Деундяк Владимир Михайлович – Южный федеральный университет; e-mail: vl.deundyak@gmail.com; 344090, г. Ростов-на-Дону, ул. Мильчакова, 8а; тел.: +79888929337; кафедра алгебры и дискретной математики; доцент.

Евпак Сергей Александрович – e-mail: sergej-evpak@yandex.ru; тел.: +79094142919; кафедра алгебры и дискретной математики; аспирант.

Мкртичян Вячеслав Виталиевич – e-mail: realdeal@bk.ru; тел.: 89044417791; кафедра алгебры и дискретной математики; доцент.

Deundyak Vladimir Mihailovich – Southern Federal University; e-mail: vl.deundyak@gmail.com; 8a, Milchinkova street, Rostov-on-Don, 344090, Russia; phone: +79888929337; the department of algebra and discrete mathematics; associate professor.

Yevpak Sergey Alexandrovich – e-mail: sergej-evpak@yandex.ru; phone: +79094142919; the department of algebra and discrete mathematics; postgraduate student.

Mkrtichan Vyacheslav Vitalievich – e-mail: realdeal@bk.ru; phone: +79044417791; the department of algebra and discrete mathematics; associate professor.

УДК 004.056

С.В. Савин, О.А. Финько

ОБЕСПЕЧЕНИЕ ЦЕЛОСТНОСТИ ДАННЫХ ПОДСИСТЕМЫ РЕГИСТРАЦИИ И УЧЕТА АВТОМАТИЗИРОВАННЫХ СИСТЕМ НА ОСНОВЕ МЕТОДА «ОДНОКРАТНОЙ ЗАПИСИ»

Решается задача повышения защищенности хранения записей данных в подсистеме регистрации и учета системы защиты информации автоматизированной системы. Актуальность решения данной задачи заключается в необходимости защиты информации от преднамеренного воздействия со стороны легальных пользователей, которые могут скрыть следы ранее реализованных деструктивных воздействий, усиливая тем самым их вредоносный эффект или предотвращая наступление юридической ответственности за совершенные ошибочные или неправомерные действия. Предложена новая методика применения электронной подписи (или криптографической хэш-функции). При этом в общем виде реализуется известный метод так называемой «однократной записи». Однако, в отличие от известных методик, в статье предлагается структурированная методика применения электронной подписи, учитывающая такие параметры, как: глубина вложенности электронной подписи в защищаемом блоке данных (записи), количество используемых при этом криптографических ключей и порядок их использования. Порядок применения подписей – есть своеобразный ключ. Электронная подпись может быть различной – простой или усиленной (квалифицированной или неквалифицированной). Вместо подписи предусматривается применение криптографических ключевых хэш-функций. Порядок применения ключей – децентрализованный (системная подпись, подпись администратора и подписи заданного (в общем случае динамически изменяющегося) количества идентифицированных пользователей). Конкретная схема использования системы подписей может представлять собой некоторый «пространственный ключ» шифрования порядка использования упомянутых пользователей. Варьируя таким образом параметрами применения подписей и их составом, методика позволяет решать задачи защиты данных подсистемы регистрации и учета в широком диапазоне требований технического задания заказчика.

Система защиты информации; подсистема регистрации и учета; защита данных; целостность информации; метод «однократной записи»; электронная подпись.

S.V. Savin, O.A. Finko

ENSURING DATA INTEGRITY REGISTRATION AND ACCOUNTING SUBSYSTEM BASED METHOD «WRITE-ONCE»

The paper solves the problem of increasing the security of data records in storage subsystem registration and account information protection system of the automated system. Relevance of the solution of this task consists in need of information security from deliberate influence from legal users. These deliberate actions can hide traces of earlier realized destructive influences. It usilivt their harmful effect or prevents occurrence of legal responsibility for perfect wrong or illegal actions. A new method of applying an electronic signature (or cryptographic hash function). For this purpose, a well-known method of "write-once". In contrast to known methods, the article proposes a concrete application of a structured method of electronic signature, using parameters such as: the nesting depth of the electronic signature in the protected data block, the number of used cryptographic keys and how to use cryptographic keys. The procedure for using signatures – is the key. An electronic signature can be simple or reinforced (qualified or unqualified). Signature can be replaced by a cryptographic hash function. The order of application keys – decentralized (systemic signature of the signature and the specified number of users (dynamic parameter)). Schema definition of the signatures may be some "space key" encryption procedure for the use of said users. Change the settings for the application of signatures and their composition technique allows us to solve the problem of data protection subsystem registration and accounting requirements in a wide range of technical specifications of the customer.

Security system; registration and accounting subsystem; data security; data integrity; the method of «write-once»; electronic signature.

Введение. Анализ необходимости защиты данных подсистемы регистрации и учета (ПРиУч) автоматизированных систем (АС).

Эффективность защиты информации в АС зависит от совершенства системы защиты информации (СЗИ) и соответственно ее подсистем [1–4]:

- управления доступом;
- обеспечения целостности;
- криптографической;
- регистрации и учета.

Изучению первых трех подсистем в литературе уделено достаточно много внимания. И незначительное место занимает ПРиУч. В то же время данная подсистема является важной и может быть источником угроз безопасности информации (БИ) в АС [4–6], что обуславливает актуальность исследования путей обеспечения защиты данных ПРиУч.

Основные функции ПРиУч возложены на аудит безопасности, который включает: распознавание, запись, хранение и анализ информации, связанные с обеспечением БИ в АС [7, 8].

Аудит безопасности использует для хранения данных журналы регистрации событий (ЖРС) операционной системы (ОС). Особенностью данных ПРиУч ОС является их динамичность и непрерывность. Данные обновляются за счет добавления новых записей (строк событий).

Из перечня известных угроз БИ в АС важными являются угрозы, основанные на злоупотреблении уполномоченными пользователями своими правами, которые приводят к уничтожению (модификации) отдельных областей хранения данных аудита безопасности, относящихся к действиям администратора [7–10]. Таким образом, злоумышленник, который проник в систему и получил привилегированные полномочия, может скрыть факт атаки [7, 8].

