АЛГОРИТМЫ МНОГОУРОВНЕВОГО КОНТРОЛЯ ЦЕЛОСТНОСТИ ЭЛЕКТРОННЫХ ДОКУМЕНТОВ В РАСПРЕДЕЛЕННЫХ СИСТЕМАХ ЭЛЕКТРОННОГО ДОКУМЕНТООБОРОТА

Васильев Я. А.[1], Пешнин М. А.[2], Тали Д. И.[3], Захаров И. Л.[4]

DOI:10.21681/3034-4050-2026-4-25-37

Ключевые слова: *цифровизация, цифровая трансформация документооборота, цифровой документ, целостность электронного документа, целостность системы, распределенные системы электронного документооборота.*

Аннотация

Цель *статьи состоит в разработке алгоритмов подготовки и реализации многоуровневого контроля целостности электронных документов, обрабатываемых распределенными системами электронного документооборота, в условиях деструктивных воздействий злоумышленников.*

Метод исследования: *для достижения поставленной цели используется иерархический подход в алгоритмизации процесса подготовки и проверки целостности многоуровневых структурно-сложных систем на примере электронного документооборота. В целях оценивания полученных результатов использовался логико-вероятностный метод И. А. Рябинина.*

Результаты исследования: *предложен комплекс алгоритмов многоуровневого контроля целостности электронных документов, обрабатываемых распределенными системами электронного документооборота, а также его программная реализация. Численная оценка результатов исследования позволила определить преимущество разработанного решения в сравнении с известным, выражающееся в повышении защищенности исследуемых систем за счет обеспечения целостности их структурных уровней путем обнаружения и локализации электронных документов и их компонентов, подвергшихся несанкционированному изменению в результате вероятной компрометации ключей подписи. Полученный результат достигается за счет применения криптографических преобразований к компонентам (контенту и метаданным) электронных документов по принципу небинарного дерева Меркла в сочетании с технологией цепной записи данных.*

Практическая ценность *разработанного решения состоит в иерархическом применении ключей подписи и проверки, генерируемых сервером вышестоящего уровня, к электронным документам, сформированным на сервере нижестоящего уровня, что позволяет повысить уровень защищенности распределенных систем электронного документооборота в условиях деструктивных воздействий со стороны злоумышленников (внутренних и внешних нарушителей) при вероятной компрометации ключей подписи.*

Вклад авторов: *Васильев Я. А. – разработка программной модели многоуровневого контроля целостности электронных документов, обрабатываемых распределенной системой электронного документооборота; Пешнин М. А. – разработка алгоритмов подготовки и реализации многоуровневого контроля целостности электронных документов, обрабатываемых распределенной системой электронного документооборота; Тали Д. И. – разработка идеи, контроль и коррекция результатов, общее руководство; Захаров И. Л. – верификация (оценка) полученных результатов.*

Введение

Широкое использование цифровых технологий и их непрерывное совершенствование становится завершающим этапом третьей промышленной революции, а также предпосылкой к трансформации общества. Повсеместная цифровизация способствует повышению эффективности бизнес-процессов и государственного управления. Следствием этих тенденций является широкое использование автоматизированных систем (АС), предназначенных для обработки информации, в том числе электронных документов (ЭлД). Активное внедрение систем электронного документооборота (СЭД) и их дальнейшая модернизация является одной из инициатив социально-экономического развития Российской Федерации[5], в рамках которого Правительство Российской Федерации запустило проведение

1 ***Васильев Ярослав Александрович***, сотрудник Краснодарского высшего военного училища им. генерала армии С. М. Штеменко, г. Краснодар, Россия. E-mail: yawasilevs@mail.ru

2 ***Пешнин Макар Андреевич***, сотрудник Краснодарского высшего военного училища им. генерала армии С. М. Штеменко, г. Краснодар, Россия. E-mail: m.peshnin@yandex.ru

3 ***Тали Дмитрий Иосифович***, кандидат технических наук, докторант специальной кафедры Краснодарского высшего военного училища им. генерала армии С. М. Штеменко, г. Краснодар, Россия. E-mail: dimatali@mail.ru

4 ***Захаров Иван Леонидович***, кандидат технических наук, старший преподаватель специальной кафедры Краснодарского высшего военного училища им. генерала армии С. М. Штеменко, г. Краснодар, Россия. E-mail: zakharovivanl@yandex.ru

5 Российская Федерация. Правительство Российской Федерации. Об утверждении стратегического направления в области цифровой трансформации государственного управления: распоряжение Правительства Российской Федерации от 16 марта 2024 г. № 637-р // Информационно-правовой портал Гарант. – URL: https://www.garant.ru/products/ipo/prime/doc/408634367/ (дата обращения: 06.05.2026).

эксперимента по цифровизации процессов электронного документооборота[6,7]. Особенностью этого эксперимента является использование цифровых документов в повседневной деятельности органов государственной власти.

Вместе с тем, говорить о переходе на полноценный безбумажный документооборот преждевременно в связи с возникновением ряда проблемных вопросов, одним из которых является несоответствие нормативной базы требованиям современного этапа технологического развития, что препятствует формированию полноценного юридически значимого электронного документооборота в рамках парадигмы «Индустрия 4.0» [1, 2].

В свою очередь, цифровая трансформация документооборота подразумевает процесс перехода организации на работу с цифровыми документами, сопровождаемый изменениями в ее цифровой и организационной структуре[8]. При этом, специалисты[9] отмечают, что существующие решения построения СЭД не позволяют перейти к принципиально новому способу управления, в целях исключения смешанных форм ЭлД, заменив их на цифровые.

Под цифровым документом (ЦД) понимается категория ЭлД, изначально созданная в цифровой форме с соблюдением правил документирования без издания его на бумажном носителе и подписанного электронной подписью (ЭП)[10]. Вместе с тем, учитывая определение «документированная информация»[11], цифровую документированную информацию (ЦДИ) можно рассматривать, как информационный объект, не подписанный ЭП, но обладающий свойствами ЦД или его части. Подобное расширение термина «электронный документ» позволяет окончательно разграничить бумажный и электронный документооборот, подводя итог в выборе методов и средств обработки такой категории ЭлД.

Изменения в терминологическом аппарате приводят к появлению новой формы перспективных СЭД, представляющей собой информационную инфраструктуру, включающую систему, обеспечивающую управление документами и доступ к ним в течение определенного времени, и системы, являющиеся источниками данных для создания ЦД[12]. Подобное представление СЭД свидетельствует о высокой степени интеграции с различными АС, что указывает на ее распределенную структуру. При этом внедрение в действующие системы таких технологий, как искусственный интеллект, распределенные реестры, облачные технологии и т.д., не только повышают эффективность исследуемых систем, но и способствует возникновению уязвимостей, что вкупе с эволюционным развитием методов и средств криптоанализа вызывает ряд угроз безопасности информации (УБИ), обрабатываемой СЭД [3–6]. Эти обстоятельства вызывают необходимость переосмысления подходов в организации управления ЦД / ЦДИ и их защите на всех этапах жизненного цикла.

Постановка задачи

Целевым предназначением СЭД является управление документами, включающее в себя их создание, ввод в систему и принятие надлежащих мер защиты при хранении. Результатом нарушения целевой функции СЭД в условиях деструктивных воздействий злоумышленников станет нарушение целостности системы в целом[13,14]. Таким образом, возникает задача по предотвращению несанкционированной модификации обрабатываемой информации в период ее жизненного цикла. В связи с этим отметим ряд особенностей, которые должны быть учтены при проектировании перспективных СЭД, в целях совершенствования документационного обеспечения управления и обеспечения защиты информации, циркулирующей в них [7].

При создании ЦД / ЦДИ $D_j^{(t_i)}(j = 1, 2, \ldots, n)$ необходимо учитывать их компонентный состав, представляющий собой в момент времени $t_i\,(i = 0, 1, \ldots, \tau)$ совокупность содержательной информации – контента $K_j^{(t_i)}$, и набора его метаданных $M_j^{(t_i)} = \{m_{i1}, m_{i2}, \ldots, m_{ig}\}$, где $m_{i1}, m_{i2}, \ldots, m_{ig}$ – реквизиты ЦД / ЦДИ (рис. 1). При подобной структуре целостность ЦД / ЦДИ имеет функциональную зависимость от двух компонент (контент

6 Российская Федерация. Правительство Российской Федерации. О проведении эксперимента по цифровизации процессов электронного документооборота, исполнения поручений и контроля исполнительской дисциплины в отдельных федеральных органах исполнительной власти: постановление Правительства Российской Федерации от 8 мая 2025 г. № 629 // Официальный интернет-портал правовой информации. URL: http://publication.pravo.gov.ru/document/0001202505140033 (дата обращения: 06.05.2026).

7 Российская Федерация. Правительство Российской Федерации. О запуске пилотного проекта по формированию единых для госорганов стандартов работы с цифровыми документами и поручениями, включая правила подготовки соответствующих документов и обмена ими: распоряжение Правительства Российской Федерации от 28 мая 2025 г. № 1350 // Информационно-правовой портал Гарант. – URL: https://www.garant.ru/products/ipo/prime/doc/411992288/ (дата обращения: 06.05.2026).

8 ГОСТ Р 59999-2025 «Цифровой документооборот организации. Требования к эталонной модели». – М.: Российский институт стандартизации, 2025.

9 Ларин М. В. Суровцева Н. Г., Терентьева Е. В. и др. Управление документами в цифровой экономике: организация, регламентация, реализация. – М.: РГГУ, 2021. – 242 с.

10 ГОСТ Р 59999-2025 «Цифровой документооборот организации. Требования к эталонной модели». – М.: Российский институт стандартизации, 2025.

