ISSN 1991-3494

ҚАЗАҚСТАН РЕСПУБЛИКАСЫ
ҰЛТТЫҚ ҒЫЛЫМ АКАДЕМИЯСЫНЫҢ

Х А Б А Р Ш Ы С Ы

ВЕСТНИК

НАЦИОНАЛЬНОЙ АКАДЕМИИ НАУК
РЕСПУБЛИКИ КАЗАХСТАН

THE BULLETIN

OF THE NATIONAL ACADEMY OF SCIENCES
OF THE REPUBLIC OF KAZAKHSTAN

1944 ЖЫЛДАН ШЫҒА БАСТАҒАН
ИЗДАЕТСЯ С 1944 ГОДА
PUBLISHED SINCE 1944

4

АЛМАТЫ
АЛМАТЫ
ALMATY

2016

ШІЛДЕ
ИЮЛЬ
JULY

«Вестник Национальной академии наук Республики Казахстан». ISSN 1991-3494
Собственник: РОО «Национальная академия наук Республики Казахстан» (г. Алматы)
Свидетельство о постановке на учет периодического печатного издания в Комитете информации и архивов Министерства культуры и информации Республики Казахстан **№5551-Ж**, выданное 01.06.2006 г.

Периодичность: 6 раз в год
Тираж: 2000 экземпляров

Адрес редакции: 050010, г. Алматы, ул. Шевченко, 28, ком. 219, 220, тел. 272-13-19, 272-13-18.
www: nauka-nanrk.kz, bulletin-science.kz

Адрес типографии: ИП «Аруна», г. Алматы, ул. Муратбаева, 75

Bulletin of the National Academy of Sciences of the Republic of Kazakhstan.
ISSN 1991-3494

Owner: RPA "National Academy of Sciences of the Republic of Kazakhstan" (Almaty)
The certificate of registration of a periodic printed publication in the Committee of Information and Archives of the Ministry of Culture and Information of the Republic of Kazakhstan N 5551-Ж, issued 01.06.2006

Periodicity: 6 times a year
Circulation: 2000 copies

Editorial address: 28, Shevchenko str., of. 219, 220, Almaty, 050010, tel. 272-13-19, 272-13-18,
http://nauka-nanrk.kz /, http://bulletin-science.kz

Address of printing house: ST "Aruna", 75, Muratbayev str, Almaty

BULLETIN OF NATIONAL ACADEMY OF SCIENCES
OF THE REPUBLIC OF KAZAKHSTAN
ISSN 1991-3494
Volume 4, Number 362 (2016), 118 – 123

HAMMING WEIGHT AS CRITERIA OF EVALUATION RESPONSE TO TIME ATTACK

A. K. Shaikhanova, D. T. Kurushbayeva, G. B. Bekeshova

Semey State University named after Shakarim, Kazakhstan.
E-mail: Igul7@mail.ru

Key words: attack, Hamming weight, β-ary method cryptosystem, modular exponentiation.

Abstract. For safe operation of the computer systems it is necessary to use firmware of counter to passive types of attacks based on the computing resources of the systems themselves. Furthermore, the information stored on the server may have different levels of secrecy, so there is a need to access distribution. Therefore, the development of methods, algorithms, software and hardware to access the distribution, which allows to maintain the specified functionality and stability of the computer system by the allocation of resources in real time, it is an urgent task. The article deals with the study of time depending on the algorithm of modular exponentiation of the Hamming weight. This research allowed to offer a method for determining the stability of this algorithm to the analysis time. Based on the results of the highest resistance to the interim analysis of the algorithm is β-ary method of modular exponentiation.

УДК 004.74.76.2

ВЕС ХЕММИНГА КАК КРИТЕРИЙ ОЦЕНКИ ЧУВСТВИТЕЛЬНОСТИ К ВРЕМЕННОЙ АТАКЕ

А. К. Шайханова, Д. Т. Курушбаева, Г. Б. Бекешова

Государственный университет им. Шакарима города Семей, Казахстан

Ключевые слова: атака, вес Хемминга, β-арный метод, криптосистема, модулярное экспоненцирование.

