УДК 512.643

БАЙЗАКОВ А.Б., МОМБЕКОВ А.Д., ДЖЭЭНБАЕВА Г.А.
Институт математики НАН КР,
КНУ им. Ж. Баласагына, Бишкек
BAIZAKOV A.B., MOMBEKOV A.D., DJEENBAEVA G.A.
Institute of Mathematics of the National Academy of Sciences of Kyrgyz Republic,
J. Balasagyn KNU, Bishkek

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ И МАГИЧЕСКИЕ МАТРИЦЫ

Магиялык квадраттар жана маалыматтык коопсуздук
Information security and magic matrices

Аннотация: *Дано само понятие «информационная безопасность», описаны основные требования к информационной безопасности даны основные методы защиты информации, даны криптографические методы защиты информации в автоматизированных системах и шифрование по магическому квадрату. Применение метода декомпозиции для магических квадратов. Приведены конкретные примеры.*

Аннотация: *"Маалыматтык коопсуздук» түшүнүгү берилди, маалыматтык коопсуздуктун негизги талаптары келтирилди жана маалыматты коргоонун негизги усулдары берилди. Автоматаштырылган системалардагы маалыматты коргоонун криптографикалык усулдары жана магиялык квадрат боюнча шифрлөө берилди. Магиялык квадраттар үчүн декомпозиция усулун колдонуу. Конкреттүү мисалдар келтирилди.*

Annotation: *The very concept of "information security" is given, the basic requirements for information security are described, and the basic methods of information protection are given. Given the cryptographic methods of protecting information in automated systems and encryption on the magic square. Application of the method of decomposition for magic squares. Concrete examples are given.*

Ключевые слова*: информационная безопасность, магический квадрат, методы защиты информации, метод декомпозиции для магических квадратов, шифрование по магическому квадрату.*

Урунттуу сөздөр*: маалыматтык коопсуздук, магиялык квадрат, маалыматты коргоонун усулдары, магиялык квадраттар үчүн декомпозиция усулу, магиялык квадрат боюнча шифрлөө.*

Keywords: *information security, magic square, information protection methods. decomposition method for magic squares, encryption by magic square.*

Информационная безопасность- состояние сохранности и защищенность информационных данных, законных прав пользователей в информационной сфере. Информационная безопасность – это процесс обеспечения конфиденциальности, целостности и доступности информации.

Конфиденциальность: Разрешение доступа к информации только авторизованным пользователям.

Целостность: Гарантия достоверности и полноты данных, а также методов их обработки.

Доступность: Гарантия доступа к данным и связанным с ней процедурам авторизованных пользователей по мере необходимости.

Под информационной безопасностью будем понимать все моменты, связанные с определением, достижением и поддержанием конфиденциальности, целостности, доступности, безотказности, подотчётности, аутентичности и достоверности данных, а также средств их обработки.

Безопасность информации - состояние защищенности информации, при котором обеспечиваются ее конфиденциальность, доступность и целостность.

Безопасностьинформации обеспечивается отсутствием недопустимого риска, связанного с утечкой данных по техническим каналам, несанкционированными и непреднамеренными воздействиями на информации, а также на другие ресурсы автоматизированной информационной технологии.

Рассмотрим **основное пункты способов защиты данных.**

Создание препятствий - это способы физического преграждения нарушителю пути к защищаемых данных (аппаратуре, носителям информации и т. д.).

Управление доступом - это способ защиты данных регулированием использования всех ресурсов компьютерной информационной технологии (структур баз данных, программных и технических средств).

Защита от доступа к ресурсам компьютера злоумышленника: а) присвоение терминалам, каналам, программным файлам непростых имен и кодов, б) убеждаться в подлинности информационных данных системы, т.е. убедиться, что лицо или устройство, сообщившее идентификатор соответствует действительности) проверить права пользователя на доступ к системе, г) автоматически регистрировать всех пользователей.

Маскировка - это способ защиты данных путем ее криптографического закрытия (шифрования).

