УДК 004.056.2 DOI: 10.26102/2310-6018/2020.29.2.002

Алгоритмизация взаимного информационного согласия в системах с распределенным реестром на основе цепочки блоков

С.С.Еськов, О.Я.Кравец
Воронежский государственный технический университет
Воронеж, Российская Федерация

Аннотация: Объектом исследования в работе являются системы распределенного реестра на основе цепочки блоков. Предметом исследования является математическое и программное обеспечение распределенной обработки данных при решении задачи достижения взаимного информационного согласования в системах распределенного реестра на основе цепочки блоков. Цель работы заключается в разработке алгоритма функционирования узла системы с возможностью реализации им нештатных функций, алгоритма взаимного информационного согласования в системе распределенного реестра на базе цепочки блоков, проведение планирования численных экспериментов для оценки эффективности математического и программного обеспечения взаимного информационного согласования в системах распределенного реестра на основе цепочки блоков. Исследование существующих подходов показало, что большинство исследований не в полной мере учитывают одновременную реализацию узлами нештатных функций и изменение структурно-параметрических характеристик системы вследствие объединения узлов в группы. В результате предложен алгоритм функционирования узла системы, учитывающий возможность реализации нештатных функций: формирование ответвления обрабатываемых данных и атаку временной блокировки. Представлен обобщенный алгоритм функционирования системы распределенного реестра на базе цепочки блоков при выполнении алгоритма взаимного информационного согласования, учитывающий возможность объединения узлов в группы. Проведено планирование численного эксперимента.

Ключевые слова: распределенный реестр, формализация, алгоритм, взаимное информационное согласование, нештатные функции, централизация.

Для цитирования: Еськов С.С., Кравец О.Я. Алгоритмизация взаимного информационного согласия в системах с распределенным реестром на основе цепочки блоков. *Моделирование, оптимизация и информационные технологии.* 2020;8(2). Доступно по: https://moit.vivt.ru/wp-content/uploads/2020/05/EskovKravets_2_20_1.pdf DOI: 10.26102/2310-6018/2020.29.2.002

Algorithmization of mutual information consent in systems with a distributed registry, based on a block chain

S.S.Eskov, O.J.Kravets
Voronezh Technical State University, Voronezh, Russian Federation

Abstract: The object of research is distributed registry systems based on a chain of blocks. The subject of the research is mathematical and software for distributed data processing in solving the problem of achieving mutual information coordination in distributed registry systems based on a chain of blocks. The purpose of the work is to develop an algorithm for the functioning of a system node with the ability to implement non-standard functions, an algorithm for mutual information matching in a distributed registry system based on a chain of blocks, planning numerical experiments to evaluate the effectiveness

of mathematical and software for mutual information matching in distributed registry systems based on a chain of blocks. The study of existing approaches has shown that most studies do not fully take into account the simultaneous implementation of non-standard functions by nodes and changes in the structural and parametric characteristics of the system due to the combination of nodes in groups. As a result, an algorithm for the functioning of the system node is proposed, which takes into account the possibility of implementing non-standard functions: the formation of a branch of the processed data and a temporary blocking attack. A generalized algorithm for the functioning of a distributed registry system based on a chain of blocks when performing an algorithm for mutual information coordination, taking into account the possibility of combining nodes into groups, is presented. The numerical experiment was planned.

Keywords: distributed ledger technology, formalization, algorithm, mutual information agreement, non-standard functions, centralization.

For citation: Eskov S.S., Kravets O.J. Algorithmization of mutual information consent in systems with a distributed registry, based on a block chain. *Modeling, Optimization and Information Technology*. 2020;8(2). Available from: https://moit.vivt.ru/wp-content/uploads/2020/05/EskovKravets_2_20_1.pdf DOI: 10.26102/2310-6018/2020.29.2.002 (In Russ).

Введение

Актуальным направлением совершенствования технологий распределенных программных систем является исследование возможностей использования в их архитектуре концепций и технологических решений на базе распределенного реестра (distributed ledger technology – DLT). Особенностью DLT является децентрализация процесса хранения данных и синхронизации этих данных на основе класса алгоритмов взаимного информационного согласования (ВИС). К алгоритмам ВИС предъявляются требования по отказоустойчивости и учету возможности нештатного функционирования отдельных узлов. В программном обеспечении практических реализаций DLT систем, например, таких, как платежные peer-to-peer системы, используется технология цепочки блоков (ЦБ), в общем случае удовлетворяющая перечисленным выше требованиям.

Наиболее известные подходы к моделированию работы DLT систем на основе ЦБ (DLT ЦБ систем) и оценке вероятности формирования альтернативной ЦБ были опубликованы [1, 2, 3] S. Nakamoto, M. Rosenfeld, В. Бутерин, C. Pinzon, C. Rocha. Однако, большинство предложенных моделей при оценке вероятности создания альтернативной ЦБ учитывают только хэшрейт и влияние временных параметров, но не учитывают взаимное влияние нештатных функций стратегий поведения узлов, таких как: атака временной блокировки и формирование ответвления обрабатываемых данных (fork). В настоящее время крайне мало работ направленных на эмпирическое обоснование адекватности оценки вероятности формирования единой ЦБ.

В данной статье предложен обобщенный подход к алгоритмизации работы DLT ЦБ систем, учитывающий объединение узлов системы в группы и реализацию ими нештатных функций стратегии поведения: атаку временной блокировки и формирование ответвления обрабатываемых данных (fork) при выполнении алгоритма ВИС, произведено планирование численных экспериментов для оценки эффективности разработанного математического и программного обеспечения.

Алгоритмизация функционирования узла DLT ЦБ системы

Определим отдельный m-й узел DLT ЦБ системы в виде конечного автомата с переменной структурой функционирующий в стохастической среде E, представленной множеством узлов системы A (за исключением m-го узла).

Представил процесс функционирования узла DLT ЦБ системы в виде обобщенного алгоритма (Рисунок 1). При этом, будем рассматривать следующие варианты стратегии поведения узла:

- выполнение алгоритма ВИС с вероятностью p непреднамеренного сбоя, b_1;
- попытка формирования ответвления обрабатываемых данных, b_2;
- публикация найденного блока, b_3;
- попытка реализации атаки временного блокирования, b_4.

