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

Булевы функции в криптографии

Специальность
10.05.01 Компьютерная безопасность
Код и наименование специальности

Анализ безопасности компьютерных систем
наименование специализации

Томск–2021

ФОС составила:
канд. физ.-мат. наук, доцент
зав. лабораторией И.А. Панкратова

Рецензент:
канд. техн. наук, доцент,
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-3. Способен на основании совокупности математических методов разрабатывать, обосновывать и реализовывать процедуры решения задач профессиональной деятельности	ИОПК-3.2 Осуществляет применение основных понятий, фактов, концепций, принципов математики и информатики для решения задач профессиональной деятельности; ИОПК-3.3 Выявляет научную сущность проблем, возникающих в ходе профессиональной деятельности, и применяет соответствующий математический аппарат для их формализации, анализа и выработки решения.	ОР-3.1.1. *Обучающийся сможет: оценить свойства булевых функций, вычислить их криптографические характеристики* ОР-3.2.1. *Обучающийся сможет: дать определения понятиям корреляционная и алгебраическая иммунность, нелинейность и совершенная нелинейность, бент-функции, запреты булевых функций*	Владеет алгоритмами вычисления и оценки криптографических характеристик булевых функций	Владеет алгоритмами вычисления криптографических характеристик булевых функций	Знает основные понятия курса: корреляционная и алгебраическая иммунность, нелинейность и совершенная нелинейность, бент-функции, запреты булевых функций	Не знает криптографических свойств булевых функций

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.		Умеет оценивать пригодность булевых функций для применения в криптосистемах	Умеет оценивать свойства булевых функций	Неуверенно оценивает свойства булевых функций	Не умеет оценивать свойства булевых функций
ПК-2. Способен проектировать и разрабатывать средства защиты информации компьютерных систем и сетей	ИПК-2.1 Разрабатывает математические модели, реализуемые в средствах защиты информации.		Уверенно применяет математический аппарат дискретных функций для решения задач, возникающих в построении и анализе криптосистем	Хорошо умеет применять математический аппарат дискретных функций для решения задач, возникающих в построении и анализе криптосистем	Недостаточно умеет применять математический аппарат дискретных функций для решения задач, возникающих в построении и анализе криптосистем	Не умеет применять математический аппарат дискретных функций для решения задач, возникающих в построении и анализе криптосистем

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.	Корреляционная иммунность	ОР-3.1.1, ОР-3.2.1	Лабораторная работа Устный зачет с оценкой
2.	Нелинейность	ОР-3.1.1, ОР-3.2.1	Лабораторная работа Устный зачет с оценкой
3.	Лавинные характеристики	ОР-3.1.1, ОР-3.2.1	Лабораторная работа Устный зачет с оценкой
4.	Алгебраическая иммунность	ОР-3.1.1, ОР-3.2.1	Практические задания Устный зачет с оценкой
5.	Запреты булевых функций	ОР-3.1.1, ОР-3.2.1	Практические задания Устный зачет с оценкой

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

3.1. Типовые задания для проведения текущего контроля успеваемости по дисциплине

Текущая аттестация по дисциплине «Булевы функции в криптографии» осуществляется в форме оценивания результатов выполнения контрольной и лабораторных работ.

Задания контрольной работы:

1. Изобразить заданную функцию f на матрице в коде Грея.
2. Визуально (по матрице) определить максимальный порядок корреляционной иммунности; проверить, удовлетворяет ли функция строгому лавинному критерию.
3. Выполнить преобразование Мёбиуса.
4. Записать алгебраическую нормальную форму функции f, найти степень.
5. Перечислить все линейные, фиктивные и квазилинейные переменные функции f.
6. Выполнить преобразование Уолша - Адамара, проверить выполнение равенства Парсеваля.
7. Найти cor f по вектору коэффициентов ПУА; проверить результат п. 1 и выполнение неравенства Зигенталера.
8. Найти N_f и наилучшее аффинное приближение (в виде АНФ) к f.
9. Вычислить функцию автокорреляции.
10. Найти CN_f и максимальную степень критерия распространения функции f.
11. Найти аннигиляторы минимальной степени для f и $f \oplus 1$; найти AI(f).
12. Является ли f уравновешенной? аффинной? линейной? совершенно нелинейной?функцией с линейной структурой? бент? платовидной? частично бент? Ответы обосновать.

