КРИПТОГРАФИЧЕСКИЙ РЕКУРСИВНЫЙ КОНТРОЛЬ ЦЕЛОСТНОСТИ МЕТАДАННЫХ ЭЛЕКТРОННЫХ ДОКУМЕНТОВ. ЧАСТЬ 1. МАТЕМАТИЧЕСКАЯ МОДЕЛЬ

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 первой из четырех, следующие будут опубликованы в ВК-6-2020, ВК-1-2021 и ВК-2-2021.

Целью исследования *является повышение уровня защищенности метаданных электронных документов в условиях деструктивных воздействий уполномоченных пользователей (инсайдеров).*

Методы исследования: *новые научные результаты позволили использовать сочетание: способ контроля целостности данных на основе метода «однократной записи»[3] и способ аутентификации сообщений на основе HMAC (hash-based message authentication)[4], а также методы теории графов.*

Результат исследования: *предложен способ криптографического рекурсивного 2-D контроля целостности метаданных электронных документов. Выполнен анализ объекта исследования, по результатам которого сделан вывод о необходимости эффективной защиты метаданных электронных документов, обрабатываемых автоматизированными информационными системами электронного документооборота. Разработана и описана математическая модель предложенного способа, основывающаяся на теории графов.*

Разработанное техническое решение позволяет реализовать функции криптографического рекурсивного двухмерного контроля целостности метаданных электронных документов, а также обеспечить возможность локализации модифицированных (с признаками нарушения целостности) записей метаданных, в условиях деструктивных воздействий уполномоченных пользователей (инсайдеров). Это, в свою очередь, позволяет снизить вероятность сговора доверенных сторон за счет введения взаимного контроля результатов их действий. Предложенное решение позволяет обеспечить контроль целостности данных, обрабатываемых ведомственными автоматизированными информационными системами электронного документооборота, где, в силу особенностей их построения, невозможно эффективное применение популярной в настоящее время в технологии «блокчейн» в существующих вариантах ее реализации.

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

DOI: 10.21681/2311-3456-2020-05-2-18

Введение

В настоящее время наблюдается тенденция перехода бумажного документооборота к электронному, что обуславливает интенсивность развития автоматизированных информационных систем электронного документооборота (АИС ЭД), в связи с чем возникает необходимость защиты данных (электронных документов), обрабатываемых в них.

В соответствии с действующим стандартом по управлению документами, электронные документы (ЭлД) состоят из контента и метаданных, которые опи-

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 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.

4 Bellare M. New Proofs for NMAC and HMAC: Security without Collision-Resistance.CRYPTO. ePrint Archive, Report 2006/043. 2006, pp.1-16.

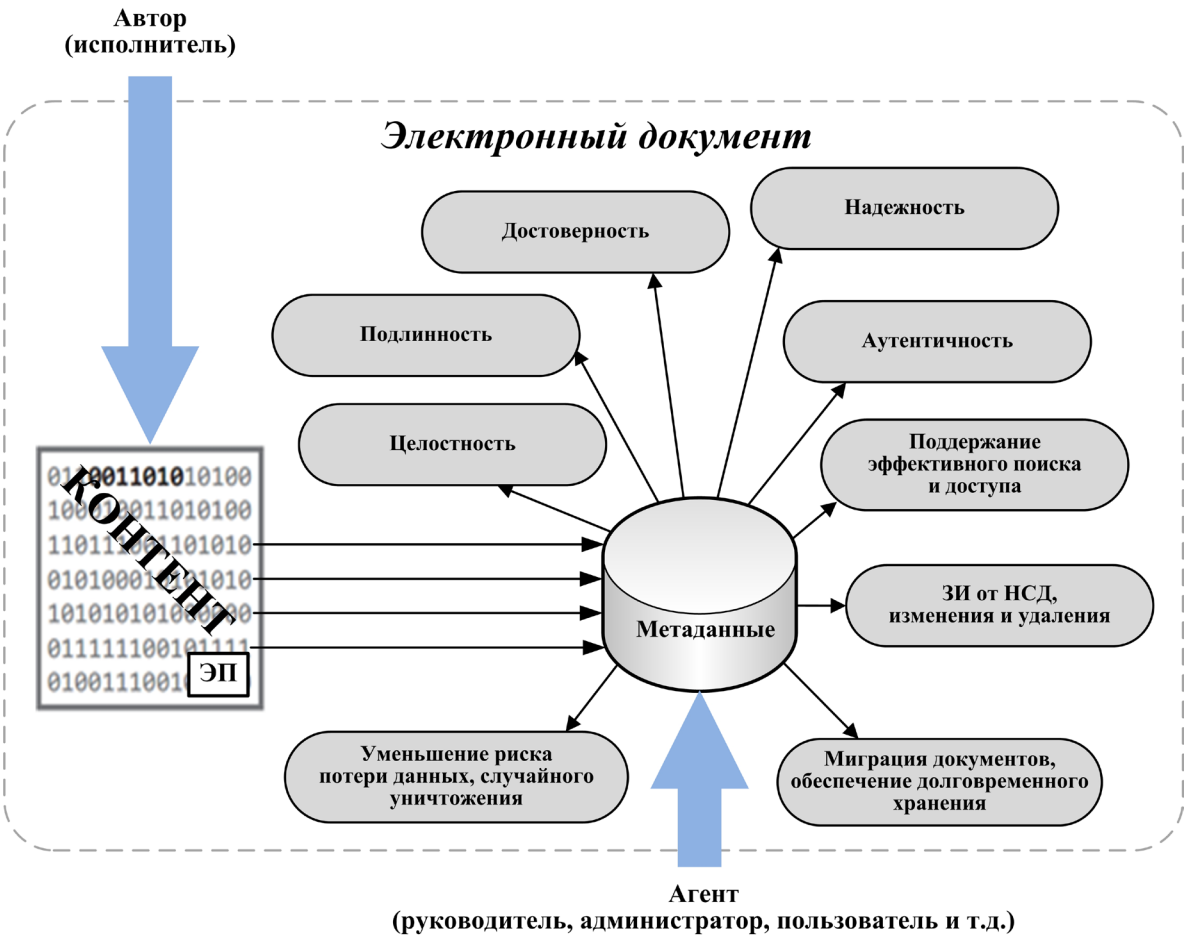


Рис. 1. Структура электронного документа и функции его метаданных

сывают контекст, контент и структуру документов, а также управление ими в течение времени[5]. Существующая структура ЭлД и функции его метаданных представлена на рис. 1 [1].

Метаданные критически важны для обеспечения значимости, сохранности и управляемости ЭлД, так как являются описанием характеристик данных в базах данных и электронных хранилищах [2]. Именно поэтому большое значение в управлении документами необходимо уделять механизму защиты метаданных в АИС ЭД.

В целях более глубокого понимания проблемы защиты метаданных необходимо в их общей классификации выделить параметры, зависящие от времени: метаданные могут быть как статическими, так и динамическими. В соответствии с действующими нормативными документами, они имеют наименование метаданных ввода документов в систему и метаданных процессов управления документами[6].

Метаданные ввода документов в систему статичны и являются лишь минимально необходимым набором элементов, идентифицирующих ЭлД в момент его создания, не отражая изменения содержания, структуры и контекста документа в течение последующего времени, что может быть представлено в алгебраическом виде, следующим образом.

Пусть $K^{(t_i)}$ – контент ЭлД, существующий и модифицируемый в дискретном времени t_i, $Z^{(t_i)}$ – метаданные ЭлД в дискретном времени t_i, где $i=0, 1, 2, ..., n$, тогда $D^{(t_i)}$ – информационный блок, представляющий собой ЭлД, создаваемый набором элементов из $K^{(t_i)}$ и $Z^{(t_i)}$, что можно записать как:

$$D^{(t_i)} = K^{(t_i)} \cup \left(\bigcup_{j=0}^{i} Z^{(t_j)} \right). \quad (1)$$

В таком случае, создание ЭлД с учетом формирования статических метаданных можно записать следующим образом:

$$D^{(t_0)} = K^{(t_0)} \cup Z^{(t_0)}, \quad (2)$$

где t_0 момент создания ЭлД.

На рис. 2 представлена структура модели формирования статических метаданных ЭлД.

5 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.

6 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.

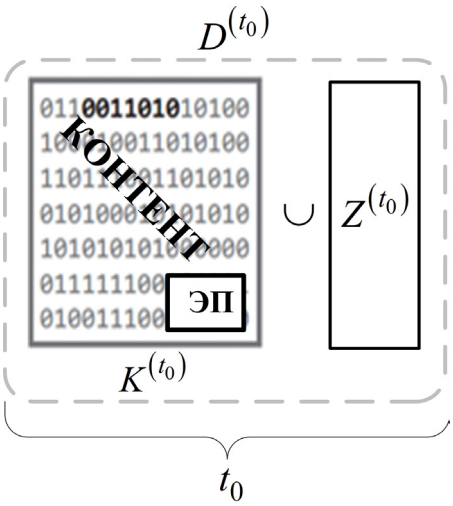


Рис. 2. Структура модели формирования статических метаданных электронного документа

Назначение метаданных делопроизводственных документов не исчерпывается целями поиска информации и требует наличия слоя динамических метаданных по следующим причинам [3].

Во-первых, официальный управленческий документ должен иметь метаданные, отражающие операции управленческой деятельности, то есть контекст создания, получения и использования документа и связи между его отдельными компонентами. Такие метаданные особенно необходимы для контроля статуса, структуры и целостности документа в любое определенное время, а также для показа его связей с другими документами (см. сноску [5]).

Во-вторых, метаданные должны документировать управленческий контекст, содержание, структуру и представление документа не только в момент создания документа или включения его в систему, но и после этого документировать управленческие процессы, в которых записи постоянно используются, включая изменения в содержании, структуре и представлении[7].

