КРИПТОГРАФИЧЕСКИЙ РЕКУРСИВНЫЙ КОНТРОЛЬ ЦЕЛОСТНОСТИ МЕТАДАННЫХ ЭЛЕКТРОННЫХ ДОКУМЕНТОВ. ЧАСТЬ 2. КОМПЛЕКС АЛГОРИТМОВ

Тали Д.И.[1], Финько О.А.[2]

От редакции: *авторы представили в редакцию нашего журнала объемное исследование, которое в силу размера не может быть опубликовано в одном номере. Редакция предложила авторам разбить полное исследование на четыре законченные части. Данная публикация является второй из четырех, следующие будут опубликованы в ВК-1-2021 и ВК-2-2021.*

Целью исследования *является разработка комплекса алгоритмов для повышения уровня защищенности метаданных электронных документов в условиях деструктивных воздействий уполномоченных пользователей (инсайдеров).*

Методы исследования: *принципы технологии цепной записи данных, методы теории алгоритмов, теоретические положения построения автоматизированных информационных систем юридически значимого электронного документооборота.*

Результат исследования: *разработан комплекс алгоритмов криптографического рекурсивного 2-D контроля целостности метаданных электронных документов. Его особенностью являются следующие возможности:*

1) *локализация модифицированных (с признаками нарушения целостности) записей метаданных электронных документов;*
2) *выявление уполномоченных пользователей (инсайдеров), осуществивших несанкционированные модификации метаданных электронных документов;*
3) *выявление факта сговора доверенных сторон за счет введения взаимного контроля результатов их действий.*

Предложенное решение позволяет реализовать функции криптографического рекурсивного двумерного контроля целостности метаданных электронных документов. При этом использование технологии цепной записи данных, в основе представленного решения, обусловлено особенностями функционирования ведомственных автоматизированных информационных систем.

Статья является продолжением работы, опубликованной в предыдущем номере журнала.

Ключевые слова: *автоматизированные информационные системы, электронный документооборот, управление метаданными, инсайдер, цепная запись данных, динамический реестр, хэш-функция, электронная подпись.*

DOI: 10.21681/2311-3456-2020-06-32-47

Введение

Метаданные являются важным звеном в управлении электронными документами (ЭлД), обрабатываемыми автоматизированными информационными системами электронного документооборота (АИС ЭД)[3], в связи с чем они подлежат защите от возможных деструктивных действий внутренних нарушителей (уполномоченных пользователей), что особенно характерно для замкнутых АИС ЭД ведомственного назначения [1-5].

1 Тали Дмитрий Иосифович, адъюнкт 21 кафедры (тактико-специальной связи) Краснодарского высшего военного орденов Жукова и Октябрьской Революции Краснознаменного училища имени генерала армии С.М. Штеменко, г. Краснодар, Россия. E-mail: dimatali@mail.ru

2 Финько Олег Анатольевич, доктор технических наук, профессор, профессор 22 кафедры (техники специальной связи) Краснодарского высшего военного орденов Жукова и Октябрьской Революции Краснознаменного училища имени генерала армии С.М. Штеменко, профессор кафедры информационной безопасности автоматизированных систем Северо-Кавказского федерального университета; академический советник Российской академии ракетных и артиллерийских наук (РАРАН), г. Краснодар, Россия. E-mail: ofinko@yandex.ru. Web: http://www.mathnet.ru/person40004.

3 ГОСТ Р ИСО 15489-1-2019 Система стандартов по информации, библиотечному и издательскому делу. Управление документами. Часть 1. Понятия и принципы. М.: Стандартинформ, 2019. 23 с.

В [1] была предложена математическая модель криптографического рекурсивного 2-D контроля целостности метаданных ЭлД. В данной статье представлен соответствующий комплекс алгоритмов, реализующий функции ранее предложенной математической модели на алгоритмическом и программном уровне.

Комплекс алгоритмов криптографического рекурсивного 2-D контроля целостности метаданных

Предлагаемый комплекс алгоритмов имеет иерархическую структуру и строится на основе взаимосвязанных компонент различного уровня [6].

Комплекс алгоритмов относится *к области обеспечения безопасности информации*, обрабатываемой АИС ЭД, и может найти применение в ведомственных системах электронного документооборота в целях контроля целостности, обрабатываемых данных, в условиях преднамеренных и непреднамеренных воздействий уполномоченных пользователей (инсайдеров).

Недостатками известных алгоритмов являются:

- отсутствие функциональной возможности установления дополнительных параметров ввода ключевых данных различных пользователей и порядка их применения (секретных для самих пользователей или для различных групп пользователей, состав которых самим пользователям не известен), позволяющих обеспечить соответствующий уровень защищенности записей данных в файле[4];
- низкий уровень защищенности данных от атак со стороны уполномоченных пользователей (необходимо наличие двух доверяющих друг другу сторон, конфиденциальность секретных ключей)[5];
- отсутствие возможности локализации записей данных с признаками нарушения целостности [7].

Разработанный комплекс алгоритмов состоит из двух частей, которые в свою очередь включают в себя по две блок-схемы (формирование и проверка криптографической рекурсивной 2-D последовательности метаданных ЭлД). *Основным предназначением комплекса является* обеспечение функциональной возможности выявления факта несанкционированного внесения изменений в метаданные ЭлД уполномоченными пользователями. При этом, за счет использования множества ключей $\mathbf{K}_U$, обеспечивается функциональная возможность выявления уполномоченных пользователей, внесших несанкционированные изменения в метаданные [8].

Содержательная постановка задачи

В соответствии со стандартом по управлению документами, ЭлД состоят из контента и метаданных, которые описывают контекст, контент и структуру документов, а также управление ими в течение времени. Метаданные являются критически важной информацией, циркулирующей в АИС ЭД и непосредственно влияющей на ее функциональные возможности, что обуславливает необходимость принятия адекватных мер по их защите от возможных несанкционированных изменений [1, 2, 8, 9].

В настоящее время защиту ЭлД, обрабатываемых АИС ЭД, обеспечивает подсистема защиты информации. Информация при этом хранится в локальной базе данных, защищаемой посредством разграничения доступа, а защита контента ЭлД, кроме того, обеспечивается средствами электронной подписи. Оказывать влияние на контент ЭлД может только автор, а на метаданные ЭлД – все, кто исполняет функции агента[6], что не исключает возможности внутренних нарушений установленной политики безопасности, выражающееся в нарушении функций управления документами [1, 2].

Именно применение электронной подписи, основанной на криптографических методах, позволяет обеспечить требуемый уровень доверия к ЭлД и, как следствие, его правовой статус [10].

Таким образом, возникает ряд *противоречий*:

- между результативностью защиты метаданных ЭлД криптографическими методами и существующими механизмами защиты (разграничения доступа) в условиях реализации уполномоченными пользователями (инсайдерами) деструктивных воздействий на АИС ЭД;
- между необходимостью реализации алгоритмов криптографической защиты метаданных, поскольку они должны быть защищены от утраты или несанкционированного удаления и сохранены либо уничтожены (как и сам ЭлД) в соответствии с установленными требованиями, и отсутствием таких алгоритмов в существующем научно-методическом аппарате защиты метаданных ЭлД.

Ограничения и допущения:

- средства защиты информации, функционирующие в АИС ЭД, могут иметь уязвимости, что способствует их использованию внутренним нарушителем в своих целях;
- внутренним нарушителем является администратор или уполномоченный пользователь, как в результате умышленных действий, так и вследствие ошибок, вызванных человеческим фактором;
- угрозы целостности метаданным могут быть реализованы, как самим внутренним нарушителем, так и через внедрение им вредоносного программного обеспечения.

В качестве *показателя эффективности* функционирования подсистемы ЗИ АИС ЭД принята вероятность нарушения целостности ЭлД $P_{(0)}$, вызванная посредством деструктивных воздействий уполномоченных пользователей на метаданные ЭлД. При этом наибольшая эффективность достигается при условии:

$$P_{(0)} < P_{\text{порог.}},$$

4 Atsushi Harada, Masakatsu Nishigaki, Masakazu Soga, Akio Takubo, Itsukazu Nakamura. A Write-Once Data Management System – ICITA 2002. Shizuoka University, Johoku, Hamamatsu, 432-8011, Japan, 2002.

5 Bellare M. New Proofs for NMAC and HMAC: Security without Collision-Resistance. CRYPTO. ePrint Archive, Report 2006/043. 2006, pp.116.

6 ГОСТ Р ИСО 23081-1-2008 Система стандартов по информации, библиотечному и издательскому делу. Процессы управления документами. Метаданные для документов. Часть 1. Принципы.– М.: Стандартинформ, 2009. – 23 с.

где $P_{\text{порог.}}$ задается требованиями тактико-технического задания заказчика [1].

Для выполнения основной задачи комплекса разрабатываемых алгоритмов, по выявлению факта несанкционированного внесения изменений в метаданные ЭлД уполномоченными пользователями (локализации модифицированных записей метаданных), реализуются следующие операции по формированию (рис. 1а, 1б) и проверке криптографической рекурсивной 2-D последовательности метаданных ЭлД (рис. 2а, 2б).

Алгоритм формирования криптографической рекурсивной 2-D последовательности метаданных

Шаг 1. Ввод исходных данных:
$z_{11}, \ldots, z_{1i_{\max}}$ – метаданные ЭлД;

k – закрытый ключ.

