УДК 004.08

Н.Д. Абасов, А.М. Анкина, Д.И. Ржевский, О.А. Финько

ОТКАЗОУСТОЙЧИВЫЙ РЕГИСТРАТОР ЗАЩИЩЁННОЙ ИНФОРМАЦИИ, ФУНКЦИОНИРУЮЩИЙ В КЛАССАХ ВЫЧЕТОВ

Рассматривается обобщенный алгоритм функционирования и структурная схема устройства регистрации информации, обеспечивающие требования по обеспечению защиты регистрируемой информации, а также высокие показатели отказоустойчивости при ограничениях на объем аппаратных и энергетических ресурсов. Для решения двух указанных задач предложено использовать единый математический аппарат модулярной арифметики. Защита информации обеспечивается известными криптопротоколами с симметричными или ассиметричными ключами, обеспечивающими необходимую защиту информации от чтения-записи или только чтения при нахождении устройства в недоверенной среде. Обеспечение необходимой отказоустойчивости устройства достигается на основе применения избыточных кодов модулярной арифметики. По отношению к методам резервирования (дублирования, троирования и пр.) достигается необходимый уровень отказоустойчивости при уменьшении энергозатрат и сокращении объема оборудования или обеспечивается увеличение информационной емкости устройства, необходимое для удовлетворения современных и перспективных требований к регистрирующим устройствам.

Китайская теорема об остатках; модулярная арифметика; система остаточных классов; устройства регистрации; криптографическая защита информации.

N.D. Abasov, A.M. Ankina, D.I. Rzhevskij, O.A. Finko

FAILSAFE RECORDER PROTECTED INFORMATION, FUNCTION IN THE RESIDUE CLASS

The generalized algorithm of functioning and the block diagram of the device of registration information providing requirements for ensuring of protection of traceable information, and also high indicators of fault tolerance is considered at restrictions on volume of equipment rooms and energy resources. For the solution of two specified tasks it is offered to use uniform mathematical apparatus of modular arithmetics. Protection of information is provided with known cryptographic protocols with the symmetric or dissymetric keys providing necessary protection of information from reading record or only of reading at finding of the device in not entrusted environment. Ensuring necessary fault tolerance of the device is reached on the basis of application of superfluous codes of modular arithmetics. In relation to methods of reservation necessary level of fault tolerance is reached at reduction of energy consumption and reduction of volume of the equipment or the increase in information capacity of the device, necessary for satisfaction of modern and perspective requirements to registering devices is provided.

Chinese Remainder Theorem; modular arithmetic; residual number system; recording devices; cryptographic protection of information.

Введение. Проблема достижения высоких показателей надёжности систем обработки и хранения информации особенно актуальна в устройствах, которые должны сохранить работоспособность в экстремальных условиях. К подобным системам относятся устройства регистрации (УР) используемые для записи, например, основных параметров передвижения транспортных средств, различных внутренних показателей подсистем, переговоров экипажа и пр. [1, 2].

Решение задачи обеспечения высоких показателей надёжности систем хранения информации, в рассматриваемом случае, достоверность восстановления после частичной её утраты, состоит не столько в совершенствовании технических средств, где любое возможное повышение надёжности достигается дорогой ценой, сколько применением таких способов представления информации, которые были бы устойчивы по отношению к возможным искажениям, частичной утрате или модификации, и позволяли бы при необходимости осуществлять коррекцию этих данных.

Наиболее распространённым методом построения надёжных систем является резервирование [3]. Существует множество различных способов резервирования, но для любого из них характерна высокая избыточность. Так, например, большинство современных УР построено по принципу резервирования системы при общем постоянном резервировании с нагруженным резервом. Очевидными недостатками подобного способа повышения надёжности является увеличение стоимости системы и её габаритов.

Анализ информационных источников выявил, что перспективными методами обеспечения высоких показателей отказоустойчивости являются методы модулярной арифметики. Помимо возможности параллельной обработки данных, приводящей к увеличению быстродействия устройства, методы модулярной арифметики обладают также и свойствами обнаружения и коррекции ошибок, что позволяет использовать их для построения высоконадёжных узлов вычислительной техники при наложенных ограничениях на аппаратурные затраты [4].

