**Каменская Елена Николаевна** – Южный федеральный университет; e-mail: Kamenskay-E@ya.ru; 347920, г. Таганрог, ул. Ленина, 157, кв. 129; тел.: 89514916863; кафедра психологии и безопасности жизнедеятельности; д.пед.н.; профессор.

**Толмачёва Лариса Владимировна** – e-mail: Tolmacheva_larisa58@mail.ru; 347909, Таганрог, ул. Прибрежная, 8; тел.: 89281544848; кафедра психологии и безопасности жизнедеятельности; к.т.н.; доцент.

**Kamenskaya Elena Nikolaevna** – Southern Federal University; e-mail: Kamenskay-E@ya.ru; 157, Lenin street, flat 129, Taganrog, 347920, Russia; phone: +79514916863; the department of psychology and safety of existence; dr. of ped. sc.; professor.

**Tolmacheva Larisa Vladimirovna** – e-mail: Tolmacheva_larisa58@mail.ru; 8, Seaside street, Taganrog, 347909, Russia; phone: +79281544848; the department of psychology and safety of existence; cand. of eng. sc.; associate professor.

УДК 004.08

**Н.Д. Абасов**

## ОРГАНИЗАЦИЯ ЖУРНАЛА ТРАНЗАКЦИИ OLTP-СИСТЕМЫ, ФУНКЦИОНИРУЮЩЕГО В ИЗБЫТОЧНОМ МОДУЛЯРНОМ КОДЕ

*В связи с повсеместной информатизацией банковской деятельности, наблюдается рост степени важности информационной безопасности автоматизированных систем обработки информации банка (АСОИБ) и обеспечения безопасности удалённых транзакций. В результате широкого распространения электронных платежей, устройств самообслуживания, таких как банкоматы и платёжные терминалы, пластиковых карт, объектом информационных атак стали денежные средства, как клиентов банков, так и самих банков. Предложен способ организации системной структуры, называемой журналом транзакций Online Transaction Processing (OLTP) – системы оперативной обработки транзакций, функционирующей в избыточном модулярном коде. Журнал транзакций позволяет, в случае возникновения разного рода сбоев, корректно зафиксировать транзакции в базе данных, свести к минимуму риск некорректного восстановления базы данных при условии повреждения журнала транзакций, минимизировать количество незавершенных операций при осуществлении обработки удаленных банковских транзакций. Приведена имитационная модель данной системы, демонстрирующая возможность восстановления согласованного состояния базы данных после возникновения аппаратных и программных сбоев.*

*OLTP–система; транзакция; транзакционная система; журнал транзакций; модулярная арифметика.*

**N.D. Abasov**

## ORGANISATION OF TRANSACTION LOG OLTP-SYSTEM FUNCTIONING IN SURPLUS MODULAR CODE

*Currently, due to the widespread computerization of banking, there is manifold increase in the value of information security of automated information processing systems of the bank (AIPSB) and secure remote transactions. As a result of widespread electronic payments, self–service devices, such as ATMs and payment terminals, cards, phishing attacks have become the object of cash as customers of banks, and the banks themselves. We propose a method of organizing the system structure called the transaction log of the Online Transaction Processing (OLTP) – line transaction processing systems operating in excess modular code. The transaction log allows in case of failure of some sort, correct fix transactions in the database, to minimize the risk of incorrect da-*

*tabase recovery provided damage transaction log, to minimize the number of pending operations in the implementation of remote processing banking transactions. Shows the simulation model of the system, showing the ability to restore a consistent state of the database after hardware and software failures.*

*OLTP–system; transaction; transaction system; the transaction log; modular arithmetic.*

**Введение.** В АСОИБ, как в любой сложной компьютерной системе, в процессе функционирования возникают ошибки и сбои, которые приводят к отказам в выполнении операции или к выполнению ошибочных операций [1, 2]. Это влечет за собой существенный финансовый риск для различных коммерческих структур и организаций, особенно тех, кто по роду своей деятельности хранит и обрабатывает ценную информацию, затрагивающую интересы большого количества людей.

