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 «Криптография»

Заведующий лабораторией инженерного конструирования

Якушкин Сергей Владимирович

Новосибирск 2023

ПОЯСНИТЕЛЬНАЯ ЗАПИСКА

Спецкурс «Криптография» направлен на изучение основных областей применения криптографии. Результаты ориентированы на получение компетенций для последующей профессиональной деятельности как в рамках данной предметной области, так и в смежных с ней областях.
Цель курса — познакомить школьников с предметной областью, пробуждение интереса школьников к научной деятельности.

ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ

Цели и задачи специального курса:

1) Сформировать у учащихся представление о криптографических алгоритмах, механизмах их работы;
2) Представить учащимся математические методы, используемые в криптографии;
3) Представить учащимся механизмы криптоанализа, элементы теории вероятности;
4) Сформировать у учащихся представлении о разработке криптографических алгоритмах и об анализе разработанного алгоритма;
5) Представить учащимся областей применения криптографических алгоритмов..

В результате освоения специального курса обучающийся должен:

1. Иметь представление о классических криптографических алгоритмах и конструкциях.
2. Иметь представление о применении криптографических алгоритмов.
3. Иметь представление об анализе криптографических алгоритмов. Уметь проверять базовые свойства криптографических алгоритмов.
4. Иметь представление о процессе разработки криптографических алгоритмов.
5. Расширить свои знания в криптографии и компьютерной безопасности.

В ходе спецкурса учащиеся должны работать индивидуально и в группах, подготовить проектную работы.
По результатам работы и по посещению будет выставлен зачёт. Зачёт недифференцированный (зачёт / незачёт).

Объём спецкурса – 40 академических часов.

Планируемое время проведения спецкурса – I-II семестры 2023-24 учебного года (сентябрь 2023 г. - май 2024 г.).

СОДЕРЖАНИЕ СПЕЦКУРСА

Занятие 1 (2 часа)
История области. История развития мировой и отечественной криптографии..
Занятие 2 (2 часа)
Введение в основы криптографии. Основные термины области. Обзор современных направлений в криптографии и криптоанализе. Задачи криптографии. Понятие криптографического протокола.
Занятие 3 (2 часа)
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.
Занятие 4 (2 часа)

Шифры замены. История использования и криптоанализа шифров замены. Элементы шифров замены в современных криптографических алгоритмах.

Занятие 5 (2 часа)

Шифры перестановки. История использования и криптоанализа шифров перестановки. Перестановки в современных криптографических алгоритмах.

Занятие 6 (2 часа)

Шифры смешанного типа. История использования и криптоанализа шифров, использующих замену и перестановку. Современные алгоритмы, основанные на заменах и перестановках.

Занятие 7 (2 часа)

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

Занятие 8 (2 часа)

Хеш-функции. Базовые принципы. Основы конструирования криптографических хеш-функций. Требования к ним. Базовые примеры современных хеш-функций. Примеры хеш-функций: MD5, SHA-3.

Занятие 9 (2 часа)

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

Занятие 10 (2 часа)

Анализ свойств хеш-функций. Применение парадокса Дней Рождения при анализе крпитографических свойств хеш-функций. Лавинный эффект и его проверка.

Занятия 11-15 (10 часа)

Разработка криптографического алгоритма.

Занятия 16-18 (6 часа)

Анализ полученного алгоритма.

Занятия 19-20 (4 часа)

Оформление исследовательского проекта.

ТЕМАТИЧЕСКОЕ ПЛАНИРОВАНИЕ

№ п/п	Наименование разделов и тем программы	Кол-во часов	Воспитательный компонент
1	История области. История развития мировой и отечественной криптографии.	2	Формирование ответственного отношения к своему здоровью и безопасности. Готовность обучающихся к саморазвитию, самостоятельности и личному самоопределению. Формирование способности к оценке своих возможностей. Наличие мотивации к целенаправленной
2	Введение в основы криптографии. Основные термины области. Обзор современных направлений в криптографии и криптоанализе. Задачи криптографии. Понятие криптографического протокола.	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	Шифры замены. История использования и криптоанализа шифров замены. Элементы шифров замены в современных криптографических алгоритмах.	2	социально значимой деятельности.
5	Шифры перестановки. История использования и криптоанализа шифров перестановки. Перестановки в современных криптографических алгоритмах.	2	Развитие и поддержка одаренности обучающихся и обеспечение участия в олимпиадах и конкурсах
6	Шифры смешанного типа. История использования и криптоанализа шифров, использующих замену и перестановку. Современные алгоритмы, основанные на заменах и перестановках.	2	Установление доверительных отношений между руководителем объединений и обучающимися и между обучающимися непосредственно через беседы, дискуссии
7	Симметричная криптография. Принципы построения симметричных шифров. Блочные и поточные шифры. Математические модели, принципы построения. Примеры шифров: DES, AES, IDEA. Криптографические примитивы симметричных шифров.	2	
8	Хеш-функции. Базовые принципы. Основы конструирования криптографических хеш-функций. Требования к ним. Базовые примеры современных хеш-функций. Примеры хеш-функций: MD5, SHA-3.	2	
9	Общие методы криптоанализа симметричных шифров. Введение в основы симметричного криптоанализа. Универсальные методы криптоанализа. Статистические и аналитические методы криптоанализа симметричных шифров.	2	
10	Анализ свойств хеш-функций. Применение парадокса Дней Рождения при анализе крпитографических свойств хеш-функций. Лавинный эффект и его проверка.	2	
11	Разработка криптографического алгоритма.	10	
12	Анализ полученного алгоритма.	6	
13	Оформление исследовательского проекта.	4	
	Всего	40	

Приложение 1

МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА

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

УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА

1. Городилова А. А., Токарева Н. Н., Шушуев Г. И. Криптография. Краткий курс.
2. Черемушкин А. В. Лекции по арифметическим алгоритмам в криптографии //М.: МЦНМО. – 2002. – Т. 104. – С. 7.
3. Алферов А. П. и др. Основы криптографии //М.: Гелиос арв. – 2002. – Т. 200. – С. 480.