

Методическая разработка
Открытый урок по учебной дисциплине
«Основы информационной безопасности»

Специальность: Организация и технология защиты информации

Группа: ОиТЗИ-15

Дата: 08.02.2016

Разработала: преподаватель ГБПОУ РС(Я) Покровский колледж, Обоюкова А.Л.

Цель: познакомить студентов с понятием криптографии, шифрованием и дешифрованием текстов различными методами

Тип урока: изучение нового материала.

Методы: объяснительно-иллюстративный, частично-поисковый.

Цели урока:

- создать условия для повышения познавательного интереса к предмету.
- способствовать развитию аналитико-синтезирующего мышления.
- способствовать формированию умений и навыков, носящих общенаучный и общеинтеллектуальный характер.

Задачи:

Образовательные:

- изучить и систематизировать знания основных понятий (код, кодирование, криптография) по теме;
- познакомить со способами шифрования и дешифрования информации;
- отрабатывать умения читать шифровки и шифровать информацию;

Развивающие:

- развивать познавательную деятельность и творческие способности студентов;
- формировать логическое и абстрактное мышление;
- развивать умение применять полученные знания в нестандартных ситуациях;
- развивать воображение и внимательность;

Воспитательные:

- воспитывать коммуникативную культуру,
- развивать положительное эмоциональное отношение к предмету, настойчивость в достижении цели, находчивость.

Формы организации деятельности на уроке: словесные, наглядные, практические.
Оборудование, материалы и программное обеспечение: интерактивная доска, ПК, презентация преподавателя, раздаточный материал.
Информационные ресурсы:

1 В. П. Мельников Информационная безопасность: Учеб. Пособие для сред. Проф. Образования/В.П.Мельников, С.А.Клейменов, А.М.Петраков; Под ред. С.А.Клейменова. – М.: Издательский центр «Академия», 2013. – 336 с.

2 http://www.if4.ru/kriptograficheskie_tekhnologii.html - криптография, криптографические технологии

Тема занятия: «Шифрование и дешифровка текстов различными методами»»

Цель: изучить методы шифрования на примере простейших классических шифров

Материальное обеспечение:

Персональный компьютер, мультимедийный проектор, демонстрационный экран;
Электронные презентации;
Карточки-задания.

План-сценарий занятия:

1. Организационный момент (5 минут)

Приветствие, проверка присутствующих на занятии.

2. Объявление темы и целей занятия

Сегодня мы с вами продолжим изучение криптографических средств защиты информации.

Тема нашего занятия «Шифрование и дешифровка текстов различными методами»».

Сегодня нам предстоит изучить методы шифрования на примере простейших классических шифров.

Мотивация:

Вам предстоит участвовать в разработке текстов различными методами.

В состав любой компьютерной системы, обязательно входит подсистема безопасности, которая обеспечивает защиту информации, хранимой, обрабатываемой и передаваемой в системе.

Мы с вами уже знаем, что для реализации программно-технических мер обеспечения информационной безопасности применяются криптографические средства. Поэтому все, что вы сегодня узнаете, пригодится вам в будущей профессиональной деятельности.

3. Актуализация опорных знаний (10 минут)

На прошлом занятии мы изучили основные понятия, термины и определения криптологии. Прежде, чем начать изучать новый материал, нам необходимо проверить, хорошо ли вы усвоили понятийный материал, который понадобится нам для изучения новой темы.

Устный опрос (сопровождается анимированной презентацией «Основные понятия криптологии»: после ответа обучающегося на слайде появляется правильный ответ):

1. Что такое криптология?
2. Дайте определение терминам криптографии: алфавит, текст. Приведите примеры алфавитов.
5. Что такое шифрование, дешифрование, ключ?

Молодцы, я вижу, что вы хорошо усвоили изученный на прошлом занятии материал и готовы к изучению новой темы.

А теперь такой вопрос: Как давно, по вашему мнению начала применяться криптография?
(Варианты ответов)

Ответ на этот вопрос мы сейчас узнаем, послушав внимательно сообщение, которое нам подготовил(а)

Сообщение (доклад) «История криптографии».

4. Объяснение нового материала (40 минут)

(сопровождается анимированными слайдами презентации «Шифрование и дешифровка текстов различными методами»[@])

Запишите тему и план урока:

Начнем с самых простых шифров одноалфавитной (моноалфавитной) замены – символы шифруемого текста заменяются другими символами, взятыми из одного алфавита.

В Древней Греции (II в. до н. э.) был известен шифр, который создавался с помощью **квадрата Полибия**.

