Алгоритмическое решение проблемы сохранения аутентичности цифровых данных

А. В. Соловьев

Федеральное государственное учреждение Федеральный исследовательский центр "Информатика и управление" Российской академии наук, г. Москва, Россия

Аннотация. Цифровые данные становятся ключевым фактором деловых и производственных процессов, поэтому любое нарушение их аутентичности может привести к весьма серьезным последствиям. В исследовании дается краткая характеристика заявленной проблемы сохранения аутентичности цифровых данных. Приводится обзор существующих способов решения проблемы, их достоинства и недостатки. Автором вводятся определения аутентичности, долговременного хранения и иные понятия и определения. В качестве решения поставленной проблемы в статье предложен алгоритм сохранения аутентичности цифровых данных при их долговременном хранении. Предложенный алгоритм подробно описан в рамках данной статьи. Основой практической реализации алгоритма является инвентаризация электронных подписей. В статье описано практическое применение реализации предложенного алгоритма. На основании успешного применения делается утверждение, что предложенный алгоритм, прошедший проверку практикой, позволят решить поставленную в статье проблему. В статье также рассматриваются возможные перспективы дальнейших исследований и практического применения предложенного алгоритма.

Ключевые слова: аутентичность цифровых данных, долговременное хранение, цифровая экономика, электронная подпись, блокчейн.

DOI 10.14357/20718632210102

Введение

Проблема долговременной сохранности цифровых данных в условиях цифровой экономики является крайне актуальной, что показано во множестве научных работ (например, [1-3]). Ведущие мировые экономики заняты решением проблемы сохранности цифровых данных [4, 5]. Для российской экономики решение этой задачи также актуальна, тем более что цифровые данные согласно Программt «Цифровая экономика Российской Федерации» (Утверждена распоряжением Правительства Российской Федерации от 28 июля 2017 г. № 1632-р) являются «ключевым фактором производства». Конечно, проблема долговременной сохранности цифровых данных является сложной комплексной проблемой, и сводить ее только к проблеме сохранению аутентичности неверно. К проблемам долговременной сохранности относятся также проблемы: независимости, интерпретируемости, аутентичности, надежности, потери семантики, устойчивости к внешним воздействиям, безопасности. Подробнее об общей постановке задачи сохранности цифровых данных описано в [6, 7]. Однако одной из важнейших проблем при долговременном хранении цифровых данных является проблема сохранения их аутентичности, т.е. уверенность спустя годы и десятилетия, что цифровые данные являются неизменными и возможно гарантированное подтверждение их авторства.

Решению проблемы сохранения аутентичности цифровых данных при долговременном хранении посвящена данная статья. Предложен алгоритм сохранения аутентичности, с помощью которого может быть решена поставленная проблема в рамках программного обеспечения программно-аппаратных систем хранения цифровых данных.

Приведем основные понятия и определения, использующиеся в тексте статьи. Определения, помеченные символом «*» введены в рамках данного исследования, остальные взяты из действующих нормативных документов.

- Электронный архив (ЭА)* – структурированное хранилище неизменяемых цифровых данных: электронных оригиналов документов (электронных изображений бумажных документов), созданное на основе законов и правил ведения архивов на конкретной территории (в конкретной стране).
- Длительное (долговременное) хранение* – хранение цифровых данных в течение более 5 лет.
- Долговременная сохранность – «период времени, в течение которого» цифровые данные «поддерживаются в качестве доступного и аутентичного свидетельства (доказательства)» (ГОСТ Р 54989-2012 /ISO TR 18492:2005 Обеспечение долговременной сохранности электронных документов (вступил в силу с 01.05.2013)).
- Аутентичные цифровые данные – цифровые данные «точность, надежность и целостность которых сохраняется с течением времени» (ГОСТ Р 54989-2012 /ISO TR 18492:2005 Обеспечение долговременной сохранности электронных документов (вступил в силу с 01.05.2013)).

Используемые в статье понятия «Электронная подпись (ЭП)», «Усиленная квалифицированная ЭП», «Удостоверяющий центр (УЦ)» соответствуют Федеральному закону «Об электронной подписи» №63-ФЗ.

