КРИПТОГРАФИЧЕСКИЙ РЕКУРСИВНЫЙ КОНТРОЛЬ ЦЕЛОСТНОСТИ МЕТАДАННЫХ ЭЛЕКТРОННЫХ ДОКУМЕНТОВ. ЧАСТЬ 3. МЕТОДИКА ПРИМЕНЕНИЯ

Тали Д.И.[1], Финько О.А.[2]

Цель исследования *состоит в разработке рекомендаций по организации криптографического рекурсивного 2-D контроля целостности метаданных электронных документов на основе технологии цепной записи данных.*

Методы исследования: *в основе предложенной методики лежат общие принципы построения цепной записи данных, представляющей собой динамический реестр, в котором внесение изменений в записи метаданных допускается без изменения ранее внесенной информации. При этом связь между записями метаданных обеспечивается за счет использования криптографической хеш-функции.*

Результат исследования: *выполнен анализ жизненного цикла электронных документов, обрабатываемых автоматизированными информационными системами электронного документооборота, по результатам которого получен вывод о необходимости защиты метаданных криптографическими методами в целях контроля их целостности и эффективного управления электронными документами. Разработана методика криптографического рекурсивного 2-D контроля целостности метаданных электронных документов, основывающаяся на ранее предложенных авторами математической модели и комплексе алгоритмов. Описаны общие и частные результаты ее применения.*

Практическое использование предложенных решений позволяет обеспечить необходимые меры по защите электронных документов в условиях изменяющейся во времени обстановки в соответствии с требованиями по управлению документами. Такой эффект достигается за счет приведения существующей структуры метаданных к виду многомерной модели, тем самым позволяя достичь требуемого уровня их защищенности.

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

Статья является 3-ей частью работы (из 4-х). Предыдущие были опубликованы в ВК_5_2020 и ВК_6_2020.

DOI: 10.21681/2311-3456-2021-1-57-68

Введение

Представленная работа является логическим продолжением исследования функциональных возможностей способа криптографического рекурсивного 2-D контроля целостности метаданных файлов электронных документов [1], и направлена на практическую реализацию решений, ранее изложенных авторами в [2, 3].

Рассматриваемый тип автоматизированных информационных систем электронного документообо-

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.

рота (АИС ЭД) предназначен для решения задач организации единого защищенного информационного пространства в части электронного документооборота за счет применения единой технологии обработки и хранения документов[3] [2]. Информационные системы, обеспечивающие управление документами и доступ к ним в течение определённого времени, называются документными системами[4].

В общем виде управление документами включает в себя 4-х этапа:

1) создание документа;
2) ввод документа в систему с целью доказательства ведения какой-либо деятельности;
3) принятие надлежащих мер по защите документа, в условиях изменяющейся во времени обстановки;
4) санкционированное уничтожение или передача документа в архив.

Необходимо отметить, что документы состоят из контента и метаданных, которые описывают контекст, контент и структуру документов, а также управление ими в течение времени. При этом метаданными документа следует управлять, как и самим документом, поскольку они должны быть защищены от утраты или несанкционированного удаления и сохранены либо уничтожены в соответствии с требованиями, определенными на основе анализа проведенной деятельности. Таким образом, 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 деструктивных воздействий [2, 3].

Выполненный анализ предметной области показал, что в настоящее время защиту электронных документов (ЭлД), обрабатываемых АИС ЭД, обеспечивает подсистема защиты информации. Информация хранится в локальной базе данных (ЛБД), защищаемой посредством принятия мер разграничения доступа, а защита контента ЭлД, кроме того, обеспечивается криптографическими средствами электронной подписи. При этом влияние на ЭлД может оказывать только автор (исполнитель), а на метаданные – все исполняющие функции агента[5], что не исключает возможности осуществления внутренних нарушений установленной политики безопасности [4, 5].

Существование данного факта вызывает расхождение с требованиями нормативных документов по управлению ЭлД, выражающееся в более надежной защите только контента документа в отрыве от его метаданных, что противоречит самому определению состава документа.

Именно применение электронной подписи, основанной на криптографических методах, позволяет обеспечить требуемый уровень доверия к ЭлД и, как следствие, его правовой статус [6]. При этом существующий научно-методический аппарат защиты метаданных ЭлД не позволяет обеспечить уровень стойкости, присущий криптографическим средствам защиты информации (при условии наличия внутренних деструктивных воздействий). По этой причине был разработан способ криптографического рекурсивного 2-D контроля целостности метаданных файлов электронных документов, обрабатываемых АИС ЭД, позволяющий устранить выявленные недостатки [1] (рис. 1).

В целях практического применения данного технического решения должностными лицами, эксплуатирующими АИС ЭД, разработана методика криптографического рекурсивного 2-D контроля целостности метаданных ЭлД на основе технологии цепной записи данных.

Методика криптографического рекурсивного 2-D контроля целостности метаданных электронных документов на основе технологии цепной записи данных

Методика представляет собой совокупность моделей и алгоритмов криптографического рекурсивного 2-D контроля целостности метаданных ЭлД [2, 3], подлежит разработке в интересах должностных лиц, эксплуатирующих АИС ЭД преимущественно ведомственного назначения, и *предназначена для решения следующих задач*:

- обеспечения криптографического рекурсивного двумерного контроля целостности метаданных;
- локализации модифицированных записей метаданных, в условиях преднамеренных воздействий уполномоченных пользователей;
- выявления нарушителей (уполномоченных пользователей);
- исключения сговора доверенных сторон за счет введения взаимного контроля результатов их действий.

