Всероссийский фестиваль методических разработок
"КОНСПЕКТ УРОКА", 2012-2013 учебный год

Клинковская Марина Викторовна

Муниципальное бюджетное общеобразовательное учреждение

гимназия № 7 г. Балтийска Калининградской области

МЕТОДЫ ШИФРОВАНИЯ ТЕКСТОВОЙ ИНФОРМАЦИИ

(8 класс)

Цели урока:

Образовательные:

— сформировать у учащихся понятие о шифровании как о методе защиты информации;

— рассмотреть различные способы шифрования, научить шифрации, дешифрации.

Развивающие:

— развивать навыки самостоятельной работы и работы в группах;

— формировать у учащихся целостное восприятие окружающего мира.

Воспитательные:

— формировать познавательный интерес учащихся;

— способствовать освоению учащимися способов эффективного взаимодействия в процессе учебной деятельности;

— воспитывать потребность в оценке своей деятельности;

— воспитывать нравственное отношение к понятиям Родина, совесть.

Тип урока: Комбинированный урок

Формы организации учебной деятельности: фронтальная, групповая, индивидуальная

Необходимое техническое оборудование и ПО: персональный компьютер учителя, проектор, персональные компьютеры учащихся, программа MyTest.

Структура и ход урока:

№	Этап урока	Деятельность учителя	Деятельность ученика	Время, мин
Перед началом урока на каждое рабочее место выкладывается стопка листов с заданиями 1-4 и зеленый/голубой лист, тыльной стороной кверху. Вверху должен лежать лист с заданием 1, и далее все листы по порядку.				
1	Организационный	Приветствие. Отметить отсутствующих.		2 мин
2	Повторение правил ТБ	1. Демонстрация иллюстраций к правилам ТБ. Вопрос — попытаться сформулировать правило ТБ по картинке. 2. Координация действий учащихся. Акцент внимания учащихся на правильных ответах. 3. В конце повторения правил учащимся задаются вопросы: — был ли записан текст правил ТБ на картинках? — какими другими словами можно заменять слова «скрытая», «зашифрованная» информация? («Спрятанная», «закодированная», и т.д.) — для чего шифруют информацию? — когда возникает необходимость закодировать информацию? Вопросы о целях шифрования *текстовой* информации. Координация	Фронтальная работа. Формулируют правила техники безопасности по картинкам. Учащиеся делают вывод о том, что, не смотря на отсутствие текстовой информации (информация была «скрыта», «зашифрована»), они смогли понять смысл, который несет каждая иллюстрация. Ответы на вопросы.	5 мин

		действий учащихся и степени их вовлеченности в образовательный процесс, организация индивидуальной работы.		
3	Изучение новой темы	Объявление темы урока, цели. Беседа по вопросу «Когда люди начали шифровать информацию? **Шифр Цезаря.** Объяснение способа шифрования. Решение примеров 1,2. Проверка результатов. **Шифр Вижинера.** Объяснение способа шифрования (Отличие от шифра Цезаря — не постоянная, а *переменная величина сдвига, использование ключевого слова*)	Ответы на вопрос. Работа с листами заданий. Пример 1. Зашифровать слово БАЙТ. Пример 2. Расшифровать слово КГЬЛХГ Пример 3. Закодировать с помощью шифра Вижинера слово АЛГОРИТМ, проверка у доски — 2 чел.	12 мин
4	Промежуточный контроль знаний	Вопросы: — Чем отличается шифр Вижинера от шифра Цезаря? — Какой шифр более надежен? Почему? — Какой шифр показался более интересным? Задание: расшифровать слово НУЛТХСЖУГЧЛВ (КРИПТОГРАФИЯ). Беседа о происхождении лексическом значении этого слова. Осуществляется	Учащиеся отвечают на вопросы. Расшифровка.	