11 ГОСТ Р 7.0.8-2025 «Система стандартов по информации, библиотечному и издательскому делу. Делопроизводство и архивное дело. Термины и определения». – М.: Стандартинформ, 2025.

12 ГОСТ Р 59999-2025 «Цифровой документооборот организации. Требования к эталонной модели». – М.: Российский институт стандартизации, 2025.

13 Приказ Министерства связи и массовых коммуникаций «Об утверждении требований по обеспечению целостности, устойчивости функционирования и безопасности информационных систем» от 25 августа 2009 г. № 104 // Информационно-правовой портал Гарант. – URL: https://base.garant.ru/196351/ (дата обращения: 06.05.2026).

14 ГОСТ Р 59341-2021 «Системная инженерия. Защита информации в процессе управления информацией системы». – М.: Стандартинформ, 2021.

и метаданные), имеющих между собой только логическую связь. Учитывая эту особенность, полная или частичная утрата одной из компонент, в условиях деструктивных воздействий злоумышленников, приведет к нарушению целостности ЦД / ЦДИ и, как следствие, сбою в работе СЭД.

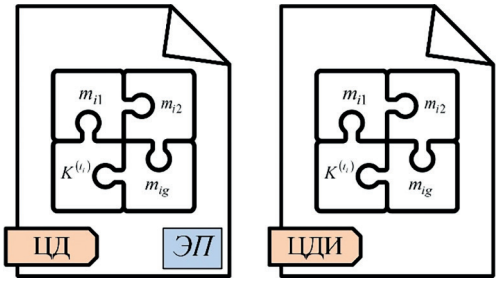


Рис. 1. Схема формирования цифрового ЦД / ЦДИ

С момента ввода в систему ЦД / ЦДИ $D_j^{(t_i)}$ подвергаются постоянным изменениям, что приводит к необходимости контроля их состояния на протяжении всего жизненного цикла. При этом хранение массивов документов $\boldsymbol{D}_{1\ldots n}^{(t_{0,\ldots,\tau})}$ в большинстве современных СЭД осуществляется в виде баз данных, где ЦД / ЦДИ должны быть структурированы таким образом, чтобы контроль целостности производился в режиме реального времени (рис. 2). В противном случае, исходя из структурных особенностей, уничтожение или несанкционированное изменение ЦД / ЦДИ $D_j^{(t_i)}$, содержащихся в массиве $\boldsymbol{D}_{1\ldots n}^{(t_{0,\ldots,\tau})}$, впоследствии приведет к нарушению функционирования системы в целом.

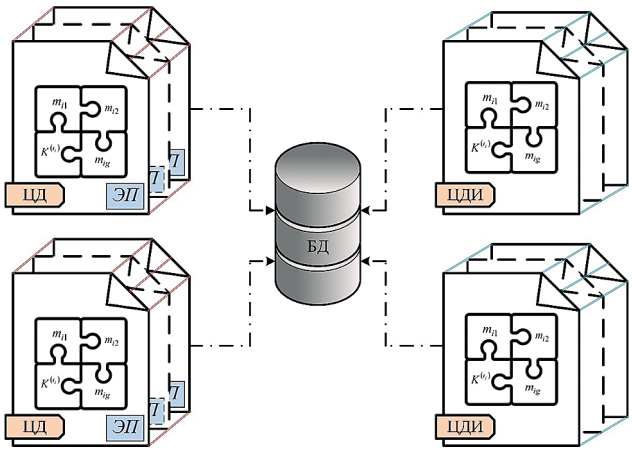


Рис. 2. Динамические изменения ЦД / ЦДИ

Кроме того, учитывая тенденции цифрового развития, современные СЭД носят территориально-распределенный характер с иерархическим принципом управления [8, 9] (рис. 3). В этих условиях выход из строя любой составляющей одного из организационных уровней по указанным выше причинам приведет к нарушению целостности[15] всей распределенной системы.

Рис. 3. Территориально-распределенная СЭД

В целях устранения выявленных недостатков к разработке предлагается комплекс алгоритмов многоуровневого контроля целостности ЦД / ЦДИ в распределенных СЭД на основе технических решений [10–12], представленный в нотации псевдокода.

Критерием качества функционирования распределенной СЭД служит выполнение условия:

$$P_{\text{н.ц.}}^{\text{разр.}} < P_{\text{н.ц.}}^{\text{прототипа}}, \quad (1)$$

где $P_{\text{н.ц.}}^{\text{разр.}}$ и $P_{\text{н.ц.}}^{\text{прототипа}}$ – вероятность нарушения целостности распределенной СЭД при разработанном и существующем способе контроля целостности ЦД / ЦДИ в условиях деструктивных воздействий злоумышленников [7].

Ограничение: в качестве деструктивных воздействий злоумышленников рассматривается компрометация ключей подписи ЦД / ЦДИ, обрабатываемых распределенной СЭД (УБИ 003: использование слабостей криптографических протоколов)[16].

Алгоритм подготовки многоуровневого контроля целостности ЦД / ЦДИ, обрабатываемых распределенной СЭД

В качестве исходных данных используется ЦД / ЦДИ $D_j^{\delta(t_i)}$ в формате *.docx, представляющий собой совокупность содержательной $K_j^{\delta(t_i)}$ и реквизитной частей $M_j^{\delta(t_i)}$, j – номер документа в массиве, где $j = 1, 2, \ldots, n$. $M_j^{\delta(t_i)} = \{m_{i1}, m_{i2}, \ldots, m_{i5}\}$, где $m_{i1}, m_{i2}, \ldots, m_{i5}$ – реквизиты ЦД / ЦДИ, t_i – момент времени, где $i = 0, 1, \ldots, \tau$, а δ – номер уровня сервера, обрабатывающего ЦД / ЦДИ, где $\delta = 1, 2, \ldots, k$. Одна из записей метаданных

15 Приказ Министерства связи и массовых коммуникаций «Об утверждении требований по обеспечению целостности, устойчивости функционирования и безопасности информационных систем» от 25 августа 2009 г. № 104 // Информационно-правовой портал Гарант. – URL: https://base.garant.ru/196351/ (дата обращения: 06.05.2026).

16 Банк данных угроз ФСТЭК // Официальный сайт. – URL: https://bdu.fstec.ru/threat (дата обращения: 06.05.2026).

$m_{i5} \in M_j^{\delta(t_i)}$ определяет уровень значимости ЦД / ЦДИ.

В целях многоуровневого контроля целостности ЦД / ЦДИ в распределенной СЭД применяются ключи $V_U = V_U^*$ (V_U – ключи подписи ЦД / ЦДИ, V_U^* – ключи проверки подписи ЦД / ЦДИ), где $V_U^{\delta(1)} = \{v_1^{\delta(1)}, v_2^{\delta(1)}, \dots, v_{\varsigma_1}^{\delta(1)}\}$ – ключи исполнителя (автора) ЦД / ЦДИ, $V_U^{\delta(2)} = \{v_1^{\delta(2)}, v_2^{\delta(2)}, \dots, v_{\varsigma_2}^{\delta(2)}\}$ – внутренние системные ключи, $V_U^{\delta(3)} = \{v_1^{\delta(3)}, v_2^{\delta(3)}, \dots, v_{\varsigma_3}^{\delta(3)}\}$ – ключи администратора системы.

Algorithm 1: Preparation of multi-level integrity control

Input: $D_j^{\delta(t_i)} = \{K_j^{\delta(t_i)}, M_j^{\delta(t_i)}\}$.
Output: $\boldsymbol{D}_{1\dots n}^{\delta(t_{0,\dots,\tau})}$.
1:**for** δ **in range** (1, ..., k):
2: **for** j **in range** (1, ..., n):
3: **for** i **in range** (0, ..., τ):
4: $H_j^{\delta(t_i)} = f(K_j^{\delta(t_i)})$
5: $h_{j1}^{\delta(t_i)} = f(m_{i1}), h_{j2}^{\delta(t_i)} = f(m_{i2}), \dots, h_{j5}^{\delta(t_i)} = f(m_{i5})$
6: $b_{j1}^{\delta(t_i)} = h_{j1}^{\delta(t_i)} \parallel h_{j2}^{\delta(t_i)}, b_{j2}^{\delta(t_i)} = h_{j3}^{\delta(t_i)} \parallel h_{j4}^{\delta(t_i)}$
7: $h_{j,1-4}^{\delta(t_i)} = b_{j1}^{\delta(t_i)} \parallel b_{j2}^{\delta(t_i)}$
8: $\tilde{H}_j^{\delta(t_i)} = f^{(v_x^{\delta(1)})}(H_j^{\delta(t_i)})$
9: $\tilde{h}_{j,1-4}^{\delta(t_i)} = f^{(v_x^{\delta(2)})}(h_{j,1-4}^{\delta(t_i)})$
10: $\tilde{h}_{j,5}^{\delta(t_i)} = f^{(v_x^{\delta(3)})}(h_{j,5}^{\delta(t_i)})$
11: $\tilde{S}_j^{\delta(t_i)} = f^{(v_x^{\delta(2)})}\tilde{H}_j^{\delta(t_i)} \parallel \tilde{h}_{j,1-4}^{\delta(t_i)} \parallel \tilde{h}_{j,5}^{\delta(t_i)}$
12: **if** ($j = 1$ **and** $i = 0$):
13: $B^{\delta(t_i)} = f^{(v_x^{\delta(2)})}(S_j^{\delta(t_i)})$
14: **else**:
15: $\hat{B}^{\delta(t_{i-1})} = f^{(v_x^{*\delta(2)})}(B^{\delta(t_{i-1})})$
16: $B^{\delta(t_i)} = f^{(v_x^{\delta(2)})}(\hat{B}^{\delta(t_{i-1})} \parallel S_j^{\delta(t_i)})$
17: **if** (δ < k):
18: $\xi^{\delta(t_i)} = f^{(v_x^{\delta+1(2)})}(B^{\delta(t_i)})$
19: **else:**
20: $\xi^{\delta(t_i)} = f^{(v_x^{\delta(2)})}(B^{\delta(t_i)})$
21:**return** $\boldsymbol{D}_{1\dots n}^{\delta(t_{0,\dots,\tau})}$.