В соответствии с формулой (1), изменения ЭлД с учетом формирования динамических метаданных, в алгебраическом виде могут быть представлены как:

$$\begin{aligned} D^{(t_1)} &= K^{(t_1)} \cup Z^{(t_1)}; \\ D^{(t_2)} &= K^{(t_2)} \cup \left(Z^{(t_1)} \cup Z^{(t_2)} \right); \\ &\vdots \\ D^{(t_n)} &= K^{(t_n)} \cup \left(\bigcup_{i=1}^{n} Z^{(t_i)} \right), \end{aligned} \qquad (3)$$

где где n конечный момент дискретного времени редактирования ЭлД.

На рис. 3 представлена структура модели формирования динамических метаданных ЭлД.

Таким образом, метаданные придают ЭлД дополнительную ценность, что делает управление метаданными одним из важнейших процессов управления документацией организации. При этом, руководствуясь требованиями вышеназванного стандарта необходимо отметить, что метаданными документа следует управлять, как управлять и самим документом, поскольку они должны быть защищены от утраты или несанкционированного изменения или удаления и сохранены либо уничтожены в соответствии с установленными требованиями.

Анализ объекта исследования

Рассмотрим процесс формирования и существующие способы защиты метаданных ЭлД в современных АИС ЭД на примере системы «БЮРОКРАТЪ»[8].

Метаданные ввода документов в систему формируются на этапе создания контента ЭлД (статические) и фиксируются в регистрационно-контрольной карточке документа (РККД), а затем продолжают накапливаться и дополняться в течение всего жизненного цикла ЭлД, осуществляя, тем самым, фиксацию процессов управ-

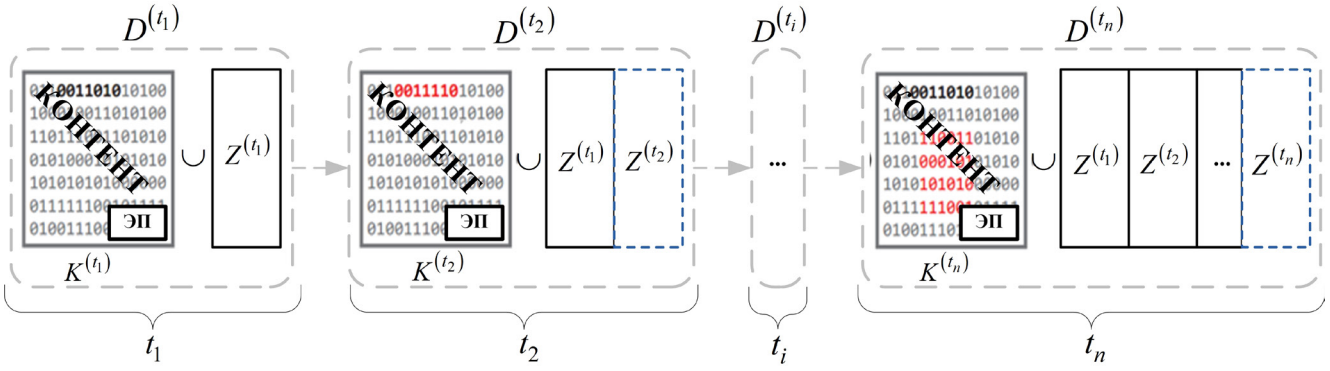


Рис. 3. Структура модели формирования динамических метаданных электронного документа

7 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.

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

ления документами (динамические). Хранение контента и РККД к нему в пределах установленных сроков обеспечивает подсистема хранения, представляющая собой локальную базу данных (ЛБД), поиск необходимой информации в которой осуществляется посредством метаданных, содержащихся в РККД.

Механизмы защиты информации, хранящейся в ЛБД, обеспечивает подсистема защиты информации. При этом метаданные, содержащиеся в РККД и контент ЭлД защищаются посредством разграничения доступа к документам базы данных, а защита контента ЭлД, кроме того обеспечивается средствами электронной подписи (ЭП), при этом влияние на контент ЭлД может оказывать только автор, а на РККД все, кто исполняет функции агента (см. сноску [6]).

На рис. 4 представлена существующая модель защиты ЭлД, обрабатываемых АИС ЭД.

реквизитную части не вносилось никаких изменений[9,10].

На практике, целостность ЭлД определяется совпадением хэш-кодов отправленного и полученного ЭлД, то есть целостностью файла ЭлД. При этом в основе алгоритмов ЭП лежат криптографические методы, основанные на использовании математических функций, которые просто вычислять в одном направлении и тяжело в другом (односторонние функции).

Вместе с тем, единственным механизмом обеспечения защиты метаданных ЭлД является функция разграничения доступа к ЛБД, в которой осуществляется их хранение. Таким образом, данный факт вызывает расхождение с положениями действующих нормативных документов по управлению документами (см. сноску [5]), выражающееся в более надежной защите только контента документа в отрыве от его метаданных, что противоречит самому определению состава ЭлД. Следствием

Рис. 4. Существующая модель защиты электронных документов, обрабатываемых АИС ЭД

Именно применение ЭП, основанной на криптографических методах позволяет обеспечить требуемый уровень доверия к ЭлД и, как следствие, его правовой статус [4]. ЭП позволяет обеспечить следующие свойства ЭлД:

1) целостность документа;
2) аутентификацию источника документа (авторство);
3) неотрицаемость автора от подписания документа;
4) защиту документа от возможной подделки.

Существующее законодательство дает следующее определения понятию «целостность» применимо к документированной информации:

целостность документа – состояние документа, при котором после его выпуска ни в содержательную, ни в

такой организации защиты являются соответствующие угрозы информационной безопасности, которые могут быть вызваны действиями злоумышленника.

Анализ угроз безопасности информации в АИС показывает, что к актуальным угрозам относятся внутренние угрозы (преднамеренные несанкционированные

9 ГОСТ 2.051-2013 Единая система конструкторской документации. Электронные документы. Общие положения. – М.: Стандартинформ, 2014. – 13 с.

10 ГОСТ Р 7.0.8-2013 Система стандартов по информации, библиотечному и издательскому делу. Делопроизводство и архивное дело. Термины и определения. – М.: Стандартинформ, 2014. – 13 с.

воздействия уполномоченных пользователей)[11,12] [5]. Результатом таких воздействий может стать преднамеренное несанкционированное изменение метаданных, что приведет к нарушению их целостности, и как следствие, потере управления над ЭлД, обрабатываемых АИС[13] [6-8]. Одной из мер обеспечения защищенности данных, является защита их целостности[14].

Методы обеспечения целостности можно разделить на криптографические и некриптографические. Проблеме обеспечения целостности данных некриптографическими методами посвящены научные исследования ученых M. Nicolett, Steven T. Eckmann, Jiawei Han, Девянина П.Н., Дубровина А.С., Трошина С.В. и других. Над разработкой криптографических методов обеспечения целостности данных работали такие ученые, как Atsushi Harada, M. Bellare, E. Biham, F. Mendel, Нураев И.Ю., Фазлиахметов Т.И., Рябков Н.С., Панасенко С.П. и другие.

Необходимо отметить, что недостатки присутствуют в обоих случаях. В первом, злоупотребление уполномоченных пользователей своими правами приводит к уничтожению (модификации) отдельных областей хранения данных, относящихся к действиям администратора. Во втором, существует возможность незаконной модификации данных со стороны лица, являющегося владельцем криптографического ключа.

Известно, что криптографические методы защиты информации являются наиболее надежным средством защиты данных. Проведенный анализ существующих способов контроля целостности данных позволил установить, что в их основе лежит применение криптографической хэш-функции[15] [9–12]. Но наибольший интерес для решения вышеназванной проблемы по организации защиты метаданных ЭлД, обрабатываемых АИС ЭД, представляет метод «однократной записи» (см. сноску [3]), а также способ аутентификации сообщений HMAC (см. сноску [4]).

В методе «однократной записи» используются две ЭП для каждой записи, чтобы один законный пользователь, который имеет криптографический ключ, не имел возможности стереть (модифицировать) уже подписанную

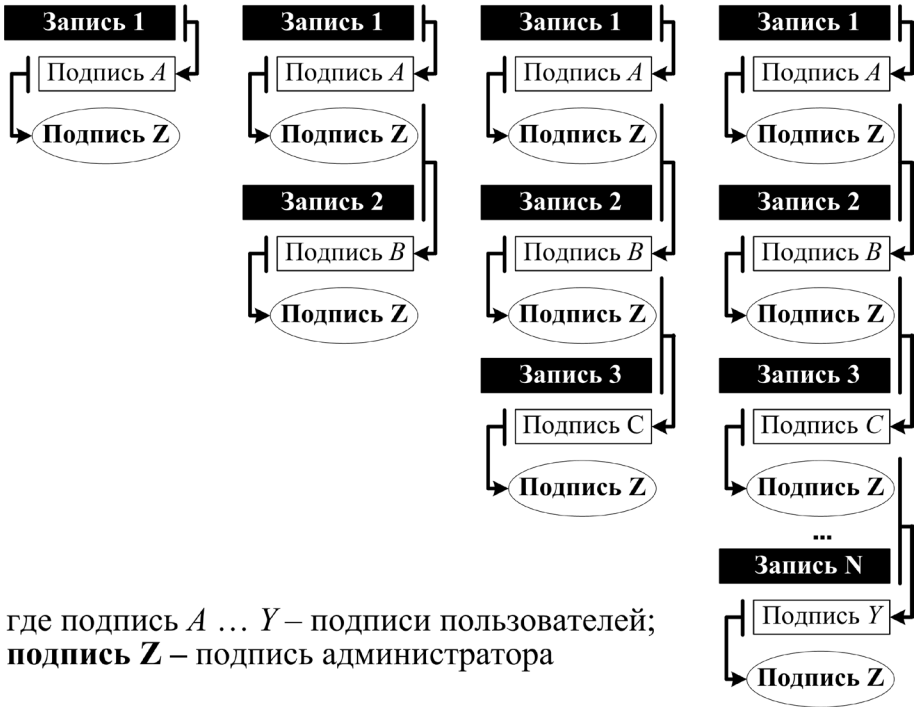


Рис. 5. Схема функционирования метода «однократной записи» [13]

(защищенную) запись, переписать и добавить подпись еще раз. Таким образом, каждая запись подписывается пользователем и администратором системы (рис. 5). Недостатком данного метода является тот факт, что внутренним нарушителем может быть сам администратор.