В процессе функционирования узлы DLT ЦБ системы в зависимости от входных данных и своего внутреннего состояния выполняют конечное число действий: проверка поступивших транзакций и блоков; обновление ЦБ; передача в сеть вновь созданных блоков; ретрансляция транзакций по сети и т.д. Будем рассматривать действия узла системы направленные непосредственно на достижение ВИС: принятие единого ЦБ, генерацию, ретрансляцию и проверку блоков.

В реальных DLT ЦБ системах в ходе достижения ВИС узлы системы должны постоянно доказывать свое участие выполнением алгоритма Proof-of-. Критерием успешности узла – увеличением его доходности D при выполнении алгоритма Proof-of- – является доля ресурсов узла относительно ресурсов всей системы. Обозначим долю ресурсов m-го узла при выполнении алгоритма Proof-of- через h_m, тогда ресурсы всей системы будут равны $H = \sum_{m=1}^{|A|} h_m$.

Так как различные операции, например, проверки транзакций и блоков имеют вполне определенные вычислительно-временные затраты, а добавление нового блока в ЦБ производится через усреднено дискретные интервалы времени, примем допущение, что DLT ЦБ система функционирует в дискретном времени $t \in N_0$.

Назовем блок, удовлетворяющий всем требованиям безопасности и являющийся по правилам алгоритма ВИС очередным на интервале времени t_n при добавлении в ЦБ, блоком с наибольшим «значением» относительно предыдущего, сгенерированного на интервале времени t_{n-1}. Назовем стабильностью работы DLT ЦБ системы вероятность формирования единой ЦБ.

Предлагаемый алгоритм состоит из следующих основных этапов:

- сбор данных;
- выполнение алгоритма ВИС;
- получение реакции среды;
- выбор варианта стратегии поведения.

На этапе сбора данных производится определение параметров автомата и правил ВИС:

- обновление или перезапись (при необходимости) ЦБ;
- проверка главного блока ЦБ;
- корректировки матрицы состояний $\| a_{ij}(X(t)) \|$;
- задание значения доли ресурсов;
- определение правил ВИС (ВИС Накамото, ВИС GHOST и т.д.).

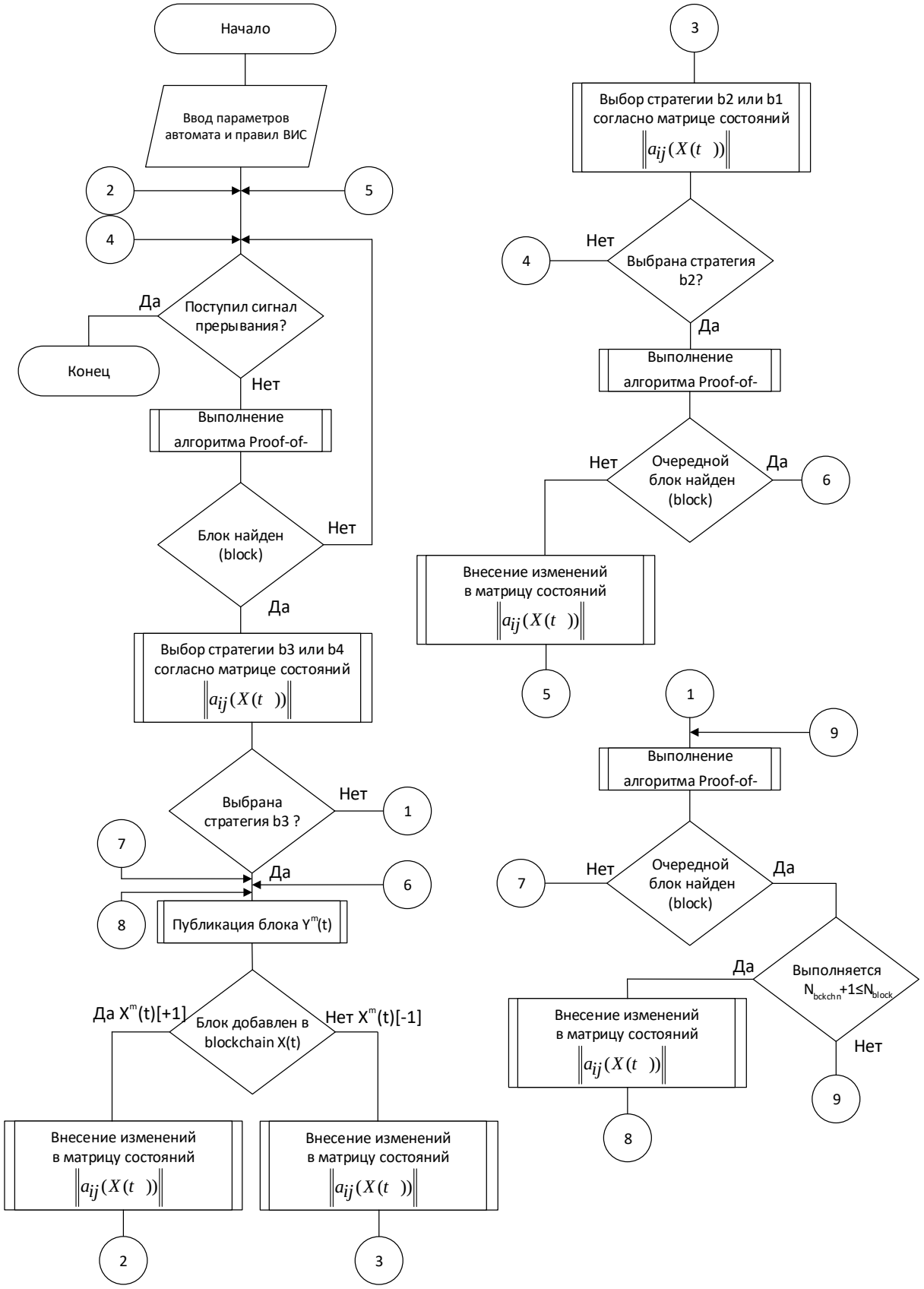

Рисунок 1. Алгоритм функционирования узла DLT ЦБ системы
Figure 1. Node of DLT BC system functioning algorithm