Шаг 2. Формирование первой строки записей метаданных, сигнатура которой задается как $H_0^{(k)} = \varnothing$, сигнатуры записей метаданных первой строки $h_{\text{зап.}0i}^{(k)} = \varnothing$ соответственно, где $i = 1, \ldots, i_{\max}$. Маркер обработки первой строки FirstString установить в значение 1.

Шаг 3. Выполнение проверки условия передачи ЭлД в архив (ЭлД не востребован). Если условие выполняется, то производится завершение алгоритма. Если условие не выполняется, то осуществляется переход к шагу 4.

Шаг 4. Выполнение мониторинга записей метаданных на наличие изменений.

Шаг 5. Выполнение проверки условия внесения изменений в записи метаданных. Если условие выполняется, то осуществляется переход к шагу 8. Если условие не выполняется, то осуществляется переход к шагу 6.

Шаг 6. Выполнение проверки условия FirstString = 1. Если условие выполняется, то осуществляется переход к шагу 7. Если условие не выполняется, то осуществляется переход к шагу 3, вышеописанные действия повторяются.

Шаг 7. Присвоение строке записей метаданных значения $S_{\text{стр.}} := \varnothing$, установка маркера FirstString в значение 0, установка счетчика количества имеющихся строк записей метаданных $j := 1$. Переход к шагу 10.

Шаг 8. Изменение значения счетчика количества имеющихся строк записей метаданных, в случае их изменения $(j := j + 1)$. Формирование новой строки записей метаданных $z_{j1}, \ldots, z_{ji_{\max}}$, содержащих внесенные изменения.

Шаг 9. Сохранение записей метаданных $z_{j1}, \ldots, z_{ji_{\max}}$, измененных в момент времени t_j.

Шаг 10. Осуществление цикла вычислений сигнатур для элементов j-й строки, где $i = 1, \ldots, i_{\max}$. По окончанию цикла вычислений выполняется переход к шагу 15.

Шаг 11. Конкатенация i-х метаданных j-й строки: $S_{\text{стр.}} := S_{\text{стр.}} \| z_{ji}$.

Шаг 12. Конкатенация метаданных и сигнатур записей метаданных предыдущей строки:
$S_{\text{зап.}} := z_{ji} \| h_{\text{зап.}(j-1)i}^{(k)}$.

Шаг 13. Вычисление сигнатуры записей метаданных j-й строки: $h_{\text{зап.}ji}^{(k)} = f\left(S_{\text{зап.}}, k\right)$.

Шаг 14 (вывод). Формирование сигнатур записей метаданных j-й строки $h_{\text{зап.}j1}^{(k)}, \ldots, h_{\text{зап.}ji_{\max}}^{(k)}$. Переход к шагу 10 (цикл операций повторяется для вычисления последующих сигнатур записей метаданных j-й строки).

Шаг 15. Конкатенация всех метаданных j-й строки и соответствующих сигнатур предыдущей строки: $S_{\text{стр.}} := S_{\text{стр.}} \| H_{j-1}^{(k)}$.

Шаг 16. Вычисление сигнатур j-х строк: $H_j^{(k)} = f\left(S_{\text{стр.}}, k\right)$.

Шаг 17 (вывод). Формирование сигнатур метаданных j-х строк $H_1^{(k)}, \ldots, H_{j_{\max}}^{(k)}$. Переход к шагу 3 (операции повторяются до тех, пор пока ЭлД востребован).

Алгоритм проверки криптографической рекурсивной 2-D последовательности метаданных

Шаг 1. Ввод исходных данных:
$z_{11}, \ldots, z_{j_{\max}i_{\max}}$ – метаданные ЭлД;
k – закрытый ключ;

$h_{\text{зап.}11}^{(k)}, \ldots, h_{\text{зап.}j_{\max}i_{\max}}^{(k)}$ – сигнатуры записей метаданных;

$H_1^{(k)}, \ldots, H_{j_{\max}}^{(k)}$ – сигнатуры строк записей метаданных.

Шаг 2. Извлечение из таблицы данных:
записей метаданных $z_{11}^*, \ldots, z_{j_{\max}i_{\max}}^* = z_{11}, \ldots, z_{j_{\max}i_{\max}}$;
сигнатур записей метаданных

$h_{\text{зап.}11}^{(k)*}, \ldots, h_{\text{зап.}j_{\max}i_{\max}}^{(k)*} = h_{\text{зап.}11}^{(k)}, \ldots, h_{\text{зап.}j_{\max}i_{\max}}^{(k)}$;

сигнатур строк записей метаданных

$H_1^{(k)*}, \ldots, H_{j_{\max}}^{(k)*} = H_1^{(k)}, \ldots, H_{j_{\max}}^{(k)}$.

Шаг 3. Присвоение сигнатурам записей метаданных нулевой строки значения $h_{\text{зап.}01}^{(k)**}, \ldots, h_{\text{зап.}0i_{\max}}^{(k)**} = \varnothing$, сигнатуре нулевой строки записей метаданных значения $H_0^{(k)**} := 0$.

Шаг 4. Осуществление цикла вычислений сигнатур для j-х строк записей метаданных, где $j = 1, \ldots, j_{\max}$. По окончанию цикла алгоритм завершается.

Шаг 5: Присвоение извлеченной строке записей метаданных значения $S_{\text{стр.}}^* := \varnothing$.

Шаг 6. Осуществление цикла вычислений сигнатур для записей метаданных j-й строки, где $i = 1, \ldots, i_{\max}$. По окончанию цикла вычислений выполняется переход к шагу 13.

Шаг 7. Конкатенация i-х метаданных j-й строки: $S_{\text{стр.}}^* := S_{\text{стр.}}^* \| z_{ji}^*$.

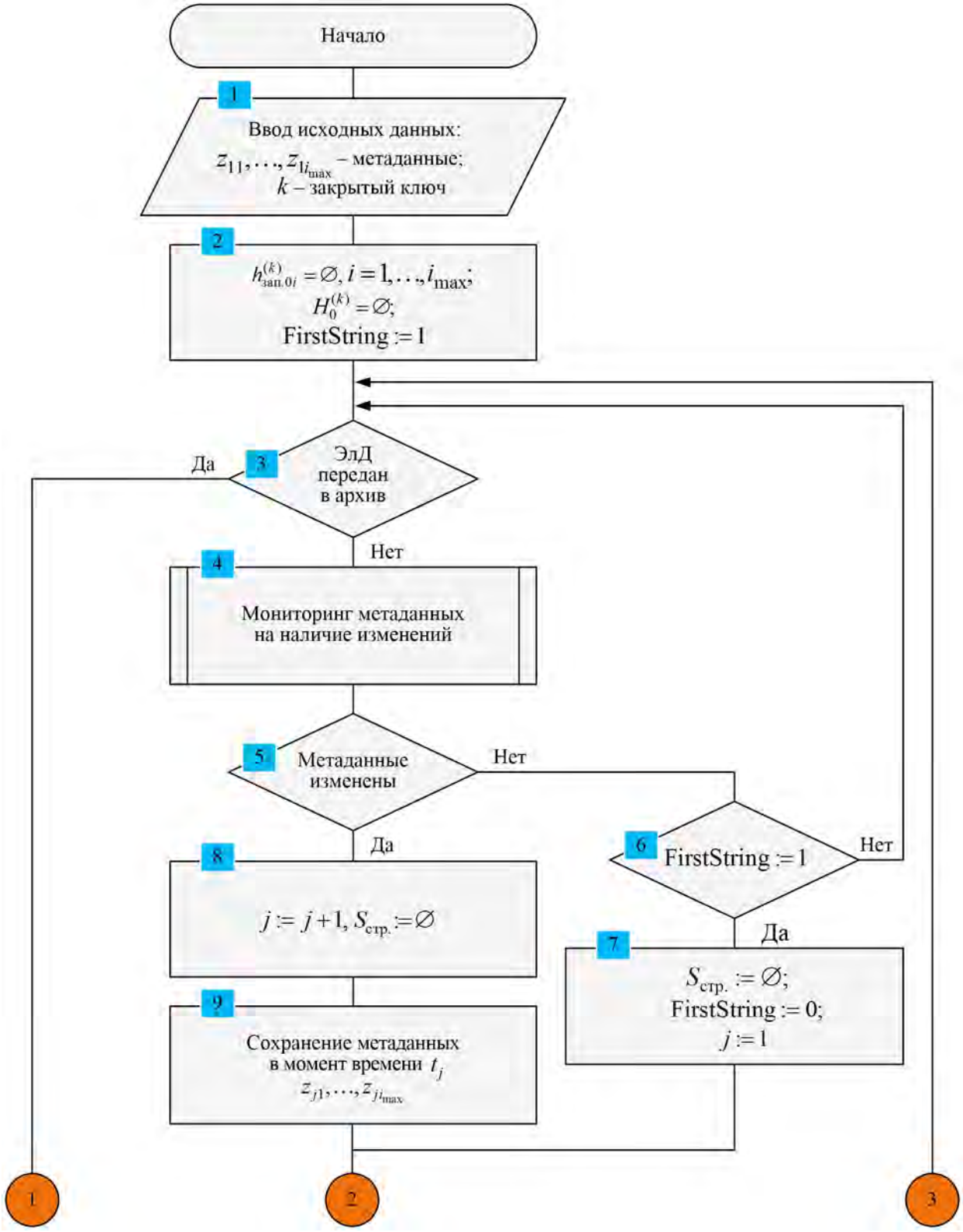

Рис. 1а. Блок-схема алгоритма формирования криптографической рекурсивной 2-D последовательности метаданных (начало)