3.2. Типовые задания для проведения промежуточной аттестации по дисциплине

Вопросы к теоретическому зачёту:

1. Утверждение о весе булевой функции

2. Разложение функции по переменным. Связь веса функции с весами коэффициентов разложения
3. Алгебраическая нормальная форма булевой функции: определение, единственность
4. Преобразование Мёбиуса: определение, формула вычисления
5. Утверждение о связи веса функции и её степени
6. Понятие линейных и квазилинейных переменных. Уравновешенность функций, имеющих такие переменные
7. Три определения корреляционной иммунности булевой функции, их равносильность, содержательный смысл
8. Корреляционный метод криптоанализа, его связь с понятием корреляционной иммунности
9. Доказать: корреляционно иммунная порядка m функция является корреляционно иммунной любого меньшего порядка
10. Свойства максимальных порядков корреляционной иммунности и устойчивости. Описать все функции в $P_2(n)$, корреляционно иммунные порядка $n - 1$
11. Утверждение об устойчивых подфункциях
12. Неравенство Зигенталера
13. Преобразование Уолша – Адамара: определение, простейшие свойства
14. Преобразование Уолша – Адамара: тождество Саркара
15. Преобразование Уолша – Адамара: соотношение ортогональности
16. Преобразование Уолша – Адамара: формула обращения
17. Преобразование Уолша – Адамара: теорема о свёртке
18. Характеризация корреляционно иммунных функций преобразованием Уолша – Адамара
19. Теорема о необходимом условии корреляционной иммунности
20. Нелинейность булевых функций: определение, формула вычисления
21. Свойства нелинейности
22. Бент-функции: определение, свойства
23. Теорема о функции Шеннона для нелинейности
24. Доказать: класс бент-функций замкнут относительно невырожденного аффинного преобразования переменных
25. Теорема о степени бент-функции
26. Характеризация бент-функций матрицами Адамара
27. Дуальная функция: определение, свойства
28. Класс функций с линейной структурой. Утверждения о классе $LS(n)$
29. Совершенная нелинейность: определение. Теорема о функции Шеннона для совершенной нелинейности (формулировка и схема доказательства)
30. Доказать: $CN_f = 2^{n-2}$, если и только если производные функции f по всем ненулевым направлениям уравновешены
31. Критерий Ротхауза
32. Нелинейность корреляционно иммунных функций (общий случай)
33. Нелинейность неоптимальных функций
34. Доказать: насыщенная функция является платовидной
35. Нелинейность функций малого порядка корреляционной иммунности
36. Автокорреляция и взаимная корреляция: определение, простейшие свойства
37. Теорема о взаимной корреляции, её следствия

38. Строгий лавинный критерий и строгий лавинный критерий порядка m: определение, содержательный смысл, простейшие свойства
39. Описать все функции в $P_2(n)$, удовлетворяющие критерию SAC($n-2$)
40. Теорема о степени функции, удовлетворяющей строгому лавинному критерию
41. Критерий распространения, его свойства
42. Теорема о функции, удовлетворяющей строгому лавинному критерию порядка $n-2$
43. Глобальные лавинные характеристики и их свойства
44. Доказать: $N_{\Delta_f} \cdot N_f 2^n$ для любой функции f из $P_2(n)$.
45. Частично бент-функции и их свойства
46. Алгебраическая атака на фильтрующий генератор
47. Понятие и верхняя оценка алгебраической иммунности. Количество аннигиляторов
48. Утверждение о влиянии аффинной добавки на алгебраическую иммунность
49. Утверждения о связи алгебраической иммунности функции со степенью и алгебраической иммунностью её подфункций
50. Утверждения о связи веса и алгебраической иммунности; нелинейности и алгебраической иммунности
51. Конструкция Мэйорана – Мак-Фарланда, её свойства
52. Понятие запрета булевой функции, его содержательный смысл
53. Доказать: функция, линейная по первой (последней) своей существенной переменной, не имеет запрета
54. Доказать: неуравновешенная функция имеет запрет

4. Методические материалы, определяющие процедуры оценивания образовательных результатов обучения

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

В течение семестра необходимо выполнение всех обязательных практических заданий, лабораторных и контрольных работ.

4.2. Методические материалы для проведения промежуточной аттестации по дисциплине.

Промежуточная аттестация по дисциплине проводится в форме устного зачета с оценкой по теоретическому материалу.