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 «Математические методы 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 «Математические методы в 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 «Математические методы в 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 «Математические методы в 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 курса 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 научной области.

Цель программы

Познакомить учеников с современными направлениями криптографии и криптоанализа, в том числе с практическими приложениями, такими как «Интернет вещей», технология «блокчейн», использование биометрических данных в криптографии, квантовая криптография и др. В рамках спецкурса разбираются основные методы и известные алгоритмы симметричной криптографии (блочные и поточные шифры, хэш-функции) и криптографии с открытым ключом (криптосистемы и понятие цифровой подписи), основные идеи криптоанализа (в том числе атаки по сторонним каналам).

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. Понятие криптографического протокола. История вопроса.

История области. История развития мировой и отечественной криптографии.

Теория секретности Шеннона. Вероятностная модель шифрсистемы. Полная избыточность языка сообщений и избыточность на букву сообщения. Теоремы Шеннона об избыточности языка сообщений, о числе ложных ключей, о совершенной секретности.

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

Введение в криптографические свойства булевых функций. Принципы построения криптографических булевых функций. Нелинейные булевы функции. Алгебраически иммунные функции. APN-функции.

Общие методы криптоанализа симметричных шифров. Введение в основы симметричного криптоанализа. Универсальные методы криптоанализа. Статистические и аналитические методы криптоанализа симметричных шифров.

Хэш-функции. Базовые принципы. Основы конструирования криптографических хэш-функций. Требования к ним. Базовые примеры современных хэш-функций.

Асимметричная криптография. Основные принципы построения и анализа асимметричных криптосистем. Математические вопросы асимметричной криптографии. Вопросы существования односторонних функций и псевдослучайных генераторов. Задачи факторизации и дискретного логарифмирования. Вопросы теории чисел. Проверка простоты числа. Протокол Диффи-Хеллмана. Криптосистемы RSA, Эль-Гамаля, Шамира и другие. Электронная цифровая подпись.

Новые направления криптографии: квантовая и постквантовая криптография.

Обзор приложений теории информации. Цифровая сотовая связь. Система безопасности GSM. Алгоритмы A5. Безопасность телефонных переговоров. Беспроводные сети WiFi. Методы шифрования WEP и WPA. Криптографические методы в противоугонных системах безопасности. Криптосистемы на основе биометрических данных.

Тематическое планирование (2 часа в неделю)

№ П/П	Тема урока	Всего часов	Воспитательный компонент

1.	**Введение в основы криптографии.** Основные термины области. Обзор современных направлений в криптографии и криптоанализе. Задачи криптографии. Понятие криптографического протокола. История вопроса.	2	Сформированность мировоззрения, соответствующего современному уровню развития науки, достижениям научно-технического прогресса и общественной практики, за счёт 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.
2.	**История области.** История развития мировой и отечественной криптографии.	2	
3	**Теория секретности Шеннона.** Вероятностная модель шифрсистемы. Полная избыточность языка сообщений и избыточность на букву сообщения. Теоремы Шеннона об избыточности языка сообщений, о числе ложных ключей, о совершенной секретности.	2	
4	**Симметричная криптография. Принципы построения симметричных шифров.** Блочные и поточные шифры. Математические модели, принципы построения. Примеры шифров: DES, Magma, AES, Kuznechik. Криптографические примитивы симметричных шифров.	2	
5	**Введение в криптографические свойства булевых функций. Принципы построения криптографических булевых функций.** Нелинейные булевы функции. Алгебраически иммунные функции. APN-функции.	2	
6	**Общие методы криптоанализа симметричных шифров.** Введение в основы симметричного криптоанализа. Универсальные методы криптоанализа. Статистические и аналитические методы криптоанализа симметричных шифров.	2	
7	**Хэш-функции.** Базовые принципы. Основы конструирования криптографических хэш-функций. Требования к ним. Базовые примеры современных хэш-функций.	2	
8	**Асимметричная криптография. Основные принципы построения и анализа асимметричных криптосистем.** Математические вопросы асимметричной криптографии. Вопросы существования односторонних функций и псевдослучайных генераторов. Задачи факторизации и дискретного логарифмирования. Вопросы теории чисел. Проверка простоты числа. Протокол Диффи-Хеллмана. Криптосистемы RSA,	2	

	Эль-Гамаля, Шамира и другие. Электронная цифровая подпись.		
9	**Новые направления криптографии: квантовая и постквантовая криптография.**	2	
10	**Обзор приложений теории информации.** Цифровая сотовая связь. Система безопасности GSM. Алгоритмы A5. Безопасность телефонных переговоров. Беспроводные сети WiFi. Методы шифрования WEP и WPA. Криптографические методы в противоугонных системах безопасности. Криптосистемы на основе биометрических данных.	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. Ященко В.В., Введение в криптографию (4-е, дополненное), МЦНМО, 2012

3. Menezes A.J, Van Oorschot P.C., Vanstone S.A. Handbook of Applied Cryptography. CRC Press, 1996.