МОДЕЛИ ЭЛЕКТРОННОГО ДОКУМЕНТА В РАМКАХ ПАРАДИГМЫ «ИНДУСТРИЯ 4.0»

Тали Д. И.[1], Финько О. А.[2]
(*Краснодарское высшее военное училище, Краснодар*)

Цифровая трансформация общества и производства постепенно вступает в стадию Индустрии 4.0, когда обслуживающая инфраструктура, в том числе и автоматизированные информационные системы юридически значимого электронного документооборота, будут способны адаптироваться под текущие условия обстановки. Однако современный этап развития таких систем характеризуется несовершенством терминологического аппарата и отождествлением объекта воздействия (электронного документа) с его бумажным прототипом, что приводит к ограничению их функциональных возможностей. Таким образом, существующая парадигма восприятия электронного документа не соответствует перспективному уровню развития автоматизированных информационных систем юридически значимого электронного документооборота в рамках концепции Индустрии 4.0. Цель работы – построение моделей электронного документа и описание метода обеспечения его целостности, позволяющего гарантировать достижение требуемого уровня защищенности автоматизированных информационных систем юридически значимого электронного документооборота, функционирующих в соответствии с положениями концепции Индустрии 4.0. Используемые методы: применение криптографических хэш-функций к компонентам (контенту и метаданным) электронного документа, результаты которых вычисляются по типу бинарного дерева Меркла в сочетании с технологией цепной записи данных. Результаты исследования: введено понятие «интегративный электронный документ», предложена новая структура электронного документа, что позволило сократить длительность его верификации и, как следствие, снизить риск реализации деструктивных воздействий на автоматизированную информационную систему.

Ключевые слова: Индустрия 4.0, контент, метаданные, управление электронными документами, целостность электронного документа.

1. Введение

Цифровые технологии с каждым годом совершенствуются и интегрируются во все сферы жизни, вызывая трансформацию общества и глобальной экономики, что становится завершаю-

[1] *Дмитрий Иосифович Тали, к.т.н.* (*dimatali@mail.ru*).
[2] *Олег Анатольевич Финько, д.т.н., профессор* (*ofinko@yandex.ru*).

щим этапом третьей промышленной революции. Подобные тенденции являются катализатором зарождения очередного этапа развития науки и техники, характеризующегося использованием новых подходов, позволяющих обеспечить эффективность государственного управления [25].

Цифровая трансформация связана с полномасштабным применением различных видов информационных систем и информационных ресурсов, предполагающих массовое использование электронных документов (ЭлД) и автоматизированных информационных систем юридически значимого электронного документооборота (АИС ЮЗ ЭД). Применение подобных технологий является одним из наиболее результативных механизмов комплексного решения задач повышения эффективности управления информацией и документацией [14].

Однако существующая нормативная и организационная база для формирования полноценного ЮЗ ЭД, основанного на принципах «Индустрии 4.0» (распределенность, виртуализация, интеллектуализация и т.д.), в настоящее время не соответствует требованиям, предъявляемым современным этапом технологического развития. Данное обстоятельство приводит к ряду трудностей, выражающихся в дублировании электронных и бумажных технологий, препятствующих переходу к безбумажному цифровому взаимодействию [13].

Подтверждением выше сказанному является неопределённость толкования Регулятором основных определений, используемых в данной предметной области. Так, под термином «электронный документ» понимается документированная информация, созданная, полученная и сохраняемая организацией или частным лицом в качестве доказательства и актива для подтверждения правовых обязательств или деловой транзакции [8]. При этом определение понятия «документ» аналогично указанному с той лишь разницей, что акцентируется внимание на фиксации информации на материальном носителе [5]. Однако состав ЭлД, в отличие от бумажного, определяется как совокупность двух компонентов: контента и метаданных, описывающих контекст, контент и структуру документов, а также управление ими в течение времени. Вместе с тем защита ЭлД, обеспечиваемая

подсистемой защиты информации АИС ЮЗ ЭД, сводится к защите метаданных посредством разграничения прав доступа и выполнению соответствующих правил, исключая криптографические средства защиты в виде электронной подписи (ЭП), которыми обеспечивается защищенность контента [8].

Исходя из этого при сложившейся структуре ЭлД его целостность имеет функциональную зависимость от двух компонент (контент и метаданные), имеющих между собой только логическую связь, что в условиях преднамеренных или непреднамеренных деструктивных воздействий уполномоченных пользователей (инсайдеров) не позволит обеспечить целостность ЭлД при полной или частичной утрате одного из них (рис. 1) [4, 23].

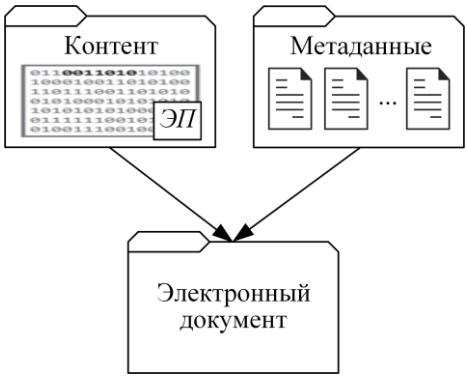

Рис. 1. Существующая схема синтеза ЭлД

Архаичность принятого в настоящее время представления о структуре ЭлД приводит к нарушению ряда требований, предъявляемых к ним в период жизненного цикла (рис. 2), выражающихся в:

1) невозможности обеспечения условий, исключающих несанкционированную модификацию ЭлД;

2) получении доступа к содержанию ЭлД для документов или их частей, не подлежащих автоматическому раскрытию государственным органам или третьим сторонам;

3) невозможности обеспечения доступности ЭлД в течение всего срока хранения [13].

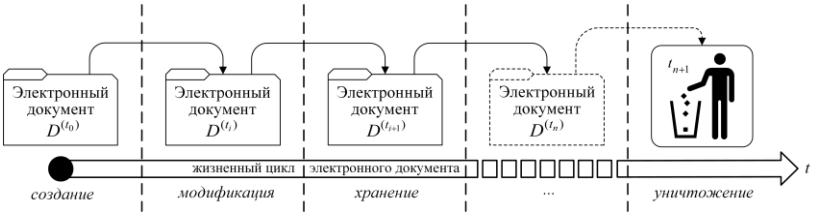

Рис. 2. Схема жизненного цикла ЭлД

Эти обстоятельства приводят к возникновению затруднений в проектировании документных систем ввиду снижения уровня их защищенности при подобной организации структуры ЭлД. Кроме того, повсеместное внедрение технологий, основывающихся на принципах Индустрии 4.0, заставляет совершенствовать и модернизировать такие системы до уровня систем обслуживания информации, характеризующихся централизацией обслуживаемых процессов и масштабируемостью обрабатываемой информации. В этих условиях основной задачей становится обеспечение целостности не столько ЭлД, сколько самой системы (инфраструктуры), обслуживающей циркулирующую в ней информацию.

Таким образом, возникает необходимость модификации не только самой структуры ЭлД, но и подходов к обеспечению его целостности, в рамках создания перспективных образцов АИС ЮЗ ЭД, функционирующих на основе принципов новой концепции.

2. Обзор существующих методов и средств контроля целостности данных

Выполненный анализ существующих методов и средств контроля целостности данных позволил установить, что в их основе лежит применение криптографической хэш-функции (ХФ) [6]. Применение подобного механизма позволит реализовать криптографическую связь компонент ЭлД и, как следствие, обеспечить формирование его единой криптографической структуры.

Наибольший интерес для решения такой задачи представляют метод «однократной записи» [27], способ аутентификации сообщений на основе HMAC (hash-based message authentication) [26], а также техническое решение [18].

Недостатком метода [27] является отсутствие 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.

В способе [26] полученный код аутентичности позволяет убедиться в том, что данные не изменялись с тех пор, как они были созданы, переданы или сохранены доверенным источником. Для такого рода проверки необходимо, чтобы две доверяющие друг другу стороны заранее договорились об использовании секретного ключа, который известен только им, что и является ограничением. Тем самым гарантируется аутентичность источника и сообщения.

Техническое решение [18] позволяет обеспечить необходимый уровень защиты записей данных в файле на основе задания соответствующих параметров метода «однократной записи»: степени вложенности в блок данных, количество используемых внешних ключей. При этом для контроля целостности данных могут быть использованы как бесключевые, так и ключевые ХФ/ЭП.

Недостатком данного технического решения является относительно высокая сложность операции контроля целостности записей данных, так как для ее реализации требуется использование всего множества ключей на всех этапах преобразования данных, что представляет существенное ограничение и техническую сложность для практического использования.

При этом, несмотря на несомненные достоинства вышеперечисленных решений, у них имеется общий недостаток, выражающийся в отсутствии технической возможности локализации записей данных с признаками нарушения целостности при реализации деструктивных воздействий уполномоченными пользователями АИС ЮЗ ЭД.

