автоматного шифратора.

При подготовке к лабораторной работе студент обязан самостоятельно изучить методические рекомендации по проведению лабораторной работы, а также ответить на контрольные вопросы по лабораторной работе. Перед выполнением лабораторной работы преподавателем проводится инструктаж по достижению целей и решению задач лабораторной работы. По выполнению лабораторной работы студент готовит отчет, в котором указываются результаты выполнения лабораторной работы. При приеме лабораторной работы преподавателем задаются контрольные вопросы, позволяющие оценить уровень знаний студентов по теме лабораторной работы.

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.

3. Оценочные материалы итогового контроля (промежуточной аттестации) и критерии оценивания

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.

При оценивании необходимо продемонстрировать достижение всех запланированных индикаторов достижения компетенций: ИОПК-10.1, ИОПК-10.2, ИОПК-13.1, ИОПК-13.2, ИОПК-13.3, ИПК-3.2.

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. Структурное описание цифрового устройства.
15. Поведенческое описание цифрового устройства.
16. Язык HDL. Типы данных.
17. Язык HDL. Операции.
18. Язык HDL. Интерфейс.
19. Язык HDL. Операторы.
20. Язык HDL. Функции.
21. САПР. Создание проекта.
22. САПР. Поведенческое описание проекта.
23. САПР. Структурное описание проекта.
24. САПР. Функциональное моделирование проекта.
25. Достоинства и недостатки аппаратной реализация криптографических алгоритмов.
26. Основы аппаратной реализации шифров на примере DES.
27. Аппаратная реализация поточных шифров на базе LFRS.
28. Аппаратные шифраторы и электронные замки.
29. 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 *всех* контрольных заданий и лабораторных работ.

Хорошо - студент овладел обязательным материалом по разделам лекционного курса, возможно с некоторыми недостатками, а также показал требуемые умения и навыки при выполнении *большинства* контрольных заданий и лабораторных работ.

Удовлетворительно - студент имеет недостаточно глубокие знания по теоретическим разделам обязательного материала дисциплины, показал требуемые умения и навыки при выполнении *части* контрольных заданий и лабораторных работ.

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

4. Оценочные материалы для проверки остаточных знаний (сформированности компетенций)

Примерный перечень контрольных вопросов для проверки остаточных знаний (при оценивании необходимо продемонстрировать достижение **всех** запланированных индикаторов достижения компетенций):

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. Структурное описание цифрового устройства.
15. Поведенческое описание цифрового устройства.
16. Язык HDL. Типы данных.
17. Язык HDL. Операции.
18. Язык HDL. Интерфейс.
19. Язык HDL. Операторы.
20. Язык HDL. Функции.
21. САПР. Создание проекта.
22. САПР. Поведенческое описание проекта.
23. САПР. Структурное описание проекта.
24. САПР. Функциональное моделирование проекта.
25. Достоинства и недостатки аппаратной реализация криптографических алгоритмов.

Информация о разработчиках

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