Муниципальное автономное общеобразовательное учреждение

«Лицей№12»

городского округа город Стерлитамак

Республики Башкортостан

|  |  |  |
| --- | --- | --- |
| РАССМОТРЕНО МО учителей математики, физики и информатикиМАОУ «Лицей №12» г.Стерлитамак РБпр. №\_\_\_ от \_\_\_\_\_\_.2019г.\_\_\_\_\_\_\_\_ Савинова Н.П. | СОГЛАСОВАНОЗам. директора МАОУ «Лицей №12 » г. Стерлитамак РБ\_\_\_\_\_\_О.Ю.Ишназарова\_\_\_\_\_\_.2019г. | УТВЕРЖДЕНОДиректор МАОУ «Лицей№12 » г.Стерлитамак РБ\_\_\_\_\_\_Е.Н. МаркеловаПриказ №\_\_\_\_\_ от «\_\_\_»\_\_\_\_2019г. |

 **ПРОГРАММА**

курса внеурочной деятельности

**«Секреты криптографии»**

(общеинтеллектуальное направление)

для обучающихся 5-7 классов

(первый год обучения

основного общего образования

на 2019 – 2020 учебный год

Составитель: Мухаметзянова Г.Р.-учитель математики, высшей категории

2019 год

 **Пояснительная записка**

 Программа курса внеурочной деятельности «Секреты криптографии» составлена на основе следующих нормативных документов:

- Федеральный государственный образовательный стандарт основного общего образования;

- ООП МАОУ «Лицей № 12» г. Стерлитамака РБ;

- Учебный план МАОУ «Лицей № 12 » г. Стерлитамак РБ на 2019-2020 учебный год.

Актуальность курса состоит в том, что он направлен на расширение знаний учащихся по математике, информатике, развитие их теоретического мышления и логической культуры. Криптография одно из перспективных направлений в науке по практической значимости.

Программа позволяет преподавателю комплексно решать образовательные задачи, а учащимся ознакомиться со многими интересными вопросами математики, информатики, выходящими за рамки школьной программы. Решение задач по криптографии закрепит интерес детей к познавательной деятельности, будет способствовать развитию мыслительных операций и общему интеллектуальному развитию. С целью повышения познавательной активности обучающихся, формирования способности самостоятельного освоения материала школьники имеют возможность познакомиться с научно – популярной литературой по проблеме применения математики. Предполагается использование компьютеров в практической части курса.

***Цели курса:***

* формирование представления о комбинаторике и теории вероятности;
* обучение учащихся: основным понятиям криптографии, основным способам шифрования и дешифрования текста, строгой математической проверки стойкости шифра;
* развитие навыков построения математических моделей шифров, алгоритмизации, программирования, навыков анализа своей деятельности;
* развитие логического мышления;
* воспитание усидчивости, внимания.

***Задачи курса:***

* изучить основы комбинаторики и теории вероятности;
* расширить кругозор учащихся в области фундаментальных наук, показать их практическую значимость;
* сформировать навыки элементарного построения криптосистем;
* изучить основные способы шифрования и дешифрования текста;
* сформировать у учащихся чёткое понимание стойкости шифра;
* научить проверять стойкость шифра математическими расчётами;
* развить у учащихся навыки программирования;
* научить создавать программный продукт на основе различных основных математических, криптографических систем;
* реализовать технические и эвристические способности учащихся в ходе проектирования и программирования различных криптографических задач;
* развить навык анализа выполненной работы;
* рассмотреть применение полученных навыков в различных областях знаний;
* развить у учащихся логическое мышление;
* воспитать у учащихся усидчивость и внимание.

Курс входит в число дисциплин, включенных в учебный план МАОУ «Лицей № 12» г. Стерлитамак РБ. Настоящая программа рассчитана на 1 год обучения и предназначена для работы с обучающимися 5-7 класса в возрасте 11-13 лет. Занятия проводятся 1 раз в неделю по 1 часу (34 часов в год).