		контроль за выполнением работы. Обеспечивается положительная реакция учеников на ответы и высказывания одноклассников, толерантное отношение к мнению товарища.		
5	**Физкультминутка — 2 мин**			
6	Рассадка учащихся для групповой работы			
7	Продолжение изучения новой темы	Тарабарская грамота. Объяснение способа шифрования. Группы получают задания для расшифровки. (Зеленые листы: «Тарабарская грамота – тайнопись, применявшаяся ранее в России для дипломатической переписки» Синие листы: «Вопрос, умеет ли компьютер думать, имеет не больше смысла, чем вопрос, умеет ли подводная лодка плавать» — Э.вайб Дейкстра.) Обсуждение фраз. Согласны ли с утверждением ученого Э.вайб Дейкстра? Почему? Рассказ об авторе книги «Может ли машина мыслить» Алане Тьюринге — математике, шифровальщике, криптографе. О раскрытии секрета шифровальной машины «Энигма».	Учащиеся разделены на группы, выбирается капитан, который будет озвучивать ответ. Группы расшифровывают данные фразы, каждая дает свой ответ. Обсуждение расшифрованных фраз.	12 мин

		Рассказ о шифровании информации в нашей стране. Котельников. Развитие после войны индустрии ЭВМ и шифровании с их помощью.		
8	Контроль знаний учащихся. Компьютерное тестирование с выставлением оценки.	Осуществляется контроль за выполнением работы.	Работа за компьютерами — выполнение теста. После выполнения проводится фронтальная проверка.	10 мин
9	Подведение итогов урока. Рефлексия.	Подведение итога урока вместе с учащимися, мотивация учащихся на углубление знаний по данной теме. Оценка работы учащихся на уроке. Учащимся раздаются первый и последний листы методического пособия — продукт деятельности учеников на уроке + теоретические сведения.	Подведение итога урока. Учащиеся отмечают наиболее интересные моменты, наиболее удачные ответы. Дают оценку продуктивности занятия.	2 мин
10	Задание на дом	Домашнее задание и список литературы — на слайде презентации		2 мин
11	Окончание урока			

Теоретические сведения к уроку информатики и ИКТ

МЕТОДЫ ШИФРОВАНИЯ ТЕКСТОВОЙ ИНФОРМАЦИИ

(8 класс)

1. **Гай Юлий Цезарь (102 или 100, Рим — 44 до н.э., там же),** выдающийся римский полководец, крупнейший политический деятель, оратор и писатель. Занимал должности трибуна, эдила, консула, наместника, великого понтифика. В ходе галльских походов 58-51 гг. завоевал всю заальпийскую Галлию, покорил 300 племен, сражался с 3 миллионами человек, уничтожил миллион варваров, получил огромные материальные ресурсы. У Цезаря было мощное, всецело ему преданное войско (10 легионов). Находясь у власти, провел ряд важных реформ: щедро раздавал права римского и латинского гражданства провинциалам, наделил землей своих ветеранов, наладил контроль за сбором налогов, осуществил перепись граждан по всей Италии, провел монетную и календарную реформы.

2. **Шифр Цезаря.** Один из самых первых известных методов шифрования. Если Гай Юлий Цезарь и не сам изобрел этот метод, то активно им пользовался. Метод основан на замене каждой буквы шифруемого текста на другую путем смещения в алфавите от исходной буквы на фиксированное количество символов (*сдвиг*), причем алфавит читается по кругу, т.е. после буквы *я* следует рассматривать букву *а*. Например, слово БАЙТ при смещении на два символа вправо (т.е. *сдвиг k = 2*), кодируется словом ГВЛФ.

3. **Блез де Вижинер (1523-1596),** французский дипломат, криптограф и алхимик. В возрасте 17 лет он поступил младшим секретарем на дипломатическую службу. Дважды, в разные годы службы, посещал с дипломатическими миссиями Рим. В этих поездках, он познакомился с книгами о криптографии и самой криптографией. Изобрел шифр с переменной величиной сдвига. Выйдя на пенсию в возрасте 47 лет, он пожертвовал 1000 ливр — свой годовой доход — беднякам Парижа.

4. **Шифр Вижинера.** Шифр с переменной величиной сдвига. Величина сдвига задается некоторым ключевым словом. Для каждой буквы ключевого слова определяется ее порядковый номер в алфавите. Набор чисел - порядковых номеров букв ключевого слова записывается под буквами кодируемого слова, начиная с первой буквы, и до конца (под одной буквой записывается одно число). Число под буквой показывает, на сколько позиций нужно «сдвинуть» кодируемую букву.

5. **Криптография —** (с греческого) «криптос» — тайный, скрытый, «графо» — пишу, ТАЙНОПИСЬ. Наука о принципах, средствах и методах преобразования информации для защиты ее от несанкционированного доступа и искажения.

