В.Л. Стефанюк, А.Х. Алхуссаин

Управление степенью защиты символьной информации с использованием метода целочисленного расщепления[1]

Аннотация. Применение модульной арифметики в задачах обеспечения контроля степенью защиты информации показано путем использования нового метода, названного целочисленным расщеплением. Приведены основные определения и понятия этого метода. Описана математическая функция возникающего преобразования, исследованы его свойства и доказаны основные теоремы, оправдывающие применимость метода расщепления в практических приложениях. Создана действующая система и приведены характерные примеры ее работы.

Ключевые слова: модульная арифметика, метод расщепления целых чисел, уровень расщепления, свойства целочисленного расщепления, целочисленные преобразования, целочисленное расщепление символов.

Введение

В настоящее время арифметика в остатках активно применяется в цифровой обработке сигналов, обработке изображений, в распределенных инфокоммуникационных системах, беспроводных сенсорных сетях, средствах обеспечения множественного доступа с кодовым разделением каналов, обнаружения и исправления ошибок, системах информационной безопасности, облачных вычислениях и пр. [1]. В статье продемонстрирован способ применения арифметики в остатках, или модульной арифметики в задаче обеспечения контроля степенью защиты информации путем использовании нового метода работы с текстом, названного целочисленным расщеплением [3, 4], при котором каждый символ текста, представленный в виде числа в соответствии с выбранной кодовой таблицей, заменяется на последовательность k целых чисел при рассмотрении расщепления k-го уровня [2].

В Разделе 1 дано определение и излагаются теоретические основы целочисленного расщепления. В Разделе 2 рассматриваются теоремы, связные с этим новым методом, и приводятся их доказательство. В Разделе 3 приводятся экспериментальные результаты применения этого метода в области обеспечения контроля степени защиты информации.

1.Основные определения и понятия

Пусть даны два *несоизмеримых* целых числа r и α, причем $r > \alpha > 0$.

Определение 1. Целочисленным расщеплением числа α по базе r, будем называть представление α в виде последовательности

$$\alpha_1, \alpha_2, \alpha_3, \cdots, \alpha_k, \qquad (1)$$

члены которой вычисляются рекуррентно следующим образом.

Обозначим через $q_1 = \left\lfloor \frac{r}{\alpha} \right\rfloor$ целую часть от деления r на α, а остаток от такого деления

[1] Работа выполнена при финансовой поддержке по программе Президиума РАН 1.5 П и фонда РФФИ (грант № 15-07-07486-а). Исследования проводились на кафедре информационных технологий Российского университета дружбы народов.

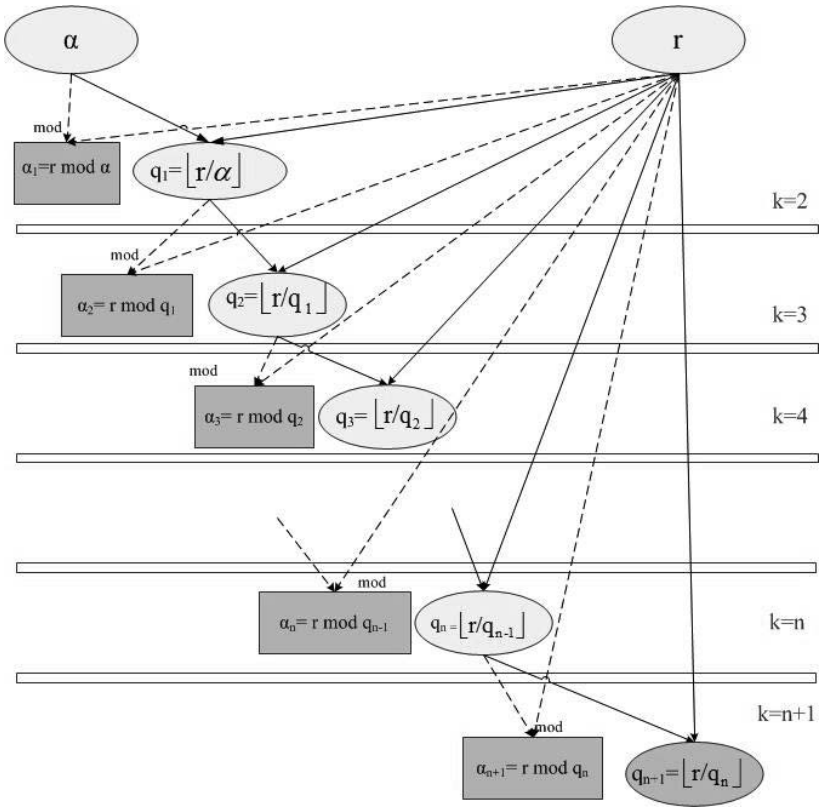

Рис. 1. Схема целочисленного расщепления числа α по базе r, при уровне расщепления $k = n+1$