Данные аудита безопасности не подлежат защите от разглашения, следовательно, нарушение целостности этих данных являются угрозой БИ в АС.

Существующие методики и алгоритмы, затрудняющие подмену или удаление данных аудита безопасности злоумышленником, не позволяют полностью решить данную задачу при хранении их в одной системе [7, 10].

Пути решения задачи обеспечения целостности данных ПРиУч АС.

Обеспечение целостности данных является одной из сложных задач защиты информации. Известно, что для обеспечения целостности данных используются следующие методы [6, 11–16]:

- избыточного кодирования;
- хэширования, в том числе криптографического;
- электронной подписи (ЭП).

Наиболее распространенным методом обеспечения целостности данных является использование средств ЭП. При этом в качестве злоумышленника может выступать и лицо, являющееся владельцем ключа ЭП.

Другие существующие методики защиты (обеспечения целостности) данных используют методы (в скобках указаны их недостатки):

- метод «цифровых отпечатков» (большой размер базы, невысокая устойчивость к модификации);
- использование меток времени (низкая криптографическая стойкость, сложность реализации в распределенных системах);
- разграничение доступа (отсутствие криптографической стойкости);
- шифрование данных (данные ПРиУч могут не являться конфиденциальными).

Таким образом, существующие методики слабо подходят для решения задачи защиты (обеспечения целостности) данных от вредоносных действий уполномоченных пользователей.

Целью работы является повышение защищенности автоматизированных информационных систем на основе разработки методики обеспечения целостности данных в подсистемах регистрации и учета АС.

Основная часть. *Разработка методики защиты данных ПРиУч АС на основе метода «однократной записи».*

Для защиты данных ПРиУч АС предлагается использовать метод «однократной записи», суть которого заключается в применении различных способов изготовления, изменения, копирования и размножения документов, которые позволяют обнаружить любое изменение в документе (запись не может быть заменена, вместо этого в документе добавляется новая запись). В частности, известен способ [17] реализации данного метода, который поясняется с помощью рис. 1.

Однако в данном способе, основанном на методе «однократной записи» и средств ЭП, не определены следующие параметры (рис. 2):

- степень вложенности ЭП в блоке данных;
- цикличность в блоке данных;
- количество ЭП (криптографических ключей ЭП).

В соответствии с поставленной целью сформулируем задачу разработки методики защиты данных ПРиУч на основе применения метода «однократной записи». Пусть, согласно [18–20]:

- $M_\varepsilon^* = \left\{\vec{m}_{t_i}, \vec{m}_{t_{i+1}}, \vec{m}_{t_{i+2}}, \ldots, \vec{m}_{t_{i+k}}\right\}$ – множество k двоичных векторов произвольной конечной длины (множество строк событий в блоке ЖРС);
- $\vec{m}_{t_{i+k}}$ – двоичный вектор произвольной конечной длины, представляющий строку события в ЖРС, соответствующий моменту времени t_{i+k};
- d_i – ключ ЭП (закрытый);
- $\vec{S}_{t_{i+k}, d_i}$ – сигнатура ЭП под строкой события (двоичным вектором произвольной конечной длины $\vec{m}_{t_{i+k}}$);
- $\vec{s}_{t_{i+k}, d_i} \to E_{d_i} : h\left(\vec{m}_{t_{i+k}}\right)$ – вычисление сигнатуры ЭП.

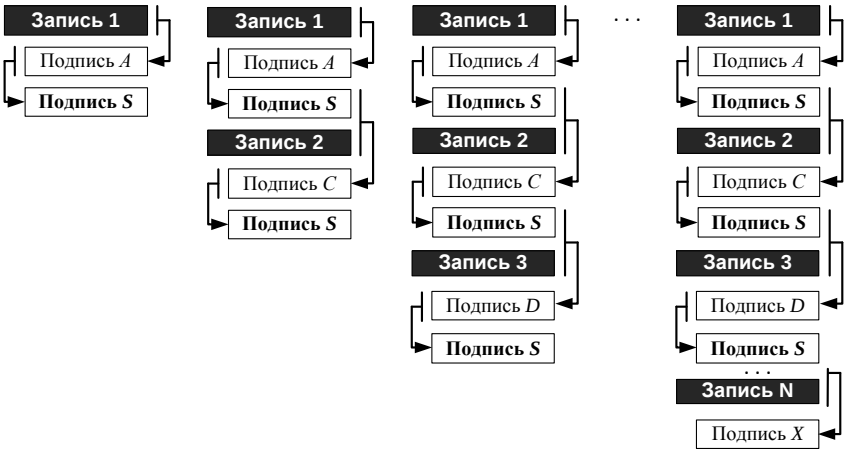

Рис. 1. Пояснение к способу «однократной записи»

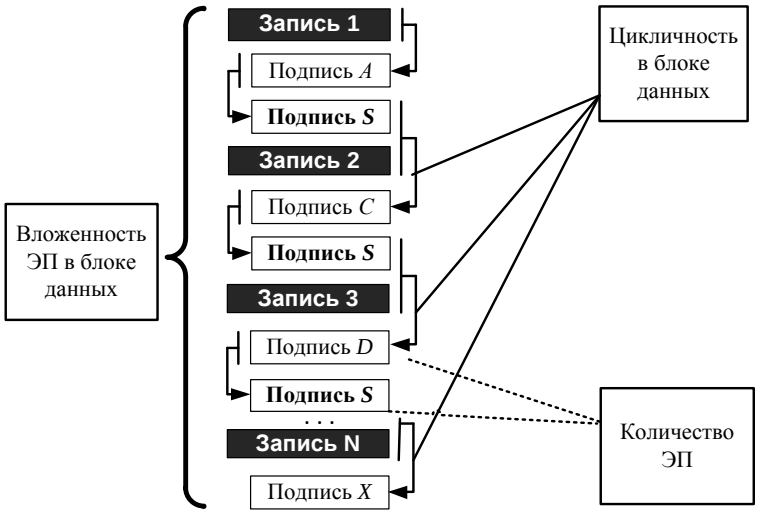

Рис. 2. Параметры способа «однократной записи»

Для обеспечения целостности данных ПРиУч 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 $||$ – символ конкатенации.

