УДК

М.Н. Мандрона, В.Н. Максымовыч

СРАВНИТЕЛЬНЫЙ АНАЛИЗ ГЕНЕРАТОРОВ ПСЕВДОСЛУЧАЙНИХ БИТОВИХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ

Введение

В современном информатизированном мире псевдослучайные числа широко используются в различных областях науки и техники, в частности, в системах защиты информации, в современных телекоммуникационных системах, в измерительной технике. В сфере защиты информации псевдослучайные числа применяют для потокового шифрования каналов связи, генерирования ключей для криптосистем, хеширования информации, формирования цифровой подписи, для создания разного рода зашумлений и т.д. Установлено, что характеристики систем безопасности зависят от характеристик их криптографических подсистем, которые определяются не только использованными методами, но и качественными показателями использованных псевдослучайных последовательностей. Поскольку безопасность криптосистемы сосредоточена на ключе, то при использовании ненадежного процесса генерации ключей вся криптосистема становится уязвимой.

Разработка генераторов ведется издавна, количество их типов большое, но критичным во многих случаях является быстродействие таких генераторов с сохранением статистической безопасности. Именно поэтому разработка аппаратно простых, быстродействующих и одновременно надежных генераторов псевдослучайных битовых последовательностей актуальна. В настоящее время известные генераторы хотя и являются быстродействующими и аппаратно простыми, однако не всегда соответствуют требованиям случайности, а построение криптостойких генераторов обычно сопровождается потерей производительности и усложнением структуры. Все эти параметры, как правило, находятся в противоречии.

Цель настоящей работы — сравнение генераторов псевдослучайных битовых последовательностей (ГПСБП) на основе модифицированных аддитивных генераторов Фибоначчи со стохастическими генераторами на основе R-блоков, которые известны как криптостойкие.

Основная часть

В предыдущих исследованиях [1–4] было установлено, что аддитивные генераторы Фибоначчи (АГФ), несмотря на простую аппаратную реализацию, формируют последовательности, которые не отвечают требованиям случайности, согласно методике NIST [5]. Произведя некоторые модификации, удалось улучшить их статистические характеристики и увеличить период повторения [2–4, 6, 7].

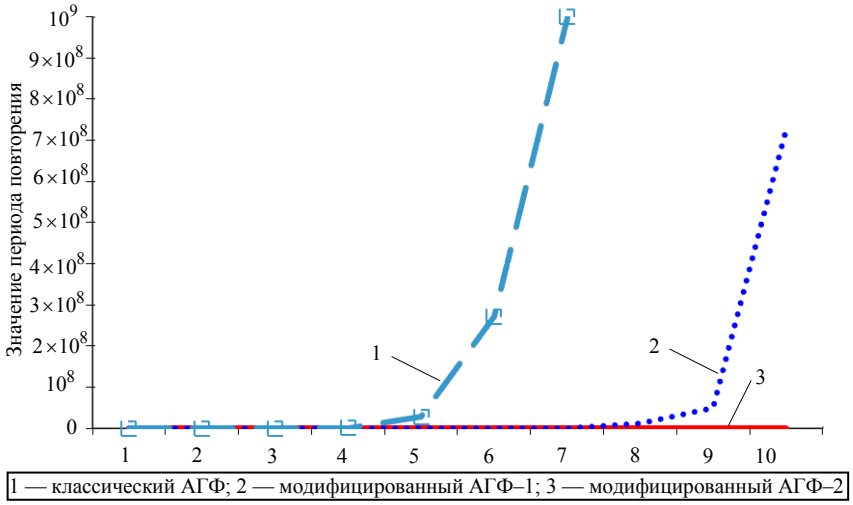
Модификация осуществлялась двумя способами. В первом, за счет дополнения классической схемы АГФ, логической схемой (ЛС) [2-4], привнесшей в работу генератора дополнительный элемент, тем самым вызвав некую путаницу. Во втором варианте мы предложили блок, содержащий комбинационный сумматор (КС) два счетчика (Сч 1 и Сч2), два блока сумматоров по модулю два (БСМ1 и БСМ2) и ЛС [4, 6, 7]. Этот блок назван блоком обеспечения статистической безопасности (БОСБ). Сравнив их характеристики (периоды повторения, статистические характеристики, линейную сложность и сложность построения) с классическим вариантом, определили существенное улучшение качества выходной последовательности. В табл. 1 и на рис. 1 приведены результаты исследования периодов повторения классического и модифицированных аддитивных генераторов Фибоначчи (МАГФ).

