Чипига Александр Федорович
Северо-Кавказский государственный технический университет
E-mail: zik@ncstu.ru.
355003, Ставрополь, ул. Морозова, 105, кв. 15.
Тел.: 8 (9624) 44-10-70.
Заведующий кафедрой информационной безопасности.

Chipiga Alexander Fedorovich
North Caucasus State Technical University.
E-mail: zik@ncstu.ru.
App. 15, 105, Morozova str., Stavropol, Russia.
Phone: 8 (9624) 44-10-70.
head of Information Security department

УДК 681.3

И.А. Калмыков, А.А. Чипига, А.В. Барильская, О.А. Кихтенко

КРИПТОГРАФИЧЕСКАЯ ЗАЩИТА ДАННЫХ В ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЯХ НА БАЗЕ НЕПОЗИЦИОННЫХ ПОЛИНОМИАЛЬНЫХ СИСТЕМ

Рассмотрен алгоритм нелинейного шифрования потока данных с операцией возведения в степень элементов расширенных полей Галуа $GF(p^v)$. Представлена структура устройства для вычисления индекса элемента поля Галуа.

Нелинейное шифрование; расширенные поля Галуа; элементы полей Галуа; полиномиальная система классов вычетов; индекс.

I.A. Kalmikov, A.A. Chipiga, A.V. Baril'skaya, O.A.Kikhtenko

CRYPTOGRAPHIC PROTECTION OF DATA IN INFORMATION TECHNOLOGY ON BASE NEPOZICIONNYH POLYNOMIAL SYSTEMS

Algorithm for non-linear encryption of a data flow with elements of extended Galois $GF(p^v)$ fields involution operation. Device structure for Galois field element index calculation is offered.

Non-linear encryption; extended Galois $GF(q^v)$; elements of extended Galois $GF(q^v)$ polynomial system of residue classes; index.

В стратегии развития Российского государства в качестве одного из приоритетов определена национальная безопасность, одним из важнейших элементов последней является информационная безопасность. Именно поэтому разработка безопасных и эффективных информационных систем является одним из приоритетных направлений развития РФ. Решая задачи создания новых технологий информационной безопасности, необходимо сочетать, с одной стороны, высокую скорость обработки и передачи больших объемов информации, а с другой – ограничения доступа к ней, обеспечивая требуемый уровень защиты информации.

Проведенный анализ работ [1,2] показал, что современные системы криптографической защиты информации не позволяют в полной мере решить данную

проблему. Существующие методы поблочного шифрования, обеспечивая требуемый уровень защиты информации от НСД, характеризуются низкой скоростью зашифрования из-за многократно выполняемых раундов (итераций). Асимметричные системы шифрования также не позволяют обеспечить реальный масштаб времени обработки данных. Системы побитового шифрования потока данных обеспечивают высокую скорость зашифрования и расшифрования. Однако данная система криптографической защиты уязвима к атакам на основе исходных и подобранных текстов из-за того, что при побитовом шифровании операция суммирования по модулю 2 является единственным способом построения обратимой функции шифрования.

Применение полиномиальной системы классов вычетов (ПСКВ) позволяет разрабатывать криптографические процедуры защиты информации, обладающие всеми достоинствами систем нелинейного шифрования, обеспечивающие реальный масштаб времени закрытия информации и операций, связанных со сложением, умножением, возведением в степень элементов расширенных полей Галуа $GF(q^{\nu})$, а также их различных комбинаций позволит существенно улучшить обеспечение конфиденциальности и целостности информации.

Рассмотрим реализацию нелинейного шифрования потока данных с операцией умножения символов конечного поля $GF(q^{\nu})$. В этом случае поток данных разбивается на блоки длиной ν разрядов. При этом полученный блок представляется как полином степени не выше l. Для шифрования символов открытого текста будут применяться ключевая последовательность, полученная с помощью генератора псевдослучайной последовательности конечного поля. При этом используется целое число l, где $l = 1,2,...,2^{\nu} - 2$, которое выбирается заранее и может быть использовано постоянно на каждом такте работы регистра сдвига или меняться по случайному или квазислучайному закону. В этом случае нелинейное шифрование блока открытых данных будет определяться выражением

$$x(z) \cdot y(z)^{l} \equiv \beta(z) \bmod q(z), \qquad (1)$$

где $y(z)$ – полиномиальная форма представления псевдослучайной последовательности элементов поля $GF(q^{\nu})$; $\operatorname{ord} y(z) \le \nu$.