Тогда ЭП $\vec{s}_{t_{i+k},\,d_i}$ для элементов из множества M_ε^*:

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

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

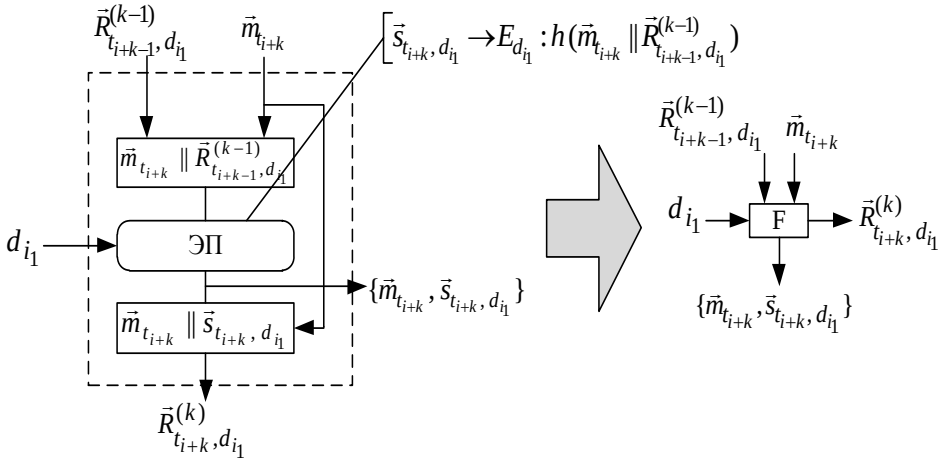

Рис. 3. Схема получения подписанной записи в блоке данных ПРиУч

Соответственно F – блок получения сигнатуры для одной ЭП $\vec{s}_{t_{i+k-1},d_{i_1}}$. Тогда схема обеспечения целостности данных ПРиУч при переходе к обозначению блоков из F может быть представлена на рис. 4.

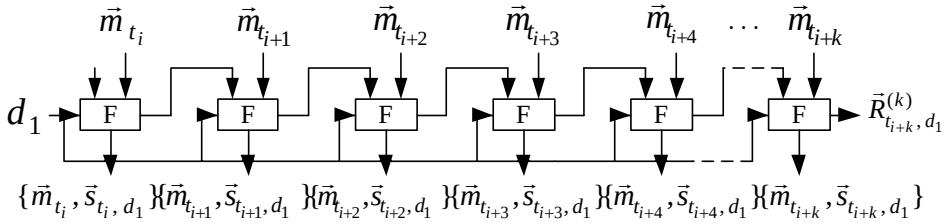

Рис. 4. Схема получения блока данных ПРиУч с одной зависимой ЭП

Таким образом, используем следующее выражение для определения вложенности ЭП, цикличности в блоке данных ПРиУч и количество используемых ЭП:

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

где $s_1, s_2, \ldots, s_h$ – коэффициенты, определяющие вложенность ЭП, h – цикличность в блоке данных, d_i – количество ЭП.

Пример: схемы получения блока данных ПРиУч с одной зависимой ЭП ($d_i=1$), соответствующие коэффициентам выражения (1): a) $s_1=1, s_2=2$; b) $s_1=2, s_2=2$; c) $s_1=1, s_2=1, s_3=2$; d) $s_1=1, s_2=1, s_3=2, s_4=1, s_5=2$, представлены на рис. 5.

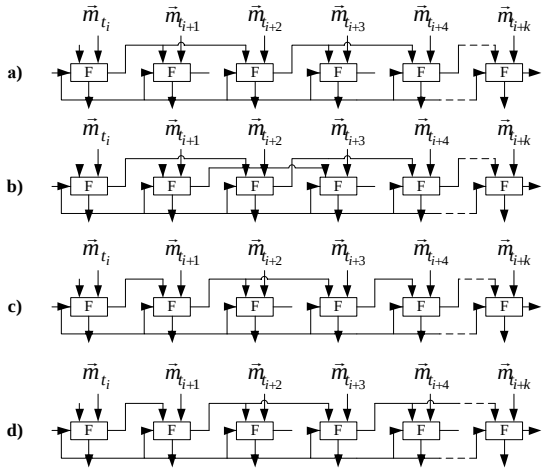

Рис. 5. Примеры схем получения блока данных ПРиУч с одной зависимой ЭП

Алгоритм обеспечения целостности данных ПРиУч с одной зависимой ЭП и конкатенацией двоичных векторов.

В данном алгоритме в качестве аргумента хэш-функции используется результат конкатенации двоичных векторов:

$$\vec{R}^{(k-1)}_{t_{i+k-1},\,d_1} = \vec{m}_{t_{i+k-1}} \,\|\, \vec{s}_{t_{i+k-1},\,d_1}.$$

ЭП $\vec{s}_{t_{i+k},\,d_1}$ для множества M_ε^*:

$$\vec{s}_{t_{i+k},\,d_1} \to E_{d_1} : h\left(\vec{m}_{t_{i+k}} \,\|\, \vec{R}^{(k-1)}_{t_{i+k-1},\,d_1}\right).$$

Тогда алгоритм для набора $\vec{s}_{t_{i+k},\,d_1}$ множества M_ε^* можно представить в виде следующих шагов:

Ввод данных: $\vec{m}_{t_{i+1}}, \vec{m}_{t_{i+2}}, \ldots, \vec{m}_{t_{i+k}}$ – множество строк событий в блоке ЖРС; d_1 – ключ ЭП; $\vec{R}^{(0)}_{t_i,\,d_1}$ – начальное заполнение блока F.