Наиболее подходящим решением является способ [19], позволяющий повысить уровень защищенности метаданных ЭлД, обрабатываемых АИС ЮЗ ЭД, с возможностью контроля их целостности. Основным преимуществом этого решения является реализация функции обнаружения и локализации несанкционированно модифицированных записей метаданных ЭлД, в случае нарушения их целостности уполномоченными пользователями (инсайдерами). Однако его недостатком является отсутствие функциональной возможности обеспечения «интегративной целостности ЭлД» (свойство целостного системного объекта, возникающее в результате взаимодействия его компонент и не присущее ни одной из них в отдельности [3, 12, 17, 23]), достигаемой за счет криптографической связности контента и метаданных, входящих в его состав, что в условиях преднамеренных или непреднамеренных деструктивных воздействий уполномоченных пользователей (инсайдеров) не обеспечивает целостности ЭлД в течение всего жизненного цикла при полной или частичной утрате одной из его компонент.

Перечисленные способы [18, 19, 26, 27] основаны на общих принципах построения цепной записи данных, однако в отличие от известных вариантов реализации технологии «блокчейн» [28–31] носят универсальный характер, что позволяет использовать их в том числе и в АИС ЮЗ ЭД с низкой интенсивностью проводимых транзакций ввиду отсутствия высоких вычислительных мощностей и малым количеством рабочих мест, входящих в общую сеть [22].

3. Постановка задачи

Воспользуемся теоретико-множественным подходом, получившим широкое распространение при описании различных технических систем [10, 16].

Пусть задана модель подсистемы ЗИ АИС ЮЗ ЭД: $Z = \{T, X, Y, D, R, C\}$, где

T – множество моментов времени в которые наблюдается подсистема ЗИ АИС ЮЗ ЭД, $t_i \in T$, $i = 0, 1, \ldots, n$; t_0 – начало эксплуатации АИС ЮЗ ЭД, t_n – конец эксплуатации АИС ЮЗ ЭД.

X – множество входных инициирующих событий (воздействий) (ИнС) на подсистему ЗИ АИС ЮЗ ЭД (например: ошибки персонала АИС ЮЗ ЭД/действия злоумышленников, отказы технических компонентов АИС ЮЗ ЭД, нарушения технологии обработки ЭлД, истечение сроков действия ключей ЭП и т.д).

Y – множество функциональных состояний подсистемы ЗИ АИС ЮЗ ЭД в результате влияния ИнС (например: функционирование в штатном режиме; функционирование в режиме несанкционированного доступа к ресурсам АИС ЮЗ ЭД внутренним/внешним нарушителем; функционирование в режиме воздействия вредоносного программного обеспечения (ВПО), сбой в работе АИС ЮЗ ЭД и т.д.).

D – множество ЭлД, изменяющихся под влиянием ИнС на подсистему ЗИ АИС ЮЗ ЭД.

R – множество выходных качественных состояний, обрабатываемых ЭлД, причем

(1) $R = \left\{ R_{(+)}^{(x_j)},\ R_{(-)}^{(x_j)} \right\}$,

где $R_{(+)}^{(x_j)}$ – состояние ЭлД, при котором его целостность под влиянием ИнС $x_j \in X$ обеспечена, $R_{(-)}^{(x_j)}$ – состояние ЭлД, при котором под влиянием ИнС $x_j \in X$ он утрачивает целостность или обеспечение указанного свойства не доступно в текущий момент функционирования АИС ЮЗ ЭД.

C – множество сценариев функционирования подсистемы ЗИ АИС ЮЗ ЭД под влиянием ИнС $x_j \in X$.

Исходя из определения [9] признаком «целостности системы» является реализация ею своего целевого предназначения. Целевым предназначением рассматриваемых систем является обеспечение целостности ЭлД. Из чего следует, что нахождение ЭлД в состоянии $R_{(+)}^{(x_j)}$ характеризует состояние целостности АИС ЮЗ ЭД, а переход ЭлД в состояние $R_{(-)}^{(x_j)}$ – состояние нарушения целостности АИС ЮЗ ЭД.

Таким образом, справедливо утверждать, что в первом случае такое развитие событий приведет к нормальному сценарию

(штатному режиму) функционирования АИС ЮЗ ЭД, а во втором – к его нарушению. Однако ЭлД $D^{(t_i)}$ в состоянии момента времени t_i представляет из себя совокупность контента $K^{(t_i)}$ и подмножества метаданных $M^{(t_i)}$ [8], что может быть записано как

(2) $D^{(t_i)} = \left\{ K^{(t_i)},\ M^{(t_i)} \right\}$,

причем $M^{(t_i)} = \left\{ m_{i1},\ m_{i2},\ m_{i3},\ldots,\ m_{in} \right\}$, где $m_{i1}, m_{i2}, m_{i3},\ldots, m_{in}$ – реквизиты ЭлД (автор, дата создания, гриф и т.д.).

Таким образом, всякое состояние R ЭлД $D^{(t_i)}$ характеризуется в каждый момент времени $t_i \in T$ состоянием контента $K^{(t_i)}$ и состоянием метаданных $M^{(t_i)}$, что может быть записано как $K^{(t_i)} = \left\{ k_{(+)}^{(x_j)},\ k_{(-)}^{(x_j)} \right\}$ и $M^{(t_i)} = \left\{ m_{(+)}^{(x_j)},\ m_{(-)}^{(x_j)} \right\}$, изменяющихся под влиянием ИнС $x_j \in X$ на подсистему ЗИ АИС ЮЗ ЭД, где $k_{(+)}^{(x_j)}$ – состояние ЭлД $D^{(t_i)}$, при котором в ходе реализации ИнС x_j целостность его контента не нарушена («1»), и $k_{(-)}^{(x_j)}$ – состояние ЭлД $D^{(t_i)}$, при котором целостность его контента нарушена («0»), $m_{(+)}^{(x_j)}$ – состояние ЭлД $D^{(t_i)}$, при котором в ходе реализации ИнС x_j целостность его метаданных не нарушена («1»), и $m_{(-)}^{(x_j)}$ – состояние ЭлД $D^{(t_i)}$, при котором целостность его метаданных нарушена («0»).

Так как ЭлД $D^{(t_i)}$ имеет функциональную зависимость от двух компонент – контента $K^{(t_i)}$ и метаданных $M^{(t_i)}$, нахождение подсистемы ЗИ АИС ЮЗ ЭД в состоянии («0») (нарушение функционирования) увеличивается до трех вариантов: (0, 0), (0, 1), (1,0) (на рис. 3 отмечены пунктиром).

В таком случае требуется минимизировать количество состояний АИС ЮЗ ЭД с признаками нарушения целостности:

(3) $Y(R(X)) \to \min \left| C \right| \ \middle|\ t_i \in T,\ i = \overline{0,\ n}$,

где $|C|$ – количество (мощность множества) сценариев нарушения функционирования подсистемы ЗИ АИС ЮЗ ЭД.

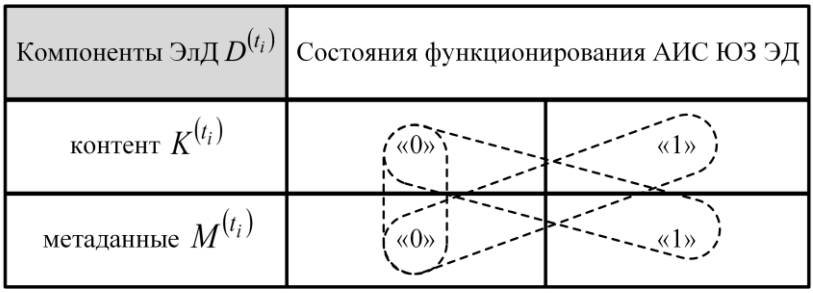

Рис. 3. Варианты сценариев нарушения функционирования АИС ЮЗ ЭД

Достичь результата возможно посредством разработки метода обеспечения целостности ЭлД за счет связности его компонент. Выполнение критерия качества функционирования подсистемы ЗИ АИС ЮЗ ЭД определяется неравенством

(4) $\left|C_{\text{разр.}}\right| < \left|C_{\text{сущ.}}\right|$,

где $|C_{\text{разр.}}|$ и $|C_{\text{сущ.}}|$ – количество сценариев нарушения функционирования подсистемы ЗИ АИС ЮЗ ЭД посредством нарушения целостности компонент $K^{(t_i)}$ и $M^{(t_i)}$ при использовании разработанной структуры ЭлД $D^{(t_i)}$ и при использовании существующей структуры ЭлД $D^{(t_i)}$ соответственно.

При этом в целях контроля целостности ЭлД, обрабатываемых АИС ЮЗ ЭД, разрабатываемый метод не должен уступать существующим по таким параметрам, как время вычисления $t_{\text{выч.}}$ (наиболее сложной операции ХФ/ЭП), а также время локализации $t_{\text{лок.}}$ записей данных (контента и/или метаданных ЭлД) с признаками нарушения целостности.

В таком случае в качестве преимущества разработанного метода требуется выполнение следующих условий:

(5) $t_{\text{выч.разр.}} \le t_{\text{выч.прототипа}}$;

(6) $t_{\text{лок.разр.}} \le t_{\text{лок.прототипа}}$,

где $t_{\text{выч.прототипа}}$, $t_{\text{лок.прототипа}}$, – время, затрачиваемое на вычисление наиболее сложной операции ХФ/ЭП и локализацию записей данных (контента и/или метаданных ЭлД) с признаками нару-

шения целостности при использовании известных методов контроля целостности данных.