1. Краткий обзор проблемы сохранения аутентичности

Из обзора правил построения ЭА в разных странах можно увидеть, что существуют три подхода к решению проблемы сохранения аутентичности.

Первый подход связан с организацией «суперзащищенного» архива цифровых данных, в котором многократное резервирование программно-технических средств ЭА, организационные меры ограничения доступа к данным должны полностью решить проблему сохранения аутентичности (примеры США, Австралии, Великобритании [8-12]).

Второй подход связан с тем, что обеспечение аутентичности возлагается на электронную подпись (пример Германии, [13]).

Третий связан с использованием технологий блокчейн [2, 14, 15].

Недостатки первого подхода связаны с тем, что «суперзащищенный» ЭА:

- может «потерять» часть данных при миграции данных, существует также возможность изменить данные при миграции;
- журналы операций также могут быть потеряны (изменены) при миграции;
- наличие в системе функций хеширования данных, хранение контрольных сумм и т.д. в РФ, например, не будет являться гарантированным подтверждением целостности данных т.к. ПО для государственных структур в РФ, содержащее криптопреобразование информации, должно быть в обязательном порядке сертифицировано;
- высокие затраты на техническую поддержку, обусловленные необходимостью постоянного обеспечения высокой степени защиты и резервирования технических средств и каналов связи.

Недостатки второго подхода (использование ЭП):

- потеря данных при миграции, однако, ее вероятность будет ниже, т.к. и цифровые данные и операции с ними могут быть заверены ЭП;
- необходимость интегрировать ЭА с сертифицированными средствами криптозащиты цифровых данных;
- сертификаты и открытые ключи ЭП обладают ограниченным сроком действия.

Недостатки третьего подхода (использование технологий блокчейн):

- в общем случае высокая энергоемкость криптопреобразований;
- отсутствие сертифицированных решений для использования в Российской Федерации;

- проблемы с долговременным хранением цепочек блоков, аналогичные проблемам долговременного хранения цифровых данных: аутентичность, интерпретируемость, независимость от алгоритмов криптографической защиты, используемых в конкретной реализации блокчейн.

Можно утверждать, что в условиях создающейся цифровой экономики РФ, второй подход выглядит намного более практичным. Действительно:

- есть сертифицированные средства криптозащиты, технологии работы с ними отработаны годами;
- появляется третья (по отношению к разработчикам и пользователям ЭА) незаинтересованная в нарушении аутентичности сторона (криптопровайдер), что позволяет больше гарантировать решение проблемы;
- цифровые данные, заверенные ЭП оказываются относительно независимыми от ПО ЭА и могут мигрировать в любую программно-аппаратную среду, что повышает сохранность аутентичности данных, даже если программная среда ЭА выйдет из строя;
- не требуется отдельно организовывать долговременное хранение, аутентичность, интерпретируемость цепочек блоков;
- достигается относительная независимость от алгоритмов криптографической защиты.

Однако полностью полагаться только на ЭП не приходится. Причин тому несколько.

Во-первых, сертификаты и открытые ключи ЭП обладают ограниченным сроком действия, поэтому спустя год или 5 лет при обращении к цифровым данным с просроченной ЭП можно получить сообщение о некорректности ЭП, что поставит под сомнение аутентичность данных.

ЭП удобно использовать в системах электронного документооборота, поскольку в них сроки работы с данными ограничиваются жизненным циклом документов, однако в системах, обеспечивающих длительное хранение, гарантированно возникнут проблемы просроченных сертификатов и ключей подписи.

Недавно вступивший в силу Федеральный закон №379-ФЗ фактически приравнивает электронный документ, заверенный усиленной квалифицированной ЭП нотариуса, к подписанному и заверенному печатью документу бумажному. Однако не оговаривается, как потом хранить электронный документ, какой срок его действия, как реестры нотариальных дел, ведущиеся в электронной форме, будут долговременно храниться и т.д.

