Андрей И. Терентьев
Московский государственный технический университет гражданской авиации,
Кронштадтский б–р, 20, Москва, 125993, Россия
e-mail: terentyev-doc@yandex.ru, http://orcid.org/0000-0002-0493-3161

КОНЦЕПТУАЛЬНАЯ СХЕМА (ПАРАДИГМА) ТЕХНОЛОГИИ СВЯЗНЫХ ДАННЫХ

DOI: http://dx.doi.org/10.26583/bit.2021.3.05

Аннотация. В статье предложена концептуальная схема (парадигма) практических взглядов и подходов в отношении технологии связных математическим, криптографическим и иным способом данных, рассматриваемых с позиции математики как некоторое множество *M*, элементами которого могут являться множества, а также конструктивные, гибридные и иные объекты, включающие, в том числе, информационную и служебную составляющие. Вводятся понятия связного множества, размерности его структуры и силы установленной связи. Утверждается, что потенциал практического применения различных систем связных данных, особенно нетрадиционно организованных структур многомерно связных данных, гораздо выше, чем это представляется в настоящее время. В качестве примера предложены двумерная структура множества *M* в виде цилиндрической трубы (линейно-кольцевая структура) и трехмерная структура в ортогональном базисе в виде куба (параллелепипеда), которые могут иметь перспективы практического использования в различных проектах цифровой экономики, где данные используются одновременно в нескольких процессах.

Ключевые слова: технологии связных данных, технологии блокчейна, связное множество, структура связного множества, размерность структуры связного множества, сила связи элементов связного множества.

Для цитирования: ТЕРЕНТЬЕВ, Андрей И. КОНЦЕПТУАЛЬНАЯ СХЕМА (ПАРАДИГМА) ТЕХНОЛОГИИ СВЯЗНЫХ ДАННЫХ. Безопасность информационных технологий, [S.l.], т. 28, № 3, с. 65–72, 2021. ISSN 2074-7136. URL: https://bit.mephi.ru/index.php/bit/article/view/1363. DOI: http://dx.doi.org/10.26583/bit.2021.3.05.

Andrey I. Terentyev
The Moscow State Technical University of Civil Aviation (MSTUCA),
Kronshtadtskiy bulvar, 20, Moscow, 125993, Russia
e-mail: terentyev-doc@yandex.ru, http://orcid.org/0000-0002-0493-3161

Conceptual scheme (paradigm) of connected data technologies

DOI: http://dx.doi.org/10.26583/bit.2021.3.05

Abstract. The paper proposes to consider blockchain technology as one of the possible technologies aimed at ensuring the integrity, availability and reliability of various data sets. In order to streamline the directions of research of such technologies, the paper proposes an initial conceptual scheme (paradigm) of practical views and approaches in relation to the technology of mathematically, cryptographically and otherwise connected data, considered from the standpoint of mathematics as a set M, the elements of which can be sets, as well as constructive, hybrid and other objects, including, inter alia, information and service components. The concepts of a connected set, the dimensions of its structure and the strength of the established connection are introduced. It is argued that the potential for practical application of various systems of connected data, especially unconventionally organized structures of multidimensionally connected data, is much higher than it seems at present. As an example, a two-dimensional structure of the set M in the form of a cylindrical pipe (linear-ring structure) is proposed, as well as a three-dimensional structure in an orthogonal basis in the form of a cube (parallelepiped), which may have prospects for practical applications in various projects of digital economy where data is used simultaneously in several processes.

Keywords: connected data technologies, blockchain technology, connected set, structure of a connected set, dimension of the structure of a connected set, strength of connection of elements of a connected set.
For citation: TERENTYEV, Andrey I. Conceptual scheme (paradigm) of connected data technologies. IT Security (Russia), [S.l.], v. 28, n. 3, p. 65–72, 2021. ISSN 2074-7136. URL: https://bit.mephi.ru/index.php/bit/article/view/1363. DOI: http://dx.doi.org/10.26583/bit.2021.3.05.