В способе аутентификации сообщений HMAC, полученный код аутентичности позволяет убедиться в том,

11 ГОСТ Р 15408-2013 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные компоненты безопасности. – М.: Стандартинформ, 2014. – 161 с

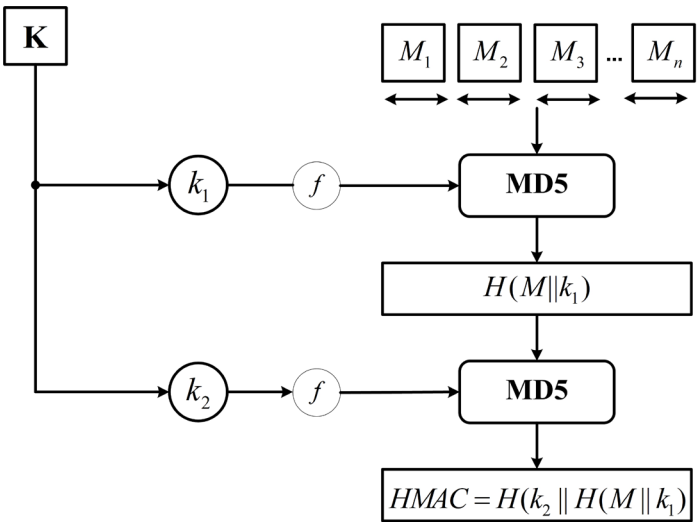
12 Аналитический центр группы компаний InfoWatch (АО «Инфовотч»). Отчет: утечки данных. Россия. 2018 год. http://www.infowatch.ru/resources/analytics/reports/russia2018.

13 Аналитический центр группы компаний InfoWatch (АО «Инфовотч»). Аналитика: Шанхайский университет раскрыл терабайты электронной почты. 2019. https://www.infowatch.ru/analytics/data-loss-cases/15714.

14 Методический документ. Меры зашиты информации в государственных информационных системах: утв. директором ФСТЭК 11.02.2014 // ФСТЭК России, 2014. – 176 с.

15 ГОСТ Р 34.11-2012 Информационная технология. Криптографическая защита информации. Функция хэширования. – М.: Изд-во стандартов, 2012. – 16 с.

что данные не изменялись каким бы то ни было способом с тех пор, как они были созданы, переданы или сохранены доверенным источником. Для такого рода проверки необходимо, чтобы, например, две доверяющие друг другу стороны заранее договорились об использовании секретного ключа, который известен только им. Тем самым гарантируется аутентичность источника и сообщения (рис. 6).



где **K** – множество секретных (внешних) ключей;
k_1, k_2 – секретные (внешние) ключи;
f – функция сжатия;
$M_1, M_2, M_3, \ldots, M_n$ – части сообщения M;
MD5 – алгоритм хеширования;
H – функция хеширования;
|| – операция конкатенации

Рис. 6. Схема функционирования способа аутентификации сообщений HMAC

Несмотря на несомненные достоинства этих способов у них имеется общий недостаток, выражающийся в отсутствии технической возможности локализации записей данных с признаками нарушения целостности, при реализации деструктивных воздействий уполномоченными пользователями на АИС ЭД.

Таким образом, для устранения выявленных недостатков в организации защиты метаданных ЭлД, обрабатываемых АИС ЭД, необходимо разработать такой способ криптографического контроля целостности, который позволит их устранить, учитывая при этом плюсы ранее известных способов.

Постановка задачи

При формализации задачи исследования необходимо [2], используя математическую запись, сформулировать суть решаемой задачи, критерий ее решения, входные и выходные данные, существенные факторы и условия задачи.

Для формализованного описания подсистемы защиты информации (ЗИ) АИС ЭД воспользуемся теоретико-множественным подходом, получившим широкое распространение при описании различных технических систем [14, 15].

Дано:

Пусть задана математическая модель подсистемы ЗИ АИС ЭД: $S=\{T, X, Y, R, Z, \delta, \varphi\}$, где

T – множество моментов времени в которые наблюдается подсистема ЗИ АИС ЭД, $t_i \in T$, $i = 0, n$; t_0 – начало эксплуатации АИС ЭД, t_n – конец эксплуатации АИС ЭД;

X – множество входных инициирующих событий (воздействий) на подсистему ЗИ АИС ЭД;

Y – множество функциональных состояний подсистемы ЗИ АИС ЭД;

R – множество выходных качественных состояний, обрабатываемых ЭлД;

Z – множество метаданных ЭлД, изменяющихся под влиянием инициирующих событий (воздействий) на подсистему ЗИ АИС ЭД;

δ – оператор переходов, отражающий механизм изменения функционального состояния Y подсистемы ЗИ АИС ЭД под воздействием внутренних и внешних инициирующих событий X;

ϕ – оператор выходов, описывающий механизм формирования выходных параметров R ЭлД, как реакции подсистемы ЗИ АИС ЭД на внутренние и внешние инициирующие события X.

Операторы δ и ϕ реализуют отображения:

$$\delta : T \times X \times Y \to Y; \quad (4)$$

$$\phi : T \times X \times Y \to R. \quad (5)$$

Всякое состояние R ЭлД характеризуется в каждый момент времени $t_i \in T$ множеством метаданных Z, изменяющихся под влиянием инициирующих событий (воздействий) X на подсистему ЗИ АИС ЭД. В качестве инициирующих событий (воздействий) X рассматриваются запросы уполномоченных пользователей на выполнение некоторой функции, реализующей деструктивные воздействия на метаданные ЭлД.

Ограничением модели подсистемы ЗИ АИС ЭД является то, что элементы множества R включает только два состояния: «1» – состояние ЭлД, при котором целостность метаданных обеспечена; «0» – состояние ЭлД, при котором целостность метаданных нарушена, что может быть записано как

$$R\left(Y,\ Z\left(X\right)\right)=$$

$$=\begin{cases}1-\text{состояние целостности метаданных ЭлД}\\0-\text{состояние нарушения целостности метаданных ЭлД.}\end{cases}$$

Переход ЭлД в процессе функционирования подсистемы ЗИ АИС ЭД в состояние «0» следует рассматривать как событие, характеризующее нарушение функционирования АИС ЭД. В то же время нахождение ЭлД в состоянии «1» следует рассматривать как событие, характеризующее состояние нормального функционирования АИС ЭД.

В общем случае вероятность обеспечения целостности ЭлД, обрабатываемого АИС ЭД, определяется формулой:

$$P_{(1)}=\prod_{k=1}^{n}P_{(1)}^{(k)},\qquad(6)$$

где $P_{(1)}^{(k)}$ – вероятность обеспечения целостности ЭлД при реализации *k*-ого инициирующего события *X* в подсистеме ЗИ АИС ЭД; n – общее количество инициирующих событий X, реализуемых в подсистеме ЗИ АИС ЭД.

Соответственно, вероятность нарушения целостности ЭлД, обрабатываемого АИС ЭД, определяется формулой:

$$P_{(0)}=1-P_{(1)}\qquad(7)$$

В этом случае критерий качества функционирования подсистемы ЗИ АИС ЭД определяться следующим выражением:

$$P_{(0)}<P_{\text{порог.}},\qquad(8)$$

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

Исходя из чего, в качестве показателя эффективности функционирования подсистемы ЗИ АИС ЭД примем вероятность нарушения целостности ЭлД $P_{(0)}$, вызванной посредством деструктивных воздействий уполномоченных пользователей на метаданные ЭлД.

С учетом существующего положения дел в качестве критерия оценки уровня защищенности метаданных ЭлД рассматривается следующее условие:

$$G:P_{(0)}<P_{(0)}^{\text{прототипа}},\qquad(10)$$

где $P_{(0)}^{\text{прототипа}}$ – вероятность нарушения целостности ЭлД, вызванная посредством деструктивных воздействий уполномоченных пользователей на метаданные ЭлД при использовании известных способов контроля целостности данных (хэш-функция).

Требуется разработать такой способ контроля целостности метаданных ЭлД

$$Q=\left\{Md,Al,Mt\right\},$$

состоящий из моделей Md, алгоритмов Al и методики Mt, который позволит при исходных данных найти вектор Y^* множества функциональных состояний подсистемы ЗИ АИС ЭД, позволяющий при заданных ограничениях повысить уровень защищенности *G* метаданных ЭлД, обрабатываемых АИС ЭД.

Математически формулировка задачи имеет вид:

$$Q:\arg\left(R\left(Y^*,\ Z\left(X\right)\right)\right)\rightarrow$$

$$\rightarrow P_{(0)}\left(R\left(Y,\ Z\left(X\right)\right)\right)<P_{(0)}^{\text{прототипа}}\qquad(11)$$

при ограничениях $C(F_{\text{допустимый}},\ T_{\text{заданные}})$.

В качестве ограничений *C* могут выступать требования:

- расходуемый ресурс не превышает допустимого $F_{\text{допустимый}}$;
- затраты времени не превышают директивных $T_{\text{заданные}}$.