Аннотация. Для безопасной эксплуатации компьютерных систем необходимо применять программно-аппаратные средства противодействия пассивным типам атак с учетом вычислительных ресурсов самих систем. Кроме того, информация, хранящаяся на сервере, может иметь разные уровни секретности, следовательно, возникает необходимость распределения доступа. Поэтому разработка методов, алгоритмов и программно-аппаратных средств распределения доступа, которые позволяют поддерживать заданную функциональность и устойчивость компьютерной системы путем распределения ресурсов в реальном времени, является актуальной задачей. В статье рассмотрено исследование зависимости времени выполнения алгоритма модулярного экспоненцирования от веса Хемминга. Данное исследование позволило предложить метод определения устойчивости этого алгоритма к временному анализу. Исходя из результатов, наивысшую стойкость к временному анализу имеет алгоритм β-арного метода модулярного экспоненцирования.

Введение. В асимметричных криптосистемах основной операцией, используемой в процессе шифрования и дешифрования, является модулярное экспоненцирование, поэтому используемая криптосистема, основанная на такой операции, должна удовлетворять определенным условиям, в частности, иметь высокое быстродействие и защищенность от атак злоумышленников. Первая проблема решается выбором оптимального метода возведения числа в степень по модулю. Вторая проблема гораздо серьезнее и требует гарантированного обеспечения устойчивости этого метода к атакам специального вида.

Выявление определенной корреляции между количеством единичных битов ключа и время выполнения соответствующего алгоритма позволяет злоумышленнику выдвинуть гипотезу относительно этого количества единичных (нулевых) битов, количественным эквивалентом которой является вес Хемминга. То есть, зная вес Хемминга, можно значительно быстрее и точно определить секретный ключ криптосистемы RSA.

Поэтому для исследования устойчивости алгоритмов необходимо установить зависимость времени выполнения соответствующего алгоритма от веса Хемминга.

Исследование зависимости времени выполнения алгоритма модулярного экспоненцирования от веса Хемминга. На рисунке 1 [1, 2] изображена зависимость времени выполнения алгоритмов бинарного метода "слева направо" *T1(n,H(n))* и "справа налево"*T2(n,H(n))*, соответственно, от веса Хемминга при длине n-$\lceil \log n \rceil = 1024$ бит, которая удовлетворяет современным требованиям к длине ключа криптосистемы. Стоит отметить, что изображение зависимости *T1(n,H(n))* и *T2(n,H(n))* от веса Хемминга совпадают. Анализ этого графика показывает, что производительность данных алгоритмов существенно зависит от веса Хемминга, а также возможность определения минимальной и максимальной производительностей, математического ожидания и т.п. Кроме того, очевидно, что устойчивость этих методов к временному анализу будет минимальной, то есть злоумышленник, измерив время выполнения алгоритма, может легко оценить количество единиц в двоичном изображении числа n, а следовательно, и определить секретный ключ путем перебора в суженном ключевом пространстве.

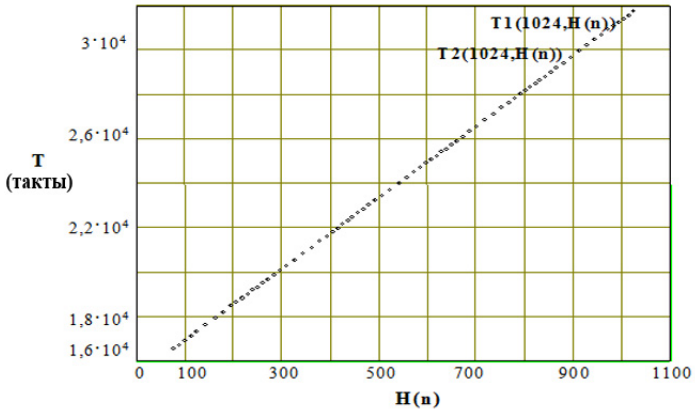

Рисунок 1 – Зависимость времени выполнения алгоритма бинарного метода от веса Хемминга