Шаг 1: Выполнить операцию конкатенации:

$$\begin{cases} \vec{m}_{t_{i+1}} \,\|\, \vec{R}^{(0)}_{t_i,\,d_1}; \\ \vec{m}_{t_{i+2}} \,\|\, \vec{R}^{(1)}_{t_{i+1},\,d_1}; \\ \ldots\ldots\ldots\ldots\ldots; \\ \vec{m}_{t_{i+k}} \,\|\, \vec{R}^{(k-1)}_{t_{i+k-1},\,d_1}. \end{cases}$$

Шаг 2: Вычислить значение ЭП:

$$\begin{cases} \vec{s}_{t_{i+1},\,d_1} \to E_{d_1} : h\left(\vec{m}_{t_{i+1}} \,\|\, \vec{R}^{(0)}_{t_i,\,d_1}\right); \\ \vec{s}_{t_{i+2},\,d_1} \to E_{d_1} : h\left(\vec{m}_{t_{i+2}} \,\|\, \vec{R}^{(1)}_{t_{i+1},\,d_1}\right); \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots; \\ \vec{s}_{t_{i+k},\,d_1} \to E_{d_1} : h\left(\vec{m}_{t_{i+k}} \,\|\, \vec{R}^{(k-1)}_{t_{i+k-1},\,d_1}\right). \end{cases}$$

Шаг 3: Выполнить операцию конкатенации:

$$\begin{cases} \vec{R}^{(1)}_{t_i, d_1} = \vec{m}_{t_{i+1}} \,\|\, \vec{s}_{t_{i+1}, d_1}; \\ \vec{R}^{(2)}_{t_i, d_1} = \vec{m}_{t_{i+2}} \,\|\, \vec{s}_{t_{i+2}, d_1}; \\ \ldots\ldots\ldots\ldots\ldots; \\ \vec{R}^{(k)}_{t_i, d_1} = \vec{m}_{t_{i+k}} \,\|\, \vec{s}_{t_{i+k}, d_1}. \end{cases}$$

Вывод результатов:

$$\begin{cases} \left\{ \vec{m}_{t_{i+1}}, \vec{s}_{t_{i+1}, d_1} \right\}; \\ \left\{ \vec{m}_{t_{i+2}}, \vec{s}_{t_{i+2}, d_1} \right\}; \\ \ldots\ldots\ldots\ldots\ldots; \\ \left\{ \vec{m}_{t_{i+k}}, \vec{s}_{t_{i+k}, d_1} \right\}. \end{cases}$$

Таким образом, рассмотренный алгоритм обеспечения целостности данных ПРиУч использует одну зависимую ЭП – $d^{(A)}_{i_1}$ и две операции конкатенации двоичных векторов (рис. 6).

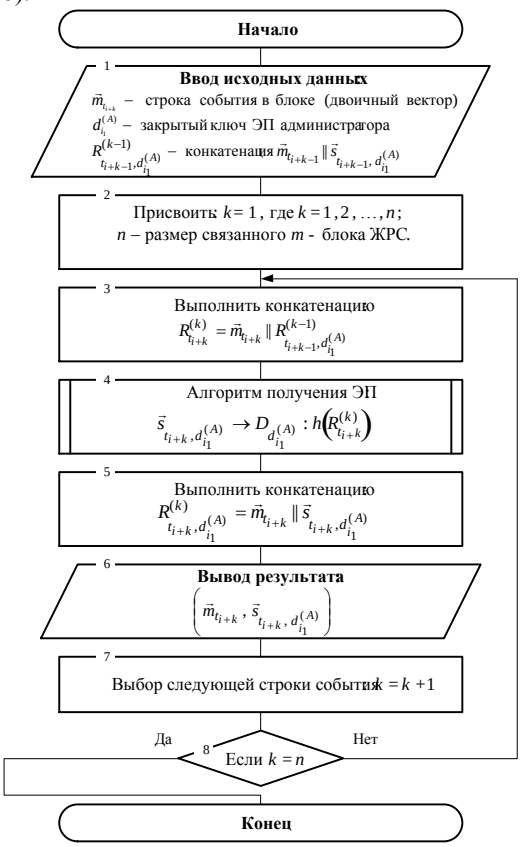

Рис. 6. Блок-схема алгоритма обеспечения целостности данных ПРиУч с одной зависимой ЭП

Алгоритм обеспечения целостности данных ПРиУч с двумя зависимыми ЭП и конкатенацией двоичных векторов.

В данном алгоритме для каждого элемента из множества M_ε^* используем две ЭП. Тогда алгоритм обеспечения целостности данных можно представить в виде следующих шагов:

Ввод данных: $\vec{m}_{t_{i+1}}, \vec{m}_{t_{i+2}}, \ldots, \vec{m}_{t_{i+k}}$ – множество строк событий в блоке ЖРС; d_1 – первый ключ ЭП; d_2 – второй ключ ЭП; $\vec{R}^{(0)}_{t_i, d_1}$ – начальное заполнение блока F.

Шаг 1: Выполнить операцию конкатенации:

$$\begin{cases} \vec{m}_{t_{i+1}} \| \vec{R}^{(0)}_{t_i, d_1, d_2}; \\ \vec{m}_{t_{i+2}} \| \vec{R}^{(1)}_{t_{i+1}, d_1, d_2}; \\ \ldots\ldots\ldots\ldots\ldots; \\ \vec{m}_{t_{i+k}} \| \vec{R}^{(k-1)}_{t_{i+k-1}, d_1, d_2}. \end{cases}$$

Шаг 2: Вычислить значение для первой ЭП:

$$\begin{cases} \vec{s}_{t_{i+1}, d_1} \to E_{d_1} : h\left(\vec{m}_{t_{i+1}} \| \vec{R}^{(0)}_{t_i, d_1, d_2}\right); \\ \vec{s}_{t_{i+2}, d_1} \to E_{d_1} : h\left(\vec{m}_{t_{i+2}} \| \vec{R}^{(1)}_{t_{i+1}, d_1, d_2}\right); \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots; \\ \vec{s}_{t_{i+k}, d_1} \to E_{d_1} : h\left(\vec{m}_{t_{i+k}} \| \vec{R}^{(k-1)}_{t_{i+k-1}, d_1, d_2}\right). \end{cases}$$