В целях пояснения работы алгоритма изложим его реализацию в виде пошагового описания.

Шаг 1–3. Все операции повторяются в отношении каждого ЦД / ЦДИ $D_j^{\delta(t_i)}$ массива на протяжении всего жизненного цикла $t_0, t_1, \dots, t_\tau$ на серверах всех уровней.

Шаг 4–5. Процедура вычисления сигнатур контента $H_j^{\delta(t_i)}$ и метаданных $h_{j1}^{\delta(t_i)}, h_{j2}^{\delta(t_i)}, \dots, h_{j5}^{\delta(t_i)}$ ЦД / ЦДИ $D_j^{\delta(t_i)}$.

Шаг 6. Процедура формирования бинарных пар $b_{j1}^{\delta(t_i)}, b_{j2}^{\delta(t_i)}$ сигнатур метаданных ЦД / ЦДИ $D_j^{\delta(t_i)}$.

Шаг 7. Процедура вычисления корневой сигнатуры $h_{j,1-4}^{\delta(t_i)}$ метаданных ЦД / ЦДИ $D_j^{\delta(t_i)}$ посредством конкатенации вычисленных ранее сигнатур бинарных пар.

Шаг 8. Криптографическое преобразование сигнатуры контента $H_j^{\delta(t_i)}$ ЦД / ЦДИ $D_j^{\delta(t_i)}$ с использованием ключей $v_x^{\delta(1)} \in V_U^{\delta(1)}$, где $x \in \{1, \dots, \varsigma_1\}$.

Шаг 9. Криптографическое преобразование корневой сигнатуры $h_{j,1-4}^{\delta(t_i)}$ метаданных ЦД / ЦДИ $D_j^{\delta(t_i)}$ с использованием ключей $v_x^{\delta(2)} \in V_U^{\delta(2)}$, где $x \in \{1, \dots, \varsigma_2\}$.

Шаг 10. Криптографическое преобразование сигнатуры $h_{j,5}^{\delta(t_i)}$ одной из записей метаданных, определяющей уровень значимости ЦД / ЦДИ $D_j^{\delta(t_i)}$, с использованием ключей $v_x^{\delta(3)} \in V_U^{\delta(3)}$, где $x \in \{1, \dots, \varsigma_3\}$.

Шаг 11. Над преобразованными сигнатурами контента $\tilde{H}_j^{\delta(t_i)}$, метаданных $\tilde{h}_{j,1-4}^{\delta(t_i)}$ и одной из записей метаданных, определяющей уровень значимости $\tilde{h}_{j,5}^{\delta(t_i)}$ ЦД / ЦДИ $D_j^{\delta(t_i)}$ производятся операции конкатенации и криптографического преобразования с использованием ключей $v_x^{\delta(2)} \in V_U^{\delta(2)}$, где $x \in \{1, \dots, \varsigma_2\}$ в целях формирования общей сигнатуры $S_j^{\delta(t_i)}$ ЦД / ЦДИ в i-й момент времени.

Шаг 12–13. В случае первичного добавления документа в систему массив будет состоять из одного документа, что влечет за собой формирование корневой сигнатуры $B^{\delta(t_i)}$ многомерной структуры ЦД / ЦДИ $\boldsymbol{D}_1^{\delta(t_{0,\dots,\tau})}$ путем криптографического преобразования общей сигнатуры ЦД / ЦДИ $S_j^{\delta(t_i)}$ с использованием ключей $v_x^{\delta(2)} \in V_U^{\delta(2)}$, где $x \in \{1, \dots, \varsigma_2\}$.

Шаг 14–16. При добавлении документа в массив, содержащий другие документы, формирование корневой сигнатуры $B^{\delta(t_i)}$ многомерного массива ЦД / ЦДИ $\boldsymbol{D}_{1\dots n}^{\delta(t_{0,\dots,\tau})}$ производится в ходе выполнения операции криптографического преобразования с использованием ключей $v_x^{*\delta(2)} \in V_U^{*\delta(2)}$ ($V_U = V_U^*$), где $x \in \{1, \dots, \varsigma_2\}$ над сигнатурой многомерной структуры ЦД / ЦДИ за предыдущий момент времени $B^{\delta(t_{i-1})}$. После этого выполняются операции конкатенации и криптографического преобразования над преобразованной сигнатурой многомерного массива ЦД / ЦДИ за предыдущий момент времени $\hat{B}^{\delta(t_{i-1})}$ и общей сигнатурой $S_j^{\delta(t_i)}$ ЦД / ЦДИ за текущий момент времени с использованием ключей $v_x^{\delta(2)} \in V_U^{\delta(2)}$, где $x \in \{1, \dots, \varsigma_2\}$.

Шаг 17–18. В случае выполнения операций вычисления сигнатур на серверах нижестоящего уровня, полученный результат $B^{\delta(t_{i-1})}$ отправляется в подсистему защиты информации, размещенную на сервере вышестоящего уровня, где над ним в целях вычисления сигнатуры контроля целостности массива ЦД / ЦДИ уровня δ производится операция криптографического преобразования с использованием ключей вышестоящего уровня $v_x^{\delta+1(2)} \in V_U^{\delta+1(2)}$.

Шаг 19–20. В случае выполнения операций вычисления сигнатур на сервере максимального уровня полученный результат $B^{\delta(t_i)}$ подлежит хранению в подсистеме защиты информации, размещенной на этом сервере, где над ним в целях вычисления сигнатуры контроля целостности

массива ЦД / ЦДИ максимального уровня δ производится операция криптографического преобразования с использованием, вырабатываемых им ключей $v_x^{\delta(2)} \in V_U^{\delta(2)}$.

Последующее сохранение в доверенной среде сигнатур: $H_j^{\delta(t_i)}$, $h_{j,1-5}^{\delta(t_i)}$, $\tilde{H}_j^{\delta(t_i)}$, $\tilde{h}_{j,1-4}^{\delta(t_i)}$, $\tilde{h}_{j,5}^{\delta(t_i)}$, $S_j^{\delta(t_i)}$, $B^{\delta(t_i)}$, $\xi^{\delta(t_i)}$ ЦД / ЦДИ, вычисленных на шагах 1–20.

Шаг 21. Процедура вывода многомерных массивов ЦД / ЦДИ, обрабатываемых на функционально разделенных серверах, в среду обработки, причем связность ЦД / ЦДИ достигается за счет применения криптографических преобразований к компонентам (контенту и метаданным) ЦД / ЦДИ по принципу небинарного дерева Меркла с получением корневой сигнатуры всего массива, обрабатываемых ЦД / ЦДИ.

Алгоритм реализации многоуровневого контроля целостности ЦД / ЦДИ, обрабатываемых распределенной СЭД

В качестве исходных данных используются многомерные массивы ЦД / ЦДИ $\mathbf{D}_{1\ldots n}^{\delta(t_0,\ldots,\tau)}$ в формате *.docx.

Algorithm 2: Implementation of multi-level integrity control

Input: $\boldsymbol{D}_{1\ldots n}^{\delta(t_0,\ldots,\tau)}$.

Output: $\boldsymbol{D}_{1\ldots n}^{\delta(t_0,\ldots,\tau)'}$.

1:**for** δ **in range** (1, ..., *k*):
2: **for** *j* **in range** (1, ..., *n*):
3: **for** *i* **in range** (0, ..., τ):
4: $H_j^{\delta(t_i)**} = f(K_j^{\delta(t_i)**})$
5: $h_{j1}^{\delta(t_i)**} = f(m_{i1}), h_{j2}^{\delta(t_i)**} = f(m_{i2}), \ldots, h_{j5}^{\delta(t_i)**} = f(m_{i5})$
6: $b_{j1}^{\delta(t_i)**} = h_{j1}^{\delta(t_i)**} \parallel h_{j2}^{\delta(t_i)**}$, $b_{j2}^{\delta(t_i)**} = h_{j3}^{\delta(t_i)**} \parallel h_{j4}^{\delta(t_i)**}$
7: $\tilde{h}_{j,1-4}^{\delta(t_i)**} = b_{j1}^{\delta(t_i)**} \parallel b_{j2}^{\delta(t_i)**}$
8: $\tilde{H}_j^{\delta(t_i)**} = f^{(v_x^{\delta(1)})}(H_j^{\delta(t_i)**})$
9: $\tilde{h}_{j,1-4}^{\delta(t_i)**} = f^{(v_x^{\delta(2)})}(h_{j,1-4}^{\delta(t_i)})$
10: $\tilde{h}_{j,5}^{\delta(t_i)**} = f^{(v_x^{\delta(3)})}(h_{j,5}^{\delta(t_i)**})$
11: $S_j^{\delta(t_i)**} = f^{(v_x^{\delta(2)})}(\tilde{H}_j^{\delta(t_i)**}) \parallel \tilde{h}_{j,1-4}^{\delta(t_i)**} \parallel \tilde{h}_{j,5}^{\delta(t_i)**}$
12: **if** ($j = 1$ **and** $i = 0$):
13: $B^{\delta(t_i)**} = f^{(v_x^{\delta(2)})}(S_j^{\delta(t_i)**})$
14: **else**:
15: $\hat{B}^{\delta(t_{i-1})**} = f^{(v_x^{*\delta(2)})}(B^{\delta(t_{i-1})**})$
16: $B^{\delta(t_i)**} = f^{(v_x^{\delta(2)})}(\hat{B}^{\delta(t_{i-1})**} \parallel S_j^{\delta(t_i)**})$
17: **if** ($\delta < k$):
18: $\xi^{\delta(t_i)**} = f^{(v_x^{\delta+1(2)})}(B^{\delta(t_i)**})$
19: **else**:
20: $\xi^{\delta(t_i)**} = f^{(v_x^{\delta(2)})}(B^{\delta(t_i)**})$
21: **if** $\xi^{\delta(t_i)**} = \xi^{\delta(t_i)*}$:
22: **print** (“Целостность $\boldsymbol{D}_{1\ldots n}^{\delta(t_0,\ldots,\tau)}$ подтверждена”)
23: **else**:
24: print (“Целостность $\boldsymbol{D}_{1\ldots n}^{\delta(t_0,\ldots,\tau)}$ нарушена”)
25:**return** $\mathbf{D}_{1\ldots n}^{\delta(t_0,\ldots,\tau)'}$.

