

Технология обеспечения достоверности информации при проведении сетевых экспертиз

Д. С. Тобин*, М. С. Голосовский, А. В. Богомолов

ФГБУН «Санкт-Петербургский Федеральный исследовательский центр Российской академии наук», г. Санкт-Петербург, Российская Федерация

199178, Российская Федерация, г. Санкт-Петербург, 14-я линия В.О., д. 39

* gniiivm.g@ya.ru

Аннотация

В статье показана актуальность совершенствования процедур сбора и обработки информации в интересах поддержки принятия решений на основе единой программной платформы сетевых экспертиз, приоритетом которого является обеспечение достоверности информации в защищенной от несанкционированного доступа платформе сетевых экспертиз вариантов решений, функционирующей в системах с ограниченными вычислительными мощностями с заданной отказоустойчивостью сети обработки информации. Обоснована целесообразность решения поставленной задачи с использованием децентрализованной блокчейн-технологии управления доступом к информации, обеспечивающей создание защищенной распределенной базы данных участников и организаторов сетевой экспертизы, обеспечивающей отслеживание, проверку и выполнение операций-транзакции с децентрализованным распределенным хранением информации и установкой меток времени по всем совершенным транзакциям. Предложена архитектура единой системы проведения сетевой экспертизы и хранения данных об экспертах, состоящая из технологических уровней, взаимодействующих в течение всей экспертизы для обеспечения криптографически безопасного голосования экспертов в среде с проверяемыми доказательствами. За счёт того, что копии блокчейн хранятся в узлах распределенной сети, платформа является устойчивой к проблемам с временным или постоянным отключением узлов, связанным со сбоями оборудования или связи, а также подключением новых узлов. За счет интеграции технологии блокчейн с технологией Docker-контейнеров платформа может быть объединена в единый блок и затем легко развернута в необходимых средах с возможностью масштабирования. Выполняемые операции, собранные в блоки, сортируются в хронологическом порядке, позволяя участникам сетевой экспертизы получать достоверную информацию по всем изменениям истории, произошедшей в сети. Результатом являются не подлежащие отмене транзакции, согласованные всеми участниками экспертизы децентрализованно. Предлагаемая технология позволяет обеспечить требуемую достоверность информации при проведении сетевых экспертиз вариантов решений в системах с ограниченными вычислительными мощностями с заданной отказоустойчивостью.

Ключевые слова: сетевая экспертиза, достоверность экспертиз, блокчейн, Docker-контейнер, распределенные вычисления.

Финансирование: исследование выполнено при государственной поддержке ведущих научных школ Российской Федерации, грант Президента Российской Федерации № НШ-2553.2020.8. «Методы, алгоритмы и технические средства мониторинга состояния операторов эргатических систем в процессе профессиональной деятельности».

Авторы заявляют об отсутствии конфликта интересов.



Контент доступен под лицензией Creative Commons Attribution 4.0 License.
The content is available under Creative Commons Attribution 4.0 License.



Для цитирования: Тобин, Д. С. Технология обеспечения достоверности информации при проведении сетевых экспертиз / Д. С. Тобин, М. С. Голосовский, А. В. Богомолов. – DOI 10.25559/SITITO.16.202003.623-632 // Современные информационные технологии и ИТ-образование. – 2020. – Т. 16, № 3. – С. 623-632.

© Тобин Д. С., Голосовский М. С., Богомолов А. В., 2020



Technology for Ensuring the Accuracy of Information during Network Examinations

D. S. Tobin*, M. S. Golosovsky, A. V. Bogomolov

St. Petersburg Federal Research Center of the Russian Academy of Sciences, St. Petersburg, Russian Federation

39, 14th Line V.O., St. Petersburg 199178, Russian Federation

* gniiivm.g@ya.ru

Abstract

The article shows the relevance of improving the procedures for collecting and processing information in the interests of supporting decision-making on the basis of a unified software platform for network examinations, the priority of which is to ensure the reliability of information in a network of expert examinations of solution options that is protected from unauthorized access and functioning in systems with limited computing power with a given fault tolerance information processing networks. The feasibility of solving the problem using a decentralized blockchain technology for managing access to information, creating a secure distributed database of participants and organizers of network expertise, providing tracking, verification and execution of transaction transactions with decentralized distributed information storage and setting time stamps for all completed transactions, is justified. The architecture of a unified system for conducting network examination and storing data about experts is proposed, consisting of technological levels interacting throughout the examination to ensure cryptographically safe voting of experts in an environment with verified evidence. Due to the fact that copies of the blockchain are stored in nodes of a distributed network, the platform is resistant to problems with temporary or permanent disconnection of nodes associated with equipment or communication failures, as well as connecting new nodes. By integrating blockchain technology with docker container technology, the platform can be combined into a single block and then easily deployed in the required scalable environments. The operations performed, collected in blocks, are sorted in chronological order, allowing participants of the network examination to receive reliable information on all changes in the history that occurred in the network. The result is non-cancellable transactions agreed upon by all participants in the examination decentralized. The proposed technology makes it possible to provide the required information reliability when carrying out network examinations of solution options in systems with limited computing power with a specified fault tolerance.

Keywords: network expertise, reliability of expertise, blockchain, docker container, distributed computing.

Funding: The study was carried out with the state support of the leading scientific schools of the Russian Federation, the grant of the President of the Russian Federation No. NSh-2553.2020.8. "Methods, Algorithms and Technical Means for Monitoring the State of Operators of Ergatic Systems in the Process of Professional Activity."

The authors declare no conflict of interest.

