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_» _____ 2021 г.

# Булевы функции в криптографии

## рабочая программа дисциплины

| | |
|---|---|
| Закреплена за кафедрой | *компьютерной безопасности* |
| Учебный план | *10.05.01 Компьютерная безопасность,*<br>*профиль «Анализ безопасности компьютерных систем»* |
| Форма обучения | *очная* |
| Общая трудоёмкость | *3 з.е.* |
| Часов по учебному плану | *108* |
| в том числе: | |
| аудиторная контактная работа | *67,45* |
| самостоятельная работа | *40,55* |
| Вид(ы) контроля в семестрах<br>*экзамен/зачет/зачет с оценкой* | *Семестр А – зачет с оценкой* |

Томск-2021

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

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

Рабочая программа дисциплины «Булевы функции в криптографии» 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**

**Цель** – изучение криптографических свойств булевых функций

Задачи: изучить теоретические основы и практические алгоритмы вычисления криптографических характеристик булевых функций

**1. Место дисциплины в структуре ОПОП**

Дисциплина «Булевы функции в криптографии» относится к части, формируемой участниками образовательных отношений Блока 1 «Дисциплины», входит в модуль «Специализация».

Пререквизиты дисциплины: Введение в математику, Дискретная математика, Языки программирования, Методы программирования

Постреквизиты дисциплины: преддипломная 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-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;<br>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.<br>Обучающийся сможет:<br>оценить свойства булевых функций, вычислить их криптографические характеристики<br>ОР-3.2.1.<br>Обучающийся сможет:<br>дать определения понятиям корреляционная и алгебраическая иммунность, нелинейность и совершенная нелинейность, бент-функции, запреты 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. | |
| ПК-2. Способен проектировать и разрабатывать средства защиты информации компьютерных систем и сетей | ИПК-2.1 Разрабатывает математические модели, реализуемые в средствах защиты информации. | |

## 3. Структура и содержание дисциплины

### 3.1. Структура и трудоемкость видов учебной работы по дисциплине

Общая трудоемкость дисциплины составляет 3 зачетные единицы, 108 часов.

Таблица 2.

| Вид учебной работы | Трудоемкость в академических часах | |
|---|---|---|
| | Семестр А | всего |
| **Общая трудоемкость** | 108 | 108 |
| **Контактная работа:** | 67,45 | 67,45 |
| Лекции (Л): | 32 | 32 |
| Практики (ПЗ) | | |
| Лабораторные работы (ЛР) | 32 | 32 |
| Семинары (СЗ) | | |
| Групповые консультации | | |
| Индивидуальные консультации | 3,2 | 3,2 |
| Промежуточная аттестация | 0,25 | 0,25 |
| **Самостоятельная работа обучающегося:** | 40,55 | 40,55 |
| *- подготовка к лабораторным работам* | 40,55 | 40,55 |
| **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 |
|---|---|---|---|---|---|---|---|
| 1 | Корреляционная иммунность | Лекции, лаб. работы, СРС | | | 20 | 1, 2, 3, 4, 5 | |
| 2 | Нелинейность | Лекции, лаб. работы, СРС | | | 20 | 1, 2, 3, 8, 9, 10 | ОР-3.1.1 ОР-3.2.1 |
| 3 | Лавинные характеристики | Лекции, лаб. работы, СРС | | | 18 | 2, 3, 8 | |
| 4 | Алгебраическая иммунность | Лекции, СРС | **А** | | 8 | 2, 6, 7, 9 | |
| 5 | Запреты булевых функций | Лекции, СРС | | | 6 | 2, 3 | |
| | **Подготовка к промежуточной аттестации в форме зачета с оценкой** | СРС | | | **33,7** | **1-10** | |
| | **Прохождение промежуточной аттестации в форме зачета с оценкой** | З/о | | | **2,3** | | |

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

Технология традиционная: лекции, разбор примеров и алгоритмов, решение практических задач (в аудитории и самостоятельно), лабораторные и контрольные работы.

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».

### 4.1. Рекомендуемая литература и учебно-методическое обеспечение

| № п/п | Авторы / составители | Заглавие | Издательство | Год издания |
|---|---|---|---|---|
| Основная литература | | | | |
| 1. | *Агибалов Г.П.* | Избранные теоремы начального курса криптографии | Томск: НТЛ | 2005 |
| 2. | *Панкратова И.А.* | Булевы функции в криптографии | СПб: Лань | 2019 |
| 3. | *Логачев О.А.*, *Сальников А.А.*, *Ященко В.В.* | Булевы функции в теории кодирования и криптологии | М: МНЦМО | 2004 |
| 4. | *Уоррен Г.* | Алгоритмические трюки для программистов | М.: Вильямс | 2003 |
| 5. | *Тарannиков Ю.В.* | О корреляционно-иммунных и устойчивых булевых функциях | Мат. вопросы кибернетики. Вып. 11. С.91-148 | 2002 |
| 6. | *Courtois N.*, *Meier W.* | Algebraic attack on stream ciphers with linear feedback | LNCS. V. 2 656. P. 345-359 | 2003 |
| 7. | *Dalai D.K.* | On some necessary conditions of Boolean functions to resist algebraic attack | Kolkata, India | 2006 |
| Дополнительная литература | | | | |
| 8. | *Фомичёв В.М.* | Методы дискретной математики в криптологии | М.: Диалог-МИФИ | 2010 |
| 9. | *Лобанов М.С.* | Точное соотношение между нелинейностью и алгебраической иммунностью | Дискретная математика. Т. 18. Вып. 3. С. 152-159 | 2006 |
| 10. | *Токарева Н.Н.* | Бент-функции: результаты и приложения. Обзор работ | Прикладная дискретная математика. № 1. С. 15-37. | 2009 |

### 4.3. Перечень лицензионного и программного обеспечения

Свободное ПО — Linux, Astra Linux и т.п.

### 4.4. Оборудование и технические средства обучения

Для реализации дисциплины необходимы лекционные аудитории (доска, мел) и компьютерный класс для проведения лабораторных работ. Вся основная и дополнительная литература, необходимая для самостоятельной работы и подготовки к зачёту, имеется в научной библиотеке ТГУ.

## 5. Методические указания обучающимся по освоению дисциплины

Рекомендуется: посещать все занятия, выполнять все домашние задания, обращаться за консультацией к преподавателю в случае возникновения вопросов.

**6. Преподавательский состав, реализующий дисциплину**

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

**7. Язык преподавания –** русский язык.