В целях пояснения работы алгоритма изложим его реализацию в виде пошагового описания.

Шаг 1–3. Все повторные операции вычисления выполняются в отношении каждого ЦД / ЦДИ $D_j^{(t_i)}$ массива на протяжении всего его жизненного цикла $t_0, t_1, \ldots, t_\tau$ на серверах всех уровней.

Шаг 4–5. Процедура вычисления сигнатур контента и метаданных ЦД / ЦДИ, где символ $H_j^{\delta(t_i)**}$ обозначает повторно вычисленную сигнатуру контента, символы $h_{j1}^{\delta(t_i)**}$, $h_{j2}^{\delta(t_i)**}$, ... , $h_{j5}^{\delta(t_i)**}$ обозначают повторно вычисленные сигнатуры метаданных.

Шаг 6. Повторная процедура формирования бинарных пар $b_{j1}^{\delta(t_i)**}$, $b_{j2}^{\delta(t_i)**}$ сигнатур метаданных ЦД / ЦДИ.

Шаг 7. Повторная процедура вычисления корневой сигнатуры $h_{j,1-4}^{\delta(t_i)}$ метаданных ЦД / ЦДИ посредством конкатенации вычисленных ранее бинарных сигнатур.

Шаг8.Повторноекриптографическоепреобразование сигнатуры контента $H_j^{\delta(t_i)**}$ ЦД / ЦДИ с использованием ключей $v_x^{\delta(1)} \in V_U^{\delta(1)}$, где $x \in \{1, \ldots, \varsigma_1\}$.

Шаг 9. Повторное криптографическое преобразование корневой сигнатуры $h_{j,1-4}^{\delta(t_i)}$ метаданных ЦД / ЦДИ с использованием ключей $v_x^{\delta(2)} \in V_U^{\delta(2)}$, где $x \in \{1, \ldots, \varsigma_2\}$.

Шаг 10. Повторное криптографическое преобразование сигнатуры $h_{j5}^{\delta(t_i)**}$ одной из записей метаданных, определяющей уровень значимости ЦД / ЦДИ, с использованием ключей $v_x^{\delta(3)} \in V_U^{\delta(3)}$, где $x \in \{1, \ldots, \varsigma_3\}$.

Шаг 11. Повторная процедура вычисления общей сигнатуры $S_j^{\delta(t_i)**}$ ЦД / ЦДИ в *i*-й момент времени путем конкатенации сигнатуры контента $\tilde{H}_j^{\delta(t_i)**}$, корневой сигнатуры метаданных $\tilde{h}_{j,1-4}^{\delta(t_i)**}$ и сигнатуры одной из метаданных, определяющей уровень значимости $\tilde{h}_{j,5}^{\delta(t_i)**}$ с последующим криптографическим преобразованием с использованием ключей $v_x^{\delta(2)} \in V_U^{\delta(2)}$, где $x \in \{1, \ldots, \varsigma_2\}$.

Шаг 12–13. В случае, если многомерная структура ЦД / ЦДИ $\boldsymbol{D}_1^{\delta(t_0,\ldots,\tau)}$ состоит из одного документа, корневая сигнатура $B^{\delta(t_i)**}$ будет повторно формироваться путем криптографического преобразования общей сигнатуры ЦД / ЦДИ $S_j^{\delta(t_i)**}$ с использованием ключей $v_x^{\delta(2)} \in V_U^{\delta(2)}$, где $x \in \{1, \ldots, \varsigma_2\}$.

Шаг 14–16. В случае, если многомерный массив ЦД / ЦДИ $\boldsymbol{D}_{1\ldots n}^{\delta(t_0,\ldots,\tau)}$ состоит из *n* документов, корневая сигнатура $B^{\delta(t_i)**}$ будет повторно формироваться в ходе выполнения операции криптографического преобразования с использованием ключей $v_x^{\delta(2)} \in V_U^{\delta(2)}$ ($V_U = V_U^*$), где $x \in \{1, \ldots, \varsigma_2\}$ над сигнатурой многомерного массива ЦД / ЦДИ за предыдущий момент времени $B^{\delta(t_{i-1})**}$.

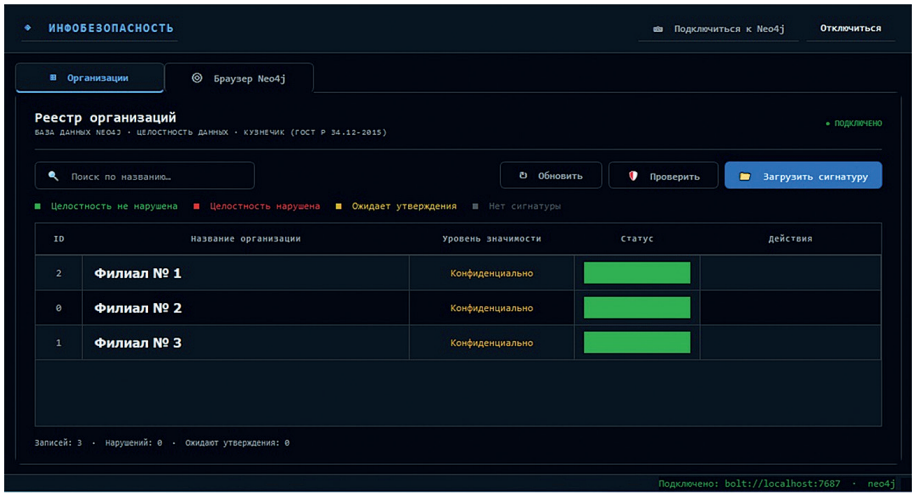


Рис. 4. Главное диалоговое окно программы

После этого выполняются операции конкатенации и криптографического преобразования над преобразованной сигнатурой многомерной структуры ЦД / ЦДИ за предыдущий момент времени $\hat{B}^{\delta(t_{i-1})**}$ и общей сигнатурой $S_j^{\delta(t_i)**}$ ЦД / ЦДИ за текущий момент времени с использованием ключей $v_x^{\delta(2)} \in V_U^{\delta(2)}$, где $x \in \{1, \dots, \varsigma_2\}$.

Шаг 17–18. В случае повторного выполнения операций вычисления сигнатур на серверах нижестоящего уровня, полученный результат $B^{\delta(t_i)**}$ отправляется в подсистему защиты информации, размещенную на сервере вышестоящего уровня, где над ним в целях повторного вычисления сигнатуры контроля целостности массива ЦД / ЦДИ уровня δ производится операция криптографического преобразования с использованием ключей вышестоящего уровня $v_x^{\delta+1(2)} \in V_U^{\delta+1(2)}$.

Шаг 19–20. В случае повторного выполнения операций вычисления сигнатур на сервере максимального уровня полученный результат $B^{\delta(t_i)**}$ подлежит хранению в подсистеме защиты информации, размещенной на этом же сервере, где над ним в целях повторного вычисления сигнатуры контроля целостности массива ЦД / ЦДИ максимального уровня δ производится операция криптографического преобразования с использованием вырабатываемых им ключей $v_x^{\delta(2)} \in V_U^{\delta(2)}$.

Выгрузка сигнатур контроля целостности массивов ЦД / ЦДИ $\xi^{\delta(t_i)*}$, прошедших процедуру хранения, из доверенной среды.

Шаг 21–24. Процедура сравнения повторно вычисленных сигнатур контроля целостности массивов ЦД / ЦДИ $\xi^{\delta(t_i)**}$ за все моменты времени $t_0, t_1, \dots, t_\tau$ их жизненного цикла, с сигнатурами контроля целостности массивов ЦД / ЦДИ $\xi^{\delta(t_i)*}$, прошедших процедуру хранения, в целях локализации нарушения целостности конкретного массива ЦД / ЦДИ. В результате сравнения делается заключение, какой из массивов ЦД / ЦДИ $\boldsymbol{D}_{1\dots n}^{\delta(t_{0,\dots,\tau})}$ был изменен.

Шаг 25. Процедура вывода многомерных массивов $\boldsymbol{D}_{1\dots n}^{\delta(t_{0,\dots,\tau})'}$ ЦД / ЦДИ, прошедших процедуру проверки, в среду обработки.

Программная реализация разработанного комплекса алгоритмов

Разработанные алгоритмы позволяют обеспечить интегративную целостность ЭлД (шаг 4–11 алгоритма № 1), а также контроль целостности многомерной структуры ЭлД (шаг 12–16 алгоритма № 2). Эти функции были реализованы в программном виде [13, 14]. Однако, предыдущие решения не учитывают процесс формирования сигнатур контроля целостности массивов ЦД / ЦДИ $\xi^{\delta(t_i)}$ и сравнение текущих значений со значениями, хранимыми в доверенной среде для проверки целостности системы. В целях практической реализации данного процесса разработано программное решение [15], экранные формы которого представлены на рис. 4–9.