Анализ графика зависимости быстродействия алгоритма β-арного метода "слева направо" *T3(n,β,H(n))*от веса Хемминга (рисунок 2) [1, 2] показывает, что, в отличие от бинарного метода (см. рисунок 2), время выполнения этого алгоритма зависит только от значения β. То есть этот алгоритм абсолютно устойчив к временной атаке.

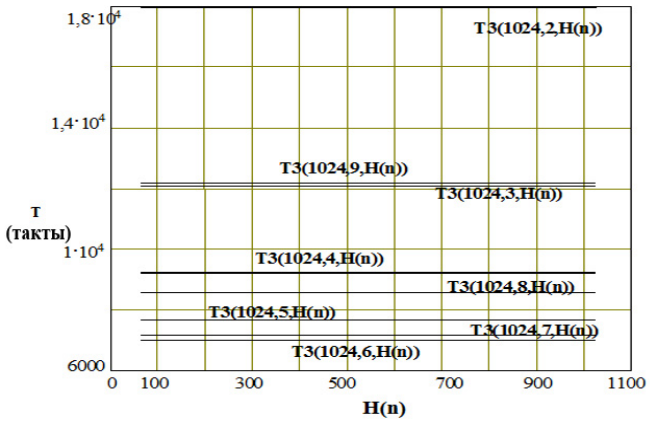

Рисунок 2 – Зависимость времени выполнения алгоритма β-арного метода "слева направо" от веса Хемминга

Исследование зависимости времени выполнения алгоритма β-арного метода "справа налево" *T4(n,β,H(n))*от веса Хемминга (рисунок 3) показывает [3], что в отличие от предыдущего (см. рисунок 2), он зависит от количества единиц в двоичном изображении числа *n*. То есть при различных значениях его параметров получаются различные характеристики быстродействия и устойчивости к временному анализу. Однако в отдельных случаях можно найти такое значение *β*, при котором возможно получение практической устойчивости, близкий к абсолютной, например, при *β*=9.

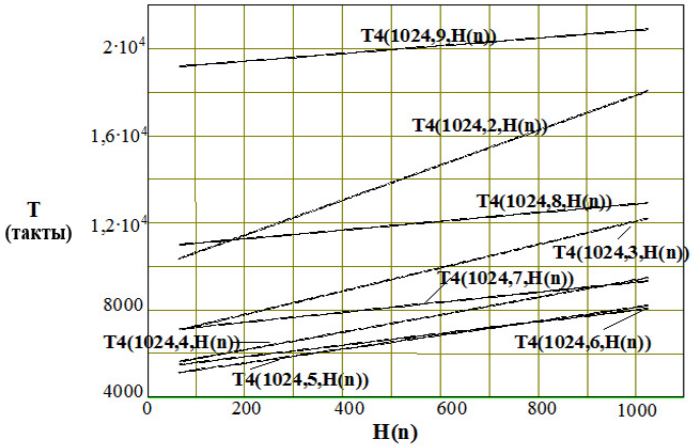

Рисунок 3 – Зависимость быстродействия алгоритма β-арного метода "справа налево" от веса Хемминга

Построим математическую модель исчисления времени, затраченного на выполнение каждого из алгоритмов реализации методов модулярного экспоненцирования. При этом, поскольку переменная *n* обрабатывается в бинарном виде, то через $\lceil \log n \rceil$ представляется длина этой бинарной последовательности.