Можно утверждать, что только использования усиленной квалифицированной ЭП недостаточно, т.к. до конца нет уверенности о моменте времени, в который ЭП была установлена. Тем самым необходимо, чтобы ЭП содержала подтвержденный штамп времени. Только такой электронный нотариат позволит подтвердить момент времени, когда ЭП была установлена и доказать ее действительность на установленный момент времени согласно №63-ФЗ.

Во-вторых, без наличия сертификата ЭП проверка подписи невозможна. Сертификат хранится в УЦ, однако нет гарантии, что УЦ (и база сертификатов) не прекратят свою деятельность раньше окончания срока хранения цифровых данных.

Тем самым можно утверждать, что цепочка сертификатов ключей ЭП должна обязательно содержаться внутри ЭП или передаваться в ЭА вместе с ЭП. Только в этом случае, при наличии всех сертификатов ЭП, есть хоть какая-то гарантия, что спустя десятилетия аутентичность заверенных ЭП цифровых данных можно будет подтвердить. Нужно еще учесть, что при проверке ЭП может потребоваться список отзыва сертификатов (СОС), актуальный на момент проставления подписи. Он также должен храниться в ЭА, т.к. по закону №63-ФЗ, УЦ должен хранить сертификаты в течение как минимум, срока их годности, который составляет не более 5 лет. Однако этот срок может быть существенно ниже срока хранения цифровых данных.

В-третьих, за срок длительного хранения цифровых данных могут измениться стандарты криптозащиты, и исчезнуть или перестать функционировать криптографические средства проверки ЭП, которая была установлена несколько десятилетий назад.

2. Алгоритмическое решение проблемы аутентичности данных

Для решения задачи обеспечения аутентичности цифровых данных автором исследования предложен алгоритм инвентаризации электрон-

ной подписи. Основная идея алгоритма – организация периодического нового заверения цифровых данных новой ЭП с сохранением реквизитов автора ЭП из старой подписи. Максимальная величина периода заверения новой подписью равна сроку действия сертификата предыдущей ЭП. Так как средства криптозащиты изменяются сравнительно медленно, такой подход дает гарантию независимости цифровых данных от конкретных средств криптографической защиты.

Предложенный алгоритм представлен на Рис. 1.

Алгоритм, названный автором алгоритмом инвентаризации электронной подписи, может быть описан следующей последовательностью шагов:

1. Проверяется «старая» ЭП, установленная на цифровых данных с помощью имеющихся сертифицированных средств криптографической защиты.

2. В случае подтверждения ее подлинности, проверяется штамп времени ЭП, который подтверждает момент установки ЭП.

3. В случае положительного результата проверки штампа времени, факт положительной