 ISSN 0572-2691

Таблица 1

Количество разрядов	Классический АГФ	Модифицированный АГФ	
		АГФ-1	АГФ-2
1	7	4	12
2	14	26	345
3	28	418	10710
4	56	1516	496485
5	112	17320	27821508
6	224	226256	271891620
7	448	878868	$>10^9$
8	896	11984790	$>10^9$
9	1792	49559052	$>10^9$
10	3584	727654100	$>10^9$

Количественно оценивая полученные результаты, можно сделать вывод, что период повторения ГПСБП увеличен на 4–6 порядков.



1 — классический АГФ; 2 — модифицированный АГФ–1; 3 — модифицированный АГФ–2

Рис. 1

Основная цель настоящей работы — сравнительный анализ предложенных нами модифицированных генераторов Фибоначчи стохастического генератора на основе R-блока [1, 8, 9].

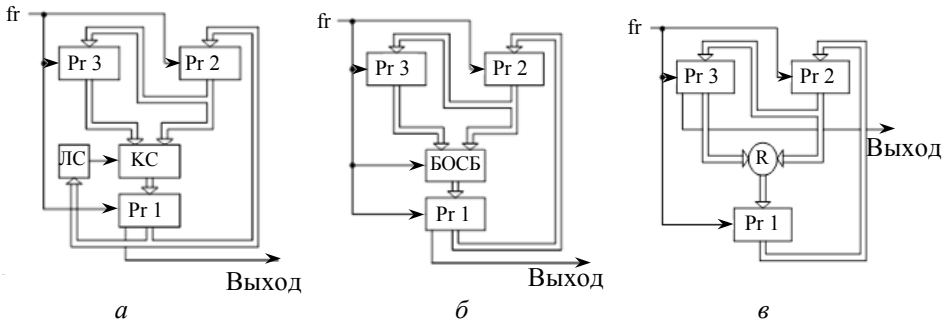
Проведен комплексный анализ характеристик ГПСБП трех типов:

(1) на основе МАГФ (рис. 2, *а*)

(2) на основе МАГФ с повышенной статистической безопасностью (рис. 2, *б*)

(3) на основе R-блока (рис. 2, *в*).

Структурные схемы генераторов приведены на рис. 2



а *б* *в*

Рис. 2

Выходные псевдослучайные битовые последовательности генераторов формируются на выходах младшего разряда одного из регистров. Оценка качества этих последовательностей проводиться по следующим показателям:

- период повторения при различных начальных состояниях структурных элементов;
- статистические характеристики (включая линейную сложность);
- объем множества различных вариантов формирования битовой последовательности, соответствующий объему ключевой информации (длине ключа).

Важным фактором, определяющим качество ГПСБП, является сложность его построения — технологичность. Генераторы, которые рассматриваются в данной работе, относятся к цифровым аппаратным генераторам, т.е. к устройствам, которые реализуются на элементной базе цифровой техники, в частности программируемых логических интегральных схемах (ПЛИС). В связи с этим предлагаем оценивать технологичность по количеству элементарных цифровых ячеек, необходимых для построения ГПСБП на ПЛИС. Такими ячейками, в случае организации ПЛИС по архитектуре FPGA (Field Programmable Gate Arrays), являются конфигурируемые логические блоки (КЛБ), предназначенные для выполнения логических функций от нескольких переменных, а также функций памяти. Итак, КЛБ могут применяться для построения не только комбинационных, но и последовательностных цифровых устройств.

Результаты комплексного анализа трех типов генераторов приведены в табл. 2. Здесь приняты следующие обозначения: (1) — ГПВБП на основе МАГФ; (2) — ГПВБП на основе МАГФ с повышенной статистической безопасностью; (3) — ГПВБП на основе R-блока.

Определение максимальных значений периода повторения $T_{p_{\max}}$ проводили с помощью имитационной модели. Для малых значений количества разрядов n перебирали все возможные комбинации начальных состояний последовательностных структурных элементов, выявляли определенные закономерности, и уже для больших значений n исследования проводили при определенных начальных состояниях.