1. Общие сведения о модулярной арифметике. Пусть заданы попарно взаимно простые модули (основания): положительные числа $m_1, m_2, \dots, m_i, \dots, m_k$,

$$\text{НОД}\left(m_i, m_j\right) = 1 \text{ для } i \neq j.$$

Значение $P = \prod_{i=1}^{k} m_i$ определяет информационный диапазон получившейся числовой системы. Любое неотрицательное целое число A может быть однозначно представлено модулярным кодом:

$$\mathrm{A} = \{\alpha_1, \alpha_2, \dots, \alpha_i, \dots, \alpha_k\},$$

компонентами которого являются натуральные числа, удовлетворяющие условию:

$$0 \leq \alpha_i < m_i, \text{ где } i = 1,2, \dots, k.$$

Фундаментальным положением, лежащим в основе модулярных вычислений, является Китайская Теорема об остатках.

Пусть даны попарно взаимно простые модули $\{m_1, m_2, \dots, m_i, \dots, m_k\}$ и число $X \in Z(P)$, модулярное представление которого $\{\alpha_1, \alpha_2, \dots, \alpha_i, \dots, \alpha_k\}$ определяется выражением

$$\alpha_i = |A|_{m_i}, \text{ где } i = 1,2, \dots, k.$$

Для каждого специального кода, от которого требуется, чтобы он обладал способностью к обнаружению и коррекции ошибок, характерно наличие двух групп цифр – информационной $J_A = \{\alpha_1, \alpha_2, \dots, \alpha_i\}$ и контрольной $K_A = \{\alpha_{k+1}, \dots, \alpha_{k+n}\}$ части кода соответственно.

Наиболее распространёнными и эффективными являются избыточные R-коды в системе остаточных классов с взаимно простыми модулями. Избыточный модулярный код (ИМК) задаётся набором модулей: $\{m_1, m_2, \dots, m_i, \dots, m_{k+1}, m_{k+2}, \dots m_{k+n}\}$, информационным диапазоном P и полным диапазоном системы с контрольными основаниями $P` = \prod_{i=1}^{k+n} m_i$. Согласно положениям модулярной арифметики, числа, с которыми оперирует устройство, лежат в диапазоне $[0, P`)$. Признаком ошибки является выполнение условия $A > P$. Под ошибкой будем понимать любое искажение значения, соответствующего какому-либо модулю в модулярном представлении числа. Выявленная ошибка может быть исправлена одним из существующих корректирующих методов [3].

2. Синтез структуры устройста регистрации, функционирующего в ИМК. Имеется i датчиков $(S_1, S_2, \dots, S_i)$, данные с которых необходимо регистрировать. Информация в виде последовательности бит a_t поступает на входы мультиплексора, где под воздействием управляющего сигнала устройства управления преобразуется в единый блок данных:

$$A = (a_t, a_{t-1}, \dots, a_0)_2,$$

представляющий собой запись числа A в двоичной системе счисления. С помощью преобразователя из позиционной системы счисления (ПСС) в ИМК двоичное представление A преобразуется в ИМК [4]:

$$\mathrm{A} = \{\alpha_1, \alpha_2, \dots, \alpha_i, \dots, \alpha_{k+n}\}.$$

Полученные наименьшие значения вычетов α_i поступают в регистры памяти и затем подвергаются шифрованию. Результат шифрования каждого i-го блока данных, взятого из регистра памяти, представлен криптограммой C_i. Процедура шифрования имеет вид [5]:

$$\begin{cases} \mathrm{C}_1 = E_{k_1^{(1)}}(\alpha_1) \pmod{m_1}, \\ C_2 = E_{k_1^{(2)}}(\alpha_2) \pmod{m_2}, \\ \dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots \\ C_i = E_{k_1^{(i)}}(\alpha_i) \pmod{m_i}, \\ \dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots \\ C_{k+n} = E_{k_1^{(k+n)}}(\alpha_{k+n}) \pmod{m_{k+n}}, \end{cases}$$

где $k_1^{(1)}, k_1^{(2)}, \dots, k_1^{(i)}, \dots, k_1^{(k+n)}$ – система ключей шифрования.

Зашифрованные блоки данных $C_1, C_2, \dots, C_i, \dots, C_{k+n}$ поступают в запоминающее устройство ($ЗУ_1$, $ЗУ_2$,…$ЗУ_i$,…$ЗУ_{k+n}$).

