Институт информационных и вычислительных технологий
МОН РК

Казахский Национальный Университет имени аль-Фараби

Университет Туран

Люблинский технический университет, Польша


МАТЕРИАЛЫ

III Международной научной конференции

«Информатика и прикладная математика»,

посвященная 80-летнему юбилею

профессора Бияшева Р.Г.

и 70-летию профессора Айдарханова М.Б.

26-29 сентября 2018 года, Алматы, Казахстан

Часть 2

Алматы 2018

СЕКЦИЯ 4
Информационная безопасность и защита данных. Программно-технические средства защиты информации. Математические методы обеспечения информационной безопасности сложных систем

Литература

1. Овчинников В.А., Антонов Я.В. Теоретико-практические аспекты электронной демократии и электронного голосования. Общероссийский научно-практический журнал «Юридический мир», М.: Юрист. № 4. 2013. С. 19-20;
2. Антонов Я.В. Электронное голосование: понятие, правовые особенности и перспективы (монография). «LAP» LAMBERT Academic Publishing, 2013. С. 16-17.
3. Лысенко В. Новые Рекомендации Совета Европы о правилах электронного голосования на выборах [Электронный ресурс] // http://www.rfsv.ru/law/pravovye-innovatsii/novye-rekomendatsii-soveta-evropy-o-pravilakh-elektronnogo-golosovaniia-na-vyborakh (дата обращения: 15.08.2018).
4. Ferraiolo D., Sandhu R., Gavrila S., Kuhn D., Chandramouli R. 2001. Proposed NIST standard for role-based access control. *ACM Trans. Inf. Syst. Secur.* 4, 3 (August 2001), 224-274. DOI=http://dx.doi.org/10.1145/501978.501980
5. Hu V. Ferraiolo D., Kuhn D. Schnitzer A. Sandlin K., Miller R. Scarfone K. (2014). Guide to attribute based access control (ABAC) definition and considerations. National Institute of Standards and Technology Special Publication. 162-800.

ЛИНЕЙНЫЕ ПРЕОБРАЗОВАНИЯ В СОВРЕМЕННЫХ СИММЕТРИЧНЫХ БЛОЧНЫХ АЛГОРИТМАХ ШИФРОВАНИЯ

Капалова Н., Хаумен А., Дюсенбаев Д., Алгазы К.

Институт информационных и вычислительных технологий
КН МОН РК, Казахстан
nkapalova@mail.ru, haumen.armanbek@gmail.com, dimash_dds@mail.ru,
kunbolat@ mail.ru

Аннотация: *В данной работе дается обзор MDS-матриц, используемых в линейных преобразованиях исходного текста различных алгоритмов шифрования. MDS-матрицы имеют определенную структуру и обладают хорошим рассеивающим свойством, что определяет их широкое применение в криптографии. В статье представлены известные алгоритмы шифрования, в которых одним из преобразований является умножение на MDS-матрицу.*

Ключевые слова: *алгоритмы шифрования, МДР-коды, MDS-матрица, рассеивание, перемешивание*.

Введение

В эпоху развития информационных технологий симметричные блочные алгоритмы шифрования являются основным криптографическим средством обеспечения конфиденциальности при обработке информации в современных

информационно-телекоммуникационных системах. Кроме того, блочные шифры используются для обеспечения целостности, а также как базовый элемент при построении других криптографических примитивов, таких как генераторы псевдослучайных последовательностей (ГПСЧ), поточные шифры и функции хеширования. Уровень стойкости и свойства симметричного блочного алгоритма шифрования, используемого в системе, в существенной степени определяют стойкость криптографической защиты информации, безопасность криптографических протоколов и защищённость информационно-телекоммуникационной системы в целом [1].