Шаг 3: Выполнить операцию конкатенации:

$$\begin{cases} \vec{m}_{t_{i+1}} \| \vec{s}_{t_{i+1}, d_1}; \\ \vec{m}_{t_{i+2}} \| \vec{s}_{t_{i+2}, d_1}; \\ \ldots\ldots\ldots\ldots; \\ \vec{m}_{t_{i+k}} \| \vec{s}_{t_{i+k}, d_1}. \end{cases}$$

Шаг 4: Вычислить значение для второй ЭП:

$$\begin{cases} \vec{s}_{t_{i+1}, d_1, d_2} \to E_{d_2} : h\left(\vec{m}_{t_{i+1}} \| \vec{s}_{t_{i+1}, d_1}\right); \\ \vec{s}_{t_{i+2}, d_1, d_2} \to E_{d_2} : h\left(\vec{m}_{t_{i+2}} \| \vec{s}_{t_{i+2}, d_1}\right); \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots; \\ \vec{s}_{t_{i+k}, d_1, d_2} \to E_{d_2} : h\left(\vec{m}_{t_{i+k}} \| \vec{s}_{t_{i+k}, d_1}\right). \end{cases}$$

Вывод результатов:

$$\begin{cases} \left\{\vec{m}_{t_{i+1}}, \vec{s}_{t_{i+1}, d_1, d_2}\right\}; \\ \left\{\vec{m}_{t_{i+2}}, \vec{s}_{t_{i+2}, d_1, d_2}\right\}; \\ \ldots\ldots\ldots\ldots\ldots; \\ \left\{\vec{m}_{t_{i+k}}, \vec{s}_{t_{i+k}, d_1, d_2}\right\}. \end{cases}$$

Таким образом, алгоритм обеспечения целостности данных ПРиУч с двумя ЭП использует две зависимые ЭП – $d_{i_1}^{(A)}$, $d_{i_1}^{(C)}$ и три операции конкатенации двоичных векторов (рис. 7).

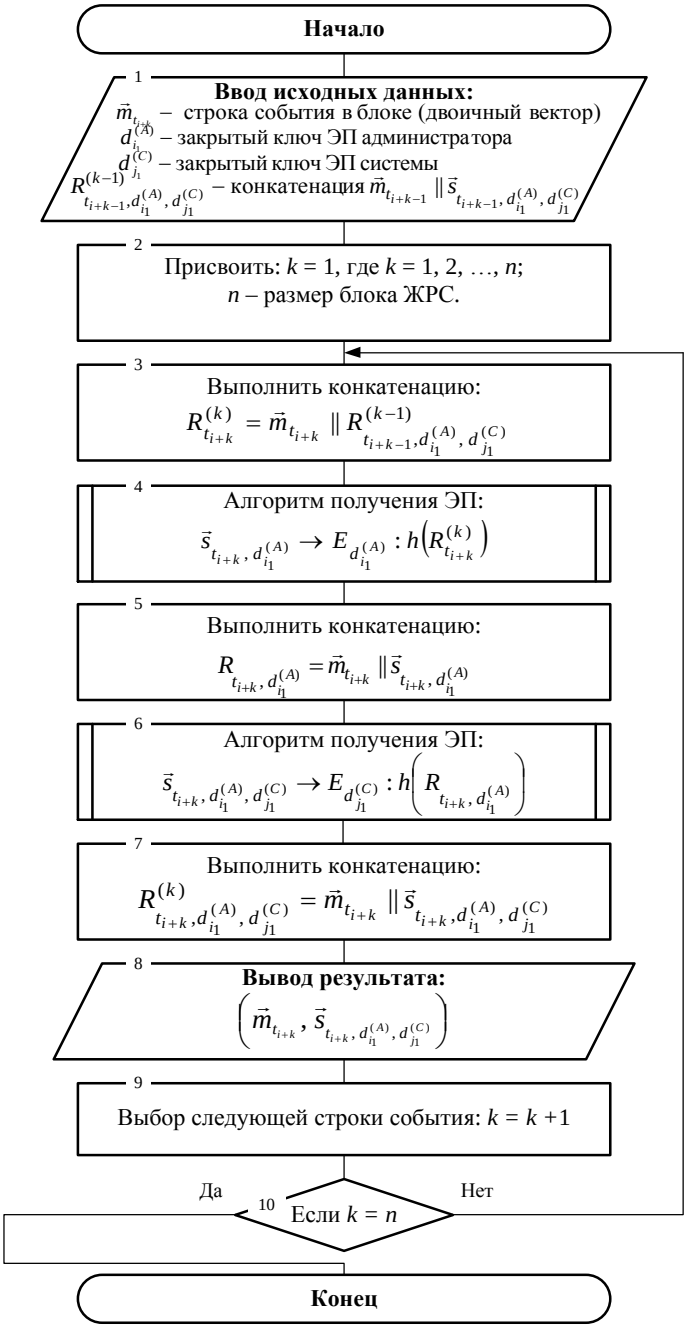

Рис. 7. Блок-схема алгоритма обеспечения целостности данных ПРиУч с двумя зависимыми ЭП

Обобщенный алгоритм обеспечения целостности данных ПРиУч с N зависимыми ЭП использует N+2 шагов для получения результата (подписанной строки события) (рис. 8).

