МИНИСТЕРСТВО ПРОСВЕЩЕНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
КОМИТЕТ ПО ОБРАЗОВАНИЮ
АДМИНИСТРАЦИИ ГОРОДА БРАТСКА
МБОУ г. Братска "СОШ № 14"

РАССМОТРЕНО
Руководитель ШМО
Калюк Г.Р.
Протокол №1 от «30» августа2023 г.

УТВЕРЖДЕНО
Директор МБОУ "СОШ №14"
Федоров С.Г.
Приказ № 171 от «01» сентября2023 г.

РАБОЧАЯ ПРОГРАММА

курса по выбору

«Введение в криптографию».

для обучающихся 9 классов

г. Братск 2023

1. Результаты освоения курса

В результате освоения содержания курса по выбору «Введение в криптографию» у обучающихся предполагается формирование универсальных учебных действий (познавательных, регулятивных, коммуникативных, личностных) позволяющих достигать предметных результатов.

Личностные результаты:

- умение ясно, точно, грамотно излагать свои мысли в устной и письменной речи, понимать смысл поставленной задачи, выстраивать аргументацию, приводить примеры и контрпримеры;
- критичность мышления, умение распознавать логически некорректные высказывания, отличать гипотезу от факта;
- креативность мышления, инициатива, находчивость, активность при решении задач по криптографии;
- способность к эмоциональному восприятию математических объектов, задач, решений, рассуждений;
- готовности и способности к саморазвитию и реализации творческого за счет развития их образного, алгоритмического и логического мышления;
- интереса к математике, информатике стремления использовать полученные знания в процессе обучения другим предметам и в жизни;
- чувства личной ответственности за качество окружающей информационной среды.

Метапредметные результаты:

- умение находить в различных источниках информацию, необходимую для решения математических проблем, представлять ее в понятной форме, принимать решение в условиях неполной и избыточной, точной и вероятностной информации;
- умение понимать и использовать математические средства наглядности (графики, диаграммы, таблицы, схемы и др.) для иллюстрации, интерпретации, аргументации;
- умение выдвигать гипотезы при решении учебных задач, понимать необходимость их проверки;
- умение применять индуктивные и дедуктивные способы рассуждений, видеть различные стратегии решения задач;
- умение самостоятельно ставить цели, выбирать и создавать алгоритмы для решения учебных проблем;
- умение планировать и осуществлять деятельность, направленную на решение задач исследовательского характера;
- создание моделей криптографических систем;
- оценивание стойкости созданного шифра.
- владение основными универсальными умениями математического характера: постановка и формулирование проблемы; поиск и выделение необходимой информации, применение методов информационного поиска; структурирование и визуализация информации; выбор наиболее эффективных способов решения задач в зависимости от конкретных условий;
- использования средств информационных и коммуникационных технологий для сбора, хранения, преобразования и передачи различных видов информации, навыки создания личного информационного пространства.

Предметные результаты:

1. Получить представление об основных способах защиты информации, о принципах классификации криптографических алгоритмов.
2. Получить представление о научной деятельности К. Шеннона.
3. Ознакомиться с понятием «симметричный шифр».
4. Получить представление о шифре «Полибианский квадрат», о шифре «Доска Полибия».
5. Научиться применять шифры «Полибианский квадрат» и «Доска Полибия» для шифрования данных.
6. Ознакомиться с теоретическими принципами обеспечения секретности при передаче информации.

7. Получить представление об основных методах криптоанализа.
8. Научиться оценивать стойкость алгоритма, исходя из длины ключа.
9. Ознакомиться с понятием
10. «биграмма», «автоключ», «магический квадрат», «блочный шифр», «матрица».
11. Научиться давать характеристику алгоритма Диффи-Хеллмана.
12. Научиться строить криптограммы с использованием алгоритма RSA.
13. Научиться применять алгоритм RSA для создания и проверки электронной цифровой подписи.

2. Содержание курса внеурочной деятельности с указанием форм организации и видов деятельности

Логико-алгоритмический компонент

Раздел 1. Введение в криптографию

Основные понятия криптографии. Клод Шеннон. Стойкость и взлом криптоалгоритмов.

Основные понятия: шифр, ключ, открытый текст, криптограмма, шифрование, дешифрование, криптография, стойкость шифра, атака, взлом, противник, теоретическая секретность, методы взлома криптоалгоритмов, вероятные слова.