Каким же условиям должен удовлетворять стойкий блочный шифр? Эти условия сформулировал К. Шеннон в ряде своих основополагающих работ по теории шифрования [2]. Стойкий шифр должен обладать свойствами перемешивания и рассеивания:

–рассеивание (diffusion): это свойство шифра, при котором один символ (бит) исходного текста влияет на несколько символов (битов) шифртекста, оптимально – на все символы в пределах одного блока. Если данное условие выполняется, то при шифровании двух блоков данных с минимальными отличиями между ними должны получаться совершенно непохожие друг на друга блоки шифртекста. Точно такая же картина должна иметь место и для зависимости шифртекста от ключа – один символ (бит) ключа должен влиять на несколько символов (битов) шифртекста. Рассеивание скрывает отношения между зашифрованным текстом и исходным текстом.

–перемешивание (confusion): это свойство шифра скрывать зависимости между символами исходного текста и шифртекста. Если шифр достаточно хорошо "перемешивает" биты исходного текста, то соответствующий шифртекст не содержит никаких статистических, и, тем более, функциональных закономерностей – опять же, для стороннего наблюдателя, обладающего лишь ограниченными вычислительными ресурсами. Перемешивание скрывает отношения между зашифрованным текстом и ключом.

Для обеспечения требований к блочным шифрам в современных алгоритмах шифрования используются различные преобразования. В данной работе речь идет о линейных преобразованиях, а именно MDS-матрицах над конечными полями.

Развитие методов криптографического анализа и средств показало, что уже в начале 90-х годов алгоритм DES не обладал необходимыми криптографическими характеристиками. В результате научных разработок появились алгоритмы нового поколения со структурой SP-сети. Общая конструкция этих алгоритмов – вариант подстановочно-перестановочной сети (SP-сети) – итерационного преобразования, состоящего из слоя подстановок (нелинейных элементов), линейного (перемешивающего) слоя и слоя наложения ключа. Такая конструкция за счет преобразования всего блока данных на каждой итерации обеспечивает гораздо более быстрое перемешивание входного вектора по сравнению с сетью Фейстеля. Данный эффект усиливается за счет использования в линейном слое так называемой MDS–матрицы (Maximal Distance Separable matrix), обеспечивающей максимально возможную зависимость бит выходного вектора от бит входного [3].

В блочных симметричных алгоритмах качестве блока линейного преобразования используется хорошо проверенное МДР-преобразование (МДР – разделимые коды с максимальным расстоянием), дающее наилучшие свойства рассеивания (распространения разности).

МДР-коды [4] или МДР-матрицы используются в основном для умножения вектора исходного текста на некоторую матрицу констант, которую обычно называют MDS-матрицей.

MDS-матрица – это такая матрица над конечным полем K, что если взять её в качестве матрицы линейного преобразования$f(x) = (MDS)x$ из пространстваK^nв пространство K^m, то любые два вектора из пространства K^{n+m}вида $(x, f(x))$будут иметь как минимум m+1 различий в компонентах. То есть набор векторов вида $(x, f(x))$ образует код, обладающий свойством максимальной разнесённости (maximum distance separable code).

MDS-матрица – проверочная матрица линейного блокового кода:

- обеспечивает максимальное рассеивание за счёт своей структуры;
- используется при создании шифров на основе SP-сети (SPN-шифров) в качестве линейных рассеивающих преобразований.

ТипыMDS-матриц:

- Матрица Вандермонда
- Инволютивная матрица (одна и та же MDS-матрица для шифрования и расшифрования)
- Матрица Коши
- Циркулярная матрица (как в Rijndael)

MDS-матрицы используется в линейных преобразованиях во многих алгоритмах шифрования.

Алгоритм AES

Advanced Encryption Standard (AES), также известный как Rijndael – симметричный алгоритм блочного шифрования, принятый в качестве стандарта правительством США по результатам конкурса AES. Для обеспечения криптостойкости алгоритм Rijndael включает в себя повторяющиеся раунды, каждый из которых состоит из замен, перестановок и наложения ключа. Здесь мы будем рассматривать только преобразование MixColumns.

Операция MixColumns задумана с тем, чтобы строки матрицы состояний "взаимодействовали" друг с другом на протяжении всех раундов. В комбинации с предыдущей операцией (ShiftRows) она наделяет каждый байт выходных данных зависимостью от каждого байта на входе.