Кроме этого, для генератора на основе R-блока, определение периода проводили несколько раз для каждого значения n (в табл. 2 зафиксировано три значения $T_{p_{\max}}$), для различных случайным образом сформированных таблиц R-блока.

Зависимости $T_{p_{\max}}$ от n приведены на рис. 3.

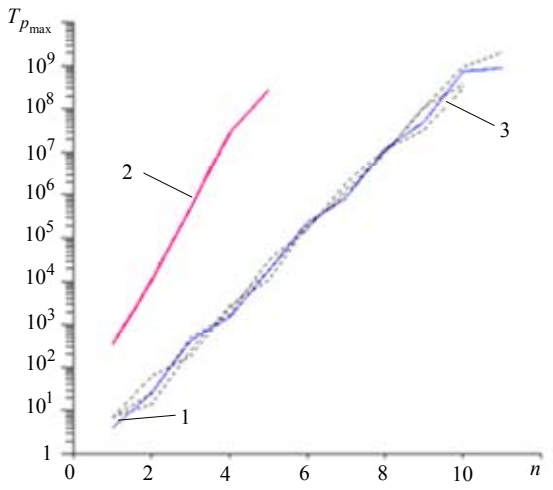


Рис. 3

Таблица 2

Количество разрядов, n	Максимальное значение периода повторения, $T_{p_{\max}}$			Результаты тестирования (тесты NIST)			Количество КЛБ		
	(1)	(2)	(3)	(1)	(2)	(3)	(1) $4n+1$	(2) $6n+1$	(3) $n \cdot 2^n + 3n$
1	4	12	7 7 7	–	–	– – –	5	7	5
2	26	345	14 63 25	–	–	– – –	9	13	14
3	418	10710	245 182 493	–	–	– – –	13	19	33
4	1516	496485	2773 2479 1766	–	–	– – –	17	25	76
5	17320	27821508	10700 18448 30390	–	–	– – –	21	31	175
6	226256	271891620	192886 166876 164037	–	–	– – –	25	37	402
7	878868	$>10^9$	1070212 1310740 1859408	–	–	– – –	29	43	917
8	11984790	$>10^9$	9271798 8765811 11745306	–	–	– – –	33	49	2072
9	49559052	$>10^9$	106185039 112327186 32987721	–	–	– – 1 –	37	55	4635
10	727654100	$>10^9$	923604327 363377277 301284807	–	–	– 3 – 4 – 1	41	61	10270
11	$>10^9$	$>10^9$	891394563 $>10^9$ $>10^9$	–	– 1	– 1 + +	45	67	22561
12	$>10^9$	$>10^9$	$>10^9$ $>10^9$ $>10^9$	–	– 1	+ + +	49	73	49188
13	$>10^9$	$>10^9$	$>10^9$ $>10^9$ $>10^9$	–	+	+ + +	53	79	106535
…									
23	$>10^9$	$>10^9$	$>10^9$ $>10^9$ $>10^9$	+	+	+ + +	93	139	192938053

Статистические характеристики исследовались с помощью тестов NIST [6], которые состоят из 15 различных тестов, включающих в себя и определение линейной сложности. Тестировалась битовая последовательность длиной 10^9 бит. Результаты тестирования приведены в табл. 2, где приняты следующие обозначения: – — большинство тестов не пройдено; 4, 3, 2, 1 — не пройдено 4, 3, 2 или 1 тесты из 15; + — все тесты пройдены. В табл. 3 приведены более подробные результаты прохождения тестов NIST тремя исследуемыми генераторами.

Таблица 3

Название тестов NIST	Результаты прохождения тестов для генераторов с количеством разрядов:											
	10			12			13			23		
	1	2	3	1	2	3	1	2	3	1	2	3
Частотный (монобитный) тест	–	–	+	–	+	+	–	+	+	+	+	+
Частотный блочный тест	–	–	+	–	+	+	–	+	+	+	+	+
Проверка кумулятивных сумм	–	–	–	–	+	+	–	+	+	+	+	+
Тест «дырок»	–	–	–	–	+	+	–	+	+	+	+	+
Тест длинной серии из единиц	–	–	+	–	+	+	–	+	+	+	+	+
Тест проверка рангов матрицы	–	–	–	–	+	+	–	+	+	+	+	+
Тест на основе дискретного преобразования Фурье	–	–	–	–	+	+	–	+	+	+	+	+
Проверка непересекающихся шаблонов	–	–	–	–	+	+	–	+	+	+	+	+
Проверка пересекающихся шаблонов	–	–	–	–	+	+	–	+	+	+	+	+
Универсальный статистический тест	–	–	–	–	–	+	–	+	+	+	+	+
Тест на основе аппроксимированной энтропии	–	–	–	–	+	+	–	+	+	+	+	+
Тест проверки случайных отклонений	–	–	–	–	+	+	–	+	+	+	+	+
Тест проверки случайных отклонений–2	–	–	–	–	+	+	–	+	+	+	+	+
Тест серии	–	–	–	–	+	+	–	+	+	+	+	+
Тест проверки линейной сложности	–	–	+	–	+	+	–	+	+	+	+	+