На втором этапе автомат выполняет алгоритм ВИС с целью формирования очередного блока. На данном этапе возможны два исхода $Y^m(t)$ на каждом интервале времени t_n: успешное решение алгоритма ВИС $Y^m(t)[+1]$ – генерация нового блока и неуспешное $Y^m(t)[-1]$ – блок не был найден. В случае $Y^m(t)[-1]$ автомат продолжает выполнять алгоритм до момента генерации нового блока. В случае успешного решения автомат имеет выбор между вариантами стратегии поведения: публикация найденного блока b_3 и попытка реализации атаки временного блокирования b_4. Данный выбор основывается на матрице состояний автомата $\| a_{ij}(X^m(t)) \|$, где $X^m(t)$ – реакция среды, ячейки которой имеют значения вероятностей перехода из одного варианта стратегии в другой. Отметим, что в начальный момент времени все вероятности равны между собой, при этом выполняется неравенства:

$$0 \le a_{ij}(X^m(t)) \le 1 \quad (1)$$

$$\sum_j a_{ij}(X^m(t)) = 1 \quad (2)$$

При выборе b_4 автомат не публикует найденный блок и продолжает выполнять алгоритм ВИС на своем найденном блоке, при этом, в случае последующих успешных решений $X^m(t)[+1]$ и выполнения неравенства:

$$N_{otr} + 1 \le N_{block} \quad (3)$$

где N_{otr} – число неуспешных решений, N_{block} – число блоков, найденных при выполнении стратегии временного блокирования, будем считать, что автомат реализовал атаку временной блокировки. В противном случае будем считать атаку не удачной. После реализации/не реализации атаки b_4 автомат возвращается в b_1. При этом в зависимости от результата проведения атаки b_4 меняются значения вероятностей переходов матрицы $\| a_{ij}(X^m(t)) \|$ в b_4 и b_3 на Δ при выполнении выражений 1 и 2.

В случае выбора варианта стратегии публикации найденного блока b_3 в зависимости от реакции $X^m(t)$ среды E: добавление блока в ЦБ или принятие другого альтернативного блока на интервале времени t_n автомат имеет следующие варианты стратегии поведения:

- в случае добавления блока в ЦБ, автомат переходит в b_1 и продолжает выполнять алгоритм ВИС;
- в случае принятия альтернативного блока автомат в зависимости от матрицы $\| a_{ij}(X^m(t)) \|$ осуществляет переход в b_1 или b_2.

При выборе b_1 автомат продолжает выполнять алгоритм ВИС.

При выборе b_2 автомат реализует попытку формирования ответвления обрабатываемых данных и продолжает выполнять алгоритм ВИС на своем, отличном от общепринятого блоке. В случае успешного решения алгоритма ВИС на последующих раундах и принятия множеством A альтернативной ЦБ, сгенерированной автоматом, атака b_2 считается успешной. Вносятся изменения в матрицу $\| a_{ij}(X^m(t)) \|$, увеличивающие значение вероятности перехода в b_2 и уменьшающие в b_1 из состояния b_3. При не принятии множеством A ЦБ автомата и отставании от единой ЦБ, автомат вносит противоположную коррекцию в матрицу $\| a_{ij}(X^m(t)) \|$ и переходит в b_1.

Алгоритмизация функционирования DLT ЦБ системы

Для представления функционирования DLT ЦБ системы при достижении взаимного информационного согласия предлагается общий алгоритм (Рисунок 2).