4. Обеспечение целостности электронных документов на основе бинарного дерева Меркла

Предлагаемое решение основывается на таких принципах системного анализа, как принцип целостности и принцип интегративности. Под первым предполагается рассмотрение исследуемого объекта в единстве его взаимодействующих частей, а под вторым – изучение свойств электронного документа как целостного системного объекта, возникающих в результате взаимодействия его компонент и не присущих ни одной из компонент в отдельности [1, 2, 10, 23].

В целях реализации этих принципов разработан соответствующий метод, содержащий совокупность правил формирования и верификации состояний ЭлД и реализующие эти правила формальные модели.

4.1. КОНЦЕПТУАЛЬНАЯ МОДЕЛЬ АИС ЮЗ ЭД, УЧИТЫВАЮЩАЯ ПРИНЦИПЫ ЦЕЛОСТНОСТИ И ИНТЕГРАТИВНОСТИ ЭЛД

Анализ публикаций в области теории систем и системного анализа [3, 11, 12, 17] позволяет сделать вывод о том, что АИС ЮЗ ЭД может рассматриваться как среда существования ЭлД, а сам ЭлД как системный объект, состоящий из двух компонент: контента и метаданных (2). Причем их функциональная зависимость очевидна: без создания контента невозможно формирование метаданных, в свою очередь без метаданных невозможно управление ЭлД, в то время как в среде АИС ЮЗ ЭД эти элементы в настоящее время имеют разную степень защиты.

Концептуальная модель АИС ЮЗ ЭД, соответствующая принципам целостности и интегративности, поясняется с помощью рис. 4. При этом предлагается достичь интегративности ЭлД за счет использования стандартных криптографических протоколов.

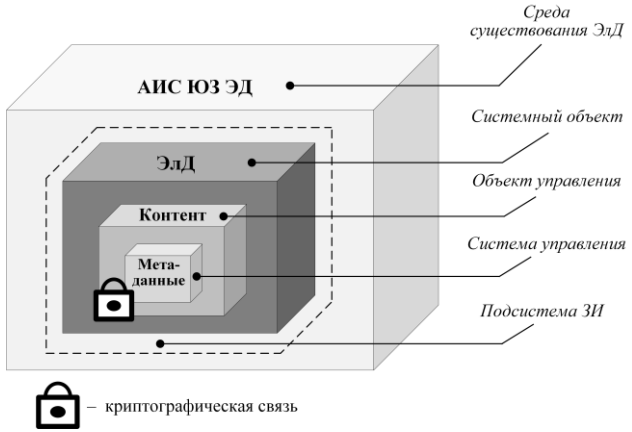

Рис. 4. Пояснение концептуальной модели АИС ЮЗ ЭД, учитывающей принципы целостности и интегративности ЭлД

4.2. ФОРМАЛЬНЫЕ МОДЕЛИ ОБЕСПЕЧЕНИЯ ЦЕЛОСТНОСТИ ЭЛД НА ОСНОВЕ БИНАРНОГО ДЕРЕВА МЕРКЛА

Применим криптографические ХФ к компонентам ЭлД (контенту и метаданным), результаты которых вычисляются по типу бинарного дерева Меркла в сочетании с технологией цепной записи данных [27–31]. Подобное решение позволит повысить уровень защищенности ЭлД, обрабатываемых АИС ЮЗ ЭД, за счет обнаружения и локализации контента и записей метаданных, подвергшихся несанкционированной модификации со стороны уполномоченных пользователей (инсайдеров).

Метод обеспечения целостности ЭлД на основе бинарного дерева Меркла можно представить следующим образом. Модель формирования ЭлД (с модифицированной структурой): множество ключей V_U разбивается на два подмножества: $V_U \in \left\{V_U^{(1)}, V_U^{(2)}\right\}$ и $V_U^* \in \left\{V_U^{*(1)},\ V_U^{*(2)}\right\}$, при этом каждые части подмножеств содержат ключи $V_U^{(q)} \in \left\{v_1^{(q)},\ v_2^{(q)}, \ldots,\ v_\varsigma^{(q)}\right\}$ и $V_U^{*(q)} \in \left\{v_1^{*(q)}, v_2^{*(q)}, \ldots,\ v_\varsigma^{*(q)}\right\}$, где q=1, 2 – принадлежность ключей соответствующей части подмножеств, для всех U=1, …,ς – номер ключа в соответствующей части подмножеств.

В рассматриваемом варианте реализации данного метода ключи $V_U^{(1)}$ являются ключами исполнителя (автора) электронного документа, ключи $V_U^{(2)}$ – внутренними системными ключами.

В момент формирования t_0 ЭлД в памяти системы обработки данных образуется информационный блок $D^{(t_0)} = \left\{K^{(t_0)}, M^{(t_0)}\right\}$, представляющий собой ЭлД, создаваемый подмножеством контента $K^{(t_0)}$ и подмножеством записей статических метаданных $M^{(t_0)} = \left\{m_{01}, m_{02}, m_{03}, \ldots, m_{0n}\right\}$, над которыми одновременно производятся операции криптографического преобразования:

$H_0 = f^{(v_x^{(1)})}(K^{(t_0)})$ на ключах $v_x^{(1)} \in V_U^{(1)}$,

$h_{01} = f^{(v_x^{(2)})}(m_{01})$ на ключах $v_x^{(2)} \in V_U^{(2)}$,

$h_{02} = f^{(v_x^{(2)})}(m_{02})$ на ключах $v_x^{(2)} \in V_U^{(2)}$,

$h_{03} = f^{(v_x^{(2)})}(m_{03})$ на ключах $v_x^{(2)} \in V_U^{(2)}$,

…,

$h_{0n} = f^{(v_x^{(2)})}(m_{0n})$ на ключах $v_x^{(2)} \in V_U^{(2)}$.

Над вычисленными значениями сигнатур h_{01}, h_{02}, h_{03}, …, h_{0n} записей статических метаданных производятся двухместные операции конкатенации: $h_{01}||h_{02}$, $h_{03}||h_{0n}$, над результатами которых выполняются операции криптографического преобразования на ключах $v_x^{(2)} \in V_U^{(2)}$:

$h_{0102} = f^{(v_x^{(2)})}(h_{01}||h_{02})$,

$h_{030n} = f^{(v_x^{(2)})}(h_{03}||h_{0n})$.

После чего над вновь вычисленными сигнатурами последовательно выполняются операции конкатенации и криптографического преобразования на ключах $v_x^{(2)} \in V_U^{(2)}$:

$h_0^{\Sigma} = f^{(v_x^{(2)})}\left(h_{0102} || h_{030n}\right)$,

результатом которой является формирование корневой сигнатуры h_0^{Σ} записей статических метаданных (рис. 5).

Затем операции конкатенации и криптографического пре-

образования на ключах $v_x^{(2)} \in V_U^{(2)}$ производятся над значением сигнатуры H_0 контента и корневой сигнатурой h_0^{Σ} записей статических метаданных, в целях получения общей корневой сигнатуры ЭлД, созданного в момент времени t_0:

$$S_0 = f^{(v_x^{(2)})}(H_0 || h_0^{\Sigma})$$

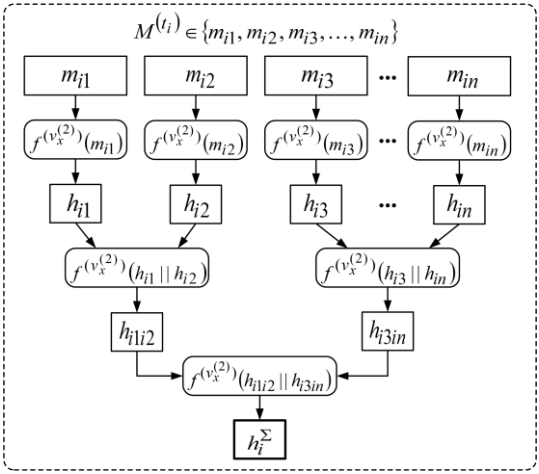

Рис. 5. Диаграмма функциональной модели формирования корневой сигнатуры записей метаданных ЭлД

После произведенных операций ЭлД вводится в систему, причем во время его жизненного цикла t_1, t_2, …, t_n при выполнении записи и редактирования повторно производятся вышеописанные операции.

При этом общая корневая сигнатура S_1 ЭлД, вычисленная в момент времени t_1, конкатенирует с общей корневой сигнатурой S_0 ЭлД, вычисленной в момент времени t_0, с одновременным криптографическим преобразованием на ключах $v_x^{(2)} \in V_U^{(2)}$, тем самым образуя сигнатуру жизненного цикла S_{01} ЭлД:

$$S_{01} = f^{(v_x^{(2)})}(S_0 | \ |S_1).$$

По мере изменения ЭлД операции повторяются в аналогичном порядке в соответствии с моментами времени t_3, t_4, …, t_n его

жизненного цикла, что формирует его модифицированную структуру (далее ЭлД с модифицированной структурой будем называть «интегративным»).

Введем понятие «интегративный электронный документ» (ИЭлД) – информационный объект, состоящий из взаимодействующих составных компонентов (контента и метаданных), возникающий в результате реализации механизма их криптографической связности, и характеризующийся целостностью [7, п.5.9]. Иллюстрированный пример ИЭлД представлен на рис. 6.

