Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Московский государственный университет имени М.В. Ломоносова»
Факультет вычислительной математики и кибернетики

«УТВЕРЖДАЮ»
Декан факультета ВМК МГУ,
академик РАН

/Соколов И.А./
«____» _____ 2022 г.

ПРОГРАММА ВСТУПИТЕЛЬНОГО ЭКЗАМЕНА

(для осуществления приема на обучение по образовательным программам высшего образования - программам подготовки научных и научно-педагогических кадров в аспирантуре)

2.3.6 – «Методы и системы защиты информации, информационная безопасность»

Программа утверждена
Ученым советом факультета
(протокол № 4 от 28 апреля 2022 г.)

Москва-2022

I. ОПИСАНИЕ ПРОГРАММЫ

Настоящая программа предназначена для осуществления приема на обучение по образовательным программам высшего образования - программам подготовки научных и научно-педагогических кадров в аспирантуре вступительного экзамена в аспирантуру по специальности «*2.3.6 Методы и системы защиты информации, информационная безопасность»* и содержит основные темы и вопросы к экзамену, список основной и дополнительной литературы и критерии оценивания.

II. ОСНОВНЫЕ РАЗДЕЛЫ И ВОПРОСЫ К ЭКЗАМЕНУ

1. Теорема о полноте для 2P. Теорема Кузнецова. Алгоритм распознавания полноты в Pk
2. Теорема Слупецкого. Особенности k-значных логик.
3. Упрощение дизъюнктивных нормальных форм.
4. Логика 1-го порядка. Выполнимость и общезначимость. Общая схема метода резолюций.
5. Автоматы и машины Тьюринга. Классы рекурсивных функций. Эквивалентность понятий частично рекурсивная функция и функция, вычислимая по Тьюрингу.
6. Классы P и NP. NP-полные задачи. Теорема Кука. NP-полные задачи на графах. NP-полнота задачи о хроматическом числе графа.
7. Основные понятия теории групп. Свойства конечных абелевых групп. Основные свойства конечных полей.
8. Основные понятия теории линейных кодов, исправляющих ошибки: линейный код, порождающая и проверочная матрица, дуальный код, длина, размерность, минимальное расстояние. Граница Хемминга. Граница Варшамова–Гильберта. Граница Синглтона. Связь минимального расстояния кода с его проверочной матрицей
9. Циклические коды. Порождающий и проверочный многочлены. Построение проверочной и порождающей матрицы кода. Граница БЧХ.
10. Коды БЧХ. Алгоритм Берлекемпа-Месси. Декодирование кодов БЧХ с помощью алгоритма Берлекемпа-Месси.
11. Коды Рида-Маллера. Декодирование кода Рида-Маллера порядка 1. Алгоритм декодирования Рида кодов Рида-Маллера высших порядков.
12. Квадратичные вычеты и невычеты. Символ Лежандра и его свойства. Символ Якоби и его свойства. Решение квадратичных сравнений по простому модулю.
13. Простые числа. Тесты на простоту: тест Соловея-Штрассена и тест Рабина-Миллера.
14. Понятие производной булевой функции. Теорема об алгебраической степени производной. Понятие сужения булевой функции и понятие подфункции. Алгебраическая нормальная форма (АНФ) булевой функции и ее параметры. Соответствие Мебиуса. Теорема о вычислении коэффициентов АНФ. Классы линейных, аффинных, симметричных и монотонных функций.
15. Вес булевых функций. Теорема Мак-Элиса о делимости веса булевой функции на степень 2.Теорема о связи веса булевой функции и ее алгебраической

степени. Теорема о границе веса для почти всех булевых функций.

16. Преобразование Фурье и преобразование Уолша булевой функции. Формулы обращения. Связь спектров Фурье и Уолша. СпектрыУолша аффинных и симметричных функций. Булевы функции с непересекающимися спектрами.

III. РЕФЕРАТ ПО ИЗБРАННОМУ НАПРАВЛЕНИЮ ПОДГОТОВКИ

Реферат по избранному направлению подготовки представляет собой обзор литературы по теме будущего научного исследования и позволяет понять основные задачи и перспективы развития темы будущей диссертационной работы. Реферат включает титульный лист, содержательную часть, выводы и список литературных источников. Объем реферата 10-15 страниц машинописного текста. В отзыве к реферату предполагаемый научный руководитель дает характеристику работы и рекомендуемую оценку, входящую в общий экзаменационный балл.

IV. ПРИМЕР ЭКЗАМЕНАЦИОННОГО БИЛЕТА

Вопрос 1.

Вопрос 2.

Вопрос 3. Содержание реферата по теме диссертационного исследования (с приложением реферата и отзыва на реферат с отметкой предполагаемого научного руководителя).

V. РЕКОМЕНДУЕМАЯ ЛИТЕРАТУРА

1. ОСНОВНАЯ

[1]Яблонский С.В. Введение в дискретную математику. М.: Наука, 1986.

[2]Алексеев В.Б. Введение в теорию сложности алгоритмов. Изд. отдел ф-та ВМиК МГУ, 2002.

[3] Применко Э.А. Алгебраические основы криптографии: Учебное пособие. М: Книжный дом «ЛИБРОКОМ», 2013. - 288 с.

[4] Чень Ч., Ли Р. Математическая логика и автоматическое доказательство теорем. М.:Мир. 1983.

[5] Виноградов И.М. Основы теории чисел. М.: Издательство Юрайт, 2020. — 123 с.

[6] Мак-Вильямс Ф., Слоэн Н. Теория кодов, исправляющих ошибки. М.: Связь, 1979

[7] Логачев О.А, Сальников А.А, Ященко В.В. Булевы функции в теории кодирования и криптологии.М.: МЦНМО, 2004.

2. ДОПОЛНИТЕЛЬНАЯ

[1] Гэри М., Джонсон Д. Вычислительные машины и труднорешаемые задачи. М.: Мир. 1982.

[2] Ященко В.В. (ред.). Введение в криптографию (2-е изд.). М:. МЦНМО, 2000

[3] Таранников Ю.В. Комбинаторные свойства дискретных структур и приложения к криптологии. М: МЦНМО, 2011.

[4] Горшков С.П., Тарасов А.В. Сложность решения систем булевых уравнений. М: КУРС, 2017.

V. КРИТЕРИИ ОЦЕНИВАНИЯ

Уровень знаний поступающих в аспирантуру МГУ оценивается по десятибалльной шкале. Приотсутствиипоступающегонавступительномэкзаменевкачествеоценкипроставляется неявка. Результаты сдачи вступительных экзаменов сообщаются поступающим в течение трех дней со дня экзамена путем их размещения на сайте и информационном стенде структурного подразделения. Вступительное испытание считается пройденным, если абитуриент получил семь баллов и выше.

VI. АВТОРЫ

1.Чижов Иван Владимирович, доцент кафедры информационной безопасности, к.ф.-м.н.