обозначим через $\alpha_1 = r \bmod \alpha$. Аналогично, обозначим пару от деления r на q_1 через $q_2 = \left\lfloor \frac{r}{q_1} \right\rfloor$ и $\alpha_2 = r \bmod q_1$.[2]

В общем случае имеем $q_i = \left\lfloor \frac{r}{q_{i-1}} \right\rfloor$ и $\alpha_i = r \bmod q_{i-1}$ $(i = 1, \ldots, k)$. Здесь принимается $q_0 \equiv \alpha$, причем натуральное число k называется уровнем расщепления,

Процесс дальнейшего целочисленного расщепления числа α по базе r, при уровне расщепления $k = n+1$, показан на Рис. 1.

Определение 2. Пусть функция Φ_k является результатом целочисленного расщепления числа α по базе r. Обозначим через $\Phi_k(\alpha)$ *отображение* числа α на упорядоченную последовательность из k целых чисел $\alpha_1, \alpha_2, \alpha_3, \ldots\ldots\ldots\ldots, \alpha_{k-2}, \alpha_{k-1}, \alpha_k$.

Тогда отображение $\Phi_k(\alpha)$ при уровне расщепления k определяется следующим соотношением:

$$\Phi_k(\alpha) = (\alpha_1, \alpha_2, \alpha_3, \ldots\ldots, \alpha_{k-2}, \alpha_{k-1}, \left\lfloor \frac{r}{q_{k-1}} \right\rfloor). \quad (2)$$

Например, отображение $\Phi_k(\alpha)$ при уровне расщепления $k = 3$ определяется следующим соотношением:

$$\Phi_3(\alpha) = \left(\alpha_1, \alpha_2, \left\lfloor \frac{r}{q_2} \right\rfloor \right).$$

Определение 3. Пусть α есть целочисленный код представления для символа A. Тогда расщеплением символа A по базе r будем называть целочисленное расщепление A по базе r на k уровней, при r, превышающем максимальное значение для используемой кодовой таблицы.

[2] $q_1 = \left\lfloor \frac{r}{\alpha} \right\rfloor$ означает округление дроби $q_1 = \frac{r}{\alpha}$ до ближайшего целого в меньшую сторону, т.е. q_1 является целым и таким, что выполняется $q_1 \le \frac{r}{\alpha}$.

2.Теоремы и их доказательство

Теорема 0. Пусть задана пара целых чисел r и α, где $\alpha \neq 0$, тогда деление с остатком для r и α однозначно, т.е. частное q и остаток α_1 определяются единственным образом.

Теорема 1. Целочисленное расщепление $\Phi_k(\alpha)$ является мономорфизмом.

Доказательство теоремы при $k=2$**.** Отображение $\Phi_2(\alpha)$ при уровне расщепления $k=2$ определяется следующим соотношением: $\Phi_2(\alpha)=(\alpha_1,q_1)$. В этом случае Теорема 1 утверждает, что выполняется следующее:

$$\alpha^{(i)} \neq \alpha^{(j)} \Rightarrow \Phi_2(\alpha^{(i)}) \neq \Phi_2(a^{(j)}).$$

Результат действия такого отображения, очевидно, является упорядоченной парой и теорема утверждает, что

$$\alpha^{(i)} \neq \alpha^{(j)} \Rightarrow \left(\alpha_1^{(i)},q_1^{(i)}\right) \neq \left(\alpha_1^{(j)},q_1^{(j)}\right). \quad (3)$$

Изучим варианты совпадений этих упорядоченных пар. Две пары $\left(\alpha_1^{(i)},q_1^{(i)}\right)$ и $\left(\alpha_1^{(j)},q_1^{(j)}\right)$ не могут совпадать, т.е. $\left(\alpha_1^{(i)}=\alpha_1^{(j)}\right)$ и $\left(q_1^{(i)}=q_1^{(j)}\right)$, если они не представляют одно и то же число, поскольку из Теоремы 0 деление с остатком для любого числа на другое число однозначно, т.е. частное и остаток определяются единственным образом, что не соответствует условию Теоремы 1: $\alpha^{(i)} \neq \alpha^{(j)}$ Отсюда следует, что совпадение двух пар невозможно и следовательно $\Phi_2(\alpha^{(i)}) \neq \Phi_2(\alpha^{(j)})$. Теорема доказана.

