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

2

АЛМАТЫ
АЛМАТЫ
ALMATY

2015

НАУРЫЗ
МАРТ
MARCH

«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 2, Number 354 (2015), 187 – 193

DISTRIBUTION OF ACCESS IN ORGANIZATION OF NETWORK SYSTEM OF INFORMATION BASED ON FUZZY LOGIC

A. K. Shaikhanova[1], D. O. Kozhakhmetova[2], M. P. Karpinski[3]

[1] Kazakh National Technical University after K. I. Satpayev, Almaty, Kazakhstan;
[2] Semey State University named after Shakarim, Kazakhstan;
[3] University of Bielsko-Biala, Poland.
E-mail: Igul7@mail.ru, dinara_kozhahmetova@mail.ru, mpkarpinski@gmail.com

Key words: time complexity, fuzzy system, information protection, modular exponentiation, RSA, Mamdani method.

Abstract. For the safe operation of computer systems it is necessary to apply the firmware counter passive types of attacks with the computing resources of the systems themselves. In addition, the information stored on the server can have different levels of privacy, so it is necessary to access the distribution. Therefore, the development of methods, algorithms, software and hardware distribution access, which allows to maintain the functionality and stability of a given computer system by allocating resources in real time, is an urgent task.

The paper considers a method of protecting information transmitted via computer networks by means of selecting a data encryption algorithm based on fuzzy logic. Proposed new method for optimal selection algorithm modular exponentiation differs from the known fact that is based on the method of determining the normalized stability of algorithms modular exponentiation to the analysis time and the mechanism of Mamdani fuzzy inference, which provides response information protection system to replace the input parameters in real time. The suggested fuzzy system allows to adequately protect data in real time taking into account the current state of the computer system itself.

УДК 004.74.76.2

РАСПРЕДЕЛЕНИЕ ДОСТУПА В ОРГАНИЗАЦИИ СЕТЕВОЙ СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ НА ОСНОВЕ НЕЧЕТКОЙ ЛОГИКИ

А. К. Шайханова[1], Д. О. Кожахметова[2], М. П. Карпинский[3]

[1] Казахский национальный технический университет им. К. И. Сатпаева, Алматы, Казахстан;
[2] Государственный университет им. Шакарима, Семей, Казахстан;
[3] Техническо-гуманитарная академия г. Бельско-Бяла, Польша

Ключевые слова: временная сложность, нечёткая система, защита информации, модулярное экспоненцирование, RSA, метод Мамдани.

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 рассмотрен метод защиты информации, передаваемой в компьютерных сетях, путем выбора алгоритма шифрования данных на основе нечёткой логики. Предложенный новый метод оптимального выбора алгоритма модулярного экспоненцирования отличается от известных тем, что

базируется на методе определения нормированной устойчивости алгоритмов модулярного экспоненцирования к временному анализу и механизме нечеткого вывода Мамдани, что обеспечивает реакцию системы защиты информации на смену входных параметров в реальном времени. Построенная нечёткая система позволяет осуществлять адекватную защиту данных в реальном времени, учитывая текущее состояние самой компьютерной системы.

Введение. Основными критериями работоспособности компьютерной системы является высокая производительность, оптимальные затраты памяти устойчивость к атакам злоумышленника. Любая компьютерная система может быть защищена от активных атак злоумышленников, которые можно обнаружить в процессе эксплуатации благодаря известным мерам политики безопасности [1]. Однако существует также возможность возникновения пассивных атак (атака временного анализа или анализа энергопотребления), которые могут осуществляться удаленно и поэтому их трудно обнаружить [2, 3]. Компьютерная система при передаче информации использует сеть для осуществления доступа клиентов. Такую сеть передачи данных можно условно разделить на защищенную и незащищенную части.