For citation: Tobin D.S., Golosovsky M.S., Bogomolov A.V. Technology for Ensuring the Accuracy of Information during Network Examinations. *Sovremennye informacionnye tehnologii i IT-obrazovanie* = Modern Information Technologies and IT-Education. 2020; 16(3):623-632. DOI: <https://doi.org/10.25559/SITITO.16.202003.623-632>



Введение

Информационно-телекоммуникационные технологии в настоящее время развиваются интенсивно, с постоянно возрастающим объемом передаваемой информацией. В результате возникает необходимость совершенствования процессов сбора и обработки информации, в том числе, для ее использования в процессе поддержки принятия решений, имеющих существенное значение для развития отраслей знаний и научно-технического прогресса [1, 2]. Специфика систем поддержки принятия таких решений определяется жесткими требованиями к обеспечению конфиденциальности и защищенности обрабатываемой информации: исходные данные должны быть надежно сохранены и верифицированы [3-5].

Приоритетным направлением развития программного обеспечения сбора и обработки информации в интересах поддержки принятия решений в сфере обеспечения обороноспособности страны является разработка единой программной платформы сетевых экспертиз вариантов решений [6-8].

Для реализации комплексного подхода к сетевой экспертизе необходима программная платформа, обладающая институциональным правовым статусом, обеспечивающим привлечение высококвалифицированных независимых экспертов или их групп для обеспечения поддержки принятия решений должностными лицами [6].

Платформа проведения сетевых экспертиз должна выполнять функции [2, 3, 5, 8]:

- формировать реестр высококвалифицированных экспертов и выявлять наиболее подготовленных из них;
- обеспечить возможность привлечения к экспертизе экспертно-аналитические организации федеральных органов исполнительной власти (ФОИВ), Российской академии наук, независимых аналитических центров, общественные научные организации, центры компетенций, а также ведущих экспертов в предметных областях;
- повышать оперативность и качество принимаемых решений на основе использования аналитических и прогнозных инструментальных средств сетевой экспертизы;
- автоматизировать процессы подготовки аналитической отчетности проведения сетевой экспертизы;
- осуществлять инструментальную и информационную поддержку деятельности привлекаемых экспертов;
- визуализировать данные с использованием средств когнитивной графики.

Создание межведомственной платформы проведения сетевой экспертизы должно обеспечить [3, 5]:

- повышение качества информационно-аналитического обеспечения подготовки решений;
- достижение положительного синергетического эффекта за счет интеграции создаваемой платформы с существующими и перспективными автоматизированными информационно-аналитическими системами ФОИВ, учреждений и организаций, функционирующих в предметной области принятия решений;
- повышение эффективности деятельности экспертного

сообщества за счет сокращения времени на организацию и проведение экспертизы, снижения трудоёмкости подготовки экспертных заключений по рассматриваемым результатам экспертиз;

- создание возможности удаленной работы экспертного сообщества, используя действующую телекоммуникационную инфраструктуру ФОИВ учреждений и организаций, функционирующих в предметной области принятия решений;
- снижение стоимости и повышение качества экспертизы.

При реализации межведомственной платформы проведения сетевой экспертизы необходимо обеспечить достоверность информации, используемой для поддержки принятия решений, с максимально возможным освобождением лиц, принимающих решения, от непосредственного участия в получении, передаче, хранении, обработке и использовании материалов и информации, оставляя за ними только функции принятия решений [2-5].

Вместе с этим, большинство известных платформ хранения и формирования управленческих решений используют централизованную архитектуру, которая уязвима к кибератакам и к проблеме единой точки отказа, когда от одного элемента зависит работоспособность всей системы. Появление новых технологий из смежных научных областей открывает новые возможности обеспечения достоверности информации принятия управленческих решений в органах военного управления.

Цель исследования

Целью исследования было разработать технологию обеспечения достоверности информации для реализации в перспективной защищенной от несанкционированного доступа платформе сетевых экспертиз вариантов решений, функционирующей в системах с ограниченными вычислительными мощностями с заданной отказоустойчивостью сети обработки информации.

Результаты и обсуждение

Наиболее подходящее решение с использованием децентрализованной технологии для управления доступом к информации является блокчейн [9-14]. Блокчейн позволит создать своего рода защищенную, распределенную базу данных, состоящую из многочисленных участников системы, которые могут отследить, проверить, и выполнить операции-транзакции и обеспечить хранение информации от большого множества других участников. Эта технология уже была применена в различных вариантах использования, таких как интеллектуальная транспортная система, управление медицинской документацией, децентрализованные веб-приложения, платформы прогноза [9, 11, 15, 16].

Такая технология минимизирует воздействие человеческого фактора на механизм сетевой экспертизы на любом уровне иерархии и требует новых форм управления проведением сетевой экспертизы, не требующих содержания контролирующих структур — за счет этого себестоимость управления проведе-



нием экспертизы снижается в разы [17, 18].

За счет блокчейн-технологии создается распределённая защищённая от несанкционированной модификации база данных реестра экспертов и базу данных по совершённым операциям платформы, в которой невозможно имитировать транзакцию, показав недействительную работу. По любой операции можно будет отследить получателя и отправителя, однако данные о них тоже представлены в виде комбинации криптографически защищённых символов. Возможна в блокчейне и установка меток времени по всем транзакциям, совершённым пользователями платформы [19].

Сетевое время маркирует транзакции, помещая их в непрерывную цепочку доказательств работы на основе хэш-функции, формируя запись, которая не может быть изменена без повторной проверки доказательства работы.

Блокчейн в цифровой форме распределяется по множеству компьютеров платформы практически в режиме реального времени: он децентрализован, и копия всей записи реестра проведенных операций доступна всем пользователям и участникам одноранговой сети. Это избавляет от необходимости иметь централизованные уполномоченные органы. Благодаря децентрализации платформа сможет обеспечить заданную защиту данных от отказов центров обработки данных.