DOI:10.21681/2311-3456-2020-06-32-47

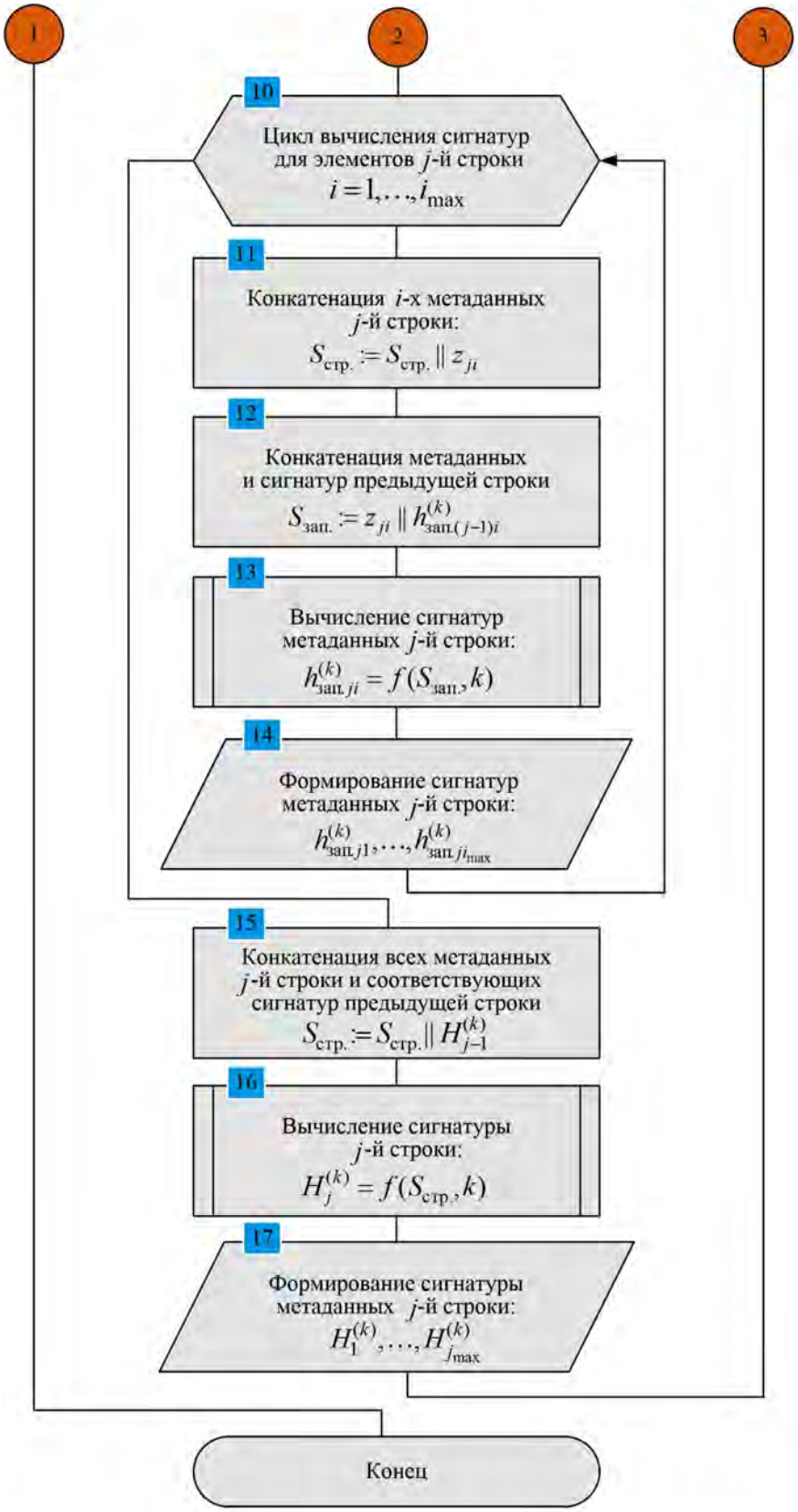

Рис. 1б. Блок-схема алгоритма формирования криптографической рекурсивной 2-D последовательности метаданных (окончание)

Шаг 8. Конкатенация метаданных и повторно вычисленных сигнатур записей метаданных предыдущей строки: $S^{*}_{\text{зап.}} := z^{*}_{ji} \,||\, h^{(k)**}_{\text{зап.}(j-1)i}$.

Шаг 9. Вычисление сигнатуры i-й записи метаданных j-й строки: $h^{(k)**}_{\text{зап.}ji} = f\left(S^{*}_{\text{зап.}},\ k\right)$.

Шаг 10. Выполнение проверки условия $h^{(k)**}_{\text{зап.}ji} = h^{(k)*}_{\text{зап.}ji}$. Если условие выполняется, то осуществляется переход к шагу 11. Если условие не выполняется, то осуществляется переход к шагу 12.

Шаг 11 (вывод). Заключение об отсутствии нарушения целостности записи z_{ji} метаданных. Переход к шагу 6 (цикл операций повторяется для вычисления последующих сигнатур записей метаданных j-й строки).

Шаг 12 (вывод). Заключение о нарушении целостности записи z_{ji} метаданных. Переход к шагу 6 (цикл операций повторяется для вычисления последующих сигнатур записей метаданных j-й строки).

Шаг 13. Конкатенация всех метаданных j-й строки и вновь вычисленных сигнатур предыдущей строки: $S^{*}_{\text{стр.}} := S^{*}_{\text{стр.}} \,||\, H^{(k)**}_{j-1}$.

Шаг 14. Вычисление сигнатуры записей метаданных j-й строки: $H^{(k)**}_{j} = f\left(S^{*}_{\text{стр.}},\ k\right)$.

Шаг 15. Выполнение проверки условия $H^{(k)**}_{j} = H^{(k)*}_{j}$. Если условие выполняется, то осуществляется переход к шагу 16. Если условие не выполняется, то осуществляется переход к шагу 17.

Шаг 16 (вывод). Заключение об отсутствии нарушения целостности записей метаданных j-й строки. Переход к шагу 4 (цикл операций повторяется для вычисления последующих сигнатур j-х строк, содержащих записи метаданных).

Шаг 17 (вывод). Заключение о нарушении целостности записей метаданных j-й строки. Переход к шагу 4 (цикл операций повторяется для вычисления последующих сигнатур j-х строк, содержащих записи метаданных).

Для решения задачи выявления нарушителей (уполномоченных пользователей), несанкционированно модифицировавших записи метаданных выполняются следующие операции по формированию (рис. 3а, 3б) и проверке (рис. 4а, 4б) криптографической рекурсивной 2-D последовательности метаданных ЭлД, с использованием ключей $\mathbf{K}_U \in \left\{\mathbf{K}^{(1)}_U, \mathbf{K}^{(2)}_U, \mathbf{K}^{(3)}_U\right\}$, где $\mathbf{K}^{(1)}_U$ – внутренние системные ключи, $\mathbf{K}^{(2)}_U$ – внешние ключи администратора системы, $\mathbf{K}^{(3)}_U$ – внешние ключи оператора системы. При этом: $\mathbf{K}^{(q)}_U \in \left\{k^{(q)}_1,\ k^{(q)}_2,\ \ldots,\ k^{(q)}_{\varsigma}\right\}$, где $q = 1,\ \ldots,\ 3$, для всех $U = 1,\ \ldots,\ \varsigma$.

Алгоритм формирования криптографической рекурсивной 2-D последовательности метаданных с использованием множества ключей $\mathbf{K}_U$

Шаг 1. Ввод исходных данных:
$z_{11},\ \ldots,\ z_{1i_{\max}}$ – метаданные ЭлД;

$\mathbf{K}_U$ – множество ключей.

Шаг 2. Формирование первой строки записей метаданных, сигнатура которой задается как $H^{(k^{(2)}_0)}_0 = \varnothing$; $H^{(k^{(3)}_0)}_0 = \varnothing$, сигнатуры записей метаданных первой строки $h^{(k^{(1)}_0)}_{\text{зап.}0i} = \varnothing$ соответственно, где $i = 1,\ \ldots,\ i_{\max}$.

Маркер обработки первой строки FirstString установить в значение 1.

Шаг 3. Выполнение проверки условия передачи электронного документа в архив (ЭлД не востребован). Если условие выполняется, то производится завершение алгоритма. Если условие не выполняется, то осуществляется переход к шагу 4.

Шаг 4. Выполнение мониторинга записей метаданных на наличие изменений.

Шаг 5. Выполнение проверки условия внесения изменений в записи метаданных. Если условие выполняется, то осуществляется переход к шагу 8. Если условие не выполняется, то осуществляется переход к шагу 6.

Шаг 6. Выполнение проверки условия FirstString = 1. Если условие выполняется, то осуществляется переход к шагу 7. Если условие не выполняется, то осуществляется переход к шагу 3, вышеописанные действия повторяются.

