Муниципальное бюджетное общеобразовательное учреждение
«Средняя школа №1» города Смоленска

РАБОЧАЯ ПРОГРАММА

по курсу по выбору
«Введение в криптографию. Как защитить свое письмо от любопытных?»

в классе 11А

Учитель информатики Артамонова А. В.
Высшая квалификационная категория

2023 - 2024

учебный год

Пояснительная записка

В настоящее время обеспечению безопасности информации уделяется все большее внимание, поэтому подготовка специалистов в данной области становится особенно важной. Однако изучать вопросы, связанные с защитой информации, нужно начиная с простейших алгоритмов и постепенно переходя к более сложным схемам шифрования.

Данный элективный курс предназначен для учащихся профильных классов с углубленным изучением информатики и математики и соответствует таким целям образовательных стандартов как:

- воспитание чувства ответственности за результаты своего труда;
- формирование установки на позитивную социальную деятельность в информационном обществе, на недопустимость действий» нарушающих правовые и этические нормы работы с информацией.

Основываясь на указанных целях, определим следующие *цели изучения элективного курса «Введение в криптографию»:*

1) получение знаний о существующих способах защиты данных и о преимуществах криптографический защиты информации;
2) понимание математических основ криптографии;
3) формирование умения работать с симметричными криптоалгоритмами при шифровании данных;
4) формирование умения осознанно выбирать алгоритм шифрования для защиты конкретной имеющейся информации;
5) понимание математических основ несимметричной криптографии;
6) формирование умения работать с существующими несимметричными криптоалгоритмами.

Общая продолжительность предлагаемого элективного курса, составляет 34 учебных часа, включая теоретические занятия, контрольные работы и тесты.

Планируемые результаты освоения курса

После изучения данного элективного курса учащиеся *научатся:*

- различать способы защиты информации;
- распознавать возможные виды информационных угроз;
- использовать математические основы симметричной криптографии;
- использовать методы шифрования, лежащие в основе симметричных криптоалгоритмов;
- использовать основные методы взлома защищенной информации;
- использовать принцип открытого распределения ключей;

- описывать характеристики различных методов защиты информации;
- разбирать преимущества использования криптографических методов защиты информации;
- применять принципы построения открытых и секретных ключей;
- работать с симметричными криптоалгоритмами защиты информации;
- работать с существующими несимметричными криптоалгоритмами;
- выбирать криптоалгоритмы для решения конкретных поставленных задач;
- применять алгоритмы криптографии для защиты информации.

После изучения элективного курса учащиеся получат возможность:

- осуществлять анализ поставленной проблемы, связанной с защитой информации;
- организовывать защиту информации (с указанием на возможность использования тех или иных методов криптографии);
- выбирать оптимальный алгоритм шифрования в зависимости от предъявляемых к нему требований.

Согласно Рабочей программе воспитания СШ №1(утверждена приказом по МБОУ «СШ №1 г. Смоленска» № 107-ОД от 15.06.2021), образование личности должно быть сориентировано не только на освоение информации, но и развитие самостоятельности, личной ответственности, созидательных способностей и качеств обучающихся, позволяющих им учиться, действовать и эффективно трудиться в современных экономических условиях. Реализация воспитательного потенциала на уроках предполагает:

- привлечение внимания обучающихся к ценностному аспекту изучаемых на уроках явлений, организацию их работы с получаемой на уроке социально значимой информацией, инициирование ее обсуждения, высказывания обучающимися своего мнения по ее поводу, выработки своего отношения к ней;
- использование воспитательных возможностей содержания учебного предмета через демонстрацию примеров ответственного, гражданского поведения, проявления человеколюбия и добросердечности, через подбор соответствующих текстов для чтения, задач для решения, проблемных ситуаций для обсуждения в классе;
- применение на уроке интерактивных форм работы обучающихся: интеллектуальных игр, стимулирующих познавательную мотивацию обучающихся; дискуссий, которые дают обучающимся возможность приобрести опыт ведения конструктивного диалога; групповой работы или работы в парах, которые учат обучающихся командной работе и взаимодействию с другими детьми;
- включение в урок игровых процедур, которые помогают поддержать мотивацию обучающихся к получению информации, налаживанию позитивных межличностных отношений в классе, помогают установлению доброжелательной атмосферы во время урока;
- инициирование и поддержку исследовательской деятельности обучающихся в рамках реализации ими индивидуальных и групповых исследовательских проектов, что даст обучающимся возможность приобрести навык самостоятельного решения

теоретической проблемы, навык генерирования и оформления собственных идей, навык уважительного отношения к чужим идеям, оформленным в работах других исследователей, навык публичного выступления перед аудиторией, аргументирования и отстаивания своей точки зрения.

Содержание курса

В рамках элективного курса «Введение в криптографию» рассматриваются вопросы, связанные с современными методами обеспечения безопасности информации. Учащимся предлагается ознакомиться с основными алгоритмами симметричной и несимметричной криптографии и с их математическими основами.

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

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

3. Шифры замены
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.

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

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

6. Математические основы асимметричной криптографии
Основные понятия: матрица, матрица-строка, матрица-столбец, вектор, односторонняя функция, функция с ловушкой (секретом), скалярное произведение, полином (многочлен), экспоненциальное преобразование.

7. Открытое распределение ключей. Алгоритм Диффи-Хеллмана. Цифровая электронная подпись. Система RSA
Основные понятия: открытое распределение ключей, открытый канал связи, секретный ключ, открытый ключ, дискретное возведение в степень, электронная цифровая подпись.

Тематическое планирование

№ п/п	Дата проведения	Тема занятия
1		Урок – экскурсия «Криптография с древних времен и до наших дней»
2		Основные понятия криптографии
3		Клод Шеннон и значение его открытий. Стойкость и взлом криптоалгоритмов
4		Математические основы криптографии. Комбинаторика
5		Основы комбинаторики
6		Основы комбинаторики
7		Математические основы криптографии. Построение ключей
8		Ключи в двоичной системе счисления
9		Промежуточное тестирование (тест № 1)
10		Математические основы симметричной криптографии. Простейший шифр замены
11		Полибианский квадрат. Доска Полибия
12		Шифрование биграммами
13		Урок – экскурсия «Шифр Цезаря»
14		Многоалфавитные. шифры замены. Шифр Виженера
15		Шифр One-Time-Pad (OTP)
16		Шифрование с автоключом. Алгоритм « Crypto »
17		Промежуточное тестирование (тест № 2)
18		Математические основы шифров перестановки. Простейший шифр перестановки
19		Магические квадраты и решетки
20		Блочные шифры
21		Американский стандарт шифрования данных DES
22		Американский стандарт шифрования данных DES
23		Российский стандарт шифрования данных

24		Промежуточное тестирование (тест № 3)
25		Математические основы асимметричной криптографии. Алгебра матриц
26		Понятие односторонней функции
27		Понятие односторонней функции
28		Понятие односторонней функции
29		Открытое распределение ключей. Алгоритм Диффи—Хеллмана
30		Открытое распределение ключей. Алгоритм Диффи—Хеллмана
31		Что такое цифровая электронная подпись?
32		Система RSA
33		Тест в рамках промежуточной аттестации (тест № 4)
34		Практическая контрольная работа