Intellectual Technologies on Transport
No 2

Интеллектуальные технологии на транспорте
№ 2

Санкт-Петербург
St. Petersburg
2017

Интеллектуальные технологии на транспорте
№ 2, 2017

Сетевой электронный научный журнал, свободно распространяемый через Интернет.
Публикует статьи на русском и английском языках с результатами исследований и практических достижений в области интеллектуальных технологий и сопутствующих им научных исследований

Журнал основан в 2015 году

Учредитель и издатель

Федеральное государственное бюджетное образовательное учреждение высшего образования «Петербургский государственный университет путей сообщения Императора Александра I» (ФГБОУ ВПО ПГУПС)

Адрес редакции
190031 Санкт-Петербург, Московский пр., 9, ПГУПС
email: itt-pgups@yandex.ru, сайт: http://itt-pgups.ru/, редактор сайта Рогальчук В.В.

ISSN 2413-2527

Журнал зарегистрирован Федеральной службой по надзору в сфере связи и массовых коммуникаций, свидетельство ЭЛ № ФС77-61707 от 07 мая 2015 г.

Журнал зарегистрирован в Российском индексе научного цитирования (РИНЦ)

Intellectual Technologies on Transport
Issue № 2, 2017

Network electronic scientific journal, open access. It publishes articles in Russian and English with the results of research and practical achievements in the field of intelligent technologies and associated research

Founded in 2015

Founder and Publisher
Federal State Educational Institution of Higher Education
«Emperor Alexander I Petersburg State Transport University»

Adress
190031, St. Petersburg, Moskovskiy pr., 9, 2–108
email: itt-pgups@yandex.ru, http://itt-pgups.ru/, Site Editor: Rogalchuk V.V.

ISSN 2413-2527

The journal is registered by the Federal Service for Supervision of Communications and Mass Media, EL №FS77-61707 testimony from May 7, 2015

The journal is registered in the Russian Science Citation Index (RSCI)

Содержание

Contents

Метод мониторинга технологических процессов на основе структурно-логического подхода

Шмелев В. В.
Военно-космическая академия им. А. Ф. Можайского
Санкт-Петербург, Россия
valja1978@yandex.ru

Аннотация. **Статья содержит описание оригинального структурно-логического подхода к моделированию технологических процессов. В качестве исходного описания процесса используется его спецификация, к которой приводятся общепринятые способы описания процессов. Подход включает этапы синтеза модели, проверки ее адекватности прототипу, верификации модели и непосредственно мониторинга технологического процесса с применением синтезированной модели. Подход отличается моделирующей мощностью, в полной мере соответствующей предметной области обработки и анализа измерительной информации ракетной техники. Приводятся краткие сведения о практической апробации подхода, показывающие его преимущество перед применяемым в настоящее время на практике подходом, основанном на рекурсивной модели.**

Ключевые слова: **ракетно-космическая техника, мониторинг технологического процесса, структурно-логический подход, рекурсивная модель процесса, моделирование процессов, сеть Петри, мультиагентный подход к моделированию.**

Введение

Усложнение не только технической структуры современный ракетно-космической техники (РКТ), но и ее функционирования – неотъемлемая часть развития космической отрасли. Естественно, при этом возрастает важность контроля качества и правильности технологических процессов, а понятие контроля расширяется до мониторинга [1]. При этом объектом мониторинга является модель технологического процесса.

Использование модели процесса, учитывающей особенности предметной области функционирования РКТ, позволяет значительно повысить качество мониторинга технологического процесса. Анализ подходов к моделированию процессов в предметной области позволил сделать вывод об их несоответствии современным требованиям специалистов по обработке и анализу телеметрической информации РКТ [2].

Перспективным направлением исследований по совершенствованию мониторинга технологических процессов в предметной области является оригинальный структурно-логический подход (СЛП) [3]. Актуальна компактная систематизация структуры СЛП. В целях обеспечения практической направленности подход будет проецироваться на технологический процесс предстартовой подготовки, пуска и полета ракеты-носителя (РН) «Союз-2».