Контент $K^{(t_i)}$ и вычисленные значения его сигнатур H_i, записи метаданных $m_{i1}, m_{i2}, m_{i3}, \ldots, m_{in}$, их сигнатуры $h_{i1}, h_{i2}, h_{i3}, \ldots, h_{in}$, общие сигнатуры h_{i1i2}, h_{i3in} записей метаданных, корневые сигнатуры h_i^{Σ} записей метаданных, общие корневые сигнатуры S_i, а также корневые сигнатуры S_{in} его жизненного цикла сохраняются в памяти системы обработки данных и используются для контроля целостности ИЭлД в моменты времени его жизненного цикла $t_0, t_1, t_2, \ldots, t_n$.

Модель верификации ИЭлД: контроль целостности осуществляется на основе извлечения из памяти системы обработки данных контента $K^{*(t_i)}$ и вычисленных значений его сигнатур H_i^*, записей метаданных $m_{i1}^*, m_{i2}^*, m_{i3}^*, \ldots, m_{in}^*$ и их сигнатур $h_{i1}^*, h_{i2}^*, h_{i3}^*, \ldots, h_{in}^*$, общих сигнатур h_{i1i2}^*, h_{i3in}^* записей метаданных, корневых сигнатур $h_i^{\Sigma*}$ записей метаданных, общих корневых сигнатур S_i^*, а также корневых сигнатур S_{in}^* его жизненного цикла, прошедших процедуру хранения и подлежащих контролю целостности.

После чего выполняются повторные операции криптографического преобразования над извлеченным контентом $K^{*(t_i)}$ и записями метаданных $m_{i1}^*, m_{i2}^*, m_{i3}^*, \ldots, m_{in}^*$. В результате чего вновь вычисленные сигнатуры

$$H_i^{**};\ h_{i1}^{**}, h_{i2}^{**}, h_{i3}^{**}, \ldots, h_{in}^{**};\ h_{i1i2}^{**}, h_{i3in}^{**};\ h_i^{\Sigma**};\ S_i^{**};\ S_{in}^{**}$$

попарно сравниваются с ранее извлеченными:

$$H_i^{*};\ h_{i1}^{*}, h_{i2}^{*}, h_{i3}^{*}, \ldots, h_{in}^{*};\ h_{i1i2}^{*}, h_{i3in}^{*};\ h_i^{\Sigma*};\ S_i^{*};\ S_{in}^{*}.$$

Заключение об отсутствии нарушения целостности делается при выполнении равенств: $S_{in}^{**} = S_{in}^{*}$; $S_i^{**} = S_i^{*}$; $H_i^{**} = H_i^{*}$; $h_i^{\Sigma**} = h_i^{\Sigma*}$; $h_{i1i2}^{**} = h_{i1i2}^{*}, h_{i3in}^{**} = h_{i3in}^{*}$; $h_{i1}^{**} = h_{i1}^{*}, h_{i2}^{**} = h_{i2}^{*}, h_{i3}^{**} = h_{i3}^{*}$, …, $h_{in}^{**} = h_{in}^{*}$, в противном случае делается заключение о нарушении целостности для соответствующих номеров сигнатур (рис. 7).

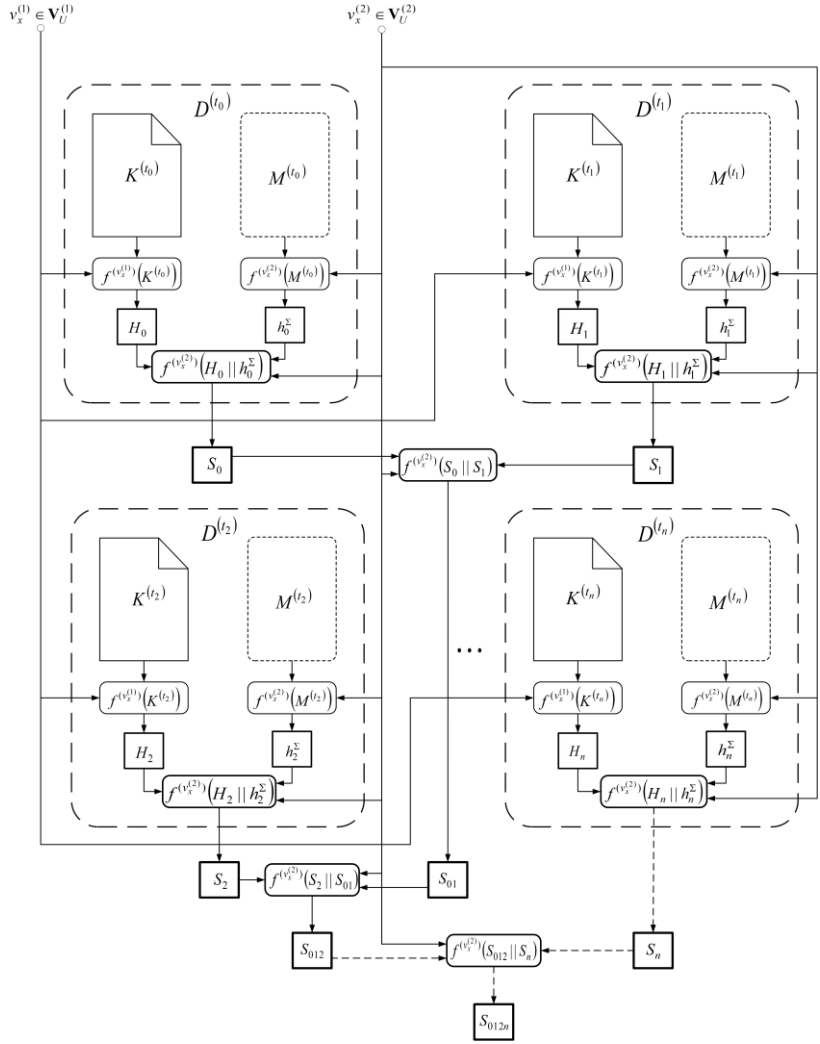

Рис. 6. Диаграмма функциональной модели формирования ИЭлД

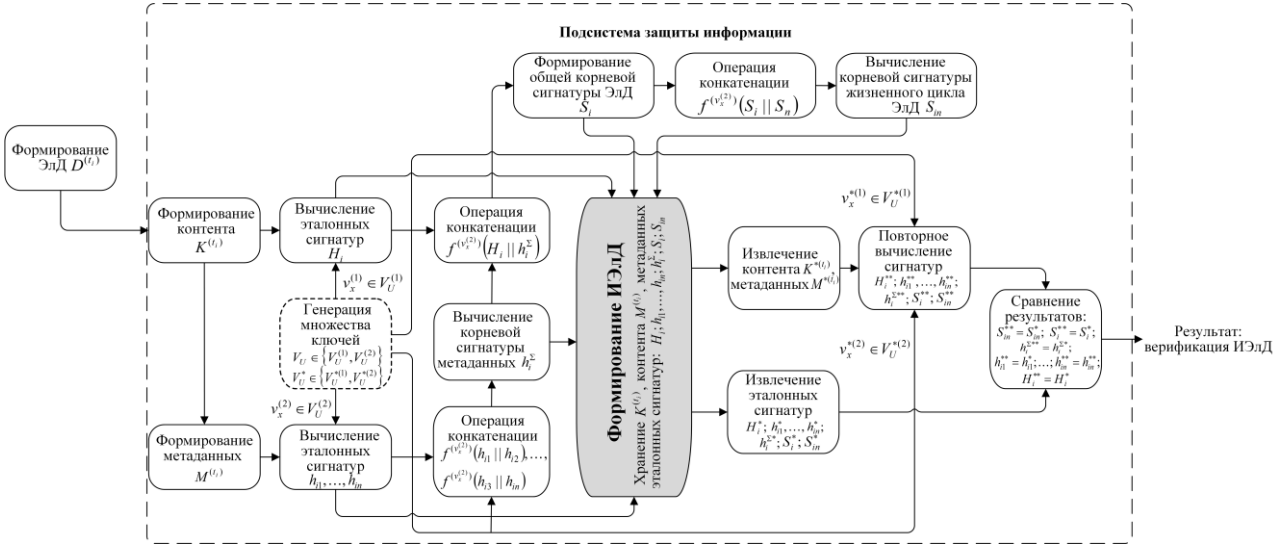

Рис. 7. Функциональная модель формирования и верификации ИЭлД

В качестве криптографического преобразования $f^{(v_x^{(1)})}(K^{(t_i)})$, $f^{(v_x^{(2)})}(m_{ij})$ используется либо ключевая ХФ, при этом $V_U = V_U^*$ (равные множества), либо ЭП, при этом $V_U \neq V_U^*$ (неравные множества).

4.3. ПРИКЛАДНЫЕ СРЕДСТВА РЕАЛИЗАЦИИ МЕТОДА ОБЕСПЕЧЕНИЯ ЦЕЛОСТНОСТИ ЭЛД НА ОСНОВЕ БИНАРНОГО ДЕРЕВА МЕРКЛА

Процесс обеспечения целостности ЭлД на основе бинарного дерева Меркла включает в себя процедуры формирования ИЭлД и верификации его состояний. В целях практического использования разработанного метода сформированы соответствующие правила, реализующие данные процедуры, представленные в виде схем и пошагового описания, выполняемых в них операций.