[@] Таблица для шифрования представляла собой квадрат 6 x 6, строки и столбцы которого пронумерованы (в исходном греческом шифре с пятью столбцами и пятью строками, т.к. число букв в русском алфавите отличается от числа букв в греческом алфавите, поэтому и размер таблицы выбран иным (квадрат 6 x 6)). В каждую клетку той таблицы записывается одна буква. В результате каждой букве соответствует пара цифр, и шифрование сводилось к замене буквы парой цифр. В шифрограмме первым указывается номер строки, а вторым — номер столбца.

В квадрате Полибия столбцы и строки можно маркировать не только цифрами, но и буквами. Порядок расположения символов в квадрате Полибия является ключом.

Идею квадрата Полибия проиллюстрируем таблицей с русскими буквами.

Шифр Цезаря реализуется заменой каждой буквы в сообщении другой буквой этого же алфавита, отстоящей от нее в алфавите на фиксированное число букв.

В своих шифровках Цезарь заменял букву исходного открытого текста буквой, отстоящей от исходной буквы впереди на три позиции.

Циклический шифр Цезаря получается заменой каждой буквы открытого текста буквами этого же алфавита, расположенными впереди через определенное число позиций, например через три позиции. Циклическим он называется потому, что при выполнении замены вслед за последней буквой алфавита вновь следует первая буква алфавита. В данном случае ключом является величина сдвига (число позиций между буквами).

Используем шифр Цезаря. Предположим, что требуется зашифровать сообщение. Запишем фрагменты русского алфавита и покажем, как выполняется шифрование (порядок замены):

В результате проведенного преобразования получится шифрограмма:

Ё Ж З Ж З Е Г.

Число ключей этого шифра невелико (оно равно числу букв алфавита). Не представляет труда вскрыть такую шифрограмму перебором всех возможных ключей. Недостатком шифра Цезаря является невысокая криптостойкость. Объясняется это тем, что в зашифрованном тексте буквы по-прежнему располагаются в алфавитном порядке, лишь начало отсчета смещено на несколько позиций.

Повысить криптостойкость позволяют шифры многоалфавитной замены (или *полиалфавитные подстановки*). При этом для замены символов открытого текста используют символы нескольких алфавитов. К наиболее известным разновидностям многоалфавитной замены относятся *одноконтурная* (обыкновенная и монофоническая) и *многоконтурная*.

Метод перестановок

Идея этого метода криптографии заключается в том, что запись открытого текста и последующее считывание шифровки производится по разным путям некоторой геометрической фигуры (например, квадрата).

Для пояснения идеи возьмем квадратную таблицу (матрицу) 8x8, будем записывать текст последовательно по строкам сверху вниз, а считывать по столбцам последовательно слева направо.

Ключом в данном случае является размер матрицы, порядок записи открытого текста и считывания шифрограммы. Естественно, что ключ может быть другим

Для повышения криптостойкости методы замены и перестановки нередко используют в сочетании с *аддитивным* методом или методом гаммирования. (этот метод вы изучите самостоятельно дома или в библиотеке по учебнику).

Если блоки открытого текста состоят из одинаковых букв, то криптограмма тоже будет

Схема шифрования **Вижинера**. Рассмотрим еще один шифр многоалфавитной замены, который был описан в 1585 г. французским дипломатом Блезом де Вижинером.

Шифрование производится с помощью так называемой таблицы Вижинера. (Каждая строка в этой таблице соответствует одному шифру простой замены (типа шифра Цезаря).

Первая строка таблицы Вижинера – строка букв открытого текста, а первый столбец таблицы – столбец букв ключа.

При шифровании открытое сообщение записывают в строку, а под ним помещают ключ.

Если ключ оказывается короче сообщения, то ключ циклически повторяют. Шифровку получают, находя символ в матрице букв шифрограммы. Символ шифрограммы находится на пересечении столбца с буквой открытого текста и строки с соответствующей буквой ключа.

За компьютером:

Выполнить действия: создать свою учетную запись и придумать пароль, затем зайти администратор и удалить свой пароль.

Подведение итогов занятия и выдача домашнего задания (5 минут)

Понравился вам сегодняшний урок? Было интересно? Мне тоже понравилась ваша работа на занятии.

Очень интересное сообщение и презентацию подготовил(а) ... (*фамилия*). Какую оценку он(а) заслужил(а)? Конечно «отлично».

Также хорошо поработали сегодня (*фамилии*)....., они получают оценку «4».

Остальные, я уверена, проявят себя на следующем занятии, которое будет практическим.

Запишите домашнее задание.