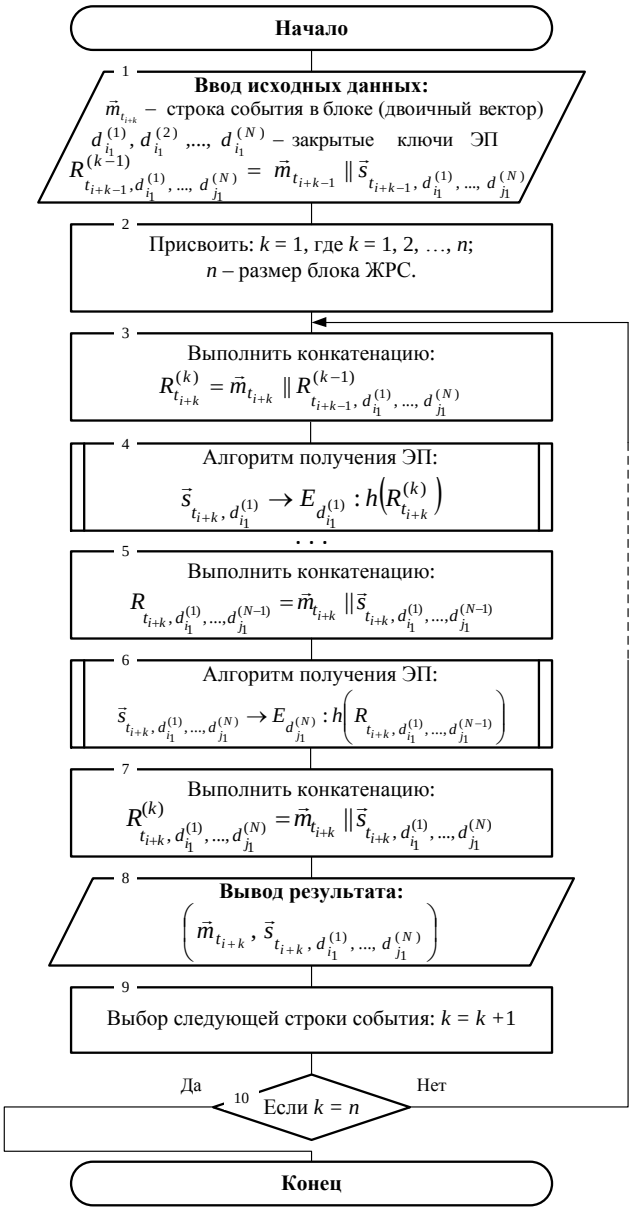

Рис. 8. Блок-схема алгоритма обеспечения целостности данных ПРиУч с N-зависимой ЭП

Для оценки разработанной методики может быть использован такой показатель, как вероятность нарушения целостности – $P_{\text{НЦ}}$, который означает изменение (удаление) одной и более записей строк в ЖРС одним или несколькими уполномоченными пользователями.

Вероятность нарушения целостности $P_{\text{НЦ}}$ как при классическом использовании средств ЭП, так и в предлагаемой методике зависит от различных совместных и независимых событий, таких как: вероятность утраты пользователем ключа ЭП (компрометация ключа ЭП), вероятность сговора уполномоченных пользователей, вероятность программно-аппаратного сбоя, вероятность нахождения пользователей на рабочих местах, и общего количества пользователей и ЭП N в АС.

Зависимости вероятностей нарушения целостности – $P_{\text{НЦ}}(n)$ для классического способа использования ЭП и разработанной методики представлены на рис. 9.

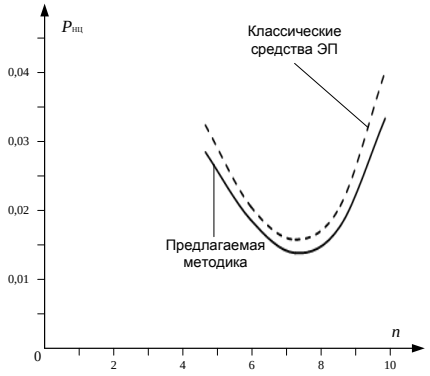

Рис 9. Вариант зависимостей вероятности нарушения целостности от количества n используемых ЭП

Выигрыш разработанной методики по сравнению с классическим использованием средств ЭП составил приблизительно 12 %, однако, так же, как и полученное оптимальное значение n носит лишь примерный характер (важно, что оптимум существует) и соответствует ряду принятых ограничений и допущений.

Заключение. В работе показано решение задачи – обеспечения целостности данных подсистемы регистрации и учета автоматизированных информационных систем на основе метода «однократной записи». Разработана структурированная методика применения ЭП, отличающаяся от известной методики [17] введением параметров:

- глубина вложенности ЭП в защищаемом блоке данных (записи), которая в общем случае может быть переменной величиной;
- количество криптографических ключей;
- порядок использования криптографических ключей.

Предлагаемая методика позволяет, путем варьирования указанными параметрами и их составом, решать задачи обеспечения целостности данных подсистем регистрации и учета автоматизированных информационных систем в широком диапазоне требований технического задания заказчика.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. ГОСТ Р 50739 – 95 (переиздан 2006). Средства вычислительной техники. Защита от несанкционированного доступа к информации. Общие технические требования. – М.: Госстандарт России, 1996.
2. Руководящий документ ГосТехКомиссии. «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации». – М.: Госстандарт России, 1992.
3. ГОСТ 50922 – 06. Защита информации. Основные термины и определения. – М.: Госстандарт России, 2006.