В незащищенной части сети клиенты могут быть случайными, поэтому они не являются надежными для сервера с точки зрения безопасности, то есть большая вероятность существования злоумышленника. Кроме того, эта часть сети, как правило, не защищена от сбоев вследствие воздействий внешней среды и является открытой для проведения всех видов современных атак на реализацию. В защищенной части сети клиенты считаются надежными и, благодаря политике безопасности, исключается существование внутреннего злоумышленника. Однако в этой части сети все же остается возможность проведения пассивной атаки временного анализа [2]. Клиенты сети известны серверу по IP-адресу и, учитывая «стаж» пользования сетью, имеют свой уровень доверия, где можно задать вероятность сбоев при передаче пакетов информации. И так, если клиент является новым для данной системы или имеет уровень доверия очень низкий, то необходимый уровень устойчивости к временному анализа должен быть максимальным, то есть равным, например, 1. И наоборот, для клиента с очень высоким уровнем доверия значение устойчивости может стремиться к 0, что обеспечит повышение быстродействия системы. Командная подсистема сервера подает на блок обработки информации данные о самой компьютерной системе, то есть допустимые затраты памяти необходимый уровень производительности.

Для защиты информации в сети необходимо оптимально выбрать метод возведения в степень по модулю для осуществления шифрования информации или проведения аутентификации клиента с помощью распространенного в настоящее время крипто алгоритма RSA. Эту задачу решает блок обработки информации, построенный на основе нечеткой логики, а именно, на механизме нечеткого вывода Мамдани [4]. Он обрабатывает входные значения производительности, затрат памяти устойчивости к временному анализу и представляет оптимальный в каждом случае метод модулярного экспоненцирования на командную подсистему сервера, которая в свою очередь, применяет его для шифрования информации. Основным преимуществом этого блока является то, что он работает в режиме реального времени, что обеспечивает более высокую устойчивость системы от атак злоумышленника, поскольку он не будет достоверно знать алгоритма шифрования [5, 6]. Блок обработки информации на основе нечеткой логики является основой системы защиты компьютерной системы. На его вход поступают критерии выбора метода модулярного экспоненцирования, среди которых необходимый уровень устойчивости к временному анализу R, производительности криптосистемы и допустимые затраты памяти сервера. Входные нечеткие данные обрабатываются под системой оптимального выбора метода возведения в степень по модулю на основе механизма нечеткого вывода по механизму Мамдани. Выходом блока обработки информации является метод модулярного экспоненцирования, что обеспечивает оптимальную конфигурацию системы защиты относительно значений входных критериев выбора.

1. Реализация нечеткой системы распределения доступа. Применя я средство Fuzzy Logic Toolbox среды MATLAB7.7.0 (R2008b) [7], можно построить нечеткую систему оптимального выбора метода модулярного экспоненцирования (method) в зависимости от значений производительности (performance), устойчивости к временному анализу (resistance) и допустимых затрат памяти (memory) [8].

В качестве бинарного метода можно использовать бинарный метод с любым направлением считывания битов, поскольку они имеют идентичную стойкость к атаке временного анализа, а их производительность практически одинакова.

Значения функций принадлежности входных переменных resistance и memory задается трапециевидной функцией, а входной переменной performance-колоколообразной функцией [4].

Функция принадлежности выхода method задается треугольной формой, причем в данном случае имеет место случай симметричной треугольной функции принадлежности [9].

Моделирование нечеткого вывода осуществляется по типу Мамдани.

Функции принадлежности для переменных resistance, performance и memory разделены натри интервала, каждая для точного описания переменных, в частности, для описания устойчивости к временному анализа применяется переменная $low \in [0,0.14]$, обозначающая низкий уровень устойчивости, $middle \in [0.0145,0.72]$- средний уровень и $high \in [0.56,1]$- высокий уровень.

Для задания производительности предлагаются переменные $high \in [0, 31000]$, $middle \in [27000, 75000]$и, $small \in [67000, 100000]$ отвечающих высокому, среднему и низкому уровням.

Допустимые затраты памяти задаются значениями, $small \in [0, 9920]$, $middle \in [9921, 2.52 \cdot 10^5]$ и, $big \in [2.49 \cdot 10^5, 5 \cdot 10^5]$, соответствующие малым, средним и большим затратам, соответственно.

Функции принадлежности для выходной переменной method можно обозначить одинаковыми интервалами на оси ординат для точного определения центра тяжести, что обозначает нечеткий вывод системы [4]. Binary обозначает бинарный метод модулярного экспоненцирования, beta-ary RTL и beta-aryLTR β-арный «справа налево» и «слева направо», соответственно, wRTL-метод скользящего окна «справа налево», awLTR-скользящего окна «слева направо» (рисунок 1).