Регламентация - это способ защиты данных и создающий такие условия автоматизированной обработки, хранения и передачи защищаемых данных, при которых возможности несанкционированного доступа к ней сводились бы к минимуму.

Принуждение - это способ защиты, при котором пользователи и персонал системы вынуждены соблюдать правила обработки, передачи и использования защищаемых данных под угрозой материальной, административной, а также уголовной ответственности.

Рассмотренные способы обеспечения безопасности реализуются на практике за счет применения различных средств защиты данных, таких как технические, программные, организационные, законодательные.

Далее, более подробно остановимься на способе маскировки данных.

Криптографические способы защиты данных в автоматизированных системах. Криптографические способы защиты данных в автоматизированных системах могут применяться как для защиты данных, так и для закрытия данных, передаваемой между различными элементами системы по каналам связи. Криптографическое преобразование как способ предупреждения несанкционированного доступа к данным имеет многовековую историю. В настоящее время разработано большое количество различных способов шифрования, созданы теоретические и практические основы их применения. Подавляющее число этих способов может быть успешно использовано и для закрытия информации.

Итак, криптография дает возможность преобразовать данные таким образом, что ее прочтение (восстановление) возможно только при знании ключа.

В качестве данных, подлежащих шифрованию и дешифрованию, рассматриваются тексты, построенные на некотором алфавите. Эти термины обозначают следующее:

Алфавит - конечное множество знаков, используемых для кодирования данных.

Текст - упорядоченный набор из элементов алфавита.

В качестве примеров алфавитов, используемых в современных информационных системах можно привести следующее:

алфавит Z33 - 32 буквы русского алфавита и пробел;

алфавит Z256 - символы, входящие в стандартные коды ASCII и КОИ-8;

бинарный алфавит - Z2 = {0,1};

восьмеричный алфавит или шестнадцатеричный алфавит;

Шифрование - это преобразовательный процесс: исходный текст, который носит также название открытого текста, заменяется шифрованным текстом.

Дешифрование - это обратный шифрованию процесс. На основе ключа шифрованный текст преобразуется в исходный.

Ключ - это информация, необходимая для беспрепятственного шифрования и дешифрования текстов.

Криптографическая система представляет собой семейство T преобразований открытого текста. Члены этого семейства индексируются, или обозначаются символом k; параметр k является ключом. Пространство ключей K - это набор возможных значений ключа. Обычно ключ представляет собой последовательный ряд букв алфавита.

Криптографические системы разделяются на симметричные и с открытым ключом.

В симметричных криптографических системах и для шифрования, и для дешифрования используется один и тот же ключ.

В системах с открытым ключом используются два ключа - открытый и закрытый, которые математически связаны друг с другом. Данные шифруются с помощью открытого ключа, который доступен всем желающим, а расшифровывается с помощью закрытого ключа, известного только адресату сообщения.

Применение метода декомпозиции для магических квадратов. Далее отметим, что магические квадраты больших размеров могли быть хорошей основой для надежной системы шифрования в криптографии.

В данной работе показано возможное разнообразие констант квадратов в подблоках при построении методом декомпозиции M матриц высокого порядка.

В качестве примера рассмотрим M матрицу сотого порядка.

Оказывается, что подблоки блоков по 400 цифр можно расположить по различной схеме: а) методом сдвига или б) методом арифметической прогрессии. При этом константы квадратов в каждом случае разные, однако, общие константы квадратов остаются неизменными: константа первого блока (рис.1) - 4010, второго блока (рис.2) - 12010,…, двадцать четвертого блока- 188010 и константа последнего

двадцать пятого блока - 196010, т.е. появляется арифметическая прогрессия состоящая из 25 членов с первым членом $a_1 = 4010$, с разностью $d = 8000$.