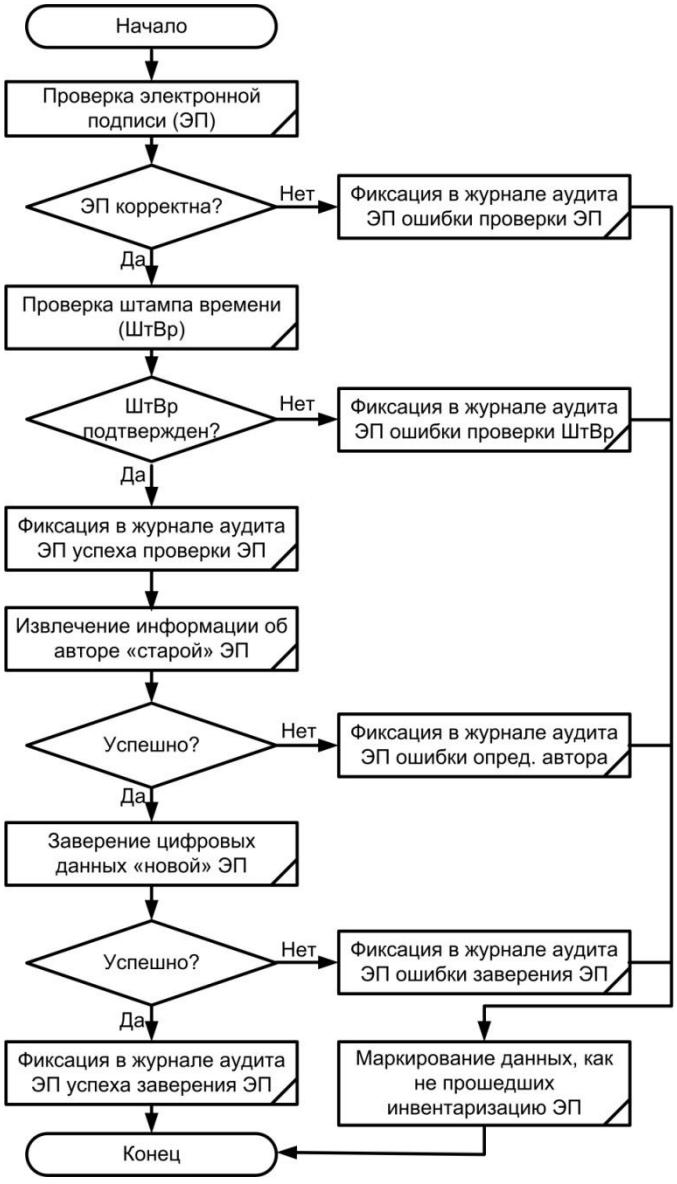

Рис. 1. Алгоритм инвентаризации электронной подписи

проверки ЭП фиксируется в журнале аудита ЭП и заверяется специальной архивной ЭП с указанием авторства проверяющего сотрудника ЭА.

4. Далее из сертификата «старой» ЭП извлекаются данные об авторе ЭП.

5. Формируется «новая» ЭП, в которую записываются данные об авторе «старой» ЭП, новой ЭП заверяются повторно цифровые данные, включая «старую» ЭП. Цепочка старых ЭП сохраняется на случай необходимости детального разбора всех этапов инвентаризации.

6. Факт заверения «новой» ЭП фиксируется в системном журнале инвентаризации ЭП, журнальная информация заверяется архивной ЭП с указанием авторства проверяющего сотрудника ЭА.

Если хотя бы одна проверка на шагах алгоритма 1 – 4 не дала положительного результата, то в журнале инвентаризации ЭП фиксируется факт нарушения аутентичности, цифровые данные помечаются как не прошедшие процедуру инвентаризации ЭП. В этом случае необходимо подробное расследование причин нарушения аутентичности.

Необходимо заметить, что процедура инвентаризации ЭП не исключает подмены или уничтожения цифровых данных административным персоналом, эксплуатирующим ЭА, но гарантирует невозможность проведения данной операции операторами ввода.

Дополнительной защитой от злонамеренных действий административного персонала является обязательное автоматическое ведение журнала аудита. Подменить цифровые данные и журнал аудита более сложная задача, особенно при разделении прав доступа на эти объекты.

В процессе выполнения алгоритма инвентаризации подтверждается корректность ЭП цифровых данных, далее данные заверяются дополнительной ЭП в подтверждение факта инвентаризации. Новая ЭП, как более криптостойкая, исключит или, по крайней мере, существенно снизит, риск появления в будущем поддельных цифровых данных, заверенных старыми «правильными» ЭП в БД ЭА.

Мощность компьютеров постоянно увеличивается, поэтому теоретически со временем возможна подделка цифровых данных (коллизия первого рода), когда подбираются цифровые данные для ЭП за приемлемое время. Борьба с этой коллизией требует постоянного усложнения криптоалгоритмов и повышения разрядности ключей ЭП. Заверяя цифровые данные новой ЭП, можно гарантировать их аутентичность при долговременном хранении.

Конечно, еще остаются вопросы, например, взаимодействия ЭА и УЦ. Особенно часто с ним сталкиваются, когда в ЭА хранятся цифровые данные, подписанные ЭП, которые выданы разными УЦ, например, в различных регионах РФ. В таком случае возникают ситуации, когда ЭА не может проверить ЭП поступивших цифровых данных из-за отсутствия корневых сертификатов УЦ. В качестве одного из промежуточных решений можно предложить организовать хранение в ЭА всех сертификатов ЭП, СОС и много другой дополнительной информации, на основании которой может быть проведено расследование и установлена аутентичность цифровых данных.

