УДК 004.056.5

ЭЛЕМЕНТЫ МЕТОДИКИ ЗАЩИТЫ ДАННЫХ В АВТОМАТИЗИРОВАННЫХ СИСТЕМАХ

***Сергей Владимирович Савин**, адъюнкт штатной очной адъюнктуры,*
E-mail: seva_xtime@mail.ru,
***Олег Анатольевич Финько**, д-р техн. наук, профессор кафедры,*
E-mail: ofinko@yandex.ru, www.ofinko.ru,
Военная академия связи (филиал, г. Краснодар),
http://www.shtemenko.ru

Разработаны и обоснованы элементы методики защиты данных на основе метода «однократной записи» с использованием средств электронной подписи и операции конкатенации двоичных векторов. Методика может быть использована для защиты (обеспечения целостности) данных в автоматизированных системах.

Ключевые слова: защита информации, автоматизированные системы, электронная подпись, конкатенация, метод «однократной записи».

Введение


С.В. Савин


О.А. Финько

Известно, что обеспечение целостности данных является одной из сложных задач защиты информации (ЗИ) в автоматизированных системах (АС) [1]. Наиболее распространенными методами обеспечения целостности данных являются криптографические, в частности электронная подпись (ЭП), которая позволяет установить авторство и целостность электронного документа. Однако в качестве злоумышленника может выступать и лицо являющееся владельцем ключа ЭП (уполномоченный пользователь). Это вносит определенные трудности для традиционного использования средств ЭП.

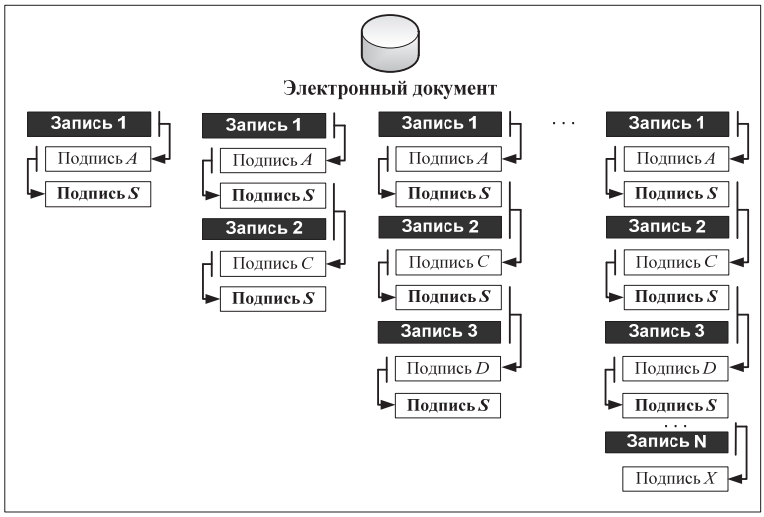

Рисунок 1 – Метод «однократной записи» для защиты электронного документа

Основная часть

Для защиты данных в АС предлагается использовать метод «однократной записи» [2], который заключается в применении различных способов обнаружения любых изменений (нарушение целостности) в документе (запись не может быть заменена, вместо этого, в документе добавляется новая запись для исправления) (рисунок 1).

В разработанных алгоритмах [3] на основе метода «однократной записи» и средств ЭП не определены следующие параметры:

- вложенность ЭП в блоке данных;
- цикличность в блоке данных;

- количество ЭП.

Таким образом, для усовершенствования методики и обеспечения необходимого уровня защищенности АС необходимо выразить данные параметры через соответствующие арифметические выражения (рисунок 2).

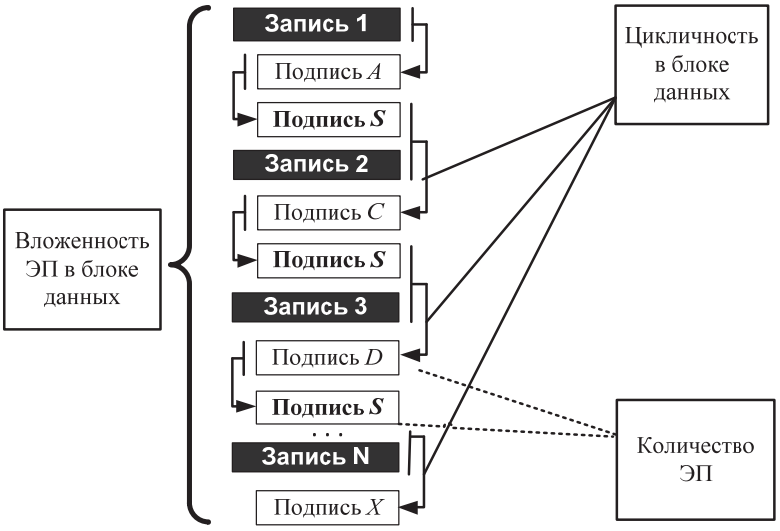

Рисунок 2 − Параметры метода «однократной записи»

Для обеспечения целостности данных с одной зависимой ЭП в качестве аргумента хэш-функции используем результат конкатенации двух двоичных векторов:

$$\vec{R}^{(k-1)}_{t_{i+k-1},\,d_i} = \vec{m}_{t_{i+k-1}} \,||\, \vec{s}_{t_{i+k-1},\,d_i},$$

где $\vec{m}_{t_{i+k}}$ – двоичный вектор произвольной конечной длины (запись в блоке данных), соответствующий моменту времени t_{i+k};

$\vec{s}_{t_{i+k},\,d_i}$ – ЭП под записью;

d_i – ключ ЭП.

