ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ИНФОРМАЦИОННЫХ СИСТЕМ С ЭЛЕМЕНТАМИ ЦЕНТРАЛИЗАЦИИ И ДЕЦЕНТРАЛИЗАЦИИ

Кругликов С.В.[1], Дмитриев В.А.[2], Степанян А.Б.[3], Максимович Е.П.[4]

Аннотация: *Статья посвящена вопросам защиты ресурсов сложных, территориально распределенных информационных систем, сочетающих в себе элементы централизации и децентрализации. Для защиты ресурсов распределенных централизованных и децентрализованных информационных систем широко применяются методы на основе отношений доверия, консенсуса, криптографической защиты. Отдельное внимание уделено механизмам логического разграничения доступа субъектов к удаленным объектам, принадлежащим другим компонентам (сегментам) распределенной информационной безопасности. Приводятся средства защиты для реализации механизма управления доступом к ресурсам распределенных информационных систем, а также принципы аутентификации пользователя. Обсуждается специфика возникающих при этом проблем безопасности и основные подходы к их решению с учетом наличия совокупности локальных сегментов (компонентов), различающихся субъектами и объектами доступа, критичностью обрабатываемой данных и моделями разграничения доступа.*

Ключевые слова: *управление доступом, анализ событий, криптографическая защита, целостность информации, сегментация информационных ресурсов, распределенные информационные системы, субъекты и объекты доступа.*

DOI:10.21681/2311-3456-2020-01-02-07

Введение

Методы защиты ресурсов информационной системы (ИС) существенно зависят от ее архитектуры. В настоящее время широкое распространение получили сложные, территориально распределенные ИС, в которых гибко сочетаются элементы централизации и децентрализации. В сложных корпоративных ИС обычно присутствуют несколько уровней управления. Степень централизации системы определяется на основе установления соотношения объемов задач, решаемых на разных уровнях и, в определенном смысле, служит мерой разделения полномочий между уровнями. Смещение основной массы решений в сторону вышестоящего уровня (повышение степени централизации) отождествляют обычно с повышением управляемости подсистем. Повышение степени децентрализации соответствует увеличению самостоятельности подсистем и уменьшению объема информации, перерабатываемой верхними уровнями, однако часто связано с усложнением управления и увеличением времени адаптации ИС.

Новые возможности, предоставляемые распределенной обработкой данных с использованием механизмов централизации и децентрализации, одновременно порождают новые проблемы безопасности, решение которых требует учета целого ряда факторов. Например, какие функции должны быть централизованы, а какие децентрализованы; каков тип реализованной децентрализации (вертикальная или горизонтальная); где хранятся данные; какова конфигурация технических средств; как распределены полномочия по принятию управленческих решений в процессе эксплуатации ИС; каким образом обеспечивается доступ к данным на узлах ИС; каким образом обеспечивается согласованность работы узлов и согласованное состояние данных (согласованное состояние во всех репликах структуры данных, количества и значений общих данных) и др. В аспекте проблемы разграничения доступа необходимо также учитывать, что территориально распределенная гетерогенная ИС часто представляется в виде совокупности локальных сегментов (компонентов, зон), различающихся субъектами и объектами доступа, критичностью обрабатываемых данных, существующими рисками и угрозами безопасности и соответственно требованиями управления доступом. Наличие подобных факторов обусловливает специфику обеспечения информационной безопасности распределенных ИС с элементами централизации и децентрализации и требуют разработки новых адекватных методов защиты, обеспечивающих достаточный уровень защищенности активов ИС, возможность управления механизмами защиты как централизованно (удаленно, с рабочего

1 Кругликов Сергей Владимирович, доктор военных наук, заместитель генерального директора по научной и инновационной работе Объединенного института проблем информатики Национальной академии наук Белоруссии, Белоруссия, Минск. E mail: kruglikov_s@newman.bas-net.by

2 Дмитриев Владимир Александрович, кандидат физико-математических наук, заведующий лабораторией Объединенного института проблем информатики Национальной академии наук Белоруссии, Белоруссия, Минск. E-mail: vladdmitr@newman.bas-net.by

3 Степанян Арарат Баркевович, кандидат технических наук, ведущий научный сотрудник Объединенного института проблем информатики Национальной академии наук Белоруссии, Белоруссия, Минск. E-mail: ararat@newman.bas-net.by

4 Максимович Елена Павловна, кандидат физико-математических наук, ведущий научный сотрудник Объединенного института проблем информатики Национальной академии наук Белоруссии, Белоруссия, Минск. E-mail: maksimovich@newman.bas-net.by

места администратора безопасности ИС), так и децентрализовано (непосредственно с конкретной рабочей станции).