3. Практическая реализация алгоритма

Идеи, заложенные при создании алгоритма инвентаризации ЭП, прошли практическое использование в рамках создания большой территориально-распределенной информационной системы – Система электронного архива персонифицированного учета Пенсионного фонда Российской Федерации. Эта крупная и сложная информационная система функционирует более 16 лет в 80 регионах РФ. В настоящее время в БД Системы хранится более 50% документов персонифицированного учета Пенсионного фонда РФ.

Результаты практического применения в рамках крупной территориально-распределенной информационной системы дают основания утверждать об успешном решении задачи обеспечения сохранности аутентичности цифровых данных на достаточно длительном сроке хранения. За время эксплуатации менялись алгоритмы криптозащиты, техническое и программное обеспечение информационной системы. Тем не менее цифровые данные были полностью сохранены.

Практическая апробация алгоритма была выполнена также в ряде реализаций систем долговременного хранения первичных электронных документов.

В перспективе данный алгоритм может стать частью комплексной технологии организации долговременного хранения цифровых данных электронных архивов различных уровней с неограниченным сроком хранения данных.

Заключение

Несмотря на то, что в последнее время появились нормативные документы, регламентирующие многие вопросы долговременной сохранности (например, ГОСТ Р 54989-2012/ISO TR 18492:2005), тем не менее, все технологические вопросы обеспечения долговременной сохранности, в частности сохранения аутентичности, возлагаются на разработчиков информационных систем.

В качестве решения проблемы сохранения аутентичности цифровых данных в данной статье предложен алгоритм обеспечения инвентаризация ЭП, который можно реализовать в программно-аппаратной среде долговременного хранения.

Предложенный алгоритм прошел проверку практикой в ряде программных проектов электронных архивов, предназначенных для долговременного хранения цифровых данных электронных документов.

В дальнейших исследованиях планируется выполнить программные реализации представленного алгоритма для различных типов и форматов цифровых данных, а также разработать алгоритм инвентаризации цифровых носителей данных для систем долговременного хранения.

В перспективе предложенный алгоритм может стать частью комплексной технологии долговременного хранения цифровых данных.

Литература

1. Суровцева, Н.Г. Хранение электронных документов: зарубежный опыт // Вестник культуры и искусства. 2017. №4(52). С. 17-23.
2. Swan, M. Blockchain: Blueprint for a New Economy. O'Reilly Media, Inc., 2015. 149 p. ISBN 978-1-491-92049-7.
3. Даниленко, А.Ю. и др. Применение технологии блокчейн в информационных системах. Часть 2. Подтверждение авторства и обеспечение целостности // Системы высокой доступности. 2018. 14(1). С. 9-12.
4. Universal Electronic Records Management (ERM) Requirements. U.S. National Archives and Records Administration. 2017. Режим доступа: https://www.archives.gov/records-mgmt/policy/universalermrequirements (дата обращения 01.02.2021).
5. National Archives Announces a New Model for the Preservation and Accessibility of Presidential Records. U.S. National Archives and Records Administration. 2017. Режим доступа: https://www.archives.gov/press/press-releases/2017/nr17-54 (дата обращения 01.02.2021).
6. Баканова, Н.Б., Соловьев, А.В. Проблемы долговременной сохранности больших данных // Информационные технологии и вычислительные системы. 2019. №2. С. 44-53. doi: 10.14357/2071863219020.
7. Solovyev, A.V. Long-Term Digital Documents Storage Technology // Lecture Notes in Electrical Engineering. 2020. vol.641, pp.901-911. ISSN 1876-1100. doi: 10.1007/978-3-030-39225-3_97.
8. Рысков, О.И. Об основных направлениях деятельности зарубежных архивов в области исследования и нормативного регулирования работы с электронной документацией // Секретарское дело. 2005. №3. С. 76.
9. Афанасьева, Л.П. Автоматизированные архивные технологии // Федеральное агентство по образованию. Государственное Образовательное учреждение высшего профессионального образования Российский Государственный Гуманитарный университет. 2005. С. 114.
10. Рысков, О.И. Основные направления деятельности национальных архивов США и Соединенного Королевства Великобритании и Северной Ирландии в области управления электронными документами правительственных учреждений // Отечественные архивы. 2004. № 3. С. 28-41.
11. Miller, J. NARA to suspend development of ERA starting in 2012 // FederalNewsRadio.com. 2012. Режим доступа: http://www.federalnewsradio.com/?sid=2204570&nid=35 (дата обращения 04.02.2021).
12. Lipowicz, A. NARA officials defend searchability of electronic archive // Federal Computer Week. 2011. Режим доступа: http://fcw.com/articles/2011/11/01/nara-officials-defending-searchability-of-electronic-archive.aspx (дата обращения 04.02.2021).
13. Preservation of Evidence of Cryptographically Signed Documents. BSI Technical Guideline TR-03125. Version 1.2 // Federal Office for Information Security. 2015. 183 p.
14. Anderson, L., Holz, R., Ponomarev, A., Rimba, P., Weber, I. New kids on the block: an analysis of modern blockchains. 2016. Режим доступа: https://arxiv.org/pdf/1606.06530.pdf (дата обращения 06.02.2021).
15. Даниленко А.Ю., Акимова Г.П. Особенности применения технологии блокчейн. // Материалы 27-й научно-технической конференции Методы и технические средства обеспечения безопасности информации 24-27 сентября 2018 года. СПб: Издательство политехнического университета. 2018. С. 73–75. ISSN 2305-994X.