Услуги, предоставляемые банками, основаны на использовании средств электронного взаимодействия банков между собой, банков и их клиентов и торговых партнеров – электронной коммерцией. В настоящее время доступ к услугам банков стал возможен из различных удаленных точек посредствам удалённых банковских транзакций – совокупности операций, сопровождающих удалённое взаимодействие платёжной системы и покупателя. Примерами удалённых транзакций могут послужить оплата услуг через платёжные терминалы, расчеты в точках продаж, использование дистанционного банковского обслуживания (ДБО), при котором доступ к счетам и операциям по ним предоставляется в любое время и с любого устройства, имеющего доступ в Интернет. Транзакция обычно включает в себя запрос, выполнение задания в соответствии с запросом, и ответ [3]. В случае банковских транзакций эти три составляющие представляют собой денежные средства, передаваемые по каналам связи. Отсюда следует, что на текущий момент, вопрос защиты удалённых банковских транзакций является особенно актуальным. В данном направлении ведутся серьезные работы, как в практическом, так и в теоретическом плане, используются передовые и дорогостоящие технологии и комплексы средств, повышающие надежность и безопасность при обработке и хранении транзакций. Целью данной работы является разработка способа организации журнала транзакций OLTP-системы, позволяющего свести к минимуму риск некорректного восстановления базы данных при условии повреждения журнала транзакций, минимизировать количество незавершенных операций при осуществлении обработки удаленных банковских транзакций, а также повысить быстродействие системы и обеспечить высокий уровень безопасности информации.

**1. OLTP–система. Журнал транзакций.** OLTP-система – система, обрабатывающая транзакции в реальном времени, работающая с небольшими по размерам транзакциями, но идущими большим потоком, с условием выполнения требования минимального времени отклика системы. OLTP–системы предназначены для ввода, структурированного хранения и обработки информации (операций, документов) в режиме реального времени.

В общем случае к OLTP–системам применяются следующие основные требования [4]:

- должна обеспечиваться нормализация данных;
- при возникновении ошибки транзакция должна вернуть систему к состоянию, которое было до начала транзакции;
- обработка транзакций осуществляется в реальном времени.

Транзакция представляет собой набор данных, состоящих из индикатора типа сообщения, информации битовых карт и элементов данных, полей сообщения [5].

Для поддержки множества операций в OLTP–системах предусмотрено ведение журнала транзакций. Это обеспечивает, в случае возникновения сбоя, правильность отражения зафиксированной транзакции в базе данных. Этим гаранти-

руется, что «откат» незафиксированной транзакции будет выполнен надлежащим образом, и она не будет отражена в базе данных после сбоя. Этим же обеспечивается возможность отмены незавершенной транзакции и «отката» всех ее операций.

Восстановление после сбоя возможно только в том случае, если не пострадал журнал транзакций. Журнал транзакций является самой важной частью OLTP–системы – это единственное место, в котором в случае сбоя гарантируется наличие описаний всех изменений базы данных.

Журнал транзакций разбит на небольшие части, называемые виртуальными файлами журналов (или файлами VLF). Это вспомогательные средства для облегчения внутреннего управления журналом транзакций.

Если журнал транзакций отсутствует или поврежден после сбоя, тогда восстановление выполнить невозможно, в результате чего база данных становится сомнительной. В этом случае базу данных необходимо восстанавливать из резервных копий или использовать для восстановления менее желательные режимы, такие как аварийное восстановление.

Существует множество различных способов резервирования, но для любого из них характерна высокая избыточность. Так, например, большинство современных высоконадежных систем построено по принципу резервирования 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 предотвращения и исправления ошибок, возникающих в результате сбоев в транзакционных системах, обеспечения высоких показателей отказоустойчивости являются методы модулярной арифметики. Помимо возможности параллельной обработки данных, приводящей к увеличению быстродействия, методы модулярной арифметики обладают также и свойствами обнаружения и коррекции ошибок, что позволяет использовать их для корректного восстановления базы данных транзакций OLTP–системы.

**2. Модулярная арифметика. Общие сведения. Имитационная модель организации функционирования журнала транзакций OLTP–системы** [7]. Пусть заданы попарно взаимно простые модули (основания): положительные числа $p_1, p_2, \dots, p_i, \dots, p_k$, НОД $(p_i, p_q) = 1$ для $i \neq q$.

Значение $P = \prod_{i=1}^{k} p_i$ определяет информационный диапазон получившейся числовой системы. Любое неотрицательное целое число А может быть однозначно представлено модулярным кодом $A = \{\alpha_1, \alpha_2, \dots, \alpha_i, \dots, \alpha_k\}$, компонентами которого являются натуральные числа, удовлетворяющие условию $0 \leq \alpha_i < p_i$, где $i = 1,2, \dots, k$.