В рамках реализации методов обеспечения информационной безопасности распределенных ИС должно быть обеспечено выполнение общих мер защиты: идентификация и аутентификация (пользователей процессов и т.д.); разграничение доступа к ресурсам системы; регистрация и анализ событий, происходящих в системе; контроль целостности объектов системы; шифрование данных ограниченного распространения; резервное копирование и восстановление данных и программного обеспечения и др.

При реализации указанных мер возникают, например, следующие общие проблемы:

- обеспечение синхронизации/согласованности хранения и обработки данных, регламентов и политик доступа в децентрализованных сегментах ИС (в частности, в случае отсутствия централизованного хранилища информации возникает необходимость производить регламентацию доступа на каждом сегменте (сервере, автоматизированном рабочем месте), а также обеспечивать непротиворечивость этих регламентов для всех взаимодействующих сегментов ИС);
- обеспечение текущего мониторинга состояния ИС (обеспечение оперативного учета событий, способных повлиять на состояние безопасности ИС и оповещения ответственных лиц независимо от их расположения в системе путем доставки уведомления в сегменты ИС с поиском назначенного получателя);
- обеспечение защиты каналов связи между сегментами ИС;
- обеспечение доступности информации (например, предотвращение недоступности информации, хранящейся в одном экземпляре на сегменте, который вышел из строя; невозможности контроля изменений информации, производимых на сегменте; невозможности восстановления предыдущего состояния информационного ресурса);
- снижение издержек на реализацию функций аутентификации, авторизации, хранения и управления учетными записями в сегментах ИС.

В рамках организационных мер защиты обостряется проблема физической защиты, безопасности персонала (его лояльности, квалификации) и организации работ с документами и документированной информацией (обеспечение необходимого уровня детализации, четкости руководств пользователей, эксплуатационной документации, инструкций).

Методы защиты

Для защиты ресурсов распределенных централизованных и децентрализованных ИС широко применяются методы на основе отношений доверия, консенсуса, криптографической защиты. В частности, важными средствами безопасности, используемыми при передаче/хранении данных, являются электронная цифровая подпись, имитовставка, хэширование, направленные на обеспечение целостности/подлинности информации, а также шифрование/дешифрование, направленные на обеспечение конфиденциальности информации. В условиях конкретной ИС выбор методов защиты при проектировании системы защиты информации зависит от архитектуры ИС, базового программного обеспечения, типа защищаемых данных, способов их обработки, хранения, передачи по каналам связи, организации управления функционированием ИС, используемых механизмов централизации/децентрализации и др.

Отдельное внимание должно быть уделено механизмам логического разграничения доступа субъектов к удаленным объектам, принадлежащим другим компонентам (сегментам) распределенной ИС. Сегментация информационных ресурсов по требованиям доступа к ним позволяет добиться более гибкого контроля доступа в зависимости от пользователей сегментов и помогает ограничить соединения между ними в зависимости от уровня доверия при выполнении транзакций. Сегментация также уменьшает ущерб от взлома системы безопасности. При злонамеренном проникновении в определенный компонент сетевая сегментация, контролирующая трафик между уровнями, снижает число и разнообразие атак.

Предметом политики разграничения доступа в распределенных ИС является рассмотрение принципов организации и механизмов доступа, в том числе и межсегментного, при котором реализовывалась бы некая общая политика безопасности, обеспечивающая как внутрисегментную, так и межсегментную безопасность и позволяющая обеспечить объединение внутрисегментных политик безопасности, основанных на различных моделях логического разграничения [1,2,3,4,5]. Особую актуальность приобретает при этом проблема интероперабельности – взаимодействия разнородных компонентов, модулей, подсистем или программных систем в гетерогенной ИС, достижение их согласованности, «взаимопонимания», способности к совместному использованию, обмену данными, запросами, совместной деятельности при решении задач, возможности определения и совместного использования (разделения) данных и услуг в пределах различных компонентов ИС.

В качестве важных парадигм при построении моделей разграничения доступа на основе локальных моделей разграничения доступа выступает отношения доверия и консенсуса.