Шаг 7. Присвоение строке записей метаданных значения $S_{\text{стр.}} := \varnothing$, установка маркера FirstString в значение 0, установка счетчика количества имеющихся строк записей метаданных $j := 1$. Переход к шагу 11.

Шаг 8: Генерация ключей с использованием множества ключей $\mathbf{K}_U$:

$k^{(1)}_U = f_1\left(\mathbf{K}^{(1)}_U\right)$ – внутренние ключи системы;

$k^{(2)}_U = f_2\left(\mathbf{K}^{(2)}_U\right)$ – внешние ключи администратора системы;

$k^{(3)}_U = f_3\left(\mathbf{K}^{(3)}_U\right)$ – внешние ключи оператора системы, $U = 1,\ \ldots,\ \varsigma$.

Шаг 9. Изменение значения счетчика количества имеющихся строк записей метаданных, в случае их модификации $\left(j := j + 1\right)$. Формирование новой строки записей метаданных $z_{j1},\ \ldots,\ z_{ji_{\max}}$, содержащих внесенные изменения.

Шаг 10. Сохранение записей метаданных $z_{j1},\ \ldots,\ z_{ji_{\max}}$, измененных в момент времени t_j.

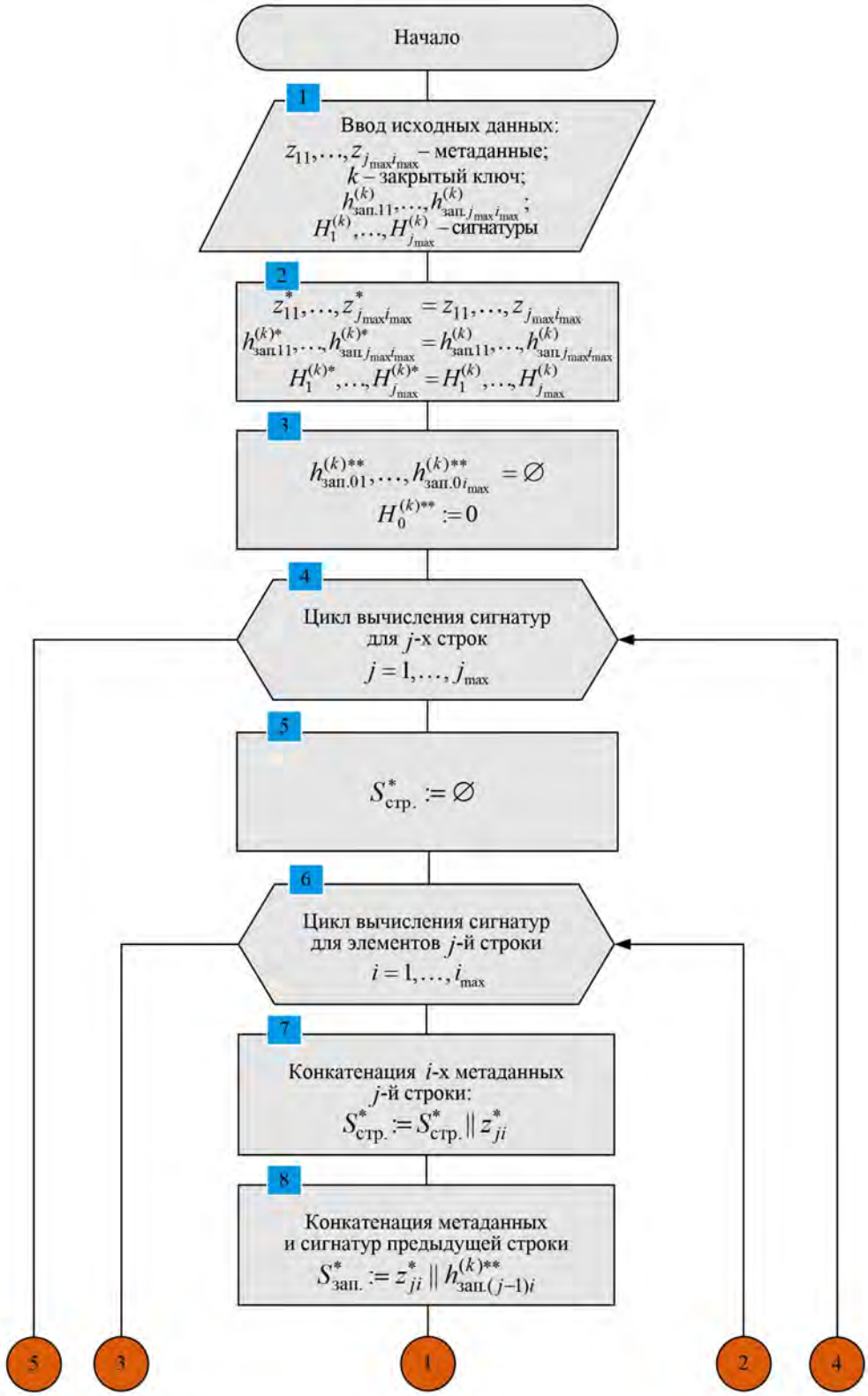

Рис. 2а. Блок-схема алгоритма проверки криптографической рекурсивной 2-D последовательности метаданных (начало)

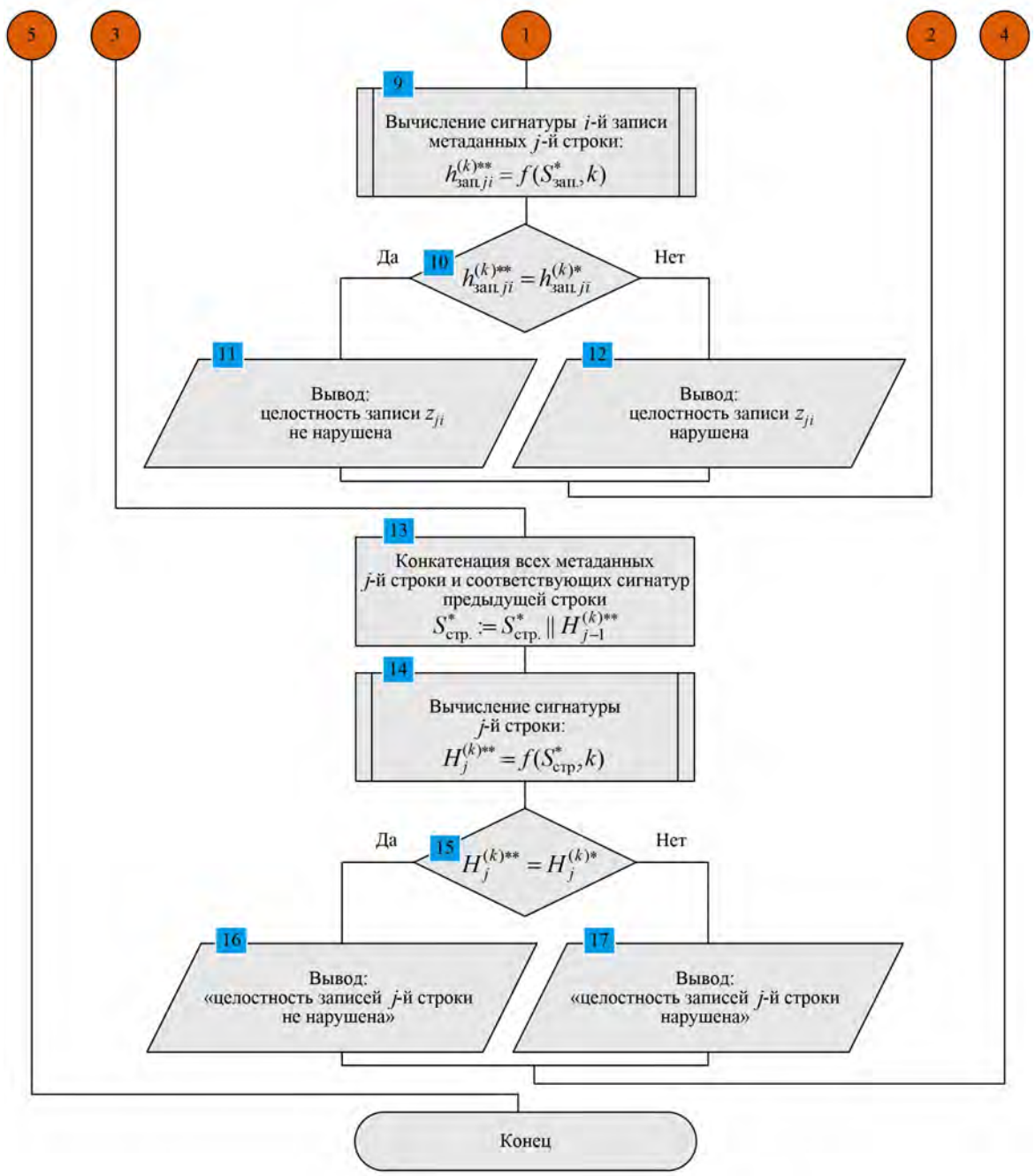

Рис. 2б. Блок-схема алгоритма проверки криптографической рекурсивной 2-D последовательности метаданных (окончание)

Шаг 11. Осуществление цикла вычислений сигнатур для элементов j-й строки, где $i = 1, \ldots, i_{\max}$. По окончанию цикла вычислений переход к шагу 16.

Шаг 12. Конкатенация i-х метаданных j-й строки: $S_{\text{стр.}} := S_{\text{стр.}} \| z_{ji}$.