Предлагаемая методика разработана на основе технологии цепной записи данных, представляющей

3 Руководство оператора по системе электронного документооборота ЛНКВ.27100-01 34 01 «ИВК Бюрократъ», 2009 г. – 120 с.

4 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.

5 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.

Рис. 1. Предлагаемая схема процесса управления электронными документами

собой динамический реестр[6]. Процесс формирования такого реестра можно условно разделить на два этапа (рис. 2):

1) формирование криптографической рекурсивной 2-D последовательности метаданных;

2) проверка криптографической рекурсивной 2-D последовательности метаданных.

Основными условиями, которые учитываются при разработке данной методики, являются следующие допущения:

- средства защиты информации, функционирующие в АИС ЭД, могут иметь уязвимости, что способствует их использованию внутренним нарушителем в своих целях;
- внутренним нарушителем является может являться администратор и / 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 [3].

Ограничением методики является возможность использования только трех подмножеств ключей множества $\mathbf{K}_U \in \left\{\mathbf{K}_U^{(1)}, \mathbf{K}_U^{(2)}, \mathbf{K}_U^{(3)}\right\}$: ключи $\mathbf{K}_U^{(1)}$ являются внутренними системными ключами; ключи $\mathbf{K}_U^{(2)}$ – внешними ключами администратора системы; ключи $\mathbf{K}_U^{(3)}$ – внешними ключами оператора системы [1-3].

Применение методики позволяет реализовать криптографический рекурсивный двумерный контроль целостности метаданных ЭлД, обрабатываемых АИС ЭД, с возможностью локализации модифицированных записей метаданных, в условиях преднамеренных воздействий уполномоченных пользователей.

В соответствии с сущностью разрабатываемой методики, поставленными целями, задачами для эффективного управления ЭлД она должна применяться на протяжении всего жизненного цикла.

Под эффективным управлением ЭлД понимается деятельность по своевременному и полному обеспечению всего жизненного цикла ЭлД в АИС ЭД в соответствии с нормами и нормативами, установленными руководящей документации[7]. На основании

6 МР 26.4.001-2018. Методический документ. Методические рекомендации ТК 26. Информационная технология. Криптографическая защита информации. Термины и определения в области технологии цепной записи данных (блокчейн) и распределенных реестров. – М.: Технический комитет по стандартизации «Криптографическая защита информации», 2018.

7 ГОСТ Р ИСО 55103-2012. Ресурсосбережение. Эффективное управление ресурсами. Основные положения. – М.: Стандартинформ, 2014. – 19 с.