Доказательство теоремы в случае, когда $k=n+1$**.** Пусть по предположению индукции теорема верна при $k=n$. Теорема определяется следующим соотношением при $k=n$. В силу этого предположения имеем при $a^{(i)} \neq a^{(j)} \Rightarrow \Phi_n(a^{(i)}) \neq \Phi_n(a^{(j)})$ и следующие последовательности не совпадают при $\alpha^{(i)} \neq \alpha^{(j)}$:

$$\left(\alpha_1^{(i)},\alpha_2^{(i)},\alpha_3^{(i)},\ldots,\alpha_{(n-1)}^{(i)},\alpha_n^{(i)},q_n^{(i)}\right) \neq \left(\alpha_1^{(j)},\alpha_2^{(j)},\alpha_3^{(j)},\ldots,\alpha_{(n-1)}^{(j)},\alpha_n^{(j)},q_n^{(j)}\right). \quad (4)$$

Индукция по *n:*

A. При $n=2$ Теорема 1 была доказана выше (при) $k=2$.

B. Пусть утверждение справедливо при $k=n$. Тогда из уравнения (4) вытекает, что если функция Φ_n является мономорфизмом то, по крайней мере, один из компонентов не совпадает, т.е.

либо $\alpha_1^{(i)} \neq \alpha_1^{(j)}$ (5)

или $\alpha_2^{(i)} \neq \alpha_2^{(j)}$ (6)

или $\alpha_3^{(i)} \neq \alpha_3^{(j)}$ (7)

……

или $\alpha_{(n-1)}^{(i)} \neq \alpha_{(n-1)}^{(j)}$ (8)

или $\alpha_n^{(i)} \neq \alpha_n^{(j)}$ (9)

или $q_n^{(i)} \neq q_n^{(j)}$ (10)

C. Требуется доказать, что при $k=n$ +1 из $\alpha^{(i)} \neq \alpha^{(j)}$ вытекает $\Phi_{n+1}\left(\alpha^{(i)}\right) \neq \Phi_{n+1}\left(\alpha^{(j)}\right)$.

Действительно, при $\alpha^{(i)} \neq \alpha^{(j)}$ имеем

$$\left(\alpha_1^{(i)},\alpha_2^{(i)},\alpha_3^{(i)},\ldots,\alpha_{(n-1)}^{(i)},\alpha_n^{(i)},\alpha_{(n+1)}^{(i)},q_{(n+1)}^{(i)}\right) \neq \left(\alpha_1^{(j)},\alpha_2^{(j)},\alpha_3^{(j)},\ldots,\alpha_{(n-1)}^{(j)},\alpha_n^{(j)},\alpha_{(n+1)}^{(j)},q_{(n+1)}^{(j)}\right) \quad (11)$$

Сравнивая соотношения (11) и (4), можно отметить, что компоненты от $\alpha_1^{(i)}$ до $\alpha_n^{(i)}$ совпадают для случаев $k=n$ и $k=n+1$, и только последний компонент $q_n^{(i)}$ в нервенстве (4), заменяется двумя компонентами $\alpha_{(n+1)}^{(i)},q_{(n+1)}^{(i)}$ в неравенстве (11). Отсюда для (11) у нас имеется два варианта:

1. Либо ни один из компонентов от $\alpha_1^{(i)}$ до $\alpha_n^{(i)}$ не совпадает с компонентами от $\alpha_1^{(j)}$ до $\alpha_n^{(j)}$ в силу уравнений (5), (6),(7),…,(8) и (9) имеем $\Phi_{n+1}\left(\alpha^{(i)}\right) \neq \Phi_{n+1}\left(\alpha^{(j)}\right)$.