Шаг 13. Конкатенация метаданных и сигнатур записей метаданных предыдущей строки:

$S_{\text{зап.}} := z_{ji} \| h^{(k_U^{(1)})}_{\text{зап.}\,j-1)i}$.

Шаг 14. Вычисление сигнатуры записей метаданных j-й строки: $h^{(k_U^{(1)})}_{\text{зап.}ji} = f\left(S_{\text{зап.}}, k_U^{(1)}\right)$.

Шаг 15 (вывод). Формирование сигнатур записей метаданных j-й строки $h^{(k_U^{(1)})}_{\text{зап.}j1}, \ldots, h^{(k_U^{(1)})}_{\text{зап.}ji_{\max}}$. Переход к шагу 11 (цикл операций повторяется для вычисления последующих сигнатур записей метаданных j-й строки).

DOI:10.21681/2311-3456-2020-06-32-47

Шаг 16. Конкатенация всех метаданных j-й строки и сигнатур предыдущей строки: $S_{\text{стр.}}^{(k_U^{(2)})} := S_{\text{стр.}} \| H_{j-1}^{(k_U^{(}}$; $S_{\text{стр.}}^{(k_U^{(3)})} := S_{\text{стр.}} \| H_{j-1}^{(k_U^{(3}}$.

Шаг 17. Вычисление сигнатур j-х строк: $H_j^{(k_U^{(2)})} = f\left(S_{\text{стр.}}, k_U^{(2)}\right); H_j^{(k_U^{(3)})} = f\left(S_{\text{стр.}}, k_U^{(3)}\right)$.

Шаг 18 (вывод). Формирование сигнатур метаданных j-х строк $H_1^{(k_U^{(2)})}, \ldots, H_{j_{\max}}^{(k_U^{(2)})}; H_1^{(k_U^{(3)})}, \ldots, H_{j_{\max}}^{(k_U^{(3)})}$, где $i = 1, \ldots, i_{\max}$ Переход к шагу 3 (операции повторяются до тех пор пока ЭлД востребован).

Алгоритм проверки криптографической рекурсивной 2-D последовательности метаданных с использованием множества ключей $\mathbf{K}_U$

Шаг 1. Ввод исходных данных:
$z_{11}, \ldots, z_{j_{\max} i_{\max}}$ – метаданные ЭлД;

$k_U^{(1)}, k_U^{(2)}, k_U^{(3)}$ – закрытые ключи, где $k_U^{(1)}$ – внутренние ключи системы; $k_U^{(2)}$ – внешние ключи администратора системы; $k_U^{(3)}$ – внешние ключи оператора системы, $U = 1, \ldots, \varsigma$;

$h_{\text{зап.}11}^{(k_U^{(1)})}, \ldots, h_{\text{зап.}j_{\max} i_{\max}}^{(k_U^{(1)})}$ – сигнатуры записей метаданных;

$H_1^{(k_U^{(2)})}, \ldots, H_{j_{\max}}^{(k_U^{(2)})}; H_1^{(k_U^{(3)})}, \ldots, H_{j_{\max}}^{(k_U^{(3)})}$ – сигнатуры строк записей метаданных.

Шаг 2. Извлечение из таблицы данных:
записей метаданных $z_{11}^*, \ldots, z_{j_{\max} i_{\max}}^* = z_{11}, \ldots, z_{j_{\max} i_{\max}}$;

сигнатур записей метаданных

$h_{\text{зап.}11}^{(k_U^{(1)})*}, \ldots, h_{\text{зап.}j_{\max} i_{\max}}^{(k_U^{(1)})*} = h_{\text{зап.}11}^{(k_U^{(1)})}, \ldots, h_{\text{зап.}j_{\max} i_{\max}}^{(k_U^{(1)})}$;

сигнатур строк записей метаданных

$H_1^{(k_U^{(2)})*}, \ldots, H_{j_{\max}}^{(k_U^{(2)})*} = H_1^{(k_U^{(2)})}, \ldots, H_{j_{\max}}^{(k_U^{(2)})}$;

$H_1^{(k_U^{(3)})*}, \ldots, H_{j_{\max}}^{(k_U^{(3)})*} = H_1^{(k_U^{(3)})}, \ldots, H_{j_{\max}}^{(k_U^{(3)})}$.

Шаг 3. Присвоение сигнатурам записей метаданных нулевой строки значения $h_{\text{зап.}01}^{(k_0^{(1)})**}, \ldots, h_{\text{зап.}0 i_{\max}}^{(k_0^{(1)})**} = \varnothing$;

сигнатуре нулевой строки записей метаданных значения $H_0^{(k_0^{(2)})**} := 0$; $H_0^{(k_0^{(3)})**} := 0$.

Шаг 4. Осуществление цикла вычислений сигнатур для j-х строк записей метаданных, где $j = 1, \ldots, j_{\max}$. По окончанию цикла вычислений алгоритм завершается.

Шаг 5. Присвоение извлеченной строке записей метаданных значения $S_{\text{стр.}}^* := \varnothing$. Установка маркера $\text{Integr}\left[i\right] := 0$, где $i = 1, \ldots, i_{\max}$.

Шаг 6. Осуществление цикла вычислений сигнатур для записей метаданных j-й строки, где $i = 1, \ldots, i_{\max}$. По окончанию цикла вычислений выполняется переход к шагу 13.

Шаг 7. Конкатенация i-х метаданных j-й строки: $S_{\text{стр.}}^* := S_{\text{стр.}}^* \| z_{ji}^*$.

Шаг 8. Конкатенация метаданных и повторно вычисленных сигнатур записей метаданных предыдущей строки: $S_{\text{зап.}}^* := z_{ji}^* \| h_{\text{зап.}\,j-1)i}^{(k_U^{(1)})**}$.

Шаг 9. Вычисление сигнатуры i-й записи метаданных j-й строки: $h_{\text{зап.}ji}^{(k_U^{(1)})**} = f(S_{\text{зап.}}^*, k_U^{(1)})$.

Шаг 10. Выполнение проверки условия $h_{\text{зап.}ji}^{(k_U^{(1)})**} = h_{\text{зап.}ji}^{(k_U^{(1)})*}$. Если условие выполняется, то осуществляется переход к шагу 11. Если условие не выполняется, то осуществляется переход к шагу 12.

Шаг 11 (вывод). Заключение об отсутствии нарушения целостности записи z_{ji} метаданных. Переход к шагу 6 (цикл операций повторяется для вычисления последующих сигнатур записей метаданных j-й строки).

Шаг 12 (вывод). Заключение о нарушении целостности записи z_{ji} метаданных. Установка маркера $\text{Integr}\left[i\right] := 0$. Переход к шагу 6 (цикл операций повторяется для вычисления последующих сигнатур записей метаданных j-й строки).

Шаг 13. Конкатенация всех метаданных j-й строки и вновь вычисленных сигнатур предыдущей строки: $S_{\text{стр.}}^{(k_U^{(2)})*} := S_{\text{стр.}}^* \| H_{j-1}^{(k_U^{(2)})}$; $S_{\text{стр.}}^{(k_U^{(3)})*} := S_{\text{стр.}}^* \| H_{j-1}^{(k_U^{(3)})**}$.

Шаг 14. Вычисление сигнатуры записей метаданных j-й строки: $H_j^{(k_U^{(2)})**} = f(S_{\text{стр.}}^{(k_U^{(2)})*}, k_U^{(2)})$; $H_j^{(k_U^{(3)})**} = f(S_{\text{стр.}}^{(k_U^{(3)})*}, k_U^{(3)})$.

Шаг 15. Осуществление цикла вычислений сигнатур для записей метаданных j-й строки, где $i = 1, \ldots, i_{\max}$. По окончанию цикла вычислений выполняется переход к шагу 4.

Шаг 16. Выполнение проверки условия $\text{Integr}\left[i\right] := 1$. Если условие выполняется, то осуществляется переход к шагу 17. Если условие не выполняется, то вычисление производится повторно.