DOI: 10.21681/2311-3456-2021-1-57-68

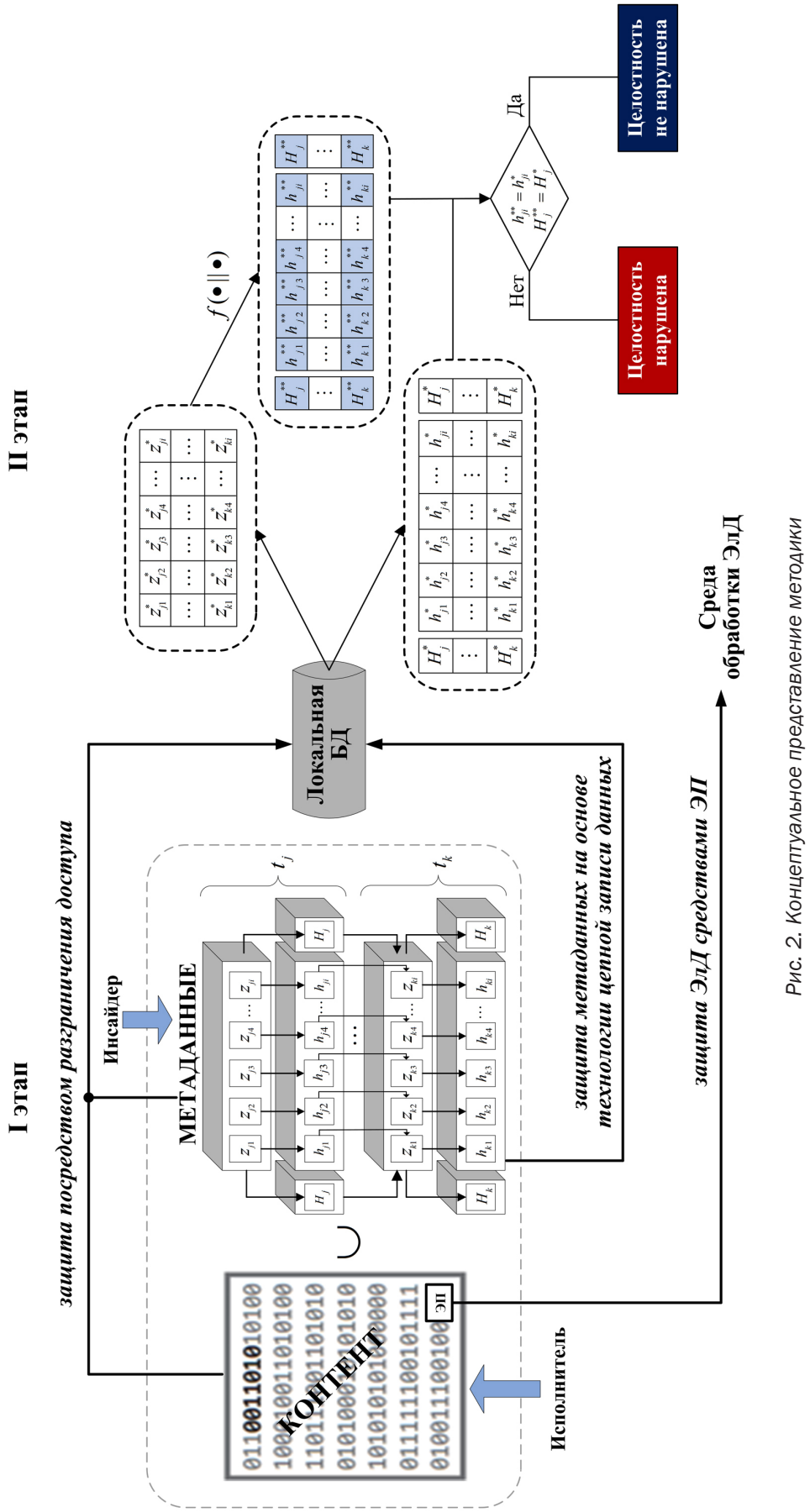


Рис. 2. Концептуальное представление методики

этого, разрабатываемая методика также состоит из четырех этапов, соответствующих требованиям по управлению ЭлД (рис. 1).

Кратко опишем этапы, реализуемые в представленной методике соотнеся их с этапами управления ЭлД (рис. 3).

Этап 1. Создание ЭлД, начало использования методики.

Одновременно с созданием контента ЭлД формируется пустая строка $S_{\text{стр.}} := \varnothing$, которая заполняется записями метаданных: $z_{j1}, \ldots, z_{ji_{\max}}$, где каждая запись является реквизитом, создаваемого ЭлД.

Если ЭлД оказался не востребованным (утратил свою значимость), то он передается на хранение в архив. Тогда применение методики завершается.

Этап 2. Формирование криптографической рекурсивной 2-D последовательности метаданных.

Если ЭлД востребован и продолжает циркулировать в АИС ЭД, то есть корректируется в моменты времени t_j $(j = 1, \ldots, k)$, задаётся условие: $j = j + 1$ на формирование новой строки. При этом агенты в целях коррекции записей метаданных используют закрытые ключи $k_{\varsigma}^{(q)} \in \mathbf{K}_U^{(q)}$ $(q = 1, \ldots, 3)$, для всех $U = 1, \ldots, \varsigma$. В результате выполнения этих процедур вычисляются сигнатуры $h_{\text{зап.}ji}^{(k_{\varsigma}^{(q)})}$ (в столбце) для каждой записи метаданных, а также сигнатуры $H_j^{(k_{\varsigma}^{(q)})}$ всей строки записей метаданных, которые в виде таблицы сохраняются в ЛБД вместе с соответствующими записями метаданных.

Описываемый этап является наиболее значимым, определяющим эффективность применения методики в целом, так как сохранённые записи и сигнатуры к ним, хранимые в ЛБД, в дальнейшем будут считаться эталонными.

Этап 3. Проверка криптографической рекурсивной 2-D последовательности метаданных (рис. 4).

В целях реализации мер по защите ЭлД в условиях изменяющейся во времени обстановки выполняется проверка целостности метаданных, состоящая в следующем:

1) из таблицы данных извлекаются сигнатуры и записи метаданных, прошедшие процедуру хранения и подлежащие контролю:
$H_1^{(2)*}, h_{11}^*, \ldots, h_{1i}^*, H_1^{(3)*}$; ...;$H_k^{(2)*}, h_{k1}^*, \ldots, h_{ki}^*, H_k^{(3)*}$ и $\left[z_{11}^* \quad \ldots \quad z_{1i}^*\right], \ldots, \left[z_{k1}^* \quad \ldots \quad z_{ki}^*\right]$;

2) выполняются повторные операции криптографического преобразования с использованием извлеченных данных, результатом которых являются вновь вычисленные сигнатуры:
$H_1^{(2)**}, h_{11}^{**}, \ldots, h_{1i}^{**}, H_1^{(3)**}$;
$H_k^{(2)**}, h_{k1}^{**}, \ldots, h_{ki}^{**}, H_k^{(3)**}$;

3) полученные сигнатуры сравниваются с ранее извлеченными из таблицы данных.

Этап 4. Заключение об отсутствии (наличии) нарушения целостности метаданных ЭлД. Завершение применения методики.

Заключение об отсутствии нарушения целостности записей метаданных делается при выполнении равенств сигнатур:
$h_{\text{зап.}ji}^{**} = h_{\text{зап.}ji}^{*}$; $H_j^{(k_{\varsigma}^{(q)})**} = H_j^{(k_{\varsigma}^{(q)})*}$,
в противном случае делается заключение о нарушении целостности записей метаданных для соответствующих номеров сигнатур.

Применение методики прекращается после окончания жизненного цикла ЭлД, то есть после его уничтожения или передачи на длительное хранение в архив.

Результаты применения разработанной методики

Как следует из общей структуры методики (рис. 3), за счет применения криптографического рекурсивного двумерного контроля целостности метаданных обеспечивается локализация модифицированных записей метаданных. Данную процедуру можно представить в виде схемы (рис. 5), которая описывает общий принцип использования методики.

В случае несанкционированной модификации записи метаданных z_{j2} ЭлД на этапе проверки криптографической рекурсивной 2-D последовательности метаданных после реализации повторного криптографического преобразования и вычисления сигнатур записей метаданных фиксируется изменение сигнатуры h_{j2}^{**} записи метаданных z_{j2}^*, что в свою очередь вызывает изменение сигнатур данной строки H_j^{**}.