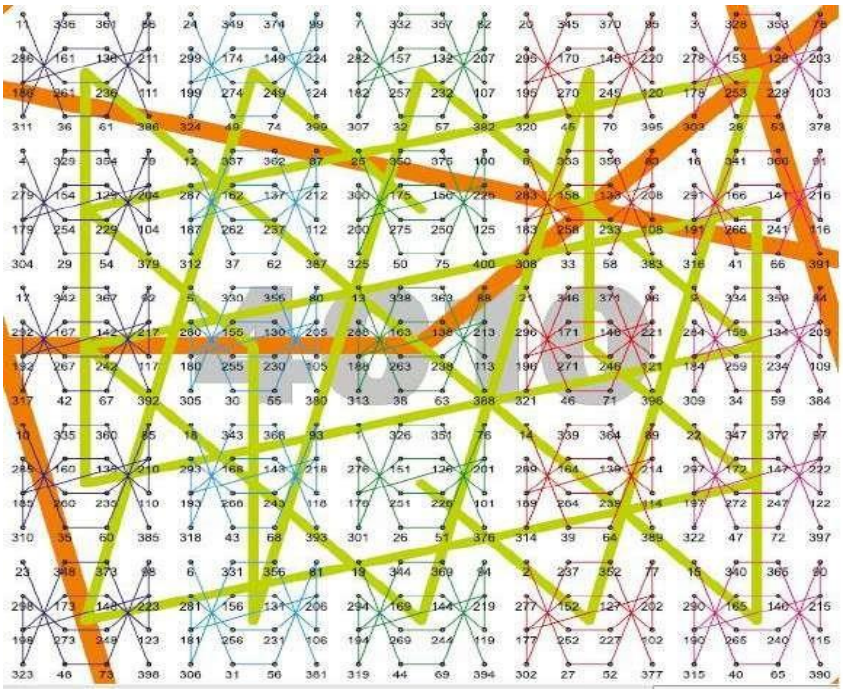

Рисунок 1. Фрагмент M матрицы сотого порядка. Первый блок

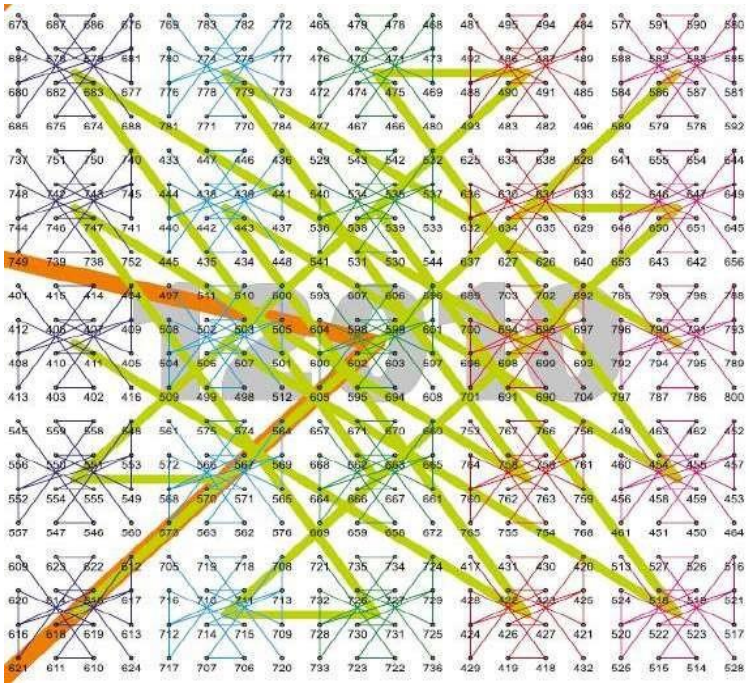

Рисунок 2. Фрагмент M *матрицы сотого порядка. Второй блок*

Константы квадратов при использовании арифметической прогрессии в подблоках

Рассмотрим 1 подблок 1 блока. В нем 16 чисел и они расположены по закону арифметической прогрессии $d = 25$, $a_1 = 1,...,a_{16} = 376$; во втором подблоке 1 блока тоже 16 чисел с

$d = 25$, $a_1 = 2,...,a_{16} = 377$; …; в 25ом подблоке: $d = 25$, $a_1 = 25,...,a_{16} = 400$. Ясно, что константы квадратов будем искать по формуле $S = a_1 + a_{16} + 4$:

2

754, 758, ..., 850. Т.е. имеем арифметическую прогрессию с $a_1 = 754$, $d = 4$, $a_{25} = 850$. Если полученную арифметическую прогрессию расположить, например, по образцу

$$\begin{pmatrix} 11 & 24 & 7 & 20 & 3 \\ 4 & 12 & 25 & 8 & 16 \\ 17 & 5 & 12 & 21 & 9 \\ 10 & 16 & 1 & 14 & 22 \\ 23 & 6 & 19 & 2 & 15 \end{pmatrix} \quad (1)$$

т.е. в виде

$$\begin{pmatrix} 794 & 846 & 778 & 830 & 762 \\ 766 & 798 & 850 & 782 & 814 \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ 818 & 770 & 802 & 830 & 786 \end{pmatrix}$$

$$\begin{pmatrix} & & \\ 790 & 822 & 754 & 806 & 838 \\ & & \\ 842 & 774 & 826 & 758 & 810 \end{pmatrix} \qquad (2)$$

M матрица (2) имеет константу квадрата 4010:

$$S = a + a_1 + a_{25} + a_5 + a_{21} = 754 + 850 + a_5 + 4010.$$

$$2 \qquad 2$$

Константы квадратов при использовании метода сдвига в подблоках.

Теперь, рассмотрим 1й подблок 1го блока. В нем 16 чисел и их расположим по образцу

$$\begin{pmatrix} 1 & 15 & 14 & 4 \\ 12 & 6 & 7 & 9 \\ 8 & 10 & 11 & 5 \\ 13 & 3 & 2 & 16 \end{pmatrix}$$

Ясно, что константой квадрата является число 34. Второй подблок 1го блока располагается, например, в виде

$$\begin{pmatrix} 17 & 31 & 30 & 20 \\ 28 & 22 & 23 & 25 \\ & 26 & 27 & \\ 24 & 19 & 18 & 21 \\ & & & 32 \\ 29 & & & \end{pmatrix}$$

Константа квадрата второго подблока есть

$$S = S_4 + mn = 34 + 16 \cdot 4 = 98.$$

Двадцать пятый подблок 1го блока располагаются, например, в виде

$$\begin{pmatrix} 385 & 399 & 398 & 388 \\ 396 & 390 & 391 & 393 \\ 392 & 394 & 395 & 389 \\ 397 & 387 & 386 & 400 \end{pmatrix}$$

Константа квадрата которой является число $S = 34 + 384 + 4 + 1570 = 1992$.

Итак, имеем 25 константу квадратов в виде 34, 98,...,1570. Если вновь полученную арифметическую прогрессию (константы квадратов) расположить по образцу (1), т.е. a_i член поставим в i ое место:

$$\begin{matrix} 674 & 1506 & 418 & 1250 & 226 & 738 & 162 \\ 1570 & 482 & & & & & 994 \\ 1058 & 290 & 738 & 1314 & & & 546 \\ 610 & 994 & 34 & 866 & & & 1378 \\ & & & & & & 930 \\ 1442 & 354 & 1186 & 98 & & & \end{matrix}$$

M матрица (3) также имеет константу квадрата 4010:

S 1 25 5 34 1570

5 4010. *a a*

2 2 (3)

Аналогично, можно поступать с каждым подблоком каждого блока при декомпозиции M матрицы. Это показывает о возможном разнообразии констант квадратов в подблоках при декомпозиции M матриц.

В заключении отметим, что возможное разнообразие констант квадратов нам дает основание о построении разнообразных M матриц высокого порядка.

3_2

Шифрование по магическому квадрату. Известно, число магических квадратов равно 8.

С возрастанием n число N различных квадратов с n^2 клетками быстро растет, и хотя общая формула, выражающая зависимость N от n, до сих пор не найдена, однако установлено, например, что существует 880 различных шестнадцатиклеточных магических квадратов, а уже при $n \geq 7$ число магических квадратов достигает сотен миллионов. Поэтому, магические квадраты больших размеров могли быть хорошей основой для надежной системы шифрования в криптографии.