Раздел 2. Математические основы криптографии

Математические основы криптографии. Комбинаторика. Математические основы криптографии. Построение ключей. Ключи в двоичной системе счисления.

Основные понятия: алфавит, комбинаторика, выборка без возвращения, выборка с возвращением, перестановка, ключ, стойкость алгоритма, код, символ, противник.

Раздел 3. Шифры замены

Математические основы симметричной криптографии. Простейший шифр замены. Полибианский квадрат. Доска Полибия. Шифрование биграммами. Шифр Цезаря. Многоалфавитные шифры замены. Шифр Виженера. Шифр One-Time-Pad (OTP). Шифрование с автоключом. Алгоритм «Crypto».

Основные понятия: шифр, шифрование, симметричный шифр, шифр замены, таблица замены, шифрообозначение, биграмма, алфавит, сдвиг, естественный номер символа, относительный номер символа, многоалфавитный шифр замены, одноразовый шифр замены, абсолютно стойкий шифр, автоключ.

Раздел 4. Шифры перестановки

Математические основы шифров перестановки. Простейший шифр перестановки. Магические квадраты и решетки

Основные понятия: шифр перестановки, подстановка, трафарет, магический квадрат.

Учебный материал данного раздела знакомит учащихся с принципами построения шифров перестановки и с их математическими основами. В качестве примера шифра перестановки учащиеся рассматривают применение магических квадратов и магических решеток.

Раздел 5. Блочные шифры

Блочные шифры. Американский стандарт шифрования данных DES. Российский стандарт шифрования данных.

Основные понятия: блок, блочный шифр, длина (размер) блока, функция шифрования, поразрядное суммирование, раунд шифрования.

Раздел 6. Математические основы асимметричной криптографии

Математические основы асимметричной криптографии. Алгебра матриц. Понятие односторонней функции. Система RSA

Основные понятия: матрица, матрица-строка, матрица-столбец, вектор, односторонняя функция, функция с ловушкой (секретом), скалярное произведение, полином (многочлен), экспоненциальное преобразование. Открытое распределение ключей. Алгоритм Диффи-Хеллмана. Цифровая электронная подпись.

3. Тематическое планирование

№	Тема	Вид занятия	Кол-во часов
1	Основные понятия криптографии	Комбинированный урок	2
2	Клод Шеннон. Стойкость и взлом криптоалгоритмов	Урок изучения теоретического материала	1
3	Математические основы криптографии. Комбинаторика.	Комбинированный урок	3
4	Математические основы криптографии. Построение ключей	Комбинированный урок	1
5	Ключи в двоичной системе счисления	Комбинированный урок	1
	Промежуточное тестирование (тест №1)	Проверка знаний	1
6	Математические основы симметричной криптографии. Простейший шифр замены	Комбинированный урок	1
7	Полибианский квадрат. Доска Полибия	Комбинированный урок	1
8	Шифрование биграммами	Комбинированный урок	1
9	Шифр Цезаря	Комбинированный урок	1
10	Многоалфавитные шифры замены. Шифр Виженера	Комбинированный урок	1
11	Шифр One-Time-Pad (OTP)	Комбинированный урок	1
12	Шифрование с автоключом. Алгоритм «Crypto»	Комбинированный урок	1
	Промежуточное тестирование (тест №2)	Проверка знаний	1
13	Математические основы шифров перестановки. Простейший шифр перестановки	Комбинированный урок	1
14	Магические квадраты и решетки	Комбинированный урок	1
15	Блочные шифры	Комбинированный урок	1
16	Американский стандарт шифрования данных DES	Комбинированный урок	2
17	Российский стандарт шифрования данных	Комбинированный урок	1
	Промежуточное тестирование (тест №3)	Проверка знаний	1
18	Математические основы асимметричной криптографии. Алгебра матриц	Комбинированный урок	2
19	Понятие односторонней функции	Комбинированный урок	3
20	Открытое распределение ключей. Алгоритм Диффи-Хеллемана	Комбинированный урок	1
21	Цифровая электронная подпись	Урок изучения теоретического материала	1
22	Система RSA	Комбинированный урок	1
	Промежуточное тестирование (тест №4)	Проверка знаний	1
	Практическая контрольная работа	Проверка знаний	1
		Итого:	34 часа