УДК 004.021: 004.312.4: 004.414.2

ПРИМЕНЕНИЕ КОМПОНЕНТНЫХ СЕТЕЙ ПЕТРИ В ЗАДАЧАХ ВЕРИФИКАЦИИ ПАРАЛЛЕЛЬНЫХ РАСПРЕДЕЛЁННЫХ СИСТЕМ

Е.А. Лукьянова

Таврический национальный университет имени В.И. Вернадского,
факультет математики и информатики, проспект Вернадского, 4.
E-mail: lukyanovaea@mail.ru

В работе рассмотрены модели Крипке двух математических моделей параллельных распределённых систем, представленных детальной и её компонентной сетями Петри. Показана бисимулярность этих моделей Крипке. Установлены возможности проверки истинности логической формулы темпоральной логики, которой задаётся требуемое свойство исследуемой параллельной распределённой системы, с помощью редуцированной модели Крипке компонентной сети Петри.

The paper discusses the Kripke structures of two mathematical models of parallel distributed systems that are presented by Petri detailed net and its component net. Bisimularity of these Kripke structures is displayed. The possibility for checking the validity of the logical formula of temporal logic is established, which gives the desired property of investigated parallel distributed system, using reduced Kripke structure of component Petri net.

Введение

Параллельные распределённые системы представляют собой сложные вычислительные системы, в которых выполняется параллельная обработка данных несколькими различными машинами системы, подключенными к локальной или глобальной сети, при возможности, как синхронного, так и асинхронного управления. Такие системы обладают недетерминированностью и характеризуются множеством взаимодействующих друг с другом процессов, результативно использующих все ресурсы сети. При этом сеть поддерживает функционирование системы как единого целого, а каждая машина системы выполняет своё задание – часть функций глобальной сети. Параллельные распределённые системы могут быть физическими, компьютерными или программными системами. В настоящее время дальнейшее перспективное развитие вычислительной техники на прямую связано с применением параллельных вычислительных систем, что в свою очередь обуславливает необходимость создания и использования новых или «модернизированных» моделей и методов параллельных вычислений и их реализаций, а так же разработки новых технологий проектирования параллельных распределённых систем. При этом приходится решать задачи, связанные с согласованностью результатов моделирования с возможной дальнейшей верификацией и адекватностью полученных результатов для анализа соответствующих исследуемых свойств исходной изучаемой задачи.

Теория параллельных систем и процессов имеет в своём арсенале достаточное количество разнообразных моделей, алгоритмов и инструментов, которые могут быть использованы при моделировании, разработке и верификации параллельных распределенных систем. Применяются структурные [1–3] и семантические [4–6] формальные модели, позволяющие эффективно анализировать функциональные особенности, структурные и поведенческие свойства систем с параллелизмом. Используются алгебры [7, 8] и логики процессов, соответственно позволяющие представлять и изучать параллельные системы как элементы алгебры, разрабатывать методы и способы спецификации и верификации параллельных процессов, используя различные логические языки, например, аппараты логических языков темпоральных логик *LTL*, *CTL*, *CTL**.

Изучаемые классы моделей характеризуются своей степенью выразительности и алгоритмической разрешимости, а, значит, выбор используемого способа моделирования изучаемой системы имеет важное определяющее значение. На сегодняшний день общепризнанно, что наилучшим формализмом, представляющим параллелизм в сложных реальных системах, является формализм сетей Петри. Применение современных моделей Петри, изучение их языков позволяет устанавливать как структурные, так и поведенческие свойства моделей, устанавливать взаимосвязи между моделями, используя различные поведенческие эквивалентности, например, применяя языковую, симуляционную, бисимуляционную эквивалентности. Это позволяет использовать высокую степень выразительности формализма сетей Петри с дальнейшими возможными преобразованиями исходных моделей для получения адекватных моделей размеры, которых позволяли бы производить их продуктивный анализ. В этом направлении в работах [9, 10] предложено использование компонентной модели Петри (*CN*-сети), применение которой для моделирования систем с параллелизмом позволяет получать редуцированные *CN*-модели (модели значительно меньших размеров относительно исходной детальной модели N). При этом имеют место бисимуляционная эквивалентность [11] компонентной сети Петри (*CN*-сети) исходной детальной модели Петри N исследуемой параллельной распределённой системы, эпиморфизм этих моделей [12] и их языков [13–15].