Задачи системы мониторинга технологических процессов

Содержательно мониторинг процессов заключается в непрерывном (в реальном времени) слежении за состоянием характеристик контролируемого процесса и в оповещении пользователя (оператора) в удобном для него виде о происходящих событиях (как штатных, так и нештатных) с объяснением автоматически принятых решений по оцениванию состояний, с формированием рекомендаций по управлению, с прогнозированием дальнейшего развития событий [4, 5].

Основные задачи при мониторинге технологического процесса: спецификации, синтеза, адекватности, верификации и непосредственно мониторинга.

Задача спецификации – точно и однозначно задать начальное, конечное состояния модели процесса, а также требуемые значения показателей/свойств процесса. Задача спецификации решается на этапе разработки технического задания на создание РКТ. Документом, определяющим спецификацию работы систем РН «Союз-2», является соответствующая циклограмма [6]. Важнейшими свойствами спецификации должны быть непротиворечивость, адекватность требованиям и задачам, решаемым объектом РКТ в целом, а также реализуемость имеющимися аппаратными и системными программными наземными и бортовыми средствами.

Задача синтеза представляет собой построение или автоматическую генерацию модели процесса по ее спецификации. Данная задача наиболее сложна и трудоемка, она изменяет устоявшийся способ представления информации о технологическом процессе. Так создается новая модель процесса работы систем РН «Союз-2», в данном случае – с применением СЛП.

Задача адекватности – проверить соответствие модели процесса ее спецификации, т. е. действительно ли процесс решает те задачи, которые на него возлагаются.

Задача верификации – найти и устранить возможные ошибки в процессе по синтезированной модели, обусловленные некорректностью (ограниченностью) спецификации. Это происходит путем доказательства важных свойств процесса, представляемого моделью, в том числе свойств, приписываемых классическим сетям Петри: непротиворечивости, корректности, активности, консервативности, живости и др. [7].

Задача мониторинга – это основная, комплексная задача, включающая операции непрерывного наблюдения (измерения) параметров процесса, вычисления значений его характеристик, сравнения полученных значений с заданными (граничными, эталонными) значениями, прогноза развития процесса, а также формирования (при необходимости) управляющих воздействий.

Спецификация технологического процесса

Рассмотрим общую форму спецификации процесса.

Технологический процесс $\Re$ описывается кортежем:

$$\Re = \langle S, L \rangle, \quad (1)$$

где $S = \{S_k \,|\, k = \overline{1, card(I_S)}\}$ – множество операций технологического процесса $\Re$; S_k – k-я операция, входящая в технологический процесс $\Re$; I_S – целочисленное положительное не пустое ограниченное множество номеров операций, тогда $\text{card}(I_S)$ – мощность множества операций или их количество. Смысловым содержанием элемента S_k является идентификатор k-й операции; $L = \{l_k \,|\, k = \overline{1, card(I_S)}\}$ – множество кортежей, обусловливающих выполнение операции S_k технологического процесса $\Re$.

Вектор l_k является многомерным кортежем:

$$l_k = \langle Id_k, t_k, \tau_k \rangle, \quad (2)$$

где $Id_k = \left\langle B_b^{(k)}, B_f^{(k)} \right\rangle$ – вектор-идентификатор операции S_k технологического процесса $\Re$, состоящий из элементов: $B_b^{(k)}$ – булева переменная, идентифицирующая условие начала выполнения операции (b – *begin*, начало); $B_f^{(k)}$ – булева переменная, идентифицирующая условие окончания выполнения операции (f – *finite*, окончание); t_k – момент начала выполнения операции S_k технологического процесса $\Re$ в единицах изменения состояний процесса (не только временных единицах), данный элемент «планируется» перед началом процесса и корректируется при его выполнении; τ_k – длительность операции S_k технологического процесса $\Re$ в единицах изменения состояний процесса.