4. *Савин С.В*. Анализ необходимости совершенствования подсистемы регистрации и учета системы защиты информации АС ВН // Сборник трудов VI-VII Всероссийской научно-технической школы-семинар (г. Геленджик – 2013). – Краснодар: ФВАС, 2013. – Т. 1. – С. 179-182.
5. *Савин С.В*. Защищенное хранение данных аудита безопасности АС // Сборник научных трудов Шестой Международной научно-технической конференции (Инфоком – 6). – Ставрополь: Северо-Кавказский федеральный университет, 2014. – Ч. 2. – С. 480-484.
6. *Шаньгин В.Ф.* Защита компьютерной информации. – М.: ДМК Пресс, 2010. – 542 с.
7. Операционная система МС ВС 3.0. Системное администрирование. Комплект технической документации на операционную систему МСВС 3.0 ФЛИР.80001-01, 2010.
8. Midsize Business Security Guidance. Microsoft Corporation. Security Monitoring and Attack Detection // Microsoft Corporation. – August 2006. – www.microsoft.com/technet/security/midsizebusiness/default.mspx, 2006.
9. ГОСТ 53110 – 08. Система обеспечения информационной безопасности сети связи общего пользования. – М.: Госстандарт России, 2009.
10. ГОСТ Р ИСО/МЭК 15408-2 – 13. Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Ч. 2. Функциональные компоненты безопасности. – М.: Госстандарт России, 2013.
11. *Biham E., Dunkelman O.* A framework for iterative hash functions. – HAIFA, IACR ePrint 2007/278. eprint.iacr.org/2007/278, July, 2007.
12. *Mendel F., Pramstaller N., Rechberger C., Kontak M., Szmidt J.* Cryptanalysis of the GOST hash function. – CRYPTO 2008, D. Wagner, Ed., vol. 5157 of LNCS, Springer. – 2008. – P. 162-128.
13. *Toshimitsu Inomata, Susumu Itagaki, Masakazu Soga, Masakatsu Nishigaki*. A Method of Tamper-proof Using Digital Signature and Patrol, and Its Application to the WWW // Information Processing Society of Japan Journal. – 2003. – Vol. 44, No. 8. – P. 2072-2084.
14. *Bellare M.* New Proofs for NMAC and HMAC: Security without Collision-Resistance. – CRYPTO 2006, ePrint Archive, Report 2006/043. – www.eprint.iacr.org/2006/043.pdf, 2006.
15. *Jongsung Kim, Alex Biryukov, Bart Preneel1, Seokhie Hong*. On the Security of HMAC and NMAC Based on HAVAL, MD4, MD5, SHA-0 and SHA-1. – Center for Information Security Technologies(CIST), Korea University, Seoul, Korea, 2006.
16. *Wang X., Yu H.* How to Break MD5 and Other Hash Functions. EUROCRYPT 2005, LNCS 3494. – Springer-Verlag, 2005. – P. 19-35.
17. *Atsushi Harada, Masakatsu Nishigaki, Masakazu Soga, Akio Takubo, Itsukazu Nakamura*. A Write-Once Data Management System, ICITA 2002. –Shizuoka University, 3-5-1 Johoku, Hamamatsu, 432-8011, Japan, 2002.
18. ГОСТ Р 34.10 – 2012. Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи. – М.: Госстандарт России, 2012.
19. ГОСТ Р 34.11 – 2012. Информационная технология. Криптографическая защита информации. Функция хэширования. – М.: Госстандарт России, 2012.
20. Федеральный закон от 06 апреля 2011 года, № 63-ФЗ «Об электронной подписи».

REFERENCES

1. GOST R 50739 – 95 (pereizdan 2006). Sredstva vychislitel'noy tekhniki. Zashchita ot nesanktsionirovannogo dostupa k informatsii. Obshchie tekhnicheskie trebovaniya [State Standard R 50739 – 95 (reprinted 2006). Computing facilities. Protection against unauthorized access to information. General technical requirements]. Moscow: Gosstandart Rossii, 1996.
2. Rukovodyashchiy dokument GosTekhKomissii. «Avtomatizirovannye sistemy. Zashchita ot nesanktsionirovannogo dostupa k informatsii. Klassifikatsiya avtomatizirovannykh sistem i trebovaniya po zashchite informatsii» [Guidance document to gasteromycete. "Automated systems. Protection against unauthorized access to information. Classification of automated systems and requirements for information protection.]. Moscow: Gosstandart Rossii, 1992.
3. GOST 50922 – 06. Zashchita informatsii. Osnovnye terminy i opredeleniya [State Standard 50922 – 06. The protection of information. Basic terms and definitions]. Moscow: Gosstandart Rossii, 2006.