 От уровня подготовленности и состава группы зависит объем теоретического материала и перечень тем для занятий. Тематика занятий отражает реальные познавательные интересы детей, содержит полезную и любопытную информацию, интересные математические факты, способные дать простор воображению.

 **Формы** организации учебных занятий: индивидуальная, групповая, работа в парах с последующем коллективным обсуждением результатов, урок-игра, урок-беседа, проектный урок, игры на внимание, смотр знаний, мини-лекция, урок-турнир.

**Планируемые результаты курса «Секреты криптографии»**

**Личностные результаты**

*У учащегося будут сформированы:*

* 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;

*Учащийся получит возможность для формирования:*

* широких познавательных интересов, инициативы и любознательности, мотивов познания и творчества;
* 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 освоения курса**

*У учащегося будут сформированы:*

* 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.

*Учащийся получит возможность для формирования умений:*

* 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 освоения курса**

*У учащегося будут сформированы:*

* умения работать с текстом (структурирование, извлечение необходимой информации), точно и грамотно выражать свои мысли в устной и письменной речи, применяя математическую терминологию и символику, использовать различные языки математики (словесный, символический, графический), развития способности обосновывать суждения, проводить классификацию;
* умения пользоваться изученными математическими формулами;
* знания основных способов представления и анализа статистических данных; умения решать задачи с помощью перебора всех возможных вариантов;
* умения решать простые комбинаторные задачи;
* умения работать с текстовыми файлами;
* умения применять изученные понятия, результаты и методы при решении задач из различных разделов курса, в том числе задач, не сводящихся к непосредственному применению известных алгоритмов.

**Введение в криптографию и первые шифры**

*Ученик научится:*

* оперировать на базовом уровне понятиями: шифр, криптография, стеганография, скитала, диск и линейка Энея; цифровая тайнопись.

*Ученик получит возможность научиться:*

* извлекать, интерпретировать и преобразовывать информацию о криптографии.

**Математические основы криптографии**

*Ученик научится:*

* оперировать на базовом уровне понятиями: выборка, перестановка, подстановка, делимость чисел, НОД;
* изменять действия для шифрования и дешифрования;
* создавать шифр на основе перестановки.

*Ученик получит возможность научиться:*

* извлекать, интерпретировать и преобразовывать информацию о шифре.

**Современные криптосистемы**

*Ученик научится:*

* оперировать на базовом уровне понятиями: криптосистемы с секретным ключом; метод гаммирования; псевдослучайные числа; криптосистема, критоанализ.
* оперировать современными методами шифрования;
* создавать шифры на основе блочных.

**Решение задач**

*Учащийся научится:*

* решать несложные задачи на шифрование и дешифрование;
* строить модель условия задачи (в виде таблицы, схемы, рисунка);
* осуществлять способ поиска решения задачи, в котором рассуждение строится от условия к требованию или от требования к условию;
* составлять план решения задачи;
* выделять этапы решения задачи;

*Учащийся получит возможность научиться:*

* моделировать рассуждения при поиске решения задач с помощью граф-схемы;
* интерпретировать результаты в задаче, исследовать полученное решение задачи;
* решать и конструировать задачи на основе рассмотрения реальных ситуаций, в которых не требуется точный результат.

Контроль за усвоением изучаемого материала осуществляется по итогам защиты проектов.

Примерные темы проектов:

1. Секреты криптографии

2. Криптография – основа информационной безопасности

3. Как защитить свою информацию

4. Современные криптосистемы

 и т.д.