Каждый столбец матрицы состояний представляется как многочлен степени 3 с коэффициентами из GF(2^8): $a(x) = a_0 + a_1x + a_2x^2 + a_3x^3$.

Новый столбец получается умножением многочлена$a(x)$на фиксированный многочлен $c(x) = \{02\} + \{01\}x + \{01\}x^2 + \{03\}x^3$ по модулю многочлена $m(x) =$

$x^4 + 1$. Так как умножение на многочлен – линейная операция, ее можно представить в виде действия с матрицей [5].

Пусть $b(x) = c(x) \otimes a(x)$

$$\begin{bmatrix} b_0 \\ b_1 \\ b_2 \\ b_3 \end{bmatrix} = \begin{bmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{bmatrix} \cdot \begin{bmatrix} a_0 \\ a_1 \\ a_2 \\ a_3 \end{bmatrix}$$

Используемая при умножении матрица является циркулярной MDS-матрицей и обладает всеми свойствами матриц данного вида.

Алгоритм Кузнечик

Кузнечик – симметричный алгоритм блочного шифрования с размером блока 128 бит и длиной ключа 256 бит.

Данный шифр утвержден в качестве стандарта ГОСТ Р 34.12-2015 "Информационная технология. Криптографическая защита информации. Блочные шифры". Стандарт действует с 1 января 2016 года.

Шифр разработан Центром защиты информации и специальной связи ФСБ России с участием ОАО "Информационные технологии и коммуникационные системы" (ОАО "ИнфоТеКС").

Новый шифр построен не на сети Фейстеля, а на SP-сети. В SP-сети преобразуется весь входной блок, а не половина, как в сети Фейстеля [6].

Как уже отмечалось ранее, использование MDS-матриц необходимо для обеспечения "быстрого" перемешивания входного вектора. С криптографической точки зрения было бы хорошо использовать большую MDS-матрицу для всего блока входных данных, однако хранить в памяти матрицу большого размера невыгодно с точки зрения эксплуатационных характеристик.

В "Кузнечике" при синтезе MDS-преобразования использовался подход, предложенный ученым-алгебраистом А.Нечаевым и заключающийся в генерации матрицы с помощью линейного регистра сдвига [7]. Такой подход позволяет в некоторых случаях существенно экономить объем требуемой для реализации алгоритма памяти и получить матрицу для всего 128-битного блока, обрабатываемого алгоритмом, в отличие от алгоритма AES, для которого такие матрицы действуют только на 32-битных подблоках. Подход, используемый в "Кузнечике", предпочтительнее, поскольку позволяет в 1,5 раза сократить число итераций по сравнению с AES и обеспечить большую защиту от атак по побочным каналам [3].

Линейное преобразование может быть реализовано не только матрицей, как это обычно делается в блочных шифрах, но и с помощью РСЛОС – линейного регистра сдвига с обратной связью, применяемого 16 раз.

Линейное преобразование задается отображением $\ell: V_8^{16} \to V_8$, которое определяется следующим образом:

$$\ell(a_{15},\dots,a_0) = \nabla(148\cdot\Delta(a_{15}) + 32\cdot\Delta(a_{14}) + 133\cdot\Delta(a_{13}) + 16\cdot\Delta(a_{12}) + 194 \cdot\Delta(a_{11}) + 192\cdot\Delta(a_{10}) + 1\cdot\Delta(a_9) + 251\cdot\Delta(a_8) + 1\cdot\Delta(a_7) + 192 \cdot\Delta(a_6) + 194\cdot\Delta(a_5) + 16\cdot\Delta(a_4) + 133\cdot\Delta(a_3) + 32\cdot\Delta(a_2) + 148 \cdot\Delta(a_1) + 1\cdot\Delta(a_0))$$

для любых $a_i \in V_8, i = 0{,}1,\dots{,}15$, где операции сложения и умножения осуществляются в поле $\mathbb{F}$, а константы являются элементами поля.