1. Цель и задачи исследования

В настоящей работе будут рассмотрены возможности использования, имеющихся результатов компонентного моделирования и инструментов компонентного анализа для верификации параллельных распределённых систем путём использования алгоритмического подхода, основанного на применении алгоритмов проверки на модели (*model checking*) [16]. Алгоритмы верификации на модели с использованием логики ветвящегося времени (*CTL – Computation Tree Logic*) [17] являются эффективными инструментами анализа последовательностей состояний в исследуемых системах, объединяющими традиционные и логические методы анализа, где свойство системы задается в виде логической формулы, истинность которой проверяется на модели Крипке, представляющей поведение системы. При этом необходимо уметь преодолевать проблему верификации реальных систем – анализ огромного числа состояний.

Цель работы: установить, что отношение бисимуляции для детальной и компонентной моделей сохраняет выполнимость формул логики *CTL*, что позволит проводить проверку спецификации (формализованного в виде логической формулы проверяемого свойства исследуемой системы) на семантической модели Крипке редуцированной сети – *CN*-сети.

Для этого в работе выполнены следующие шаги:

1) осуществлён переход от моделей Петри (двудольных графов) сетей N и *CN* к их соответствующим моделям Крипке (графам с одним типом вершин), на которых интерпретируется логика *CTL*;

2) выяснена бисимуляционная эквивалентность полученных моделей Крипке;

3) определено, каким образом устанавливать выполнимость формулой *CTL* логики на модели Крипке детальной модели Петри по выполнимости соответствующих формул *CTL* логики на модели Крипке компонентной модели Петри.

Таким образом, основная задача – показать, что применение компонентной сети Петри, позволяющей выражать в достаточно компактном виде сложные системы с параллелизмом, может быть использовано и при верификации таких систем с использованием метода проверки на модели.

2. Модель Крипке для сетей Петри, моделирующих системы с параллельными процессами, с использованием компонентного моделирования

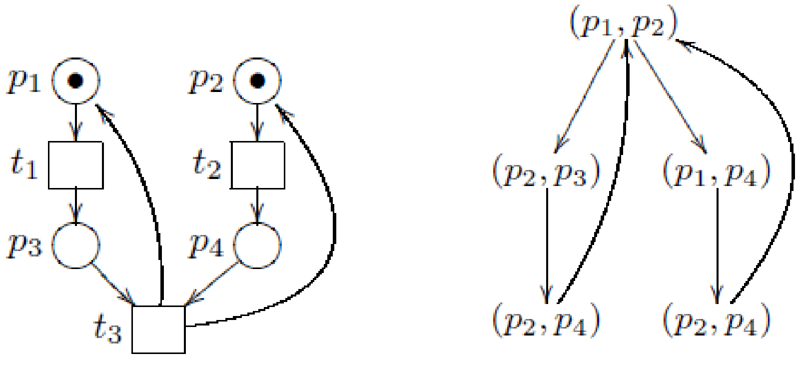
Для исследуемой системы с параллельными процессами строится её формальная модель в виде детальной сети Петри. Полученная сеть исследуется на наличие составных компонент [9, 18] (компонент-мест C_p и компонент-переходов C_t). Результат – выделение в детальной модели Петри N составных компонент, в частности, наличие параллельных процессов обязательно обеспечит возможность выделения в детальной сети составных компонент, при этом, в случае параллельных процессов, это могут быть либо одинаковые, либо однотипные составные компоненты [19]. Таким образом, будет получена ещё одна формальная модель исходной исследуемой системы – компонентная сеть Петри *CN*, которая эпиморфна исходной детальной модели N [12].

Модель Крипке – это структура, отражающая достижимые в системе состояния, а это означает, что модель Крипке для сети Петри будет представляться графом достижимых в сети разметок. Такая модель достаточно выразительно представляет параллелизм – функционирование параллельных процессов (их поведение и взаимодействие).

Имея две адекватные модели исследуемой системы (сети N и *CN*) построим для каждой её модель Крипке.

Рассмотрим несколько примеров.

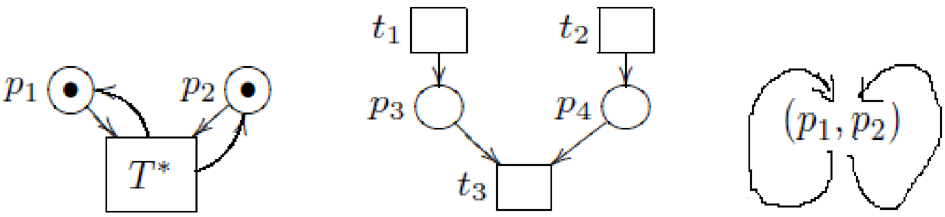
На рис. 1, а показана небольшая сеть Петри, моделирующая функционирование двух синхронизируемых параллельных процессов, на рис. 1, б – её модель Крипке.



