2. Greg N. Gregoriou. Operational Risk Toward Basel III: Best Practices and Issues in Modeling, Management, and Regulation. The Wiley Finance Series, 2010, 498 p.
3. International Convergence of Capital Measurement and Capital Standarts Basle Committee on Banking Supervision. Basel: Guli, 1988.
4. Powel. Basel II and developing countries: Sailing through the sea of standards, рабочий документ по стратегическим исследованиям Всемирного банка №3387, 2004, стр. 27
5. Basel Capital Accord, Базель I Соглашение о достаточности капитала, Базельский комитет по банковскому надзору, Basel: Guli, 1988.
6. International Convergence of Capital Measurement and Capital Standarts Basle Committee on Banking Supervision. Basel: Guli, 2006.
7. http://www.bis.org/publ/bcbs118.htm - Basel II: International Convergence of Capital Measurement and Capital Standards: A Revised Framework November 2005.
8. www.bis.org/publ/bcbs107.pdf - The International Convergence of Capital Measurement and Capital Standards: a Revised Framework, Basel II Framework, 2004.
9. http://www.vedomosti.md/news/Natsionalnyi_Bank_Moldovy_Budet_Podvergat_Kommercheskie_Banki_Ezhemesyachnomu_Stresstestu - Национальный банк Молдовы будет подвергать коммерческие банки ежемесячному стресс-тесту. Молдавские ведомости, №2 (1348) от 13 января 2011 г.
10. http://www.nbm.md – сайт НБМ

# РАЗРАБОТКА АЛГОРИТМА КОДА АУТЕНТИФИКАЦИИ СООБЩЕНИЙ

***Татьяна БИЛЫК,***
*Московский государственный институт электроники и математики (технический университет) (Российская Федерация)*

*This article describes the Message authentication code algorithm, which was developed by the author. This algorithm ensures the authenticity of the message between two or more parties to the transaction. The algorithm may use variable key and tag lengths.*

*1. Введение*

Код аутентификации сообщений представляет собой функцию, получающую на вход два аргумента (сообщение произвольной длины и известный отправителю и получателю секретный ключ), на выходе выдается результат, называемый имитовставкой. Обычно имитовставка передается или хранится вместе с самими защищаемыми данными. При получении данных, пользователь вычисляет значение имитовставки и сравнивает ее с имеющимся контрольным значением. Несовпадение

говорит о том, что данные были изменены либо подделаны. Таким образом, код аутентификации сообщений обеспечивает целостность и подлинность информации.

*2. Стойкость кода аутентификации сообщений*

Исследования показали, что сложность атаки на код аутентификации сообщений с длиной секретного ключа t бит и длиной имитовставки n бит оценивается как $O(2^{\min(t, n/2)})$, а число операций для её реализации $\min(t, n/2)$. Увеличивая параметры t и n, мы можем увеличить защищенность алгоритма, однако выбор слишком больших значений приведет к удорожанию его эксплуатации. В настоящее время минимально «безопасными» параметрами можно считать 128 битную длину ключа и 256 битную длину имитовставки, однако в связи с ростом вычислительных возможностей предвидится увеличение этих значений. Оптимальным является выбор t и n, удовлетворяющих соотношению $\begin{cases} t = n/2 \\ t \geq 128 \\ n \geq 256 \end{cases}$ (1)

*3. Постановка задачи*

В связи с неоднозначностью определения верхней границы параметров t, n, необходимо разработать универсальный алгоритм кода аутентификации сообщений, позволяющий выбирать любые t, n, удовлетворяющие соотношению (1).

*4. Существующие подходы построения кода аутентификации сообщений*

В настоящее время существуют следующие подходы построения кода аутентификации сообщений: на основе хэш-функции, на основе блочного шифра, на основе «универсального» хэширующего преобразования. Исследования показали, что для построения кода аутентификации сообщений, удовлетворяющего приведенным требованиям, оптимальным является второй подход. Далее приводится описание алгоритма кода аутентификации сообщений, разработанного на основе алгоритма CMAC.

*5. Алгоритм кода аутентификации сообщений*

Второй подход в простейшем виде заключается в использовании блочного шифра в режиме сцепления блоков шифртекста. Имитовставкой при этом является последний выходной блок шифрующего преобразования, т.е. длина имитовставки равна длине выхода этого преобразования. Для решения поставленной задачи был разработан алгоритм блочного преобразования, выдающий на выходе блоки любой длины кратной 64 битам. Обозначим b – длину имитовставки в битах, b кратно 64.

*5.1 Получение ключевой информации*

Алгоритм для инициализации требует один секретный ключ K` длины b/2 бит, на основе которого вычисляется ключ K длины кратной 256 бит и ключи K1, K2 длины b/2 бит каждый:

1) Вычисляем $L = E_K(0^b, K')$, где E – блочное преобразование, описанное в п. 5.3;
2) Вычисляем $K1 = L \cdot u$, где выражение $L \cdot u$ - произведение L и u в поле $GF(2^b)$;
3) Вычисляем $K2 = L \cdot u^2$;
4) Если $b/2 = 32s : 256$, то K=K` и конец, иначе переходим к следующему шагу;

5) Разбиваем $K'$ на блоки длины 256 бит, последний блок будет неполным: $K'[1],...,K'[\lfloor s/8 \rfloor], K'[\lfloor s/8 \rfloor + 1]$.

6) Вычисляем $K'[i] = K[i]$ для $\forall i = \overline{1, \lfloor s/8 \rfloor}$ и $K'[\lfloor s/8 \rfloor + 1] = Hash(K[\lfloor s/8 \rfloor + 1])$, где Hash – вычисление хэш-функции по алгоритму ГОСТ Р 34.11-94.