Введение

В настоящее время научным и профессиональным сообществом достаточно широко и в ряде случаев эмоционально обсуждаются проблемы эффективности, потенциальных возможностей и границ применимости популярной технологии блокчейн (blockchain), поскольку с каждым годом становится все более очевидным, что она во многом не оправдывает возлагаемых на нее обществом завышенных ожиданий, несмотря на отдельные примеры ее успешного использования. При этом суть самой технологии не нова. Можно привести исторические примеры более двухтысячелетнего использования идеи передачи наследуемых признаков или свойств вновь создаваемым объектам или сущностям для обеспечения их аутентичности, которые применяются по сей день.

Широкий спектр мнений о рыночных и социальных перспективах распространения и внедрения технологии блокчейн изложен в [1–3]. Конкретные вопросы его практического применения и стандартизации рассмотрены в [4] и приведены основные первоисточники и наиболее часто цитируемые определения технологии блокчейн, из которых следует, что в настоящее время понятие технологии блокчейн устойчиво связано с одновременным использованием технологии распределенного реестра и специальной криптографической процедуры, основанной на свойствах функции хэширования и древовидном способе хэширования данных, посредством которой обеспечивается связь блоков данных, входящих в формируемую и постоянно удлиняющуюся рекуррентную последовательность (цепь). Кроме этого, в [4] аргументированно отмечается, что остается еще много нерешенных вопросов в области унификации и реализации технологии блокчейн. Характерные примеры критического отношения к завышенным ожиданиям, связанным с этой технологией приведены в [5–6]. К этому следует добавить, что на практике часто происходит смешение или отождествление технологии блокчейн с другими сопоставимыми методиками, процессами и технологиями, которые также направлены на обеспечение целостности, доступности и достоверности различных массивов данных, но основаны на иных принципах обеспечения их связанности. При этом все подобные технологии призваны способствовать формированию высокого уровня доверия у потенциальных пользователей к использующим их прикладным системам, что в условиях тотальной цифровизации и сопутствующего ей взрывного роста количества киберпреступлений очень востребовано обществом. Это в свою очередь побуждает разработчиков-практиков предлагать различные пути решения этой проблемы. Однако в области теории какого-либо единого базиса для описания и исследования технологий связных данных не существует.

1. Исходная концептуальная схема (парадигма) технологии связных данных

Учитывая изложенное, автор предпринял попытку сформировать некую исходную концептуальную схему практических взглядов и подходов в отношении технологии связных[1] тем или иным способом данных, которая могла бы дать повод для дальнейшей

[1]Термин «связный» применяется в отношении совокупности элементов (множества) и употребляется в значении, которое используется в математике и основывается, в том числе на его толковании в русском языке следующим образом: хорошо и последовательно организованный, логически стройный. Его не следует путать со словом «связанный», которое имеет другие значение. При этом, рассматривая

научно-практической дискуссии. Приводимые далее утверждения достаточно очевидны и не требуют доказательства. При необходимости они могут быть доказаны, однако это выходит за рамки настоящей статьи. К используемым в статье элементам дискретной математики можно обратиться, в том числе, в классических работах [7–9] и более современных источниках, например, [10]. Предлагаемые ниже постулаты и суждения упорядочены согласно авторскому представлению об их логической взаимосвязи и последовательности:

1. Любые данные или наборы данных (далее – данные) могут быть тем или иным способом представлены и идентифицированы. При этом для конкретной практической задачи всегда существует способ их идентификации, при котором идентификаторы не будут совпадать (повторяться).

2. Любые данные, в том числе идентифицированные, могут быть тем или иным способом представлены как элементы некоторого множества M, которое может быть задано посредством перечисления всех его элементов: $M = \{m_1, m_2, ..., m_k\}$, или посредством указания порождающей процедуры (алгоритма) или свойства, на основании которого они принадлежат этому множеству: $M = \{m|P(m)\}$. При этом следует учитывать, что элементами множества могут являться множества, а также конструктивные, гибридные и иные сложно структурированные объекты, включающие, в том числе, информационную и служебную составляющие.

