МОДЕЛИРОВАНИЕ И УПРАВЛЕНИЕ В ТЕХНИЧЕСКИХ СИСТЕМАХ

УДК 003.26; 004.056

Современные информационные технологии криптографической защиты данных

М.Ю. Иванов

Братский государственный университет, ул. Макаренко 40, Братск, Россия
nis@brstu.ru
Статья получена 12.07.2015, принята 9.09.2015

Представлены результаты исследований базовых математических и алгоритмических аспектов симметричных криптографических преобразований информации путем замены (подстановки) и перестановки символов, а также гаммирования. Приводятся примеры работы блочного шифра с использованием Р-блоков и метода одиночной перестановки по паролю символов. Описаны криптоалгоритм функционирования и фрагменты программного кода, реализующего преобразование информации с помощью шифра TEA (задействованы биективные математические функции: сложение и исключающее «ИЛИ», а также битовые сдвиги), на основе классической сети Фейштеля с двумя ветвями по 32 бита. Предложен эффективный криптоалгоритм, надежность которого обусловлена тем, что перестановка символов осуществляется не на конкретно заданное, а на произвольное количество позиций, определяемое встроенным в среду разработки высококачественным датчиком псевдослучайных чисел. Показана возможность автоматизированного шифрования текстовых данных случайной перестановкой символов для защиты конфиденциальной информации, хранящейся в ненадежных источниках или при передаче ее по незащищенным каналам связи.

Ключевые слова: информационная безопасность; шифрование; симметричные криптографические системы; блочные шифры; информационные технологии; программное обеспечение.

Modern information technologies for data cryptographic protection

M.Yu. Ivanov

Bratsk State University; 40, Makarenko, Bratsk, Russia
nis@brstu.ru
Received 12.07.2015, accepted 9.09.2015

The research results has been presented for basic mathematical and algorithmic aspects of symmetric cryptographic transformations of information by replacing (substitution) and permutation of symbols as well as gamming. Some illustrative examples have been given describing the operation of the block cipher with P-blocks and a single permutation method of a password of symbols used. Cryptographic algorithm of operation has been described as well as fragments of a program code that implements the information transformation with a cipher TEA (involved bijective mathematical functions: addition and an exclusive «OR», as well as bit shifts), based on the classic Feistel's network with two 32-bit branches. An efficient cryptographic algorithm has been offered, the reliability of which is due to the fact that the permutation of symbols is not done on something particular predetermined but on any number of positions defined by the integrated software detector of pseudorandom numbers. The possibility has been demonstrated for automated encryption of text data by using random permutation of symbols to protect confidential information stored in the untrusted sources, as well as for transferring it over insecure channels.

Key words: information security; encryption; symmetric cryptographic systems; block ciphers; information technology; software.

Введение. Сегодня, в период развития информационной экономики, информация является обыкновенным товаром, то есть объектом купли-продажи. Многие западные фирмы преуспевают только благодаря тому, что могут получить необходимые сведения всего на несколько дней или часов раньше своих конкурентов. Соответственно, и значительная доля таких организаций рискует разориться в течение короткого промежутка времени после разглашения некоторых критически важных данных, лежащих в основе их деятельности.

Особый, нематериальный характер информации делает исключительно легким ее копирование и модифицирование, в силу чего она становится крайне привлекательным объектом различного рода правонарушений.

Защита информации является в настоящее время очень широким понятием, включающим в себя самые разнообразные методы и средства: от охранников в

дверях серверной или операционного зала до генераторов помех для «уносящих» информацию излучений, возникающих при работе электронно-вычислительной техники.

В данном исследовании из всего спектра инструментов информационной безопасности рассматриваются те, которые никак не связаны с характеристиками материальных носителей данных, а основаны на манипулировании самой информацией и используют лишь ее имманентные свойства. Речь пойдет об автоматизированных способах криптографического преобразования (шифрования) данных, поскольку использование современных информационных технологий способствует повышению эффективности любой сферы деятельности [1–9], в том числе и информационной безопасности.