Математическая модель криптографического рекурсивного 2-D контроля целостности метаданных электронных документов

На основании проведенного анализа существующих способов контроля целостности данных, в целях устранения выявленных недостатков было принято решение использовать технологию цепной записи данных, представляющую собой реестр, данные в который записываются блоками, таким образом, что каждый новый блок включает информацию о предыдущем блоке[16].

Под реестром понимается совокупность данных, структурированных и хранимых в целях их учета, поиска, обработки и контроля, которыми и являются метаданные ЭлД. Причем допускается внесение информации в блоки (записи метаданных) без изменения ранее внесенной информации, что представляет собой динамический реестр. При этом связь с блоками (записями метаданных) будет обеспечиваться за счет использования криптографической хэш-функции. Применительно к задаче повышения защищенности метаданных технология цепной записи данных выглядит, как показано на рис. 7 [1].

На основе данной технологии строится цепочка доверия (криптографическая рекурсивная двухмерная последовательность метаданных ЭлД), представляющая собой связь с предыдущим блоком после проведенной транзакции (изменения метаданных в РККД), чтобы информацию внутри транзакций нельзя было подделать, каждая транзакция внутри блока подверга-

16 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.

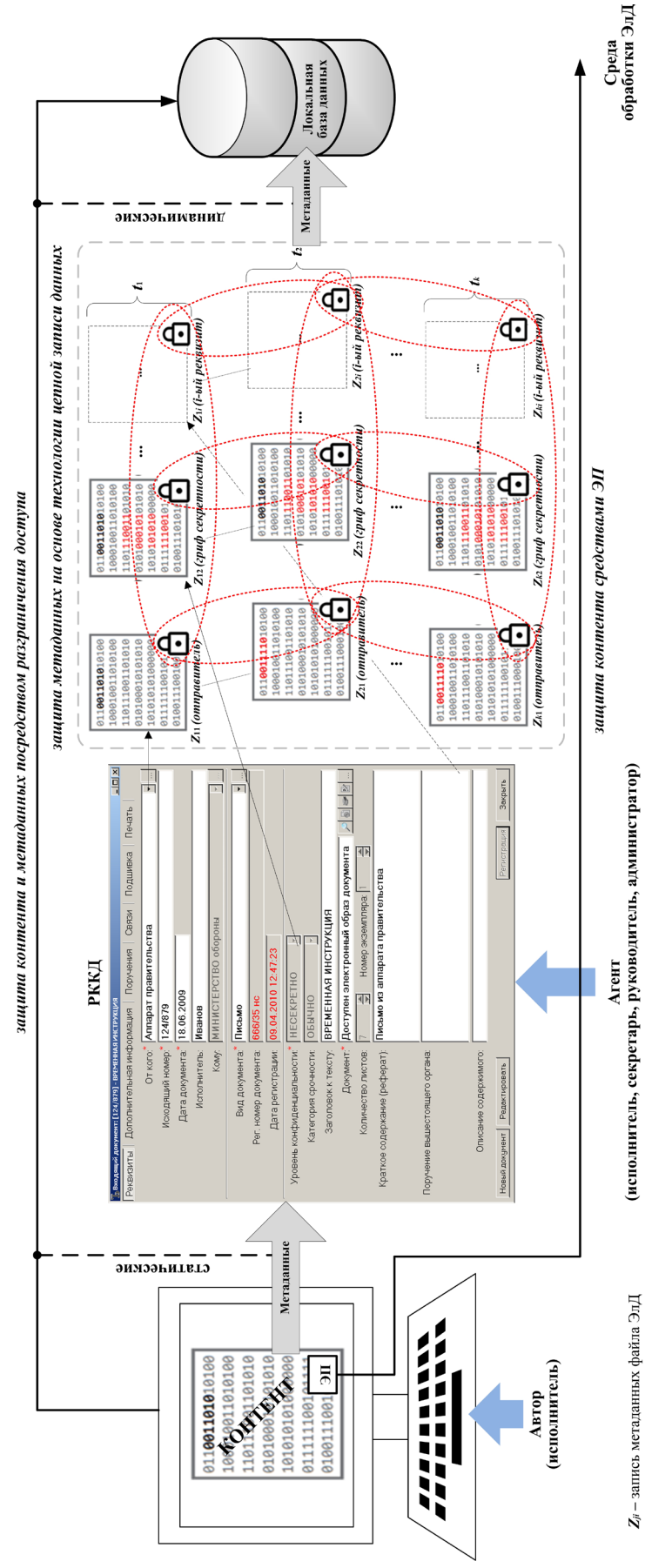


Рис. 7. Концептуальное представление модели формирования метаданных электронного документа на основе технологии цепной записи данных

ется криптографическому преобразованию. Внесение каких-либо изменений в записи метаданных без выполнения процедуры модификации всей цепочки доверия (криптографической рекурсивной двухмерной последовательности метаданных ЭлД), начиная с того момента времени, в который были внесены изменения, невозможно [16].

Целью предлагаемого технического решения является повышение уровня защищенности метаданных ЭлД, обрабатываемых АИС ЭД, с возможностью контроля их целостности, а также обнаружения и локализации номеров несанкционированно модифицированных записей метаданных, в случае нарушения их целостности уполномоченными пользователями (инсайдерами).

Данное техническое решение осуществляется следующим образом [17].

Множество ключей $\mathbf{K}_U$ разбивается на два подмножества:

$\mathbf{K}_U \in \{\mathbf{K}_U^{(1)}, \mathbf{K}_U^{(2)}, \mathbf{K}_U^{(3)}\}$ и $\mathbf{K}_U^* \in \{\mathbf{K}_U^{*(1)}, \mathbf{K}_U^{*(2)}, \mathbf{K}_U^{*(3)}\}$ содержащие три группы ключей $\mathbf{K}_U^{(1)}$ – внутренние системные ключи, $\mathbf{K}_U^{(2)}$ – внешние ключи администратора системы, $\mathbf{K}_U^{(3)}$ – внешние ключи оператора системы.

При этом каждые подмножества $\mathbf{K}_U^{(q)} \in \{k_1^{(q)}, k_2^{(q)}, \ldots, k_\varsigma^{(q)}\}$ и $\mathbf{K}_U^{*(q)} \in \{k_1^{*(q)}, k_2^{*(q)}, \ldots, k_\varsigma^{*(q)}\}$,

где $q = 1, \ldots, 3$, для всех $U = 1, \ldots, \varsigma$ (рис.8).

При выполнении операции записи и редактирования ЭлД в моменты времени $t_1, t_2, \ldots, t_k$ в памяти системы обработки данных формируются строки:

$\mathbf{m}(t_1) = [z_{11} \ \ldots \ z_{1i}]$, $\mathbf{m}(t_2) = [z_{21} \ \ldots \ z_{2i}]$, …,

$\mathbf{m}(t_k) = [z_{k1} \ \ldots \ z_{ki}]$, содержащие записи метаданных $z_{j1}, z_{j2}, \ldots, z_{ji}$ для всех $j = 1, \ldots, k$ и столбцы:

$$\mathbf{M}_1(t_1, t_2, \ldots, t_k) = [z_{11} \ z_{21} \ \ldots \ z_{k1}],$$
$$\mathbf{M}_2(t_1, t_2, \ldots, t_k) = [z_{12} \ z_{22} \ \ldots \ z_{k2}],$$
$$\vdots$$
$$\mathbf{M}_i(t_1, t_2, \ldots, t_k) = [z_{1i} \ z_{2i} \ \ldots \ z_{ki}],$$

являющиеся реквизитами ЭлД, обрабатываемых АИС ЭД.

Над записями $z_{11}, \ldots, z_{1i}$ метаданных в соответствующих столбцах в момент времени t_1 выполняются операции криптографического преобразования (рис. 9):

$f^{k_\varsigma^{(1)}}(z_{11}), \ldots, f^{k_\varsigma^{(1)}}(z_{1i})$, на ключах $k_\varsigma^{(1)} \in \mathbf{K}_U^{(1)}$, в результате чего образуются значения сигнатур $h_{11}, \ldots, h_{1i}$.

Над каждой парой полученных значений сигнатур $h_{11}, \ldots, h_{1i}$ и записей метаданных $z_{21}, \ldots, z_{2i}$, измененных в момент времени t_2, выполняется операция конкатенации: $z_{21} \| h_{11}, \ldots, z_{2i} \| h_{1i}$, над результатами которой выполняются операции