Условия начала и окончания операции описываются предикатами:

$\Pr(B_b^{(k)})$ – предикат, при истинности которого допускается начало выполнения операции S_k технологического процесса $\Re$, в качестве аргументов могут содержаться булевы переменные других операций и произвольные логические операции над ними;

$\Pr(B_f^{(k)})$ – предикат, при истинности которого допускается окончание выполнения операции S_k технологического процесса $\Re$.

Модель технологического процесса общего вида

Синтез модели технологического процесса заключается в построении модели по его спецификации. Рассмотрим последовательно структуру моделей операции, процесса и порядок генерации модели по спецификации (1) процесса.

Операция представляется кортежем:

$$S = \left\langle P, T, F, B, H^+, H^-, M \right\rangle. \quad (3)$$

На рис. 1 представлена схема модели операции, которую целесообразно использовать для придания конструктивности модели операции.

Для проверки работы модели операции на рис. 1 использована среда CPNTools [8–10], позволяющая создавать и исследовать иерархические сложные модифицированные (цветные и расширенные) модели процессов.

Элементы рис. 1 несут смысловую нагрузку позиций, переходов, дуг и фишек инструмента сетей Петри [7]. В кортеже (3) используются элементы:

• $P = \{P_{\text{вн}}, P_{in}, P_{out}\} = \{p_i \,|\, i \in I_P\}$ – конечное непустое множество позиций схемы операции S, I_P – множество номеров позиций, $P_{\text{вн}}$, P_{in} и P_{out} – множества, соответственно, внутренних, входных и выходных позиций. Элементы множества $P_{\text{вн}}$ на рис. 1 обозначается кругами, P_{in} – полукругами с выходящими стрелками, P_{out} – полукругами с входящими стрелками;

• $T = \{t_j \,|\, j \in I_T\}$ – конечное непустое множество переходов схемы операции S, I_T – множество номеров переходов. На рис. 1 элементы множества T обозначены прямоугольниками;

• $F : P \times T \to N$ – входная функция инцидентности, описывающая кратность входной дуги от позиции p_i к переходу t_j схемы операции S и ставящая в соответствие каждой паре $< p_i, t_j >$, $i \in I_P$, $j \in I_T$ элемент множества целых неотрицательных чисел N. На рис. 1 вариант входной функции инцидентности F обозначается линией с одной стрелкой от кругов (полукругов) к прямоугольникам. Линия с обозначением <…> является кратной;

• $B : P \times T \to Nb$ – входная функция инцидентности, описывающая сбрасывающую дугу от позиции p_i к переходу t_j схемы операции S и ставящая в соответствие каждой паре $< p_i, t_j >$, $i \in I_P$, $j \in I_T$ элемент бинарного множества $Nb = \{0,1\}$. На рис. 1 вариант входной функции инцидентности B обозначается линией с двумя стрелками на одном конце от кругов (полукругов) к прямоугольникам;

• $H^+ : T \times P \to N$ – выходная функция инцидентности, описывающая кратность выходной «классической» дуги от перехода t_j в позицию p_i схемы операции S и ставящая в соответствие каждой паре $< t_j, p_i >$, $i \in I_P$, $j \in I_T$ элемент множества целых неотрицательных чисел N. На рис. 1 вариант выходной функции инцидентности H^+ обозначается линией с одной стрелкой от прямоугольника к кругу (полукругу). Линия с двунаправленными стрелками – возвращающая;

• $H^- : T \times P \to N$ – выходная функция инцидентности, описывающая кратность выходной извлекающей («неклассической») дуги от перехода t_j в позицию p_i сети и ставящая в соответствие каждой паре $< t_j, p_i >$, $i \in I_P$, $j \in I_T$ элемент множества целых неотрицательных чисел N. На рис. 1 вариант выходной функции инцидентности H^- обозначается линией с одной стрелкой от прямоугольника к кругу (полукругу), противоположный стрелке конец линии содержит малый круг;

• $M : P \to N$ – функция разметки, которая каждому элементу $p_i \in P$ ставит в соответствие элемент множества целых неотрицательных чисел N. На рис. 1 вариант функции разметки M обозначается точками внутри кругов.