Теоретические основы криптографии. Известно, что все существующие методы криптографического преобразования (шифрования) информации подразделяются на симметричные и асимметричные (двухключевые) [10–11].

Наиболее доступными для коммерческого использования являются симметричные способы шифрования, характеризующиеся более простыми и, соответственно, быстрыми операциями по преобразованию данных, не снижающими, впрочем, их надежность, поскольку криптоалгоритм при необходимости легче модифицировать [12].

Все многообразие симметричных криптосистем основывается на трех базовых криптоалгоритмах:

1. Алгоритм замены (подстановки) — наиболее простой и эффективный способ шифрования, заключающийся в замене символов исходного текста на другие символы того же или другого алфавита по заранее обусловленной схеме (моноалфавитная подстановка) [13]. Разновидностью алгоритмов замены являются распространенные сегодня блочные шифры (семейство обратимых преобразований блоков (частей фиксированной длины) исходного текста), то есть фактически блочный шифр представляет собой систему подстановки блоков. Методика создания цепочек из зашифрованных блочными алгоритмами последовательностей битов позволяет осуществлять криптографическое преобразование пакетов данных неограниченной длины, а отсутствие статистической корреляции между блоками используется для вычисления контрольных сумм пакетов данных при архивации и хэшировании.

2. Алгоритм перестановки — несложный метод криптографического преобразования, заключающийся в перестановке местами символов исходного текста по некоторому правилу (формуле) [14].

3. Гаммирование — символы шифруемого текста складываются с символами некоторой псевдослучайной последовательности (гаммой). Если же эта последовательность является истинно случайной (например, полученной с помощью физического датчика), и каждый ее фрагмент используется только один раз, возможно получение абсолютно стойкой криптосистемы с одноразовым ключом. Необходимо отметить, что гаммирование не всегда рассматривают как отдельный вид криптографических преобразований, поскольку псевдослучайная последовательность символов может вырабатываться, например, с помощью того же блочного шифра.

Таким образом, криптографические преобразования текстов сводятся к перестановкам (перемещениям), заменам (подстановкам) символов в строке или комбинациям обоих методов. Поскольку при перестановках коды символов не меняются, для шифрования текстовых файлов в большинстве случаев их можно использовать без всяких ограничений.

Традиционным видом блочного шифрования является применение так называемых P-блоков — таблиц перестановки (англ. *permutation box*), в которых открытые биты, буквы или символы исходного текста переставляются в некотором новом порядке (горизонтальном, вертикальном, двойном и т. д.). Ключом в данном случае является размер таблицы. Например, сообщение «МИЛЛИОН ЕВРО ПЕРЕЧИСЛЕН НА ВАШ СЧЕТ» записывается по столбцам в таблицу из пяти строк и шести столбцов (рис. 1).

М	О	О	Ч	Н	Ш
И	Н	П	И	Н	С
Л	Е	Е	С	А	Ч
Л	В	Р	Л	В	Е
И	Р	Е	Е	А	Т

Рис. 1. Исходное сообщение, распределенное в таблице из пяти строк и шести столбцов

Для получения шифрованного сообщения текст считывается по строкам и группируется, например, по пять букв, в результате чего получается следующая последовательность: МООЧН ШИНПИ НСЛЕЕ САЧЛВ РЛВЕИ РЕЕАТ.

Несколько большей стойкостью к раскрытию обладает метод одиночной перестановки по паролю символов. Он отличается от предыдущего тем, что столбцы таблицы переставляются по ключевому слову, фразе или набору чисел, совпадающему по длине со строкой таблицы. При использовании в качестве пароля, например, слова «САЛЬДО», получится схема, приведенная на рис. 2.

С	А	Л	Ь	Д	О
5	1	3	6	2	4
М	О	О	Ч	Н	Ш
И	Н	П	И	Н	С
Л	Е	Е	С	А	Ч
Л	В	Р	Л	В	Е
И	Р	Е	Е	А	Т

Рис. 2. Исходное сообщение, подготовленное к шифрованию по паролю

В верхней строке таблицы записан пароль, а номера под буквами определены в соответствии с естественным порядком соответствующих букв пароля в алфавите (если встречаются одинаковые буквы, то они нумеруются слева направо).

