shkolanauki.ru

Актуальность внедрения курса криптографии в школьную программу

Беляков Денис Александрович, магистрант
Кубанский государственный университет (г. Краснодар)

Аннотация. *В статье рассматривается вопрос внедрения курса криптографии в школы. Готовы ли ученики к изучению соответствующего курса и с какого возраста его лучше вводить.*

Ключевые слова: *криптография, актуальность, курс, школьная программа.*

В связи с бурным развитием науки и техники почти все данные о человеке перешли в электронный формат. В школах появились электронные дневники, в больницах электронные карты, даже в магазинах мы расплачиваемся электронными деньгами. Сейчас почти все ученики школ практически всё свободное время проводят в телефонах и компьютерах, постоянно общаясь между собой. Но большинство учеников даже не подозревают, что перед отправкой сообщения, оно тщательно шифруется. Именно вопросами грамотного шифрования данных уже долгое время занимается криптография. Криптография – составляющая криптологии, которая занимается исследованием и разработкой методов шифрования данных. У учеников очень мало представления о криптографии и в дальнейшем при выборе специальности, мало кто задумывается о поступлении в ВУЗы именно на эти направления. В свою очередь государству требуется всё больше людей, реально разбирающихся в сфере криптографии. В связи с этим встал вопрос об актуальности внедрения курса криптографии в школьную программу. Целью такого курса является:

1. Развитие у учащихся логического мышления.
2. Получению учащимися знаний по основам программирования.
3. Получению знаний по криптографии для дальнейшего использования в ВУЗах.
4. Формирование у учащихся исследовательских навыков.
5. Мотивация учащихся на дальнейшее изучение математики и информатики.

Чтобы разобраться, нужен ли в школах данный курс, в качестве эксперимента проведено пять уроков среди учащихся 7-х, 8-х, 9-х, 10-х и 11-х классов. Классы выбраны таким образом, чтобы понимать, с какого возраста лучше всего вводить данный курс.

Каждый урок был разбит на 4 части. В первой части урока ученикам рассказано что такое криптография, краткая ее история и роль в современном мире. Даны некоторые определения из криптографии:

1. Ключ – это информация, которая необходима для шифрования и расшифровывания сообщений.
2. Алгоритм - набор правил (инструкций), определяющих содержание и порядок операций по шифрованию и дешифрованию информации.
3. Шифрование - процесс применения шифра к защищаемой информации, т.е. преобразование исходного сообщения в зашифрованное.
4. Дешифрование - процесс, обратный шифрованию, т. е. преобразование шифрованного сообщения в исходное.

В следующем этапе урока ученикам продемонстрированы некоторые простейшие шифры:

1. Шифр Цезаря
2. Шифр простой замены
3. Шифр Полибия
4. Шифр Виженера

Каждый вариант шифра был сопровожден соответствующим примером.

К окончанию урока ученикам предложено решить по одному заданию из ранее продемонстрированных шифров.

Задача №1. Шифр Цезаря.

Используя шифр Цезаря, зашифровать сообщение: шифр назван в честь римского полководца Гая Юлия Цезаря. При шифровании использовать ключ 5, алфавит русский.

Задача №2. Шифр простой замены.

Используя шифр простой замены, зашифровать сообщение: пусть будет так, как мы хотели. Ключ шифра выбрать самостоятельно и занести в таблицу.

Задача №3. Шифр Полибия.

Использовать русский алфавит. Буквы алфавита в произвольном порядке вписать в прямоугольник 5х6.

	1	2	3	4	5
1	К	Р	Б	Ю	Ы
2	Ф	Т	А	Щ	О
3	Д	Н	Я	И	Е
4	С	Ь	В	М	Ш
5	Э	Г	Л	Ц	П
6	Ж	У	Х	З	Ч

Рисунок 1. **Пример прямоугольника**.

Зашифровать сообщение: криптография.

Задача №4. Шифр Виженера.

Используя шифр Виженера, зашифровать сообщение: компьютер. Ключевое слово: ваза.

При анализе ответов, предоставленных учениками на предложенные задачи, получены следующие данные:

Таблица 1. Результаты тестирования

Количество правильно решенных задач	7 класс (17 учеников)	8 класс (16 учеников)	9 класс (13 учеников)	10 класс (14 учеников)	11 класс (17 учеников)
4	7 уч.	7 уч.	5 уч.	8 уч.	11 уч.
3	5 уч.	4 уч.	4 уч.	4 уч.	5 уч.
2	3 уч.	4 уч.	3 уч.	2 уч.	1 уч.
1	2 уч.	1 уч.	1 уч.	0 уч.	0 уч.
0	0 уч.	0 уч.	0 уч.	0 уч.	0 уч.

В конце занятия, проведен опрос учеников на заинтересованность к предмету криптографии и актуальность внедрения курса в школьную программу. Подавляющее число тестируемых хотели бы больше узнать о криптографии и готовы посещать данный курс. Заинтересованность учеников составила около 70% от общего числа тестируемых.

Из конечных полученных результатов проведенных уроков можно сделать следующие выводы. Проводить курс криптографии в школе нужно, но не стоит его делать обязательным предметом для всех, чтобы не нагружать учеников дополнительным объемом заданий. Вводить курс криптографии стоит не раньше 10-11 классов, т.к. по результатам тестирования именно эти классы лучше справились с поставленной задачей. Обязательно же вводить курс криптографии стоит для учеников 10-11 классов, выбравших информационно-технологический профиль или другие, тесно связанные с углубленным изучением математики и информатики. Это сформирует у учащихся исследовательские навыки, поспособствует развитию логического мышления и даст первоначальные основы программирования. Для 7-9 классов стоит проводить лишь ознакомительные уроки, где можно рассказывать историю появления криптографии и разбирать простейшие задачи. Данные уроки дадут представление учащимся о криптографии и будут являться одним из аргументов при будущем выборе профиля.

Литература:

1. М.Г.Адигеев. Введение в криптографию. Методические указания для студентов механико-математического факультета. Ростов-на-Дону 2002 г. 35стр.