а б

Рис. 1. а – детальная сеть Петри, синхронизирующая два параллельных процесса;
б – её модель Крипке

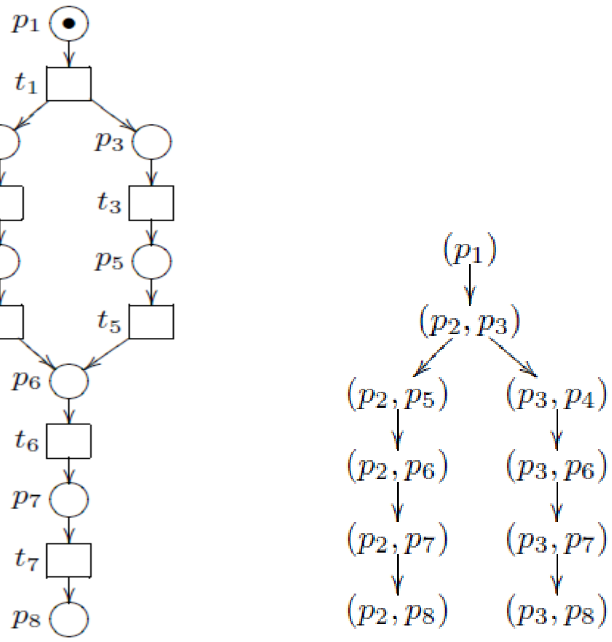
В рассматриваемой детальной сети Петри можно выделить одну составную компоненту – компоненту-переход, в которую практически полностью оформляются рассматриваемые два параллельных процесса и в которой происходит их синхронизация. На рис. 2, а, в соответственно показаны компонентная сеть Петри, отвечающая исходной детальной сети Петри с рис. 1, а, и её модель Крипке. Эта компонентная сеть содержит составную компоненту – компоненту-переход T^*, показанную на рис. 2, б.



а б в

Рис. 2. а – компонентная сеть Петри для сети Петри с рис. 1, а; б – её компонента-переход T^*;
в – её модель Крипке

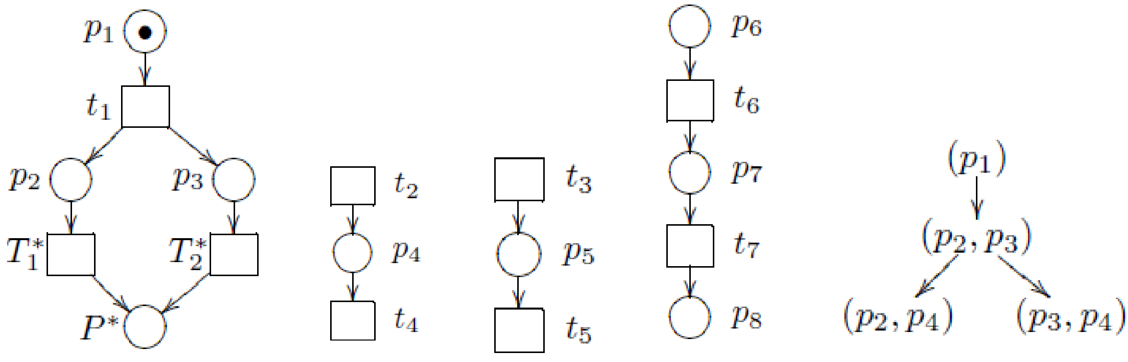
На рис. 3, а показана детальная сеть Петри из [15], синтезирующая два параллельных процесса. Данная сеть, хотя является и небольшой, её модель Крипке, отражающая достижимые состояния, для показа в работе достаточно громоздкая. Покажем её основной участок (рис. 3, б), который непосредственно и отражает синтез независимо функционирующих параллельных процессов. Остальные состояния, не являющиеся существенными характеристиками сети, из рассмотрения можно исключить в связи с тем, что рассматриваемые параллельные процессы функционируют самостоятельно (независимо друг от друга) и не синхронизируются, поэтому эти исключённые состояния являются «шумом» и только утяжеляют восприятие.