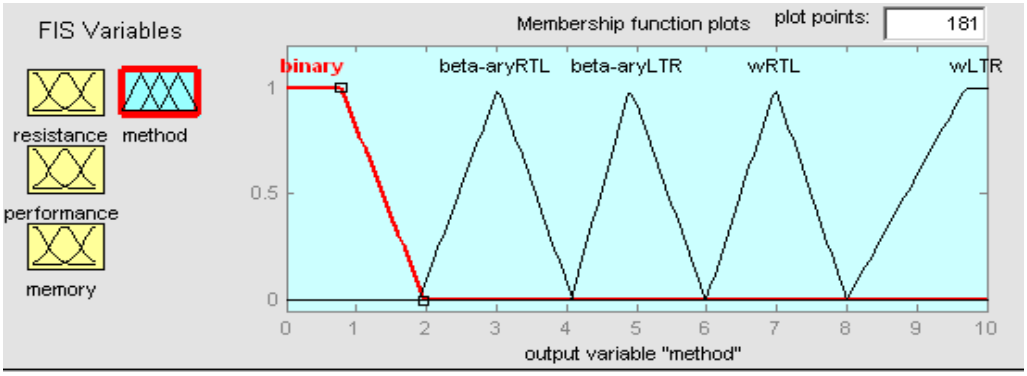


Рисунок 1 – Функции принадлежности переменной method

Для построения предложенной нечеткой системы применяется логический вывод по механизму Мамдани, который находит минимальные площади в изображениях функций принадлежности входных переменных, после чего осуществляется объединение усеченных площадей по максимальному закону, и, наконец, находится центр тяжести окончательной фигуры, абсцисса которой и является выводом нечеткой системы [6-8].

База знаний для построения данной нечеткой модели состоит из правил типа «если-то» [10], все входные переменные имеют по три нечетких состояния и еще одно состояние none, когда значение входной переменной не задано системой. Случай, когда значения всех входных переменных не заданы, на практике применить невозможно, поэтому количество правил нечеткого вывода исследуемой системы будет $N = 4 \cdot 4 \cdot 4 - 1 = 63$.

Нечеткий вывод модели выбора метода модулярного экспоненцирования, построенного на основе заданных 63 правил с текущими значениями переменных resistance, performance, memory и method, имеет вид, представленный на рисунке 2 [10].

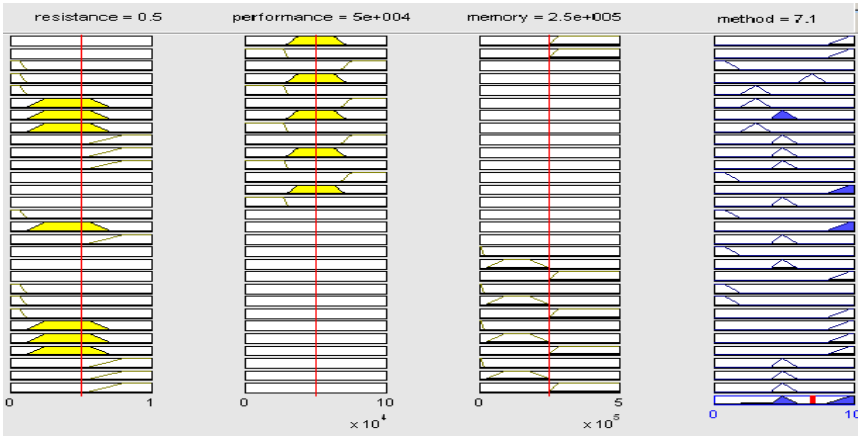
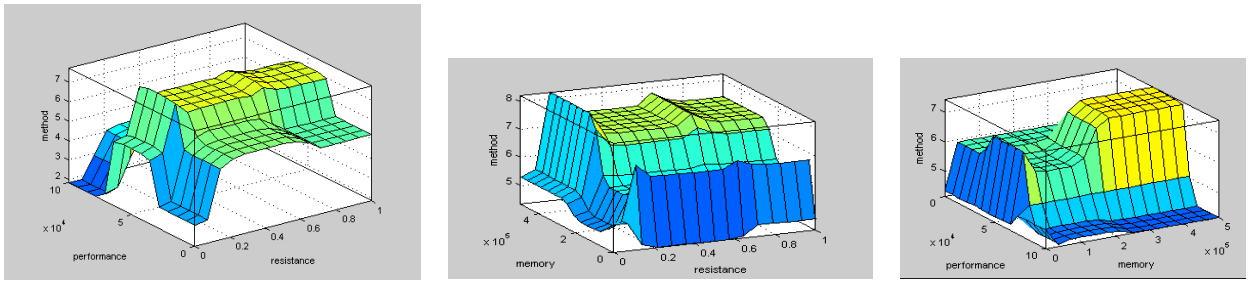