Шаг 17. Выполнение проверки условия $H_j^{(k_U^{(2)})**} = H_j^{(k_U^{(2)})*}$. Если условие выполняется, то осу-

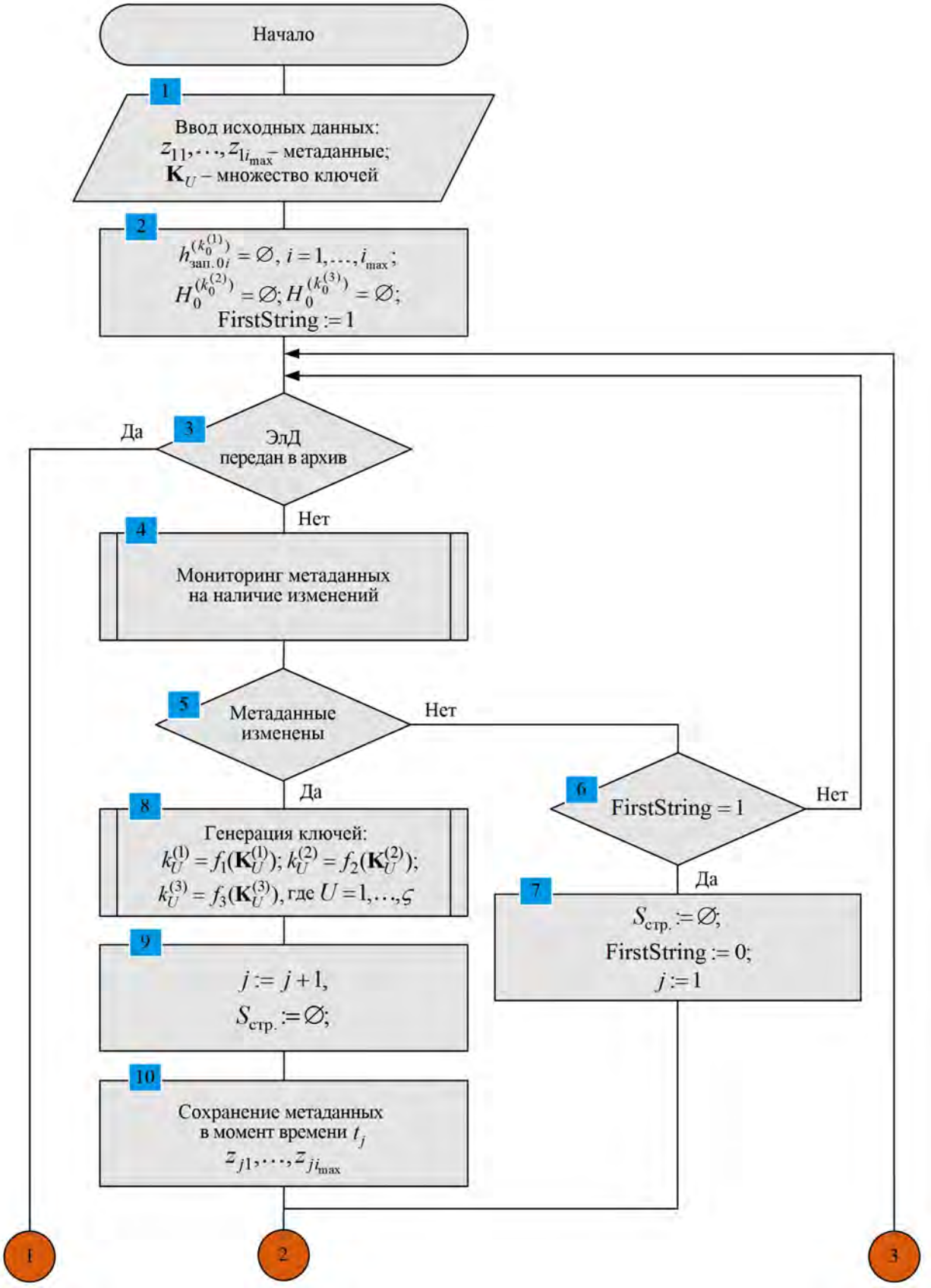

Рис. 3а. Блок-схема алгоритма формирования криптографической рекурсивной 2-D последовательности метаданных с использованием множества ключей $\mathbf{K}_U$ (начало)

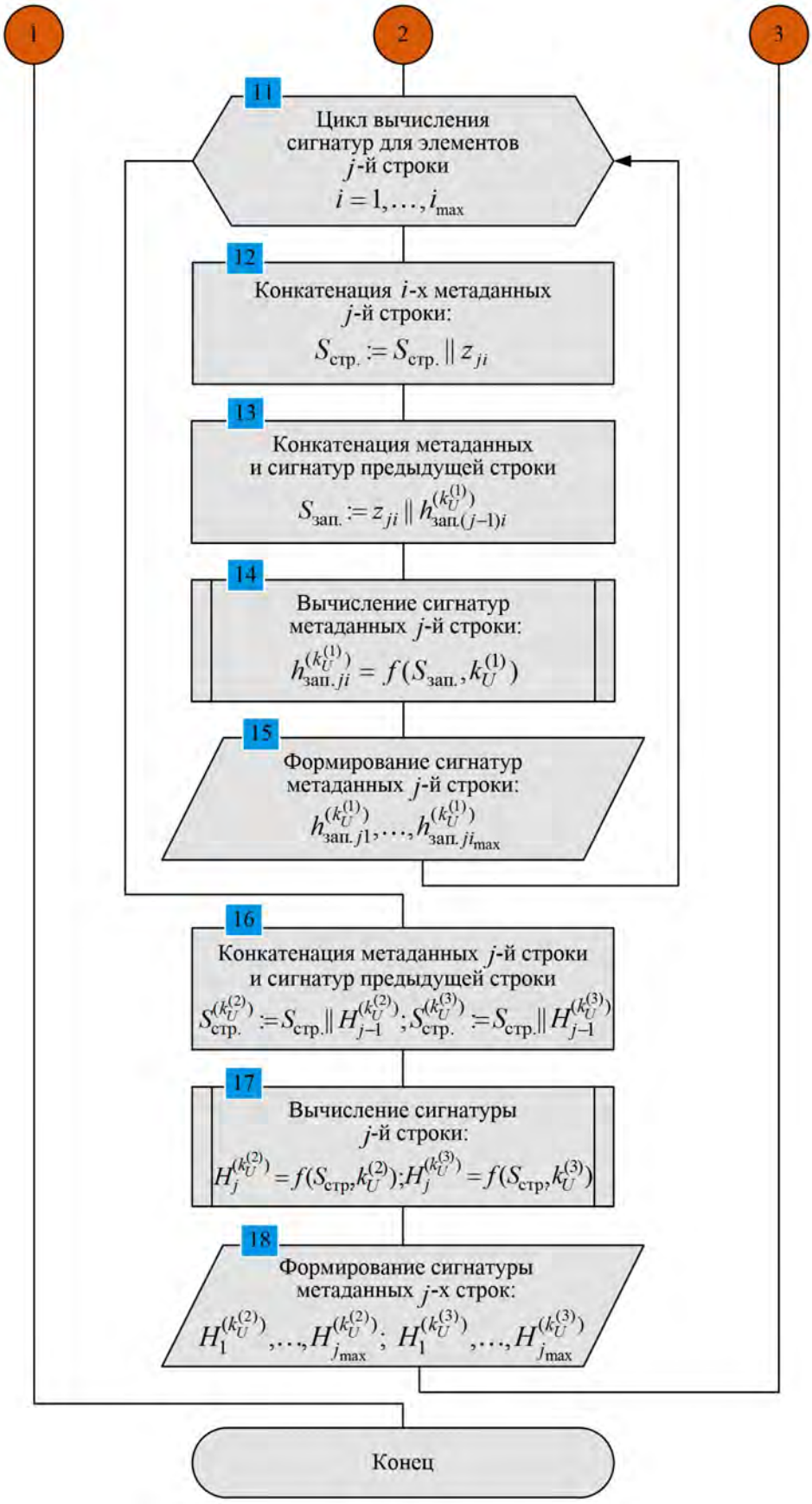

Рис. 3б. Блок-схема алгоритма формирования криптографической рекурсивной 2-D последовательности метаданных с использованием множества ключей t_j (окончание)