Осуществление доступа субъекта к удаленному объекту из иного сегмента ИС, как правило, возможно только с использованием другого субъекта, расположенного в том же сегменте распределенной ИС, что и объект доступа. Например, доверие между клиентом и сервером для различных сетевых протоколов уровня приложений FTP, SSH, Telnet и др.

Отношение доверия между сегментами A и B распределенной ИС определяется подмножеством пар $T_{A,B}=\{(a,b)\}\subset S(A)\times S(B)$, где $S(A)$. $S(B)$ – субъекты сегментов A и B. Если $(a,b)\in T_{A,B}$, то субъект a может получить доступ к объектам сегмента B посредством субъекта b [2].

DOI:10.21681/2311-3456-2020-01-02-07

В аспекте управления доступом доверие рассматривается как мера готовности стороны a с некоторой относительной уверенностью предоставить стороне b запрашиваемый доступ, несмотря на возможные негативные последствия (то есть принимая в расчет возможный ущерб от действий стороны b, не согласующихся с заявленной ролью).

Методы на основе отношений доверия между субъектами ИС фактически являются способом формализации отношений пользователей и должны позволять:

- проверить уровень доверия пользователя (объекта доверия);
- узнать, кто является «доверителями» пользователя, которые присвоили ему такой уровень доверия;
- не допускать подделки пользователем своего уровня доверия;
- не допускать подделки чужого уровня доверия другими пользователями;
- управлять возможностью доступа пользователя в зависимости от его уровня доверия (например, предоставлять доступ, если текущая оценка уровня доверия пользователя превышает некоторый установленный порог).

Существует много подходов к оценке уровня (степени) доверия. В частности, решение об уровне доверия пользователя может приниматься на основании данных централизованной службы (центра), выступающей в качестве доверенной стороны, либо самостоятельно субъектами доверия, например, на основе мониторинга действий пользователя в системе, опыта прошлых взаимодействий с ним, сведений об оценках других пользователей (с учетом репутации этих пользователей). В качестве простой оценки уровня доверия может использоваться, например, взвешенная сумма положительных отзывов об участнике от других участников, умноженных на коэффициент доверия к тому, кто этот отзыв оставил. Ряд вычислительных моделей репутации/доверия приведен, например, в [6, 7, 8, 9].

Один из общих подходов к управлению доступом к ресурсам гетерогенной распределенной ИС состоит в следующем:

- осуществляется разбиение ИС на локальные сегменты (компоненты) монолитные с точки зрения механизмов разграничения доступа;
- определяются множества необходимых информационных потоков между компонентами и внешних информационных потоков, которые должны быть реализованы для обеспечения функционирования ИС и управления доступом пользователей к ресурсам ИС;
- в каждом локальном сегменте (компоненте) определяются с учетом действующих механизмов/средств управления доступом локальные модели разграничения доступа;
- определяются условия, гарантирующие возможность сопряжения моделей разграничения доступа всех взаимодействующих между собой сегментов, формируется предоставление одних моделей в терминах других;
- формализуются процедуры предоставления субъектам необходимого авторизованного доступа к ресурсам разных сегментов ИС на основе отношений доверия и в соответствии c согласованными между собой локальными политиками разграничения доступа сегментов ИС;
- формируется на основе интеграции полученных результатов общая объединенная модель управления доступом к ресурсам ИС.

Наряду с отношением доверия для защиты ресурсов в распределенных системах с элементами децентрализации можно использовать также алгоритмы консенсуса, соответствующим образом адаптированные для применения в корпоративной среде [10,11,12]. Создание блоков может не требовать доказательства работы (proof-of-work) [13]. Вместо него, для консенсуса могут использоваться алгоритмы консенсуса с аутентифицированными участниками, в которых участники заранее известны и аутентифицированы, например, Practical Byzantine Fault Tolerance (PBFT) [14], основанный на обмене данными между узлами и подходящий для работы в доверенных сетях, например таких как внутрикорпоративные или межорганизационные блокчейны. Другой пример – протокол создания блоков, используемый в BitShares. В подобных алгоритмах у каждого обработчика транзакций есть пара ключей – закрытый и открытый. Создатели блоков известны и определяются по цифровой подписи блока. Реализация подобного подхода применительно к модели системы учета профессиональных компетенций граждан и траекторий их развития предложена, например, в [15].