Так, правило формирования ИЭлД можно сформулировать следующим образом (рис. 8):

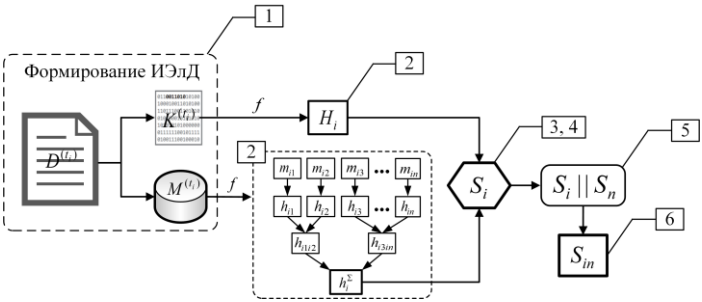

Рис. 8. Схема формирования ИЭлД

Шаг 1. Формирование $D^{(t_i)}$ посредством создания контента $K^{(t_i)}$ и соответствующих ему записей метаданных $M^{(t_i)}$.

Шаг 2. Вычисление сигнатуры H_i контента $K^{(t_i)}$ и корневой сигнатуры записей метаданных h_i^{Σ}.

Шаг 3. Вычисление общей корневой сигнатуры S_i (рис. 8 – гексагон).

Шаг 4. Повтор произведенных операций для каждого последующего момента времени.

Шаг 5. Выполнение операции конкатенации общей корневой сигнатуры S_i с полученной в каждый последующий момент времени.

Шаг 6. Вычисление сигнатуры S_{in} его жизненного цикла.

В таком случае правило верификации ИЭлД представляет собой следующую последовательность выполнения операций (рис. 9).

Шаг 1. Формирование $D^{(t_i)}$, заключающееся в повторном вычислении сигнатур H_i^{**}; $h_{i1}^{**}, h_{i2}^{**}, h_{i3}^{**}, \ldots, h_{in}^{**}$; $h_{i1i2}^{**}, h_{i3in}^{**}$; $h_i^{\Sigma**}$; S_i^{**}; S_{in}^{**}.

Шаг 2. Извлечение эталонных сигнатур (прошедших процедуру хранения) H_i^{*}; $h_{i1}^{*}, h_{i2}^{*}, h_{i3}^{*}, \ldots, h_{in}^{*}$; $h_{i1i2}^{*}, h_{i3in}^{*}$; $h_i^{\Sigma*}$; S_i^{*}; S_{in}^{*}.

Шаг 3. Сравнение результатов: $S_{in}^{**} = S_{in}^{*}$; $S_i^{**} = S_i^{*}$; $H_i^{**} = H_i^{*}$; $h_i^{\Sigma**} = h_i^{\Sigma*}$; $h_{i1i2}^{**} = h_{i1i2}^{*}, h_{i3in}^{**} = h_{i3in}^{*}$; $h_{i1}^{**} = h_{i1}^{*}, h_{i2}^{**} = h_{i2}^{*}, h_{i3}^{**} = h_{i3}^{*}, \ldots, h_{in}^{**} = h_{in}^{*}$.

Шаг 4. Заключение об отсутствии (нарушении) целостности (результат: верификация ИЭлД).

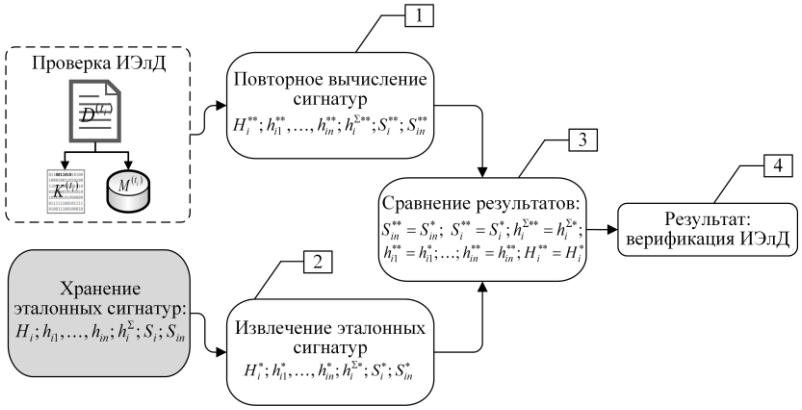

Рис. 9. Схема верификации ИЭлД

Таким образом, указанные правила позволяют создать алгоритмы и программное обеспечение, реализующее метод

обеспечения целостности электронных документов на основе бинарного дерева Меркла.

5. Результаты исследования разработанного метода

Исходя из постановки задачи, а также учитывая существующую структуру ЭлД (2), процесс функционирования АИС ЮЗ ЭД может быть описан следующей моделью: в любой произвольный момент времени t_i, в процессе обработки ЭлД, подсистема ЗИ АИС ЮЗ ЭД может находиться в одном из четырех состояний по отношению к обрабатываемому ЭлД $D^{(t_i)}$ при возникновении ИнС $x_j \in X$ в АИС ЮЗ ЭД [21]:

(7) $R_{(+)}^{(x_j)}(t_i) = D^{(t_i)}\left(k_{(+)}^{(x_j)},\ m_{(+)}^{(x_j)}\right) \to 1,$

где $R_{(+)}^{(x_j)}(t_i)$ – состояние ЭлД $D^{(t_i)}$, при котором в ходе реализации ИнС x_j целостность его компонентов не нарушена («1»); символ «$\to$» далее по тексту читать как «отсюда следует».

(8) $R_{(-)}^{(x_j)}(t_i) = D^{(t_i)}\left(k_{(+)}^{(x_j)},\ m_{(-)}^{(x_j)}\right) \to 0,$

где $R_{(-)}^{(x_j)}(t_i)$ – состояние ЭлД $D^{(t_i)}$, при котором в ходе реализации ИнС x_j целостность его метаданных нарушена («0»).

(9) $R_{(-)}^{(x_j)}(t_i) = D^{(t_i)}\left(k_{(-)}^{(x_j)},\ m_{(+)}^{(x_j)}\right) \to 0,$

где $R_{(-)}^{(x_j)}(t_i)$ – состояние ЭлД $D^{(t_i)}$, при котором в ходе реализации ИнС x_j целостность его контента нарушена («0»);

(10) $R_{(-)}^{(x_j)}(t_i) = D^{(t_i)}\left(k_{(-)}^{(x_j)},\ m_{(-)}^{(x_j)}\right) \to 0,$

где $R_{(-)}^{(x_j)}(t_i)$ – состояние ЭлД $D^{(t_i)}$, при котором в ходе реализации ИнС x_j целостность его компонентов нарушена («0»).

Переход ЭлД в состояние «0» рассматривается как событие, нарушающее состояние его целостности и, как следствие, приводящее к нарушению функционирования АИС ЮЗ ЭД. При этом насчитывается до трех таких сценариев с учетом существующей структуры ЭлД (8), (9), (10) (рис. 10б, в, г).

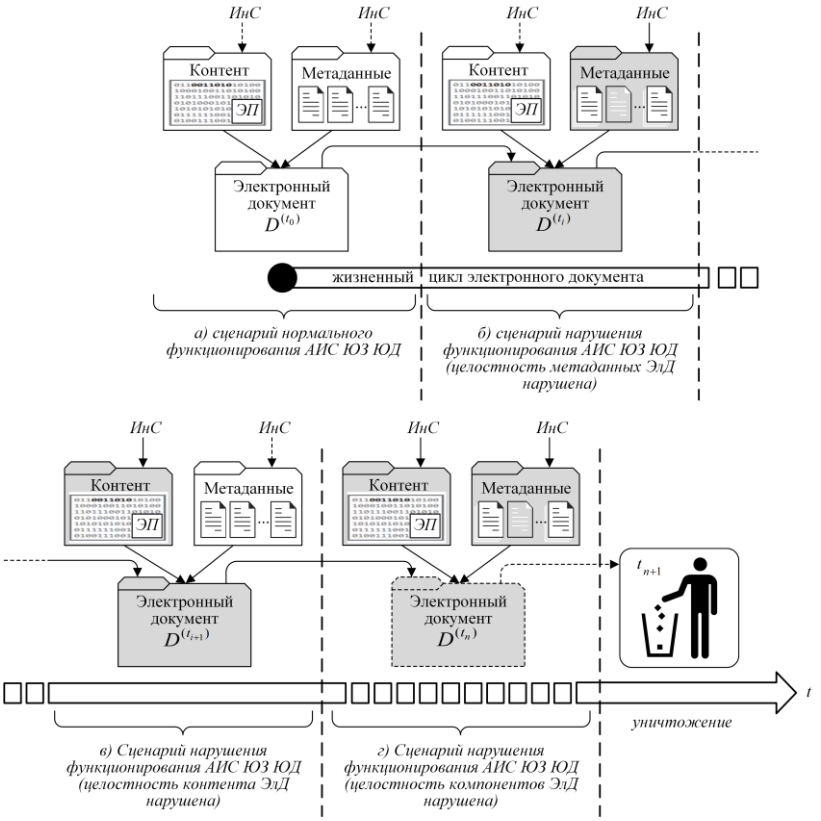

Рис. 10. Сценарии перехода АИС ЮЗ ЭД в различные режимы функционирования в процессе жизненного цикла ЭлД

В качестве практического примера можно привести ситуацию, при которой подсистема ЗИ АИС ЮЗ ЭД успешно нейтрализовала ИнС $x_j \in X$, вызванные воздействием ВПО/действиями злоумышленников, чем обеспечила целостность компонентов обрабатываемого ЭлД и, как следствие, штатный режим функционирования АИС ЮЗ ЭД (рис. 10а).