В "Кузнечике" используются следующие константы при умножении:

(148, 32, 133, 16, 194, 192, 1, 251, 1, 192, 194, 16, 133, 32, 148, 1).

Алгоритм Twofish

Twofish – симметричный алгоритм блочного шифрования с размером блока 128 бит и длиной ключа до 256 бит. Число раундов – 16. Разработан группой специалистов во главе с Брюсом Шнайером. Являлся одним из пяти финалистов второго этапа конкурса AES.

Основой алгоритма Twofish является функция **g**. На вход функции подается 32-битное число X, которое затем разбивается на четыре байта x_0, x_1, x_2, x_3. Каждый из получившихся байтов пропускается через свой S-блок (S-box). Получившиеся 4 байта на выходах S-блоков интерпретируются как вектор с четырьмя компонентами. Этот вектор умножается на фиксированную матрицу MDS размером 4x4, причем вычисления проводятся в поле Галуа$GF(2^8)$ по модулю неприводимого многочлена$x^8 + x^6 + x^5 + x^8 + 1$[8]. Матрица MDS имеет вид:

$$MDS = \begin{pmatrix} 01 & EF & 5B & 5B \\ 5B & EF & EF & 01 \\ EF & 5B & 01 & EF \\ EF & 01 & EF & 5B \end{pmatrix}$$

В Twofish свойство максимальной разнесённости матрицы MDS означает, что общее количество меняющихся байт вектора **a** и вектора **b=(MDS)a** не меньше пяти. Другими словами, любое изменение только одного байта в **a** приводит к изменению всех четырёх байтов в **b**.

Алгоритм "Калина"

"Калина" является украинским стандартом шифрования данных (ДСТУ 7624:2014), введенным 2015 году. Новый национальный стандарт поддерживает размер блока и длину ключа шифрования 128, 256 и 512 бит (длина ключа равна размеру блока или в два раза превышает его), обеспечивая нормальный, высокий и сверхвысокий уровень стойкости. Высокоуровневая конструкция использует хорошо исследованную Square-подобную SPN-структуру, применяемую в алгоритмах AES/Rijndael, Whirlpool, "Кузнечик" и многих других. Цикловое преобразование построено на базе таблиц подстановки (S-блоков) и умножения на

МДР-матрицу над конечным полем, обеспечивая необходимые криптографические свойства. Применение именно такой конструкции позволяет обеспечить доказуемую стойкость к дифференциальному, линейному и другим видам криптоанализа, одновременно обеспечивая эффективную реализацию на широком спектре программных ипрограммно-аппаратных платформ. При выборе размера МДР-матрицы был принят вовнимание размер кэша L1 современных иперспективных процессоров, что позволило оптимизировать быстродействие программной реализации шифра [9].

В алгоритме "Калина" для колонки матрицы состояний используется линейное преобразование MixColumns. В этом преобразовании каждый элемент новой матрицы вычисляется по формуле:

$$w_{ij} = (v >>> i) \otimes G_j,$$

где $\otimes$ - скалярное произведение векторов, v- вектор, G_j- колонка матрицы состояния.

Вектор v- имеет следующий вид:

$$v = (0x01,0x01,0x05,0x01,0x08,0x06,0x07,0x04)$$

При циркулярном сдвиге этого вектора получится циркулярная МДР-матрица следующего вида:

$$\begin{pmatrix} 01 & 01 & 05 & 01 & 08 & 06 & 07 & 04 \\ 04 & 01 & 01 & 05 & 01 & 08 & 06 & 07 \\ 07 & 04 & 01 & 01 & 05 & 01 & 08 & 06 \\ 06 & 07 & 04 & 01 & 01 & 05 & 01 & 08 \\ 08 & 06 & 07 & 04 & 01 & 01 & 05 & 01 \\ 01 & 08 & 06 & 07 & 04 & 01 & 01 & 05 \\ 05 & 01 & 08 & 06 & 07 & 04 & 01 & 01 \\ 01 & 05 & 01 & 08 & 06 & 07 & 04 & 01 \end{pmatrix}$$

При расшифровании используется матрица, обратная к данной.