2. Либо компоненты от $\alpha_1^{(i)}$ до $\alpha_n^{(i)}$ совпадают с соответствующими компонентами от $\alpha_1^{(j)}$ до $\alpha_n^{(j)}$. В этом случае в уравнении (4) остался один компонент $q_n^{(i)}$, который не совпадает с компонентом $q_n^{(j)}$, из-за соотношения (10), которое говорит, что $q_n^{(i)} \neq q_n^{(j)}$. Однако этот компо-

нент при $k = n+1$ в уравнении (11) заменен двумя компонентами $\alpha^{(i)}_{(n+1)}, q^{(i)}_{(n+1)}$ и $\alpha^{(j)}_{(n+1)}, q^{(j)}_{(n+1)}$, поэтому в этой ситуации у нас опять возникает два варианта в неравенстве (11):

1. Либо остальные компоненты $\alpha^{(i)}_{(n+1)}, q^{(i)}_{(n+1)}$ совпадают с $\alpha^{(j)}_{(n+1)}, q^{(j)}_{(n+1)}$, тогда

$$q^{(i)}_{(n+1)} = q^{(j)}_{(n+1)} = q_{n+1}, \quad (12)$$

а также

$$\alpha^{(i)}_{(n+1)} = \alpha^{(j)}_{(n+1)} = \alpha_{n+1} \quad (13)$$

Поскольку из формул (11), (12), (13) и (4) следует, что $r = q^{(i)}_n * q^{(i)}_{(n+1)} + \alpha^{(i)}_{(n+1)}$ и тогда $q^{(i)}_n = \frac{r - \alpha^{(i)}_{(n+1)}}{q^{(i)}_{(n+1)}}$, то получаем

$$q_{ni} = \frac{r - \alpha_{n+1}}{q_{n+1}}, \quad (14)$$

а поскольку из (11), (12), (13) и (4) вытекает $r = q^{(j)}_n * q^{(j)}_{(n+1)} + \alpha^{(j)}_{(n+1)}$ и, следовательно $q^{(j)}_n = \frac{r - \alpha^{(j)}_{(n+1)}}{q^{(j)}_{(n+1)}}$, то получаем

$$q^{(j)}_n = \frac{r - \alpha_{(n+1)}}{q_{(n+1)}}. \quad (15)$$

Из уравнений (14) и (15) видно, что $q^{(i)}_n = q^{(j)}_n$. Таким образом, этот вариант исключается, поскольку он не соответствует начальному условию в данном пункте, а именно $q^{(i)}_n \neq q^{(j)}_n$.

2. Либо, по крайней мере, один из компонентов $\alpha^{(i)}_{(n+1)}, q^{(i)}_{(n+1)}$ не совпадает с компонентами $\alpha^{(j)}_{(n+1)}, q^{(j)}_{(n+1)}$, а это значит что $\Phi_{n+1}\left(\alpha^{(i)}\right) \neq \Phi_{n+1}\left(\alpha^{(j)}\right)$.

При A и B, совпадение последовательностей невозможно, т.е. если $\alpha^{(i)} \neq \alpha^{(j)}$, то имеем $\Phi_{n+1}\left(\alpha^{(i)}\right) \neq \Phi_{n+1}\left(\alpha^{(j)}\right)$. Таким образом, при A, B и C согласно принципу математической индукции, из $a^{(i)} \neq a^{(j)}$ вытекает, что $\Phi_n(a^{(i)}) \neq \Phi_n(a^{(j)})$ справедливо для любого натурального n. Теорема доказана.

Теорема 2. Целочисленное расщепление обратимо. При расщеплении символа A в соответствии с кодовой таблицей он превращается в последовательность k целых чисел. При этом доказательство этой теоремы носит очевидной характер, поскольку каждый шаг преобразования обратим по правилу: $\frac{(r-\alpha)}{q}$.

Теорема 3. Целочисленное расщепление определяется однозначно. Из Теоремы 1 мы получили, что целочисленное расщепление является мономорфизмом, т.е. два различных числа отображаются в виде двух неравных упорядоченных[3] последовательностей целых чисел. Это означает, что для двух различных чисел расщепление не может быть в виде различных упорядоченных последовательностей, т.е. каждое число расщепляется единственным образом.

Приведенные выше теоремы ведут к следующему следствию: расщепление символа A является мономорфизмом, обратимо, и однозначно восстановимо по расщеплению. Процедура расщепления применяется в данной работе к отдельным символам передаваемого текста.