А	Д	Л	О	С	Ь
1	2	3	4	5	6
О	Н	О	Ш	М	Ч
Н	Н	П	С	И	И
Е	А	Е	Ч	Л	С
В	В	Р	Е	Л	Л
Р	А	Е	Т	И	Е

Рис. 3. Зашифрованное сообщение, распределенное в таблице в соответствии с паролем

При считывании и группировке текста по строкам по пять букв (рис. 3) получится последовательность ОНОШМ ЧННПС ИИЕАЕ ЧЛСВВ РЕЛЛР АЕТИЕ. Для повышения надежности результата преобразования уже зашифрованное сообщение можно зашифровать повторно, причем размеры второй таблицы должны отличаться, но вместе с тем оставаться симметричными первой таблице. Например, первая таблица может состоять из пяти строк и шести столбцов, а вторая таблица — из шести строк и пяти столбцов.

Таким образом, при реализации описанной выше схемы защиты посторонним лицам может быть известен алгоритм шифрования, но неизвестен небольшой фрагмент секретной информации — ключ, одинаковый как для отправителя, так и для получателя сообщения.

Достаточно длинный и не смысловой пароль способен создать уже значительные трудности при попытке взлома, если только злоумышленник не раздобудет фрагмент исходного текста, по которому, конечно же, легко восстановить весь пароль и расшифровать текст.

Практическая реализация методов криптографии. На сегодняшний день разработано достаточно много стойких блочных шифров, в алгоритмах которых используется определенный набор биективных математических функций. Таким образом, схему функционирования блочного шифра можно описать следующим образом: *Z = EnCrypt(X,Key), X = DeCrypt(Z,Key)*, где *Z* — зашифрованный блок данных; *X* — исходный блок данных; *Key* — ключ; *EnCrypt* — функция шифрования; *DeCrypt* — функция дешифрования.

Одним из самых простых в реализации, но признанно стойких, является блочный шифр TEA (англ. *Tiny Encryption Algorithm*), разработанный в 1994 г. учеными Кембриджского университета [15]. Параметры TEA следующие: размер блока — 64 бита, длина ключа — 128 битов.

В данном криптоалгоритме использована классическая сеть Фейштеля (нем. *Feistel*) с двумя ветвями по 32 бита каждая (рис. 4). Образующая функция *F* обратима. В качестве операции наложения используется арифметическое сложение. Также задействованы битовые сдвиги и исключающее «ИЛИ» (XOR).