3. Множество M будем считать связным, если на нем установлено бинарное или иное отношение R, обладающее свойством связности (на других свойствах, в том числе рефлективности, симметричности и транзитивности, пока останавливаться не будем). Соответственно данные, которые представляются элементами такого множества, будут являться в той или иной степени связанными между собой.

4. Свойство (порождающая процедура, функция, алгоритм), посредством которого устанавливается взаимосвязь между элементами множества и обеспечивается его связность, может быть любой природы, в зависимости от решаемой научной или практической задачи. Например, природа свойства (порождающей процедуры, функции, алгоритма), обеспечивающего связность, может быть:

- математической (числовой, логической, аналитической и т.п.);
- криптографической;
- семантической;
- визуально-смысловой;
- лексикографической;
- табличной;
- комбинированной и иной[2].

5. На связном множестве M может быть установлено отношение порядка, при котором нумерация (индексирование) его элементов будет не случайной (будет носить регулярный характер).

Таким образом возможно последовательное порождение всех элементов множества M, которое будет являться перечислимым и разрешимым. Это позволяет, в том числе, проверить для любого элемента такого множества актуальность свойства связности, т.е.

особенности и взаимосвязь отдельных, например, двух конкретных элементов множества, находящихся в каком-либо отношении, можно использовать термины «связь», «связаны» и т.п.

[2]В технологии блокчейн использована криптографическая порождающая процедура на базе хэш-функции. В качестве одной из основ для математической порождающей процедуры могут, по мнению автора, эффективно использоваться числовые линейные блоковые корректирующие коды над кольцом конечных десятичных дробей [11].

выполнение порождающей процедуры (функции, алгоритма) и наличие установленной ею связи с любым другим элементом этого множества. Если результат проверки отрицательный, то считается, что рассматриваемый элемент множеству M не принадлежит.

6. Установление связности элементов множества, а также отношение порядка, задаваемое на множестве, должны иметь здравый смысл и конкретную цель, обусловленные решаемой научной или практической задачей. При этом основная цель обеспечения связности – это существенное затруднение или исключение возможности бесконтрольного или нештатного изменения (модификации) таких структур и их элементов. Иные задачи, в том числе, направленные на обеспечение приватности, анонимности, репликации, децентрализации, производительности, масштабируемости и т.п., решаются посредством применения других методов и технологий.

7. Установление связности элементов и отношения порядка на множестве (совокупности множеств) может быть линейным или нелинейным, односвязным или многосвязным, а также n-мерным (многомерным), что определяет структуру множества M. В случае многомерности ($n \geq 2$) такое множество уместно называть системой связных множеств (подмножеств). Примером одномерной ($n = 1$) структуры может являться последовательность или кольцо, двумерной ($n = 2$) – таблица или матрица (в ортогональном базисе), а также труба или объекты спирально-винтового типа. Простейшим примером трехмерной ($n = 3$) структуры множества M является куб или параллелепипед (в ортогональном базисе).

8. Результирующая сила S установленной связи (т.е. условная стойкость к ее изменению или нарушению) зависит от сложности T порождающей процедуры, p – глубины рекурсии, n-мерности структуры множества M и мощности множества M:

$$S = \partial\,(T, p, n, |M|),$$

где ∂ – функция соответствующих аргументов.

Интуитивно понятно, чем алгоритмически сложнее порождающая процедура и глубже рекурсия, тем больше элементов множества M будут вовлечены в установление такой связи и тем больше результирующая сила связи между элементами связного множества, полученного в результате этой процедуры. Соответственно, чем больше n, тем больше у каждого элемента множества M соседних (т.е. окружающих его) элементов, которые могут быть задействованы в установление связи. При больших значениях p, n и $|M|$ (где $|M|$ – мощность множества M) изменение установленного ранее порядка или замена (модификация) элемента, с сохранением связности множества M, может является трудновыполнимой задачей, а при $n > \mu$ эта задача может быть теоретически не выполнимой (где μ – некоторое пороговое значение, сложным образом зависящее от мощности множества M, алгоритмической сложности T порождающей процедуры и глубины рекурсии p).