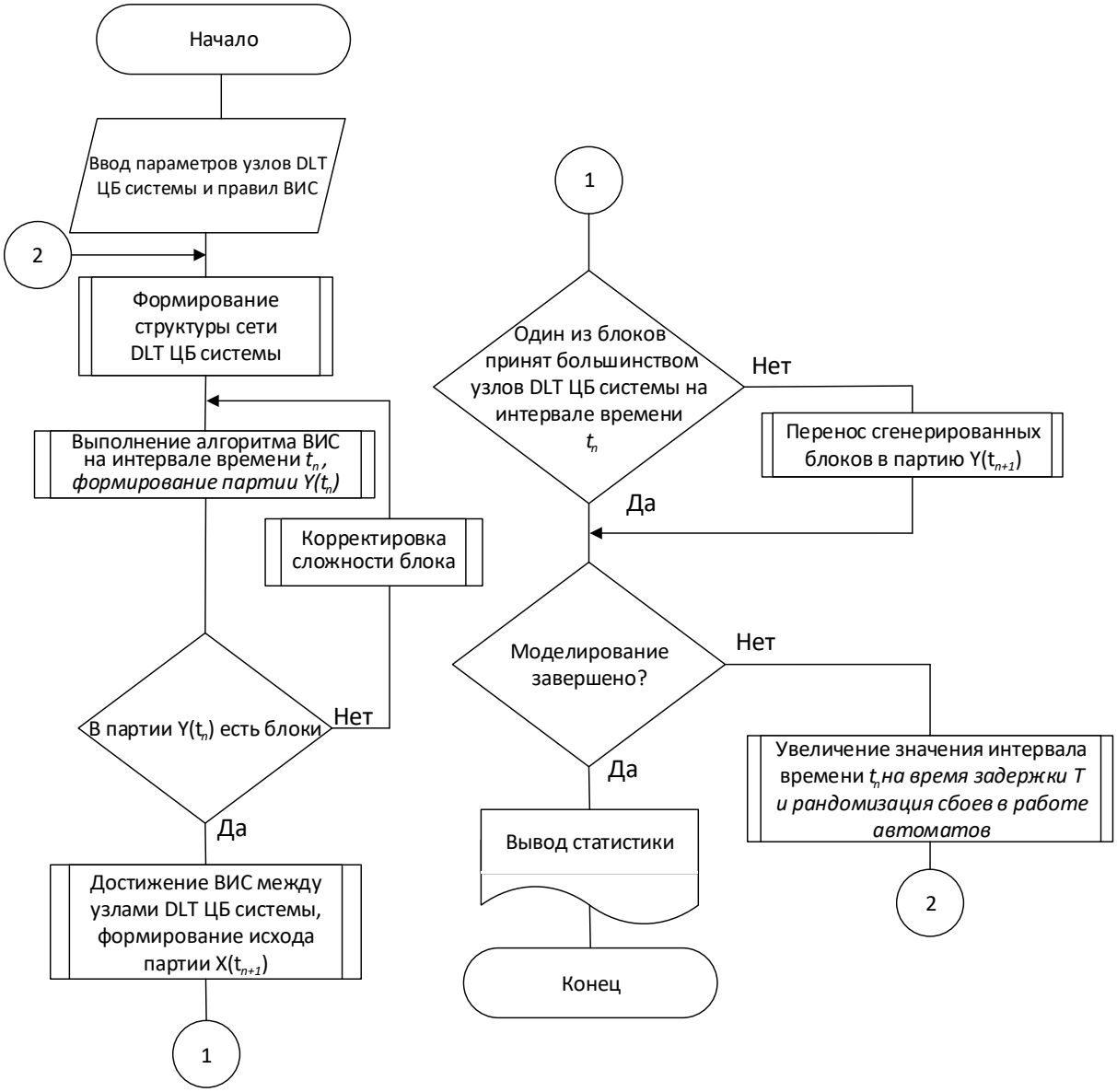

Рисунок 2. Алгоритм функционирования DLT ЦБ системы
Figure 2. DLT BC system functioning algorithm

Предложенный алгоритм функционирования DLT ЦБ системы является итерационным и учитывает возможность сбоев в работе узлов, отсутствие сгенерированных блоков на интервале времени t_n, образованном заданным периодом задержки T генерации блоков.

Алгоритм состоит из следующих основных этапов:

- ввод параметров узлов DLT ЦБ системы и правил ВИС;
- формирование структуры сети DLT ЦБ системы;
- выполнение алгоритма ВИС на интервале t_n, формирование партии $Y(t)$;
- корректировка сложности блока;

- достижение ВИС между узлами DLT ЦБ системы, формирование исхода партии $X(t)$.

Этап ввода параметров узлов DLT ЦБ системы и правил ВИС предназначен для формирования узлов и реализации этапа сбора данных отдельными узлами.

Основная функция этапа формирования структуры сети DLT ЦБ системы является создание связей между автоматами множества A;

Шаг выполнения алгоритма ВИС на интервале времени t_n и формирования партии $Y(t)$ предназначен для имитации работы системы по выполнению ВИС. На этом этапе автоматы генерируют новые блоки и в зависимости от выбранного варианта стратегии поведения публикуют их, либо реализуют нештатные функции: формирование ответвления обрабатываемых данных и атаку временной задержки.

В ходе целесообразного поведения – постоянной подстройки, выбора вариантов поведения в зависимости от условий среды узлов системы и заложенной сложности генерации блока по требованиям безопасности конкретной реализации ВИС вероятны ситуации отсутствия нового блока на интервале времени t_n, вызванные попыткой реализации нештатных функций, как отдельным узлом системы, так и группой узлов.

Алгоритм поддерживает заданное значение времени задержки T между периодами генерации блоков, на этапе корректировки сложности блока, путем изменения сложности решения нового блока на каждом интервале времени t_n. Данное правило алгоритма позволяет увеличить стабильность работы системы и удовлетворить требования безопасности алгоритмов взаимного информационного согласования – среднее число генерации блоков за период времени T близкого единице.

В случае опубликования блоков на интервале времени t_n, формируется партия $Y(t_n) = (Y^1(t_n), Y^2(t_n), ..., Y^{|A|}(t_n))$, где $Y^m(t_n)$ – выходной сигнал m-го узла DLT ЦБ системы. При опубликовании блока выходной сигнал $Y^m(t_n)$ является блоком с заданными параметрами времени генерации, уникального номера, номера автомата, который его создал (в алгоритме GHOST добавляется поле номеров блоков «дядей»). В случае отсутствия блока $Y^m(t_n)$ является пустым сигналом.

На этапе достижения ВИС между узлами DLT ЦБ системы определяется блок, который будет добавлен в ЦБ и формируется исход партии $X(t_{n+1}) = (X^1(t_{n+1}), X^2(t_{n+1}), ..., X^{|A|}(t_{n+1}))$, при этом все сигналы $X^m(t_{n+1})$ для каждого m-го автомата имеют одно и то же значение – блок, добавленный в ЦБ, отнесенный к классам $X(t)[+1]$ или $X(t)[-1]$ в зависимости от номера узла сгенерировавшего блок. В случае принятия большинством узлов системы (более 51%) исхода партии $X(t_{n+1})$ происходит рандомизация сбоев в работе узлов системы, увеличение t_n на значение T и переход алгоритма на следующую итерацию. При отсутствии ВИС между автоматами, блоки, сгенерированные на интервале t_n, будут перенесены и учтены на следующем ВИС на интервале t_{n+1}.

Стремление увеличить доходность выполнения алгоритма ВИС каждым отдельных узлов DLT ЦБ системы приводит к появлению эффекта групп (совместного поведения) путем структурно-параметрических модификаций, таких, например, как объединение нескольких узлов в группы (пул). Данный подход приводит к централизации и увеличению доли сгенерированных блоков определенной группой узлов, что негативно влияет на стабильность работы всей системы. На Рисунке 3 представлена структура DLT ЦБ системы, учитывающая возможность объединения

отдельных узлов в группы посредством механизма информационного обмена.