В противном случае те же ИнС $x_j \in X$ вызывают нарушение целостности метаданных при защищенном контенте (например, посредством уничтожения базы данных, в которой осуществляется их хранение, что приведет к невозможности нахождения,

обрабатываемого ЭлД) и, как следствие, самого ЭлД, что вызовет переход АИС ЮЗ ЭД в режим нарушения функционирования (рис. 10б).

Другим вариантом реализации ИнС $x_j \in X$ станет нарушение целостности контента при защищенных метаданных (например, компрометация ключей подписи контента и внесение в него нелегитимных изменений злоумышленником без внесения изменений в метаданные, что приведет к несанкционированному изменению содержательной части ЭлД) и, как следствие, самого ЭлД, что также вызовет переход АИС ЮЗ ЭД в режим нарушения функционирования (рис. 10в).

В качестве последнего варианта реализации ИнС $x_j \in X$ рассмотрим ситуацию, при которой злоумышленником является администратор АИС ЮЗ ЭД, имеющий доступ к ключам подписи контента ЭлД, а также расширенные права на внесение изменений в его метаданные. При таком сценарии доступ к обрабатываемому ЭлД может быть утрачен ввиду нарушения его целостности (контента и метаданных), что приведет к переходу АИС ЮЗ ЭД в режим нарушения функционирования (рис. 10г).

Разработанный метод позволяет сократить количество сценариев нарушения функционирования АИС ЮЗ ЭД за счет формирования ИЭлД, иллюстрированный пример приведен на рис. 11.

Таким образом, предлагаемый метод учитывает требования (3) по минимизации количества сценариев $|C|$ нарушения функционирования АИС ЮЗ ЭД, а также позволяет достичь необходимого критерия качества функционирования подсистемы ЗИ АИС ЮЗ ЭД (4). Кроме того, предполагается, что новая структура ЭлД позволит сократить временные затраты на его верификацию (обнаружение и локализацию компонентов ЭлД с признаками нарушения целостности).

В целях получения численной оценки результатов исследования произведем сравнительный анализ разработанного технического решения [20] с прототипом, в качестве которого используется способ [19].

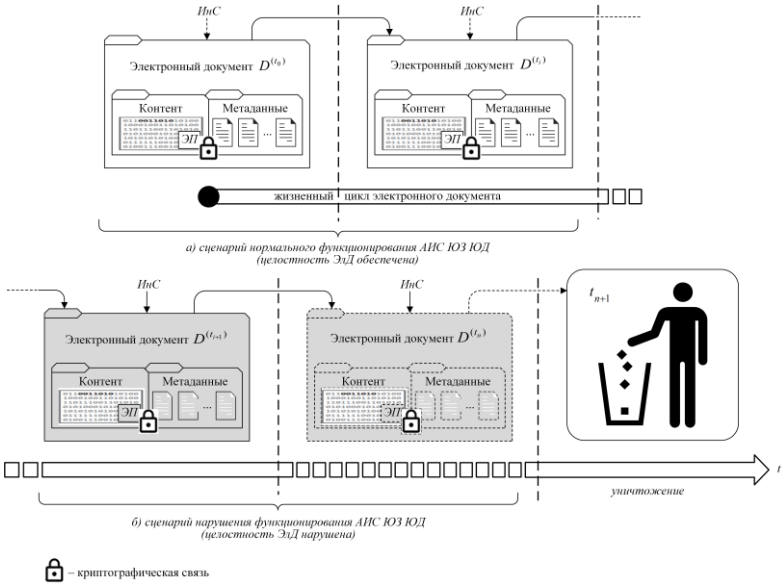

Рис. 11. Сценарии перехода АИС ЮЗ ЭД в различные режимы функционирования в процессе жизненного цикла ИЭлД

Для чего произведем расчет количества операций по вычислению ХФ/ЭП в зависимости от количества совершаемых преобразований в течение жизненного цикла ЭлД.

При использовании известного технического решения [19]:

(11) $t_{\text{выч.прототипа}} = (k-1)\ (n+1)$.

При использовании разработанного технического решения [20]:

(12) $t_{\text{выч.разр.}} = \sum_{i=0}^{\log_2 n} \frac{n}{2^i} + k + 1,$

где n – количество реквизитов (метаданных), содержащихся в ЭлД; k – количество моментов времени, в которые производятся преобразования ЭлД.

Построим графики соответствующих зависимостей для ЭлД, содержащего 64 реквизита, при условии 10 преобразований в период его жизненного цикла (рис. 12).

Рис. 12. Результат оценки количества операций вычисления ХФ/ЭП в зависимости от количества совершаемых преобразований в течение жизненного цикла ЭлД

Рассчитаем среднее количество операций по вычислению ХФ/ЭП при использовании известного и разработанного решения:

$$(13)\quad H_{\text{ср.}} = \frac{H_2 + H_3 + \ldots + H_{10}}{n\ (k-1)},$$

где n – количество реквизитов (метаданных), содержащихся в ЭлД; k – количество моментов времени, в которые производятся преобразования ЭлД; H_i – операции по вычислению ХФ/ЭП.

Вычисления производятся при условии 10 преобразований ЭлД в период его жизненного цикла, при этом $k = 2$ – начало преобразований.

Воспользовавшись формулой (13), получим:

$H_{\text{ср.прототипа}} = 167,5;$

$H_{\text{ср.разр.}} = 73.$

Полученный результат позволяет сделать вывод о том, что разработанное техническое решение [20] позволяет сократить количество операций по вычислению ХФ/ЭП в 2,3 раза в срав-

нении с известным [19], что в процентном соотношении соответствует сокращению $t_{\text{выч.}}$ на 56,4 % [24].

Таким образом, выполнение условия (5) оценки разработанного метода достигнуто.

Далее произведем расчет количества сравнений компонентов ЭлД при выполнении процедуры верификации в зависимости от момента времени, в котором было обнаружено первое несоответствие.

При использовании известного технического решения [19]:

(14) $t_{\text{лок.прототипа}} = (k-i)\ n + (k-i-1)\ (n-1)$.

При использовании разработанного технического решения [20]:

(15) $t_{\text{лок.разр.}} = 2 + \sum_{i=0}^{\log_2 n} 2^i + (k-i)$,

где n – количество реквизитов (метаданных), содержащихся в ЭлД; k – количество моментов времени, в которые производятся преобразования ЭлД; i – момент времени, в который было обнаружено первое несоответствие.

Построим графики соответствующих зависимостей для ЭлД, содержащего 64 реквизита, при условии обнаружения первого несоответствия на 5-м моменте времени его жизненного цикла (рис. 13).

На основе полученных результатов вычислим среднее количество сравнений ХФ/ЭП с эталонными значениями при использовании известного и разработанного решения:

(16) $L_{\text{ср.}} = \dfrac{L_1 + L_2 + \ldots + L_9}{n\ (i-1)}$,

где n – количество реквизитов (метаданных), содержащихся в ЭлД; i – количество моментов времени, в которые производятся операции сравнения ХФ/ЭП с эталонными значениями; L_i – операции сравнения ХФ/ЭП с эталонными значениями.

При использовании формулы (16) получим

$L_{\text{ср.прототипа}} = 288{,}5$;

$L_{\text{ср.разр.}} = 75$.

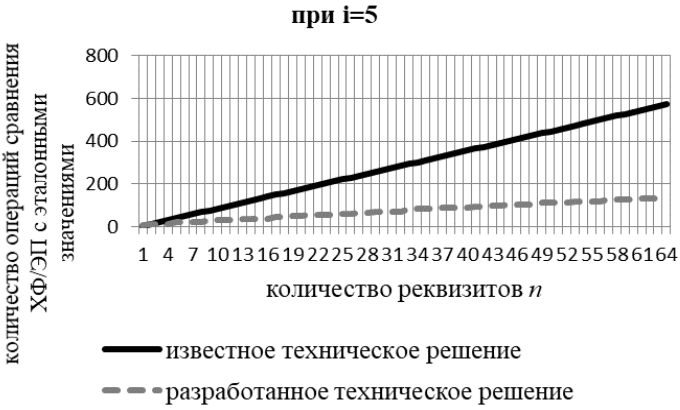

Рис. 13. Результат оценки количества операций сравнения ХФ/ЭП в зависимости от момента времени, в котором было обнаружено первое несоответствие

Разработанное техническое решение [20] позволяет сократить количество операций сравнения ХФ/ЭП с эталонными значениями в 3,84 раза в сравнении с известным [19], что в процентном соотношении соответствует сокращению $t_{\text{лок.}}$ в среднем на 74,5 % [24].

Исходя из того, что ущерб, наносимый АИС ЮЗ ЭД, увеличивается пропорционально времени реализации угрозы [15], анализ полученных результатов (13), (16) позволяет сделать вывод о том, что сокращение количества криптографических операций приводит к снижению длительности верификации ЭлД, что позволяет уменьшить вероятность реализации деструктивных воздействий на подсистему ЗИ АИС ЮЗ ЭД и, как следствие, повысить уровень защищенности АИС ЮЗ ЭД.