Для достижения консенсуса блокчейн использует множество (более трех) распределённых участников сети: они задействуют свои компьютеры, чтобы аутентифицировать и проверить каждый новый блок — например, чтобы гарантировать, что какая-либо одна транзакция не пройдет несколько раз. Новые блоки принимаются сетью, как только большинство ее участников соглашаются, что они допустимы.

Блокчейн программируем: инструкции встроены в блоки, это позволяет выполнять транзакции или иные действия только при соблюдении определенных условий и может сопровождаться дополнительными цифровыми данными.

Блокчейн делает возможным решение многих проблем, связанных с цифровой идентификацией пользователей платформы [20]. Системы аутентификации в блокчейне строятся на неопровержимой проверке идентификационных данных, для чего используются цифровые подписи на основе шифрования с открытым ключом. Для аутентификации личных данных сетевых экспертов через блокчейн проверяется: была ли транзакция подписана корректным закрытым ключом пользователя, а у кого именно имеется доступ к этому закрытому ключу — неважно.

База данных блокчейна может сохранить профили экспертов, личные данные экспертов, касаемые реализации проекта, обобщенные данные проекта. В качестве пользовательского устройства может выступать персональный компьютер, ноутбук, смартфон, через которые конечные пользователи могут считать или записать данные в сеть блокчейна. Криptomаршрутизаторы в локальных сетях будут соединять подсети экспертов к серверу через технологии блокчейна.

В статье предлагается архитектура единой системы проведения сетевой экспертизы и хранения данных об экспертах (далее — Платформа), построенная на многослойной архитектуре, основанной на технологии блокчейн, которая включает несколько инноваций. Разработанная система обеспечивает высокую пропускную способность и низкие издержки, что

позволяет запускать ее на устройствах с низкой пропускной способностью.

Платформа состоит из технологических уровней, которые взаимодействуют друг с другом в различных случаях в течение всей экспертизы для обеспечения криптографически безопасного голосования экспертов в среде с проверяемыми доказательствами. Ниже представлена визуализация технологических уровней.

На рис. 1 отображен процесс работы системы и показано взаимодействие ее компонентов: разработанная Платформа определяет инфраструктуру проведения сетевой экспертизы.

Разработанная модель платформы проведения сетевой экспертизы проекта блокчейн сети, в которую входят узлы (автоматизированные рабочие места, подключенные к сети блокчейна) с разрешениями на запись, управляемые руководителем экспертизы и признанными внешними консенсусными узлами, а также узлы с разрешениями только для чтения (аудиторские узлы), в роли которых могут быть автоматизированные рабочие места сетевых экспертов. Эта блокчейн-сеть обеспечивает неизменяемую запись всех данных в узлах платформы по всей сети и выступает в качестве центрального канала связи, хранилища всей системы. Платформа проведения сетевой экспертизы проекта — это распределённая база данных для лиц, принимающих участие в экспертизе, в которую при прохождении авторизации эксперт может отправлять подписанные данные в виде сообщений и результатов голосования. Процесс отправки криптографически подписанных и аутентифицированных данных сохраняется в блокчейн — таким образом, весь процесс голосования на платформе становится безопасным, закрытым и может быть проверен в любой момент времени указанными для контроля пользователями (аудиторскими узлами).

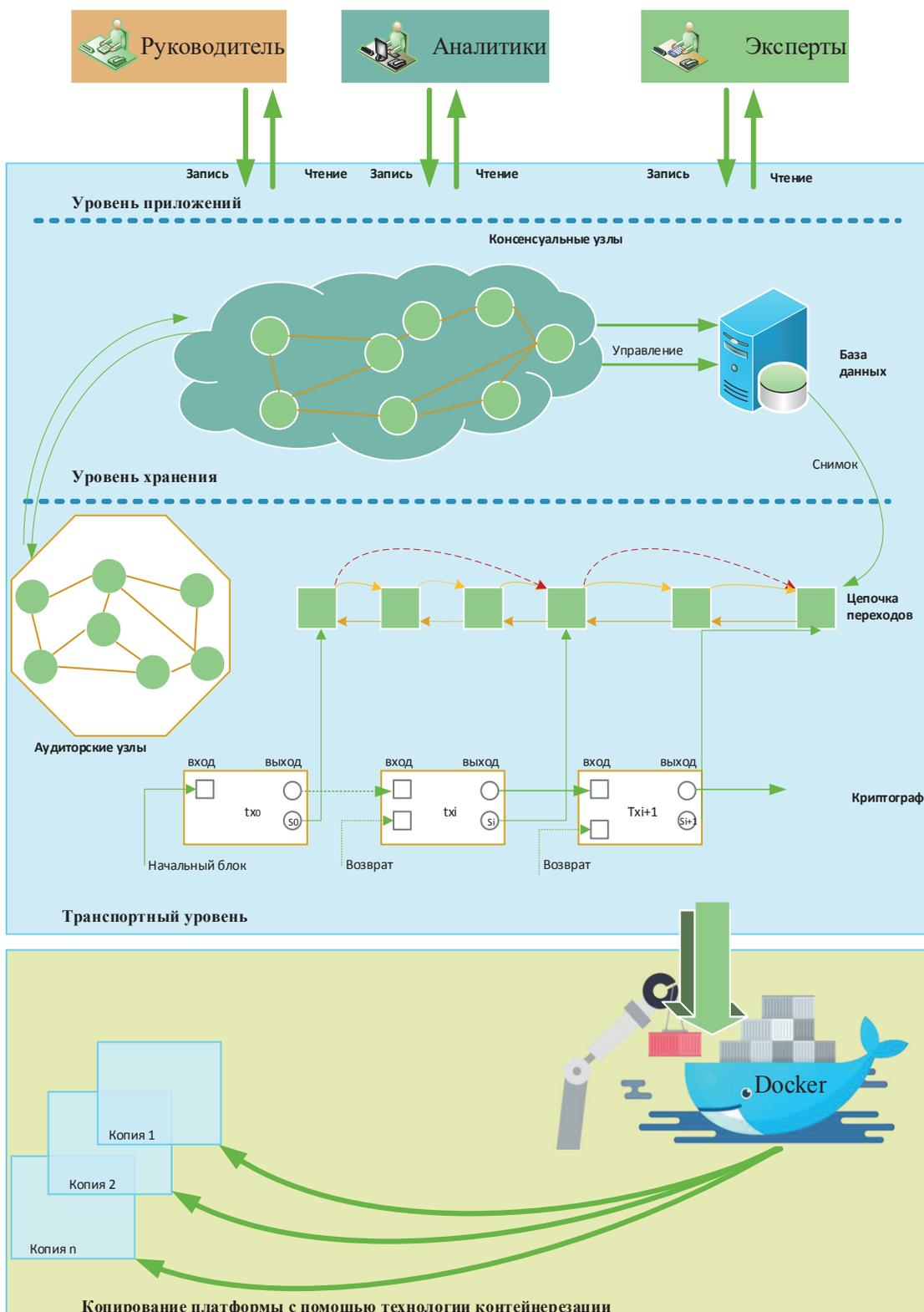
Поскольку копии блокчейн хранятся в узлах распределённой сети, это делает платформу устойчивой к проблемам с временным или постоянным отключением узлов, связанным со сбоями оборудования или связи, а также подключением новых узлов.