Усовершенствование MDS-матриц известных алгоритмов шифрования

Как изложино выше, MDS-матрицы используются при создании SPN-шифров в качестве линейных рассеивающих преобразований.

В последное время учеными ведутся работы по усовершенствованию этих линейных рассеивающих преобразований. Бразильские учетные в своей работе[10] предлагает использовать в алгоритме AESдругую MDS-матрицу размером 16x16.

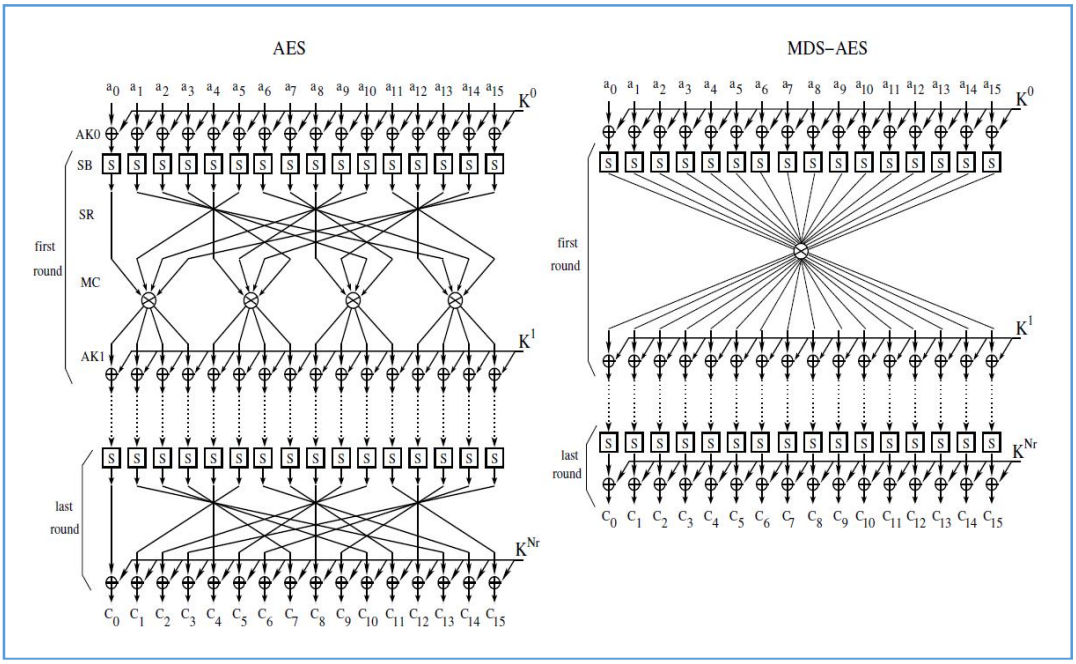

Рис. 1. Схемы алгоритма AES и его модификации

В модифицированном MDS-AES алгоритме используется инволютивная MDS-матрица.