*5.2 Основной алгоритм кода аутентификации сообщений*

Входное сообщение дополняется с конца 32 битами, содержащими длину сообщения. Результат M разбивается на блоки длины b бит. Имитовставка вычисляется применением к входному сообщению шифрующего преобразования E в режиме сцепления блоков шифртекста. При этом если последний блок входного сообщения полный, то к нему предварительно операцией XOR прибавляется ключ K1, иначе блок дополняется слева нулями и операцией XOR складывается с K2. Последний выходной блок преобразования E является имитовставкой.

*5.3 Преобразование E*

Преобразование E основывается на двукратном применении алгоритма шифрования ГОСТ 28147–89 в режиме простой замены и одной операции перестановки. Для введения зависимости от порядка следования 64–битных блоков в сообщении к каждым 64 битам прибавлять операцией XOR их порядковый номер (нумерация сквозная для всего защищаемого сообщения).

На вход E получает b–битный вектор M[i], $i = \overline{1, n}$, который разбивается на 64–битные блоки R[j], $j = \overline{1, s}$, где s = b/64, а также очередной порядковый номер 64-битного блока l и ключ K длины $256 \bullet \lceil s/8 \rceil$ бит.

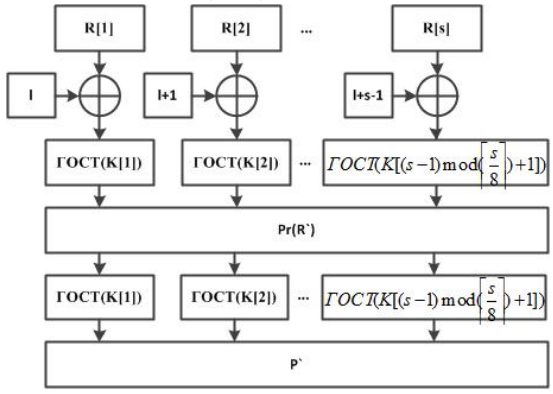


***Рис. 1.* Преобразование E**

Преобразование E представлено на рисунке 1 и состоит из следующих вычислений:

1. $R[j] = R[j] \oplus (l + j - 1)$ для $\forall j = \overline{1, s}$.
2. $R`[j] = ГОСТ(R[j], K[(j-1) \bmod(\lceil s/8 \rceil) + 1])$ для $\forall j = \overline{1, s}$, где ГОСТ – шифрование по алгоритму ГОСТ 28147-89 в режиме простой замены.
3. $P = \Pr(R`)$, где $R` = R`[1] \| ... \| R`[s]$, Pr – перестановка, описанная в п. 5.4.
4. $P`[j] = ГОСТ(P[j], K[(j-1) \bmod(\lceil s/8 \rceil) + 1])$ для $\forall j = \overline{1, s}$, где $P = P[1] \| ... \| P[s]$.

*5.4 Перестановка Pr*

На вход Pr поступает вектор R длины b бит, каждые 64 бита которого разбиваются на s фрагментов. Если $64 \vdots s$, то длина каждого фрагмента равна 64/s, иначе каждый 64 битный блок разбивается на s-1 фрагментов длины $\lfloor 64/s \rfloor$ бит и один неполный фрагмент длины $64-(s-1)\bullet\lfloor 64/s \rfloor$ бит. Далее к полученной последовательности $r_{1,1}, r_{1,2}, ..., r_{1,s}, r_{2,1}, r_{2,2}, ..., r_{2,s}, ..., r_{s,1}, r_{s,2}, ..., r_{s,s}$ применяется перестановка, как показано на рис. 2, по соотношению: $r'_{i,j} = r_{(i+j-2) \bmod s+1, j}$ для $\forall i, j = \overline{1,s}$. В результате получаем последовательность 64-битных блоков, каждый из которых зависит от каждого 64-битного блока, полученного на вход Pr.

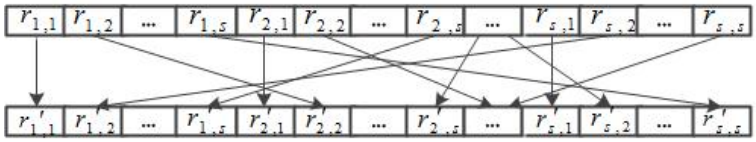

***Рис. 2.*** **Перестановка Pr**

# ОБЕСПЕЧЕНИЕ СТАНДАРТИЗАЦИИ БИЗНЕС ПРОЦЕССОВ ОБРАБОТКИ ДАННЫХ В ИНФОРМАЦИОННЫХ СИСТЕМАХ И ВНЕДРЕНИЕ ПОЛИТИКИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

***Михаил НИЩИЙ,***
*Эксперт (Республика Молдова)*

*The purpose of this article is to discuss practical aspects of possible directions for standardization of data processing and business processes based on international standards ISO 27001, ISO 9001 and ITIL library in terms of improving information security systems.*

Целью настоящей статьи является обсуждение практических аспектов разработки и внедрения системы управления информационной безопасностью в организации, предоставляющей социальные услуги населению.

Внедрение политики ИБ предполагает разработку совокупности документированных правил, регламентов, процедур, инструкций или руководящих принципов в области информационной безопасности, которыми должны руководствоваться сотрудники организации в своей повседневной деятельности. При этом, как правило, основное внимание уделяется требованиям и рекомендациям соответствующей международной и внутригосударственной нормативно-методической базы в области защиты информации. Особое значение этот факт имеет , когда организация внедряет