Все теоремы допускают естественное обобщение, связанное с динамикой, возникающей в приложениях, а именно, можно рассматривать обобщенное расщепление уровня *k* по векторной базе:

$$\vec{r} = (r_1, ..., r_k).$$

В этом случае очередной (*i*-й) шаг процесса целочисленного расщепления выполняется при новом значении базы расщепления. Такое расщепление оказывается наиболее полезным в приложениях, связанных с защитой передаваемой информации.

3. Экспериментальные результаты

3.1. Контроль степени защиты информации

Следующие примеры показывают возможность контроля степени защиты информации с использованием метода целочисленного расщепления символа.

[3] Упорядоченность здесь понимается как отражение очевидного порядка построения компонентов расщепления, аналогично показанному на Рис. 1.

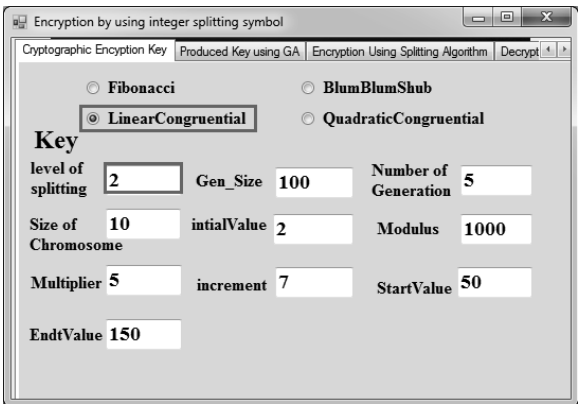

Рис. 2. Секретный ключ
(уровень целочисленного расщепления равен 2)

Рис. 3. Шифрованный текст
в согласии с секретным ключом
(уровень целочисленного расщепления равен 2)

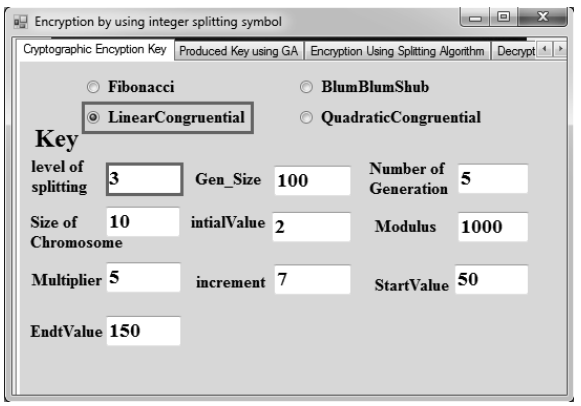

Рис. 4. Секретный ключ
(уровень целочисленного расщепления равен 3)

Рис. 5. Шифрованный текст
в согласии с секретным ключом
(уровень целочисленного расщепления равен 3)

Если уровень целочисленного расщепления символа равен 2. Для эксперимента был выбран исходный текст «A». Если выбирается секретный ключ как показано на Рис. 2, то мы получим шифрованный текст={901 332}, как показано на Рис. 3.

Если уровень целочисленного расщепления символа равен 3 для того же секретного ключа, как показано на Рис. 4, то мы получим шифрованный текст={973 368 339}, как показано на Рис. 5.

3.2. Применение целочисленного расщепления отображается различными сочетаниями целых чисел

Один и тот же символ отображается в системе с расщеплением разными сочетаниями двух чисел при *k=2*, как показано на Рис. 6. Каждый символ отображается различными сочетаниями трех чисел при *k=3*, как показано на Рис. 7.

Заключение

В настоящем исследовании был предложен новый математический подход, который представляет целое число по базе другого числа в виде последовательности из *k* целых чисел (расщепление *k*-го уровня), предназначенный, прежде всего, для использования в области контроля степени зашиты информации.[4] Определено понятие целочисленного расщепления целого числа, используемое также при расщеплении символов. Доказано, что так определенное целочисленное расщепление является однозначным, обратимым преобразованием и обладает свойством мономорфизма.

Программная часть работы была реализована с использованием языка C#. Разработанный метод тестировался на текстах из русских и английских символов и показал успешную работу.

[4] Заявка на изобретение была направлена авторами в ФИПС 8 декабря 2015 г.