$$M_{16\times 16} = \begin{bmatrix}
01_x & 03_x & 04_x & 05_x & 06_x & 07_x & 08_x & 09_x & 0a_x & 0b_x & 0c_x & 0d_x & 0e_x & 10_x & 02_x & 1e_x \\
03_x & 01_x & 05_x & 04_x & 07_x & 06_x & 09_x & 08_x & 0b_x & 0a_x & 0d_x & 0c_x & 10_x & 0e_x & 1e_x & 02_x \\
04_x & 05_x & 01_x & 03_x & 08_x & 09_x & 06_x & 07_x & 0c_x & 0d_x & 0a_x & 0b_x & 02_x & 1e_x & 0e_x & 10_x \\
05_x & 04_x & 03_x & 01_x & 09_x & 08_x & 07_x & 06_x & 0d_x & 0c_x & 0b_x & 0a_x & 1e_x & 02_x & 10_x & 0e_x \\
06_x & 07_x & 08_x & 09_x & 01_x & 03_x & 04_x & 05_x & 0e_x & 10_x & 02_x & 1e_x & 0a_x & 0b_x & 0c_x & 0d_x \\
07_x & 06_x & 09_x & 08_x & 03_x & 01_x & 05_x & 04_x & 10_x & 0e_x & 1e_x & 02_x & 0b_x & 0a_x & 0d_x & 0c_x \\
08_x & 09_x & 06_x & 07_x & 04_x & 05_x & 01_x & 03_x & 02_x & 1e_x & 0e_x & 10_x & 0c_x & 0d_x & 0a_x & 0b_x \\
09_x & 08_x & 07_x & 06_x & 05_x & 04_x & 03_x & 01_x & 1e_x & 02_x & 10_x & 0e_x & 0d_x & 0c_x & 0b_x & 0a_x \\
0a_x & 0b_x & 0c_x & 0d_x & 0e_x & 10_x & 02_x & 1e_x & 01_x & 03_x & 04_x & 05_x & 06_x & 07_x & 08_x & 09_x \\
0b_x & 0a_x & 0d_x & 0c_x & 10_x & 0e_x & 1e_x & 02_x & 03_x & 01_x & 05_x & 04_x & 07_x & 06_x & 09_x & 08_x \\
0c_x & 0d_x & 0a_x & 0b_x & 02_x & 1e_x & 0e_x & 10_x & 04_x & 05_x & 01_x & 03_x & 08_x & 09_x & 06_x & 07_x \\
0d_x & 0c_x & 0b_x & 0a_x & 1e_x & 02_x & 10_x & 0e_x & 05_x & 04_x & 03_x & 01_x & 09_x & 08_x & 07_x & 06_x \\
0e_x & 10_x & 02_x & 1e_x & 0a_x & 0b_x & 0c_x & 0d_x & 06_x & 07_x & 08_x & 09_x & 01_x & 03_x & 04_x & 05_x \\
10_x & 0e_x & 1e_x & 02_x & 0b_x & 0a_x & 0d_x & 0c_x & 07_x & 06_x & 09_x & 08_x & 03_x & 01_x & 05_x & 04_x \\
02_x & 1e_x & 0e_x & 10_x & 0c_x & 0d_x & 0a_x & 0b_x & 08_x & 09_x & 06_x & 07_x & 04_x & 05_x & 01_x & 03_x \\
1e_x & 02_x & 10_x & 0e_x & 0d_x & 0c_x & 0b_x & 0a_x & 09_x & 08_x & 07_x & 06_x & 05_x & 04_x & 03_x & 01_x
\end{bmatrix}.$$

Рис. 2. MDS-матрица модифицированного алгоритма AES

Особенностью данной схемы является использование одной матрицы как для зашифрования, так и для расшифрования.

В работе [11] авторы предлагают еще одну модификацию алгоритма AES. Здесь используется MDS-матрица размером 8x8.

$$H = \begin{bmatrix} 01 & 03 & 04 & 05 & 06 & 08 & 0B & 07 \\ 03 & 01 & 05 & 04 & 08 & 06 & 07 & 0B \\ 04 & 05 & 01 & 03 & 0B & 07 & 06 & 08 \\ 05 & 04 & 03 & 01 & 07 & 0B & 08 & 06 \\ 06 & 08 & 0B & 07 & 01 & 03 & 04 & 05 \\ 08 & 06 & 07 & 0B & 03 & 01 & 05 & 04 \\ 0B & 07 & 06 & 08 & 04 & 05 & 01 & 03 \\ 07 & 0B & 08 & 06 & 05 & 04 & 03 & 01 \end{bmatrix}$$

Рис. 3. MDS-матрица размером 8x8

Заключение

Рассмотренные в данной работе линейные преобразования в известных алгоритмах используются для повышения криптостойкости шифра. Главная цель этих преобразований – обеспечить алгоритмы свойством рассеивания. Для реализации применяются матрицы разного вида. Хорошо реализованная MDS-матрица в алгоритме существенно рассеиваетэлементы блока. Поэтому при создании нового алгоритма или модификации существующего алгоритма большое внимание следует уделять конструкции MDS-матрицы. В связи с этим при построении разработанной нами модели симметричного блочного шифрования используются следующие криптографические процедуры:

- табличная замена *S*;
- преобразование *MSB*, в котором блок байтов умножается на MDS-матрицу;
- преобразование *MSB*, в котором производится перестановка байтов в блоке.