Псевдослучайные последовательности элементов расширенных полей Галуа $GF(q^{\nu})$ могут сниматься с различных ячеек (линий задержек) регистра сдвига и в различной последовательности. При этом будут создаваться различные псевдослучайные последовательности символов конечных полей, причем каждая из них не будет циклически сдвинутой относительно другой ПСП. Это позволяет за счет применения порождающих алгоритмов создавать адаптивные криптографические системы высокой стойкости путем задания неопределенности хода шифрования.

Как показано в ряде работ [3 – 5], для сокращения выполнения мультипликативных операций по модулю, целесообразно использовать индексы элементов полей Галуа $GF(q^{\nu})$, порожденных неприводимым полиномом $p(z)$. На рис. 1 приведена структура устройства нелинейного шифрования в полиномиальной системе классов вычетов, реализующего алгоритм (1).

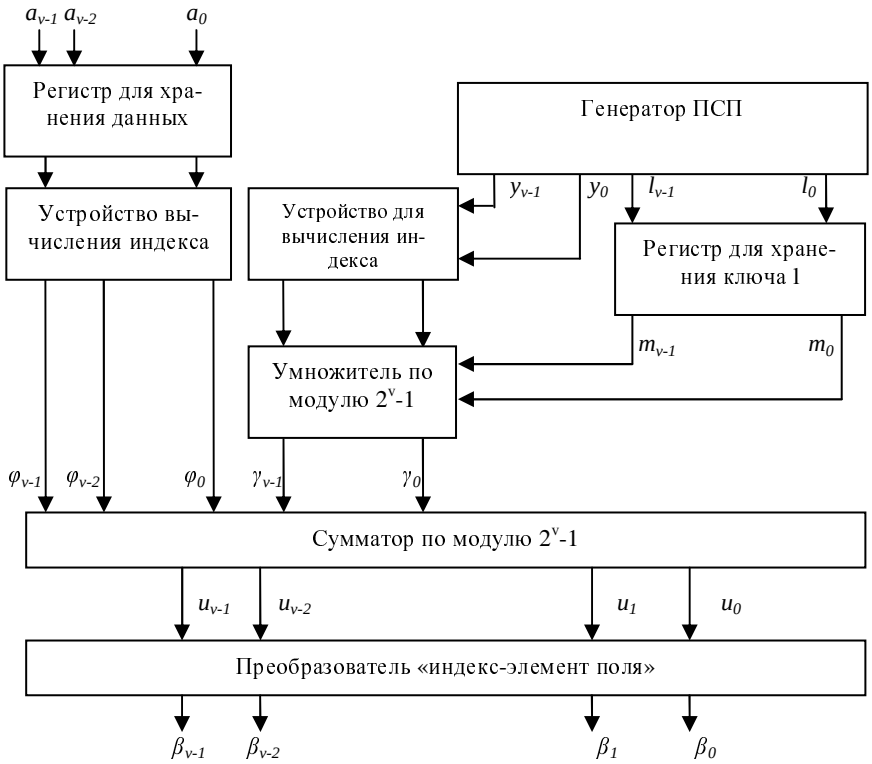

Рис. 1. Структура шифратора

Устройство работает следующим образом. С генератора ПСП на входы устройств выбора l и выбора $y(z)$ подаются биты, снятые с ячеек регистров сдвига. Под действием управляющего сигнала определяется последовательность элементов поля $GF(q^v)$, т.е. значения l и $y(z)$. Последнее поступает на блок определения индекса элемента, с выхода которого двоичный код поступает на первый вход умножителя по модулю $M = q^v - 1$, на второй вход которого подается значение l, представленное в двоичном коде. С выхода модулярного умножителя снимается результат

$$\gamma = l \cdot m \bmod q^v - 1, \tag{2}$$

где m – это индекс элемента $y(z)$ в расширенном поле Галуа $GF(q^v)$.