В связи с тем, что данное техническое решение основано на общих принципах построения цепной записи данных, модифицированная запись метаданных вызовет нарушения целостности сигнатур, как в столбце данного реквизита, так и в сигнатурах последующих строк записей метаданных, что позволяет отследить всю цепь изменений вплоть до момента первичной модификации записи.

При сравнении вновь вычисленных сигнатур с ранее извлечёнными получим неравенства:
$h_{j2}^{**} \neq h_{j2}^{*}, \ldots, h_{k2}^{**} \neq h_{k2}^{*}; H_j^{**} \neq H_j^{*}, \ldots, H_k^{**} \neq H_k^{*}$.

Таким образом, проанализировав цепь изменений метаданных, определим первичный момент модификации, который начинается с сигнатуры h_{j2}^{**} записи метаданных z_{j2}^*, что свидетельствует о внесении несанкционированных изменений в эту запись.

Дополнительными возможностями представленного решения (за счет использования ключей $\mathbf{K}_U \in \left\{\mathbf{K}_U^{(1)}, \mathbf{K}_U^{(2)}, \mathbf{K}_U^{(3)}\right\}$ [3]) являются:

- выявление нарушителей;
- исключение сговора доверенных сторон, за счет обеспечения взаимного контроля над действиями уполномоченных пользователей АИС ЭД;

DOI: 10.21681/2311-3456-2021-1-57-68

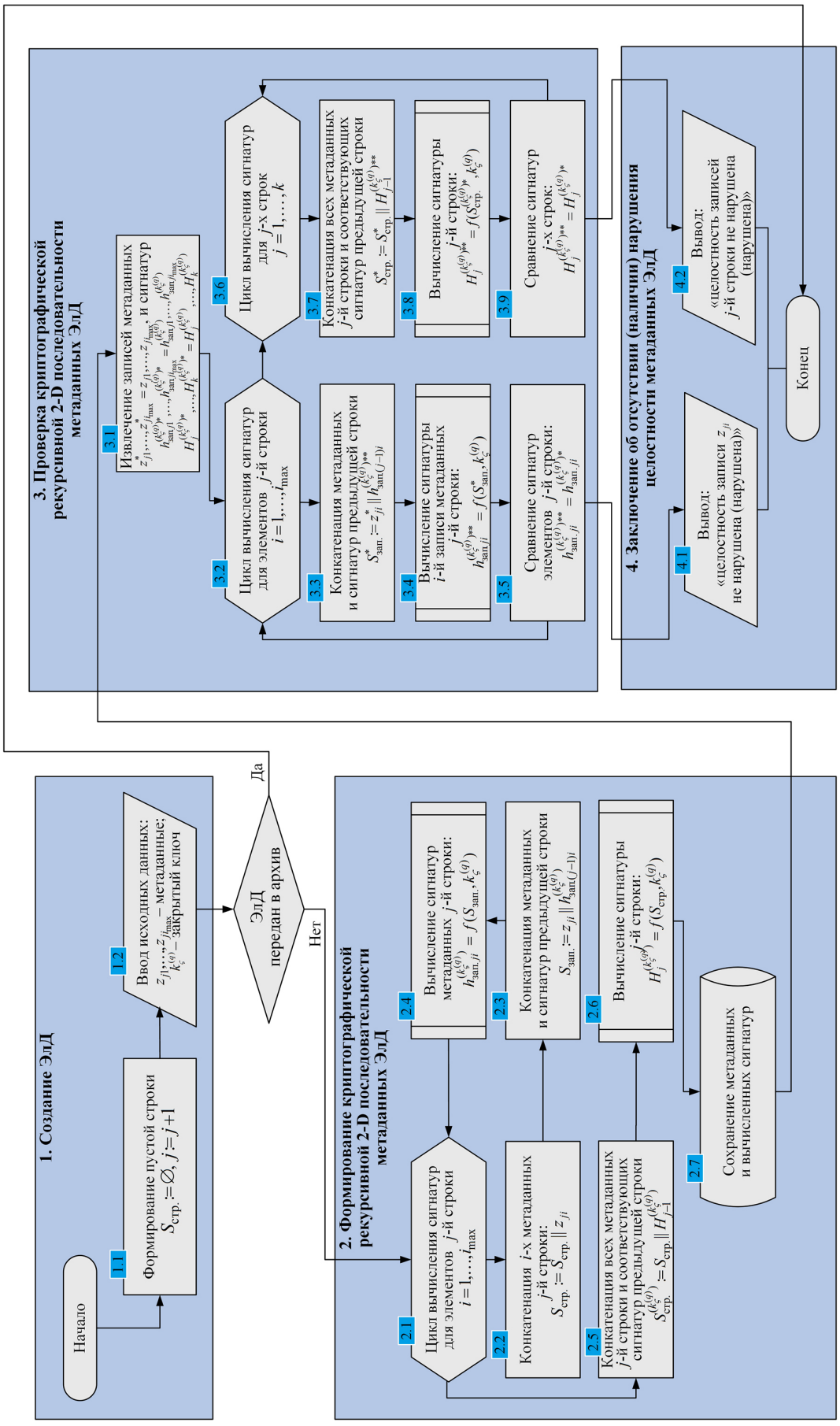


Рис. 3. Структура методики криптографического рекурсивного 2-D контроля целостности метаданных ЭлД, обрабатываемых АИС ЭД, на основе технологии цепной записи данных