Кроме того, в качестве средств защиты для реализации механизма управления доступом к ресурсам распределенных ИС используются также средства аутентификации, авторизации, цифровые подписи, сертификаты, регламентирование назначения и контроля полномочий и др.

В частности, аутентификация пользователя может быть основана на следующих принципах:

- предъявление пользователем пароля;
- предъявление пользователем доказательств, что он обладает секретной ключевой информацией;
- предъявление ответов на некоторые тестовые вопросы;
- предъявление пользователем некоторых неизменных признаков, неразрывно связанных с ним;
- предоставление доказательств того, что пользователь находится в определенном месте в определенное время;
- установление подлинности пользователя некоторой третьей доверенной стороной, в частности, на основании сертификата открытого ключа.

Для распределенных корпоративных ИС типичными являются модель доверительных междоменных отношений по принципу строгой иерархии или модель с реверсивными сертификатами. В первой модели каждый пользователь изначально имеет и доверяет только сертификату корневого удостоверяющего центра (УЦ). Доверительные отношения пользователей устанавлива-

ются только через корневой УЦ и цепочку находящихся между ними УЦ. Модель с реверсионными сертификатами отличается тем, что нижестоящий УЦ может создавать сертификаты для вышестоящего удостоверяющего центра. Каждый пользователь изначально доверяет только открытому ключу того УЦ, в котором он зарегистрирован. Любая цепочка сертификатов будет начинаться с сертификата локального УЦ и заканчиваться сертификатом УЦ конечного пользователя. Пользователи, находящиеся в одном домене, могут напрямую взаимодействовать друг с другом через сертификат их общего УЦ. Недостатком этой схемы является то, что при взаимодействии пользователей из разных доменов требуется обработка достаточно длинной цепочки сертификатов. Для решения данной проблемы нужна установка прямых доверительных отношений между соответствующими УЦ.

В качестве средств защиты ресурсов распределенных ИС следует упомянуть также средства обеспечения конфиденциальности и целостности передаваемых данных (криптографические методы шифрования, электронной цифровой подписи, имитовставки, хэширования). Конфиденциальность обеспечивается с помощью алгоритмов и методов симметричного и асимметричного шифрования, а также путем взаимной аутентификации абонентов на основе многоразовых и одноразовых паролей, цифровых сертификатов, смарткарт и т.п. Целостность/подлинность передаваемых данных обычно достигается с помощью различных вариантов технологии электронной цифровой подписи, имитовставки, хэширования.

Заключение

Одним из современных направлений исследования возможности реализации методов защиты для распределенных корпоративных сетей с элементами децентрализации является технология корпоративного (эксклюзивного) блокчейна, когда обработка транзакций осуществляется определенным списком лиц или компаний, чьи личности установлены и имеют соответствующий допуск к информации. Корпоративный блокчейн создает структуру управления, которая отличается прозрачностью, адаптивностью и гибкостью по сравнению с открытой системой. Он более востребован в тех областях, где требуется решение специфических бизнес-задач. В этом случае можно создавать новые блоки без доказательства работы. Вместо него используются алгоритмы консенсуса с участниками прошедшими аутентицификацию. При этом любой обработчик транзакций имеет пару ключей (открытый и закрытый). В рамках корпоративного блокчейна реализуются криптография на эллиптических кривых, хеширование и алгоритмы работы блокчейна (связка блоков (хэш каждого блока записывается как компонент следующего блока), адресация транзакций (отслеживание транзакций, например, с помощью учетные записи верифицированных и авторизованных участников), подтверждение транзакций (включение их в состав блока), нахождение консенсуса.

Получает развитие также технология корпоративного сайдчейна, позволяющая токенам и другим цифровым активам одного блокчейна безопасным образом использоваться в другом блокчейне и затем (в случае необходимости) быть возвращенными в оригинальный блокчейн. Концепция сайдчейнов, как отдельных блокчейнов с двусторонней привязкой к родительскому блокчейну, предполагает возможность создания в будущем широкой сети множества сплетенных между собой блокчейнов, у каждого из которых будет свой протокол, правила и набор функций.