Наиболее распространёнными и эффективными являются избыточные R–коды в системе остаточных классов с взаимно простыми модулями. Избыточный модулярный код (ИМК) задаётся набором модулей: $\{p_1, p_2, \dots, p_i, \dots, p_{k+1}, p_{k+2}, \dots, p_{k+n}\}$, информационным диапазоном Р и полным диапазоном системы с контрольными основаниями $P` = \prod_{i=1}^{k+n} p_i$. Согласно положениям модулярной арифметики, числа, с которыми оперирует устройство, лежат в диапазоне $[0, P`)$. Одним из признаков 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.

Рассмотрим имитационную модель журнала транзакций OLTP–системы, разработанную в среде моделирования MatLab Simulink, функционирующую в избыточном модулярном коде (ИМК), изображённую на рис. 1.

Транзакция, в виде последовательности бит $d_t$, поступает на входы мультиплексора, где под воздействием управляющих сигналов устройства управления преобразуется в блок данных размером *t* бит, представляющий собой запись числа *A* в двоичной системе счисления: $A = (d_t, d_{t-1}, \dots, d_1)_2$.

Далее блок данных *A* поступает в преобразователь из позиционной системы счисления (ПСС) в ИМК, в котором происходит преобразование двоичного кода в избыточный модулярный код.

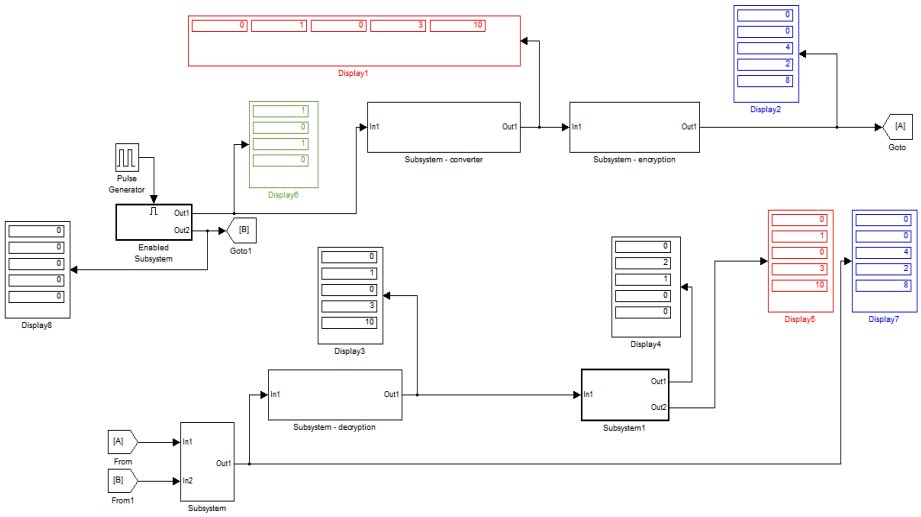


*Рис. 1. Имитационная модель OLTP-системы, функционирующая в ИМК*

Пусть $A = (d_t d_{t-1} \dots d_2 d_1)_2$ – t–разрядное целое двоичное число, которое лежит в пределах интервала $[0, 2^t - 1]$, основания ИМК $p_1, p_2, \dots, p_i, \dots, p_{k+1}, \dots, p_{k+n}$ а ИМК $A = \langle \alpha_1, \alpha_2, \dots, \alpha_i, \dots, \alpha_{k+1}, \dots, \alpha_{k+n} \rangle$, такое что $A = \langle |A|_{p_1}, |A|_{p_2}, \dots, |A|_{p_i}, \dots, |A|_{p_{k+1}}, \dots, |A|_{p_{k+n}} \rangle$. Выразим величину числа A следующим образом:

$$A = 2^{t-1} d_t + 2^{t-2} d_{t-1} + \dots + 2^2 d_3 + 2^1 d_2 + 2^0 d_1 = \sum_{l=1}^{t} (2^{l-1} d_l), \qquad (1)$$

где $l = 1, 2, \dots, t$ – позиции двоичных разрядов $d_j \in \{0,1\}$, в соответствии с которыми однозначно определяются веса этих разрядов в двоичной системе счисления.

