

Программа
III Математической студенческой школы НИЯУ МИФИ

Секция 1: Дискретная математика и ее приложения

Дата и формат (очно/онлайн)	Время	ФИО	Должность	Тема занятия
21.11.23 (очно)	18:00-18:15			Открытие секции. Приветственное слово.
21.11.23 (очно)	18:15 - 20:15	Денисов Олег Викторович	к.ф.-м.н., доцент, «Инновационные коммуникационные технологии»	Разностные атаки на вероятностные модели блочных шифрсистем
22.11.23 (очно)	18:00 - 20:00	Пудовкина Марина Александровна	зам. зав. каф. №41 ИИКС НИЯУ МИФИ, д.ф.-м.н., профессор ИИКС	Теоретико-групповые методы криптографии
23.11.23 (онлайн)	18:00 - 20:00	Дурнев Валерий Георгиевич	д.ф.-м.н., профессор, ЯрГУ им Демидова, кафедра «Компьютерная безопасность и математические методы обработки информации»	Алгоритмически неразрешимые проблемы. Возможное и невозможное в математике - где граница?
24.11.27, 27.11.27 (онлайн, 2 дня)	18:00 - 20:00	Малыгина Екатерина Сергеевна	к.ф.-м.н. доцент ВШЭ МИЭМ	1. Введение в теорию кодирования (24.11.27) 2. Кодовые криптосистемы Мак-Элиса и Нидерайтера (27.11.27)

29.11.23 (онлайн)	18:00 - 20:00	Антонов Кирилл Валентинович	ассистент каф 41	Цепные дроби в криптоанализе
30.11.23, 01.12.23 (очно, 2 дня)	18:00 - 20:00	Поляков Михаил Вадимович	старший преподаватель каф 41, каф ИУ8 МГТУ им. Н.Э. Баумана	Асимптотически оптимальный метод синтеза схем, реализующих булевы функции
02.12.23, 03.12.23 (дистанционно)	CTF-соревнование в тематике киберпанка “Бегущий по HTML”			
04.12.23 (онлайн)	18:00 - 20:00	Новоселов Семен Александрович	к.ф.-м.н., доцент, БФУ им Канта	Криптосистемы на эллиптических кривых
05.12.23 (онлайн)	18:00 - 20:00	Мурин Дмитрий Михайлович	к.ф.-м.н., зав.каф. «Компьютерная безопасность и математические методы обработки информации» ЯрГУ им. Демидова	Некоторые вопросы теории сложности вычислений
07.12.23 (онлайн)	18:00 - 20:00	Козлов Александр Александрович	старший преподаватель каф 41, каф ИУ8 МГТУ им. Н.Э. Баумана	Линейные и разностные свойства ARX (add, rotate, xor) операций в приложении к криптоанализу
08.12.23 (очно- дистанционно)	18:00-20:00			Закрытие секции, подведение итогов. Разбор задач. Награждение участников.