Параллельно с этим открытый текст в виде двоичного кода степени меньше v записывается в регистр для временного хранения. С выхода регистра двоичный параллельный код подается на блок определения индекса элемента поля $GF(q^v)$. Вычисленное значение индекса

$$\varphi = \sum_{j=0}^{\nu-1} 2^j \cdot \varphi_j \qquad (3)$$

поступает на второй вход сумматора по модулю $q^{\nu}-1$, который реализует алгоритм

$$U = \varphi + \gamma \bmod q^{\nu} - 1 = \varphi + (l \cdot m \bmod q^{\nu} - 1) \bmod q^{\nu} - 1. \qquad (4)$$

Полученный результат в двоичном коде подается на преобразователи индекс-элемент поля Галуа, благодаря которому справедливо сравнение

$$\beta(z) = g^u \bmod p(z), \qquad (5)$$

где g – первообразный элемент мультипликативной группы.

В ходе исследований была проведена сравнительная оценка выполнения нелинейного шифрования в ПСКВ с использованием индексного представления и без него. Известно, что для вычисления степени a^n, где a – элемент некоторого кольца достаточно выполнить $2\left[\log_2 n\right]$ умножений. Тогда время реализации выражения (1) без индексного представления будет определяться

$$T_1 = T_{умн} + 2 \cdot \left[\log_2 n\right] T_{умн} = (2\left[\log_2 n\right] + 1) \cdot T_{умн},$$

где $T_{умн}$ – время выполнения операции умножения. Если использовать комбинационные умножители, которые характеризуются минимальными временными задержками и положить, что сумматор содержит три логических ступени, то

$$T_1 = 3a \cdot t_{зд.р.} \left(2\left[\log_2 n\right] + 1\right), \qquad (6)$$

где $t_{зд.р.}$ – время задержки распространения сигналов.

Проведя анализ структуры разработанного шифратора, очевидно, что время на выполнение операции нелинейного шифрования

$$T_2 = T_{уст.выб.} + T_{эл-индекс} + T_{мод.умн.} + T_{мод.сум.} + T_{индекс-эл}. \qquad (7)$$

В работах [4 – 6] представлены устройства реализации операции преобразования элемент – индекс и обратно. Проведенные исследования показали, что

$$T_{эл-индекс} = T_{индекс-эл} = T_{НЕ} + T_{И} + T_{CD} = t_{зд.р.} + t_{зд.р.} + 3t_{зд.р.} = 5t_{зд.р.}, \qquad (8)$$

где $T_{НЕ}$, $T_{И}$ – время срабатывания элементов И, НЕ соответственно;

T_{CD} – время отклика шифратора.

Проведя анализ известных схемных решений модульных умножителей и сумматора, было определено, что если положить, что $T_{мод.умн.} = T_{мод.сум.} = T_{умн.}$, то имеем

$$T_2 = 15t_{зд.р.} + 6at_{зд.р.} = (15 + 6a)t_{зд.р.}. \quad (9)$$

Сравнительная характеристика временных затрат на выполнение нелинейного шифрования с использованием индексного представления и без него показана на рис. 1. Полученные результаты свидетельствуют о том, что применение индексов позволило повысить быстродействие нелинейного шифрования. При этом при увеличении разрядности обрабатываемых данных возрастает и выигрыш в производительности.

Процедура дешифрования принятого сообщения сводится к выполнению следующего выражения

$$\beta(z) \cdot y(z)^{-l} \equiv \alpha \bmod p(z). \quad (10)$$

Вычисление величины $y(z)^{-l} \bmod p(z)$ на приемной стороне может быть сведено к возведению элементов поля $GF(q^v)$ в степень l по модулю $p(z)$ и вычислению полинома. Для сокращения времени дешифрования можно также использовать индексное представление элементов поля Галуа.

Рассматривая вопросы разработки систем криптографической защиты информации, функционирующей в ПСПВ, нельзя не отметить, что организация безопасной связи внутри групп абонентов с динамически меняющимся составом участников является актуальной задачей в незащищенной среде. Для предотвращения несанкционированного доступа со стороны лиц, не входящих в группу, необходимо вычисление некоторого общего секретного ключа, который может быть определен только участниками группы. При этом каждый абонент группы должен участвовать в генерации секретного ключа [1].

Простейшей схемой получения общего ключа для группы абонентов является схема с доверенным сервером, в котором один из пользователей посылает ему запрос на связь с абонентами, а сервер рассылает каждому абоненту общий ключ для связи внутри группы и список участников группы в зашифрованном виде. Но при такой схеме возникают сложности при высокой динамичности группы [1]. Поэтому для обеспечения доступа к конфиденциальному ресурсу в многопользовательской информационной среде используются криптографические протоколы разделения секретов.