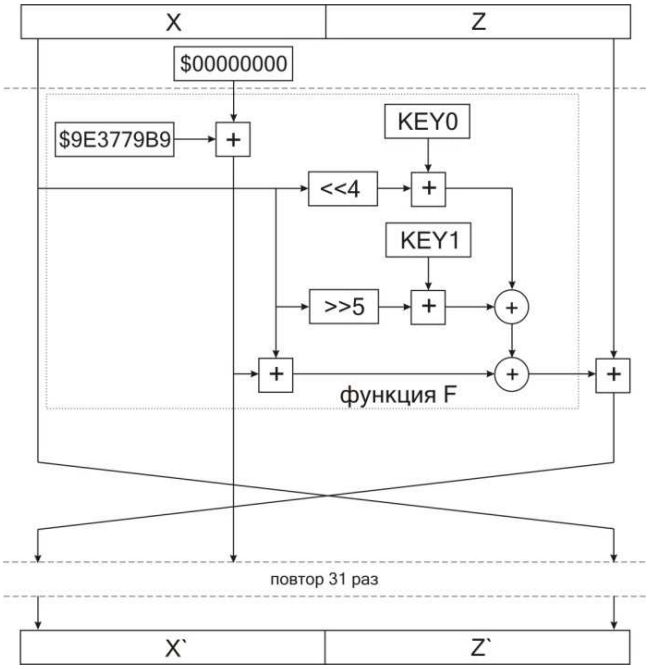

Рис. 4. Криптоалгоритм TEA

Криптопреобразования по алгоритму TEA могут быть описаны на языке программирования Pascal с помощью следующего фрагмента кода:

```
type
TLong2 = array[0..1] of longint;
TLong2x2 = array[0..1] of TLong2;
const
Delta = $9E3779B9;
var
key: TLong2x2;
procedure EnCryptRouting(var data);
var
y, z, sum: longint;
a: byte;
begin
y:= TLong2(data)[0];
z:= TLong2(data)[1];
sum:= 0;
for a:= 0 to 31 do
  begin
  inc(sum,Delta);
  inc(y,((z shl 4)+key[0,0]) xor
(z+sum) xor ((z shr 5)+key[0,1]));
  inc(z,((y shl 4)+key[1,0]) xor
(y+sum) xor ((y shr 5)+key[1,1]));
  end;
TLong2(data)[0]:= y;
TLong2(data)[1]:= z
end;
```

Для быстрой работы с целыми числами определены процедуры *Inc(X) X:=X+1* и *Inc(X,N) X:=X+N*. Квадратными скобками функции *key[0,0]* обозначено простое объединение («склеивание») двух блоков информации равной величины в один — удвоенной разрядности.

Отличительной чертой криптоалгоритма TEA являются малый размер исполняемого программного кода и простота операций над исходным текстом. Недостаток шифра TEA — это относительно низкое быстродействие из-за повторения цикла Фейштеля 32 раза, что необходимо для тщательного «перемешивания» данных.

С учетом вышеизложенного целесообразно предложить иной способ шифрования текстовой информации случайной перестановкой символов.

Следует отметить, что текст по-прежнему выступает основным средством передачи информации и представляет собой, как известно, набор абзацев, состоящих, в свою очередь, из строк. На работу со строками ориентированы все без исключения текстовые процессоры турбо-сред компиляторов, а также большинство других текстовых процессоров.

Большинство языков программирования высокого уровня предоставляют разработчику готовые средства для работы со строками переменной длины. Традиционно младший байт внутреннего представления такой строки содержит ее текущую длину, далее следуют символы строки от первого до последнего. Максимальная длина строки в таком представлении равна 256 символам. Иногда на описание текущей длины строки отводится два байта (например, в среде программирования Borland Delphi), в результате чего максимальная длина строки составляет уже 65 534 символа. В программах, написанных на языках программирования C и C++, широко используются строки теоретически неограниченной длины.

Разработанный криптоалгоритм преобразования исходного текста основан на традиционном блочном шифре (перестановка блоков сообщения определенной длины), но вместе с тем для повышения надежности шифрования перестановка символов осуществляется не на конкретно заданное, как в шифре TEA, а на произвольное количество позиций, определяемое встроенным в среду Borland C++ Builder высококачественным датчиком псевдослучайных чисел.

Таблица перестановок *CryptTab*, играющая роль гаммы шифра, также создается случайным образом при каждом запуске программы. Номер элемента *i* и соответствующее значение *CryptTab[i]* указывают положение переставляемых элементов в строке. Процедуры шифрования и дешифрирования отличаются направлением перебора символов строки.

Программа для ЭВМ реализована с помощью среды визуального проектирования Borland C++ Builder. На рис. 5 представлен фрагмент программного кода, реализующего шифрование текстовой информации, а на рис. 6 — главная рабочая форма программы.

Программа имеет Windows-ориентированный интерфейс и может быть использована для защиты конфиденциальной информации, хранящейся в ненадежных источниках или при передаче ее по незащищенным каналам связи.