Внедрение и развертывание технологии блокчейн возможно интегрировать с использованием Docker-контейнеров (Docker). В качестве контейнера будут выступать одноранговые узлы или ноды. Каждый одноранговый узел может содержать хранилище данных для записи блока транзакций в реестре.

Поскольку контейнеры переносимы, платформа может быть объединена в единый блок и затем развернута в необходимых средах без внесения каких-либо изменений в сам контейнер.

Блокчейн функционирует как журнал транзакций, который записывает все изменения состояния. Операции, собранные в блоки, криптографически связанные между собой, образуют последовательность цепочек, в которой записаны все транзакции платформы проведения сетевой экспертизы проекта. Они сортируются в хронологическом порядке, позволяя участникам сетевой экспертизы получать достоверную информацию по всем изменениям истории, произошедшей в сети. Приоритетным подходом к сортировке является подход, основанный на методах синхронизированных эстафет [21-23]. Результатом являются не подлежащие отмене транзакции, согласованные всеми участниками сети децентрализованно.





Р и с. 1. Модель защищенной от несанкционированного доступа платформы проведения сетевой экспертизы

F i g. 1. A model of an unauthorized access protected platform for performing network expertise



При необходимости создать закрытую сеть или установить ограничения на то, какие транзакции может видеть каждая из участвующих сторон используется Docker [9]. Docker позволяет быстро развернуть или масштабировать систему до необходимых параметров технологию блокчейн в сети сетевых экспертиз, создать копии нодов и узлов сети. Все это сокращает время тестирования, разработки и развертывания Платформы.

Идентификация эксперта будет обеспечиваться путём ввода пользовательского ключа. Пользовательские ключи хранятся в аппаратном модуле безопасности HSM (hardware security module), в зашифрованном виде с использованием специальных мастер-ключей защиты.

HSM — это физическое вычислительное устройство, которое позволяет формировать, хранить и управлять цифровыми ключами. Аппаратный модуль безопасности также используется для управления ключами Transparent Data Encryption для баз данных пользователей платформы, обеспечивая как логическую, так и физическую защиту этих материалов от несанкционированного использования и потенциальных угроз. Возможно применять отечественные аппаратные модули (КриптоПро HSM и ViPNet HSM) имеющие соответствующие сертификаты и поддерживающие российские криптографические алгоритмы ГОСТ Р 34.10-2012, ГОСТ Р 34.11-2012. По оценкам разработчиков пакетная обработка данных позволяет формировать до 50000 электронных подписей в секунду.

Эксперту предоставляется возможность осуществления записи транзакции в сеть блокчейна. Прежде, чем отправить транзакцию в сеть, необходимо чтобы участник предоставил сети блокчейна сертификат, который содержит закрытый ключ для подписания транзакции. Транзакция может быть определена как процесс чтения или записи данных из реестра, которая выполняется в сети блокчейна [24, 25].

Основными преимуществами внедрения блокчейна в платформу являются прозрачность транзакций, высокая безопасность, улучшенная трассируемость требований, высокая эффективность, низкая цена внедрения, и отсутствие возможности стороннего вмешательства в искажение верифицированных данных.

Анализ имеющегося опыта использования блокчейн-технологий и программного обеспечения Docker [6-18] позволяет утверждать, что такая комбинация обеспечивает требуемую достоверность информации при проведении сетевых экспертиз вариантов решений в системах с ограниченными вычислительными мощностями с заданной отказоустойчивостью.