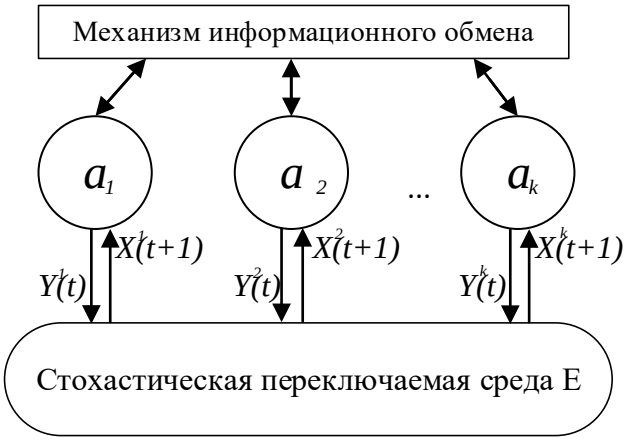

Рисунок 3. Структура DLT ЦБ системы в виде коллектива автоматов с возможностью объединения в группы

Figure 3. The structure of the DLT BC system in the form of a collective of machines with the possibility of combining into groups

Вероятность образования альтернативной ЦБ в результате реализации одного или нескольких вариантов стратегии нештатного функционирования узла, увеличивается с ростом централизации системы. Для оценки централизации системы введем показатель W отражающий отношение максимального значения ресурсных мощностей h_z, сосредоточенных в одной группе (пуле) или узле DLT ЦБ системы к общему значению ресурсной мощности всей системы $\sum_{z=1}^{M} h_z$, где M – число групп и отдельных узлов в системе:

$$W = \frac{\mathrm{Max}(h_z)}{\sum_{z=1}^{M} h_z} \quad (4)$$

Число циклов работы алгоритма задается при формировании структуры сети, что обеспечивает конечность выполнения алгоритма сигналом прерывания.

Разработка структуры программного обеспечения системы управления DLT ЦБ системой

Для оценки влияния учета нештатных функций узлов системы, корректировки времени задержки генерации блоков и возможности объединения узлов системы в группы на вероятность формирования единой ЦБ разработаем имитационную модель на основе алгоритмов процесса функционирования узла DLT ЦБ системы и процесса достижения ВИС между ее узлами. Выбор имитационного моделирования обуславливается возможностью проведения направленного вычислительного эксперимента и его достаточная распространенность для выполнения такого класса задач, доказывающая эффективность применения данного метода исследования на практике.

На данный момент существует большое количество программного обеспечения предназначенного для имитационного моделирования: COMNET III, Arena, Taylor, MATLAB, AnyLogic, ARIS и другие.

Однако, использование коммерческого ПО накладывает ограничение на гибкость

разрабатываемой модели, например, отсутствие возможности изменения значений параметров для некоторых законов распределения, а так же в большинстве своем не являются свободно распространяемыми. В связи с этим, имитационная модель была разработана в среде программирования C++ Builder на языке программирования C++. Данная среда является универсальной, свободно распространяемой и позволяет подробно описать и воспроизвести процесс взаимодействия элементов.

Описание модельного времени будет пошаговым в связи с принятым выше допущением. Структура информационного взаимодействия модулей программной реализации имитационной модели представлена на Рисунках 4-6. Декомпозиция разработанных модулей формирования параметров узлов DLT системы и моделирования работы алгоритма взаимного информационного согласования DLT системы на основе ЦБ представлены на Рисунках 5 и 6.

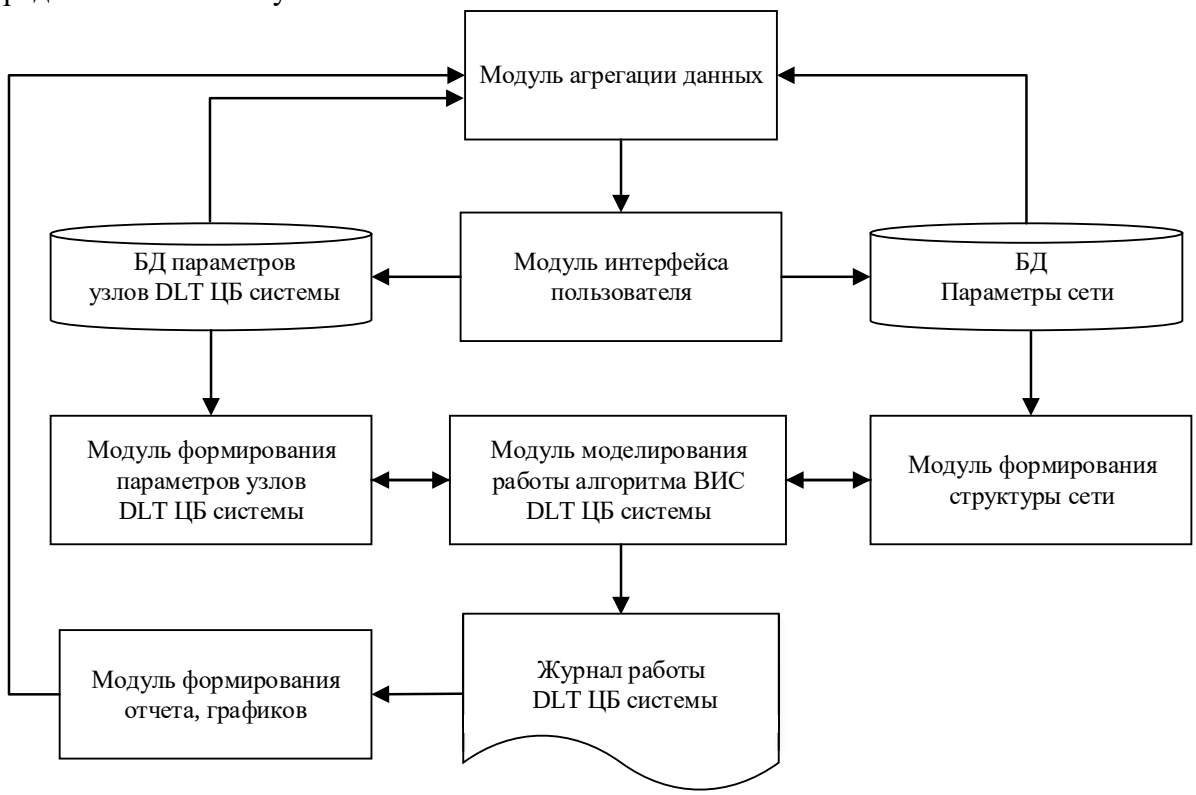

Рисунок 4. Структура информационного взаимодействия модулей программного обеспечения системы управления DLT ЦБ системой

Figure 4. The structure of the information interaction of the software modules of the control system DLT BC system

Учет особенностей реализации алгоритмов ВИС конкретных DLT систем реализован в модуле определения валидной ЦБ (ВИС Накамото, GHOST, и т.д.) и модуле БД параметров сети путем загрузки параметров из модуля интерфейса пользователя (Рисунок 6). Модуль определения валидной ЦБ (ВИС Накамото, GHOST, и т.д.) позволяет использовать для определения очередности добавления блоков в ЦБ такие особенности реализации различных алгоритмов ВИС, как правило наиболее «длинной» цепи относительно генезиса блока и правило наиболее «тяжелого» блока.