а б

Рис. 3. а – детальная сеть Петри, синтезирующая два параллельных процесса;
б – участок её модели Крипке, отражающий синтез независимо
функционирующих параллельных процессов

В детальной сети Петри с рис. 3, а могут быть выделены составные компоненты несколькими вариантами, например, могут быть выделены три компоненты-места, две из которых будут одинаковыми, или могут быть выделены три одинаковые компоненты-переходы. Приведём вариант, когда в рассматриваемой детальной сети Петри будут выделены и компоненты-места и компоненты-переходы. Для этого варианта на рис. 4 а, д, соответственно показаны компонентная сеть Петри и её модель Крипке. Предложенная компонентная сеть содержит одинаковые компоненты-переходы T_1^*, T_2^*, показанные соответственно на рис. 4, б, в и компоненту-место P^*, показанную на рис. 4, г.



а б в г д

Рис. 4. а – компонентная сеть Петри для сети Петри с рис. 3, а; б, в – её компоненты-переходы T_1^* и T_2^* соответственно; г – её компонента-место P^*; д – её модель Крипке

В работе [11] установлена эквивалентность в функционировании детельной N и компонентной *CN* сетей Петри на уровне бисимуляционной эквивалентности. Бисимуляция сетей N и *CN* доказана на основании гомоморфизма графов достижимых разметок сетей N и *CN*, обоснованного с помощью отношения компоненты χ_1, введённого на множестве вершин графа достижимых разметок сети N. Установленная бисимуляция рассматривалась как отношение, задаваемое на множестве вершин, объединения графов достижимых разметок, сетей N и *CN*. Учитывая вышесказанное и то, что модель Крипке для сети Петри представляется графом достижимых в сети разметок, получаем, что между вершинами моделей Крипке детальной и её компонентной сетей Петри имеется симметричное отношение R – бисимуляция, при котором для каждой пары $(a_1, a_2) \in R$ (где a_1 и a_2 – соответственно вершины моделей Крипке сети N и сети *CN*) выполняется следующее условие:

если $a_1 \xrightarrow{\mu} a'_1$ (для некоторого действия μ и вершины a'_1 модели Крипке сети N), то существует вершина a'_2 модели Крипке сети *CN*, такая, что $a_2 \xrightarrow{\mu^*} a'_2$ и $(a'_1, a'_2) \in R$.

Действие μ^* определяется из следующих знакосочетаний:

1) на множестве вершин некоторой модели Крипке определим знакосочетание $a \xrightarrow{\mu} a'$, где a, a' – вершины модели Крипке, μ – ребро из a в a';

2) $a_1 \xrightarrow{\tau^*} a_2$, когда либо $a_1 = a_2$, либо в модели Крипке есть путь из a_1 в a_2 с рёбрами, помеченными τ;

3) $a_1 \xrightarrow{\mu^*} a_2$, когда либо $\mu = \tau$ и $a_1 = a_2$, либо $a_1 \xrightarrow{\tau^*} a'_1 \xrightarrow{\mu} a'_2 \xrightarrow{\tau^*} a_2$, где a'_1, a'_2 некоторые вершины модели Крипке.

Таким образом, модель Крипке компонентной сети *CN* бисимулярна модели Крипке соответствующей исходной детальной сети Петри N, значит, имеет место корректная редукция модели Крипке исходной детальной сети Петри исследуемой системы. Эта редукция заключается в том, что редуцированная модель Крипке имеет меньшее количество состояний и может быть получена как модель Крипке компонентной сети Петри исходной детальной сети Петри N, в которой предварительно выделяются составные компоненты (компоненты-места C_p и компоненты-переходы C_t).

3. Модель Крипке компонентной сети Петри как модель её детальной сети Петри

Формальная модель исследуемой системы представлена двумя её моделями: детальной сетью Петри N и её редуцированной компонентной сетью Петри *CN*. Построенные соответствующие для сетей N и *CN* модели Крипке обозначим соответственно K_N и K_{CN}. Модель Крипке выступает в качестве подробной схемы работы исследуемой системы, на которой можно выполнять проверку спецификаций системы, состоящих из набора формальных утверждений о свойствах, которым должна удовлетворять исследуемая система. Набор этих свойств будем задавать с помощью темпоральной логики – логики *CTL*. Формулы логики *CTL* строятся из элементарных высказываний, булевских функций и временных операторов. Используются временные операторы: □ («для всех путей вычисления»), ◇ («для некоторого пути вычисления»), между которыми выполняется отношение двойственности и за которыми следует один из следующих линейных временных операторов: ○ («следующий момент»), ⊙ («когда-то в будущем»), ● («всегда»), ◐ («до тех пор, пока»), ⊖ («высвободить») [19].