На выполнение бинарного метода затрачивается время [4]:

– при считывании "слева направо":

$$T1(n) = t + c + \sum_{i=k-1}^{0} r_i + \sum_{i=k-1|n_i=1}^{0} s_i = t + c + \lceil \log n \rceil \cdot r + H(n) \cdot s, \quad (1)$$

– при считывании "справа налево":

$$T2(n) = t + c + b + \sum_{i=0|n_i=1}^{k-1} s_i + \sum_{i=0}^{k-1} r_i = t + c + b + H(n) \cdot s + \lceil \log n \rceil \cdot r. \quad (2)$$

Через*H(n)*обозначен вес Хемминга, то есть количество единиц в бинарном представлении *n*.

На исполнение β-арного метода затрачивается время [4]:

– при считывании “слева направо”:

$$T3(n,w) = t + c + \sum_{i=1}^{\beta-1} s_i + c + \sum_{i=k-1}^{0} (d_i + s_i) = t + 2c + \left(\frac{\lceil \log n \rceil}{w} + 2^w - 1 \right) \cdot s + \frac{\lceil \log n \rceil}{w} \cdot d \quad (3)$$

– при считывании "справа налево":

$$T4(n,w) = t + b + \sum_{w=1}^{\beta-1} c_w + \sum_{0}^{k-1} \left(d_{\{i|n_i=0\}} + s_{\{i|n_i=1\}} + d_{\{i|n_i=1\}} \right) + 2c + \sum_{w=\beta-1}^{1} 2s_w = \\ = t + \left(2^w + 1\right)c + b + \frac{\lceil \log n \rceil}{w} \cdot d + \left(\frac{\lceil \log n \rceil}{w} - W_0(n) + 2^{w+1} - 2 \right) \cdot s \quad (4)$$

где $W_0(n)$ – количество нулевых битов в изображении числа *n* по основанию *β*; *w* – показатель степени двойки в $\beta = 2^w$.

Очевидно, что в бинарном изображении числа n является $\lceil \log n \rceil - H(n)$ нулевых битов. Для перевода числа в β-арную систему счисления бинарное изображение n разбивают на окна длиной w. Отсюда следует, что верхняя оценка $W_0(n)$ [5, 6]:

$$W_0^{\max}(n) = \left\lfloor \frac{\lceil \log n \rceil - H(n)}{w} \right\rfloor. \tag{5}$$

С другой стороны, нижняя оценка легко может быть определена как

$$W_0^{\min}(n) = \left\lfloor \frac{(\lceil \log n \rceil - H(n)) \cdot w}{(w-1) \cdot \lceil \log n \rceil} \right\rfloor. \tag{6}$$

На выполнение метода скользящего окна затрачивается время [99]:

– при считывании "слева направо":

$$\begin{aligned} T5(n,|w_i|) &= b + s + \sum_{j=1}^{2^{|w_i|}-1} s_j + t + 2c + \sum_{i=0}^{k-1} \left((r+c)_{\{i|n_i=0\}} + (q+s+c+r)_{\{i|n_i=1\}} \right) = \\ &= b + s + \left(2^{|w_i|} - 1\right)s + t + 2c + (k - H(n))(r+c) + p(q+s+c) + r(|w_o| + \ldots + |w_i|) = \\ &= t + b + 2c + kr + 2^{|w_i|} s + p(q+s+c) + (k - H(n))c = \\ &= t + b + (2 + p + \lceil \log n \rceil - H(n))c + \lceil \log n \rceil r + \left(2^{|w_i|} + p\right)s + pq \end{aligned} \tag{7}$$

– при считывании "справа налево":

$$\begin{aligned} T6(n,|w_i|) &= t + b + \sum_{\{j=1,3,\ldots,2^{|w_i|}-1\}} c_j + c + \sum_{i=k-1}^{0} \left((r+c)_{\{i|n_i=0\}} + (q+s+c+d)_{\{i|n_i=1\}} \right) + \sum_{\{v=2^{|w_i|}-1,\ldots,5,3\}} (2s_v) + c = \\ &= t + b + \left(2^{2|w_i|-2} + 1\right)c + (k - H(n))(r+c) + p(q+s+c+d) + 2^{2|w_i|-1} s + c = \\ &= t + b + \left(2^{2|w_i|-2} + 2 + \lceil \log n \rceil - H(n) + p\right)c + (\lceil \log n \rceil - H(n))r + \left(2^{2|w_i|-1} + p\right)s + pq + pd, \end{aligned} \tag{8}$$

где p – количество окон; $(|w_0| + \ldots + |w_i|)$ – сумма всех нечетных окон (равная весу Хемминга, поскольку эти окна состоят только из единичных битов).