Заключение

Для совершенствования процедур сбора и обработки информации в интересах поддержки принятия решений на основе единой программной платформы предложена архитектура единой системы проведения сетевой экспертизы и хранения данных об экспертах, состоящая из технологических уровней, взаимодействующих в течение всей экспертизы для обеспечения криптографически безопасного голосования экспертов в среде с проверяемыми доказательствами. За счёт того, что копии блокчейн хранятся в узлах распределенной сети, платформа является устойчивой к проблемам с временным или по-

стоянным отключением узлов, связанным со сбоями оборудования или связи, а также подключением новых узлов. За счет интеграции технологии блокчейн с технологией Docker-контейнеров платформа может быть объединена в единый блок и затем легко развернута в необходимых средах с возможностью масштабирования. Выполняемые операции, собранные в блоки, сортируются в хронологическом порядке, позволяя участникам сетевой экспертизы получать достоверную информацию по всем изменениям истории, произошедшей в сети. Результатом являются не подлежащие отмене транзакции, согласованные всеми участниками экспертизы децентрализованно.

Предлагаемая технология позволяет обеспечить требуемую достоверность информации при проведении сетевых экспертиз вариантов решений в системах с ограниченными вычислительными мощностями с заданной отказоустойчивостью.

Список использованных источников

- [1] Fernández-Caramès, T. M. Towards Post-Quantum Blockchain: A Review on Blockchain Cryptography Resistant to Quantum Computing Attacks / T. M. Fernández-Caramès, P. Fraga-Lamas. — DOI 10.1109/ACCESS.2020.2968985 // IEEE Access. — 2020. — Vol. 8. — Pp. 21091-21116. — URL: <https://ieeexplore.ieee.org/document/8967098> (дата обращения: 26.07.2020).
- [2] Brinckman, A. A Comparative Evaluation of Blockchain Systems for Application Sharing Using Containers / A. Brinckman [et al.]. — DOI 10.1109/eScience.2017.80 // 2017 IEEE 13th International Conference on e-Science (e-Science). — Auckland, New Zealand, 2017. — Pp. 490-497. — URL: <https://ieeexplore.ieee.org/document/8109185> (дата обращения: 26.07.2020).
- [3] Фёдоров, М. В. Математическая модель автоматизированного контроля выполнения мероприятий в органах военного управления / М. В. Фёдоров, К. М. Калинин, А. В. Богомолов, А. Н. Стецюк // Информационно-измерительные и управляющие системы. — 2011. — Т. 9, № 5. — С. 46-54. — URL: <https://elibrary.ru/item.asp?id=16313311> (дата обращения: 26.07.2020). — Рез. англ.
- [4] Богомолов, А. В. Средства обеспечения безопасности информации в современных автоматизированных системах / А. В. Богомолов, Д. С. Чуйков, Ю. А. Запорожский // Информационные технологии. — 2003. — № 1. — С. 2-8.
- [5] Сетевая экспертиза / Д. А. Губанов, Н. А. Коргин, Д. А. Новиков, А. Н. Райков. — М.: Эгвес, 2010. — URL: <https://elibrary.ru/item.asp?id=25312607> (дата обращения: 26.07.2020).
- [6] Sultan, S. Container Security: Issues, Challenges, and the Road Ahead / S. Sultan, I. Ahmad, T. Dimitriou. — DOI 10.1109/ACCESS.2019.2911732 // IEEE Access. — 2019. — Vol. 7. — Pp. 52976-52996. — URL: <https://ieeexplore.ieee.org/document/8693491> (дата обращения: 26.07.2020).
- [7] Belotti, M. A Vademecum on Blockchain Technologies: When, Which, and How / M. Belotti, N. Božić, G. Pujolle,



