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
« 19 » мая 20 22 г.

Рабочая программа дисциплины

Булевы функции в криптографии

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
2022

Код дисциплины в учебном плане: Б1.В.04.03

СОГЛАСОВАНО:
Руководитель ОП
_____ В.Н. Тренькаев

Председатель УМК
_____ С.П. Сущенко

Томск – 2022

1. Цель и планируемые результаты освоения дисциплины

Целью освоения дисциплины является формирование следующих компетенций:

– ОПК-3 – Способен на основании совокупности математических методов разрабатывать, обосновывать и реализовывать процедуры решения задач профессиональной деятельности.

– ОПК-10 – Способен анализировать тенденции развития методов и средств криптографической защиты информации, использовать средства криптографической защиты информации при решении задач профессиональной деятельности.

– ПК-2 – Способен разрабатывать требования к программно-аппаратным средствам защиты информации компьютерных систем и сетей.

Результатами освоения дисциплины являются следующие индикаторы достижения компетенций:

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.

ИОПК-10.1 Осуществляет анализ тенденций развития методов и средств криптографической защиты информации.

ИПК-2.2 Разрабатывает математические модели, реализуемые в средствах защиты информации.

2. Задачи освоения дисциплины

– изучить криптографические свойства булевых функций

– изучить теоретические основы и практические алгоритмы вычисления криптографических характеристик булевых функций.

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

Десятый семестр, зачет с оценкой

5. Входные требования для освоения дисциплины

Для успешного освоения дисциплины требуются результаты обучения по следующим дисциплинам: Введение в математику, Дискретная математика, Языки программирования.

6. Язык реализации

Русский

7. Объем дисциплины

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

8. Содержание дисциплины, структурированное по темам

Тема 1. Корреляционная иммунность
Тема 2. Нелинейность
Тема 3. Лавинные характеристики
Тема 4. Алгебраическая иммунность
Тема 5. Запреты булевых функций

9. Текущий контроль по дисциплине

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

10. Порядок проведения и критерии оценивания промежуточной аттестации

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

Примерный перечень теоретических вопросов

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

11. Учебно-методическое обеспечение

а) Электронный учебный курс по дисциплине в электронном университете «Moodle»

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

12. Перечень учебной литературы и ресурсов сети Интернет

а) основная литература:

– Агибалов Г.П. Избранные теоремы начального курса криптографии. – Томск: НТЛ, 2005.

– Бабаш А.В., Шанкин Г.П. Криптография. М.: СОЛОН-Р, 2002.

– Лобанов М.С. Точное соотношение между нелинейностью и алгебраической иммунностью // Дискретная математика. 2006. Т.18. Вып.3. С.152-159.

– Логачев О.А., Сальников А.А., Ященко В.В. Булевы функции в теории кодирования и криптологии. – М: МНЦМО, 2004.

– Панкратова И.А. Булевы функции в криптографии: учебное пособие. Томск: Изд. Дом ТГУ, 2014; СПб: Лань, 2019.

б) дополнительная литература:

– Тарannиков Ю.В. О корреляционно-иммунных и устойчивых булевых функциях // Мат. вопросы кибернетики. Вып.11. 2002. С.91-148.

– Токарева Н.Н. Бент-функции: результаты и приложения. Обзор работ // Прикладная дискретная математика. 2009. № 1. С.15-37.

– Токарева Н.Н. Обобщения бент-функций. Обзор работ // Дискрет. анализ и исслед. операций. 2010. Т.17. № 1. С.34-64.

– Уоррен Г. Алгоритмические трюки для программистов. М.: Вильямс, 2003.

– Фомичёв В.М. Дискретная математика и криптология. М.: Диалог-МИФИ, 2003.
– Courtois N., Meier W. Algebraic attack on stream ciphers with linear feedback // LNCS. 2003. V.2656. P.345-359.
– Dalai D.K. On some necessary conditions of Boolean functions to resist algebraic attack. Ph. D. Thesis. Kolkata, India, 2006.
– Meier W., Pasalic E., Carlet C. Algebraic attack and decomposition of Boolean functions // LNCS. 2004. V.3027. P.474-491.

13. Перечень информационных технологий

а) лицензионное и свободно распространяемое программное обеспечение:
– Microsoft Office Standart 2013 Russian: пакет программ. Включает приложения: MS Office Word, MS Office Excel, MS Office PowerPoint, MS Office On-eNote, MS Office Publisher, MS Outlook,
– публично доступные облачные технологии (Google Docs, Яндекс диск и т.п.).

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.
Аудитории для проведения занятий лабораторных работ, 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

Панкратова Ирина Анатольевна, к.ф.м.н., доцент, зав. лаб. компьютерной криптографии