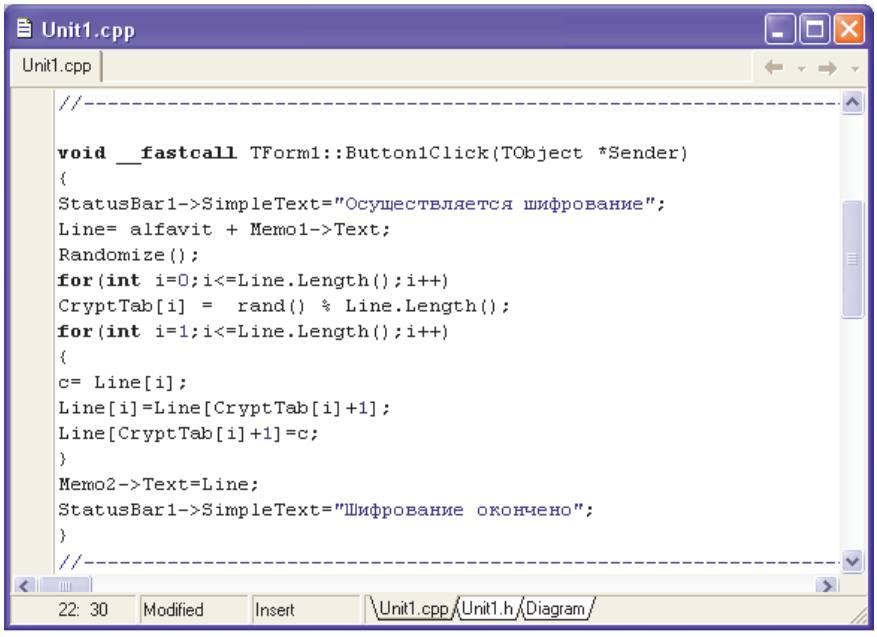

Рис. 5. Фрагмент программного кода

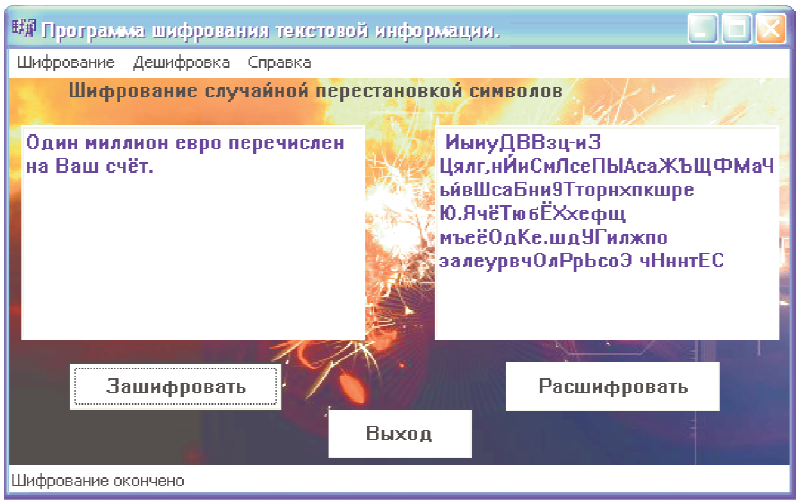

Рис. 6. Главная рабочая форма программы

Заключение

Рассмотрены теоретические основы симметричных методов криптографии на примере реализации блочных шифров. С учетом достоинств и недостатков популярного шифра TEA предложен эффективный криптоалгоритм, надежность которого обусловлена перестановкой символов не на конкретно заданное, а на произвольное количество позиций. С помощью среды визуального проектирования Borland C++ Builder разработана компьютерная программа для шифрования текстовых данных случайной перестановкой символов.

Литература

1. Иванов М.Ю. Структура и принципы функционирования экспертных систем для оценки деятельности хозяйствующего субъекта // Проблемы социально-экономического развития Сибири. 2012. № 3 (9). С. 18-22.

2. Иванов М.Ю. Экспертные системы для оценки деятельности хозяйствующего субъекта // Проблемы социально-экономического развития Сибири. 2012. № 3 (9).

3. Бабкин А.Л., Иванов М.Ю. Экспресс-оценка стратегии использования заемных средств ZaemSredstva v. 1.1: программа для ЭВМ. Св. ГР. № 2010615865 Рос. Федерация; зарег. в реестре Федер. службы по интеллектуальной собственности, пат. и товарным знакам 08.09.2010.