С учетом (1), выражение для получения *i*–й знакопозиции $\alpha_i = |A|_{p_i}$, будет иметь вид:

$$\alpha_i = |2^{t-1} d_t + 2^{t-2} d_{t-1} + \dots + 2^2 d_3 + 2^1 d_2 + 2^0 d_1|_{p_l} = |\sum_{l=1}^{t} (2^{l-1} d_l)|_{p_l}. \qquad (2)$$

Полученные наименьшие значения вычетов $\alpha_i$ 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, адаптированная к ИМК, имеет вид [8]:

$$\begin{cases} C_1 = E_{k_1^{(1)}}(\alpha_1) \pmod{p_1}, \\ C_2 = E_{k_1^{(2)}}(\alpha_2) \pmod{p_2}, \\ \dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots \\ C_i = E_{k_1^{(i)}}(\alpha_i) \pmod{p_i}, \\ \dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots \\ C_{k+n} = E_{k_1^{(k+n)}}(\alpha_{k+n}) \pmod{p_{k+n}}, \end{cases}$$

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 запоминающие устройства $VLF_1, VLF_2, \dots, VLF_i, \dots, VLF_{k+n}$.

Рассмотрим метод коррекции ошибок, основанный на R–кодах модулярной арифметики.

Пусть ИМК задан системой оснований $p_1, p_2, \dots, p_i, \dots, p_{k+1}, \dots, p_{k+n}$, полным диапазоном системы $P`$, ортогональными базисами системы $B_1, B_2, \dots, B_i, \dots, B_{k+1}, \dots, B_{k+n}$ и их весами $m_1, m_2, \dots, m_i, \dots, m_{k+1}, \dots, m_{k+n}$ причём:

$$B_i = m_i \frac{P'p}{p_i},\ i = \overline{1,n},$$

где $m_i$ – целое положительное число, которое назовём весом ортогонального базиса системы.

Данные условия определяют систему чисел $\alpha_1, \alpha_2, \dots, \alpha_i, \dots, \alpha_{k+1}, \dots, \alpha_{k+n}$, обладающую свойствами обнаружения и исправления ошибок.

В момент обращения к журналу транзакций массив шифрованных данных $C_1, C_2, \dots, C_i, \dots, C_{k+n}$ попадает в регистры памяти, после чего происходит процедура расшифрования, представленная в форме выполнения следующих процедур:

$$\begin{cases} \alpha_1 = D_{k_2^{(1)}}(C_1) \pmod{p_1}, \\ \alpha_2 = D_{k_2^{(2)}}(C_2) \pmod{p_2}, \\ \dots \\ \alpha_i = D_{k_2^{(i)}}(C_i) \pmod{p_i}, \\ \dots \\ \alpha_{k+n} = D_{k_2^{(k+n)}}(C_{k+n}) \pmod{p_{k+n}}. \end{cases}$$

Далее массив данных $\{\alpha_1, \alpha_2, \dots, \alpha_i, \dots, \alpha_{k+n}\}$ поступает в блок обнаружения, коррекции ошибок и преобразования из ИМК в ПСС.

На первом этапе задача этого блока состоит в проверке поступивших данных. Предлагаемый способ реализации контроля данных базируется на переводе ИМК в полиадический код.

Значения разрядов полиадического кода $\{z_1, z_2, \dots, z_{n+k}\}$ по модулям $p_1, p_2, \dots, p_i, \dots, p_{k+1}, \dots, p_{k+n}$ могут быть получены из ИМК $\{\alpha_1, \alpha_2, \dots, \alpha_i, \dots, \alpha_{k+n}\}$ с помощью системы сравнений:

$$\begin{cases} z_1 = \alpha_1, \\ z_2 = \left| |p_1^{-1}|_{p_2}(\alpha_2 - z_1) \right|_{p_2}, \\ z_3 = \left| |p_2^{-1}|_{p_3}\left(|p_1^{-1}|_{p_3}(\alpha_3 - z_1) - z_2\right) \right|_{p_3}, \\ \dots \\ z_n = \left| |p_{n-1}^{-1}|_{p_n}\left(|p_{n-2}^{-1}|_{p_n}\left(\dots |p_2^{-1}|_{p_n}\left(|p_1^{-1}|_{p_n}(\alpha_n - z_1) - z_2\right)\dots\right) - z_{n-1}\right) \right|_{p_n} \\ \dots \end{cases}$$

Пусть $A = \{z_1, z_2, \dots, z_{n+k}\}$ – полученный результат вычислений. Тогда $A$ лежит в диапазоне разрешённых значений, когда и только когда избыточные цифры полиадического кода являются нулевыми, т.е. $z_{n+r} = 0$ для $r = 1, 2, \dots, k$.