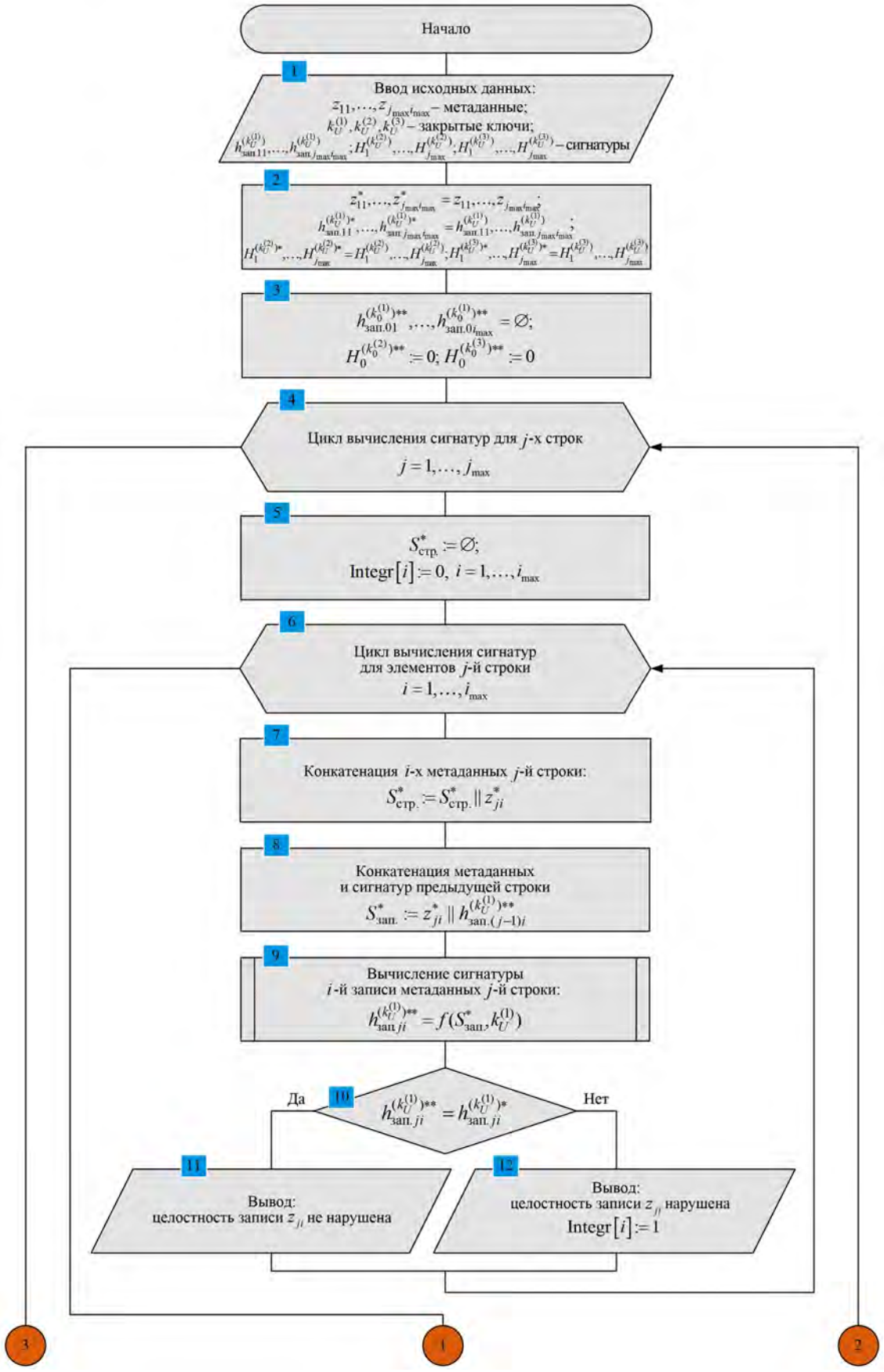

Рис. 4а. Блок-схема алгоритма проверки криптографической рекурсивной 2-D последовательности метаданных с использованием множества ключей $\mathbf{K}_U$ *(начало)*

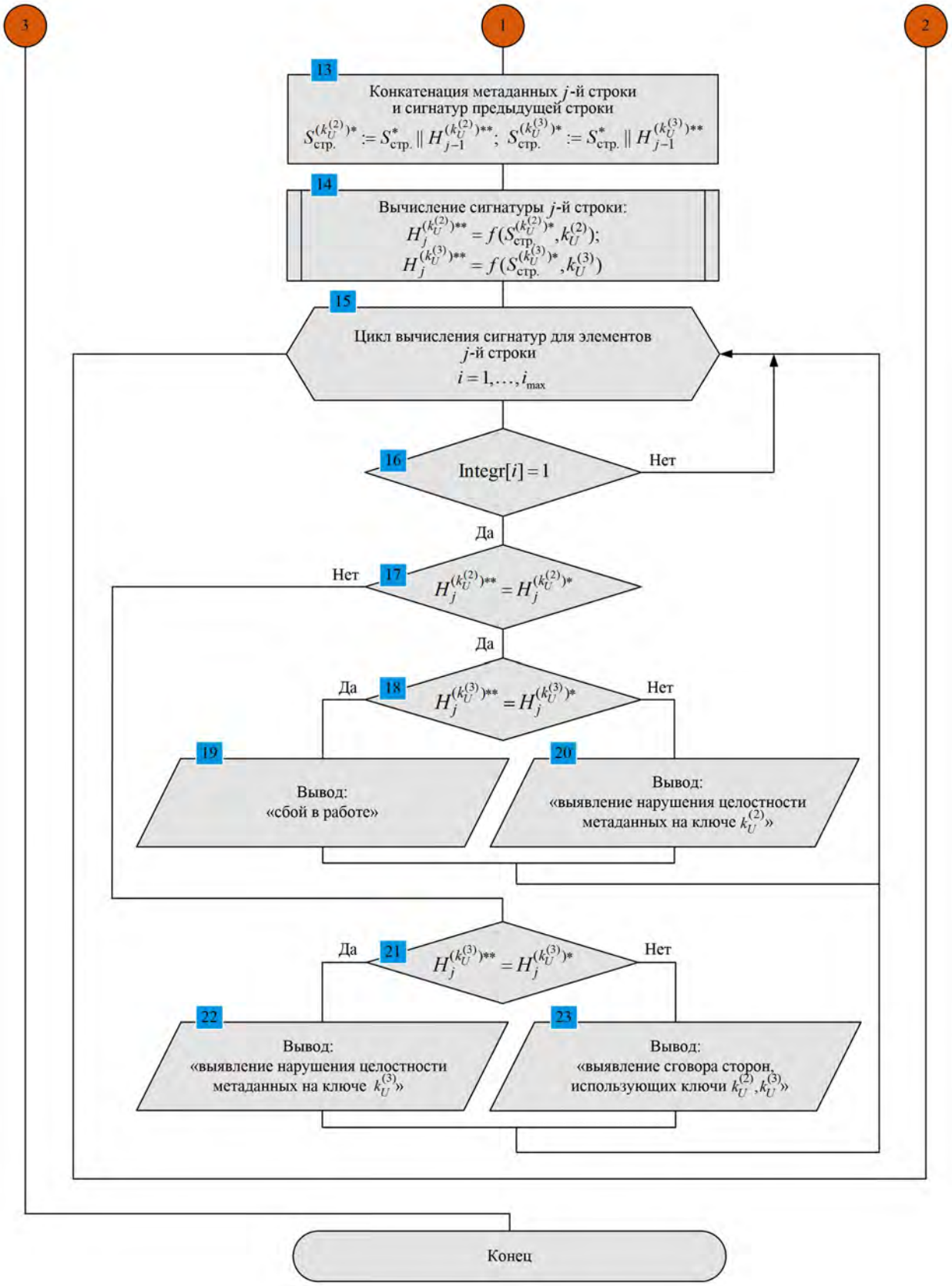

Рис. 4б. Блок-схема алгоритма проверки криптографической рекурсивной 2-D последовательности метаданных с использованием множества ключей $\mathbf{K}_U$ *(окончание)*

ществляется переход к шагу 18. Если условие не выполняется, то осуществляется переход к шагу 21.

Шаг 18. Выполнение проверки условия $H_j^{(k_U^{(3)})**} = H_j^{(k_U^{(3)})*}$. Если условие выполняется, то осуществляется переход к шагу 19. Если условие не выполняется, то осуществляется переход к шагу 20.

Шаг 19 (вывод). Заключение о сбое в работе системы. Переход к шагу 15 (цикл операций повторяется для вычисления последующих сигнатур элементов j-й строки).

Шаг 20 (вывод). Заключение о выявлении нарушения целостности метаданных с использованием ключа $k_U^{(2)}$. Переход к шагу 15 (цикл операций повторяется для вычисления последующих сигнатур элементов j-й строки).

Шаг 21. Выполнение проверки условия $H_j^{(k_U^{(3)})**} = H_j^{(k_U^{(3)})*}$. Если условие выполняется, то осуществляется переход к шагу 22. Если условие не выполняется, то осуществляется переход к шагу 23.

Шаг 22 (вывод). Заключение о выявлении нарушения целостности метаданных с использованием ключа $k_U^{(3)}$. Переход к шагу 15 (цикл операций повторяется для вычисления последующих сигнатур элементов j-й строки).

Шаг 23 (вывод). Заключение о выявлении сговора сторон, использующих ключи $k_U^{(2)}$, $k_U^{(3)}$. Переход к шагу 15 (цикл операций повторяется для вычисления последующих сигнатур элементов j-й строки).

Представленный комплекс алгоритмов удовлетворяет основным требованиям, предъявляемым к ним теорией алгоритмов (дискретность, детерминированность, сходимость, массовость) [11-15].

Выводы

Предложенные в статье решения являются логическим продолжением ранее проводимых исследований в области построения перспективных систем юридически значимого электронного документооборота, и направлены на практическую реализацию в ведомственных АИС ЭД [16, 17].

Представленный комплекс алгоритмов разработан на основе ранее предложенной авторами математической модели криптографического рекурсивного 2-D контроля целостности метаданных ЭлД [1]. Практическое применение данного технического решения позволит повысить уровень защищённости метаданных ЭлД, обрабатываемых АИС ЭД, в условиях деструктивных действий уполномоченных пользователей (инсайдеров).