Для загрузки сигнатур контроля целостности массивов ЦД / ЦДИ $\xi^{\delta(t_i)*}$ пользователю необходимо нажать кнопку «Загрузить сигнатуру». В открывшемся диалоговом окне (рис. 5) добавить файлы, полученные от предприятий нижнего организационного уровня и содержащие сигнатуры контроля целостности, а также указать криптографический ключ, предназначенный для их преобразования. После нажатия кнопки «Загрузить» преобразованные сигнатуры сохраняются в графовой базе данных Neo4j.

В случае повторной загрузки сигнатуры контроля целостности пользователь утверждает ее

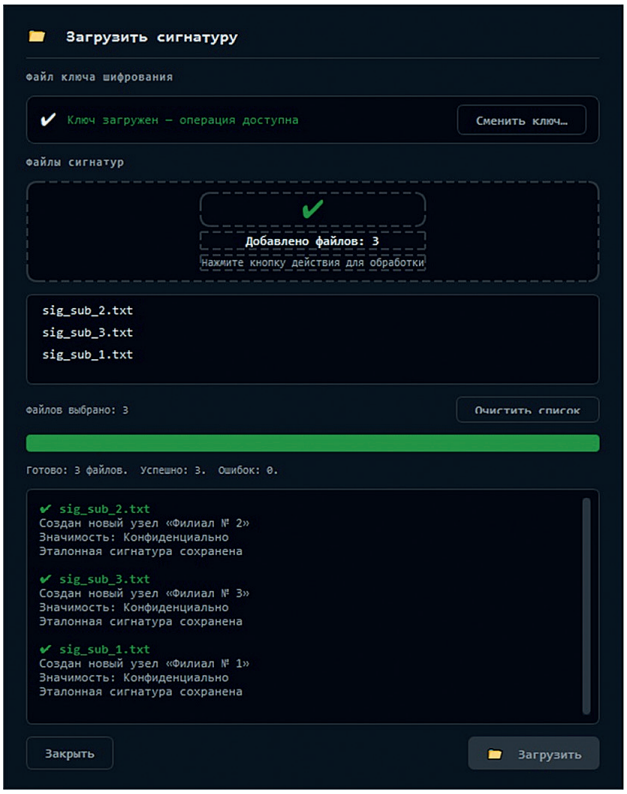


Рис. 5. Экранная форма загрузки сигнатур контроля целостности

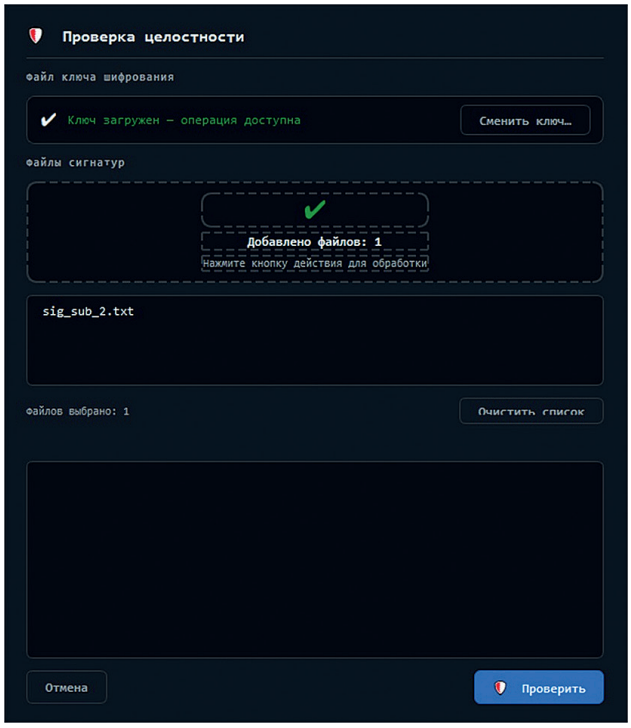


Рис. 7. Экранная форма проверки целостности многомерных массивов ЦД / ЦДИ, обрабатываемых в структурных организациях

новое значение для внесения изменений в базу данных (рис. 6).

Для проверки целостности многомерных массивов ЦД / ЦДИ, обрабатываемых в организациях нижнего организационного уровня, необходимо нажать кнопку «Проверить», после чего во всплывающей форме (рис. 7) указать проверяемые сигнатуры и криптографический ключ, с применением которого они были преобразованы перед сохранением в базе данных. Далее нажать кнопку «Проверить».

Результаты проверки представлены на рисунках 8–9.

Предполагается, что представленное программное решение найдет свое применение в перспективных СЭД в целях обеспечения целостности обрабатываемых массивов информации.

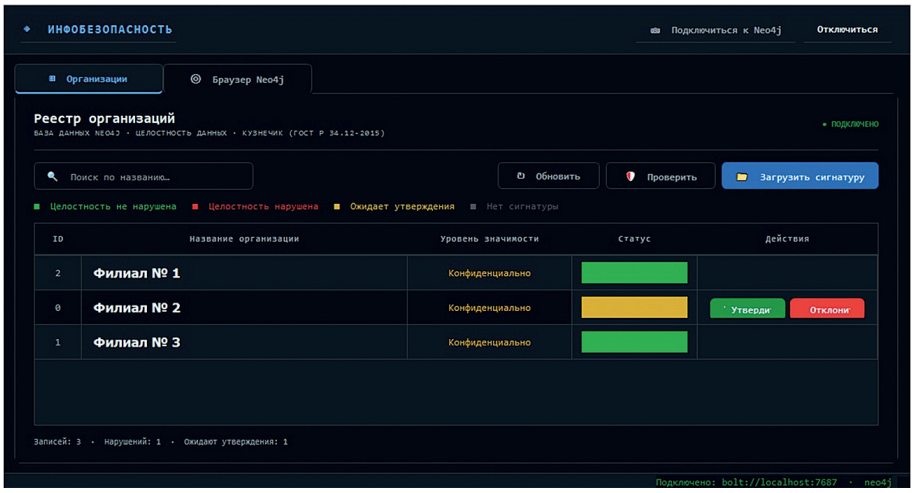
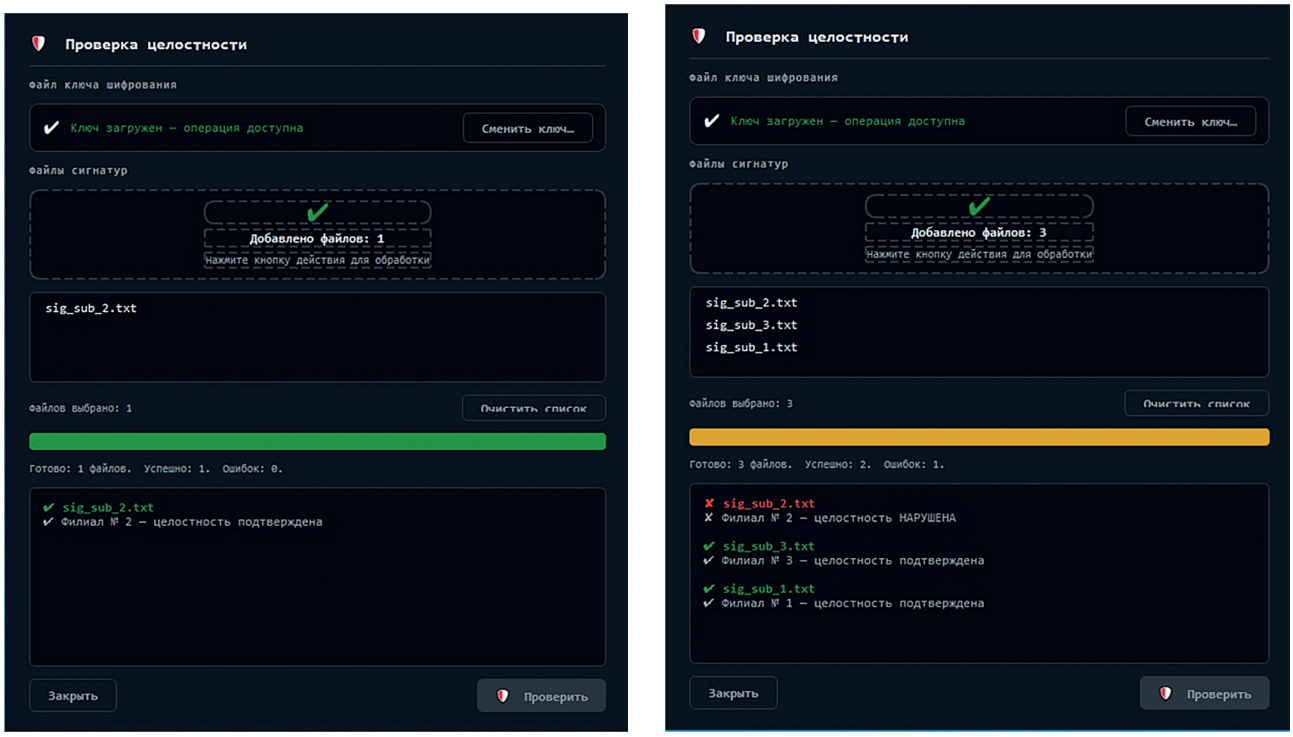


Рис. 6. Экранная форма в случае повторной загрузки сигнатуры контроля целостности



а) *б)*

Рис. 8. Заключение о состоянии обрабатываемых многомерных массивов ЦД / ЦДИ: а) при отсутствии нарушений целостности; б) при наличии нарушений целостности