Рисунок 2 – Нечеткий вывод модели выбора метода модулярного экспоненцирования

Поверхности значений нечеткой системы на основе механизма Мамдани представлены на рисунке 3 [10]. Они подтверждают правильность построения базы правил нечеткого вывода.



а б в

Рисунок 3 – Поверхность значений выхода нечеткой системы на основе механизма Мамдани в зависимости от значений: а – устойчивости к временному анализу и производительности; б – затрат памяти устойчивости к временному анализа; в – производительности и затрат памяти

2. Совершенствование предложенной нечеткой системы. Основной недостаток нечеткого вывода, построенного на классическом механизме Мамдани, заключается в том, что для любых входных данных необходимо обрабатывать всю базу правил, то есть осуществлять три шага. Такой путь обработки нечетких данных снижает быстродействие системы и требует больших затрат памяти, поэтому стоит усовершенствовать метод выбора метода модулярного экспоненцирования, основанный на классическом методе Мамдани, который бы удовлетворял требования к быстродействию.

Суть предлагаемого метода выбора метода возведения в степень по модулю заключается в том, что процесс обработки входящей нечеткой информации разделено на этапы обучения и эксплуатации. Во время обучения средства обработки нечеткой информации определены области функций принадлежности выхода для каждого из правил.

При эксплуатации сначала происходит сравнение входных данных со значениями функций принадлежности выхода в определенных базой правил областях памяти, где хранятся значения упомянутых функций принадлежности выхода, соответствующих каждому правилу нечеткого вывода. Далее отсекаются значения функций принадлежности выхода, которые превышают входные данные. Затем выбираются минимальные значения функций принадлежности выхода, полученных после отсечения, и строится из этих минимальных значений соответствующая фигура. Последней операцией метода обработки нечетких данных является поиск центра тяжести фигуры, полученной в результате сложения отсеченных функций принадлежности выхода.

Сравнение операций предлагаемого метода обработки нечеткой информации и классического метода Мамдани при эксплуатации приведены в таблице 1.

Таблица 1 – Операции по обработке нечеткой информаци

№ п/п	Операции нечеткого вывода по классическому механизму Мамдани	Операции нечеткого вывода предлагаемого метода	
		Совпадающие операции предлагаемого метода	Новые операции предлагаемого метода
1	Сравнение входных данных со значениями функций принадлежности входов	–	Сравнение входных даннях со значениями функций принадлежности выходов в соответствующих областях ПЗУ
2	Нахождение наименьшего значения функций принадлежности входов по каждому из входов, которые соответствуют базе правил	–	–
3	Отсечения на оси ординат функций принадлежности выхода значений, превышающих значения, найденные в п. 2	–	Отсечения на оси ординат функий принадлежности выхода во всех соответствующих областях многоканального блока памяти значений, которые превышают значения, найденные в п. 1
4	Нахождение среди отсеченных функий принадлежности выхода, имеющих максимальную амплитуду	–	Нахождение среди отсеченных функий принадлежности выхода, во всех соответствующих областях многоканального блока памяти, имеющих минимальную амплитуду
5	Нахождение суммы найденных в п. 4 значений отсеченных функции принадлежности выхода, что образует конечную фигуру	Нахождение суммы найденных в п. 4 значений отсеченных функции принадлежности выхода, что образует конечную фигуру	–
6	Нахождение центра тяж ести фигуры, полученной в п. 5	Нахождение центра тяж ести фигуры, полученной в п. 5	–