Авторами было показано возможное разнообразие констант квадратов в подблоках при построении методом декомпозиции магических квадратов высокого порядка [1]. Было построено магический квадрат матрицу сотого порядка [4].

В заключении отметим, что возможное разнообразие констант квадратов нам дает основание о построении разнообразных M матриц высокого порядка[5].

В настоящее время, обеспечения информационной безопасности является огромной проблемой. Известно, что методом магических квадратов широко пользуются при шифровании секретной информации. При этом, ключом расшифровки является сам магический квадрат. Возьмем, к примеру, следующий магический квадрат

2	7	6
9	5	1
4	3	8

С помощью данного магического квадрата дешифруем следующее секретное слово эке вбж нэо Как это сделать?

К нашему квадрату рядом с цифрами перепишем по порядку данный набор букв.

2 э	7 к	6 е
9 в	5 б	1 ж
4 н	3 э	8 о

Теперь данные каждой ячейки напишем так, чтобы цифры расположились по порядку, начиная с единицы: Жээнбеков.

В данном случае магический квадрат послужил как ключ.

В некоторых случаях приходится решать обратные задачи. По исходным шифрованным данным можно восстановить ключ зашифровки.

Например, Бекжан в своей тетради зашифровал фразу «компьютер». Так он получил следующее: ютокьремп

После этого, его сестренка Акмарал стерла все цифры данного магического квадрата. Какая цифра была расположена на нижнем правом углу?

		?

(Ответ: 4).

Возможно встретиться и такой случай: Мы, засекретив слово методом магических квадратов, получили следующее:

ПАИ*УНРН*ЕРИКДМЗ

К сожалению, некоторые данные в квадрате стерлись. Необходимо восстановить магический квадрат и найти засекреченное слово.

1			
8	13		
10	3	16	
15	6	9	4

(Ответ: ПРЕЗИДИУМ*НАН*КР)

Эти вышеуказанные примеры показывают актуальность исследования магических матриц, в том числе высокого порядка, так как результаты исследования могут быть теоретическим обоснованием декодирования при передаче информации, а также шифрования в криптографии.

Далее отметим, что существует программа, реализующая шифрование введенного текста. В реализованной программе шифрование введенного пользователем текста осуществляется методом шифр поворотная решетка. Магический квадрат (неограниченное количество символов) отображает количество введенных символов и позволяет дешифровать зашифрованный текст [8].

Однако, реализованная программа не предусматривает создание самого магического квадрата. Мы считаем, что комплексная программа по созданию программы магического квадрата высокого порядка и шифровании (дешифровании) введенного текста будет обогащать криптографические методы защиты данных в автоматизированных системах.

Список цитируемых источников:

1. Байзаков А. Б., Момбеков А.Д. О некоторых свойствах квадратных матриц, сохраняющие симметрии //Известия НАН КР. – Бишкек: Илим, 2018.–С.25-38.
2. Ю. В. Чебраков. Теория магических матриц. Выпуск ТММ-1. – С. –Петербург, 2008.
3. Heinz H. Magic Squares, Magic Stars & Other Patterns. – Last updated Nov 2009. – http://www.magic-squares.net/

4. Байзаков А.Б., Момбеков А.Д., Шаршенбеков М.М. Использование свойств констант квадратов при построении М матриц высокого порядка методом декомпозиции. // Вестник Института математики НАН КР. -2018. -№1.- С75-79.
5. Байзаков А.Б., Момбеков А.Д., Айтбаев К.А. О разнообразии констант квадратов в подблоках при декомпозиции матриц // Доклады НАН КР, Бищкек, 2017. -№2.- С19-24.
6. http://rain.ifmo.ru/cat/view.php/theory/coding/cryptography-2005/history.
7. https://www.anti-malware.ru/threats/information-security-threats.
8. http://www.allbest.ru/.

Рецензент: Искандаров С. *– доктор физико-математических наук, профессор Институт математики НАН КР*