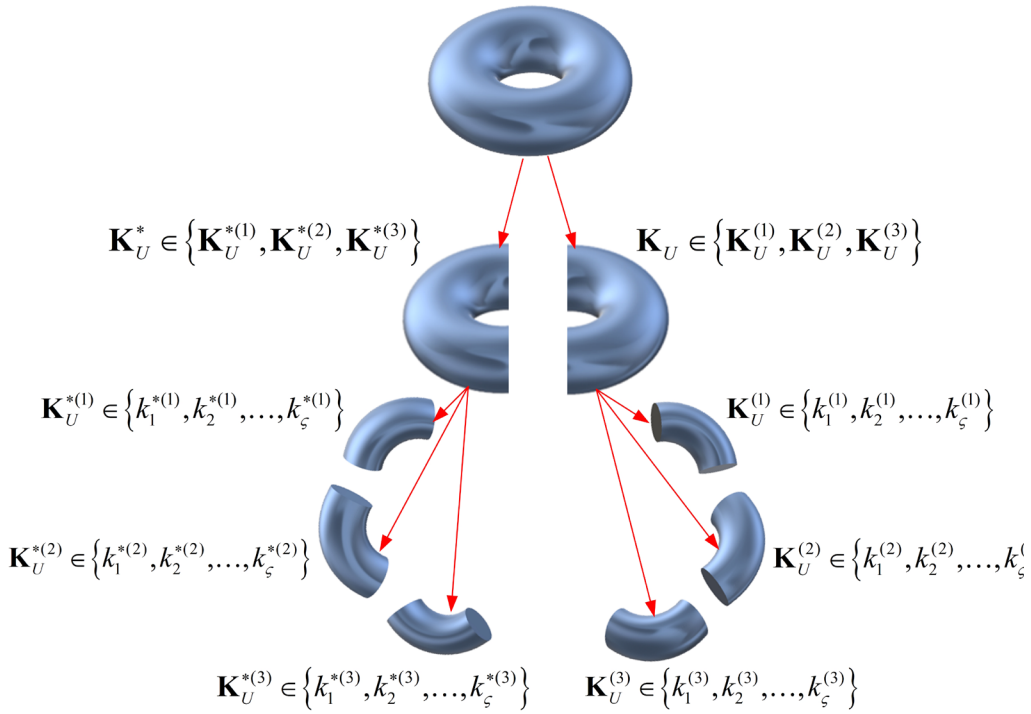


Рис. 8. Схема разбиения множества ключей $\mathbf{K}_U$

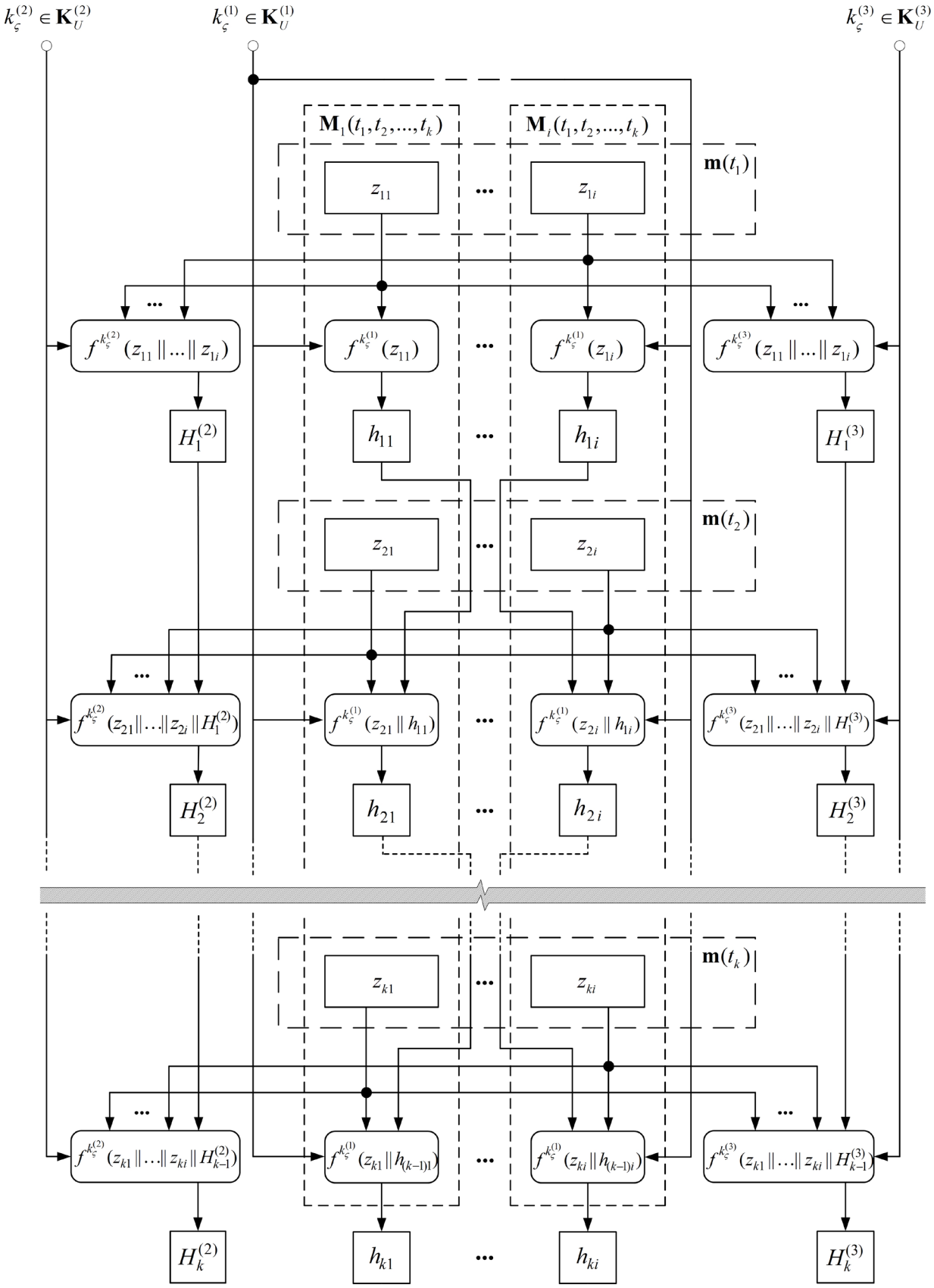


Рис. 9. Функциональная схема криптографического рекурсивного 2-D контроля целостности метаданных электронных документов, обрабатываемых автоматизированными информационными системами электронного документооборота

криптографического преобразования (рис. 9):

$$f^{k_\varsigma^{(1)}}\left(z_{21}\|h_{11}\right),\ldots,f^{k_\varsigma^{(1)}}\left(z_{2i}\|h_{1i}\right).$$

После чего операции над записями метаданных выполняются в аналогичном порядке (рис.10) внутри каждого столбца:

$$\mathbf{M}_1(t_1,\ t_2,\ldots,\ t_k)=\left[z_{11}\quad z_{21}\quad\ldots\quad z_{k1}\right],$$
$$\mathbf{M}_2(t_1,\ t_2,\ \ldots,\ t_k)=\left[z_{12}\quad z_{22}\quad\ldots\quad z_{k2}\right],$$
$$\vdots$$
$$\mathbf{M}_i(t_1,\ t_2,\ \ldots,\ t_k)=\left[z_{1i}\quad z_{2i}\quad\ldots\quad z_{ki}\right],$$

в соответствии с моментами времени $t_3,\ t_4,\ \ldots,\ t_k$.

В тоже время в строке $\mathbf{m}(t_1)=\left[z_{11}\quad\ldots\quad z_{1i}\right]$, в момент времени t_1, выполняются операции криптографического преобразования всех записей $z_{11},\ \ldots,\ z_{1i}$ метаданных строки (рис. 9):

$$f^{k_\varsigma^{(2)}}\left(z_{11}\|\ldots\|z_{1i}\right)\text{ на ключах }k_\varsigma^{(2)}\in\mathbf{K}_U^{(2)},$$
$$f^{k_\varsigma^{(3)}}\left(z_{11}\|\ldots\|z_{1i}\right)\text{ на ключах }k_\varsigma^{(3)}\in\mathbf{K}_U^{(3)},$$

в результате которых, образуются значения сигнатур $H_1^{(2)}$ и $H_1^{(3)}$ соответственно.

Над полученными сигнатурами и последующими записями $z_{2l},\ \ldots\ z_{2i}$ метаданных строки $\mathbf{m}(t_2)=[z_{21}\ \ldots\ z_{2i}]$, измененными в момент времени t_2, выполняются операции конкатенации:

$$z_{21}\|\ldots\|z_{2i}\|H_1^{(2)}\text{ и }z_{21}\|\ldots\|z_{2i}\|H_1^{(3)},$$

над результатами которых производится операция криптографического преобразования (рис. 9):

$$f^{k_\varsigma^{(2)}}\left(z_{21}\|\ldots\|z_{2i}\|H_1^{(2)}\right)\text{ на ключах }k_\varsigma^{(2)}\in\mathbf{K}_U^{(2)},$$
$$f^{k_\varsigma^{(3)}}\left(z_{21}\|\ldots\|z_{2i}\|H_1^{(3)}\right)\text{ на ключах }k_\varsigma^{(3)}\in\mathbf{K}_U^{(3)}.$$

По мере поступления новых записей метаданных операции повторяются в аналогичном порядке (рис. 10) в соответствии с моментами времени $t_3,\ t_4,\ \ldots,\ t_k$.

Все записи метаданных:

$$\left[z_{11}\quad\ldots\quad z_{1i}\right],\ \ldots,\ \left[z_{k1}\quad\ldots\quad z_{ki}\right]$$

и соответствующие сигнатуры:

$$H_1^{(2)},\ h_{11},\ \ldots,\ h_{1i},\ H_1^{(3)};\ \ldots;$$
$$H_k^{(2)},\ h_{k1},\ \ldots,\ h_{ki},\ H_k^{(3)}$$

сохраняются в памяти системы обработки данных в виде таблицы данных (табл. 1).