В общем случае, когда элемент m_i множества M не является первым или последним, минимальное количество связей h_{min} элемента m_i определяется количеством соседних с ним элементов и зависит от размерности n множества M следующим образом: $h_{min} = 2n$. Например, в случае одномерной структуры множества M (т.е. при $n = 1$) соседними элементами с m_i являются m_{i-1} и m_{i+1}, а $h_{min} = 2$.

Максимально возможное количество связей h_{max} элемента m_i множества M с другими элементами этого множества зависит не только от размерности n множества M, но и от используемой порождающей такое связное множество процедуры, в том числе глубины рекурсии. Предельное значение h_{max} определяется следующим образом: $h_{max} = |M|–1$.

9. Отношение порядка может устанавливаться тем или иным способом, в том числе рекуррентным.

Если отношение порядка установлено рекуррентным способом, то при $n = 1$ множество M можно рассматривать как рекуррентную последовательность, в которой для любой пары элементов будет выполняться отношение строго порядка $m_i R m_j$, а для каждой пары соседних элементов (m_{i-1}, m_i) или (m_i, m_{i+1}) рекуррентной последовательности будет выполняться отношение доминирования $m_{i-1} R m_i$ и $m_i R m_{i+1}$. Абстрактное графическое представление такой последовательности в ортогональном базисе приведено на рис. 1.

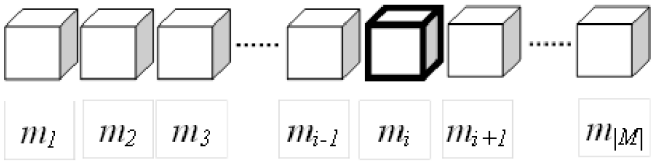

Рис. 1. Абстрактное графическое представление рекуррентной последовательности (n=1)
Fig. 1. Abstract graphical representation of a recurrent sequence (n=1)

Формулу общего члена рекуррентной последовательности можно представить следующим образом:

$$m_i = f(i, m_{i-1}, m_{i-2}, \ldots, m_{i-p}),$$

где f – порождающая процедура, функция или алгоритм формирования членов последовательности; m_i – i-ый или общий член последовательности, а i – порядковый номер (индекс), $i \in N$ (N – множество натуральных чисел); p – ранг рекуррентной последовательности (количество предыдущих членов последовательности, участвующих в формировании текущего члена последовательности).

По принципу образования элементов это рекуррентная последовательность, а, по сути, полученная таким образом вся совокупность элементов – это связное перечислимое разрешимое и упорядоченное множество, допускающее, при необходимости, дополнение его новыми элементами.

10. Любые данные могут быть тем или иным способом представлены в виде наборов чисел или одного числа. Если средством обработки таких данных является электронное техническое устройство (электронная вычислительная машина), то соответствующие числа или число будут являться элементами кольца конечных десятичных дробей D.

2. Примеры нетрадиционно организованных структур связных данных

Абстрактное графическое представление двухмерной структуры ($n = 2$) связного множества M в виде таблицы или матрицы достаточно тривиально. Характерной особенностью такой прямоугольной структуры является то, что составляющие ее линейные подмножества, ориентированные по строкам и столбцам, могут являться постоянно растущими последовательностями (цепями). Существенно больший интерес для исследования вызывают нетрадиционно организованные структуры связных данных. В связи с этим автором предлагается к рассмотрению двумерная структура в виде цилиндрической трубы (линейно-кольцевая структура), которая приведена на рис. 2. Преимущества и перспективы практического использования такой структуры в большей степени связаны с процессами, которые носят цикличный характер. Например, в часе