Как видно из таблицы 1, все операции предлагаемого метода близки к операциям классического механизма Мамдании по сложности не превышают их. Однако количество операций в предлагаемом методе меньше, что приводит к росту его производительности. Уменьшение количества операций обусловлено тем, что на этапе обучения (предшествующего этапу эксплуатации) определены области функций принадлежности выхода для каждого из правил. Результаты записаны в соответствующие области многоканального блока памяти, откуда они выбираются при выполнении операций пп.3, 4 таблицы 1.Такая предварительная подготовка собственной позволяет избежать операций, предусмотренной в п. 2 метода Мамдани. Так как временная сложность является основным критерием оценки алгоритма, то рассматривая операции нечеткого вывода предлагаемого метода и механизма Мамдани, описанные в таблице1, для сравнения сложности этих алгоритмов стоит рассмотреть только несовпадающие операции. В таблице 2 представлены временные сложности каждой операции рассмотренных методов нечеткого вывода, учитывая вычисления сложности, проведенные в [11-13]. Анализ таблицы 2 показывает, что временная сложность предлагаемого метода обработки нечеткой информации на $O(n^2)$ меньше, чем сложность механизма нечеткого вывода Мамдани.

Выводы. Таким образом, предлагаемый метод, согласно значениям временной сложности, представленных в [11-13], имеет быстродействие в 4 раза выше, чем классический (при использовании аналогичной аппаратной базы). Уменьшить количество операций в предлагаемом методе и выполнять их именно таким образом, как это указано в таблице 1, удается лишь за счет предварительной обработки на этапе обучения. Дальнейшими исследованиям и может быть реализация данного метода на ПЛИС или ПЛМ.

Таблица 2 – Временная сложность несовпадающих операций нечеткого вывода по механизму Мамдани предлагаемого метода

Операции нечеткого вывода по классическому механизму Мамдани	Временная сложность операций нечеткого вывода по механизму Мамдани	Операции нечеткого вывода предлагаемого метода	Временная сложность операций нечеткого вивода предлагаемого метода
1. Сравнение входных данных со значениями функции принадлежности входов	O(log *n*)	1. Сравнение входных даннях со значениями функции принадлежности выходов в соответствующих областях ПЗУ	O(log *n*)
2. Нахождение наименьшего значения функции принадлежности входов по каждому из входов, которые соответствуют базе правил	O(*n*)	–	–
3. Отсечения на оси ординат функций принадлежности выходных значений, превышающих значение, заданное в п.2	O(log *n*)	3. Отсечения на оси ординат функций принадлежности выхода, во всех соответствующих областях многоканального блока памяти значений, которые превышают значение, найденное в п.1	O(log *n*)
4. Нахождение среди отсеченных фунций принадлежности выхода, имеющих максимальную амплитуду	O(n^2)	4. Нахождение среди отсеченных функций принадлежности выхода, во всех соответствующих областях многоканального блока памяти имеющих минимальную амплитуду	O(*n*)

ЛИТЕРАТУРА

[1] Васильцов И.В. Атаки специального вида на криптоприборы и методы борьбы с ними. / Под ред. В. П. Широчина-Кременец: Издательский центр КОГПИ, 2009. – 264 с.

[2] Brumley D., Boneh D. Remote Timing Attacksare Practical [Электронный ресурс] – Режим доступа: http:/crypto. stanford.edu/~dabo/pubs/papers/ssl-timing.pdf

[3] Quisquater J.-J., Koeune F. Side Channel Attacks / State-of-the-art regarding side channel attacks: report, October. 2010. – 47 p. [Электронный ресурс]–Режим доступа: http:/www.ipa.go.jp/security/enc/CRYPTREC/fy15/doc/1047_Side_Channel_report.pdf

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

[5] Patent US2010/0177887A1, Int.Cl.H04L9/28. Montgomery-based modular exponentiation secured against hidden channel attacks / M. Ciet, B. Feix; Gemalto SA(FR). – Appl. N 12 /666,892; May 2, 2008; Jul. 15,2010.