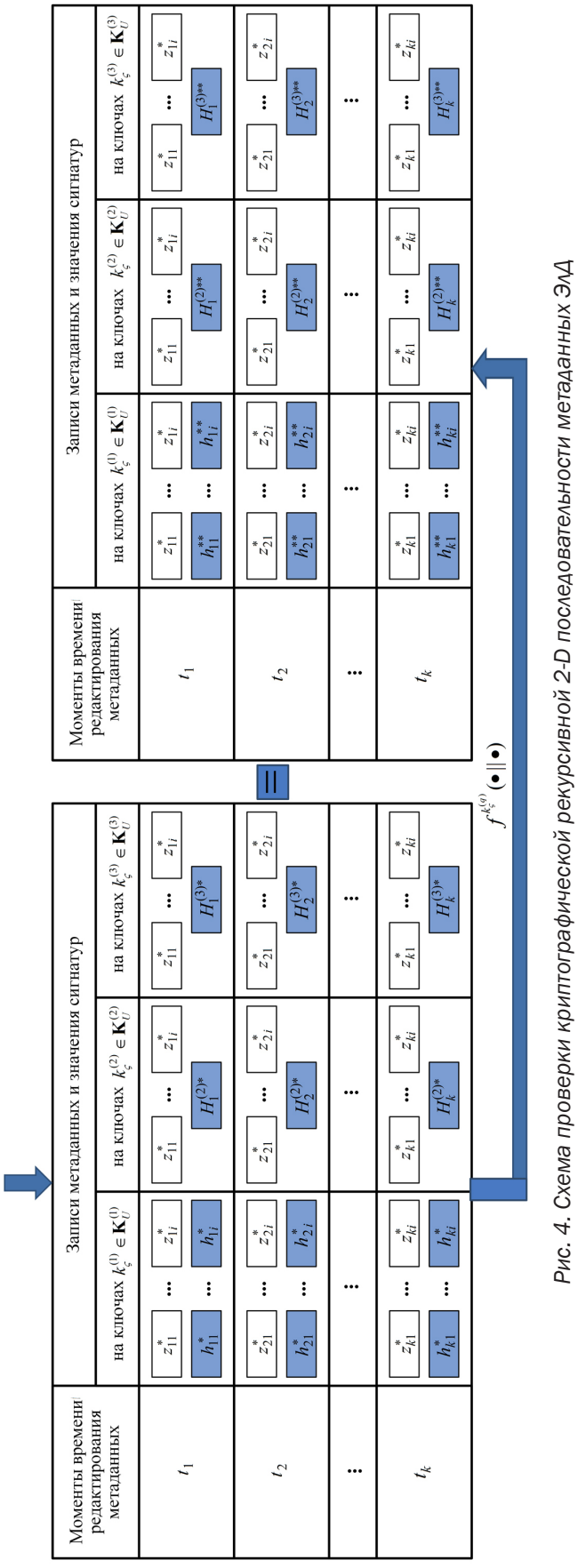


Рис. 4. Схема проверки криптографической рекурсивной 2-D последовательности метаданных ЭлД