Таким образом, в качестве критерия истинности числа $A$ используется тот факт, что цифры полиадического кода по избыточным основаниям ИМК для правильного числа равны нулю. Достоинством данного метода является то, что при неравенстве нулю любой разрядной цифры $z_{n+1}, \dots, z_{n+k}$ процесс перевода прекращается. Это позволит сократить средний объём вычислений, требуемый для обнаружения ошибок.

В случае истинности числа $A$ исходное представление в двоичной форме формируется из полученных коэффициентов обобщённой полиадической системы:

$$A = z_{n+k}p_{n+k-1}p_{n+k-2} \dots p_1 + z_3p_2p_1 + z_2p_1 + z_1$$

В случае выявления ошибки коррекция осуществляется на основе одного из существующих методов. Рассмотрим механизм коррекции ошибки, основанный на методе проекций.

Определим $A_{ij}$ полученное из $A$ исключением цифр по основаниям $p_i$ и $p_j$ проекцией числа $A$ по основаниям $p_i$ и $p_j$, причём $i \neq j$.

Вычислим проекции числа $A$ по всем основаниям: $A_{12}, \dots, A_{ij}$. Среди этих проекций выявим

$$A_{ij} < \frac{P'}{p_{n+1} \cdots p_{n+k}},$$

тогда ошибочными являются цифры $\alpha_i,\ \alpha_j$.

После того, как выявлены ошибочные цифры, осуществляется их исправление по формуле:

$$\alpha_i = \widetilde{\alpha_i} + \left[\frac{p_i(1+kp_{n+1})}{p_{n+1}m_i}\right].$$

**Выводы.** Предложенный способ организации журнала транзакций OLTP-системы оперативной обработки транзакций позволяет сводить к минимуму риск некорректного восстановления базы данных при условии повреждения журнала транзакций, свести к минимуму количество незавершённых операций при осуществлении удалённых транзакций, вызванных сбоями транзакций, узлов (системы), носителей информации за счет корректирующих способностей модулярного кода. Также способность данных, представленных модулярным кодом, к параллельной обработке и, соответственно, к параллельной организации работы подсистем при обработке нормализованных данных транзакций и адаптированная к ИМК процедура шифрования позволят повысить быстродействие системы и обеспечить высокий уровень безопасности информации.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. *Семин Г.* Автоматизация коммерческого банка: взгляд из России // Read. Me – 1996. – № 10. – С. 7-11.
2. Автоматизация банковской деятельности / Московское Финансовое Объединение / Под ред.С.И. Кумока. – М.:МФО, 1994. – 256 с.
3. *Рассел Д., Кон Р.* Обработка транзакций. – М.: VSD, 2013. – 81 с.
4. *Деднев М.А., Дыльнов Д.В., Иванов М.А.* Защита информации в банковском деле и электронном бизнесе. – М.: Кудиц–образ, 2004. – 512 с.
5. ISO 8583:2003. Сообщения, инициированные банковскими карточками для финансовых операций. Требования к обмену сообщениями. – Введ. 15.06.2003. – 204 с.
6. *Голдовский И.* Безопасность платежей в Интернете. – СПб.: Питер, 2001. – 240 с.
7. *Акушский И.Я., Юдицкий Д.И.* Машинная арифметика в остаточных классах. – М.: Советское радио, 1968. – 440 с.
8. *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 О.А. Финько.

**Абасов Низам Джавидович** – Южный федеральный университет; e-mail: galactic_07@mail.ru; 347928, г. Таганрог, ул. Чехова, 2; тел.: +79649090220; кафедра безопасности информационных технологий; аспирант.

**Abasov Nizam Dzhavidovich** – Southern Federal University"; e-mail: galactic_07@mail.ru; 2, Chekhova Street, Taganrog, 347928, Russia; phone: +79649090220; the department of security in data processing technologies; postgraduate student.