Из аналитического представления (7), (8) следует, что существует обратная зависимость времени выполнения алгоритмов метода скользящего окна при считывании "слева направо" $T5(n,|w_i|,H(n))$ и "справа налево" $T6(n,|w_i|,H(n))$, соответственно, от веса Хемминга. Однако, поскольку эта зави-симость является небольшой, то можно считать, что для определенного класса прикладных задач можно успешно использовать указанные алгоритмы, поскольку их устойчивость к временному анализу выше по сравнению с другими методами.

Таким образом, проведенные исследования показали, что β-арный метод модулярного экспоненцирования устойчив к пассивным атакам, в которых проводится анализ веса Хемминга, в частности, к опасной атаки временного анализа.

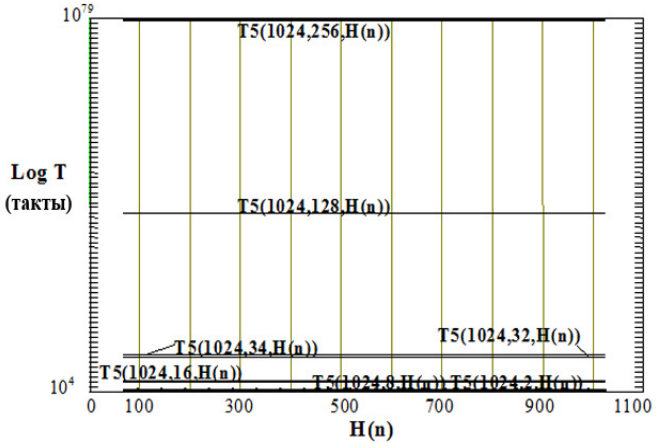

Рисунок 4 – Зависимость быстродействия алгоритма метода скользящего окна при считывании "слева направо" от веса Хемминга

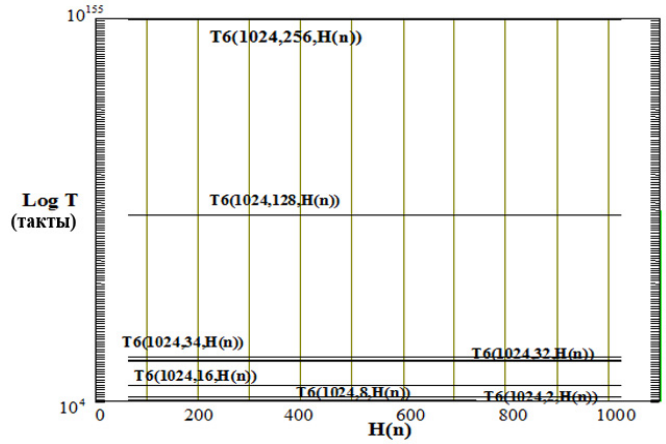

Рисунок 5 – Зависимость
быстродействия алгоритма
метода скользящего окна при считывании
"справа налево" от веса Хемминга

На рисунках 4 и 5 изображены зависимость времени выполнения этих алгоритмов от веса Хемминга, при $W_0(n) = W_0^{\max}(n)$, что является благоприятной условием для криптоанализа [2].

Вывод. Таким образом, для оценки устойчивости других методов модулярного экспоненцирования необходим критерий устойчивости к временному анализу, отражающий зависимость времени выполнения соответствующих алгоритмов от веса Хемминга.