В целях подтверждения данного утверждения произведем анализ данных, полученных в результате использования (14), (15) (таблица 1).

Для представления зависимости вероятности реализации деструктивных воздействий от времени выполнения процедуры контроля целостности ЭлД используем функцию вида

(17) $f(x)=\frac{1}{1+e^{-x}}-0{,}5$.

Таблица 1. Результаты расчета количества операций сравнения ХФ/ЭП с эталонными значениями в соответствии с моментом времени жизненного цикла ЭлД

i	1	2	3	4	5	6
$t_{\text{лок.прототипа}}$	1080	953	826	699	572	445
$t_{\text{лок.разр.}}$	138	137	136	135	134	133
i	7		8		9	
$t_{\text{лок.прототипа}}$	318		191		64	
$t_{\text{лок.разр.}}$	132		131		130	

Исходя из особенностей моделируемого процесса введём допущения:

1) $P(0)=0$;
2) $\lim\limits_{t\to\infty}P(t)=1$,

где P – вероятность успешной реализации деструктивных воздействий.

В таком случае формула (17) примет вид

(18) $P(T_{\text{контр}})=\frac{2}{1+e^{-T_{\text{контр}}}}-1$.

При этом общее время выполнения процедуры контроля целостности ЭлД зависит от количества операций сравнения ХФ/ЭП с эталонными значениями, что можно записать как

(19) $T_{\text{контр.}}=t_{\text{опер.}}\times t_{\text{лок.}}$,

где $T_{\text{контр.}}$ – общее время выполнения процедуры контроля целостности ЭлД; $t_{\text{опер.}}$ – время выполнения операции, причем $t_{\text{опер.}}=10^{-3}$ с.

Используя таблицу 1 и формулы (18), (19), построим график соответствующих зависимостей для известного и разработанного решений (рис. 14).

С помощью полученных результатов определим вероятность успешной реализации деструктивных воздействий при

использовании известного и разработанного решений в процессе жизненного цикла ЭлД (таблица 2).

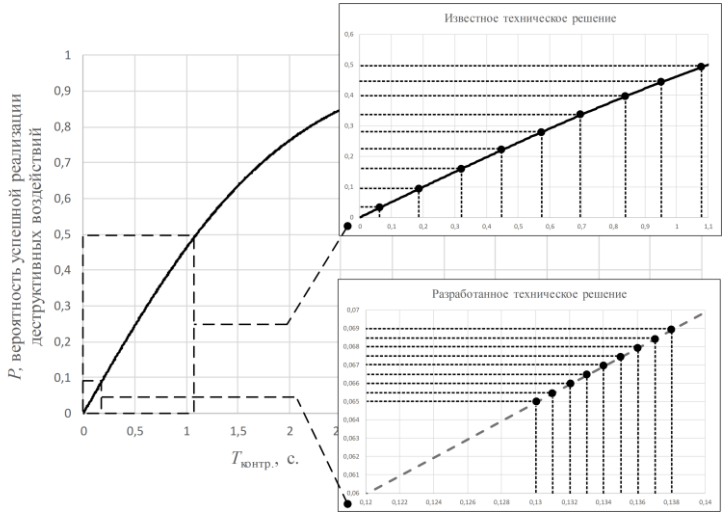

Рис. 14. Зависимость вероятности успешной реализации деструктивных воздействий от времени выполнения процедуры контроля целостности ЭлД

Таблица 2. Вероятность успешной реализации деструктивных воздействий в соответствии с моментом времени жизненного цикла ЭлД

i	1	2	3	4	5	6
$P_{\text{прототипа}}$	0,5	0,45	0,4	0,34	0,28	0,23
$P_{\text{разр.}}$	0,069	0,0685	0,068	0,0675	0,067	0,0665
ΔP_i	**0,431**	**0,3815**	**0,332**	**0,2725**	**0,213**	**0,1635**
i	7		8		9	
$P_{\text{прототипа}}$	0,17		0,09		0,04	
$P_{\text{разр.}}$	0,066		0,0655		0,065	
ΔP_i	**0,104**		**0,0245**		**–0,025**	

Значения разности $P_{\text{прототипа}} - P_{\text{разр.}} = \Delta P_i$ характеризуют снижение вероятности успешной реализации деструктивных воздействий на подсистему ЗИ АИС ЮЗ ЭД при использовании

предложенного решения, что свидетельствует о повышении уровня защищенности АИС ЮЗ ЭД. Однако при несанкционированном изменении ЭлД в 9-й (в примере) момент времени результат уступает известному за счет особенностей реализации криптографических операций (структура бинарного дерева Меркла). Поэтому данный механизм целесообразно применять для ЭлД долгосрочного хранения, в то время как известное решение подходит для контроля целостности ЭлД с коротким сроком жизни.

Таким образом, поставленная задача на разработку метода обеспечения целостности ЭлД на основе бинарного дерева Меркла, удовлетворяющего установленным критериям (4), (5), (6) полностью решена.

Оценка объема памяти W, необходимого для хранения данных формируемых на протяжении всего жизненного цикла ЭлД, при условии размера ХФ 64 бита:

– при использовании известного технического решения [19]:

(20) $W_{\text{прототипа}} = 64(k-1)\ (n+1)$;

– при использовании разработанного технического решения [20]:

(21) $W_{\text{разр.}} = \left(\sum_{i=0}^{\log_2 n} \frac{n}{2^i} + 2 \right) 64k + 64(k-1)$.

Зависимости для ЭлД, содержащего 64 реквизита, в процессе его жизненного цикла $k = 10$ представлены на рис. 15.

Средний объем памяти, требуемый для хранения данных преобразуемых на протяжении всего жизненного цикла ЭлД, при использовании известного и разработанного решения:

(22) $W_{\text{ср.}} = \frac{W_2 + W_3 + \ldots + W_{10}}{n\ (k-1)}$,

где n – количество реквизитов (метаданных), содержащихся в ЭлД; k – количество моментов времени, в которые производятся преобразования ЭлД; W – объем памяти.

Вычисления производятся при условии выполнения десяти преобразований ЭлД в период его жизненного цикла, при этом $k = 2$ – начало преобразований.

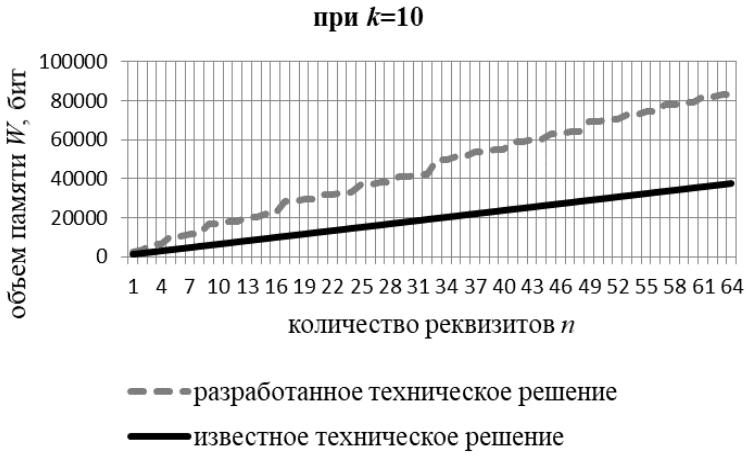

Рис. 15. Результат оценки необходимого объема памяти для хранения данных

С помощью (22) получим:

$W_{\text{ср.прототипа}} = 10720$ (бит);

$W_{\text{ср.разр.}} = 27181$ (бит).

Таким образом, представленные результаты достигаются за счет увеличения объема памяти хранимых данных в среднем в 2,53 раза [24] в сравнении с известным решением [19]. Предполагается, что увеличение объема памяти станет незначительным для АИС ЮЗ ЭД ввиду меньшего количества ЭлД долговременного хранения в сравнении с количеством ЭлД с коротким сроком хранения.

6. Выводы

Введено понятие «интегративный ЭлД», характеризующийся целостностью, достигаемой за счет связности его компонентов. Представленный подход в формировании ЭлД учитывает особенности структуры, динамику и непрерывность его изменений в процессе жизненного цикла. Это соответствует принципам концепции «Индустрия 4.0», заключающимся в реализации функции аудита в режиме реального времени как за счет цен-

трализации обслуживаемых процессов (на примере АИС ЮЗ ЭД с низкой интенсивностью проводимых транзакций), так и за счет их виртуализации (технологии цифровых двойников) (на примере АИС ЮЗ ЭД крупных компаний, имеющих распределенную архитектуру).

Полученные результаты позволяют повысить уровень защищенности АИС ЮЗ ЭД посредством сокращения количества криптографических операций, производимых над ЭлД, а также длительности выполнения процедуры его верификации (обнаружения и локализации компонентов с нарушенной целостностью).