DOI: 10.21681/2311-3456-2021-1-57-68

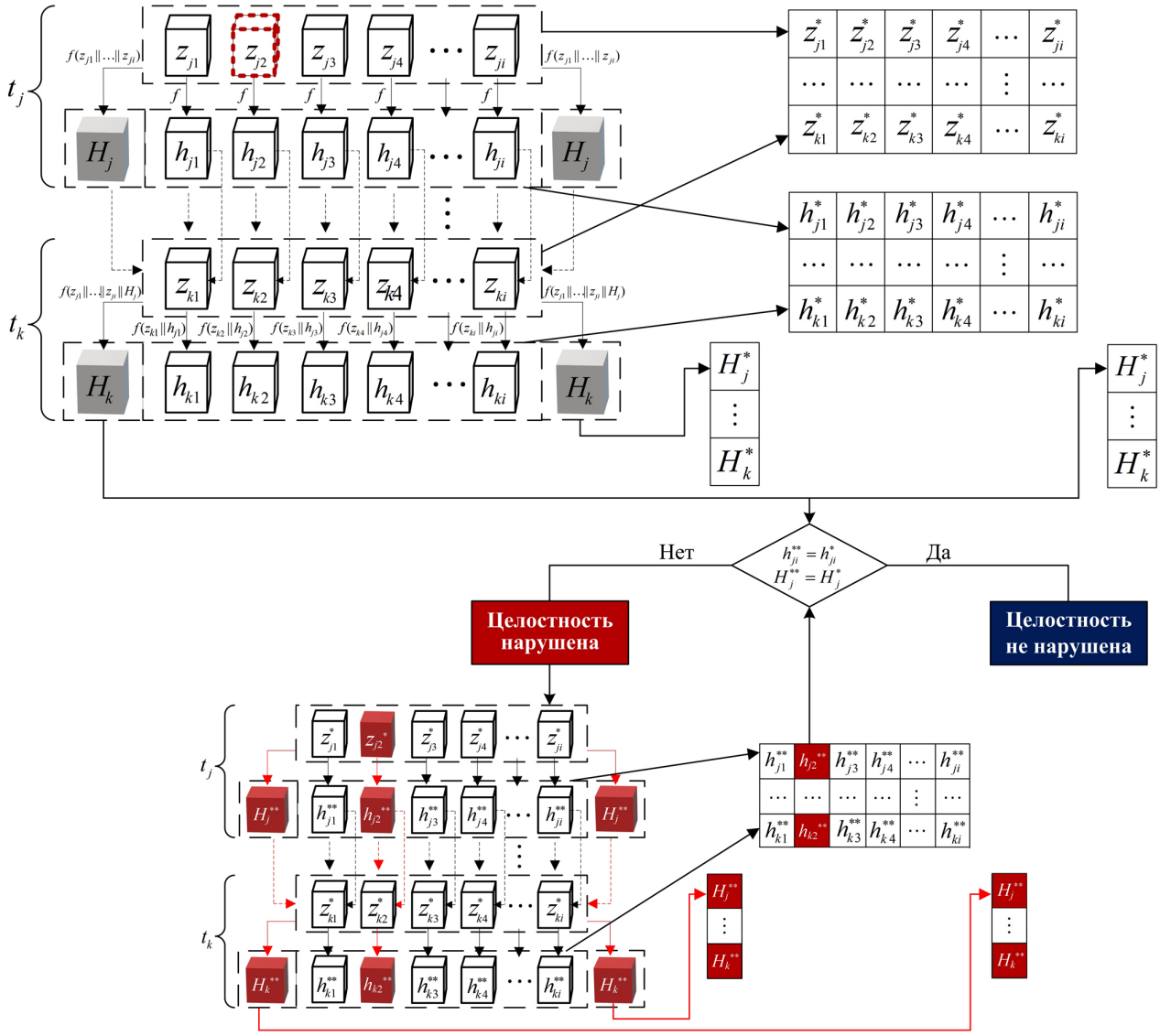


Рис. 5. Схема локализации несанкционированно модифицированных записей метаданных

- выявление сбоя в работе АИС ЭД, вызванного ошибками в работе программного обеспечения (или его дефектами).

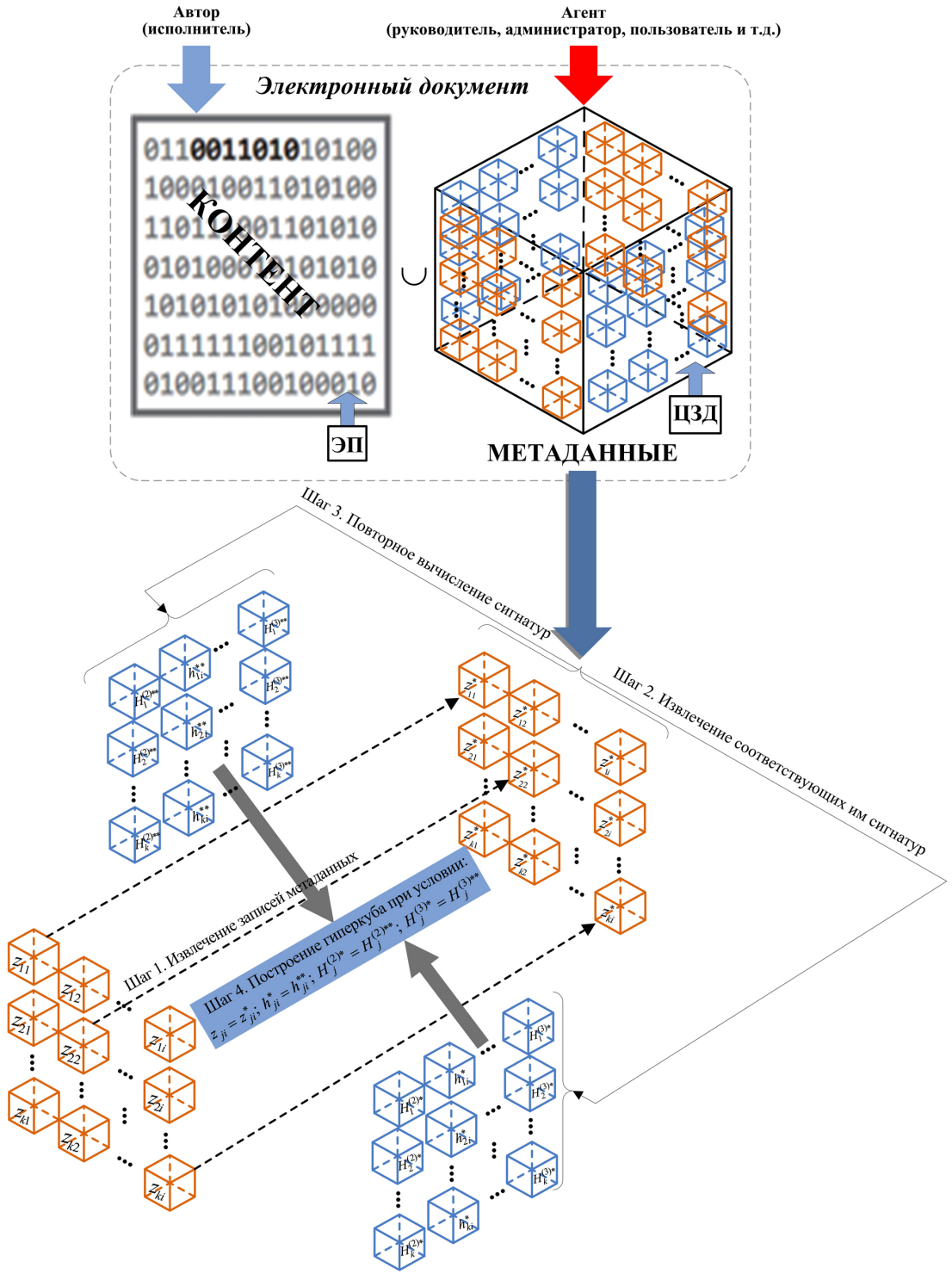
Применение полученных результатов в целях управления электронными документами

Основная роль АИС ЭД в повседневной деятельности любой современной организации – эффективное управление ЭлД [7]. При этом основным требованием, предъявляемым к таким системам, является защита обрабатываемых документов от несанкционированного изменения и возможность выявления (отслеживания) любых санкционированных изменений, добавлений или удалений в документе.