Планирование численных экспериментов для оценки эффективности математического и программного обеспечения ВИС в DLT ЦБ системах

Имитационное моделирование предполагает следующие этапы [6]:

- создание модели;

- разработка алгоритма имитационной модели;
- проведения исследования на ЭВМ;
- корректировка (модификация) объекта с учетом результатов эксперимента.

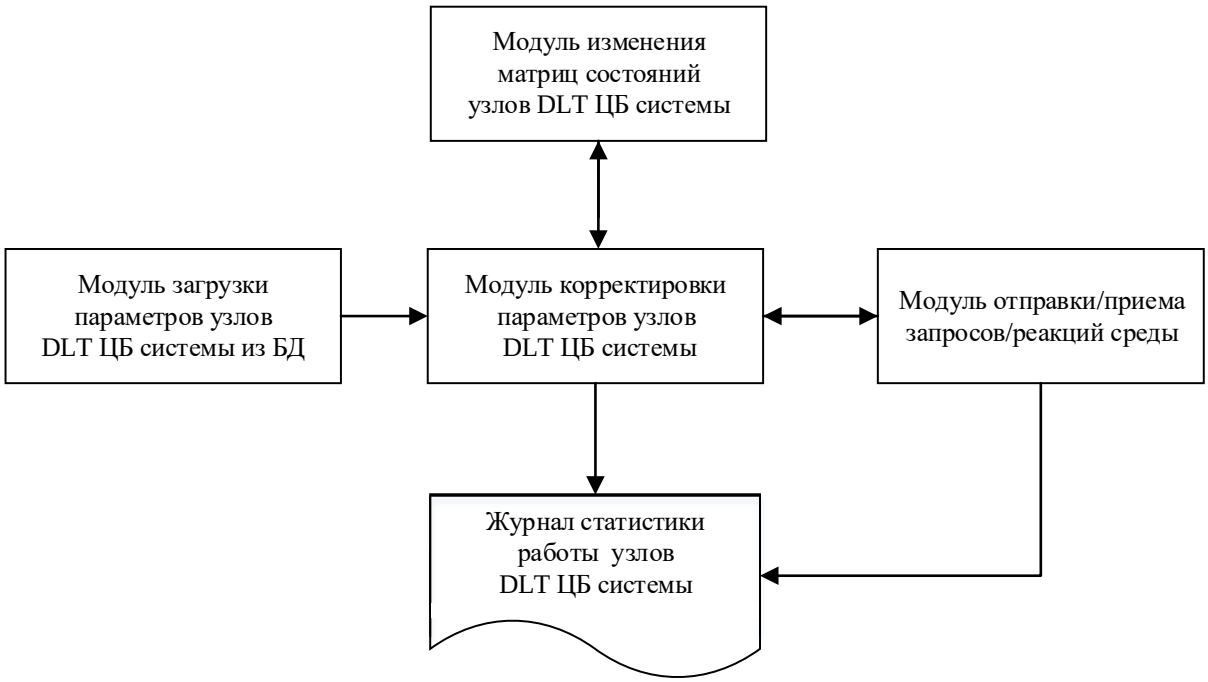

Рисунок 5. Структура информационного взаимодействия в модуле формирования параметров узлов DLT ЦБ системы

Figure 5. The structure of information interaction in the module for generating parameters of DLT BC nodes

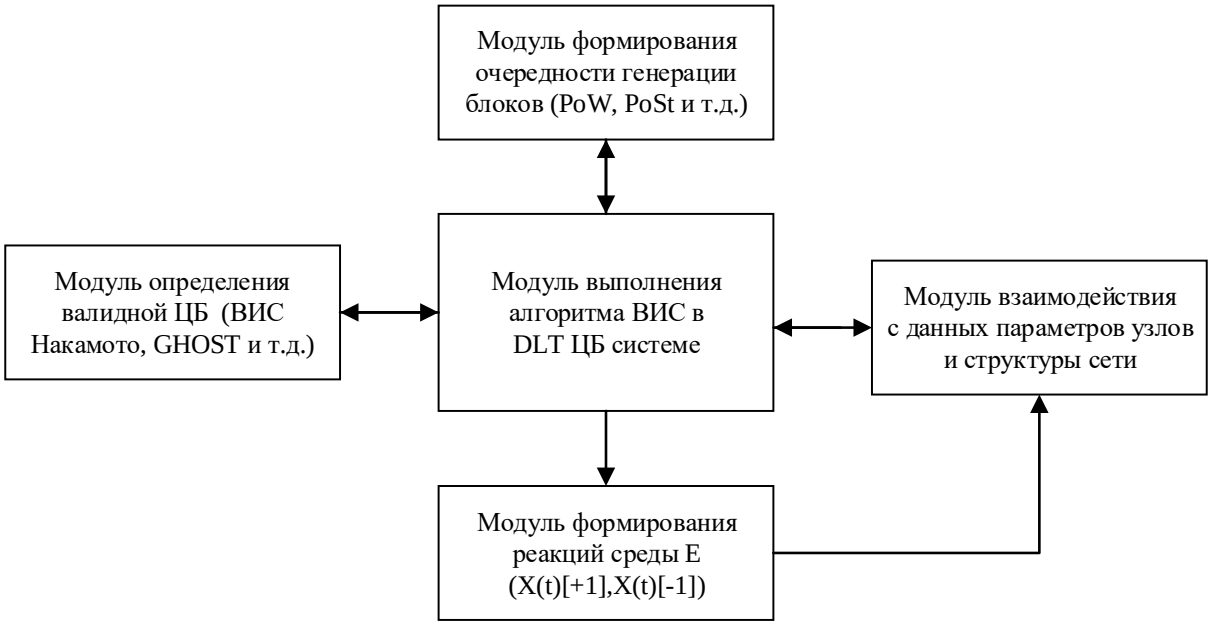

Рисунок 6. Структура информационного взаимодействия в модуле моделирования работы алгоритма ВИС DLT ЦБ системы