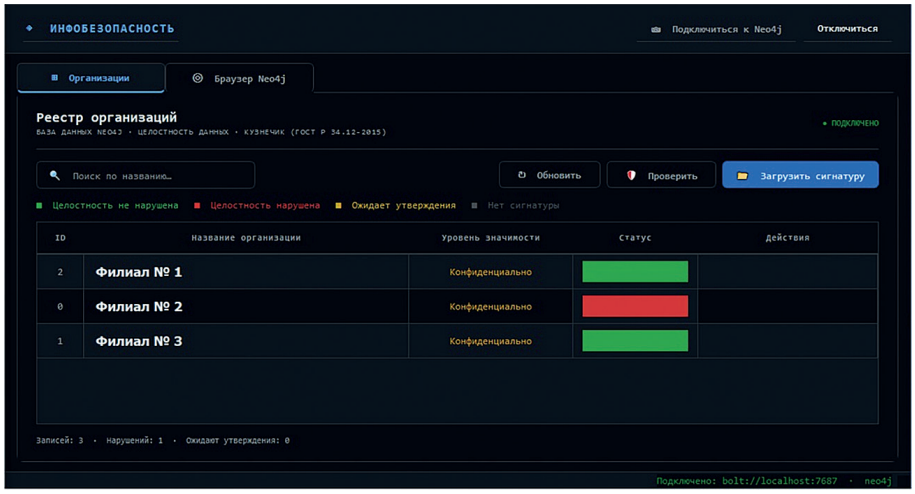


Рис. 9. Главное диалоговое окно программы при наличии элементов с нарушением целостности

Оценка полученных результатов и выводы

Воспользуемся логико-вероятностным методом (ЛВМ) [16-21] для сравнения уровня защищенности распределенной СЭД, обеспечиваемого за счет использования разработанного решения [15], с прототипом, в качестве которого выступает распределенная СЭД с «линейной» процедурой[17] контроля целостности массива ЦД / ЦДИ, осуществляемой внутри каждого уровня независимо от вышестоящего.

17 Месарович М. Д., Мако Д., Такахара И. Теория иерархических многоуровневых систем // М.: Мир, 1973. – 344 с.

В целях моделирования процесса функционирования распределенной СЭД с «линейной» процедурой контроля целостности массива ЦД / ЦДИ, построим один из возможных сценариев ее перехода в опасное состояние (нарушение целостности) в результате успешной реализации УБИ злоумышленником (рис. 10). В этом случае функционирование распределенной СЭД будет нарушено при условии одновременной компрометация ключей: $v_x^{\delta(1)} \in V_U^{\delta(1)}$, $v_x^{\delta(2)} \in V_U^{\delta(2)}$, $v_x^{\delta(3)} \in V_U^{\delta(3)}$, вырабатываемых сервером одного из трех уровней.

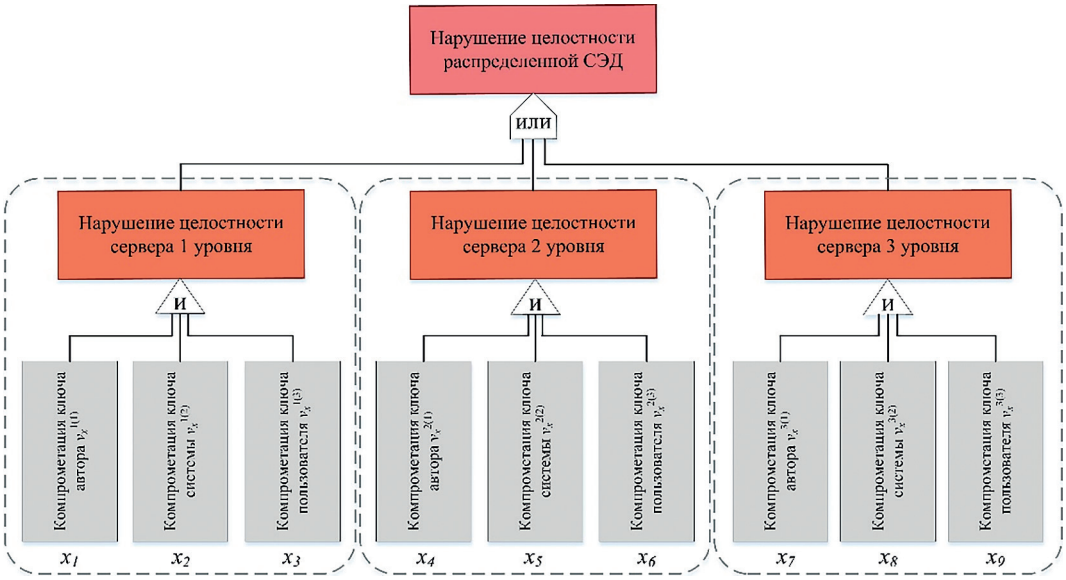


Рис. 10. Сценарий реализации угрозы нарушения функционирования распределенной СЭД при осуществлении «линейной» процедуры контроля целостности массива ЦД / ЦДИ

Рассматриваемому сценарию будет соответствовать следующая ФАЛ, описывающая функцию перехода распределенной СЭД в опасное состояние:

$$f(x_1, \dots, x_9) = \\ = (x_1 \wedge x_2 \wedge x_3) \vee (x_4 \wedge x_5 \wedge x_6) \vee (x_7 \wedge x_8 \wedge x_9). \quad (2)$$

В соответствии с ЛВМ преобразуем полученную ФАЛ (2) в форму перехода к полному замещению, допускающую замену логических переменных соответствующими вероятностями. Для этого представим рассматриваемую функцию в виде СДНФ. Затем осуществим переход от логической функции к ее вероятностной интерпретации. При этом каждая буква заменяется вероятностью ее равенства единице: $P\{x_r = 1\} = R_r$, $P\{x_r = 0\} = P\{\bar{x}_r = 1\} = Q_r = 1 - R_r$, где R_r – вероятность наступления события x_r.

Принимая во внимание отсутствие статистических данных и, как следствие, допущение о том, что все события равновероятны, получим следующий полином, определяющий вероятность перехода распределенной СЭД в опасное состояние[18]:

$$P^{f(x_1, \dots, x_9) = 1} = R^9 - 3R^6 + 3R^3. \quad (3)$$

18 Рябинин И. А. Надежность и безопасность структурно-сложных систем // СПб.: Политехника, 2012. – 276 с.

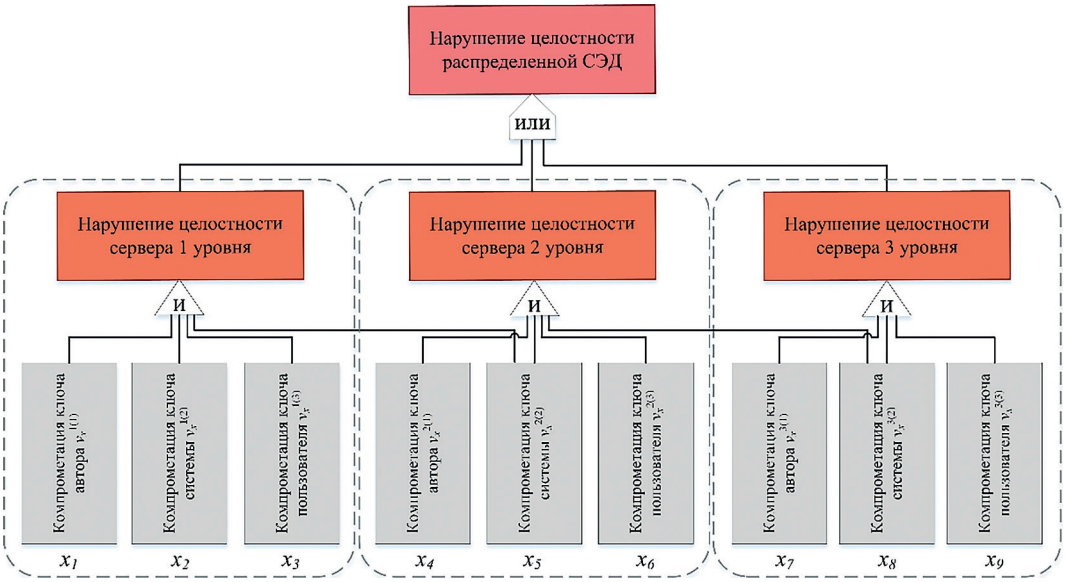


Рис. 11. Сценарий реализации угрозы нарушения функционирования распределенной СЭД с учетом разработанного программного решения

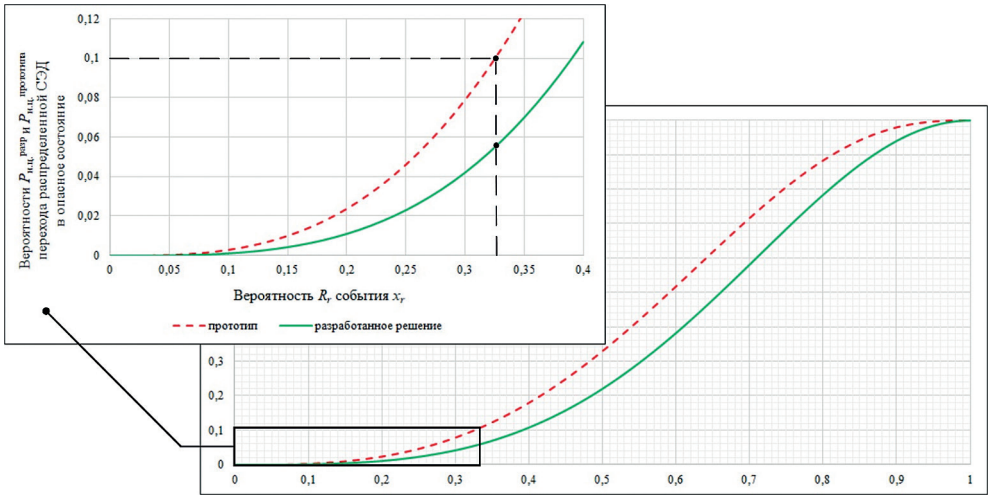


Рис. 12. Сравнительный анализ зависимостей вероятности перехода распределенной СЭД в опасное состояние в результате реализации угрозы компрометации ключей подписи

Далее на основе ЛВМ построим сценарий реализации угрозы нарушения функционирования распределенной СЭД с учетом разработанного решения (рис. 11). В этом случае функционирование распределенной СЭД будет нарушено при одновременной компрометации ключей: $v_x^{\delta(1)} \in V_U^{\delta(1)}$, $v_x^{\delta(2)} \in V_U^{\delta(2)}$, $v_x^{\delta(3)} \in V_U^{\delta(3)}$, вырабатываемых сервером одного из трех уровней, а также ключа $v_x^{\delta+1(2)} \in V_U^{\delta+1(2)}$, вырабатываемого сервером вышестоящего уровня.