Пригодным для использования является ЭлД, который может быть найден, извлечен, воспроизведен и интерпретирован в течение времени, установленного заинтересованными сторонами или нормативными документами. Метаданные документов обеспечивают их пригодность для использования путем предоставления информации, которая может потребоваться для извлечения и поиска таких ЭлД. В связи с этим, в целях поддержания и создания логических связей между контентом и метаданными, последние должны быть описаны и зафиксированы в схемах метаданных[8].

Поскольку рассматриваемый объект исследования реализует функции хранения, обрабатываемой информации, критичным является время получения

8 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.



ЭП – электронная подпись

ЦЗД – цепная запись данных

– записи метаданных, где $z_{ji} = z^*_{ji}$

– сигнатуры записей (строк) метаданных, где $h^*_{ji} = h^{**}_{ji}$; $H^{(2)*}_j = H^{(2)**}_j$; $H^{(3)*}_j = H^{(3)**}_j$

Рис. 6. Преобразование структуры ЭлД с учетом полученных результатов

DOI: 10.21681/2311-3456-2021-1-57-68

ответов на запросы пользователей системы. В таком случае схемы метаданных уместно представлять в виде упорядоченных многомерных массивов (гиперкубов), что позволит оперативно извлекать необходимую информацию о состоянии ЭлД [8, 9].

В основе многомерных моделей данных лежит концепция многомерных кубов или гиперкубов [10]. Они представляют собой упорядоченные многомерные массивы, которые также часто называют OLAP-кубами («On-Line Analytical Processing» – оперативная аналитическая обработка). Технология OLAP представляет собой методику оперативного извлечения нужной информации из больших массивов данных и формирования соответствующих отчетов [11, 12].

Воспользуемся данной технологией в сочетании с разработанным решением. В таком случае процесс построения гиперкуба реализуется следующим образом.

Шаг 1. Извлечение записей метаданных z^*_{ji}, прошедших процедуру хранения.

Шаг 2. Извлечение сигнатур h^*_{ji}, $H^{(q)*}_j$, соответствующих записям метаданных z^*_{ji}.

Шаг 3. Повторное вычисление сигнатур h^{**}_{ji}, $H^{(q)**}_j$ от записей метаданных z^*_{ji}.

Шаг 4. Формирование гиперкуба при условии: $z_{ji} = z^*_{ji};\ h^*_{ji} = h^{**}_{ji};\ H^{(2)*}_j = H^{(2)**}_j;\ H^{(3)*}_j = H^{(3)**}_j$.

Результатом такого подхода станет преобразование структуры ЭлД (рис. 9), которая позволит обеспечить не только их целостность, но и эффективность управления, что является важнейшими задачами, стоящими перед АИС ЭД.

Выводы

Контроль целостности метаданных рассмотрен как составная часть процесса по управлению ЭлД в рамках принятия надлежащих мер по защите документа в условиях изменяющейся во времени обстановки. Использование принципа цепной записи данных в решении поставленных задач позволило обеспечить технические возможности по локализации несанкционированно модифицированных записей метаданных, а также организовать взаимный контроль над действиями уполномоченных пользователей АИС ЭД.

Решение, предложенное в данной статье, является логическим продолжением ранее выполненных авторами исследований в области анализа и синтеза перспективных систем юридически значимого электронного документооборота и ориентированно на реализацию, преимущественно, в ведомственных АИС ЭД [13, 14].

Полученные результаты, в сочетании с многомерным представлением данных, позволяют надежно защитить метаданные, обеспечив при этом эффективность управления ЭлД, обрабатываемыми АИС ЭД. В представленном решении цепная запись данных является «надстройкой» над классической базой данных, в роли которой выступают метаданные, представленные в виде многомерной модели. Такой подход позволит регламентировать порядок представления информации, хранимой в базе данных, эффективно использовать разработанный механизм контроля целостности метаданных, а также определить порядок внесения, фиксации и отслеживания изменений [15, 16].

Литература

1. 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.
2. 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: 10.21681/2311-3456-2020-05-2-18
3. Тали Д.И., Финько О.А. Криптографический рекурсивный контроль целостности метаданных электронных документов. Часть 2. Комплекс алгоритмов // Вопросы кибербезопасности. 2020. № 6 (40). С. 32-47. DOI: 10.21681/2311-3456-2020-06-32-47
4. 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.
5. Hartmann K., Giles K. UAV exploitation: A new domain for cyber power // 8th International Conference on Cyber Conflict (CyCon). 2016. Pp. 205-221.
6. Баранов А.В. Системы юридически значимого электронного документооборота // Актуальные проблемы экономики современной России. 2015. Т. 2. № 2. С. 28-31
7. 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.
8. Тарасов С.В. СУБД для программиста. Базы данных изнутри. М.: СОЛОН-Пресс, 2015. 320 с.
9. Диченко С.А., Финько О.А. Обобщенный способ применения хэш-функции для контроля целостности данных // Наукоемкие технологии в космических исследованиях земли. 2020. Т. 12. № 6. С. 48-59. DOI: 10.36724/2409-5419-2020-12-6-48-59.