ЛИТЕРАТУРА

[1] Tomescu M.L., Petrov G. A Stability Analysis Method for Nonlinear Systems with Fuzzy Logic Controller // Symbolic and Numeric Algorithms for Scientific Computing (SYNASC'06): 8-th Symposium, 2006: Proceedings. – 2006. – P. 122-128.

[2] Шайханова А.К., Оспанов Е.А., Карпинский Н.П. Методы модулярного экспоненциирования, применяющиеся для защиты информации в компьютерных системах // Вестник КазНТУ им. К. И. Сатпаева. – 2015. – № 2(108). – С. 268-274.

[3] Shaikhanova A., Shangytbaeva G., Ahmetov B., Beisembekova R. Comparison of methods of treatment of fuzzy information for distribution of access in computer systems // Research Journal of Applied Sciences, Engineering and Technology. – 2015. – Vol. 10, Issue 9. – P. 1082-1088.

[4] Штовба С.Д. Обеспечение точности и прозрачности нечеткой модели Мамдани при обучении поэкспериментальным данным // Проблемы управления и информатики. – 2007. – № 4. – С. 102–114.

[5] Shaikhanova A.K., Zolotov A.D., Stepanova O.A., Karpinski M.P., Dubchak L.O. Fuzzy system of access distribution within a computer network // Journal of Theoretical and Applied Information Technology. – 2015. – Vol. 80, Issue 1. – P. 105-113.

[6] Шайханова А.К., Золотов А.Д., Карпинский Н.П. Оценка устойчивости методов модулярного экспоненцирования на основе вероятностных приближений // Вестник национальной академии наук Республики Казахстан. – 2015. – № 2. – С. 198-205.

REFERENCES

[1] Tomescu M.L., Petrov G. A Stability Analysis Method for Nonlinear Systems with Fuzzy Logic Controller // Symbolic and Numeric Algorithms for Scientific Computing (SYNASC'06): 8-th Symposium, 2006: Proceedings. 2006. P. 122-128 (in Eng.).

[2] Shayhanova A.K., Ospanov E.A., Karpinski N.P. Methods modular eksponentsiirovaniya used to protect the information in computer systems. Herald of KazNTU. K.I.Satpaeva. 2015. № 2(108). P. 268-274 (in Russ.).

[3] Shaikhanova A., Shangytbaeva G., Ahmetov B., Beisembekova R. Comparison of methods of treatment of fuzzy information for distribution of access in computer systems // Research Journal of Applied Sciences, Engineering and Technology. 2015. Vol. 10, Issue 9. P. 1082-1088 (in Eng.).

[4] Shtovba S.D. Ensuring the accuracy and transparency of Mamdani fuzzy model for teaching po eksperimentalnym data // Problems of control and informatics. 2007. N 4. P. 102-114 (in Russ.).

[5] Shaikhanova A.K., Zolotov A.D., Stepanova O.A., Karpinski M.P., Dubchak L.O. Fuzzy system of access distribution within a computer network // Journal of Theoretical and Applied Information Technology. 2015. Vol. 80, Issue 1. P. 105-113 (in Eng.).

[6] Shaikhanova A.K., Zolotov A.D., Stepanova O.A., Karpinski M.P., Dubchak L.O. Fuzzy system of access distribution within a computer network // Journal of Theoretical and Applied Information Technology. 2015. Vol. 80, Issue 1. P. 105-113 (in Russ.).

ХЕММИНГ САЛМАҒЫ – УАҚЫТША ШАБУЫЛҒА СЕЗІМТАЛДЫҚ БАҒАСЫНЫҢ КРИТЕРИЙІ

А. К. Шайханова, Д. Т. Курушбаева, Г. Б. Бекешова

Семей қаласының Шәкәрім атындағы мемлекеттік университеті, Қазақстан

Түйін сөздер: шабуыл, Хемминг салмағы, β-лы әдісі, криптожүйе, модулярлы экспоненцирлеу.