Существует несколько алгоритмов разделения секретного ключа на секретные доли. Но все они предполагают, что ни один абонент группы не сможет вычислить пароль без помощи других абонентов группы. При этом любая схема разделения секрета состоит из двух взаимосвязанных протоколов: протокола формирования и распределения долей секрета между абонентами и протокола восстановления секрета группой пользователей с помощью их секретных долей. Первый протокол описывает последовательность действий системы и пользователей, в результате которых каждый авторизованный абонент получает свою долю секретно-

го ключа. Второй протокол предназначен для того, чтобы законные пользователи, собравшись вместе и объединив свои секретные доли, могли восстановить секретный ключ.

В данной работе рассматривается пороговая схема (m,n) разделения секрета с использованием полиномиальной системы классов вычетов.

В данной схеме используются неприводимые полиномы $p_i(z)$. Для реализации (m,n)-пороговой схемы разделения секрета выбирается полином $p_l(z)$, степень которого превышает полиномиальную форму секрета $M(z)$, т.е.

$$\operatorname{ord} p_l(z) > \operatorname{ord} M(z), \tag{11}$$

где M – секрет.

Затем выбираются неприводимые полиномы $p_i(z)$, удовлетворяющие условию

$$\operatorname{ord} p_i(z) \le \operatorname{ord} p_l(z), \tag{12}$$

где $i=1,2,...,n$.

При этом степени полиномов должны быть упорядочены по возрастанию

$$\operatorname{ord} p_1(z) < \operatorname{ord} p_2(z) \le \operatorname{ord} p_3(z) ... \le \operatorname{ord} p_n(z). \tag{13}$$

Для создания (m,n) схемы проверяется выполнение условия

$$\operatorname{ord}(p_1(z)\cdot p_2(z)\cdot ... p_m(z)) > \operatorname{ord}(p_l(z)\cdot p_{n-m+2}(z)\cdot p_{n-m+3}(z) ... p_n(z)). \tag{14}$$

Чтобы определить доли секрета и их распределить между абонентами группы, выбирается полином $r(z)$ и вычисляется значение

$$M^*(z) = M(z) + r(z)\cdot p_l(z). \tag{15}$$

В качестве долей для каждого пользователя выступают остатки

$$M_i^*(z) \equiv M(z) \bmod p_i(z). \tag{16}$$

Используя китайскую теорему об остатках, m пользователей способны восстановить значение $M^*(z)$, а затем, зная $r(z)$ и $p_l(z)$, определить секрет $M(z)$. При этом группа из $m-1$ абонентов не способна будет получить значение $M(z)$. Для эффективной работы (m,n) схемы разделения секрета в ПСКВ необходимо определить предельное значение полинома $r(z)$, которое позволило бы

при меньших временных затратах определить $M^*(z)$, а также выполнить преобразование обратное (16).

Теорема. Если в (m,n) модулярной полиномиальной пороговой схеме, в которой справедливо

$$\operatorname{ord} p_1(z) \le \operatorname{ord} p_2(z) \le ... \le \operatorname{ord} p_n(z),$$

имеет место соотношение

$$\operatorname{ord} r(z) < \operatorname{ord}(P(z)/\, p_l(z)), \tag{17}$$

где $P(z) = \prod_{i=1}^{n} p_i(z)$ – полный диапазон, то такая пороговая схема обеспечивает восстановление секрета $M(z)$ для любого набора m пользователей группы, состоящей из n абонентов.

Доказательство.

Известно, что для получения долей в полиномиальной модулярной (m,n) пороговой схеме производится вычисление полинома-образа

$$M^*(z) = M(z) + r(z) \cdot p_l(z), \tag{18}$$

где $M(z)$ – секрет; $p_l(z)$ – неприводимый полином.

При этом необходимо

$$\operatorname{ord} M(z) < \operatorname{ord} p_l(z). \tag{19}$$

Так система неприводимых полиномов $p_i(z)$, $i = 1,2,...,n$ упорядочена по степеням, что для однозначного восстановления секрета $M(z)$ необходимо обеспечить

$$\operatorname{ord} M(z) < \operatorname{ord} P_m(z), \tag{20}$$

где $P_m(z) = \prod_{i=1}^{m} p_i(z)$ – произведение наименьших выбранных неприводимых полиномов.