Как правило, при создании нового алгоритма или модификации существующего алгоритма шифрования с применением MDS-матрицы сначала исследуются ее свойства. В нашем случае исследованы свойства разработанной MDS-матрицы. При анализе этой MDS-матрицы получены положительные результаты ее рассеивающих свойств.

Литература

1. Горбенко И.Д., Долгов В., Олейников Р.В., Руженцев В.И., Михайленко М.С., Горбенко Ю.И., Разработка требований и принцип проектирования перспективного симметричного блочного алгоритма шифрования. // Известия южного федерального университета. Технические науки, № 1, том 76, 2007.

2. К. Шеннон. Работы по теории информации и кибернетике, М., ИЛ, 1963, с. 333–369

3. Бондаренко А., Маршалко Г., Шишкин В. ГОСТ Р 34.12–2015: чего ожидать от нового стандарта? // Журнал "Information Security/ Информационная безопасность"№4, 2015

4. Мак-Вильямс Ф. Дж., Слоэн Н. Дж. А. Теория кодов, исправляющих ошибки: Пер. с англ. — М: Связь, 1979. — 744 с.

5. Бабенко Л.К., Ищукова Е.А. Современные алгоритмы блочного шифрования и методы их анализа. – М.: Гелиос АРВ, 2006. – 376 с.

6. Ищукова Е. А., Кошуцкий Р. А., Бабенко Л. К. Разработка и реализация высокоскоростного шифрования с использованием алгоритма Кузнечик. // Auditorium: электронный научный журнал Курского государственного университета.2015. № 4 (08)

7. С. Гонсалес, Е. Коусело, В.Марков, А. Нечаев. Параметры рекурсивных МДР-кодов. Дискретная математика, т. 12, вып. 4. 2000.

8. Панасенко С.П. Алгоритмы шифрования. Специальный справочник. – СПб.: БХВ-Петербург, 2009. – 576 с.:ил.

9. Олейников Р., Горбенко И. О новом украинском стандарте шифрования. // Журнал "Компьютерное обозрение", 2015г., http://ko.com.ua/o_novom_ukrainskom_standarte_shifrovaniya_110863.

10. Jorge Nakahara Jr, ElcioAbrah˜ao. A New Involutory MDS Matrix for the AES. // International Journal of Network Security, Vol.9, No.2, PP.109–116, Sept. 2009.

11. R.Elumalai, Dr.A.R.Reddy. Improving Diffusion Power of AES Rijndael with8x8 MDS Matrix. // International Journal of Scientific & Engineering Research Volume 2, Issue 3, March-2011.

ОБ ОДНОМ МЕТОДЕ ОБРАБОТКИ ЭКСПЕРТНОЙ ИНФОРМАЦИИ

Мазаков Т.Ж., Исимов Н.Т., Жолмагаметова Б.Р., Карымсакова Н.Т., Ыдырышбаева М.Б.

КазНУ имени аль-Фараби
Институт информационных и вычислительных технологий, КН МОН РК

Аннотация. *В данной статье проанализированы проблемы мониторинга и управления социально-эпидемиологической ситуации. Предложена новая математическая модель и алгоритм для обработки экспертной информации по оценке эпидобстановки с учетом эпидеомиологических, социальных и экономических показателей региона. Исследованы свойства математического алгоритма.*

Ключевые слова. *Эпидобстановка, функционал, градиентный метод.*

Введение. Одна из актуальных задач медицины состоит в своевременной профилактике различных эпидемических болезней с помощью медико-