Соловьев Александр Владимирович. Федеральное государственное учреждение "Федеральный исследовательский центр "Информатика и управление" Российской академии наук" г. Москва, Россия. Главный научный сотрудник, доктор технических наук. Количество печатных работ: 120. Область научных интересов: системный анализ, системы управления базами данных, теория надежности, математическое моделирование, долговременное хранение электронных документов. e-mail: soloviev@isa.ru

Algorithmic Solution of the Problem of Authenticity of Digital Data

A. V. Solovyev

Federal Research Center “Computer Science and Control” of Russian Academy of Sciences, Moscow, Russia

Abstract. The problem of control and keeping of the authenticity of digital data during long-term storage in the digital economy is becoming extremely urgent. Digital data is becoming a key factor in business and production processes, so any violation of their authenticity can lead to very serious consequences. The study provides a brief description of the stated problem of authenticity of digital data. An overview of the existing methods of solving the problem, their advantages and disadvantages is given. The author introduces definitions of authenticity, long-term keeping and other concepts and definitions. As a solution to the problem posed, the article proposes an algorithm for maintaining the authenticity of digital data during their long-term keeping. The proposed algorithm is described in detail within the framework of this article. The basis for the practical implementation of the algorithm is an inventory of electronic signatures. The article describes the practical application of the implementation of the proposed algorithm. Based on the successful application, the statement is made that the proposed algorithm, which has been tested in practice, will solve the problem posed in the article. The article also discusses possible prospects for further research and practical application of the proposed algorithm.

Keywords: authenticity of digital data, long-term keeping, digital economy, electronic signature, blockchain.