Позиции «Старт», «Стоп», «ПриостВып» (приостановка выполнения операции) и «ПродВып» (продолжение выполнения операции) являются позициями, получающими

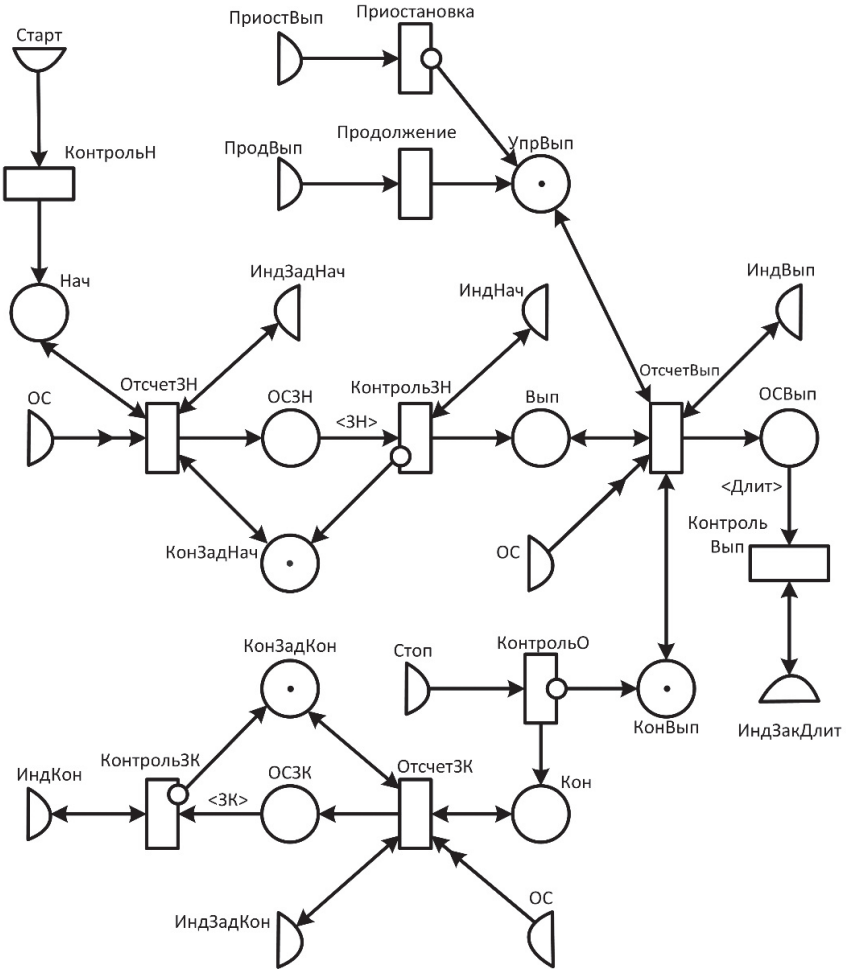


Рис. 1. Схема модели операции

управляющие сигналы от внешних схем. Данные позиции обеспечивают выполнение требования управляемости модели процесса. Управляющие позиции можно считать бинарными, так как они могут быть в двух состояниях: нет ни одной фишки, есть только одна фишка.

Позиция «ОС» (отсчет событий) содержит отсчеты событий, используемые для смены состояния модели операции. В качестве таких событий могут выступать метки времени или факты наступления событий при контроле не временны́х, а событийных процессов. Позиция «ОС» по содержанию является бинарной, так как последующими переходами обрабатывается только факт прихода отсчета, но не количество ранее совершившихся событий, т. е. количество имеющихся в позиции «ОС» фишек. Этим обеспечивается инвариантность модели к типу единиц изменения состояния операции.