Итак, статистической безопасности достигает ГПСБП на основе МАГФ (1) при минимальном количестве разрядов 23, ГПСБП с повышенной статистической безопасностью (2) — при 13, ГПСБП на основе R-блока (3) — при 12. Таким образом, разработанный модифицированный ГПСБП с БОСБ по своим параметрам близок к криптостойкому ГПСБП на основе R-блока.

Сложность построения ГПСБП определяли по количеству КЛБ, необходимых для их реализации. В случае генератора на основе МАГФ (рис. 2, *а*) это количество равно $4n + 1$, где $4n$ соответствует общему количеству разрядов Рг1, Рг2, Рг3, КС, а ЛС может быть построена на одном КЛБ. Для генератора на основе МАГФ с повышенной статистической безопасностью необходимое количество КЛБ равно $6n + 1$. Это объясняется построением БЗСБ [6, 7]. Для генератора на основе R-блока минимально необходимое количество КЛБ равна $n \cdot 2^n + 3n$, где $n \cdot 2^n$ — количество КЛБ необходимо для реализации *R*-блока по принципу построения оперативной памяти, а $3n$ — количество КЛБ, необходимых для реализации регистров Рг1 — Рг3 (см. рис. 2, *в*).

Зависимости количества КЛБ от числа разрядов структурных элементов трех генераторов приведены на рис. 4: (1) — на основе МАГФ, (2) — на основе МАГФ с БОСБ, (3) — на основе R-блока. Здесь крестиками отмечено значение n, при которых исходная последовательность генератора проходит все тесты из набора NIST.

Таким образом, касательно достижения статистической безопасности получены следующие результаты: для варианта (1) — необходимо 93 КЛБ при $n = 23$; для варианта (2) — 79 КЛБ при $n = 13$; для варианта (3) — 49188 КЛБ при $n = 12$. Итак, предложенные нами ГПВБП имеют простую структуру, т.е. требует в 600 раз меньшего количества конфигурируемых логических блоков ПЛИС для аппаратной реализации по сравнению с генераторами на основе R-блоков с сохранением такого же уровня статистической безопасности.

В процессе разработки цифровых ГПСБП их быстродействие можно определить аналитически или с помощью системы автоматизированного проектирования (САПР) ПЛИС. С помощью аналитического способа можно предварительно оце-

нить, выявить структурные элементы и их связи, которые замедляют работу генератора; сделаны необходимые схемотехнические изменения. При этом оценки максимально возможной частоты тактовых импульсов осуществляются с помощью аналитических уравнений, определяющих время переходных процессов в устройстве. САПР ПЛИС позволяет определить быстродействие ГПСБП в процессе их имплементации в кристалл.

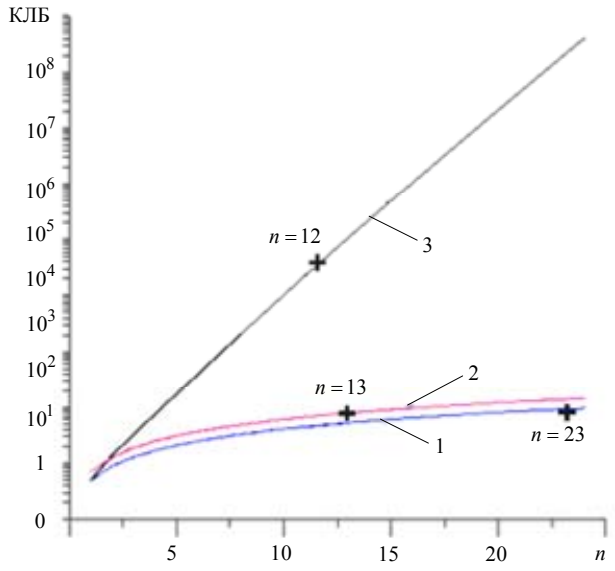


Рис. 4

Быстродействие генератора (1), изображенного на рис. 2, а, определяется максимальным временем, необходимым для завершения переходного процесса в схеме, который начинается в момент поступления на тактовый вход рабочего фронта импульса и завершается формированием нового значения числа на выходе КС:

$$t_{пп} = t_{\text{Рг}} + t_{\text{ЛС}} + t_{\text{КС}}, \qquad (1)$$

где, $t_{\text{Рг}}$, $t_{\text{ЛС}}$ и $t_{\text{КС}}$ — время срабатывания Рг, ЛС и КС соответственно.

Быстродействие генератора (2) (рис. 2, *б*), учитывая, что счетчики работают медленнее регистров, можно оценить временем срабатывания элементов схемы:

$$t_{пп} = t_{\text{Сч}} + t_{\text{ЛС}} + t_{\text{КС}} + 2 \cdot t_{\text{БСМ}}, \qquad (2)$$

где $t_{\text{Сч}}$, $t_{\text{ЛС}}$, $t_{\text{КС}}$, $t_{\text{БСМ}}$ — время срабатывания счетчиков Сч1 и Сч2, ЛС, КС и БСМ1 и БСМ2, которые входят в состав БОСБ [4, 6, 7].

Итак, быстродействие таких генераторов (рис.2, *а*, *б*) прежде всего зависит от времени срабатывания КС и ЛС, поскольку регистры памяти Рг1–Рг3 работают синхронно и задержка их срабатывания равна задержке срабатывания одного триггера.

Быстродействие КС может быть увеличено при использовании известных способов построения комбинационных сумматоров с параллельным и последовательно-параллельным переносом и никак не влияет на период повторения генератора и его статистические характеристики.

Время срабатывания ЛС зависит от схемотехники реализации и от количества входов, которое может быть разным. Уменьшение этого количества позволяет существенно повысить быстродействие устройства в целом.

Быстродействие генератора (3) (рис. 2, *в*) определяется временем срабатывания элементов схемы, которое при синхронной работе регистров, равно

$$t_{nn} = t_{\text{Рг}} + t_{\text{R}}\ , \qquad (3)$$

где t_{R} — время считывания данных из оперативной памяти.

Поскольку время срабатывания регистров параллельного типа может быть сведено к времени срабатывания одного триггера, быстродействие такого типа генераторов при их аппаратной реализации определяется быстродействием оперативных запоминающих устройств (ОЗУ). Отдельной процедурой при создании ГПВБ на основе R-блоков является заполнение таблицы преобразования R-блока [1, 8, 9]. Этот процесс требует дополнительного времени при обновлении таблиц, а при аппаратной реализации генератора — еще и наличия дополнительных блоков.

Таким образом, генераторы на основе МАГФ значительно превосходят по быстродействию генераторы на основе R-блоков.

Криптографическим ключом ГПСБП на основе МАГФ является исходное состояние регистров Рг1–Рг3. Полное множество значений этих состояний равно $Q_0{}^{м} = 2^{3n}$ при длине ключа $3n$. Однако статистически безопасным можно считать только то множество, которое соответствует выходным битовым последовательностям, проходящим все тесты NIST. Исходя из проведенных исследований, это множество включает в себя не меньше $Q_0{}^{c} = 2^{3n-1}$ значений, соответствующих длине ключа $3n - 1$.

Криптографическим ключом ГПСБП на основе МАГФ с БОСБ можно считать начальные состояния регистров Рг1–Рг3 и счетчиков Лч1 и Лч2, которые входят в состав БОСБ [6]. В этом случае статистически безопасное множество включает в себя не меньше $Q_0{}^{c} = 2^{5n-1}$ значений, соответствует длине ключа $5n - 1$.