Литература

1. Гайдамакин Н.А. Теоретические основы компьютерной безопасности – Екатеринбург: Уральский государственный университет им. Горького А.М. – 2008. – 212 с.
2. Иткес А.А. Управление доступом к ресурсам распределенных информационных систем на основе отношений доверия: диссертация ... кандидата физико-математических наук: 05.13.19 / Иткес А.А.; [Место защиты: Моск. гос. ун т им. М.В. Ломоносова]. Москва, 2010. 151с.
3. Иткес А.А. Объединение моделей логического разграничения доступа для сложноорганизованных распределенных информационных систем // Проблемы информатики. 2010. № 1. С. 85-95.
4. Иткес А.А. Реляционная модель логического разграничения доступа // Интеллектуальные системы. Теория и приложения. 2016. Т. 20. № 4. С. 49-54.
5. Васенин В.А., Иткес А.А., Шапченко К.А., Бухонов В.Ю. Реляционная модель логического разграничения доступа на основе цепочек отношений // Программная инженерия. 2015. № 9. С. 30-31.
6. Губанов Д.А. Обзор онлайновых систем репутации/доверия // [Электронный ресурс]. URL: http://www.mtas.ru/search/search_results_ubs_new.php?publication_id=18622&IBLOCK_ID=10.
7. Голован С.В. Эффект забывания в теории коллективной репутации. 1999. М.: Российская экономическая школа. 38 с.
8. Ермаков Н.С., Иващенко А.А., Новиков Д.А. Модели репутации и норм деятельности. 2005. М.: ИПУ РАН. – 67 с.
9. Новиков Д.А., Чхартишвили А.Г. Прикладные модели информационного управления. 2004. М.: ИПУ РАН. 130 с.
10. Герасимов И.Ю., Чижов И.В. Алгоритм консенсуса платформы Tendermint и механизм Proof Of Lock Change // International Journal of Open Information Technologies. 2019. Т. 7. № 6. С. 24-29.
11. Иванова Г.С. Анализ алгоритмов консенсуса в блокчейн-системах // Технологии инженерных и информационных систем. 2019. № 1. С. 35-44.

12. Музыченко В.А. Организация индекса распределенной поисковой системы, работающей по алгоритму консенсуса BFT // Моделирование, оптимизация и информационные технологии. 2019. Т. 7. № 3 (26). / [Электронный ресурс]. URL: https://moit.vivt.ru/?page_id=9992&lang=ru.
13. Can we afford integrity by proof-of-work? Scenarios inspired by the bitcoin currency / J. Becker [et al.] // The economics of information security and privacy. Berlin, Heidelberg: Springer, 2013. P. 135-156.
14. Lamport L., Shostak R., Pease M. The Byzantine generals problem // ACM Transactions on Programming Languages and Systems (TOPLAS). 1982. Vol. 4. No. 3. P. 382–401.
15. Новиков С.П., Михеенко О.В., Кулагина Н.А., Казаков О.Д. Цифровизация учета профессиональных компетенций граждан на основе технологий распределенных реестров и смарт-контрактов // Бизнес-информатика. 2018. № 4 (46). С. 43-53.

Рецензент: *Марков Алексей Сергеевич, доктор технических наук, старший научный сотрудник, профессор Московского государственного технического университета им. Н.Э. Баумана, г. Москва, Россия. E-mail: a.markov@bmstu.ru*

INFORMATION SECURITY OF INFORMATION SYSTEMS WITH ELEMENTS OF CENTRALIZATION AND DECENTRALIZATION

Kruglikov S.V.[5] , Dmitriev V.A.[6] , Stepanian A.B.[7] , Maksimovich E.P.[8]

Annotation: *The article is dedicated to the issues of protecting the resources of complex, territorially distributed information systems that incorporate the elements of centralization and decentralization. To protect the resources of distributed centralized and decentralized information systems, methods based on trust relationships, consensus, cryptographic security are widely used. Special attention is given to the mechanisms of logical distinction of subjects' access to remote objects belonging to other components (segments) of distributed information security. Protection means used to implement the mechanism of managing the access to the resources of the distributed information systems are provided as well as the principles of user authentication. The specifics of the security problems arising in this case and the main approaches to their solutions are discussed taking into consideration a set of local segments (components) that differ by access subjects and objects, criticality of the data processed and access management models.*

Keywords: *access management, event analysis, cryptographic protection, information integrity, information resource segmentation, distributed information systems, entities and access facilities.*