60 минут, в сутках 24 часа, в году 12 месяцев. В связи с этим кольцевая структура органично подходит для создания связного множества цифровых данных, отражающих события (факты, соглашения, транзакции), произошедшие, например, за текущие сутки, а линейная связь одноименных (имеющих одинаковые индексы) элементов из каждого кольца в постоянно растущую последовательность (цепь) позволяет сформировать защищенное от модификации множество цифровых данных, отражающих события в конкретным момент времени суток, но произошедшие в течение какого-либо более продолжительного временного периода, например, недели, месяца или года. При этом линейный рост соответствующих последовательностей (цепей) не ограничен, а новые кольца по мере их формирования «нанизываются» на трубу.

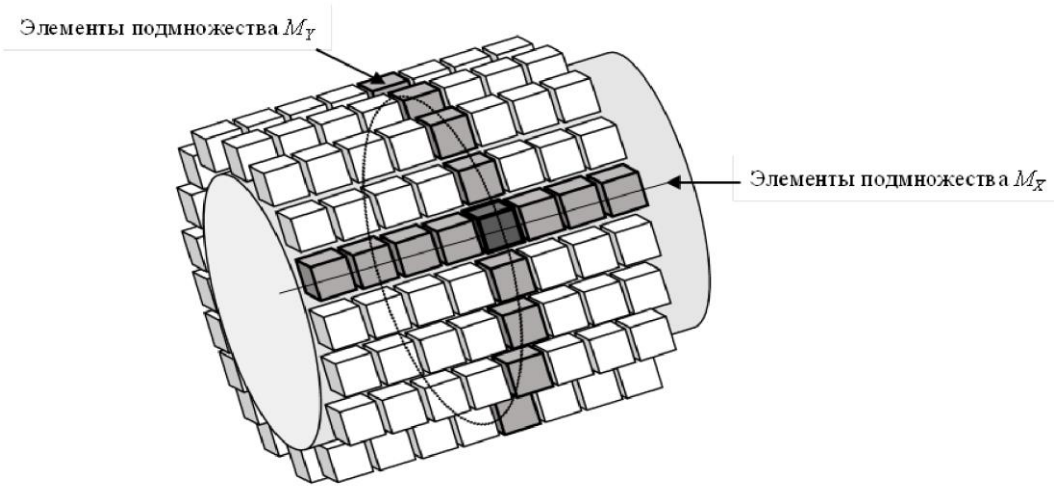

Рис. 2. Абстрактное графическое представление двухмерной структуры (n = 2) связного множества M в виде цилиндрической трубы
Fig. 2. Abstract graphical representation of a two-dimensional structure (n = 2) of a connected set M in the form of a cylindrical tube

Следует отметить, что порождающая процедура (функция, алгоритм), посредством которой будет устанавливаться взаимосвязь между элементами кольцевого и линейного подмножеств с целью обеспечения их связности, может быть любой природы, что зависит от решаемой практической задачи. Если за основу взята технология блокчейн, то порождающая процедура, обеспечивающая связность каждого из подмножеств, в силу использования функции хэширования, будет являться (согласно предложенной в п. 4 классификации) криптографической. В случае использования иных принципов обеспечения взаимосвязи между элементами подмножеств, например, посредством их кодирования числовым линейным блоковым корректирующим кодом [11], порождающая процедура (по предложенной в п. 4 классификации) будет математической. Также может использоваться комбинированная порождающая процедура, сочетающая в себе различные принципы обеспечения связности подмножеств.

Абстрактное графическое представление трехмерной структуры ($n = 3$) множества M в ортогональном базисе в виде куба приведено на рис. 3. Поскольку каждый элемент таким образом организованного связного множества одновременно входит в каждое из составляющих его связных подмножеств M_x, M_y и M_z, то результирующая сила установленной связи S, а следовательно и стойкость связного множества к модификации, будет (при прочих равных условиях) выше, чем в любой двумерной структуре.