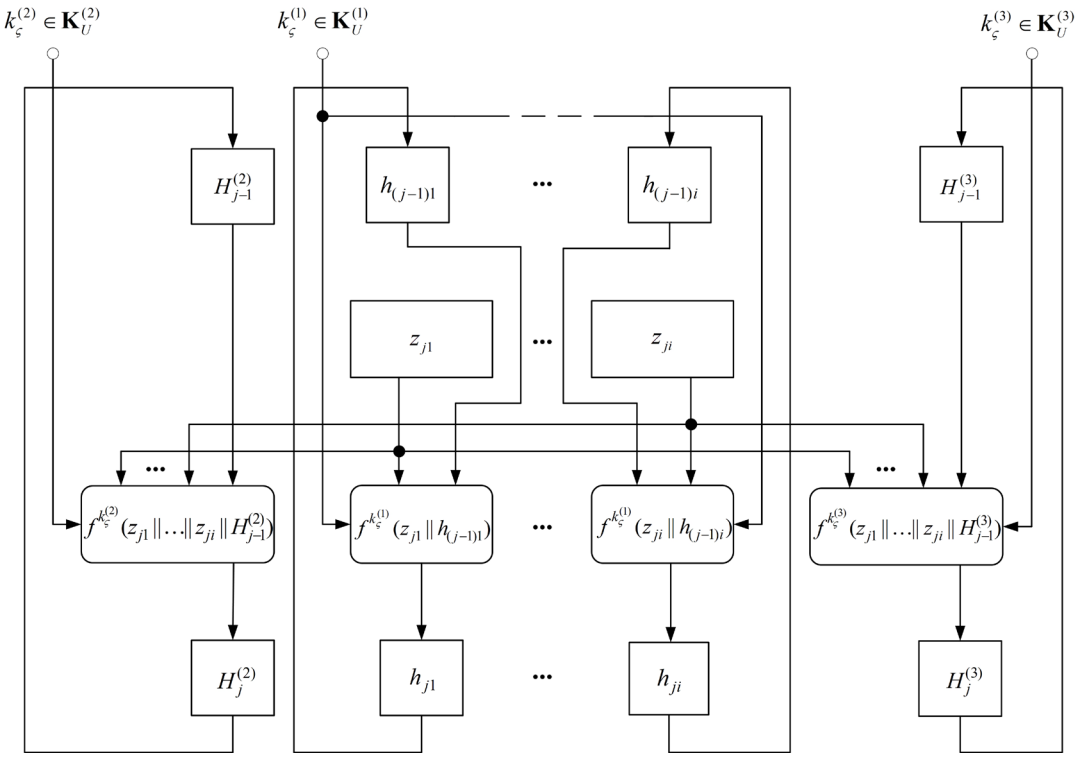


Рис. 10. Схема, поясняющая цикличность выполнения операций криптографического преобразования метаданных электронных документов

Особенностью разработанного решения является возможность его реализации в двух вариантах.

В первом случае, операция криптографического преобразования $f^{k_\varsigma^{(q)}}\left(z_{ji} \| h_{(j-1)1}\right)$; $f^{k_\varsigma^{(q)}}\left(z_{j1} \| \ldots \| z_{ji} \| H_{j-1}^{(q)}\right)$ является ключевой хэш-функцией (рис. 11), причем как на этапе подготовки, так и на этапе контроля целостности записей метаданных выполняется равенство $\mathbf{K}_U^{(q)} = \mathbf{K}_U^{*(q)}$, где $q = 1, \ldots, 3$ для всех $U = 1, \ldots, \varsigma$.

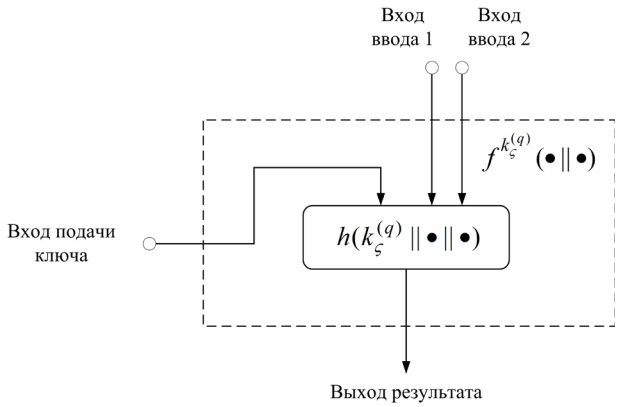


Рис. 11. Вариант реализации функции криптографического преобразовани $f^{k_\varsigma^{(q)}}(\bullet \| \bullet)$ посредством ключевой хэш-функции

Во втором случае, операция криптографического преобразования $f^{k_\varsigma^{(q)}}\left(z_{ji} \| h_{(j-1)1}\right)$; $f^{k_\varsigma^{(q)}}\left(z_{j1} \| \ldots \| z_{ji} \| H_{j-1}^{(q)}\right)$ может являться электронной подписью (рис. 12), включающей в себя последовательно выполняемые преобразования бесключевой хэш-функции и функцию асимметричного криптографического преобразования, причем $\mathbf{K}_U^{(q)} \neq \mathbf{K}_U^{*(q)}$, то есть на этапе подготовки записей метаданных ЭлД используется подмножество ключей $\mathbf{K}_U^{(q)}$, а на этапе контроля целостности записей метаданных используется подмножество ключей $\mathbf{K}_U^{*(q)}$.

Контроль целостности записей метаданных осуществляется на основе извлечения из таблицы данных сигнатур:

$$H_1^{(2)*}, h_{11}^*, \ldots, h_{1i}^*, H_1^{(3)*}; \ldots;$$
$$H_k^{(2)*}, h_{k1}^*, \ldots, h_{ki}^*, H_k^{(3)*}$$

и записей:

$$\left[z_{11}^* \quad \ldots \quad z_{1i}^*\right], \ldots, \left[z_{k1}^* \quad \ldots \quad z_{ki}^*\right],$$

прошедших процедуру хранения и подлежащих контролю целостности, над которыми производятся повторные операции криптографического преобразования.

Таблица 1

Данные, сохраненных записей метаданных и их значений сигнатур

Моменты времени t редактирования метаданных	Записи метаданных и значения сигнатур		
	на внутренних ключах системы $k_\varsigma^{(1)} \in \mathbf{K}_U^{(1)}$	на внешних ключах администратора $k_\varsigma^{(2)} \in \mathbf{K}_U^{(2)}$	на внешних ключах оператора $k_\varsigma^{(3)} \in \mathbf{K}_U^{(3)}$
t_1	z_{11} ... z_{1i} h_{11} ... h_{1i}	z_{11} ... z_{1i} $H_1^{(2)}$	z_{11} ... z_{1i} $H_1^{(3)}$
t_2	z_{21} ... z_{2i} h_{21} ... h_{2i}	z_{21} ... z_{2i} $H_2^{(2)}$	z_{21} ... z_{2i} $H_2^{(3)}$
⋮	⋮	⋮	⋮
t_k	z_{k1} ... z_{ki} h_{k1} ... h_{ki}	z_{k1} ... z_{ki} $H_k^{(2)}$	z_{k1} ... z_{ki} $H_k^{(3)}$

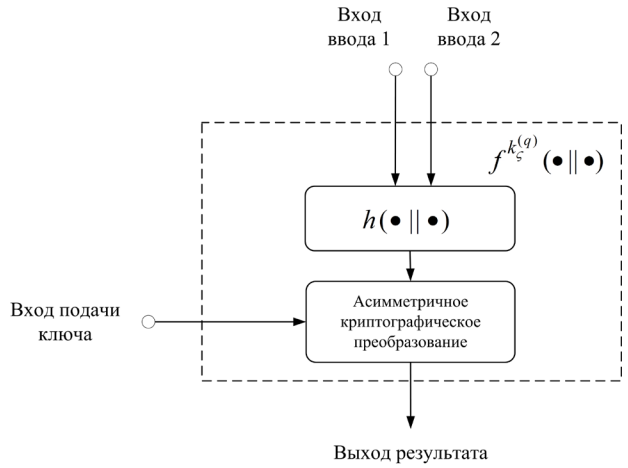


Рис. 12. Вариант реализации функции криптографического преобразования $f^{k_\varsigma^{(q)}}(\bullet \| \bullet)$ посредством электронной подписи

В результате чего вновь вычисленные сигнатуры:

$H_1^{(2)**}, h_{11}^{**}, \ldots, h_{1i}^{**}, H_1^{(3)**}; \ldots;$

$H_k^{(2)**}, h_{k1}^{**}, \ldots, h_{ki}^{**}, H_k^{(3)**}$

попарно сравниваются с ранее извлеченными:

$H_1^{(2)*}, h_{11}^{*}, \ldots, h_{1i}^{*}, H_1^{(3)*}; \ldots;$

$H_k^{(2)*}, h_{k1}^{*}, \ldots, h_{ki}^{*}, H_k^{(3)*}.$

Заключение об отсутствии нарушения целостности сигнатур делается при выполнении равенств:

$$H_j^{(q)**} = H_j^{(q)*}; \quad h_{ji}^{(q)**} = h_{ji}^{(q)*},$$

где $q = 1, \ldots, 3, \ j = 1, \ldots, k,$ в противном случае делается заключение о нарушении целостности для соответствующих номеров сигнатур.

Используя теорию графов, разработаем математическую модель описываемого решения.

Любой поэтапно рассматриваемый процесс со случайными исходами на отдельных этапах может быть представлен некоторым ориентированным графом, то есть перечислением вершин графа операций, подлежащих выполнению, и указанием последовательности перехода от одной операции к другой, что означает задание ребер графа и выбор направлений на них. Одна из вершин графа соответствует началу работ, другая их окончанию. Тогда реализация процесса соответствует блужданиям по графу, ведущим из начала в конец [18].

Пусть имеем ориентированный граф $G(X, E)$, обладающий следующими свойствами:

1) существует единственная вершина $x_0 \in X$, из которой дуги выходят;
2) существует единственная вершина $x_n \in X$, в которую дуги входят;
3) в графе отсутствуют замкнутые пути;

из любой вершины x_i существует путь, проходящий из x_0 в x_n, содержащий эту дугу.

Множество вершин такого графа $\{x_i\}$ называют событиями, а множество дуг $\{(x_i, x_j)\}$ – работами (обозначение и термины заимствованы из [19]). Граф, удовлетворяющий этим ограничениям, называется сетевым графом.