References

1. Haidamakin N.A. Teoreticheskie osnovy komp'juternoy bezopasnosti – Ekaterinburg: Ural'skij gosudarstvennjij universitet imeni Gor'kogo A.M. 2008. 212 s.
2. Itkes A.A. Upravlenie dostupom k resursam raspredelennyh informatsionnyh sistem na osnove otnoshenija doverija: dissertatsiya ... kandidata phiziko-matematicheskih nauk: 05.13.19 / Itkes A.A.; [Mesto zashchity: Mosk. gos. un-t im. M.V.Lomonosova]. M., 2010. 151 s.
3. Itkes A.A. Ob»edinenie modelej logicheskogo razgranichenija dostupa dlja slozhnoorganizovannyh raspredelennyh informatsyonnyh sistem // Problemy informatiki. 2010. № 1. S. 85-95.
4. Itkes A.A. Reljatsyonnaja model' logicheskogo razgranichenija dostupa // Intellektual'nye sistemy. Teorija I prilozhenija. 2016. T. 20. № 4. S. 49-54.

5 Sergey Kruglikov, Dr.Sc., Deputy General Director for Research and Innovation of the United Institute of Informatics Problems of the National Academy of Sciences of Belarus, Minsk, Belarus. E mail: kruglikov_s@newman.bas-net.by

6 Vladimir Dmitriev, Ph.D., Head of laboratory of the United Institute of Informatics Problems of the National Academy of Sciences of Belarus, Minsk, Belarus. E-mail: vladdmitr@newman.bas-net.by

7 Ararat Stepanian, Ph.D., Leading Researcher of the United Institute of Informatics Problems of the National Academy of Sciences of Belarus, Minsk, Belarus. E-mail: ararat@newman.bas-net.by

8 Elena Maksimovich, Ph.D., Leading Researcher of the United Institute of Informatics Problems of the National Academy of Sciences of Belarus, Minsk, Belarus. E-mail: maksimovich@newman.bas-net.by

5. Vasenin V.A., Itkes A.A., Shapchenko K.A., Buhonov V.Ju. Reljatsyonnaja model' logicheskogo razgranichenija dostupa na osnove tsepochek otnoshenij // Programmnaja inzhenerija. 2015. № 9. S. 30-31.
6. Hubanov D.A. Obzor onlaynovyh sistem reputatsii/doverija // [Electronic resource]. – URL: http://www.mtas.ru/search/search_results_ubs_new.php?publication_id=18622&IBLOCK_ID=10.
7. Golovan S.V. Effekt zabyvanija v teorii kollektivnoj reputatsii. 1999. M.: Rossijskaja ekonomicheskaja shkola. 38 s.
8. Ermakov N.S., Ivashchenko A.A., Novikov D.A. Modeli reputatsii i norm dejatel'nosti. 2005. M.: IPU RAN. 67 s.
9. Novikov D.A., Chkhartishvili A.G. Prikladnye modeli informatsionnogo upravlenija. 2004. M.: IPU RAN. 130 s.
10. Gerasimov I.Yu., Chizhov I.V. Algoritm konsensusa platformy Tendermint i mehanizm Proof Of Lock Change // International Journal of Open Information Technologies. 2019. T. 7. № 6. S. 24-29.
11. Ivanova G.S. Analiz algoritmov konsensusa v blokchejn-sistemah // Tehnologija inzhenernyh in informatsionnyh sistem. 2019. № 1. S. 35-44.
12. Muzychenko V.A. Organizatsyja indeksa raspredelennoj poiskovoj sistemy, rabotayushchej po algoritmu konsensusa BFT // Modelirovanie, optimizatsija i informatsionnye tehnologii. 2019. T. 7. № 3 (26). / [Electronic resource]. URL: https://moit.vivt.ru/?page_id=9992&lang=ru.
13. Can we afford integrity by proof-of-work? Scenarios inspired by the bitcoin currency / J. Becker [et al.] // The economics of information security and privacy. Berlin, Heidelberg: Springer, 2013. P. 135-156.
14. Lamport L., Shostak R., Pease M. The Byzantine generals problem // ACM Transactions on Programming Languages and Systems (TOPLAS). 1982. Vol. 4. No. 3. P. 382–401.
15. Novikov S.P., Miheenko O.V., Kulagina N.A., Kazakov O.D., Tsifrovizatsija ucheta professional'nyh kompetentsij grazhdan na osnove tehnologiy raspredelennyh reestrov i smart-kontractov // Biznes-informatika. 2018. № 4 (46). S. 43-53.

DOI:10.21681/2311-3456-2020-01-02-07