Модель Крипке K_N представляется четвёркой $K_N = (G, G_0, R, f)$, где G – множество состояний, $G_0 \subseteq G$ – подмножество начальных состояний, $R \subseteq G \times G$ – отношение переходов, $f : G \to B(P)$ – функция, помечающая каждое состояние множеством атомарных высказываний, истинных в этом состоянии, P – множество атомарных высказываний, $B(P)$ – булеан множества P. Соответственно модель Крипке K_{CN} – четвёрка $K_{CN} = (G', G'_0, R', f')$. Отметим, что пути в моделях соответствуют вычислениям системы. И для модели Крипке $K = (G, G_0, R, f)$, для каждого состояния $g \in G$ и каждой формулы φ *CTL*-логики ее значением $g(\varphi)$ в состоянии g является булева константа 1 или 0, которая определяется индуктивно:

1) если $\varphi = p \in P$, то φ определена в K;

2) $g(1) \overset{def}{=} 1, \quad g(0) \overset{def}{=} 0$;

3) $g(\overline{\varphi}) \overset{def}{=} \overline{g(\varphi)}, \quad g(\varphi \wedge \eta) \overset{def}{=} g(\varphi) \wedge g(\eta), \quad g(\varphi \vee \eta) \overset{def}{=} g(\varphi) \vee g(\eta)$.

Проверка набора формальных требований к функционированию системы на модели Крипке заключается в нахождении в множестве G_0 подмножества всех состояний, в которых выполняется формула φ и если этому подмножеству принадлежат все начальные состояния системы, то модель Крипке удовлетворяет свойству φ.

Множество состояний модели Крипке K_N отношением компоненты χ_1 [11] разбивается на непересекающиеся классы эквивалентности, в каждый такой класс попадают состояния, для которых выполняются условия:

1) каждое состояние модели Крипке K_N само с собой находится в отношении χ_1;

2) два состояния модели Крипке K_N находятся в отношении χ_1, если они являются состояниями одного участка модели Крипке K_N, который отражает динамику функционирования соответствующей составной компоненты, выделенной в сети N.

Если состояние модели Крипке K_N не является состоянием ни одного из участков модели Крипке сети N, отражающего динамику функционирования составной компоненты, выделенной в N, то это состояние само представляет класс эквивалентности – единичный класс. Отметим, что если при построении компонентной сети начальные вершины сети не включать в составные компоненты, то тогда начальные состояния моделей Крипке K_N и K_{CN} совпадают и при этом начальные состояния модели K_N являются единичными классами эквивалентности.

Согласно работе [11] рассмотренная бисимуляция моделей Крипке K_N и K_{CN} может быть определена через установление гомоморфизма h рассматриваемых моделей K_N и K_{CN}, в результате которого каждый участок модели K_N, отражающий динамику функционирования составной компоненты, инкапсулируется в одно состояние (состояние-инкапсулянт) в модели K_{CN}, т.е. при отображении h каждый класс эквивалентности (единичный в том числе), построенный на множестве состояний модели K_N по отношению χ_1, отображается в соответствующее одно состояние модели K_{CN}, что происходит с сохранением отношения переходов для образов состояний модели K_N.

Имеют место следующие правила взаимосвязанной проверки для моделей K_N и K_{CN}:

1) для единичного класса эквивалентности и атомарного высказывания $p \in P$ выполняется

$$f(g) = f'(h(g)),\ \text{где } g \text{ – любое состояние из } G,\ h(g) = g',\ g' \in G';$$

2) для неединичного класса эквивалентности и атомарного высказывания $p \in P$ истинного в каждом состоянии участка модели Крипке K_N, отражающего динамику функционирования соответствующей составной компоненты, выделенной в сети N, имеем истинность этого атомарного высказывания в соответствующем состоянии-инкапсулянте модели K_{CN};

3) если атомарное высказывание $p \in P$ истинно в состоянии-инкапсулянте модели K_{CN}, то проверку на истинность атомарного высказывания в модели K_N достаточно проводить в состояниях только одного из одинаковых участков модели K_N, отражающих динамику функционирования одинаковых составных компонент;

4) если формула φ *CTL*-логики не выполняется на редуцированной модели Крипке K_{CN} , то эта формула не выполняется и на модели Крипке исходной детальной модели Петри.