10. Громов Ю.Ю., Иванова О.Г., Яковлев А.В., Однолько В.Г. Управление данными. – Тамбов: «ТГТУ», 2015. 192 с.
11. Murray D.R., Newman M.B. Probability analyses of combining background concentrations with model-predicted concentrations. // J. Air Waste Manag. Assoc. 2016, vol. 64, no. 3, pp. 248-254.
12. Диченко С.А., Финько О.А. Гибридный крипто-кодовый метод контроля и восстановления целостности данных для защищённых информационно-аналитических систем // Вопросы кибербезопасности. 2019. № 6 (34). С. 7-14. DOI: 10.21681/2311-3456-2019-6-17-36.
13. Елисеев Н.И., Финько О.А. Теоретические аспекты развития системы электронного документооборота Министерства обороны Российской Федерации // Военная мысль. 2015. № 7. С. 55-63.
14. 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.
15. Гуселев А.М., Лавриков И.В., Маршалко Г.Б., Шишкин В.А. Технологии цепной записи данных и распределенных реестров: криптографический скачок вперед, шаг назад или путь в никуда // Материалы научно-практической конференции «РусКрипто-2017». https://www.ruscrypto.ru/resource/archive/rc2017/files/02_guselev_lavrikov_marchalko_shishkin.pdf
16. 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.

CRYPTOGRAPHIC RECURSIVE CONTROL OF INTEGRITY OF METADATA ELECTRONIC DOCUMENTS. PART 3. APPLICATION METHODOLOGY

***Tali D.I.*[9], *Finko O.A.*[10]**

The purpose *of the study is to develop recommendations for organizing a cryptographic recursive 2-D control of the integrity of electronic documents metadata based on chain data recording technology.*

Research methods*: the proposed methodology is based on the general principles of constructing a chain data record, which is a dynamic registry, where changes in metadata records are allowed without changing the previously entered information. In this case, the relationship between the metadata records is ensured through the use of a cryptographic hash function.*

Research result: *the analysis of the life cycle of electronic documents processed by automated information systems of electronic document management was carried out, based on the results of which it was concluded that it is necessary to protect metadata by cryptographic methods in order to control their integrity and effectively manage electronic documents. The technique of cryptographic recursive 2-D control of the integrity of metadata of electronic documents, based on the previously proposed by the authors a mathematical model and a set of algorithms, has been developed. General and particular results of its application are described.*

The practical use of the proposed solutions makes it possible to provide the necessary measures to protect electronic documents in a time-changing environment, in accordance with the requirements for document management. This effect is achieved by bringing the existing metadata structure to the form of a multidimensional model, thereby making it possible to achieve the required level of their security.

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

9 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

10 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: www.mathnet.ru/person40004. ORCID 0000-0002-7376-271

DOI: 10.21681/2311-3456-2021-1-57-68

References

1. 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.
2. 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.
3. Tali D.I., Finko O.A. Kriptograficheskiy rekursivnyy kontrol' tselostnosti metadannykh elektronnykh dokumentov. Chast' 2. Kompleks algoritmov // Voprosy kiberbezopasnosti. 2020. № 6 (40). S. 32-47.
4. 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.
5. Hartmann K., Giles K. UAV exploitation: A new domain for cyber power // 8th International Conference on Cyber Conflict (CyCon). 2016. Pp. 205-221.
6. 6. Baranov A.V. Sistemy yuridicheski znachimogo elektronnogo dokumentooborota // Aktual'nyye problemy ekonomiki sovremennoy Rossii. 2015. T. 2. № 2. S. 28-31
7. 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.
8. Tarasov S.V. SUBD dlya programmista. Bazy dannykh iznutri. M.: SOLON-Press, 2015. 320 s.
9. Dichenko S.A., Finko O.A. Obobshchennyj sposob primeneniya hesh-funkcii dlya kontrolya celostnosti dannyh // Naukoyemkiye tekhnologii v kosmicheskikh issledovaniyakh Zemli. 2020. T. 12. № 6. S. 48-59. DOI: 10.36724/2409-5419-2020-12-6-48-59.
10. Gromov YU.YU., Ivanova O.G., Yakovlev A.V., Odnol'ko V.G. Upravleniye dannymi. – Tambov: «TGTU», 2015. 192 s.
11. Murray D.R., Newman M.B. Probability analyses of combining background concentrations with model-predicted concentrations // J. Air Waste Manag. Assoc. 2016, vol. 64, no. 3, pp. 248-254.
12. Dichenko S.A., Finko O.A. Gibridnyy kripto-kodovyy metod kontrolya i vosstanovleniya tselostnosti dannykh dlya zashchishchonnykh informatsionno-analiticheskikh sistem // Voprosy kiberbezopasnosti. 2019. № 6 (34). S. 7-14. DOI: 10.21681/2311-3456-2019-6-17-36.
13. Yeliseyev N.I., Finko O.A. Teoreticheskiye aspekty razvitiya sistemy elektronnogo dokumentooborota Ministerstva oborony Rossiyskoy Federatsii // Voyennaya mysl'. 2015. № 7. S. 55-63.
14. 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.
15. Guselev A.M., Lavrikov I.V., Marshalko G.B., Shishkin V.A. Tekhnologii tsepnoy zapisi dannykh i raspredelennykh reyestrov: kriptograficheskiy skachok vpered, shag nazad ili put' v nikuda // Materialy nauchno-prakticheskoy konferentsii «RusKripto-2017». https://www.ruscrypto.ru/resource/archive/rc2017/files/02_guselev_lavrikov_marchalko_shishkin.pdf
16. Savin S.V., Finko O.A., Eliseev N.I. Sistema kontrolya celostnosti zhurnalov nepreryvno vedushchihsya zapisej dannyh // Patent na izobreteniye RU 2637486, opubl. 04.12.2017, byul. № 34.