**Содержание курса внеурочной деятельности «Секреты криптографии»**

|  |  |  |
| --- | --- | --- |
| **Раздел** | **Теоретическая часть** | **Практическая часть** |
| **Введение в криптографию и первые шифры** | Инструктаж по технике безопасности.Как защитить свое послание**.**Из истории криптографии.Где применяется и как применяется. Поиск информации по теме «Способы шифрования» (работа в парах) |  Обзорная лекция с элементами практической работы.Поиск сценарий применения полученных знаний в жизни.Мозговой штурм. |
| **Математические основы криптографии** | Мини-лекции: Основы криптоанализа. Криптостойкость.Криптоатака. Подстановка. Шифр Цезаря. Перестановка.  | Игры на внимание. Практическое занятие. Использование платформы «Электронная игровая школа СФ ФГ БОУ ВО БГУ» |
| **Современные криптосистемы** | Гаммирование. Основные понятия теории вероятности. Блочные шифры.Современные криптосистемы с открытым ключом.Для чего компьютеру нужна криптография? Как зашифровать файл? Современные средства криптозащиты. Электронная цифровая подпись. Алгоритм Диффи-Хеллмана. Криптография и криптовалюта. Что такое «блокчейн»? | Практикум по решению задач. Игры. Урок –турнир «Шерлок Холмс». Использование платформы «Электронная игровая школа СФ ФГ БОУ ВО БГУ» |
| **Решение задач** | Блиц-опрос по пройденному материалу  | Решение учащимися готовых задач, составление задач по теме. Выставка работ, на которых представлен зашифрованный текст. Проектный урок. Урок- турнир. Смотр знаний «Математическое лото». Конкурс на лучшую презентацию |

**Тематическое планирование**

|  |  |  |
| --- | --- | --- |
| **№** | Разделы | Количество часов |
| I | Введение в криптографию и первые шифры | 4 |
| II | Математические основы криптографии | 9 |
| III | Современные криптосистемы | 10 |
| IV | Решение задач | 11 |
|  | Итого | 34 |

**Учебно-методическое обеспечение образовательного процесса**

Литература для учителя

1. А.В. Бабаш, Г.П. Шанкин «Криптография» Москва, СОЛОН-Р, 2002 г.

2. С.И. Бобровский «Delphi 7. Учебный курс» Санкт-Петербург, Питер, 2003г.

3. Ростовцев А.Г., Маховенко Е.Б. Теоретическая криптография. – М.: Изд. Профессионал, 2005.

4. Алферов А.П., Зубков А.К., Кузьмин А.С., Черемушкин А.В. Основы криптографии: Учебное пособие. – М.: Гелиос АРВ, 2002.

5. <http://mathinfinity.net.ru/article/6/> различные шифры

6. <http://www.rbardalzo.narod.ru/kripto2.html> криптография и математика

Для ученика

1. Адаменко, Михаил Основы классической криптологии. Секреты шифров и кодов / Михаил Адаменко. - Москва**: Машиностроение**, 2014. - 256 c
2. Бабаш, А. В. История криптографии. Часть I / А.В. Бабаш, Г.П. Шанкин. - М.: Гелиос АРВ, 2002.
3. Баричев С. Криптография без секретов. – 2004.
4. Криптография: скоростные шифры / А. Молдовян и др. - М.: БХВ-Петербург, 2002. - 496 c.
5. [http://wiki.saripkro.ru/index.php/Исследование\_учащихся\_Секреты\_криптографии](http://wiki.saripkro.ru/index.php/%D0%98%D1%81%D1%81%D0%BB%D0%B5%D0%B4%D0%BE%D0%B2%D0%B0%D0%BD%D0%B8%D0%B5_%D1%83%D1%87%D0%B0%D1%89%D0%B8%D1%85%D1%81%D1%8F_%D0%A1%D0%B5%D0%BA%D1%80%D0%B5%D1%82%D1%8B_%D0%BA%D1%80%D0%B8%D0%BF%D1%82%D0%BE%D0%B3%D1%80%D0%B0%D1%84%D0%B8%D0%B8)

*Обзор литературы по криптографии*

<http://www.diary.ru/~eek/p76084072.htm>