При этом очевидно, что справедливо неравенство

$$\operatorname{ord} M^*(z) < \operatorname{ord} P(z), \tag{21}$$

где $P(z)=\prod_{i=1}^{n} p_i(z)$ – полный диапазон.

Разделим обе стороны выражения (18) на значение $p_l(z)$

$$\left[\frac{M^*(z)}{p_l(z)}\right]=\left[\frac{M(z)+r(z)p_l(z)}{p_l(z)}\right], \qquad (22)$$

где $[\ ]$ – наименьшее целое.

Проведя преобразование выражения (22), получаем

$$\left[\frac{M^*(z)}{p_l(z)}\right]=\left[\frac{M(z)}{p_l(z)}\right]+\left[\frac{r(z)p_l(z)}{p_l(z)}\right]. \qquad (23)$$

Но согласно неравенству (20)

$$\left[\frac{M(z)}{p_l(z)}\right]=0\ .$$

Тогда

$$\left[\frac{M^*(z)}{p_l(z)}\right]=r(z)\ . \qquad (24)$$

Используя условие (21), получаем

$$\operatorname{ord}\left(\frac{P(z)}{p_l(z)}\right)>\operatorname{ord} r(z)\ .$$

Теорема доказана.

Рассмотрим пример. Пусть в качестве исходного полинома выбрали $p_l(z)=z^4+z+1$. Значение секрета равно $M(z)=z^3$. Необходимо построить $(3,4)$ пороговую схему, функционирующую в полиномиальной системе классов вычетов. Выбираем неприводимые полиномы $p_1(z)=z+1$; $p_2(z)=z^2+z+1$; $p_3(z)=z^4+z^3+z^2+z+1$; $p_4(z)=z^4+z^3+1$. Данный набор многочленов определяет полный диапазон

$$P(z) = \prod_{i=1}^{4} p_i(z) = z^{11} + z^8 + z^7 + z^5 + z^3 + z^2 + z + 1\frac{1}{2}.$$

Определим значение диапазона

$$P_m(z) = \prod_{i=1}^{3} p_i(z) = z^7 + z^6 + z^5 + z^2 + z + 1.$$

Согласно условию (15) имеем

$$\operatorname{ord} r(z) < \operatorname{ord}\left(\frac{P(z)}{p_l(z)}\right) = 7.$$

Пусть $r(z) = z^6$.

Для определения образа $M^*(z)$ воспользуемся выражением (15). Имеем

$$M^*(z) = (z^3 + z^6 \cdot (z^4 + z + 1)) \bmod P_m(z) = z^6 + z^5 + z^3 + z^2.$$

Определим доли секретов секрета $M(z)$:

$$M_1^*(z) = M^* \bmod p_1(z) = 0,$$

$$M_2^*(z) = M^* \bmod z^2 + z + 1 = 0,$$

$$M_3^*(z) = M^* \bmod z^4 + z^3 + z^2 + z + 1 = z^3 + z^2 + z + 1,$$

$$M_4^*(z) = M^* \bmod z^4 + z^3 + 1 = z^3.$$

Пусть в восстановлении секрета $M(z)$ будут участвовать первый, третий и четвертый пользователи. Они обмениваются значениями $M_1^*(z)$, $p_1^*(z)$, $M_3^*(z)$, $p_3^*(z)$, $M_4^*(z)$, $p_4^*(z)$ и вычисляют ортогональные базисы:

$$B_1 = z^8 + z^4 + z^2 + z + 1.$$

$$B_3 = z^6 + z^5 + z^4 + z^3 + z^2 + 1.$$

$$B_4 = z^8 + z^6 + z^5 + z^3 + z + 1.$$

Затем, определив свое значение

$$P_3(z) = p_1(z) \cdot p_3(z) \cdot p_4(z) = z^9 + z^8 + z^5 + z^4 + z^3 + 1,$$

используют китайскую теорему об остатках (КТО) для восстановления образа $M^*(z)$:

$$M^*(z) = (M_1^*(z) \cdot B_1(z) + M_3^*(z) \cdot B_3(z) + M_4^*(z) \cdot B_4(z)) \bmod P_3(z) =$$
$$= (z^{11} + z^8 + z^7 + z^6 + z + 1) \bmod z^9 + z^8 + z^5 + z^4 + z^3 + 1 = z^6 + z^5 + z^3 + z^2.$$

Зная значение $r(z) = z^6$ и используя выражение

$$M(z) = M^*(z) + r(z) p_l(z),$$

данные абоненты восстанавливают секрет $M(z) = z^3$.