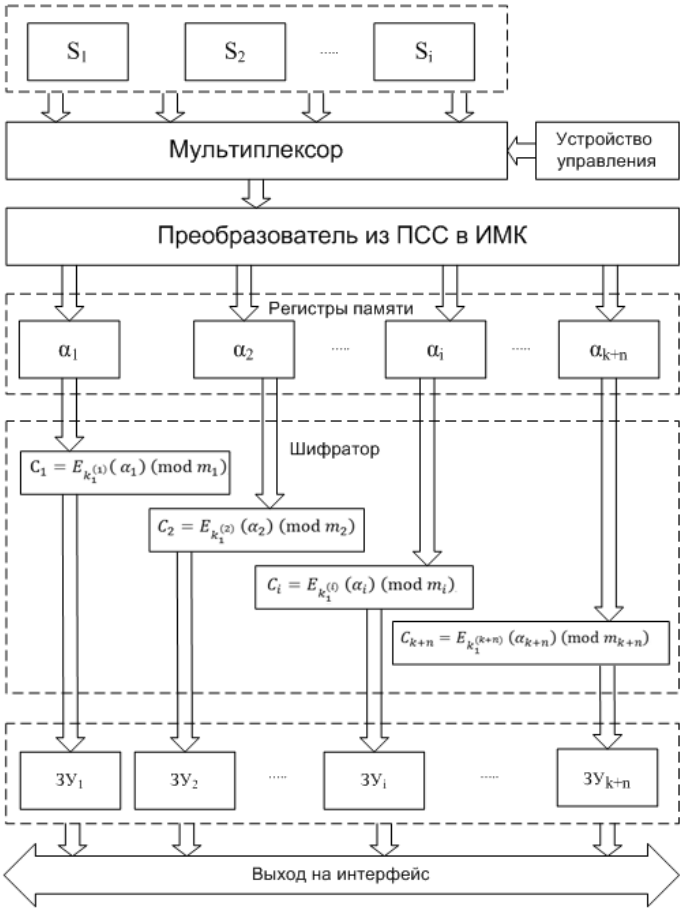

Рис. 1. Обобщенная схема УР функционирующего в ИМК

На рис. 2 изображена обобщенная структурная схема считывателя. Пусть система модулей $m_1, m_2, \dots, m_i, \dots, m_k$ дополнена ещё n избыточными модулями $m_{k+1}, \dots m_{k+n}$, такими что:

$$\text{НОД}\left(m_i, m_j\right) = 1, \text{ где } i, j = 1,2, \dots, k+n,$$

$$m_1, m_2, \dots, m_i, \dots, m_k < m_{k+1} < m_{k+2} < \dots < m_{k+n}.$$

Данные предположения определяют систему чисел $\alpha_1, \alpha_2, \dots, \alpha_i, \dots, \alpha_{k+n}$ обладающую свойствами обнаружения и исправления ошибок. Посредством интерфейса сопряжения, массив зашифрованных данных $C_1, C_2, \dots, C_i, \dots, C_{k+n}$ попадает в регистры памяти считывателя, после чего происходит процедура расшифрования, представленная в форме выполнения следующих действий:

$$\begin{cases} \alpha_1 = D_{k_2^{(1)}}(C_1) \pmod{m_1}, \\ \alpha_2 = D_{k_2^{(2)}}(C_2) \pmod{m_2}, \\ \dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots \\ \alpha_i = D_{k_2^{(i)}}(C_i) \pmod{m_i}, \\ \dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots \\ \alpha_{k+n} = D_{k_2^{(k+n)}}(C_{k+n}) \pmod{m_{k+n}}. \end{cases}$$

Попадая в блок обнаружения, коррекции ошибок и преобразования из ИМК в ПСС массив данных $\alpha_1, \alpha_2, \dots, \alpha_i, \dots, \alpha_{k+n}$ подвергается проверке на наличие ошибок, которые после выявления исправляются.

Демультиплексор под воздействием устройства управления осуществляет преобразование данных для последующей их передачи на интерфейс данных.