Аннотация. Жүйелердің есептеу қорларын есепке ала отырып, пассивті типті шабуылдарға бағдарламалы-аппаратталған кері әрекетті құралдарды компьютерлік жүйелерді қауіпсіз эксплуатациясы үшін қолдану қажет. Одан басқа, серверде сақталып жатқан ақпараттың әр түрлі құпия деңгейлері бар, яғни рұқсатты тарату қажеттілігі туады. Сондықтан, нақты уақытта қорды тарату жолымен компьютерлік жүйенің берілген функционалдылығы мен тұрақтылығын қолдауға мүмкіндік беретін рұқсатты таратудың әдістері, алгоритмдері және бағдарламалау-аппаратты құралдарды жетілдіру өзекті міндет болып табылады. Мақалада Хемминг салмағына модулярлы экспоненцирлеу алгоритмін орындау уақытының тәуелділігін зерттеуі қарастырылған. Бұл зерттеу осы алгоритмнің уақыттық анализге деген тұрақтылығын анықтау әдісін ұсынуға мүмкіндік берді. Нәтижелерді қортытындылағанда уақыттық талдауға қатысты ең жоғары тұрақтылық модулярлы экспоненцирлеудің β-лы әдісінің алгоритмінде болады.

Поступила 21.06.2016 г.

Publication Ethics and Publication Malpractice
in the journals of the National Academy of Sciences of the Republic of Kazakhstan

For information on Ethics in publishing and Ethical guidelines for journal publication see http://www.elsevier.com/publishingethics and http://www.elsevier.com/journal-authors/ethics.

Submission of an article to the National Academy of Sciences of the Republic of Kazakhstan implies that the described work has not been published previously (except in the form of an abstract or as part of a published lecture or academic thesis or as an electronic preprint, see http://www.elsevier.com/postingpolicy), that it is not under consideration for publication elsewhere, that its publication is approved by all authors and tacitly or explicitly by the responsible authorities where the work was carried out, and that, if accepted, it will not be published elsewhere in the same form, in English or in any other language, including electronically without the written consent of the copyright-holder. In particular, translations into English of papers already published in another language are not accepted.

No other forms of scientific misconduct are allowed, such as plagiarism, falsification, fraudulent data, incorrect interpretation of other works, incorrect citations, etc. The National Academy of Sciences of the Republic of Kazakhstan follows the Code of Conduct of the Committee on Publication Ethics (COPE), and follows the COPE Flowcharts for Resolving Cases of Suspected Misconduct (http://publicationethics.org/files/u2/New_Code.pdf). To verify originality, your article may be checked by the Cross Check originality detection service http://www.elsevier.com/editors/plagdetect.

The authors are obliged to participate in peer review process and be ready to provide corrections, clarifications, retractions and apologies when needed. All authors of a paper should have significantly contributed to the research.

The reviewers should provide objective judgments and should point out relevant published works which are not yet cited. Reviewed articles should be treated confidentially. The reviewers will be chosen in such a way that there is no conflict of interests with respect to the research, the authors and/or the research funders.

The editors have complete responsibility and authority to reject or accept a paper, and they will only accept a paper when reasonably certain. They will preserve anonymity of reviewers and promote publication of corrections, clarifications, retractions and apologies when needed. The acceptance of a paper automatically implies the copyright transfer to the National Academy of Sciences of the Republic of Kazakhstan.

The Editorial Board of the National Academy of Sciences of the Republic of Kazakhstan will monitor and safeguard publishing ethics.

Правила оформления статьи для публикации в журнале смотреть на сайте:

www:nauka-nanrk.kz

http://www.bulletin-science.kz/index.php/ru/

Редакторы *М. С. Ахметова, Д. С. Аленов*
Верстка на компьютере *Д. Н. Калкабековой*

Подписано в печать 07.07.2016.
Формат 60x881/8. Бумага офсетная. Печать – ризограф.
17,4 п.л. Тираж 2000. Заказ 4.