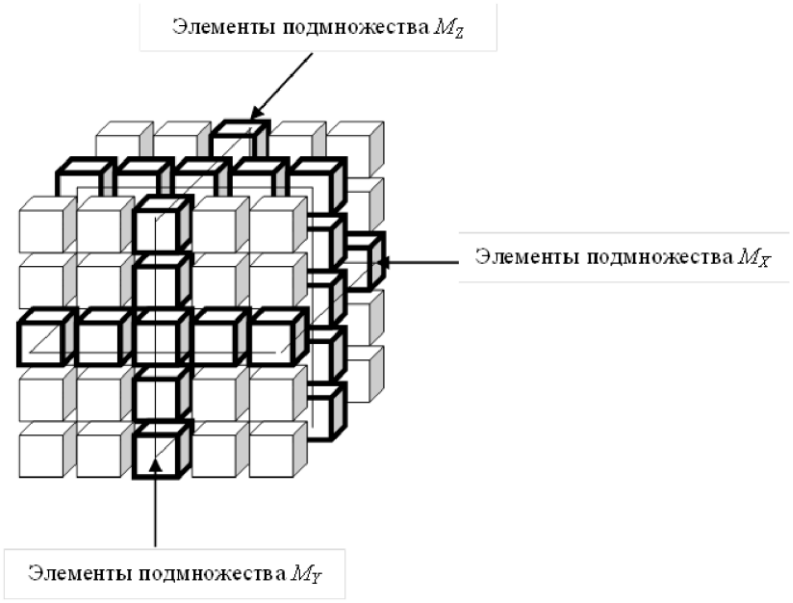

Рис. 3. Абстрактное графическое представление трехмерной структуры (n = 3) связного множества M в виде куба
Fig. 3. Abstract graphical representation of the three-dimensional structure (n = 3) of a connected set M in the form of a cube

Заключение

С потребительской точки зрения организованные подобным образом связные множества являются источниками той или иной информации, необходимой пользователю в конкретный момент времени, т.е. информационными системами, базами или массивами данных. Основное требование, которое к ним предъявляется пользователем – соответствие заявленным характеристикам, в том числе связанным с их целостностью и достоверностью.

Общественная и научная дискуссии в отношении специфики использования связных данных ведутся, в основном, применительно к системам, основанным на технологии блокчейн (функции хэширования) и имеющим одномерную структуру. Однако потенциал применения различных систем связных данных может быть выше в случае построения многомерных структур, а также использования отличных от технологии блокчейн (альтернативных) порождающих процедур, например, основанных на числовом помехоустойчивом кодировании блоков данных. В ближайшем будущем они могут быть востребованы в различных областях и проектах цифровой экономики, особенно в тех, где данные используются одновременно в нескольких процессах. Однако это требует дополнительных исследований, которые в настоящее время ведутся автором.

СПИСОК ЛИТЕРАТУРЫ:

1. Генкин А., Михеев А. Блокчейн: Как это работает и что ждет нас завтра. М.: Альпина Паблишер, 2018. – 592 с.
2. Дон Тапскотт, Алекс Тапскотт. Технология блокчейн: то, что движет финансовой революцией сегодня / [пер. с англ. К. Шашковой, Е. Ряхиной]. М.: Эксмо, 2018. – 443 с.
3. Шваб, Клаус. Технологии Четвертой промышленной революции: [перевод с английского]. М.: Эксмо, 2018. – 320 с.
4. Будзко, Владимир И.; Милославская, Наталья Г. Вопросы практического применения технологии блокчейна. Безопасность информационных технологий, [S.l]. Т. 26, № 1. С. 36–45, 2019. ISSN 2074-