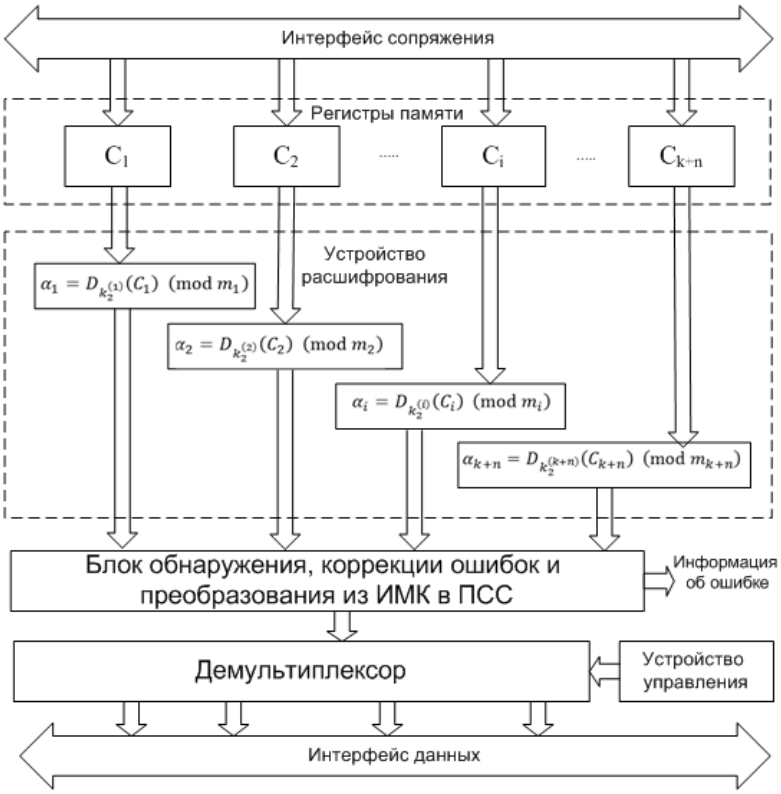

Рис. 2. Обобщенная структурная схема считывателя

Заключение. По сравнению с методами резервирования, ИМК позволяет минимизировать объём избыточного оборудования УР при более высоких уровнях показателей надёжности. Применение методов шифрования обеспечивает необходимый уровень защиты информации, хранящейся в УР.

При ассиметричном шифровании ($k_1^{(i)}$ – открытый ключ шифрования) обеспечивается высокий уровень безопасности информации при компрометации ключей шифрования, используемых в УР.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Российская Федерация. Правительство. О федеральных правилах использования воздушного пространства и федеральных авиационных правилах: утв.постановлением Правительства РФ от 27 марта 1998г. №360: в ред. постановления Правительства РФ от 15.04.2000 №344 // Собр.законодательства РФ. – 1998. – № 14, ст. 1593; – 2000. – № 17, ст. 1875.
2. ОСТ 1 01080–95. Устройства регистрации бортовые с защищенными накопителями. Общие технические требования. – Введ. 01.01.1997. – М.: Изд–во НИИСУ, 1997. – 40 с.
3. *Острейковский В.А.* Теория надежности – М.: Высш. шк., 2003. – 463 с.
4. *Акушский И.Я., Юдицкий Д.И.* Машинная арифметика в остаточных классах. – М.: Советское радио, 1968. – 440 с.
5. *Ржевский Д.А., Елисеев Н.И., Абасов Н.Д., Финько О.А.* Электронная подпись, устойчивая к деструктивным воздействиям // Известия ЮФУ. Технические науки. – 2011. – № 12 (125). – С.140-146.

Статью рекомендовал к опубликованию д.т.н., профессор В.Н. Марков.

Абасов Низам Джавидович – Федеральное государственное автономное образовательное учреждение высшего профессионального образования «Южный федеральный университет»; e-mail: galactic_07@mail.ru; 347928, г. Таганрог, ул. Чехова, 22; тел.:+79528169696; аспирант.

Анкина Анастасия Михайловна – e-mail: moonriel@yandex.ru; тел.:+79054384978; аспирантка.

Ржевский Дмитрий Игоревич – Филиал Военной академии связи (г. Краснодар); e-mail: ofinko@yandex.ru; 350035, г. Краснодар, ул. Красина, 4; тел.: +79615874848; старший специалист отдела.

Финько Олег Анатольевич – e-mail: ofinko@yandex.ru; тел.: +79615874848; профессор.

Abasov Nizam Dzhavidovich – Federal State-Owned Autonomy Educational Establishment of Higher Vocational Education “Southern Federal University”; e-mail: galactic_07@mail.ru; 22, Chekhova Street, Taganrog, 347928, Russia; phone: +79528169696; postgraduate student.

Ankina Anastasiya Mikhailovna – e-mail: moonriel@yandex.ru; phone: +79054384978; postgraduate student.

Rzhevskij Dmitriy Igorevich – Branch of the Military Academy of Communications (Krasnodar); e-mail: ofinko@yandex.ru; 4, Krasina, Krasnodar, 350035, Russia; phone: +79615874848; senior specialist of the department.

Finko Oleg Anatolievich – e-mail: ofinko@yandex.ru; phone: +79615874848; professor.