Для ГПСБП на основе *R*-блока криптографическим ключом могут быть начальные состояния регистров Рг1–Рг3 и варианты заполнения таблицы R-блока. Начальным состояниям регистров соответствует множество $\text{Q}_0{}^{c} = 2^{3n-1}$ и соответственно длина ключа $3n - 1$. Для таблицы R-блока существует всего $(2^{\text{n}})!$ вариантов ее заполнения, которым можно поставить в соответствие длину ключа $\lceil \log[(2^n)!] \rceil$, где скобки $\lceil\ \rceil$ означают выделение наименьшего целого числа, большего или равного выражению в скобках.

Заключение

В процессе сравнительного анализа установлено, что характеристики разработанного ГПСБП на основе МАГФ с БОСБ (2) приближены, а в некоторых аспектах значительно лучше характеристик стохастического ГПСБП на основе R-блока (3), в частности:

- статистическая безопасность достигается почти при одинаковом количестве разрядов 13 против 12.
- период повторения увеличен в 43 раза, при таком же количестве разрядов структурных элементов;
- имеет простую структуру, т.е. требует в 600 раз меньшего количества конфигурируемых логических блоков ПЛИС для аппаратной реализации с сохранением такого же уровня статистической безопасности.

М.М. Мандрона, В.М. Максимович

ПОРІВНЯЛЬНИЙ АНАЛІЗ ГЕНЕРАТОРІВ ПСЕВДОВИПАДКОВИХ БІТОВИХ ПОСЛІДОВНОСТЕЙ

Здійснено порівняльний аналіз характеристик генераторів псевдовипадкових бітових послідовностей на основі модифікованого адитивного генератора Фібоначчі і генератора на основі R-блоку. Досліджено періоди повторення, статистичну безпеку, швидкодію, складність побудови та об'єм ключової інформації (довжину ключа).

M.N. Mandrona, V.N. Maksymovych

COMPARATIVE ANALYSIS OF PSEUDORANDOM BIT SEQUENCE GENERATORS.

The comparative analysis of characteristics of the pseudorandom bit sequence generators based on modified additive Fibonacci generator and the generator based on R-block is carried out. Repetition periods, the statistical security, speed, difficulty of construction and the amount of key information (key length) are investigated.

1. *Иванов М.А.*, *Чугунков И.В.* Криптографические методы защиты информации в компьютерных системах и сетях. — М. : Изд-во НИЯУ МИФИ, 2012. — 400 с.
2. *Mandrona M.M.*, *Maksymovych V.M.* Investigation of the statistical characteristics of the modified Fibonacci generators // Journal of Automation and Information Sciences. — 2014. — **46**, N 12 — P. 48–53.
3. *Апаратна* реалізація і дослідження модифікованих генераторів Фібоначчі / Ю.М. Костів , В.М. Максимович, М.М. Мандрона, О.І. Гарасимчук // Комп'ютерні технології друкарства. — 2013. — Вип. 29. — С. 167–174.
4. *Мандрона М.М.* Апаратні генератори псевдовипадкових бітових послідовностей з покращеними характеристиками : Дис. канд. техн. наук : 05.13.21. — Львів, 2015. — 146 с.
5. NIST SP 800–22. — A statistical test suite for random and pseudorandom number generator for cryptographic applications. — http://csrc.nist.gov/publications/nistpubs// SP800-22rev1a.pdf [Accessed: April. 2010].
6. *Generator* of pseudorandom bit sequence with increased cryptographic security / M.M. Mandrona , Yu.M. Kostiv, V.M. Maksymovych, O.I. Harasymchuk // Metallurgical and Mining Industry. — 2014. — N 5. — P. 81–86.
7. *Development* of a statistical security pseudorandom bit sequence generator by applying the systemic theoretical approach / M.M. Mandrona, V.M. Maksymovych, O.I. Harasymchuk, Yu.M. Kostiv // Metallurgical and Mining Industry: scientific and technical jornal. — 2016. — N.2. — P. 96–101.
8. *Дослідження* генераторів псевдовипадкових послідовностей побудованих з використанням R-блоків / М.М. Мандрона, В.М. Максимович, Ю.М. Костів, О.І. Гарасимчук // Інформаційна безпека. — 2013. — № 4 (12). — С. 84–92.
9. *Examination* of multi link generators of pseudorandom sequences built using R-blocks / M.M. Mandrona, Yu.M. Kostiv, V.M. Maksymovych, O.I. Harasymchuk // Sustainable development. — 2014. — N 18. — P.110-118.

Получено 16.05.2016
После доработки 18.07.2016