- S. Secci. — DOI 10.1109/COMST.2019.2928178 // IEEE Communications Surveys & Tutorials. — 2019. — Vol. 21, no. 4. — Pp. 3796-3838. — URL: <https://ieeexplore.ieee.org/document/8760539> (дата обращения: 26.07.2020).
- [8] Богомолов, А. В. Автоматизация обработки информации при проведении коллективных сетевых экспертиз / А. В. Богомолов, Р. С. Климов // Автоматизация. Современные технологии. — 2017. — Т. 71, № 11. — С. 509-512. — URL: <https://elibrary.ru/item.asp?id=30671233> (дата обращения: 26.07.2020). — Рез. англ.
- [9] Hang, L. Design and Implementation of an Integrated IoT Blockchain Platform for Sensing Data Integrity / L. Hang, D.-H. Kim. — DOI 10.3390/s19102228 // Sensors. — 2019. — Vol. 19, no. 10. — Article 2228. — URL: <https://www.mdpi.com/1424-8220/19/10/2228> (дата обращения: 26.07.2020).
- [10] Намиот, Д. Е. HyperCat — структура и модели применения / Д. Е. Намиот, В. П. Куприяновский, Е. В. Зубарева // CEUR Workshop Proceedings: Selected Papers of the First International Scientific Conference Convergent Cognitive Information Technologies (Convergent 2016). Moscow, Russia, November 25-26, 2016; ed. by V. Sukhomlin, E. Zubareva, M. Shneps-Shnepe. — 2016. — Vol. 1763. — Pp. 208-213. — URL: <http://ceur-ws.org/Vol-1763/paper25.pdf> (дата обращения: 26.07.2020). — Рез. англ.
- [11] Блокчейн: как это работает и что ждёт нас завтра / А. Генкин, А. Михеев; ред. А. Петров. — Москва: Альпина Паблишер, 2018.
- [12] Константинов, Н. Э. Блокчейн как платформа для разработки IoT / Н. Э. Константинов, М. Г. Городничев, Р. А. Гематудинов. — DOI 10.24411/2072-8735-2018-10147 // T-Comm: Телекоммуникации и транспорт. — 2018. — Т. 12, № 9. — С. 63-68. — URL: <https://www.elibrary.ru/item.asp?id=36273295> (дата обращения: 26.07.2020).
- [13] Крутова, А. В. Перспективы применения технологии блокчейн в государственной сфере в Российской Федерации / А. В. Крутова, Т. А. Пестерева, В. С. Поварнищина // Инновационное развитие экономики: тенденции и перспективы. — 2018. — Т. 1. — С. 227-232. — URL: <https://elibrary.ru/item.asp?id=36435786> (дата обращения: 26.07.2020).
- [14] Сизоненко, А. Б. Модель защищенной подсистемы контроля документных систем на основе технологии «блокчейн» / А. Б. Сизоненко, О. М. Булгаков, С. Г. Ключев // Моделирование, оптимизация и информационные технологии. — 2018. — Т. 6, № 2. — С. 293-300. — URL: <https://elibrary.ru/item.asp?id=35378195> (дата обращения: 26.07.2020). — Рез. англ.
- [15] Zheng, W. NutBaaS: A Blockchain-as-a-Service Platform / W. Zheng, Z. Zheng, X. Chen, K. Dai, P. Li, R. Chen. — DOI 10.1109/ACCESS.2019.2941905 // IEEE Access. — 2019. — Vol. 7. — Pp. 134422-134433. — URL: <https://ieeexplore.ieee.org/document/8840920> (дата обращения: 26.07.2020).
- [16] Радюкова, Я. Ю. Блокчейн: перспективы развития и проблемы внедрения / Я. Ю. Радюкова, Е. А. Колесниченко, С. О. Епифанова. — DOI 10.21869/2223-1560-2018-22-3-120-127 // Известия Юго-Западного государственного университета. — 2018. — № 3(78). — С. 120-127. — URL: <https://elibrary.ru/item.asp?id=36322054> (дата обращения: 26.07.2020). — Рез. англ.
- [17] Голосовский, М. С. Модель жизненного цикла разработки программного обеспечения в рамках научно-исследовательских работ / М. С. Голосовский // Автоматизация. Современные технологии. — 2014. — № 1. — С. 43-46. — URL: <https://elibrary.ru/item.asp?id=21077730> (дата обращения: 26.07.2020). — Рез. англ.
- [18] Сухомлин, В. А. Методологические аспекты концепции цифровых навыков / В. А. Сухомлин, Е. В. Зубарева, А. В. Якушин. — DOI 10.25559/SITITO.2017.2.253 // Современные информационные технологии и ИТ-образование. — 2017. — Т. 13, № 2. — С. 146-152. — URL: <https://elibrary.ru/item.asp?id=30258665> (дата обращения: 26.07.2020). — Рез. англ.
- [19] Lei, K. Groupchain: Towards a Scalable Public Blockchain in Fog Computing of IoT Services Computing / K. Lei, M. Du, J. Huang, T. Jin. — DOI 10.1109/TSC.2019.2949801 // IEEE Transactions on Services Computing. — 2020. — Vol. 13, issue 2. — Pp. 252-262. — URL: <https://ieeexplore.ieee.org/document/9061111> (дата обращения: 26.07.2020).
- [20] Kwon, S. DIVDS: Docker Image Vulnerability Diagnostic System / S. Kwon, J. Lee. — DOI 10.1109/ACCESS.2020.2976874 // IEEE Access. — 2020. — Vol. 8. — Pp. 42666-42673. — URL: <https://ieeexplore.ieee.org/document/9016185> (дата обращения: 26.07.2020).
- [21] Ларкин, Е. В. Дискретный подход к моделированию синхронизированных эстафет / Е. В. Ларкин, А. Н. Привалов, А. В. Богомолов. — DOI 10.36535/0548-0027-2020-02-3 // Научно-техническая информация. Серия 2. Информационные процессы и системы. — — — URL: <https://elibrary.ru/item.asp?id=42599387> (дата обращения: 26.07.2020). — Рез. англ.
- [22] Ларкин, Е. В. Дискретная модель парных эстафет / Е. В. Ларкин, А. В. Богомолов, А. Н. Привалов, Н. Н. Добровольский. — DOI 10.14529/mmp180306 // Вестник Южно-Уральского государственного университета. Серия: Математическое моделирование и программирование. — 2018. — Т. 11, № 3. — С. 72-84. — URL: <https://elibrary.ru/item.asp?id=35683967> (дата обращения: 26.07.2020).
- [23] Ларкин, Е. В. Эстафеты по выбранным альтернативным маршрутам / Е. В. Ларкин, А. В. Богомолов, А. Н. Привалов, Н. Н. Добровольский. — DOI 10.14529/mmp180102 // Вестник Южно-Уральского государственного университета. Серия: Математическое моделирование и программирование. — 2018. — Т. 11, № 1. — С. 15-26. — URL: <https://elibrary.ru/item.asp?id=32711844> (дата обращения: 26.07.2020).
- [24] Соколов, И. А. Платформа поддержки исследований и подготовки научных кадров факультета вычислительной математики и кибернетики московского государственного университета имени М.В. Ломоносова / И. А. Соколов, В. А. Сухомлин, Е. В. Зубарева, Д. Е. Намиот. — DOI 10.25559/SITITO.15.201902.456-467 // Современные информационные технологии и ИТ-образование. — 2019. — Т. 15, № 2. — С. 456-467. — URL:



<https://elibrary.ru/item.asp?id=41244515> (дата обращения: 26.07.2020). — Рез. англ.

- [25] Семенов, А. В. Блокчейн как инструмент защиты информации / А. В. Семенов, Д. В. Суханов // Теория и практика современной науки. — 2018. — № 6(36). — С. 596-598. — URL: <https://elibrary.ru/item.asp?id=35691425> (дата обращения: 26.07.2020). — Рез. англ.

Поступила 26.07.2020; одобрена после рецензирования 05.10.2020; принята к публикации 29.10.2020.