Литература

1. Тали Д.И., Финько О.А. Криптографический рекурсивный контроль целостности метаданных электронных документов. Часть 1. Математическая модель // Вопросы кибербезопасности. 2020. № 5 (39). С. 2-18. DOI: 10.21681/2311-3456-2020-05-02-18
2. Тали Д.И. Модель угроз безопасности метаданным в системе электронного документооборота военного назначения // Вопросы оборонной техники. Серия 16: Технические средства противодействия терроризму. 2020. № 139-140. С. 95-101.
3. Hartmann K., Giles K. UAV exploitation: A new domain for cyber power // 8th International Conference on Cyber Conflict (CyCon). 2016. Pp. 205-221.
4. Куксов И. Как невидимые данные электронных документов приводят к реальным проблемам. 2017. https://www.kaspersky.ru/blog/office-documents-metadata/14277/
5. Путькина Л.В. Роль информационных систем и технологий в управлении предприятиями сферы услуг // Nauka-Rastudent.ru. 2016. № 5. С. 13.
6. Селиверстов Д.Е., Попов А.М., Захаров Е.Н. Алгоритм оценки и определения направлений повышения качества тренажерных комплексов для подготовки операторов робототехнических комплексов военного назначения // Стратегическая стабильность. 2017. №2 (79) С. 17-20.
7. Савин С.В., Финько О.А., Елисеев Н.И. Система контроля целостности журналов непрерывно ведущихся записей данных // Патент на изобретение RU 2637486, опубл. 04.12.2017, бюл. № 34.
8. Тали Д.И., Финько О.А., Елисеев Н.И., Диченко С.А., Барильченко С.А. Способ криптографического рекурсивного 2-D контроля целостности метаданных файлов электронных документов // Патент на изобретение RU 2726930, опубл. 16.07.2020, бюл. №20.
9. Жигалов К.Ю., Подлевских А.П., Аветисян К.Р. Направления развития систем обеспечения безопасности электронного документооборота в современных условиях // Современные наукоемкие технологии. 2019. № 2. С. 52-56.
10. Баранов А.В. Системы юридически значимого электронного документооборота // Актуальные проблемы экономики современной России. 2015. Т. 2. № 2. С. 28-31.
11. Пруцков А.В., Волкова Л.Л. Математическая логика и теория алгоритмов. М.: ИНФРА-М, 2018. 152 с.
12. Максимов Р.В., Орехов Д.Н., Соколовский С.П. Модель и алгоритм функционирования клиент-серверной информационной системы в условиях сетевой разведки // Системы управления, связи и безопасности. 2019. № 4. С. 50-99.
13. Селиверстов Д.Е. Алгоритм оценки качества сложных технических систем на основе моделей методологии АСФ // В сборнике: Наукоёмкие технологии на современном этапе развития машиностроения. Материалы VIII Международной научно-технической конференции. 2016. С. 204-207.

14. Гумбаталиев Р.З., Садигов А.С., Ахмедов Г.Г. Основные черты алгоритмов // В сборнике: Collection of scientific articles XVI International correspondence scientific specialized conference. 2020. С. 31-37.
15. Захаров Е.Н., Пипко В.С., Баль М.А. Общий анализ различных алгоритмов для возможного математического обеспечения интеллектуальных систем передачи информации // Труды ФГУП «НПЦАП». Системы и приборы управления. 2018. № 1. С. 59-62.
16. Елисеев Н.И., Финько О.А. Теоретические аспекты развития системы электронного документооборота Министерства обороны Российской Федерации // Военная мысль. 2015. № 7. С. 55-63.
17. Елисеев Н.И., Финько О.А. Управление целостностью системы юридически значимого электронного документооборота в условиях межформатных преобразований электронных документов // Проблемы управления. 2014. № 3 С. 68-73.

CRYPTOGRAPHIC RECURSIVE CONTROL OF INTEGRITY OF METADATA ELECTRONIC DOCUMENTS. PART 2. COMPLEX OF ALGORITHMS

D.I. Tali[7], O.A. Finko[8]

The purpose *of the study is to develop a set of algorithms to increase the level of security of metadata of electronic documents in conditions of destructive influences from authorized users (insiders).*

Research methods: *the principle of chain data recording technology, methods of the theory of algorithms, theoretical provisions for the construction of automated information systems of legally significant electronic document management.*

The result of the research: *a complex of algorithms for cryptographic recursive 2-D control of the integrity of metadata of electronic documents has been developed. Its feature is the following features:*

1. *localization of modified (with signs of integrity violation) metadata records of electronic documents;*
2. *identification of authorized users (insiders) who have carried out unauthorized modifications to the metadata of electronic documents;*
3. *identification of the fact of collusion of trusted parties through the introduction of* mutual control of the results of their actions.

The proposed solution allows to implement the functions of cryptographic recursive two-dimensional control of the integrity of metadata of electronic documents. At the same time, the use of the technology of chain data recording, at the heart of the presented solution, is due to the peculiarities of the functioning of departmental automated information systems of electronic document management.

Keywords: *automated information systems, electronic document management, metadata management, insider, chain data recording, dynamic ledger, hash function, electronic signature.*

References

1. Tali D.I., Finko O.A. Kriptograficheskiy rekursivnyy kontrol' tselostnosti metadannykh elektronnykh dokumentov. Chast' 1. Matematicheskaya model' // Voprosy kiberbezopasnosti. 2020. № 5 (39). S. 2-18. DOI: 10.21681/2311-3456-2020-05-02-18
2. Tali D.I. Model' ugroz bezopasnosti metadannym v sisteme elektronnogo dokumentooborota voyennogo naznacheniya // Voprosy oboronnoy tekhniki. Seriya 16: Tekhnicheskiye sredstva protivodeystviya terrorizmu. 2020. № 139-140. S. 95-101.
3. Hartmann K., Giles K. UAV exploitation: A new domain for cyber power // 8th International Conference on Cyber Conflict (CyCon). 2016. Pp. 205-221.
4. Kuksov I. Kak nevidimyye dannyye elektronnykh dokumentov privodyat k real'nym problemam. https://www.kaspersky.ru/blog/office-documents-metadata/14277/
5. Put'kina L.V. Rol' informatsionnykh sistem i tekhnologiy v upravlenii predpriyatiyami sfery uslug // Nauka-Rastudent.ru. 2016. № 5. S. 13.

7 Dmitry Tali, postgraduate student of department 21 (tactical and special communication) special, Krasnodar Higher Military Orders of Zhukov and the October Revolution Red Banner School named after General of the Army S.M. Shtemenko, Krasnodar, Russia. E-mail: dimatali@mail.ru

8 Oleg Finko, Dr.Sc., Professor, Professor of department 22 (special communication technology), Krasnodar Higher Military Orders of Zhukov and the October Revolution Red Banner School named after General of the Army S.M. Shtemenko, professor of the Department of Information Security of Automated Systems, North Caucasus Federal University, Academic Advisor of the Russian Academy of Rocket and Artillery Sciences (RARAN), Krasnodar, Russia. E-mail: ofinko@yandex.ru. Web: http://www.mathnet.ru/person40004. ORCID 0000-0002-7376-271

6. Seliverstov D.Ye., Popov A.M., Zakharov Ye.N. Algoritm otsenki i opredeleniya napravleniy povysheniya kachestva trenazhernykh kompleksov dlya podgotovki operatorov robototekhnicheskikh kompleksov voyennogo naznacheniya // Strategicheskaya stabil'nost'. 2017. №2 (79) S. 17-20.
7. Savin S.V., Finko O.A., Yeliseyev N.I. Sistema kontrolya tselostnosti zhurnalov nepreryvno vedushchikhsya zapisey dannykh // Patent na izobreteniye RU 2637486, opubl. 04.12.2017, byul. № 34.
8. Tali D.I., Finko O.A., Yeliseyev N.I., Dichenko S.A., Baril'chenko S.A. Sposob kriptograficheskogo rekursivnogo 2-D kontrolya tselostnosti metadannykh faylov elektronnykh dokumentov // Patent na izobreteniye RU 2726930, opubl. 16.07.2020, byul. №20.
9. Zhigalov K.Yu., Podlevskikh A.P., Avetisyan K.R. Napravleniya razvitiya sistem obespecheniya bezopasnosti elektronnogo dokumentooborota v sovremennykh usloviyakh // Sovremennyye naukoyemkiye tekhnologii. 2019. № 2. S. 52-56.
10. Baranov A.V. Sistemy yuridicheski znachimogo elektronnogo dokumentooborota // Aktual'nyye problemy ekonomiki sovremennoy Rossii. 2015. T. 2. № 2. S. 28-31
11. Prutskov A.V., Volkova L.L. Matematicheskaya logika i teoriya algoritmov. M.: INFRA-M, 2018. 152 s.
12. Maksimov R.V., Orekhov D.N., Sokolovskiy S.P. Model' i algoritm funktsionirovaniya kliyent-servernoy informatsionnoy sistemy v usloviyakh setevoy razvedki // Sistemy upravleniya, svyazi i bezopasnosti. 2019. № 4. S. 50-99.
13. Seliverstov D.Ye. Algoritm otsenki kachestva slozhnykh tekhnicheskikh sistem na osnove modeley metodologii ASF // V sbornike: Naukoyomkiye tekhnologii na sovremennom etape razvitiya mashinostroyeniya. Materialy VIII Mezhdunarodnoy nauchno-tekhnicheskoy konferentsii. 2016. S. 204-207.
14. Gumbataliyev R.Z., Sadigov A.S., Akhmedov G.G. Osnovnyye cherty algoritmov // V sbornike: Collection of scientific articles XVI International correspondence scientific specialized conference. 2020. S. 31-37.
15. Zakharov Ye.N., Pipko V.S., Bal' M.A. Obshchiy analiz razlichnykh algoritmov dlya vozmozhnogo matematicheskogo obespecheniya intellektual'nykh sistem peredachi informatsii // Trudy FGUP «NPTSAP». Sistemy i pribory upravleniya. 2018. № 1. S. 59-62.
16. Yeliseyev N.I., Finko O.A. Teoreticheskiye aspekty razvitiya sistemy elektronnogo dokumentooborota Ministerstva oborony Rossiyskoy Federatsii // Voyennaya mysl'. 2015. № 7. S. 55-63.
17. Yeliseyev N.I., Finko O.A. Upravleniye tselostnost'yu sistemy yuridicheski znachimogo elektronnogo dokumentooborota v usloviyakh mezhformatnykh preobrazovaniy elektronnykh dokumentov // Problemy upravleniya. 2014. № 3 S. 68-73.