Воспользуемся предлагаемым графом, в целях описания процедуры контроля целостности метаданных ЭлД, обрабатываемых АИС ЭД (рис. 13, 14). Для чего сопоставим вершины графа с элементами, разработанного решения:

x_0 – вершина графа, соответствующая записям (строкам записей) метаданных z_{ji}; $\left[z_{j1} \ \ldots \ z_{ji}\right]$, формируемым в процессе создания и изменения ЭлД;

x_1 – вершина графа, соответствующая вычисленным сигнатурам h_{ji}; $H_j^{(q)}$ записей (строк записей) метаданных z_{ji}; $\left[z_{j1} \ \ldots \ z_{ji}\right]$;

x_2 – вершина графа, соответствующая записям (строкам записей) метаданных z_{ji}^*; $\left[z_{j1}^* \ \ldots \ z_{ji}^*\right]$, прошедшим процедуру хранения и подлежащих контролю целостности;

x_3 – вершина графа, соответствующая результатам сравнения вычисленных сигнатур $h_{ji}^{\sim}$; $H_j^{(q)\sim}$, где $h_{ji}^* = h_{ji}^{**}$; $H_{ji}^{(q)*} = H_{ji}^{(q)**}$ записей (строк записей) метаданных;

$\{(x_0, x_1)\}$ – операция f_1 криптографического преобразования вида: $f^{k_\varsigma^{(q)}}\left(z_{ji} \| h_{(j-1)i}\right)$, где q=1; $f^{k_\varsigma^{(q)}}\left(z_{j1} \| \ldots \| z_{ji} \| H_{j-1}^{(q)}\right)$, где q=2, 3;

$\{(x_0, x_2)\}$ – операция f_1 извлечения записей (строк записей) метаданных z_{ji}; $\left[z_{j1} \ \ldots \ z_{ji}\right]$ из таблицы данных;

$\{(x_1, x_3)\}$ – операция a_2 извлечения сигнатур h_{ji}; $H_j^{(q)}$ записей (строк записей) метаданных z_{ji}; $\left[z_{j1} \ \ldots \ z_{ji}\right]$ из таблицы данных;

$\{(x_2, x_3)\}$ – операция f_2 повторного криптографического преобразования вида: $f^{k_\varsigma^{(q)}}\left(z_{ji}^* \| h_{(j-1)i}^{**}\right)$, где q =1; $f^{k_\varsigma^{(q)}}\left(z_{j1}^* \| \ldots \| z_{ji}^* \| H_{j-1}^{(q)**}\right)$, где q =2, 3.

В таком случае предлагаемое решение можно представить в виде математической модели, которая представляет собой коммутативную диаграмму, описывающую процедуру контроля целостности метаданных ЭлД, обрабатываемых АИС ЭД.

Коммутативность означает, что для любых выбранных начального и конечного события, для соединяющих их ориентированных путей, композиция соответствующих путей морфизмов не зависит от выбора пути [20]:

$$f_2 \circ a_1 = a_2 \circ f_1. \qquad (12)$$

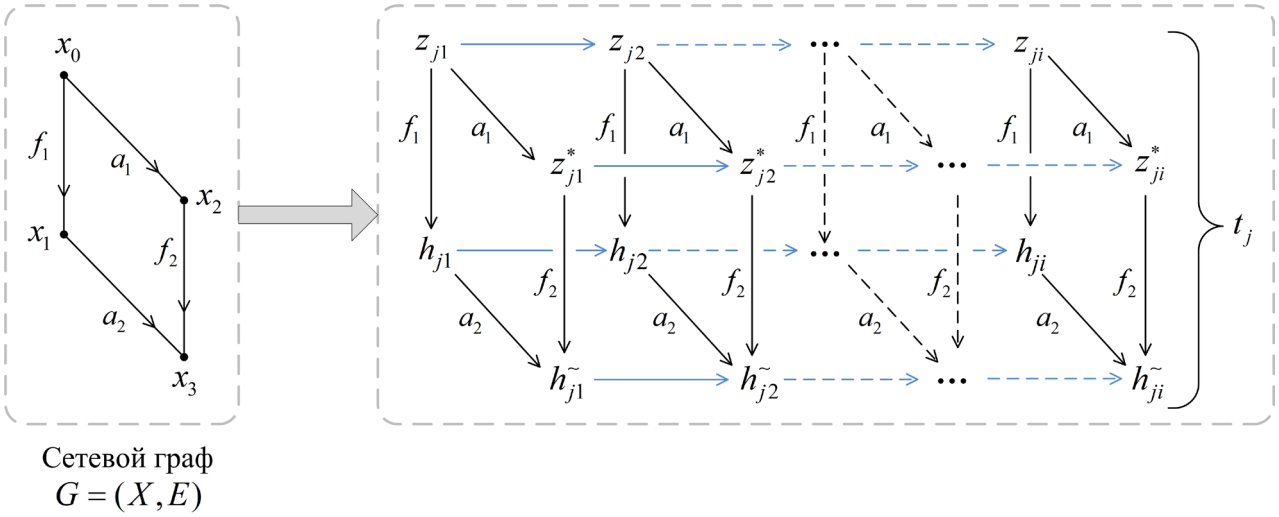


Рис. 13. Коммутативная диаграмма контроля целостности метаданных электронных документов для записей метаданных поэлементно

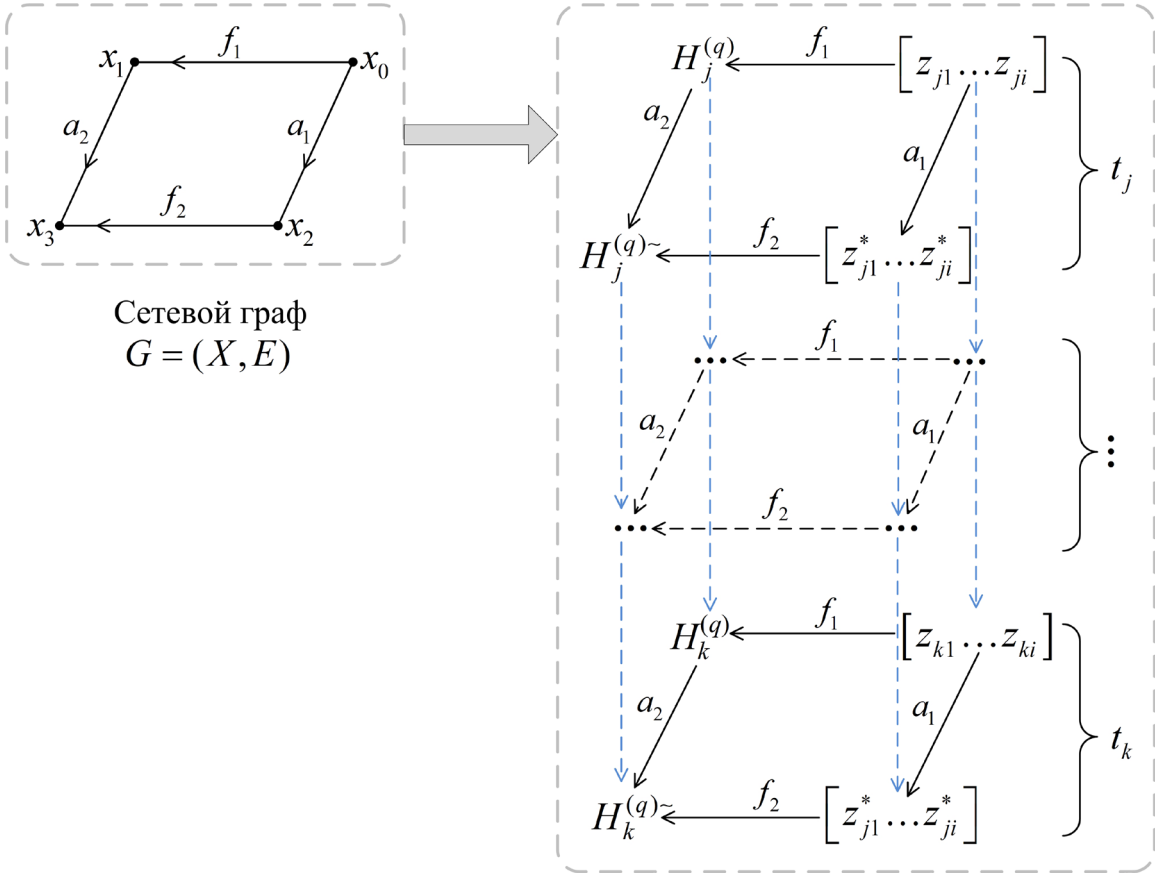


Рис. 14. Коммутативная диаграмма контроля целостности метаданных электронных документов для строк записей метаданных

Результатом вышеописанных операций станет сравнение извлеченных сигнатур $h^{*}_{ji}; H^{(q)*}_{j}$, прошедших процедуру хранения, и повторно вычисленных сигнатур $h^{**}_{ji}; H^{(q)**}_{j}$. При условии их равенства свойство коммутативности выполняется.

Данная математическая модель справедлива как для записей метаданных в столбцах (рис.13), так и для метаданных строк записей (рис.14).

Представленные диаграммы являются гомоморфизмами цепных комплексов, в которых каждый следующий сетевой граф оказывается коммутативным [21]:

$$f : A_n \to B_n; \quad \forall n \in \mathbb{N}. \tag{13}$$

Таким образом, *научная новизна моделей* заключается, в том числе, в применении математического аппарата теории графов для решения задачи контроля целостности метаданных ЭлД, обрабатываемых АИС ЭД, за счет выявленного свойства коммутативности, содержащегося в разрабатываемом решении.

Практическая значимость заключается в обеспечении возможности выявления модифицированных записей метаданных ЭлД, обрабатываемых АИС ЭД, в условиях преднамеренных и непреднамеренных воздействий уполномоченных пользователей (инсайдеров).

Выводы

Представленный способ контроля целостности данных, обрабатываемых АИС ЭД, учитывает динамику и непрерывность изменения метаданных ЭлД. Способ основан на последовательном использования криптографических преобразований (ключевой хэш-функции или ЭП), что позволило расширить функциональные возможности подсистемы ЗИ АИС ЭД за счет использования технологии цепной записи данных.