При условии, что все события равновероятны, получим следующий полином, определяющий вероятность перехода распределенной СЭД в опасное состояние:

$$P^{f(x_1, \ldots, x_9)\,9} - 2R^7 - R^6 + 2R^4 + R^3. \quad (4)$$

На основе (3) и (4) построим графики зависимостей вероятностей $P_{н.ц.}^{разр.}$ и $P_{н.ц.}^{прототипа}$ перехода распределенной СЭД в опасное состояние в результате реализации угрозы компрометации ключей подписи с учетом «линейной» процедуры контроля целостности массива ЦД / ЦДИ, осуществляемой внутри каждого уровня независимо от вышестоящего, и разработанного решения (рис. 12).

Рассчитаем выигрыш разработанного решения [15] в сравнении с использованием «линейной» процедуры контроля целостности массива ЦД / ЦДИ, осуществляемой внутри каждого уровня независимо от вышестоящего:

$$Ср.\ выигрыш = \left(1 - \frac{\int_0^{0,33} P_{н.ц.}^{разр.} dR}{\int_0^{0,33} P_{н.ц.}^{прототипа} dR}\right) \cdot 100\ \%. \quad (5)$$

Расчет выигрыша производился на практически значимом интервале вероятности перехода распределенной СЭД в опасное состояние (0; ...; 0,1), так как при переходе за его пределы события x_r будет считаться реализованными, а распределенная СЭД перейдет в опасное состояние (средний выигрыш составил ≈ 49 % при $R \approx 0{,}33$).

Полученные результаты свидетельствуют о достижении критерия (1), а применение разработанного решения позволяет повысить уровень защищенности распределенных СЭД за счет снижения вероятности нарушения целостности их структурных уровней. Достоверность полученных результатов определяется использованием апробированного математического аппарата логико-вероятностного метода.

Предполагается, что предлагаемый комплекс алгоритмов и представленная программная модель могут послужить основой для разработки протоколов функционирования существующих и перспективных СЭД.

Литература

1. Ларин М. В. Цифровая трансформация управления документами // В сборнике: «Генеральный регламент»: 300 лет на службе России: От коллежского делопроизводства до цифровой трансформации управления документами. Материалы Международной научно-практической конференции. Российский государственный гуманитарный университет, Историко-архивный институт, Факультет архивоведения и документоведения, Кафедра автоматизированных систем документационного обеспечения управления, Российское общество историков-архивистов (РОИА). Москва, 2021. – С. 10–19.
2. Ларин М. В. Документоведение в цифровую эпоху // В сборнике: Пичетовские чтения – 2024. История: наука, образование, память. Материалы международной научно-практической конференции, посвященной 90-летию исторического факультета Белорусского государственного университета. Минск, 2024. – С. 16–22.
3. Doosti M. Unclonability and Quantum Cryptanalysis: From Foundations to Applications // Laboratory for Foundations of Computer Science. School of Informatics. University of Edinburgh, 2022. – P. 341.
4. Veda Chatiyode, Baghavathi Priya S. Cryptanalysis of post-quantum cryptographic schemes: securing IoT and smart cities in the quantum era // In book: Post-Quantum cryptography and IoT communications for sustainable urban development. 2025. – Pp. 171–204.
5. Xie H., Xia Q., Wang K., Li Y., Yang L. Quantum automated tools for finding impossible differentials // Mathematics, 2024. – № 12, 2598. – URL: doi.org/10.3390/math12162598.
6. Blessing Guembe, Ambrose Azeta, Sanjay Misra, Victor Chukwudi Osamor, Luis Fernandez-Sanz & Vera Pospelova (2022) // The Emerging Threat of Ai-driven Cyber Attacks: A Review, Applied Artificial Intelligence, 36:1, 2037254, DOI: 10.1080/08839514.2022.2037254.
7. Тали Д. И., Финько О. А. Концептуальная модель функционирования системы цифрового документооборота в рамках парадигмы «Индустрия 4.0» // Вопросы кибербезопасности, 2025. – № 5 (69). – С. 68–77. – DOI 10.21681/2311-3456-2025-5-68-77.
8. Саяркин В. А., Михайличенко А. В., Паращук И. Б. Вопросы формулировки комплексных показателей надежности и защищенности системы электронного документооборота на базе распределенной сети мобильных дата-центров // В сборнике: «Проблемы технического обеспечения войск в современных условиях. Труды VII межвузовской научно-практической конференции». Санкт-Петербург, 2022. – С. 210–214.
9. Das M., Tao X., Cheng J.C.P. A Secure and Distributed Construction Document Management System Using Blockchain // In book: Proceedings of the 18th International Conference on Computing in Civil and Building Engineering, 2021. – P. 850–862. – DOI:10.1007/978-3-030-51295-8_59.
10. Тали Д. И., Финько О. А. и др Способ обеспечения интегративной целостности электронного документа // Патент на изобретение RU 2812304, опубл. 29.01.2024, бюл. № 4.
11. Тали Д. И., Финько О. А., Диченко С. А. Способ формирования и контроля целостности многомерной структуры электронных документов // Патент на изобретение RU 2840783, опубл. 28.05.2025, бюл. № 16.
12. Тали Д. И., Финько О. А. Способ и система распределенного контроля целостности электронных документов при вероятной компрометации ключей подписи // Патент на изобретение RU 2844401, опубл. 29.07.2025, бюл. № 22.
13. Пешнин М. А., Васильев Я. А., Тали Д. И. Алгоритмическое обеспечение интегративной целостности электронных документов, обрабатываемых системами электронного документооборота // Защита информации. Инсайд, 2025. – № 6 (126). – С. 38–44.
14. Пешнин М. А., Васильев Я. А., Тали Д. И. Программная модель контроля целостности многомерных массивов электронных документов // Свидетельство о государственной регистрации программы для ЭВМ RU 2025697115, опубл. 23.12.2025.
15. Пешнин М. А., Васильев Я. А., Тали Д. И. Программная модель многоуровневого контроля целостности многомерных массивов электронных документов // Свидетельство о государственной регистрации программы для ЭВМ RU 2026665081, опубл. 20.05.2026.
16. Калашников А. О., Аникина Е. В., Бугайский К. А., Молотов А. А. Применение логико-вероятностного метода в информационной безопасности. Часть 6 // Вопросы кибербезопасности, 2025. – № 1 (65). – С. 96–107. – DOI: 10.21681/2311-3456-2025-1-96-107.
17. Калашников А. О., Аникина Е. В., Бугайский К. А. Применение логико-вероятностного метода в информационной безопасности. Часть 7 // Вопросы кибербезопасности, 2026. – № 1 (71). – С. 59–68. – DOI: 10.21681/2311-3456-2026-1-59-68.
18. Попков Г. В., Гумиров В. Ш., Гумиров А. В., Овчинникова Е. А. К вопросу применения логико-вероятностных методов для реализации систем поддержки, принятия решений в области кибербезопасности // Телекоммуникации, 2025. – № 2. – С. 32–39.
19. Крюкова Е. С., Ткаченко В. В., Михайличенко А. В., Паращук И. Б. Вопросы оценки надежности современных систем хранения данных для мобильных дата-центров // Наукоемкие технологии в космических исследованиях Земли, 2021. – Т. 13. – № 5. – С. 86–95.
20. Демин А. В. Глубокое обучение адаптивных систем управления на основе логико-вероятностного подхода // Известия Иркутского государственного университета. Серия: Математика, 2021. – Т 38. – С. 65– 83. – DOI: https://doi.org/10.26516/1997-7670.2021.38.65
21. Викторова В. С., Степанянц А. С. Вычисление показателей надежности в немонотонных логико-вероятностных моделях многоуровневых систем // Автоматика и телемеханика, 2021. – № 5. – С. 106–123. – DOI: 10.31857/S000523102105007X.