DOI 10.14357/20718632210102

References

1. Surovtsev, N.G. 2017. Hraneniye elektronnih dolumentov: zarubezhniy opyt [Storage of electronic documents: foreign experience]. Vestnik kultury I iskusstva [Bulletin of culture and art] 4(52): 17-23.
2. Swan, M. 2015. Blockchain: Blueprint for a New Economy. O'Reilly Media, Inc. 149 p. ISBN 978-1-491-92049-7.
3. Danilenko, A.Y., Pashkina, E.V., Pashkin, M.A., and Solovyev, A.V. 2018. Primeneniye tehnologii blockchain v informacionnih systemah. Chast 2. Podtverzhdeniye avtorstva I obespecheniye celostnosti [The use of blockchain technology in information systems. Part 2. Confirmation of authorship and integrity.]. Systemy visokoy dostupnosti [High Availability Systems] 14(1): 9–11.
4. Universal Electronic Records Management (ERM) Requirements. U.S. National Archives and Records Administration. 2017. Available at: https://www.archives.gov/records-mgmt/policy/universalermrequirements (accessed February 1, 2021).
5. National Archives Announces a New Model for the Preservation and Accessibility of Presidential Records. U.S. National Archives and Records Administration. 2017. Available at: https://www.archives.gov/press/press-releases/2017/nr17-54 (accessed February 1, 2021).
6. Bakanova, N.B., and Solovyev, A.V. 2019. Problemy dolgovremennoy sokhrannosti bol'shikh dannykh [Problems of long-term preservation of big data]. Informatsionnyye tekhnologii i vychislitel'nyye sistemy [Information Technology and Computing Systems] 2: 44-53. doi: 10.14357/2071863219020.
7. Solovyev, A.V. 2020. Long-term storage technology of digital documents. Lecture Notes in Electrical Engineering. 641: 901-911. ISSN 1876-1100. doi:10.1007/978-3-030-39225-3_97.
8. Ryskov, O.I. 2005. Ob osnovnih napravleniyah deyatelnosti zarubezhnih arhivnih organov v oblasti issledovaniya I normativnogo regulirovaniya raboti s elektronnoi dokumentaciey [On the main activities of foreign archival bodies in the field of research and regulatory work with electronic documentation]. Sekretarskoye delo [Secretarial business] 3: 76.

9. Afanasyeva, L.P. 2005. Avtomatizirovannie arhivniye tehnologuu [Automated Archive Technologies]. Federal'noye agentstvo po obrazovaniyu. Gosudarstvennoye Obrazovatelnoye uchrezhdeniye vysshego professional'nogo obrazovaniya Rossiyskiy Gosudarstvenniy Gumanitarniy universitet [Federal Agency for Education. State Educational Institution of Higher Professional Education Russian State University for the Humanities]: 114.
10. Ryskov, O.I. 2004. Osnovniye napravleniya deyatelnosti nacional'nih arhivov USA I Soedinennogo Korolevstva Velikobritanii I Severnoy Irlandii v oblasti upravleniya elektonnimi dokumentami pravitelstvennih uchrezhdeniy [The main activities of the national archives of the United States and the United Kingdom of Great Britain and Northern Ireland in the field of management of electronic documents of government agencies]. Otechestvenniye Arhivy [Russian archives] 3: 28-41.
11. Miller, J. 2012. NARA to suspend development of ERA starting in 2012. Available at: http://www.federalnewsradio.com/?sid=2204570&nid=35 (accessed February 4, 2021).
12. Lipowicz, A. 2011. NARA officials defend searchability of electronic archive [Electronic resource]. Federal Computer Week. Available at: http://fcw.com/articles/2011/11/01/nara-officials-defending-searchability-of-electronic-archive.aspx (accessed February 4, 2021).
13. Preservation of Evidence of Cryptographically Signed Documents. BSI Technical Guideline TR-03125 (Version 1.2). 2015. Federal Office for Information Security. 183 p
14. Anderson, L, Holz, R, Ponomarev, A, Rimba, P, and Weber, I. 2016. New kids on the block: an analysis of modern blockchains. Available at: https://arxiv.org/pdf/1606.06530.pdf (accessed February 6, 2021).
15. Danilenko, A.Y., and Akimova, G.P. 2018. Osobennosti primeneniya tekhnologii blockchain [Features of using blockchain technology]. Materialy 27-y nauchno-tekhnicheskoy konferentsii Metody i tekhnicheskiye sredstva obespecheniya bezopasnosti informatsii 24-27 sentyabrya 2018 goda. SPb: Izdatel'stvo politekhnicheskogo universiteta [Proceedings of the 27th scientific and technical conference Methods and technical tools of information security 24-27 September 2018. St. Petersburg: Publishing House of the Polytechnic University]: 73–75.

Solovyev A. V. Chief Researcher, Doctor of Technical Sciences. Federal Research Center "Computer Science and Control" of Russian Academy of Sciences, 44/2 Vavilova str., Moscow, 119333, Russia. e-mail: soloviev@isa.ru