В отличие от известных вариантов реализации технологии «блокчейн» предложенное решение позволяет обеспечить процедуру контроля целостности данных, обрабатываемых ведомственными АИС ЭД, с учетом низкой интенсивности проводимых транзакций, а также малого количества автоматизированных рабочих мест.

Литература

1. Тали Д.И., Елисеев Н.И. Анализ процесса формирования и защиты метаданных электронных документов в системе электронного документооборота МО РФ // Состояние и перспективы развития современной науки по направлению «АСУ, информационно-телекоммуникационные системы» сборник статей конференции. Федеральное государственное автономное учреждение «Военный инновационный технополис «ЭРА»», 2019. С. 129-135.
2. Макаренко С.И. Справочник научных терминов и обозначений. СПб.: Наукоемкие технологии, 2019. 254 с.
3. Когаловский М.Р. Электронные библиотеки экономико-математических моделей: экономико-математические и информационные модели // Проблемы рыночной экономики. 2018. № 4. С. 89-97.
4. Баранов А.В. Системы юридически значимого электронного документооборота // Актуальные проблемы экономики современной России. 2015. Т. 2. № 2. С. 28-31
5. 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.
6. Hartmann K., Giles K. UAV exploitation: A new domain for cyber power // 8th International Conference on Cyber Conflict (CyCon). 2016. Pp. 205-221.
7. Куксов И. Как невидимые данные электронных документов приводят к реальным проблемам. 2017. https://www.kaspersky.ru/blog/office-documents-metadata/14277/. (Дата доступа 26.10.2020)
8. Путькина Л.В. Роль информационных систем и технологий в управлении предприятиями сферы услуг // Nauka-Rastudent.ru. 2016. № 5. С. 13.
9. Диченко С.А. Концептуальная модель обеспечения целостности информации в современных системах хранения данных // Информатика: проблемы, методология, технологии. Сборник материалов XIX международной научно-методической конференции. Под ред. Д.Н. Борисова. Воронеж, 2019. С. 697-701.
10. Савин С.В., Финько О.А. Контроль целостности данных на основе совместного использования хэш-функций и теории линейного кодирования // Информационное противодействие угрозам терроризма. 2015. № 24. С. 353-358.
11. Lakshmanan R., Arumugam S.Construction of a(k,n)-visual cryptography scheme // Designs, Codes and Cryptography. 2017. V. 82. №. 3. Pp. 629–645.
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. 17-36.
13. 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.
14. Баушев С.В. Удостоверяющие автоматизированные системы и средства. Введение в теорию и практику / Под ред. С.В. Баушева, А.С. Кузьмина. СПб.: БХВ-Петербург, 2016. 304 с.
15. Советов Б.Я. Моделирование систем / Под ред. Б.Я. Советова, С.А. Яковлева. М.: Юрайт, 2016. 343 с.
16. Курило А.П. Трудный путь к универсуму // BIS Journal №4 (27), 2017. [https://ib-bank.ru/bisjournal/post/602.
17. 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.
18. Зубарев Ю.М. Основы надежности машин и сложных систем. СПб.: Лань. 2017. 180 с.

19. Краковцев А.А., Скоба А.Н. Применение графовых баз данных для решения задачи поиска ассоциативных правил // Знание. 2017. № 3-1 (43). С. 82-87.
20. Артюхов А.В., Куликов Г.Г., Речкалов А.В. Логическая структура концептуальной модели информационно-аналитической системы (ИАС), основанной на слабоструктурированныхзнаниях производственной системы // Вестник Южно-Уральского государственного университета. Серия: Компьютерные технологии, управление, радиоэлектроника. 2018. Т. 18. № 4. С. 78-87.
21. Кораблёв Ф.Г. Коциклические квазоидные инварианты узлов // Сибирский математический журнал. 2020. Т. 61. № 2. С. 344-366.

CRYPTOGRAPHIC RECURSIVE CONTROL OF INTEGRITY OF METADATA ELECTRONIC DOCUMENTS. PART 1. MATHEMATICAL MODEL

***D.I. Tali*[17], *O.A. Finko*[18]**

The purpose *of the research is to increase the level of security of electronic document metadata in the face of destructive influences from authorized users (insiders).*

Research methods: *new scientific results allowed using a combination of data integrity control method based on the «write once» method and of authentication of HMAC messages (hash-based message authentication, as well as graph theory methods.*

Research result: a method of cryptographic recursive 2-D control of the integrity of electronic documents metadata is proposed. The analysis of the object of the study was carried out, based on the results of which it was concluded that it is necessary to effectively protect the metadata of electronic documents processed by automated information systems of electronic document management. Developed and described a mathematical model of the proposed method, based on graph theory.

The developed technical solution makes it possible to implement the functions of cryptographic recursive two-dimensional control of the integrity of the metadata of electronic documents, as well as to provide the possibility of localizing modified (with signs of violation of integrity) metadata records, in conditions of destructive influences of authorized users (insiders). This, in turn, reduces the likelihood of collusion between trusted parties by introducing mutual control over the results of their actions. The proposed solution makes it possible to ensure control of the integrity of data processed by departmental automated information systems of electronic document management, where, due to the peculiarities of their construction, it is impossible to effectively use the currently popular blockchain technology.

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

References

1. Tali D.I., Yeliseyev N.I. Analiz protsessa formirovaniya i zashchity metadannykh elektronnykh dokumentov v sisteme elektronnogo dokumentooborota MO RF // Sostoyaniye i perspektivy razvitiya sovremennoy nauki po napravleniyu «ASU, informatsionno-telekommunikatsionnyye sistemy» sbornik statey konferentsii. Federal'noye gosudarstvennoye avtonomnoye uchrezhdeniye «Voyennyy innovatsionnyy tekhnopolis «ERA»», 2019. S. 129-135.
2. Makarenko S.I. Spravochnik nauchnykh terminov i oboznacheniy. – SPb.: Naukoyemkiye tekhnologii, 2019. 254 s.
3. Kogalovskiy M.R. Elektronnyye biblioteki ekonomiko-matematicheskikh modeley: ekonomiko-matematicheskiye i informatsionnyye modeli // Problemy rynochnoy ekonomiki. 2018. № 4. S. 89-97.
4. Baranov A.V. Sistemy yuridicheski znachimogo elektronnogo dokumentooborota // Aktual'nyye problemy ekonomiki sovremennoy Rossii. 2015. T. 2. № 2. S. 28-31

17 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

18 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, 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

5. 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.
6. Hartmann K., Giles K. UAV exploitation: A new domain for cyber power // 8th International Conference on Cyber Conflict (CyCon). 2016. Pp. 205-221.
7. Kuksov I. Kak nevidimyye dannyye elektronnykh dokumentov privodyat k real'nym problemam. https://www.kaspersky.ru/blog/office-documents-metadata/14277/.
8. Put'kina L.V. Rol' informatsionnykh sistem i tekhnologiy v upravlenii predpriyatiyami sfery uslug // Nauka-Rastudent.ru. 2016. № 5. S. 13.
9. Dichenko S.A. Kontseptual'naya model' obespecheniya tselostnosti informatsii v sovremennykh sistemakh khraneniya dannykh // Informatika: problemy, metodologiya, tekhnologii. Sbornik materialov XIX mezhdunarodnoy nauchno-metodicheskoy konferentsii. Pod red. D.N. Borisova. Voronezh, 2019. S. 697-701.
10. Savin S.V., Finko O.A. Kontrol' tselostnosti dannykh na osnove sovmestnogo ispol'zovaniya khesh-funktsiy i teorii lineynogo kodirovaniya // Informatsionnoye protivodeystviye ugrozam terrorizma. 2015. № 24. S. 353-358.
11. Lakshmanan R., Arumugam S.Construction of a(k,n)-visual cryptography scheme // Designs, Codes and Cryptography. 2017. V. 82. №. 3. Pp. 629–645.
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. 17-36.
13. Savin S.V., Finko O.A., Yeliseyev N.I. Sistema kontrolya tselostnosti zhurnalov nepreryvno vedushchikhsya zapisey dannykh // Patent na izobreteniye RU 2637486 C2, opubl. 04.12.2017, byul. № 34.
14. Baushev S.V. Udostoveryayushchiye avtomatizirovannyye sistemy i sredstva. Vvedeniye v teoriyu i praktiku / Pod red. S.V. Bausheva, A.S. Kuz'mina. SPb.: BKHV-Peterburg, 2016. 304 s.
15. Sovetov B.YA. Modelirovaniye sistem / Pod red. B.YA. Sovetova, S.A. Yakovleva. M.: Yurayt, 2016. 343 s.
16. Kurilo A.P. Trudnyy put' k universumu // BIS Journal №4 (27), 2017. [https://ib-bank.ru/bisjournal/post/602.
17. 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.
18. Zubarev YU.M. Osnovy nadezhnosti mashin i slozhnykh sistem. SPb.: Lan'. 2017. 180 s.
19. Krakovtsev A.A., Skoba A.N. Primeneniye grafovykh baz dannykh dlya resheniya zadachi poiska assotsiativnykh pravil // Znaniye. 2017. № 3-1 (43). S. 82-87.
20. Artyukhov A.V., Kulikov G.G., Rechkalov A.V. Logicheskaya struktura kontseptual'noy modeli informatsionno-analiticheskoy sistemy (IAS), osnovannoy na slabostrukturirovannykhznaniyakh proizvodstvennoy sistemy // Vestnik Yuzhno-Ural'skogo gosudarstvennogo universiteta. Seriya: Komp'yuternyye tekhnologii, upravleniye, radioelektronika. 2018. T. 18. № 4. S. 78-87.
21. Korablov F.G. Kotsiklicheskiye kvazoidnyye invarianty uzlov // Sibirskiy matematicheskiy zhurnal. 2020. T. 61. № 2. S. 344-366.