Figure 6. The structure of information interaction in the module for modeling the operation of the VIS DLT BC algorithm

Для возможности проверки адекватности разработанной модели после проведения вычислительного эксперимента, зададим начальные значения параметров имитационного моделирования в соответствии с реальной DLT ЦБ системой – платежной peer-to-peer системой Bitcoin:

- определим правило ВИС, как правило, наиболее длинной «цепи»;
- определим число автоматов участвующих в алгоритме ВИС 10000 шт.;
- время задержки генерации блока T = 10 мин.;
- время распространения блока по сети 6,5 с (достижение более 50% узлов);
- суммарный объем ресурсов всей системы $H = \sum_{n=1}^{|A|} h_n$ (сложность майнинга) $16*10^{12}$ H/s;
- оценка централизации системы Bitcoin. Каждый блок имеет coinbase-транзакцию, которая чаще всего указывает (имеет тег) на объект (пул, узел), создавший блок, например тег Poolin. Однако, данные тега могут быть изменены узлом или пулом с целью скрыть реальную долю хешрейта в системе. Например, пул Slushpool использует множество различных адресов для тегирования блоков, а F2Pool только один адрес 1KFHE7w8BhaENAswwryaoccDb6qcT6DbYY. Учитывая данный факт, произведем оценку централизации системы (Рисунок 7).

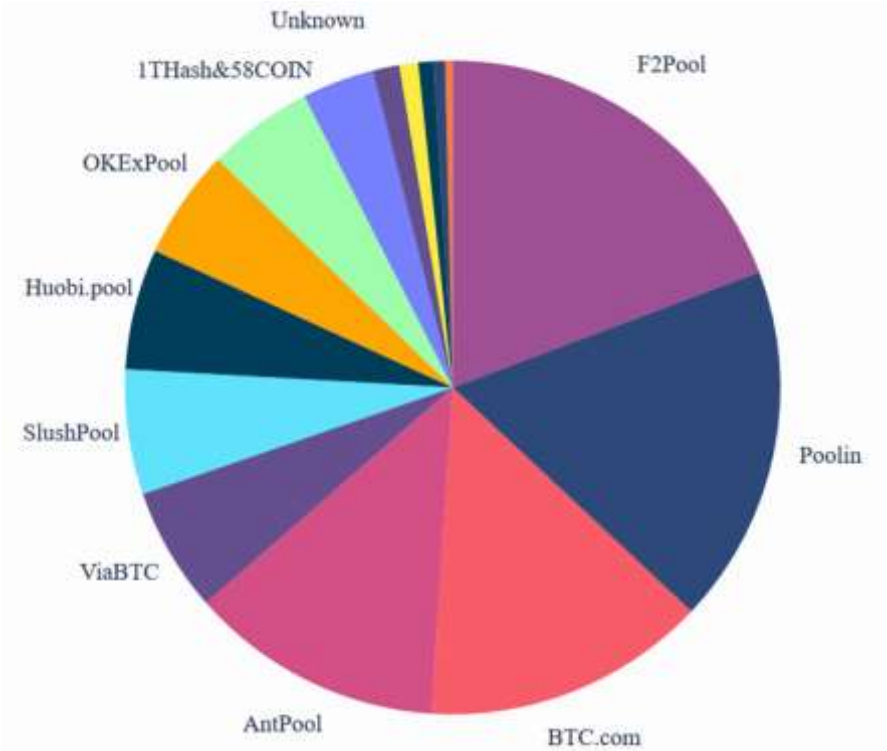

Рисунок 7. Распределение доли ресурсов по узлам и группам (пулам) в Bitcoin (использованы данные [4])

Figure 7. Distribution of the share of resources among nodes and groups (pools) in Bitcoin (data used [4])

Как видно из Рисунка 7, более половины ресурсов систем составляют 4 пула: F2Pool, Poolin, BTC.com и AntPool. На их долю пришлось 340 сгенерированных блоков из 535: F2Pool 103 блока, Poolin 95 блоков, BTC.com 75 блоков, AntPool 67 блоков, что свидетельствует о значительной централизации системы.

Таким образом для моделирования работы системы Bitcoin необходимо разбить 10 000 автоматов на 15 групп по числу пулов. При этом процентное соотношение долей ресурсов этих групп относительно всей сети – коэффициенты централизации будут распределены в соответствии с Таблицей 1.

Исходные данные получены с использованием [5] в ходе наблюдения за системой Bitcoin в течение 4 дней и будут применены как входные данные имитационной модели. Для использования полученных данных в моделировании процесса ВИС экстраполируем значения показателей на период 10^{10} раундов.

Адекватность разработанных алгоритмов процесса функционирования узла DLT ЦБ системы и процесса достижения ВИС между узлами будем оценивать корреляционным анализом полученных значений с результатами мониторинга реальных платежных систем. Выходные данные имитационной модели являются: количество блоков, добавленных в цепочку блоков за весь период моделирования, среднее время задержки генерации блоков, централизация системы, число добавленных блоков относительно ресурсной мощности узла системы.