Тогда ЭП $\vec{s}_{t_{i+k},\,d_i}$ для элементов множества $M_\varepsilon^* = \left\{\vec{m}_{t_i}, \vec{m}_{t_{i+1}}, \vec{m}_{t_{i+2}}, \ldots, \vec{m}_{t_{i+k}}\right\}$ (множество записей в блоке данных):

$$\vec{s}_{t_{i+k},\,d_i} \to E_{d_i} : h\left(\vec{m}_{t_{i+k}} \,||\, \vec{R}^{(k-1)}_{t_{i+k-1},\,d_i}\right).$$

Схема получения подписанной записи включает одну операцию вычисления сигнатуры ЭП и две операции конкатенации двоичных векторов (рисунок 3).

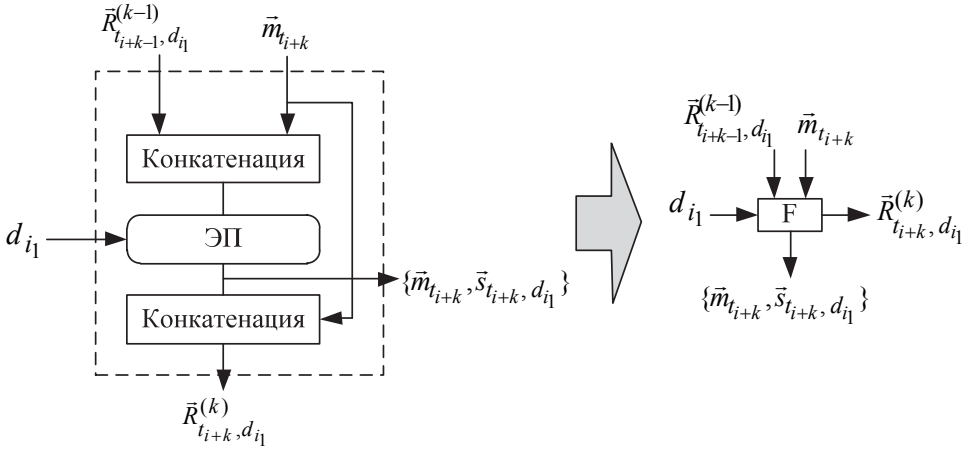

Рисунок 3 − Схема получения подписанной записи в блоке данных

Соответственно, F – цикл получения сигнатуры для одной ЭП $\vec{s}_{t_{i+k-1},d_{i_1}}$. Тогда, схема обеспечения целостности данных при переходе к обозначению блоков из F (рисунок 4).

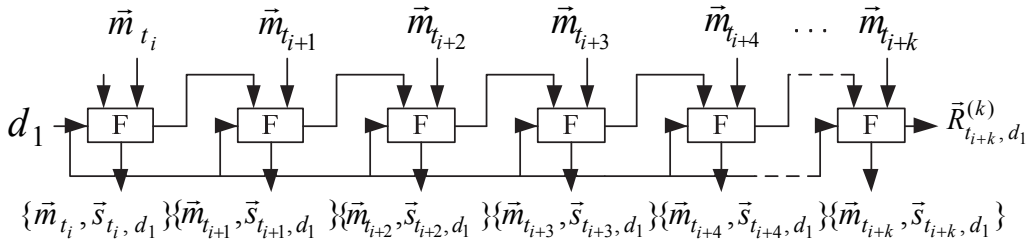

Рисунок 4 − Схема получения блока данных с одной зависимой ЭП

Таким образом, используем следующее выражение для определения параметров в методе «однократной записи»:

$$\vec{R}^{(k-(s_1,s_2,..,s_h))}_{t_{i+k-1},d_i} = \vec{m}_{t_{i+k-(s_1,s_2,..,s_h)}} \| \vec{s}_{t_{i+k-(s_1,s_2,..,s_h)},d_i}\ , \qquad (1)$$

где $(s_1, s_2, .., s_h)$ – коэффициенты, определяющие вложенность ЭП – k, цикличность в блоке данных – h, количество ЭП – d_i.

Вывод

Таким образом, в отличие от [2, 3] в статье представлены новые элементы методики защиты данных в АС на основе метода «однократной записи». Разработано и обосновано соответствующее выражение (1), коэффициенты которого могут быть как статичные (не изменяются во времени), так и динамичные (изменяются по соответствующему алгоритму), что позволяет обеспечить защиту данных в АС.

Литература

1. *Шаньгин В.Ф.* Защита компьютерной информации / В.Ф. Шаньгин. М.: ДМК Пресс, 2010. 542 с.: ил.

2. *Atsushi Harada, Masakatsu Nishigaki, Masakazu Soga, Akio Takubo, Itsukazu Nakamura*, A Write-Once Data Management System, ICITA2002 ISBN: 1-86467-114-9. Shizuoka University, 3-5-1 Johoku, Hamamatsu, 432-8011, Japan, 2001.

3. *Савин С.В.* Алгоритмы защиты данных подсистемы регистрации и учета АС с использованием метода однократной записи / сб. матер. Шестой международной научной конференции «Технические и технологические системы (ТТС – 14)». Краснодар: ФВУНЦ ВВС ВВА, 2014. С. 310–315.

The elements of the methodology of data Protection in automated system

Sergey Vladimirovich Savin, *Professor, Associate postgraduate full-time, Branch of the Military Academy of Communications (Krasnodar).*

Oleg Anatolievich Finko*, Branch of the Military Academy of Communications (Krasnodar).*

Develop and prove the elements of the methodology of data protection on the basis of «write-once» with the use of electronic signatures and the concatenation of binary vectors. The technique may be used to protect (integrity) of the data in automated systems.

Keywords: *information protection, automated, electronic signature, concatenation, the method of «write once».*