Рис. 6. Зашифрованный текст отображается разными сочетаниями чисел (уровень расщепления равен 2)

Рис. 7. Зашифрованный текст отображается разными сочетаниями чисел (уровень расщепления равен 3)

Литература

1. Червяков Н.И., Ляхов П.А., Бабенко М.Г., Лавриненко И.Н., Лавриненко А.В. Компьютерные вычисления на основе модулярной алгебры. Издательско-информационный центр «Фабула». 2015,210 с.
2. Stefanyuk V.L., Alhussain A.H. Symmetric Encryption on the Base of Splitting Method// Bulletin of PFUR, Series Mathematics,Information Sciences, Physics. № 2. 2016, pp.53-61.
3. Стефанюк В.Л., Алхуссайн А.Х. Криптография и кодирование как методы защиты информации// Информационно-Телекоммуникационные Технологии и Математическое моделирование высокотехнологичных систем. М.: РУДН. 18-22 апреля 2016, с.181-182.
4. Стефанюк В.Л., Алхуссаин А.Х. Симметричное шифрование на основе метода расщепления// Естественные и технические науки. № 3 (93). 2016. Издательство «Спутник +», с.130-133.

Стефанюк Вадим Львович. Ведущий научный сотрудник Института проблем передачи информации РАН (ИППИ). Профессор Кафедры информационных технологий Российского университета дружбы народов. Окончил МГУ им. В.М. Ломоносова в 1962 году. Доктор технических наук. Автор 250 печатных работ. Область научных интересов: искусственный интеллект, коллективное поведение автоматов, мобильная радиосвязь, мета-экспертные системы, аксиоматика сбора свидетельств, транзакционный анализ в обучении, динамические экспертные системы, теоретико-категорные методы, цепи Маркова-Стефанюка, творческое решение задач, семиотическая интроспекция, целочисленная (модульная) арифметика, безопасная передача символьной информации, метод расщепления, интеллектуальные системы подготовки конференций. E-mail: stefanuk@iitp.ru

Алхуссайн Амани Хасн. Аспирантка Российского университета дружбы народов (РУДН). Окончила РУДН в 2013 году. Автор нескольких десятков статей. Область научных интересов: теория систем обеспечения безопасности передачи и хранения информации, практическое программирование соответствующих систем, применение детерминированного генетического алгоритма для улучшения вероятностных свойств псевдослучайных последовательностей. E-mail: amanie.alhussain@mail.ru

The control of the level of symbol information safety with the use of integer-valued splitting method
V.L. Stefanuk, A.H. Alhussain

Abstract: Application of module arithmetic in the problem of control of the level information safety is demonstrated in the paper with the use of a new technique referred to in the paper as integer-valued splitting. The basic definitions and concepts of the method are provided. Arousing mathematical mapping is described in details, its properties have been studied and the basic theorems have been proven with the purpose to justify the use of splitting in practical applications. The corresponding system for safe symbol transmission was programmed and used in the paper to illustrate some special features of the approach.
Keywords: module arithmetic, integer splitting method, level of splitting, integer-valued splitting properties, integer transformations, integer-valued symbol splitting.

Stefanuk Vadim Lvovich. Leading researcher in the Institute of Information Transmission Problems (IPPI RAS). He graduated from Moscow State University in 1962. He is Doctor of Technical Sciences since 1991. He is professor in the Department of Information Technologies in Peoples' Friendship University of Russia (RUDN). Author of 240 scientific works. His research interests include artificial intelligence, collective behavior of automata, mobile radio, meta-expert systems, axiomatic collecting of evidences, transactional analysis training, dynamic expert systems, theoretical and categorical methods, Markov-Stefanuk chains, creative problem solving, semiotic introspection, integer (modular) arithmetic, secure transmission of character information, splitting method, intelligent system for conference preparation. E-mail: stefanuk@iitp.ru

Alhussain Amanie Hasn. She graduated from Peoples' Friendship University of Russia (RUDN) in 2013. She is about to end her postgraduate studies at the Department of Information Technology in RUDN. Her research interests inclide the theory of systems for providing secured transmission and storage of information, practical programming of the relevant systems, and the usage of deterministic genetic algorithm for improving the probability properties of pseudo-random sequences. She published several dozens of papers and reports. Repeatedly her works received high praises, and were awarded diplomas. In the Rospatent located her application under consideration (jointly with Professor V.L. Stefanuk) on the new method for providing protection of the character information. Now she is preparing to defend her PhD thesis. E-mail: amanie.alhussain@mail.ru