Таблица 1. Коэффициент централизации пулов в системе Bitcoin
Table 1. Pool centralization coefficient in the Bitcoin system

Наименование Пула	Число добытых блоков	Коэф. централизации
F2Pool	103	19,25
Poolin	95	17,75
BTC.com	75	14,01
AntPool	67	12,52
ViaBTC	33	6,16
SlushPool	33	6,16
Huobi.pool	32	5,98
OKExPool	29	5,42
1THash&58COIN	28	5,23
Unknown	19	3,55
BTC.TOP	7	1,3
NovaBlock	5	0,93
EMCD.IO	4	0,75
Bitcoin.com	3	0,56
WAYI.CN	2	0,37

Для оценки вероятности формирования единой ЦБ $P_{ед}$ в ходе моделирования введем вероятностный показатель, учитывающий влияние выбора стратегий поведения автоматов, коэффициентов централизации системы и изменение времени задержки генерации блоков:

$$P_{ед} = 1 - P_{альт} = 1 - f(S_{МВ}, S_{ЦС}, S_{Т}) \quad (5)$$

где $P_{альт}$ – вероятность создания альтернативной ЦБ, $S_{МВ}$ – множество матриц состояний автоматов, $S_{ЦС}$ – множество коэффициентов централизации сети, $S_{Т}$ – множество вариантов времени задержки генерации блоков.

Стоит отметить, что имитационная модель не дает собственное решение, в отличие от аналитической, она лишь позволяет получить результат (выходные данные) на основании набора входных данных [6].

Программная реализация разработанной модели (Рисунки 4-6) будет основана на

алгоритмах, изображенных в виде структурных схем (Рисунок 1, 2) функционирования отдельного узла и DLT ЦБ системы, представляющих собой в совокупности логическую схему имитационной модели.

Для проведения эксперимента выбран метод сценарного планирования [7]. Под сценарием проведения эксперимента понимается последовательность событий, описывающая функционирование реальной DLT ЦБ системы. Рассмотрим следующие сценарии:

1) Штатное функционирование всех узлов DLT ЦБ системы в ходе выполнения алгоритма ВИС для оценки адекватности разработанной модели относительно реальной DLT ЦБ системы.
2) Попытка реализации атаки временной блокировки группой узлов в зависимости от централизации системы для оценки влияния централизации на вероятность реализации данной атаки.
3) Попытка формирования ответвления обрабатываемых данных группой узлов в зависимости от централизации системы для оценки влияния централизации на вероятность реализации данной атаки.
4) Попытка реализации одной группой ответвления обрабатываемых данных, а второй атаки временной блокировки для оценки влияния одновременной реализации нештатных функций на стабильность работы системы.

При формировании сценариев учитывались все возможные варианты реализации рассматриваемы нештатных функций. При этом сценарий 4 предполагает одновременную реализацию нештатных функций двух групп узлов, что является наихудшим условием функционирования DLT ЦБ системы.

Заключение

При разработке алгоритмов взаимного информационного согласования в системе распределенного реестра на базе цепочки блоков получены результаты:

1. Предложенный алгоритм функционирования узла системы учитывает возможность реализации нештатных функций: формирование ответвления обрабатываемых данных и атаку временной блокировки.
2. Обобщенный алгоритм функционирования системы распределенного реестра на базе цепочки блоков при достижении взаимного информационного согласования между узлами системы учитывает возможность объединения узлов в группы.
3. Проведено планирование численного эксперимента.

Дальнейшая работа будет заключаться в проведении численного эксперимента для оценки эффективности разработанного математического и программного обеспечения взаимного информационного согласования в системах распределенного реестра на основе цепочки блоков.

ЛИТЕРАТУРА

1. Nakamoto S. *Bitcoin: A Peer-to-Peer Electronic Cash System*. 2009. https://bitcoin.org/bitcoin.pdf.
2. Rosenfeld M. *Analysis of hashrate-based double-spending.* arXiv:1402.2009. 2014.
3. Pinzón C., Rocha C. Double-spend Attack Models with Time Advantange for Bitcoin. Electronic Notes in Theoretical Computer Science. 2016;329:79-103 https://doi.org/10.1016/j.entcs.2016.12.006.
4. https://bitinfocharts.com/ru/bitcoin
5. https://www.blockchain.com/charts/pools

6. Лычкина Н.Н. *Имитационное моделирование экономических процессов.* http://simulation.su/uploads/files/default/2005-uch-posob-lychkina-1.pdf
7. Бусленко В.Н. *Автоматизация имитационного моделирования сложных систем*. – М.: Наука, 1977.

REFERENCES

1. Nakamoto S. *Bitcoin: A Peer-to-Peer Electronic Cash System*. 2009. https://bitcoin.org/bitcoin.pdf.
2. Rosenfeld M. *Analysis of hashrate-based double-spending.* arXiv:1402.2009. 2014.
3. Pinzón C., Rocha C. Double-spend Attack Models with Time Advantange for Bitcoin. Electronic Notes in Theoretical Computer Science. 2016;329:79-103 https://doi.org/10.1016/j.entcs.2016.12.006.
4. https://bitinfocharts.com/ru/bitcoin
5. https://www.blockchain.com/charts/pools
6. Lychkina N.N. *Simulation of economic processes.* http://simulation.su/uploads/files/default/2005-uch-posob-lychkina-1.pdf
7. Buslenko V.N. *Automation of complex systems simulation*. – M.: Science, 1977.

ИНФОРМАЦИЯ ОБ АВТОРАХ / INFORMATION ABOUT THE AUTHORS

Еськов Станислав Сергеевич, соискатель, кафедра автоматизированных и вычислительных систем, Воронежский государственный технический университет, Воронеж, Российская Федерация.
e-mail: csit@bk.ru

Stanislav S. Yeskov, Applicant, Department of Automated and Computing Systems, Voronezh State Technical University, Voronezh, Russian Federation.

Кравец Олег Яковлевич, д.т.н., профессор, Воронежский государственный технический университет, кафедра автоматизированных и вычислительных систем, Воронежский государственный технический университет, Воронеж, Российская Федерация.
e-mail: csit@bk.ru
ORCID: 0000-0003-0420-6877

Oleg J. Kravets, Doctor of Technical Sciences, Professor, Voronezh State Technical University, Department of Automated and Computing Systems, Voronezh State Technical University, Voronezh, Russian Federation.