[6] Patent US 6,282,290B1, Int. Cl.H04K9/28. High speed modular exponentiator/GAPowell, MWWilson, KQTruong, CPCurren; Mykotronx, Inc. (US). – Appl. N 08/828,368; Mar. 28, 1997; Aug. 28,2001.

[7] Лазарев Ю.Ф. Моделирование динамических систем в Matlab. Электронное учебное пособие. – К.: НТУУ«КПИ», 2011. – 421 с. – [Электронный ресурс]. – Режим доступа: http:/kafpson.kpi.ua/Arhiv/Lazarev/mds_matlab.pdf

[8] Карпинский М.П., Дубчак Л.О., Васильков Н.М. Защита информации на основе нечеткой системы // Информатика и математические методы в моделировании. – 2011. – Т. 1, № 3. –С. 236-242.

[9] Гостев В.И., Скуртов С.Н., Панченко И.В. Определение управляющих воздействий на выходе нечеткого регулятора при идентичных треугольных функциях принадлежности с увеличенным наклоном // Вестник Хмельницкого национального университета. Технические науки. – 2007. –№ 5. – С. 253-256.

[10] Дубчак Л.А. База правил нечеткой системы выбора метода модулярного экспоненцирования // Современные компьютерные информационные технологии (ACIT'2012): II Всеукраинская школа-семинар молодых ученых и студентов, 4-5 мая, 2012 г.: Материалы. – Тернополь, 2012. – С. 202.

[11] Constantinescu N., Simion E. Linear Complexity Computations of Cryptographic Systems Telecommunications: International Conference, 4–7 June, 2001: IEEE, Bucharest, 2001.– Vol. 1. – P. 85- 89.

[12] Шайханова А.К., Жангисина Г.Д. Параллельные вычисления в организации сетевой системы // Научный журнал «Вестник Семипалатинского государственного университета им. Шакарима». – 2013. – № 1(61).

[13] Shaikhanova A.K., ZhangisinaG.D. About Parallel Computers // International Journal of Computer Science Engineering and Information Technoligy Research. IC value: 3.0, Edition: APR 2014.

REFERENCES

[1] Vasiltsov I.V. *A special kind of attack on kriptopribory and methods of dealing with them*. Ed. V. P. Shirochin-Kremenets: Publishing Center Korn, **2009**. 264 p. (in Russ.).

[2] Brumley D., Boneh D. *Remote Timing Attacksare Practical.* [electronic resource] -Mode access: http: /crypto.stanford. edu/~dabo/pubs/papers/ssl-timing.pdf (in Eng.).

[3] Quisquater J.-J., Koeune F. *Side Channel Attacks*. State-of-the-art regarding side channel attacks: report, October. **2010.** 47 p. [Electronic resource] -Mode access: http: / www. ipa.go.jp/security/enc/CRYPTREC/fy15/doc/1047_Side_Channel_report.pdf (in Eng.).

[4] Shtovba S.D. *Ensuring the accuracy of transparency Mamdani fuzzy model for teaching the experimental data.* Problems of management and informatics. **2007.** N 4. S.102-114. (in Russ.).

[5] Patent US 2010 / 0177887A1, Int.Cl.H04L9 / 28. Montgomery-based modular exponentiation secured against hidden channel attacks. M. Ciet, B. Feix; Gemalto SA (FR). Appl. N 12 / 666,892; May 2, 2008; Jul. 15, 2010. (in Eng.).

[6] Patent US 6,282,290B1, Int.Cl.H04K9 / 28. High speed modular exponentiator / GAPowell, MWWilson, KQTruong, CPCurren; Mykotronx, Inc. (US). -Appl. No.08 / 828,368; Mar.28, 1997; Aug.28,2001. (in Eng.).

[7] Lazarev Yu. *Simulation of dynamic systems in Matlab.* Electronic Textbook. K.: "KPI", 2011. 421 p. [Electronic resource]. Operation access: http: /kafpson.kpi.ua/Arhiv/Lazarev/mds_matlab.pdf (in Russ.).

[8] Karpinski M.P., Dubchak L.O., Vasilkov N.M. *Protection of information systems based on fuzz*y. *Informatics and Mathematical Methods in 2011. Modelirovanii*. **2011**. Vol. 1, N 3. P. 236-242. (in Russ.).