MULTI-LEVEL INTEGRITY CONTROL ALGORITHMS FOR ELECTRONIC DOCUMENTS IN DISTRIBUTED ELECTRONIC DOCUMENT MANAGEMENT SYSTEMS

Vasiliev Y. A.[19], Peshnin M. A.[20], Tali D. I.[21], Zakharov I. L.[22]

Keywords: *digitalization, digital transformation of document management, digital document, integrity of electronic document, integrity of system, distributed electronic document management systems.*

Abstract

The purpose *of the article is to develop algorithms for the preparation and implementation of multi-level integrity control of electronic documents processed by distributed electronic document management systems under the conditions of destructive influences of intruders.*

Research method: *to achieve this goal, a hierarchical approach to algorithmic design of the process of preparing and verifying the integrity of multi-level, structurally complex systems was used, using electronic document management as an example. I. A. Ryabinin's logical-probabilistic method was used to evaluate the obtained results.*

Research results: *a set of algorithms for multi-level integrity control of electronic documents processed by distributed electronic document management systems, as well as its software implementation, are proposed. A numerical evaluation of the research results revealed the advantage of the developed solution over existing approaches, resulting in increased security of the studied systems by ensuring the integrity of their structural levels through the detection and localization of electronic documents and their components that have been subject to unauthorized modification due to the potential compromise of signature keys. This result is achieved by applying cryptographic transformations to components (content and metadata) of electronic documents based on the non-binary Merkle tree principle in combination with chain-based data recording technology.*

The practical value *of the developed solution lies in the hierarchical application of signature and verification keys generated by a higher-level server to electronic documents generated on a lower-level server, which allows for an increased level of security for distributed electronic document management systems in the face of destructive attacks from intruders (internal and external) in the event of a possible compromise of signature keys.*

Contribution of the authors: *Vasiliev Ya. A. – development of a software model for multi-level control of the integrity of electronic documents processed by a distributed electronic document management system; Peshnin M. A. – development of algorithms for the preparation and implementation of multi-level integrity control of electronic documents processed by a distributed electronic document management system; Tali D. I. – development of the idea, control and correction of results, general management; Zakharov I. L. – verification (evaluation) of the obtained results.*

References

1. Larin M.V. Tsifrovaya transformatsiya upravleniya dokumentami // V sbornike: «General'nyy reglament»: 300 let na sluzhbe Rossii: Ot kollezhskogo deloproizvodstva do tsifrovoy transformatsii upravleniya dokumentami. Materialy Mezhdunarodnoy nauchno-prakticheskoy konferentsii. Rossiyskiy gosudarstvennyy gumanitarnyy universitet, Istoriko-arkhivnyy institut, Fakul'tet arkhivovedeniya i dokumentovedeniya, Kafedra avtomatizirovannykh sistem dokumentatsionnogo obespecheniya upravleniya, Rossiyskoye obshchestvo istorikov-arkhivistov (ROIA). M.:, 2021. – Pp. 10–19.
2. Larin M. V. Dokumentovedeniye v tsifrovuyu epokhu // V sbornike: Pichetovskiye chteniya – 2024. Istoriya: nauka, obrazovaniye, pamyat'. Materialy mezhdunarodnoy nauchno-prakticheskoy konferentsii, posvyashchennoy 90-letiyu istoricheskogo fakul'teta Belorusskogo gosudarstvennogo universiteta. Minsk, 2024. – Pp. 16–22.
3. Doosti M. Unclonability and Quantum Cryptanalysis: From Foundations to Applications // Laboratory for Foundations of Computer Science. School of Informatics. University of Edinburgh, 2022. – P. 341.
4. Veda Chatiyode, Baghavathi Priya S. Cryptanalysis of post-quantum cryptographic schemes: securing IoT and smart cities in the quantum era // In book: Post-Quantum cryptography and IoT communications for sustainable urban development, 2025. Pp. 171–204.
5. Xie H., Xia Q., Wang K., Li Y., Yang L. Quantum automated tools for finding impossible differentials // Mathematics, 2024. – No 12, 2598. – URL: doi.org/10.3390/math12162598.
6. Blessing Guembe, Ambrose Azeta, Sanjay Misra, Victor Chukwudi Osamor, Luis Fernandez-Sanz & Vera Pospelova (2022) // The Emerging Threat of Ai-driven Cyber Attacks: A Review, Applied Artificial Intelligence, 36:1, 2037254, DOI: 10.1080/08839514.2022.2037254.

19 ***Yaroslav A. Vasiliev***, employee of the Krasnodar Higher Military School named after General of the Army S. M. Shtemenko, Krasnodar, Russia. E-mail: yawasilevs@mail.ru

20 ***Makar A. Peshnin***, employee of the Krasnodar Higher Military School named after General of the Army S. M. Shtemenko, Krasnodar, Russia. E-mail: m.peshnin@yandex.ru

21 ***Dmitry I. Tali***, Ph.D. of Technical Sciences, doctoral student of the special department of the Krasnodar Higher Military School named after General of the Army S. M. Shtemenko, Krasnodar, Russia. E-mail: dimatali@mail.ru

22 ***Ivan L. Zakharov***, Ph.D. of Technical Sciences, Senior Lecturer of the Special Department of the Krasnodar Higher Military School named after General of the Army S. M. Shtemenko, Krasnodar, Russia. E-mail: zakharovivanl@yandex.ru

7. Tali D. I., Fin'ko O. A. Kontseptual'naya model' funktsionirovaniya sistemy tsifrovogo dokumentooborota v ramkakh paradigmy «Industriya 4.0» // Voprosy kiberbezopasnosti, 2025. – No 5 (69). – Pp. 68–77. – DOI: 10.21681/2311-3456-2025-5-68-77.
8. Sayarkin V. A., Mikhaylichenko A. V., Parashchuk I. B. Voprosy formulirovki kompleksnykh pokazateley nadezhnosti i zashchishchennosti sistemy elektronnogo dokumentooborota na baze raspredelennoy seti mobil'nykh data-tsentrov // V sbornike: «Problemy tekhnicheskogo obespecheniya voysk v sovremennykh usloviyakh. Trudy VII mezhvuzovskoy nauchno-prakticheskoy konferentsii». Sankt-Peterburg, 2022. – Pp. 210–214.
9. Das M., Tao X., Cheng J. C. P. A Secure and Distributed Construction Document Management System Using Blockchain // In book: Proceedings of the 18th International Conference on Computing in Civil and Building Engineering, 2021. – Pp. 850–862. – DOI:10.1007/978-3-030-51295-8_59.
10. Tali D. I., Fin'ko O. A. i dr. Sposob obespecheniya integrativnoy tselostnosti elektronnogo dokumenta // Patent na izobreteniye RU 2812304, opubl. 29.01.2024, byul. No 4.
11. Tali D. I., Fin'ko O. A., Dichenko S. A. Sposob formirovaniya i kontrolya tselostnosti mnogomernoy struktury elektronnykh dokumentov // Patent na izobreteniye RU 2840783, opubl. 28.05.2025, byul. No 16.
12. Tali D. I., Fin'ko O. A. Sposob i sistema raspredelennogo kontrolya tselostnosti elektronnykh dokumentov pri veroyatnoy komprometatsii klyuchey podpisi // Patent na izobreteniye RU 2844401, opubl. 29.07.2025, byul. No 22.
13. Peshnin M. A., Vasil'yev Ya. A., Tali D. I. Algoritmicheskoye obespecheniye integrativnoy tselostnosti elektronnykh dokumentov, obrabatyvayemykh sistemami elektronnogo dokumentooborota // Zashchita informatsii. Insayd, 2025. – No 6 (126). – Pp. 38–44.
14. Peshnin M. A., Vasil'yev Ya.A., Tali D. I. Programmnaya model' kontrolya tselostnosti mnogomernykh massivov elektronnykh dokumentov // Svidetel'stvo o gosudarstvennoy registratsii programmy dlya EVM RU 2025697115, opubl. 23.12.2025.
15. Peshnin M. A., Vasil'yev Ya. A., Tali D. I. Programmnaya model' mnogourovnevogo kontrolya tselostnosti mnogomernykh massivov elektronnykh dokumentov // Svidetel'stvo o gosudarstvennoy registratsii programmy dlya EVM RU 2026665081, opubl. 20.05.2026.
16. Kalashnikov A. O., Anikina Ye.V., Bugayskiy K. A., Molotov A. A. Primeneniye logiko-veroyatnostnogo metoda v informatsionnoy bezopasnosti. Chast' 6 // Voprosy kiberbezopasnosti, 2025. – No 1 (65). – Pp. 96–107. DOI: 10.21681/2311-3456-2025-1-96-107.
17. Kalashnikov A. O., Anikina Ye. V., Bugayskiy K. A. Primeneniye logiko-veroyatnostnogo metoda v informatsionnoy bezopasnosti. Chast' 7 // Voprosy kiberbezopasnosti, 2026. – No 1 (71). – Pp. 59–68. – DOI: 10.21681/2311-3456-2026-1-59-68.
18. Popkov G. V., Gumirov V. Sh., Gumirov A. V., Ovchinnikova Ye. A. K voprosu primeneniya logiko-veroyatnostnykh metodov dlya realizatsii sistem podderzhki, prinyatiya resheniy v oblasti kiberbezopasnosti // Telekommunikatsii, 2025. – No 2. – Pp. 32–39.
19. Kryukova Ye. S., Tkachenko V. V., Mikhaylichenko A. V., Parashchuk I. B. Voprosy otsenki nadezhnosti sovremennykh sistem khraneniya dannykh dlya mobil'nykh data-tsentrov // Naukoyemkiye tekhnologii v kosmicheskikh issledovaniyakh Zemli, 2021. – V. 13. – No 5. – Pp. 86–95.
20. Demin A. V. Glubokoye obucheniye adaptivnykh sistem upravleniya na osnove logiko-veroyatnostnogo podkhoda // Izvestiya Irkutskogo gosudarstvennogo universiteta. Seriya: Matematika, 2021. – V. 38. – Pp. 65–83. DOI: https://doi.org/10.26516/1997-7670.2021.38.65.
21. Viktorova V. S., Stepanyants A. S. Vychisleniye pokazateley nadezhnosti v nemonotonnykh logiko-veroyatnostnykh modelyakh mnogourovnevykh sistem // Avtomatika i telemekhanika, 2021. – No 5. – Pp. 106–123. DOI: 10.31857/S000523102105007X .