7136. URL: https://bit.mephi.ru/index.php/bit/article/view/1178 (дата обращения: 19.02.2021). DOI: http://dx.doi.org/10.26583/bit.2019.1.04.
5. Колодзей А. Ключ к паутине. Перспективы использования блокчейн-технологий в цифровом государстве // BIS JOURNAL. 2019, № 1. С. 106–111. URL: https://ib-bank.ru/bisjournal/number_pdf/61 (дата обращения: 19.04.2021).
6. Катанкина А. Аргументы против фактов. Удачный маркетинговый ход или экономически успешная стратегия? // BIS JOURNAL. 2019, № 1. С. 112–113. URL: https://ib-bank.ru/bisjournal/number_pdf/61 (дата обращения: 19.04.2021).
7. Б.Л. ван дер Варден. Алгебра: Пер. с нем. М.: Наука, 1979. – 624 с.
8. Кузнецов О.П., Адельсон-Вельский Г.М. Дискретная математика для инженера. – 2-е изд., перераб. и доп. М.: Энергоатомиздат, 1988. – 480 с.
9. Горбатов В.А. Фундаментальные основы дискретной математики. Информационная математика. М.: Наука. Физматлит, 1999. – 544 с.
10. Андерсон, Джеймс А. Дискретная математика и комбинаторика: Пер. с англ. М.: Издательский дом «Вильямс», 2003. – 960 с.
11. Терентьев А.И. Элементы теории и практики числовых линейных блоковых корректирующих кодов. М.: Альтекс, 2000. – 204 с.

REFERENCES:

[1] Genkin A., Mikheev A. Blockchain: How it works and what awaits us tomorrow. M.: Alpina Publisher, 2018. – 592 p. (in Russian).
[2] Don Tapscott, Alex Tapscott. Blockchain Revolution: How the Technology Behind Bitcoin and Other Cryptocurrencies is Changing the World. M.: Eksmo, 2018. – 443 p. (in Russian).
[3] Klaus Schwab. Shaping the Fourth Industrial Revolution. M.: Eksmo, 2018. –320 p. (in Russian).
[4] Budzko, Vladimir I.; Miloslavskaya, Natalia G. Issues of Practical Application of Blockchain Technology. IT Security (Russia), [S.l]. Vol. 26. No. 1. P. 36–45, 2019. ISSN 2074-7136. URL: https://bit.mephi.ru/index.php/bit/article/view/1178 (accessed: 19.02.2021). DOI: http://dx.doi.org/10.26583/bit.2019.1.04 (in Russian).
[5] Colodzey A. The key to the web. Prospects for the use of blockchain technologies in the digital state. BIS JOURNAL. 2019. No. 1. P. 106–111. URL: https://ib-bank.ru/bisjournal/number_pdf/61 (accessed: 19.04.2021) (in Russian).
[6] Catankina A. Arguments against facts. Marketing Success or Economically Successful Strategy? BIS JOURNAL. 2019. No. 1. P. 112–113. URL: https://ib-bank.ru/bisjournal/number_pdf/61 (accessed: 19.04.2021) (in Russian).
[7] B.L. Van Der Waerden. Algebra. Springer-Verlag. Berlin. Heidelberg. New York. 1971 (in Russian).
[8] Kuznetsov O.P., Adelson-Velsky G.M. Discrete math for an engineer. – 2nd ed. M.: Energoatomizdat, 1988. – 480 p. (in Russian).
[9] Gorbatov V.A. Fundamentals of discrete mathematics. Information mathematics. M.: Science. Fizmatliit, 1999. – 544 p. (in Russian).
[10] James A. Anderson. Discrete Mathematics with Combinatorics. M.: Publishing house «Williams», 2003. – 960 p. (in Russian).
[11] Terentyev A.I. Elements of the theory and practice of numeric linear block error-correcting codes. M.: Alteks, 2000. – 204 p. (in Russian).

Поступила в редакцию – 20 апреля 2021 г. Окончательный вариант – 20 августа 2021г.
Received – April 20, 2021. The final version – August 20, 2021.