[9] GostevV.I., Skurtov S.N., Panchenko I.V. *The definition of control actions at the output of fuzzy controller under identical triangular membership function with increased tilt.* Herald of Hmelnitskiy National University. Technical sciences. **2007**. N 5. P. 253-256. (in Russ.).

[10] Dubchak L.A. *The rule base of fuzzy system to choose the method of modular exponentiation. Sovremennye computer information technology* (ACIT'2012): II All-Ukrainian Workshop for young scientists and students, May 4-5, 2012: Materials, Ternopil, **2012**. P. 202. (in Russ.).

[11] Constantinescu N., Simion E. *Linear Complexity Computations of Cryptographic Systems. Telecommunications: International Conference,* 4–7 June, 2001: IEEE, Bucharest. **2001.** Vol. 1. P. 85- 89. (in Eng.).

[12] Shaikhanova A.K., Zhangisina G.D. *Parallel computing in the organization of the network system. Scientific journal "Bulletin of the Semey State University named after Shakarim*». 2013. № 1 (61). (in Russ.).

[13] Shaikhanova A.K., Zhangisina G.D. *About Parallel Computers. International Journal of Computer Science Engineering and Information Technoligy Research*. IC value: 3.0, Edition: APR. **2014.** (in Eng.).

АНЫҚ ЕМЕС ЛОГИКА НЕГІЗІНДЕ АҚПАРАТТЫ ҚОРҒАУ ЖЕЛІЛІК ЖҮЙЕСІНІҢ ҰЙЫМЫНДАҒЫ РҰҚСАТТЫҢ ТАРАТЫЛУЫ

А. К. Шайханова[1], Д. О. Қожахметова[2], М. П. Карпинский[3]

[1] Қ. И. Сәтбаев атындағы Қазақ ұлттық техникалық университеті, Алматы, Қазақстан;
[2] Шәкәрім атындағы мемлекеттік университет, Семей, Қазақстан;
[3] Бельско-Бяла қаласының Технико-гуманитарлық академиясы, Польша

Тірек сөздер: уақытылы күрделік, анық емес жүйе, ақпаратты қорғау, модулярды экспоненцирлеу, RSA, Мамдани әдісі.

Аннотация. Компьютерлік жүйелерді қауіпсіз пайдалану үшін жүйелердің өздерінің есептік ресурстарын ескере отырып, программалы-аппараттық құралдарын пайдаланған жөн. Одан басқа, серверде сақталатын ақпараттың әртүрлі құпия деңгейлері болады, соған орай рұқсаттың таратылу қажеттілігі туады. Сол үшін қазіргі уақыттағы таратылу жолымен шешілетін компьютерлік жүйелердің тұрақтылығы және берілген функционалдылықты қолдайтын әдістердің, алгоритмдердің және программалы-ақпараттық құралдары маңызды тапсырма болып саналады. Мақалада анық емес логика негізінде құжаттарды шифрлық алгоритм жолымен таңдалатын, компьютерлік желілерде берілетін ақпараттық қауіпсіздік әдісі қарастырылған. Берілген жаңа модулярлі экспоненцирлеудің оптималды алгоритм таңдау әдісі белгілі әдістерден айырмашылығы – Мамданидың анық емес қорытынды механизмінде және уақытылы анализге модулярлі экспоненцирлеудің қалыпты, тұрақты алгоритмдерін анықтау әдісінде тіркелген, бұл қазіргі уақыттағы ауыспалы кіріс парамертлерінің ақпаратты қорғау жүйелерінің реакциясын қамтамасыз етеді. Құрастырылған анық емес жүйе – компьютерлік жүйелердің ағымдағы күйін ескере отырып, қазіргі уақыттағы құжаттардың қолданбалы қауіпсіздігін жүзеге асыруға мүмкіндік береді.

Поступила 20.03.2015 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

bulletin-science.kz

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

Подписано в печать 14.04.2015.
Формат 60x881/8. Бумага офсетная. Печать – ризограф.
18,9 п.л. Тираж 2000. Заказ 2.