Литература

1. ВАСИЛЬЕВ Н.В., ТИТОВ Г.С., РАКОВ И.В. *Технологии построения систем защищенного электронного документооборота* // Техника средств связи. – 2022. – №2(158). – С. 53–61. – DOI 10.24412/2782-2141-2022-2-53-61.
2. ВЕЛИГУРА А.В. *Моделирование управления большими стохастическими динамическими системами* // Социально-экономические и технические системы: исследование, проектирование, оптимизация. – 2021. – №2(88). – С. 32–39.
3. ВОЛКОВА В.Н., ЛОГИНОВА А.В., ЛЕОНОВА А.Е. и др. *Закономерности теории систем: состояние исследований и применения* // В сб.: «Системный анализ в проектировании и управлении. Сборник научных трудов XXVI Международной научно-практической конференции. В 3-х частях». – СПб., 2023. – С. 65–74.
4. ГВОЗДЕВ В.Е., ВАСИЛЬЕВ В.И., ГУЗАИРОВ М.Б. и др. *Поддержка управления функциональной безопасностью аппаратно-программных комплексов на основе системных архетипов* [Электронный ресурс] // Моделирование, оптимизация и информационные технологии. – 2022. – №10(2). – URL: https://moitvivt.ru/ru/journal/pdf?id=1181 (дата обращения: 10.08.2024). – DOI: 10.26102/2310-6018/2022.37.2.025.
5. *ГОСТ Р ИСО 15489-1-2007. Система стандартов по информации, библиотечному и издательскому делу. Управле-*

ние документами. – Введ. 01.01.2007. – М.: Стандартинформ, 2007. – 34 с.
6. *ГОСТ Р 34.11-2012. Информационная технология. Криптографическая защита информации. Функция хэширования.* – М.: Изд-во стандартов, 2012. – 16 с.
7. *ГОСТ Р 43.0.10-2017. Информационное обеспечение техники и операторской деятельности. Информационные объекты, объектно-ориентированное проектирование в создании технической информации.* – М.: Стандартинформ, 2018. – 23 с.
8. *ГОСТ Р ИСО 15489-1-2019 Система стандартов по информации, библиотечному и издательскому делу. Управление документами. Ч. 1. Понятия и принципы.* – М.: Стандартинформ, 2019. – 23 с.
9. *ГОСТ Р 59341-2021. Системная инженерия. Защита информации в процессе управления информацией системы.* – М.: Стандартинформ, 2021. – 58 с.
10. ДИЧЕНКО С.А. *Модель контроля целостности многомерных массивов данных* // Автоматическое управление и компьютерные науки. – 2021. – Т. 55, № 8. – С. 1188–1193.
11. КАЛИНИН В.И., ЮСУПОВ Р.М., СОКОЛОВ Б.В. *Междисциплинарное взаимодействие и развитие теории систем, кибернетики и информатики* // В сб.: «Системный анализ в проектировании и управлении. Сборник научных трудов XXVI Международной научно-практической конференции. В 3-х частях». – СПб., 2023. – С. 7–13.
12. КАЛИНИН В.Н., СОКОЛОВ Б.В. *Теория системных исследований как основа фундаментальной общенаучной подготовки молодых ученых* // В сб.: «XIV Всероссийское совещание по проблемам управления. Сборник научных трудов». – М., 2024. – С. 3735–3740.
13. *Концепция развития электронного документооборота в хозяйственной деятельности. Решение президиума Правительственной комиссии по цифровому развитию, использованию информационных технологий для улучшения качества жизни и условий ведения предпринимательской деятельности от 25 декабря 2020 г. № 34.* // Официальный

интернет-портал правовой информации [Электронный ресурс]. – 2022. – URL: http:// https://www.nalog.gov.ru/html/sites/www.new.nalog.ru/docs/edo/edo_concept.pdf (дата обращения: 10.08.2024).

14. ЛАРИН М.В. СУРОВЦЕВА Н.Г., ТЕРЕНТЬЕВА Е.В. и др. *Управление документами в цифровой экономике: организация, регламентация, реализация*. – М.: РГГУ, 2021. – 242 с.
15. ЛИПАЕВ В.В. *Надежность и функциональная безопасность комплексов программ реального времени*. – М., 2013. – 176 с.
16. МАХОВ Д.С. *Повышение устойчивости управления параметрами функционирования пространственно-распределенных радиотехнических систем робототехнических комплексов на основе нечетких множеств* // Вопросы оборонной техники. Серия 16: Технические средства противодействия терроризму. – 2020. – №5–6(143–144). – С. 36–44.
17. НОВИКОВ Д.А. *Принцип декомпозиции в задачах управления организационно-техническими системами* // В сб.: «Математическая теория управления и ее приложения (МТУиП-2020). Материалы конференции». – СПб.: Государственный научный центр Российской Федерации АО «Концерн «ЦНИИ «Электроприбор», 2020. – С. 256–259.
18. *Патент РФ 2637486, 04.12.2017*.
19. *Патент РФ 2726930, 16.07.2020*.
20. *Патент РФ 2812304, 29.01.2024*.
21. РЯБИНИН И.А., СТРУКОВ А.В. *Решение одной задачи оценки надежности структурно-сложной системы разными логико-вероятностными методами* // Труды Международной научной школы «Моделирование и анализ безопасности и риска в сложных системах» (МАБР-2019). – 2019. – С. 159–172.
22. 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.

23. ТАЛИ Д.И. *Принцип целостности и интегративности в формировании электронного документа* // Правовая информатика. – 2022. – №3. – С. 72–83. – DOI: 10.21681/1994-1404-2022-3-72-83.
24. ТАЛИ Д.И., ЗАХАРОВ И.Л., СЕВРЮГИН А.А. и др. *Программная модель оценивания способа обеспечения интегративной целостности электронных документов, обрабатываемых автоматизированными информационными системами электронного документооборота* // Программа для ЭВМ № 2023613837. – 2023. – Бюл. №2.
25. ШВАБ К. *Четвертая промышленная революция.* – М.: Эксмо, 2021. – 208 с.
26. BELLARE M. *New Proofs for NMAC and HMAC: Security without Collision-Resistance* // CRYPTO. ePrint Archive, Report 2006/043. – 2006. – P. 1-16.
27. HARADA A., NISHIGAKI M., SOGA M. et al. *A Write-Once Data Management System* // ICITA. Shizuoka University, Johoku, Hamamatsu. –2002. – P. 432–8011.
28. KIAYIAS A., RUSSELL A., BERNARDO D. et al. *Ouroboros: A Provably Secure Proof-of-Stake Blockchain Protocol* // Lecture Notes in Computer Science. – 2017. – Vol. 10401 LNCS. – Springer, Cham. – P. 357–388. – DOI: 10.1007/978-3-319-63688-7_12.
29. KORPELA K., HALLIKAS J., DAHLBERG T. *Digital Supply Chain Transformation toward Blockchain Integration* // Proc. of the 50th Hawaii Int. Conf. on System Sciences. – 2017. – P. 4182–4191. – DOI: 10.24251/HICSS.2017.506.
30. MADHWAL Y., NURLYBAY D., YANOVICH Y. *Blockchain Extension for PostgreSQL Data Storage* // Proc. of the 3rd Blockchain and Internet of Things Conf. (BIOTC-2021), July 8–10, 2021, Ho Chi Minh City, Vietnam. – ACM, New York, NY, USA. – 6 p. – DOI: 10.1145/3475992.3476002.
31. TZIPORA H., BENHAMOUDA F., ANGELO DE CARO et al. *Initial Public Offering (IPO) on Permissioned Blockchain Using Secure Multiparty Computation* // Proc. of the IEEE Int. Conf. on Blockchain (Blockchain). IEEE, 2019. – P. 91–98. – – DOI: 10.1109/Blockchain.2019.00021.

ELECTRONIC DOCUMENT MODEL WITHIN THE INDUSTRY 4.0 PARADIGM

Dmitry Tali, Krasnodar Higher Military School, Krasnodar, Cand.Sc., Phd student (dimatali@mail.ru).
Oleg Finko, Krasnodar Higher Military School, Krasnodar, Doctor of Science, professor (ofinko@yandex.ru).

Abstract: The digital transformation of society and production is gradually entering the stage of Industry 4.0, when the servicing infrastructure, including automated information systems of legally significant electronic document management, will be able to independently understand their environment and adapt to the current conditions of the situation. However, the current stage of development of such systems is characterized by the imperfection of the terminology and the identification of the object of influence (electronic document) with its paper prototype, which leads to a limitation of their functionality. Thus, the existing paradigm of perception of an electronic document does not correspond to the promising level of development of automated information systems of legally significant electronic document management within the framework of the concept of Industry 4.0. The purpose of the work: the formation of models of an electronic document and a description of the method of ensuring its integrity, which allows to guarantee the achievement of the required level of security of automated information systems of legally significant electronic document management, functioning in accordance with the provisions of the concept of Industry 4.0. The methods used: application of cryptographic hash functions to the components (content and metadata) of an electronic document, the results of which are calculated using the binary Merkle tree type in combination with the chain data recording technology. Results of the study: the concept of "integrative electronic document" was introduced, a new structure of the electronic document was proposed, which made it possible to reduce the duration of its verification, and as a result, reduce the risk of destructive impacts on the automated information system.

Keywords: Industry 4.0, content, metadata, electronic document management, electronic document integrity.

УДК 519.7
ББК 32.811

Статья представлена к публикации членом редакционной коллегии А.А. Печниковым.

Поступила в редакцию 17.09.2024.
Опубликована 31.05.2025.