4. *Savin S.V.* Analiz neobkhodimosti sovershenstvovaniya podsistemy registratsii i ucheta sistemy zashchity informatsii AS VN [Analysis of the need to improve the registration subsystem and system accounting information protection AC HV], *Sbornik trudov VI-VII Vserossiyskoy nauchno-tekhnicheskoy shkoly – seminar* [Proceedings of the VI-VII all-Russian scientific-technical school-seminar] (g. Gelendzhik – 2013). Krasnodar: FVAS, 2013. Vol. 1, pp. 179-182.
5. *Savin S.V.* Zashchishchennoe khranenie dannykh audita bezopasnosti AS [Secure storage of audit data security AC], *Sbornik nauchnykh trudov Shestoy Mezhdunarodnoy nauchno-tekhnicheskoy konferentsii (Infokom – 6)* [Proceedings of the Sixth International scientific and technical conference (InfoCom – 6)]. Stavropol': Severo-Kavkazskiy federal'nyy universitet, 2014, Part 2, pp. 480-484.
6. *Shan'gin V.F.* Zashchita komp'yuternoy informatsii [Protection of computer information]. Moscow: DMK Press, 2010, 542 p.
7. Operatsionnaya sistema MS VS 3.0. Sistemnoe administrirovanie. Komplekt tekhnicheskoy dokumentatsii na operatsionnuyu sistemu MSVS 3.0 FLIR.80001-01, 2010 [Operating system MS SA 3.0. System administration. The technical documentation on the operating system MSVS 3.0 FLIR.80001-01, 2010].
8. Midsize Business Security Guidance. Microsoft Corporation. Security Monitoring and Attack Detection // Microsoft Corporation. August 2006. Available at: http://www.microsoft.com/technet/ security/ midsizebusiness/default.mspx, 2006.
9. GOST 53110 – 08. Sistema obespecheniya informatsionnoy bezopasnosti seti svyazi obshchego pol'zovaniya [State Standard 53110 – 08. The system of ensuring information security of the public communications network]. Moscow: Gosstandart Rossii, 2009.
10. GOST R ISO/MEK 15408-2 – 13. Informatsionnaya tekhnologiya. Metody i sredstva obespecheniya bezopasnosti. Kriterii otsenki bezopasnosti informatsionnykh tekhnologiy. Ch. 2. Funktsional'nye komponenty bezopasnosti [State Standard R ISO/IEC 15408-2 – 13. Information technology. Methods and means of security. Evaluation criteria information technology security. Part 2. Functional security components]. Moscow: Gosstandart Rossii, 2013.
11. *Biham E., Dunkelman O.* A framework for iterative hash functions. HAIFA, IACR ePrint 2007/278. eprint.iacr.org/2007/278, July, 2007.
12. *Mendel F., Pramstaller N., Rechberger C., Kontak M., Szmidt J.* Cryptanalysis of the GOST hash function. CRYPTO 2008, D. Wagner, Ed., vol. 5157 of LNCS, Springer. 2008, pp. 162-128.
13. *Toshimitsu Inomata, Susumu Itagaki, Masakazu Soga, Masakatsu Nishigaki*. A Method of Tamper-proof Using Digital Signature and Patrol, and Its Application to the WWW, *Information Processing Society of Japan Journal*, 2003, Vol. 44, No. 8, pp. 2072-2084.
14. *Bellare M.* New Proofs for NMAC and HMAC: Security without Collision-Resistance. – CRYPTO 2006, ePrint Archive, Report 2006/043. Available at: http://www.eprint.iacr.org/ 2006/043.pdf, 2006.
15. *Jongsung Kim, Alex Biryukov, Bart Preneel1, Seokhie Hong*. On the Security of HMAC and NMAC Based on HAVAL, MD4, MD5, SHA-0 and SHA-1. Center for Information Security Technologies(CIST), Korea University, Seoul, Korea, 2006.
16. *Wang X., Yu H.* How to Break MD5 and Other Hash Functions. EUROCRYPT 2005, LNCS 3494. Springer-Verlag, 2005, pp. 19-35.
17. *Atsushi Harada, Masakatsu Nishigaki, Masakazu Soga, Akio Takubo, Itsukazu Nakamura*. A Write-Once Data Management System, ICITA 2002. Shizuoka University, 3-5-1 Johoku, Hamamatsu, 432-8011, Japan, 2002.
18. GOST R 34.10 – 2012. Informatsionnaya tekhnologiya. Kriptograficheskaya zashchita informatsii. Protsessy formirovaniya i proverki elektronnoy tsifrovoy podpisi [State Standard R 34.10 – 2012. Information technology. Cryptographic protection of information. The processes of formation and verification of digital signature]. Moscow: Gos-standart Rossii, 2012.
19. GOST R 34.11 – 2012. Informatsionnaya tekhnologiya. Kriptograficheskaya zashchita informatsii. Funktsiya kheshirovaniya [State Standard R 34.11 – 2012. Information technology. Cryptographic protection of information. The hash function]. Moscow: Gosstandart Rossii, 2012.
20. Federal'nyy zakon ot 06 aprelya 2011 goda, № 63-FZ «Ob elektronnoy podpisi» [The Federal law from 06 April 2011, № 63-FZ "On electronic signature"].

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

Савин Сергей Владимирович – Филиал Военной академии связи (г. Краснодар); e-mail: seva_xtime@mail.ru; 350063, г. Краснодар, ул. Красина, 4; тел.: +79189808621; адъюнкт.

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

Savin Sergey Vladimirovich – Branch of the Military Academy of Communications (Krasnodar); e-mail: seva_xtime@mail.ru; 4, Krasina, Krasnodar, 350063, Russia; phone: +79189808621; associate postgraduate full-time.

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

УДК 621.3.037.3: 004.04

Л.К. Бабенко, Ф.Б. Буртыка, О.Б. Макаревич, А.В. Трепачева

ОБОБЩЕННАЯ МОДЕЛЬ СИСТЕМЫ КРИПТОГРАФИЧЕСКИ ЗАЩИЩЕННЫХ ВЫЧИСЛЕНИЙ*

Рассматривается проблема организации вычислений над зашифрованными данными. Эта задача в последнее время приобрела большую актуальность в связи с развитием парадигмы облачных вычислений и необходимостью обеспечения адекватных мер их защиты. Однако разнообразные примитивы работы с зашифрованными данными, такие как полностью гомоморфное шифрование, функциональное шифрование, многосторонние секретные вычисления, решают свои задачи лишь в ограниченном контексте. Тогда как построение реальной системы защищенных вычислений требует разработки некой общей теории организации защищенных вычислений, использующей системный подход. Предлагается разделить всю функциональность, которую должна поддерживать система защищенных вычислений на несколько уровней, взаимодействие между которыми осуществлялось бы через интерфейсы. Представленная шестиуровневая аналитическая модель под названием «Стек интерфейсов защищенных вычислений» («СИЗВ») призвана стандартизировать и облегчить деятельность исследователей и разработчиков в области систем криптографически защищенных вычислений, т.е. таких систем, в которых обработка конфиденциальных данных ведется недоверенной стороной и, следовательно, ни на одном из этапов обработки информация не может быть расшифрована. Для каждого из уровней очерчивается проблематика, с которой исследователи имеют дело, раскрывается круг вопросов, которые должны быть решены, а также дается краткий обзор работ по данной тематике. Самый верхний уровень является самым абстрактным и предоставляет свой интерфейс прикладному программисту, затем идут два уровня, имеющие дело с внутренним представлением программ, далее – уровень, предназначенный для анализа и синтеза архитектуры виртуальной машины, уровень работы с криптографическими схемами и протоколами и, наконец, уровень аппаратной реализации элементарных операций. Необходимым условием функционирования системы криптографически защищенных вычислений является проработка и реализация в полной мере каждого из этих уровней.

Полностью гомоморфное шифрование; функциональное шифрование; многосторонние секретные вычисления; системы защищенных вычислений; аналитическая модель; защищённые облачные вычисления.

L.K. Babenko, Ph.B. Burtyka, O.B. Makarevich, A.V. Trepacheva

A GENERAL MODEL OF CRYPTOGRAPHICALLY SECURE COMPUTING SYSTEM

The paper deals with the problem of organization the computations over encrypted data. Recently this problem has become increasingly important due to the extension of the cloud computing paradigm and the need for adequate measures to protect them. However, a number of primitives for working with encrypted data, such as a fully homomorphic encryption, functional encryp-

* Работа выполнена при финансовой поддержке РФФИ в рамках научного проекта №15-07-00597 а.