4. Бабкин А.Л., Иванов М.Ю. Оценка уровня профессионализма управления развитием и дивидендной политикой UpravRazvDivPolit v. 1.1: программа для ЭВМ. Св. ГР. № 2010615962 Рос. Федерация; зарег. в реестре Федер. службы по интеллектуальной собственности, пат. и товарным знакам 13.09.2010.

5. Бабкин А.Л., Иванов М.Ю. Сетевое планирование сложных работ SetPlanSlRab v. 1.1: программа для ЭВМ. Св. ГР. № 2011617043 Рос. Федерация; зарег. в реестре Федер. службы по интеллектуальной собственности, пат. и товарным знакам 12.09.2011.

6. Иванов М.Ю., Осинцев С.Ю. Автоматизированное обслуживание абонентов компьютерной сети AvtObsl AbKompSet v. 1.1: программа для ЭВМ. Св. ГР. № 2011617045 Рос. Федерация; зарег. в реестре Федер. службы по интеллектуальной собственности, пат. и товарным знакам 12.09.2011.

7. Иванов М.Ю. Автоматизированный кадровый учет коммерческого предприятия AvtoKadr v.1.1: программа для ЭВМ. Св. ГР. № 2012660195 Рос. Федерация; зарег. в реестре Федер. службы по интеллектуальной собственности, пат. и товарным знакам 13.11.2012.

8. Иванов М.Ю. Автоматизированный учет работ (заказов) автотранспортного предприятия AvtoTrans v. 1.1: программа для ЭВМ. Св. ГР. № 2013611968 Рос. Федерация; зарег. в реестре Федер. службы по интеллектуальной собственности, пат. и товарным знакам 11.02.2013.

9. Иванов М.Ю. Автоматизированный учет грузопассажирских железнодорожных перевозок AvtoGruzPasZhD v. 1.1: программа для ЭВМ. Св. ГР. № 2013613949 Рос. Федерация; зарег. в реестре Федер. службы по интеллектуальной собственности, пат. и товарным знакам 19.04.2013.

10. Иванов М.Ю., Ивахтин М.А., Ремизов И.А. Шифрование текстовой информации на основе дискретного логарифмирования CipherText v. 1.1: программа для ЭВМ. Св. ГР. № 2008614025 Рос. Федерация; зарег. в реестре Федер. службы по интеллектуальной собственности, пат. и товарным знакам 25.08.2008.

11. Иванов М.Ю. Шифрование текстовой информации методом возведения целых чисел в большие степени по модулю CipherTextStepMod v. 1.1: программа для ЭВМ. Св. ГР. № 2012613807 Рос. Федерация; зарег. в реестре Федер. службы по интеллектуальной собственности, пат. и товарным знакам 23.04.2012.

12. Иванов М.Ю. Современные методы цифровой подписи и шифрования информации // Труды Братского государственного университета. Сер. Экономика и управление. 2008. Т. 1. С. 153-157.

13. Иванов М.Ю. Шифрование текстовой информации методом замены блоков CiphTextBlock v. 1.1: программа для ЭВМ. Св. ГР. №2012613808 Рос. Федерация; зарег. в реестре Федер. службы по интеллектуальной собственности, пат. и товарным знакам 23.04.2012.

14. Иванов М.Ю. Шифрование текстовой информации методом блочных перестановок CipherTextBlock v. 1.1: программа для ЭВМ. Св. ГР. №2010615864 Рос. Федерация; зарег. в реестре Федер. службы по интеллектуальной собственности, пат. и товарным знакам 08.09.2010.

15. Wheeler D., Needham R. TEA, a tiny encryption algorithm. Lecture Notes in Computer Science. Leuven: Springer-Verlag, 1994. Vol. 1008. P. 363-366.

References

1. Ivanov M.Yu. The structure and principles of expert systems functioning to evaluate economic entity activity // Issues of Social - Economic Development of Siberia. 2012. № 3 (9). P. 18-22.

2. Ivanov M.Yu. Expert systems for economic entity activity assessment // Issues of Social - Economic Development of Siberia. 2012. № 3 (9).