Представленные в статье материалы свидетельствуют о целесообразности применения системы классов вычетов для обеспечения более высокой степени криптографической защиты потока данных.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. *Шнайер Б.* Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си [Текст] / М.: Изд-во “ТРИУМФ”, 2003. – 816 с.

2. *Иванов М.А.* Теория, применение и оценка качества генераторов псевдослучайных последовательностей [Текст] / М.А. Иванов, И.В. Чугунов // М.: КУДИЗ-ОБРАЗ, 2003. – 240 с.

3. *Чипига А.А.* Алгоритм обеспечения информационной скрытности для адаптивных средств передачи информации [Текст]/ И.А. Калмыков, А.А. Чипига // Инфокоммуникационные технологии. –2007. – №3. – С. 159 – 162.

4. *Калмыков И.А.* Устройство для вычисления индекса элементов поля Галуа по модулю [Текст]/ И.А. Калмыков, А.В. Барильская, О.А. Кихтенко // Успехи современного естествознания / Материалы заочной электронной конференции «Современные телекоммуникационные и информационные технологии», Российская Академия Естествознания. – М., 2007.

5. *Калмыков, И.А.* Алгоритм обеспечения информационной скрытности для адаптивных средств защиты информации [Текст]/ И.А. Калмыков, А.В. Барильская, О.А. Кихтенко // Материалы VIII Всероссийского конкурса студентов и аспирантов по информационной безопасности «SIBINFO-2008». – Томск: ТГУСУР, 2008.

6. *Калмыков И.А.* Обеспечение информационной скрытности для адаптивных средств защиты информации. Алгоритм нелинейного шифрования [Текст]/ И.А. Калмыков, А.В. Барильская, О.А. Кихтенко // Материалы Третьей международной научно-технической конференция «Инфокоммуникационные технологии в науке, производстве и образовании». – Ставрополь: СевКавГТУ, 2008.

Калмыков Игорь Анатольевич
Северо-Кавказский государственный технический университет
E-mail: kia762@yandex.ru.
355040 г. Ставрополь, ул. Шпаковская 92/1, кв. 28.
Тел.: 8 (903) 4163533.
Профессор.

Kalmikov Igor Anatolievich
North Caucasus State Technical University

E-mail: kia762@yandex.ru.
App 28, 92/1 Shpakovskaya str., Stavropol, 355040, Russia.
Phone: 8 (903) 4163533.
Professor.

Чипига Александр Александрович
Северо-Кавказский государственный технический университет
E-mail: zik@ncstu.ru.
355003, Ставрополь, ул. Морозова, 105, кв. 15.
Тел.: 8 (9624) 50-19-28.
Аспирант кафедры защиты информации.

Chipiga Alexander Aleksandrovich
North Caucasus State Technical University.
E-mail: zik@ncstu.ru.
App. 15, 105, Morozova str., Stavropol, Russia.
Phone: 8 (9624) 50-19-28.
Post-graduate student of Information Security department.

Барильская Анастасия Валерьевна
Северо-Кавказский государственный технический университет.
E-mail: stasya-super@yandex.ru.
355019,г. Ставрополь, ул. Биологическая, 8, кв. 26.
Тел.: 8 (905) 4437060.
Аспирантка.

Baril'skaya Anastasiya Valerievna
North Caucasus State Technical University.
E-mail: stasya-super@yandex.ru.
App. 26, 8, Biologicheskaya str., Stavropol, 355019, Russia.
Phone: 8 (905) 4437060.
Post-graduate student.

Кихтенко Ольга Александровна
Северо-Кавказский государственный технический университет.
E-mail: koa87@list.ru.
355057, г. Ставрополь, ул. Шпаковская, 70/2, кв. 40.
Тел.: 8 (962) 4412046.
Аспирантка.

Kikhtenko Olga Aleksandrovna
North Caucasus State Technical University.
E-mail: stasya-super@yandex.ru.
App. 40, 70/2, Shpakovskaya str., Stavropol, 355057, Russia.
Phone: 8 (905) 4437060.
Post-graduate student.