Об авторах:

Тобин Дмитрий Сергеевич, научный сотрудник, ФГБУН «Санкт-Петербургский Федеральный исследовательский центр Российской академии наук» (199178, Российская Федерация, г. Санкт-Петербург, 14-я линия В.О., д. 39), ORCID: <http://orcid.org/0000-0002-6747-1259>, gniiivm.g@ya.ru

Голосовский Михаил Сергеевич, старший научный сотрудник, ФГБУН «Санкт-Петербургский Федеральный исследовательский центр Российской академии наук» (199178, Российская Федерация, г. Санкт-Петербург, 14-я линия В.О., д. 39), кандидат технических наук, ORCID: <http://orcid.org/0000-0002-1956-9956>

Богомолов Алексей Валерьевич, главный научный сотрудник, ФГБУН «Санкт-Петербургский Федеральный исследовательский центр Российской академии наук» (199178, Российская Федерация, г. Санкт-Петербург, 14-я линия В.О., д. 39), доктор технических наук, профессор, ORCID: <http://orcid.org/0000-0002-7582-1802>

Все авторы прочитали и одобрили окончательный вариант рукописи.

References

- [1] Fernández-Caramès T.M., Fraga-Lamas P. Towards Post-Quantum Blockchain: A Review on Blockchain Cryptography Resistant to Quantum Computing Attacks. *IEEE Access*. 2020; 8:21091-21116. (In Eng.) DOI: <https://doi.org/10.1109/ACCESS.2020.2968985>
- [2] Brinckman A. et al. A Comparative Evaluation of Blockchain Systems for Application Sharing Using Containers. In: *2017 IEEE 13th International Conference on e-Science (e-Science)*. Auckland, New Zealand; 2017. p. 490-497. (In Eng.) DOI: <https://doi.org/10.1109/eScience.2017.80>
- [3] Fedorov M.V., Kalinin K.M., Bogomolov A.V., Stetsyuk A.N. Mathematical model of automated monitoring the implementation of activities in the organs of military command and control. *Informatsionno-izmeritelnye i upravlyayushchie sistemy = Information-measuring and Control Systems*. 2011; 9(5):46-54. Available at: <https://elibrary.ru/item.asp?id=16313311> (accessed 26.07.2020). (In Russ., abstract in Eng.)
- [4] Bogomolov A.V., Chuykov D.S., Zaporozhskiy Yu.A. Means of ensuring information security in modern automated systems. *Informacionnye Tehnologii = Information Technologies*. 2003; (1):2-8. (In Russ.)
- [5] Gubanov D.A., Korgin N.A., Novikov D.A., Raykov A.N. *Setevaya jekspertiza [Network Expertise]*. Egves, Moscow; 2010. Available at: <https://elibrary.ru/item.asp?id=25312607> (accessed 26.07.2020). (In Russ.)
- [6] Sultan S., Ahmad I., Dimitriou T. Container Security: Issues, Challenges, and the Road Ahead. *IEEE Access*. 2019; 7:52976-52996. (In Eng.) DOI: <https://doi.org/10.1109/ACCESS.2019.2911732>
- [7] Belotti M., Božić N., Pujolle G., Secci S. A Vademecum on Blockchain Technologies: When, Which, and How. *IEEE Communications Surveys & Tutorials*. 2019; 21(4):3796-3838. (In Eng.) DOI: <https://doi.org/10.1109/COMST.2019.2928178>
- [8] Bogomolov A.V., Klimov R.S. Automation of information processing during collective network examinations. *Avtomatizatsiya. Sovremennyye Tekhnologii*. 2017; 71(11):509-512. (In Russ., abstract in Eng.)
- [9] Hang L., Kim D.-H. Design and Implementation of an Integrated IoT Blockchain Platform for Sensing Data Integrity. *Sensors*. 2019; 19(10):2228. (In Eng.) DOI: <https://doi.org/10.3390/s19102228>
- [10] Namiot D., Kupriyanovsky V., Zubareva E. HyperCat — the structure and use cases. *CEUR Workshop Proceedings*. 2016; 1763:208-213. Available at: <http://ceur-ws.org/Vol-1763/paper25.pdf> (accessed 26.07.2020). (In Russ., abstract in Eng.)
- [11] Genkin A.S., Mikheyev A.A. *Blokcheyn. Kak rabotayet i chto zhdet nas zavtra [Blockchain How it works and what awaits us tomorrow]*. Moscow, Alpina Publisher LLC; 2018. (In Russ.)
- [12] Konstantinov N.E., Gorodnichev M.G., Gematudinov R.A. Blockchain as an IoT development platform. *T-Comm: Телекоммуникации и транспорт*. 2018; 12(9):63-68. (In Eng.) DOI: <https://doi.org/10.24411/2072-8735-2018-10147>
- [13] Krutova A.V., Pestereva T.A., Povarnitsyna V.S. *Perspektivy primeneniya tekhnologii blokcheyn v gosudarstvennoy sfere v Rossiyskoy Federatsii [Prospects for the application of blockchain technology in the public sphere in the Russian Federation]*. *Innovatsionnoye razvitiye ekonomiki: tendentsii i perspektivy = Innovative Development of the Economy: Trends and Prospects*. 2018; 1:227-232. Available at: <https://elibrary.ru/item.asp?id=36435786> (accessed 26.07.2020). (In Russ.)
- [14] Sizonenko A.B., Bulgakov O.M., Klyuev S.G. Model of Protected Tracking Subsystem of Records System Based on Blockchain Technology. *Modelirovaniye, optimizatsiya i informatsionnyye tekhnologii = Modeling, Optimization and Information Technology*. 2018; 6(2):293-300. Available at: <https://elibrary.ru/item.asp?id=35378195> (accessed 26.07.2020). (In Russ., abstract in Eng.)
- [15] Zheng W., Zheng Z., Chen X., Dai K., Li P., Chen R. NutBaaS: A Blockchain-as-a-Service Platform. *IEEE Access*. 2019; 7:134422-134433. (In Eng.) DOI: <https://doi.org/10.1109/ACCESS.2019.2941905>
- [16] Radyukova Ya.Yu., Kolesnichenko E.A., Epifanova S.O. Blockchain: Development Prospects and Implementation Challenges. *Izvestiya Yugo-Zapadnogo gosudarstvennogo universiteta = Proceedings of Southwest State University*. 2018; (3):120-127. (In Russ., abstract in Eng.) DOI: <https://doi.org/10.21869/2223-1560-2018-22-3-120-127>