Позиции «ИндЗадНач» (индикация степени отсчета задержки начала операции), «ИндНач» (индикация фактического старта выполнения операции), «ИндВып» (индикация степени выполнения операции), «ИндЗадКон» (индикация степени отсчета задержки окончания операции), «ИндКон» (индикация фактического окончания выполнения операции) и «ИндЗакДлит» (индикация планируемого окончания выполнения операции по длительности) являются индикаторными и обеспечивают наблюдаемость модели операции. Данные позиции должны использоваться внешними схемами для определения траектории развития процесса в целом путем сравнения значений в данных позициях с некоторыми эталонами. Управляющие позиции «ИндЗадНач», «ИндВып» и «ИндЗадКон» являются счетными по содержанию, так как содержат количество отсчетов событий, полученных за соответствующий интервал. Позиции «ИндНач», «ИндКон» и «ИндЗакДлит» являются бинарными, так как смыслосодержащими являются только состояния наличия и отсутствия фишек.

Внутренние позиции и переходы обеспечивают смену состояния операции, т. е. изменение разметок выходных (индикаторных) позиций в зависимости от разметок входных (управляющих) позиций. Внутренние позиции и переходы: «Нач» (начало), «ОтсчетЗН» (отсчет задержки начала), «ОСЗН» (отсчет событий задержки начала), «КонтрольЗН» (контроль задержки начала), «КонЗадНач» (окончание отсчета задержки начала фактического выполнения ТО), «Вып» (выполняется), «ОтсчетВып» (отсчет фактического выполнения), «ОСВып» (отсчет событий выполнения), «КонтрольВып» (контроль выполнения), «УпрВып» (управление выполнением операции), «Приостановка» (приостановка выполнения операции), «Продолжение» (продолжение выполнения операции), «КонВып» (контроль выполнения операции), «КонтрольО» (контроль окончания), «Кон» (окончание), «ОтсчетЗК» (отсчет задержки окончания), «ОСЗК» (отсчет событий задержки окончания), «КонтрольЗК» (контроль

задержки окончания), «КонЗадКон» (окончание отсчета задержки фактического окончания выполнения ТО).

Для обеспечения компактности изложения формальная модель операции не приводится. Она достаточно легко формируется по схеме рис. 1 и составу кортежа (4).

Представленная на рис. 1 схема модели операции является максимально общей по возможности наблюдения и управления состоянием процесса. Поскольку схема на рис. 1 универсальна, совокупность элементов схемы операции за исключением входных и выходных позиций можно заменить специальным переходом-процедурой (рис. 2). Переход-процедура обозначен прямоугольником с двойными линиями. В левой части приведены входные позиции, формирующие траекторию развития процесса, в правой – выходные (индикаторные) позиции, показывающие ход процесса. Внутри перехода-процедуры приведены значения длительностей задержки начала выполнения (<ЗН>), задержки окончания выполнения (<ЗК>) и непосредственно выполнения операции (<Длит>).

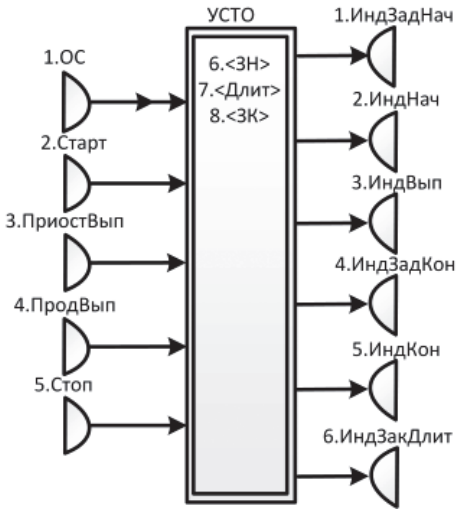


Рис. 2. Переход-процедура – компактная графическая модель операции

Модель процесса представляет собой кортеж:

$$\hat{\Re} = \langle S, \Im, Q \rangle, \qquad (4)$$

где S – множество операций процесса, каждая из которых – кортеж (3); $\Im = \begin{pmatrix} \Im_{in} : P_{out}^{(l)} \times P_{in}^{(k)} \to N \\ \Im_{out} : P_{out}^{(k)} \times P_{in}^{(m)} \to N \end{pmatrix}$ – векторная функция инцидентности, описывающая логику технологического процесса $\hat{\Re}$; $\Im_{in}$ – входная функция инцидентности операции S_k, где $\Im_{in} : P_{out}^{(l)} \times P_{in}^{(k)} \to N$ описывает «склеивание» выходных позиций операции S_l и входных позиций операции S_k; $\Im_{out} : P_{out}^{(k)} \times P_{in}^{(m)} \to N$ описывает «склеивание» выходных позиций операции S_k и входных позиций операции S_m, $l,k,m \in I_S$. Перечень «склеиваемых» входных позиций из множества $P_{in}^{(k)}$={«ОС», «Старт», «Стоп», «ПриостВып», «ПродВып»} (см. рис. 1, 2) и выходных из множества $P_{out}^{(k)}$= ={«ИндЗадНач», «ИндНач», «ИндВып», «ИндЗадКон», «ИндКон», «ИндЗакДлит»} определяет логику развития моделируемого технологического процесса; $Q = \{Q_k \,|\, k = \overline{1, card(I_S)}\}$ – множество ограничений технологического процесса $\hat{\Re}$; Q_k – множество отношений, ограничивающий выбор альтернативы развития k-й операции. Ограничение Q_k операции S_k также является множеством $Q_k = \{q_c^{(k)} \,|\, c = \overline{1, card(Q)}\}$, где $q_c^{(k)}$ – c-й вид ограничения операции S_k; c – порядковый номер ограничения; $card(Q)$ – количество накладываемых ограничений.

Синтез модели технологического процесса

Синтез модели технологического процесса заключается в установлении функционального соответствия между элементами кортежа $\hat{\Re}$ (4) и кортежа $\Re$ (1). Непосредственно необходимо определить переход от элементов кортежа $\Re$ (1) к входным позициям перехода процедуры «Старт» и «Стоп» (см. рис. 1, 2) для каждой операции процесса, а также функцию, определяющую длительность выполнения операции (<Длит>). Номер операции определяет переменная k.

Разметка позиции «Старт» определяется результатом проверки предиката $\Pr(B_b^{(k)})$:

$$M(\text{Старт}) = \begin{cases} 1, & \text{если } \Pr(B_b^{(k)}) = \text{"истина"} \\ 0, & \text{если } \Pr(B_b^{(k)}) = \text{"ложь"} \end{cases}.$$

Разметка позиции «Стоп» определяется результатом проверки предиката $\Pr(B_f^{(k)})$:

$$M(\text{Стоп}) = \begin{cases} 1, & \text{если } \Pr(B_f^{(k)}) = \text{"истина"} \\ 0, & \text{если } \Pr(B_f^{(k)}) = \text{"ложь"} \end{cases}.$$

Длительность операции <Длит> задается равной переменной τ_k:

$$F < \text{ОСВып}, \text{КонтрольВып} > = < \text{Длит} > = \tau_k.$$

Входные позиции «ОС», «ПриостВып» и «ПродВып» перехода процедуры, переменные <ЗН> и <ЗК> (см. рис. 2) являются уникальными и не требуют определения через элементы кортежа $\Re$ (1).

Рассмотрим порядок определения структуры процесса $\hat{\Re}$, а именно множества $\Im$.