Заключение

Компонентная сеть Петри, являясь адекватной редукцией детальных сетей Петри – выразительных математических моделей параллельных распределённых систем, обладающая значительно меньшими размерами, позволяет проводить эффективный анализ структурных свойств [10, 18], поведенческих свойств [13–15] исходной детальной сети Петри исследуемой параллельной распределённой системы. В работе проведены исследования на возможность применения компонентной сети Петри к верификации параллельных распределённых систем с использованием автоматической проверки с помощью метода *Model Checking,* предполагающего применение аппарата темпоральной логики *CTL*, проверка формул которой проводится на семантической модели Крипке. В работе показано, что проверку истинности логической формулы логики *CTL*, с помощью которой задаётся устанавливаемое свойство исследуемой параллельной распределённой системы, математическая модель которой представлена сетью Петри, можно проводить с помощью редуцированной модели Крипке её компонентной сети Петри.

1. *Карп Р.М., Миллер Р.Е.* Параллельные схемы программ // Кибернетический сборник. – М.: Мир, 1976. – Т. 13. – С. 5–61.
2. *Котов В.Е.* Сети Петри. – М.: Наука, 1984. – 157 с.
3. *Котов В.Е., Нариньяни А.С.* Асинхронные вычислительные процессы над памятью // Кибернетика. – 1966. – № 3. – С. 64–71.
4. *Clarke E.M., Emerson E.A.* Design and synthesis of synchronization skeletons using branching time temporal logic // Lect. Notes Comput Sci. – 1981. – Vol. 131. – P. 52–71.
5. *Jaffe J.* The use of queues in parallel dataflow evaluation of 'if-then-while' programs // MIT, Laboratory for Computer Science. Tech. Rep. TM-104, May 1978.
6. *Roux J.-L., Berthomieu B.* Verification of local area network protocol with Tine, a software package for time Petri nets // Proc. 7th Europ. Workshop on Application and Theory of Petri Nets. – 1986. – P. 183–205.
7. *Zuberek W.M.* Timed Petri nets and preliminary performance evaluation // Proc. 7th Annual Symp. on Comp. Archit. – 1980. – P. 88–96.
8. *Davis A.L.* A data flow evaluation system based on the concept of recursive locality // Proc. Nat. Comput. Conf., New York, June 4-7, 1979. Arlington: AFIPS Press. – 1979. – Vol. 48. – P. 1079–1086.
9. *Лук'янова О.О.* Про компонентне моделювання систем з паралелізмом // Наукові записки НаУКМА. Комп'ютерні науки. – 2012. – Т. 138. – С. 47–52.
10. *Лукьянова Е.А.* О компонентном анализе параллельных распределенных систем // ТВИМ. – 2011. – № 2. – С. 71–81.
11. *Лук'янова О.О.* Пробісимуляційну еквівалентність детальної моделі Петрі та її *CN*-моделі досліджуваної паралельної розподіленої системи // Вісник КНУ імені Тараса Шевченка. Серія: фізико-математичні науки. – 2013.– Спецвипуск.
12. *Лукьянова Е.А.* О гомоморфизме компонентной сети Петри // Кибернетика и системный анализ. – 2014. – № 1.
13. *Лук'янова О.О.* Про зв'язок мови *CN*-моделі з компонентами-переходам і мови детальної моделі Петрі паралельної розподіленої системи // Вісник КНУ імені Тараса Шевченка. Серія: фізико-математичні науки. – 2012. – № 4. – С. 145–150.
14. *Lukyanova E.* Component modeling: on connections of detailed Petri model and component model of parallel distributed system // ITHEA. – 2013. – Vol. 2, № 1. – P. 15–22.
15. *Лукьянова Е.А.* О языке компонентной сети Петри с компонентами-местами и компонентами-переходами // ТВИМ. – 2011. – № 2. – С. 71–81.
16. *Clarke E.M., Grumberg O., Peled D.* Model Checking // The MIT Press, 1999. – 314 p.
17. *Kenneth L. McMillan* Symbolic Model Checking. – CMU-CS-92-131. – 1992.
18. *Лукьянова Е.А., Дереза А.В.* Исследование однотипних структурних элементов *CN*-сети в процессе компонентного моделирования и анализа сложной системы с параллелизмом // Кибернетика и системный анализ. – 2012. – № 6. – С. 20–29.
19. *Лукьянова Е.А.* Метод верификации свойств реактивной системы на модели // ТВИМ. – 2006. – № 2. – С. 60–68.