- [17] Golosovskiy M.S. *Model' zhiznennogo cikla razrabotki programmynogo obespecheniya v ramkah nauchno-issledovatel'skih rabot* [Life cycle model of the software development within scientifically-research works]. *Avtomatizatsiya. Sovremennye tekhnologii* = Automation. Modern technologies. 2014; (1):43-46. Available at: <https://elibrary.ru/item.asp?id=21077730> (accessed 26.07.2020). (In Russ., abstract in Eng.)
- [18] Sukhomlin V.A., Zubareva E.V., Yakushin A.V. *Metodologicheskie aspekty koncepcii cifrovyyh navykov* [Methodological aspects of the Digital Skills Concept]. *Sovremennye informacionnyye tekhnologii i IT-obrazovanie* = Modern Information Technologies and IT-Education. 2017; 13(2):146-152. (In Russ., abstract in Eng.) DOI: <https://doi.org/10.25559/SITITO.2017.2.253>
- [19] Lei K., Du M., Huang J., Jin T. Groupchain: Towards a Scalable Public Blockchain in Fog Computing of IoT Services Computing. *IEEE Transactions on Services Computing*. 2020; 13(2):252-262. (In Eng.) DOI: <https://doi.org/10.1109/TSC.2019.2949801>
- [20] Kwon S., Lee J. DIVDS: Docker Image Vulnerability Diagnostic System. *IEEE Access*. 2020; 8:42666-42673. (In Eng.) DOI: <https://doi.org/10.1109/ACCESS.2020.2976874>
- [21] Larkin E.V., Privalov A.N., Bogomolov A.V. Discrete Approach to Simulating Synchronized Relay Races. *Automatic Documentation and Mathematical Linguistics*. 2020; 54(1):43-51. (In Eng.) DOI: <https://doi.org/10.3103/S0005105520010082>
- [22] Larkin E.V., Bogomolov A.V., Privalov A.N., Dobrovolsky N.N. Discrete Model of Paired Relay-Race. *Vestnik Yuzhno-Ural'skogo gosudarstvennogo universiteta. Seriya: Matematicheskoye modelirovaniye i programmirovaniye* = Bulletin of the South Ural State University. Series: Mathematical Modelling, Programming and Computer Software. 2018; 11(3):72-84. (In Eng.) DOI: <https://doi.org/10.14529/mmp180306>
- [23] Larkin E.V., Bogomolov A.V., Privalov A.N., Dobrovolsky N.N. Relay Races Along a Pair of Selectable. *Vestnik Yuzhno-Ural'skogo gosudarstvennogo universiteta. Seriya: Matematicheskoye modelirovaniye i programmirovaniye* = Bulletin of the South Ural State University. Series: Mathematical Modelling, Programming and Computer Software. 2018; 11(1):15-26. (In Eng.) DOI: <https://doi.org/10.14529/mmp180102>
- [24] Sokolov I.A., Sukhomlin V.A., Zubareva E.V., Namiot D.E. Support Platform for Researches and Training of Scientific Personnel of the Faculty of Computational Mathematics and Cybernetics of Lomonosov Moscow State University. *Sovremennye informacionnyye tekhnologii i IT-obrazovanie* = Modern Information Technologies and IT-Education. 2019; 15(2):456-467. (In Russ., abstract in Eng.) DOI: <https://doi.org/10.25559/SITITO.15.201902.456-467>
- [25] Semenov A.V., Sukhanov D.V. Blockchain as an Information Security Tool. *Teoriya i praktika sovremennoy nauki* = Theory and Practice of Modern Science. 2018; (6):596-598. Available at: <https://elibrary.ru/item.asp?id=35691425> (accessed 26.07.2020). (In Russ., abstract in Eng.)

About the authors:

Dmitry S. Tobin, Researcher, St. Petersburg Federal Research Center of the Russian Academy of Sciences (39, 14th Line V.O., St. Petersburg 199178, Russian Federation), ORCID: <http://orcid.org/0000-0002-6747-1259>, gniiivm.g@ya.ru

Mikhail S. Golosovsky, Senior Researcher, St. Petersburg Federal Research Center of the Russian Academy of Sciences (39, 14th Line V.O., St. Petersburg 199178, Russian Federation), Ph.D. (Engineering), ORCID: <http://orcid.org/0000-0002-1956-9956>

Alexey V. Bogomolov, Chief Researcher, St. Petersburg Federal Research Center of the Russian Academy of Sciences (39, 14th Line V.O., St. Petersburg 199178, Russian Federation), Dr.Sci. (Engineering), Professor, ORCID: <http://orcid.org/0000-0002-7582-1802>

All authors have read and approved the final manuscript.

*Submitted 26.07.2020; approved after reviewing 05.10.2020;
accepted for publication 29.10.2020.*