6. **Тарабарская грамота —** тайнопись, применявшаяся ранее в России для дипломатической переписки. (На уроке «Методы шифрования текстовой информации» ученикам не объясняется, что такое тарабарская грамота – информацию о ней учащиеся расшифруют сами, выполняя задание № 5 – голубой лист). При шифровании тарабарской грамотой буквы, обозначающие гласные звуки, а также буквы Ъ, Ь не кодируются, остаются без изменения.

Согласные буквы алфавита выписываются в две строки: в первой строке — по-порядку, во второй строке — в обратном порядке:

б	в	г	д	ж	з	к	л	м	н	п	р	с	т	ф	х	ц	ч	ш	щ
щ	ш	ч	ц	х	ф	т	с	р	п	н	м	л	к	з	ж	д	г	в	б

Правило шифрования согласных букв: первая буква в любой строке таблицы меняется на последнюю в той же строке, вторая — на предпоследнюю, и т.д.

Проанализировав таблицу, можно увидеть «симметрию», красным цветом выделены буквы вокруг «центра симметрии» таблицы. Эта таблица — ключ шифра — может быть оформлена короче:

б	в	г	д	ж	з	к	л	м	н
щ	ш	ч	ц	х	ф	т	с	р	п

В этом шифре каждая согласная меняется на букву, расположенную непосредственно над ней или под ней в таблице.

7. **Алан Матисон Тьюринг (1912 – 1954),** английский математик, логик, криптограф, оказавший существенное влияние на развитие информатики. Автор книги «Может ли машина мыслить». Кавалер Ордена Британской империи (1945). Предложенная им в 1936 году абстрактная вычислительная «Машина Тьюринга» позволила формализовать понятие алгоритма и до сих пор используется во множестве теоретических и практических исследований. Во время Второй мировой войны Тьюринг работал в британском криптографическом центре, где возглавлял одну из групп, занимавшихся расшифровкой закодированных немецкой шифровальной машиной «Энигма» сообщений воздушного и военно-морского флотов фашистской Германии. В начале 1940 года он разработал дешифровальную машину «Бомба», позволявшую читать сообщения люфтваффе, после этого англичане оказались в курсе всех деталей операций, планируемых воздушным флотом Геринга. В 1942 году Тьюринг принял участие в создании новой шифровальной машины «Колосс». Эта машина легко победила «Энигму». Тьюринг своим математическим гением, несомненно, приблизил победу над фашизмом.

8. **Владимир Александрович Котельников, (1908-2005), (24 августа (6 сентября) 1908, Казань — 11 февраля 2005, Москва) —** советский и

российский учёный в области радиотехники, радиосвязи и радиолокации планет.

В 1939 году Котельникову было поручено решение важной государственной задачи — создание шифратора для засекречивания речевых сигналов с повышенной стойкостью к дешифрованию. Сложная засекречивающая аппаратура «Соболь» разработанная под руководством Котельникова, использовалась в действующей армии. Эта аппаратура обеспечивала шифрование речевых сигналов для закрытой радиосвязи, и зашифрованные сигналы не поддавались декодированию.

9. После войны стала развиваться **индустрия электронно-вычислительных машин**, с помощью которых можно было надежно кодировать информацию. Шифрование текстов и защита информации в настоящее время осуществляются с помощью компьютеров с использованием сложнейших математических алгоритмов.

Литература:

1. Агафонова И.В., Дмитриева О.М. Линейные регистры сдвига и поточные шифры // Компьютерные инструменты в школе, 2011. №2. С.3-8

2. Златопольский Д.М. Простейшие методы шифрования текстовой информации. – М.:Чистые пруды, 2007.-32с.-(Библиотечка «Первого сентября», серия «Информатика». Вып.5(17)/2007.

3. Школьный биографический словарь. Составитель и гл. редактор профессор А.П.Горкин. ООО «Издательство «РОСМЭН-ПРЕСС», 2002.

4. Энциклопедия для детей. [т.22.] Информатика/ред. Коллегия: М. Аксенова, Е. Журавлева, А. Леонов. – М.:Мир энциклопедий Аванта+, Астрель, 2008.- 624 с.: ил.//Борисенко В. Современная криптография.-С.575.

5. Энциклопедия для детей.[т.22.] Информатика/ред. Коллегия: М. Аксенова, Е. Журавлева, А. Леонов. – М.: Мир энциклопедий Аванта+, Астрель, 2008.- 624 с.: ил.//Борисенко В. Устройство «Энигмы».-С.576.