3. Babkin A.L., Ivanov M.Yu. Rapid assessment strategy for the use of borrowed funds ZaemSredstva v. 1.1: programma dlya EVM. Sv. GR. № 2010615865 Ros. Federatsiya; zareg. v reestre Feder. sluzhby po intellektual'noi sobstvennosti, pat. i tovarnym znakam 08.09.2010.

4. Babkin A.L., Ivanov M.Yu. Assessing the level of professional development management and dividend policy UpravRazvDivPolit v. 1.1: programma dlya EVM. Sv. GR. № 2010615962 Ros. Federatsiya; zareg. v reestre Feder. sluzhby po intellektual'noi sobstvennosti, pat. i tovarnym znakam 13.09.2010.

5. Babkin A.L., Ivanov M.Yu. Network planning complex work SetPlanSlRab v. 1.1: programma dlya EVM. Sv. GR. № 2011617043 Ros. Federatsiya; zareg. v reestre Feder. sluzhby po intellektual'noi sobstvennosti, pat. i tovarnym znakam 12.09.2011.

6. Ivanov M.Yu., Osintsev S.Yu. Automated customer service network AvtObslAbKompSet v. 1.1: programma dlya EVM. Sv. GR. № 2011617045 Ros. Federatsiya; zareg. v reestre Feder. sluzhby po intellektual'noi sobstvennosti, pat. i tovarnym znakam 12.09.2011.

7. Ivanov M.Yu. Automated personnel account a commercial enterprise AvtoKadr v.1.1: programma dlya EVM. Sv. GR. № 2012660195 Ros. Federatsiya; zareg. v reestre Feder. sluzhby po intellektual'noi sobstvennosti, pat. i tovarnym znakam 13.11.2012.

8. Ivanov M.Yu. Automated accounting jobs (orders) motor transport enterprise AvtoTrans v. 1.1: programma dlya EVM. Sv. GR. № 2013611968 Ros. Federatsiya; zareg. v reestre Feder. sluzhby po intellektual'noi sobstvennosti, pat. i tovarnym znakam 11.02.2013.

9. Ivanov M.Yu. Automated accounting utility rail traffic AvtoGruzPasZhD v. 1.1: programma dlya EVM. Sv. GR. № 2013613949 Ros. Federatsiya; zareg. v reestre Feder. sluzhby po intellektual'noi sobstvennosti, pat. i tovarnym znakam 19.04.2013.

10. Ivanov M.Yu., Ivakhtin M.A., Remizov I.A. Text information encryption based on the discrete logarithmization CipherText v. 1.1: programma dlya EVM. Sv. GR. № 2008614025 Ros. Federatsiya; zareg. v reestre Feder. sluzhby po intellektual'noi sobstvennosti, pat. i tovarnym znakam 25.08.2008.

11. Ivanov M.Yu. Text information encryption by method of integers involution to a large power, modulo CipherTextStepMod v. 1.1: programma dlya EVM. Sv. GR. № 2012613807 Ros. Federatsiya; zareg. v reestre Feder. sluzhby po intellektual'noi sobstvennosti, pat. i tovarnym znakam 23.04.2012.

12. Ivanov M.Yu. Advanced methods of digital signature and data encryption // Trudy Bratskogo gosudarstvennogo universiteta. Ser. Ekonomika i upravlenie. 2008. T. 1. P. 153-157.

13. Ivanov M.Yu. Text information encryption by replacing blocks method CiphTextBlock v. 1.1: programma dlya EVM. Sv. GR. №2012613808 Ros. Federatsiya; zareg. v reestre Feder. sluzhby po intellektual'noi sobstvennosti, pat. i tovarnym znakam 23.04.2012.

14. Ivanov M.Yu. Text information encryption by block permutations method CipherTextBlock v. 1.1: programma dlya EVM. Sv. GR. №2010615864 Ros. Federatsiya; zareg. v reestre Feder. sluzhby po intellektual'noi sobstvennosti, pat. i tovarnym znakam 08.09.2010.

15. Wheeler D., Needham R. TEA, a tiny encryption algorithm. Lecture Notes in Computer Science. Leuven: Springer-Verlag, 1994. Vol. 1008. P. 363-366.