МИНОБРНАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное учреждение высшего образования
«Новосибирский национальный исследовательский государственный университет»
(Новосибирский государственный университет, НГУ)
Структурное подразделение Новосибирского государственного университета –
Специализированный учебно-научный центр Университета (СУНЦ НГУ)
Министерство науки и высшего образования Российской Федерации

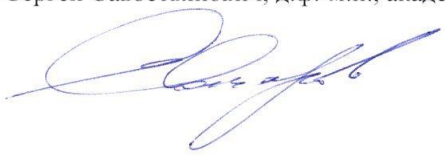
СОГЛАСОВАНО Заместитель директора по УР _____(Петровская О.В.) 23 ноября 2023 г.	УТВЕРЖДЕНО На заседании ученого совета СУНЦ НГУ Протокол № 48 от 23 ноября 2023 г.	УТВЕРЖДАЮ Директор СУНЦ НГУ _____(Некрасова Л.А.) 23 ноября 2023 г.

РАБОЧАЯ ПРОГРАММА

курса внеурочной деятельности «Олимпиадные задачи в криптографии»

Заведующий кафедрой дискретной математики и информатики

Гончаров Сергей Савостьянович, д.ф.-м.н., академик РАН



Новосибирск 2023

Пояснительная записка

Программа по курсу внеурочной деятельности «Олимпиадные задачи по криптографии» предназначена для проведения занятий в системе дополнительного образования общеобразовательных учреждений. Рабочая программа дает представление о целях, общей стратегии обучения, воспитания и развития обучающихся средствами дисциплины «Олимпиадные задачи по криптографии»; дает примерное распределение учебных часов по тематическим разделам курса и рекомендуемую (примерную) последовательность их изучения с учетом межпредметных и внутрипредметных связей, логики учебного процесса, возрастных особенностей обучающихся.

Курс «Олимпиадные задачи по криптографии» отражает основные области применения криптографии. Результаты ориентированы на получение компетентностей для компетентностей для последующей профессиональной деятельности как в рамках данной предметной области, так и в смежных с ней областях. Изучение дисциплины обеспечивает учащихся, ориентированных на специальности в области криптографии и подготовку к участию в олимпиадах.

Педагогическая целесообразность

Позволяет решить проблему занятости свободного времени детей, формированию навыков общего выбора методов для решения конкретных задач криптографии, пробуждение интереса детей к новой деятельности в области олимпиадного движения.

Цель программы

Подготовить учеников к участию в олимпиадах по криптографии, таких как: «Всероссийская олимпиада школьников по математике и криптографии», которая проводится Институтом криптографии, связи и информатики Академии ФСБ в ноябре, и «Международная олимпиада по криптографии NSUCRYPTO» (школьная секция), основной организатор которой – Новосибирский государственный университет. Спецкурс включает разбор необходимого материала, решение задач, в том числе в форме командных соревнований, знакомство с основными понятиями криптографии.

Планируемые результаты

К концу обучения по данной программе учащиеся должны

- Знать основной набор понятий современной криптографии, наиболее часто используемые математические принципы в криптографии.
- Уметь ориентироваться в современных и классических методах криптографии
- Владеть навыками общего выбора методов для решения конкретных задач криптографии.

Содержание программы

Введение в основы криптографии. Основные термины области. Обзор современных направлений в криптографии и криптоанализе. Задачи криптографии.

История области. Применение исторических шифров в олимпиадных задачах.

Алгебра в криптографии. Основные свойства. Обзор современных алгебраических методов для решения олимпиад.

Знакомство с международной олимпиадой по криптографии, с ее спецификой, особенностями.

Шифры замены. История использования и криптоанализа шифров замены. Обзор задач с использование шифров замены. Базовые примеры методов подхода к таким задачам.

Шифры перестановки. История использования и криптоанализа шифров перестановки. Обзор задач с использование шифров перестановки. Базовые примеры методов подхода к таким задачам.

Шифры смешанного типа. История использования и криптоанализа шифров, использующие замену и перестановку. Обзор задач с использование шифров с заменой и перестановкой. Базовые примеры методов подхода к таким задачам.

Арифметика остатков. Задачи факторизации и дискретного логарифмирования. Вопросы теории чисел. Проверка простоты числа. Протокол Диффи-Хеллмана. Криптосистемы RSA, Эль-Гамаля, Шамира и другие.

Протоколы. Блочные и поточные шифры. Математические модели, принципы построения. Примеры шифров: DES, Magma, AES, Kuznechik. Криптографические примитивы симметричных шифров.

Частотный анализ. Применение частотного анализа к большому тексту с неизвестной заменой.

Тематическое планирование (2 часа в неделю)

№ П/П	Тема урока	Всего часов	Воспитательный компонет
1.	**Введение в основы криптографии.** Основные термины области. Обзор современных направлений в криптографии и криптоанализе. Задачи криптографии.	2	Сформированность мировоззрения, соответствующего современному уровню развития науки, достижениям научно-технического прогресса и общественной практики, за счёт

2.	**История области.** Применение исторических шифров в олимпиадных задачах.	2	понимания роли информационных ресурсов, информационных процессов. Интерес к сферам профессиональной деятельности, связанным с информатикой, программированием и информационными технологиями, основанными на достижениях науки информатики и научно-технического прогресса, умение совершать осознанный выбор будущей профессии и реализовывать собственные жизненные планы/ Готовность осуществлять проектную и исследовательскую деятельность индивидуально и в группе.
3	**Алгебра в криптографии.** Основные свойства. Обзор современных алгебраических методов для решения олимпиад.	2	
4	**Знакомство с международной олимпиадой по криптографии**. Ее специфика, особенности.	2	
5	**Шифры замены.** История использования и криптоанализа шифров замены. Обзор задач с использование шифров замены. Базовые примеры методов подхода к таким задачам.	2	
6	**Шифры перестановки.** История использования и криптоанализа шифров перестановки. Обзор задач с использование шифров перестановки. Базовые примеры методов подхода к таким задачам.	2	
7	**Шифры смешанного типа.** История использования и криптоанализа шифров, использующие замену и перестановку. Обзор задач с использование шифров с заменой и перестановкой. Базовые примеры методов подхода к таким задачам.	2	
8	**Арифметика остатков.** Задачи факторизации и дискретного логарифмирования. Вопросы теории чисел. Проверка простоты числа. Протокол Диффи-Хеллмана.	2	

	Криптосистемы RSA, Эль-Гамаля, Шамира и другие.		
9	**Протоколы**. Блочные и поточные шифры. Математические модели, принципы построения. Примеры шифров: DES, Magma, AES, Kuznechik. Криптографические примитивы симметричных шифров.	2	
10	**Частотный анализ.** Применение частотного анализа к большому тексту с неизвестной заменой.	2	
ОБЩЕЕ КОЛИЧЕСТВО ЧАСОВ ПО ПРОГРАММЕ		20	

Материально-техническое обеспечение программы

- Презентационное оборудование (мультимедиа-проектор, экран, компьютер для управления)
- Компьютерный класс (с выходом в Internet)

Список источников информации

1. Материалы международных конференций по криптографии: ISIT, EUROCRYPT, CRYPTO, FSE, ASIACRYPT, SIBECRYPT, BFCA и др.

2. Зубов А.Ю., Зязин А.В., Никонов Н.В., Рамоданов С.М., Фролов А.А., Олимпиады по криптографии и математике для школьников, МЦНМО, 2019

3. Ященко В.В., Введение в криптографию (4-е, дополненное), МЦНМО, 2012