Логическое условие начала k-й операции описывается с помощью отношения

$$B_{\Pr_b} : \Pr(B_f^{(l)}) \times \Pr(B_b^{(k)}) \to \Im_{in} : P_{out}^{(l)} \times P_{in}^{(k)} \to N;$$
$$P_{in}^{(k)} = \{\text{ОС}, \text{Старт}, \text{Приостановка}, \text{Продолжение}\}.$$

Отношение $B_{\Pr_b}$ определяет взаимосвязь l-й и k-й операций. В рамках СЛП отношение $B_{\Pr_b}$ преобразуется в функцию инцидентности $\Im_{in}$ между выходными позициями перехода-процедуры l-й и входными позициями перехода-процедуры k-й операций. Данная функция будет определять условие начала k-й операции. Это обеспечивается наличием во множестве $P_{in}^{(k)}$ позиции «Старт».

Логическое условие окончания k-й операции описывается с помощью отношения

$$B_{\Pr_f} : \Pr(B_f^{(m)}) \times \Pr(B_b^{(k)}) \to \Im_{in} : P_{out}^{(m)} \times P_{in}^{(k)} \to N;$$
$$P_{in}^{(k)} = \{\text{ОС}, \text{Стоп}, \text{Приостановка}, \text{Продолжение}\}.$$

Отношение B_{Pr_f} определяет взаимосвязь m-й и k-й операций. В рамках СЛП отношение B_{Pr_f} также преобразуется в функцию инцидентности $\Im_{in}$ между выходными позициями перехода-процедуры m-й и входными позициями перехода-процедуры k-й операций. Но только уже данная функция будет определять условие окончания k-й операции. Это обеспечивается наличием во множестве $P_{in}^{(k)}$ позиции «Стоп».

Конкретный перечень используемых позиций $P_{in}, P_{out} \in P$ определяется видом взаимосвязи B_{Pr_b} и B_{Pr_f}.

Составляющая $\Im_{out}$ векторной функции инцидентности $\Im$ предыдущей операции формируется автоматически при формировании составляющей $\Im_{in}$ векторной функции инцидентности $\Im$ очередной операции.

Особенностью предметной области является возможность наложения на технологический процесс $\hat{\Re}$ различного рода ограничений Q. Приведем вербальный и графический способ представления ограничений Q для модели процесса $\hat{\Re}$, созданной в соответствии с положениями СЛП.

Для описания ограничений предлагается использовать инструмент G-моделирования, разработанный М. Ю. Охтилевым [11] и нашедший применение в практике автоматизации подготовки и пуска РН «Союз-2» [1]. Однако в нашем случае изменится область применения данного инструмента. Ограничение – это правило классической структуры «Если предикат истинен, по выполняется соответствующее действие».

Рассмотрим графический способ описания ограничений. Основой реализации учета ограничений является предикатный переход. На рис. 3 представлен фрагмент схемы операции только из одной входной позиции.

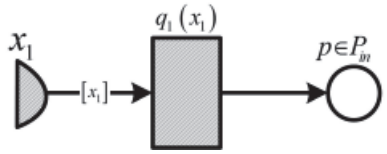


Рис. 3. Графическое представление реализации ограничений технологического процесса

Заштрихованный полукруг представляет собой позицию, включающую значение соответствующего аргумента. Данная позиция содержит не просто фишку в классическом ее понимании в теории сетей Петри, но именно фишку – значение аргумента. С учетом особенностей предметной области в качестве аргументов могут выступать отдельное значение телеметрируемых параметров, совокупности значений, числовые результаты обработки параметров, качественные результаты контроля и диагностирования систем ракетно-космической техники и наземного оборудования. Такая позиция может быть названа z-позицией (z – значение). Относительно разметки z-позиций следует отметить, что $m(z_i) \in \{0,1\}$, т. е. в z-позиции может присутствовать только одна фишка. Источником информации в z-позициях являются средства измерений, вычислительные алгоритмы, внешние относительно схемы модели технологического процесса.

Дуга, на которую нанесено обозначение аргумента в квадратных скобках $[\cdot]$, соединяет только z-позиции и предикатные переходы. Такие дуги можно назвать z-дугами. Они предназначены для передачи фишек только со значениями соответствующего аргумента.

Предикатный переход обозначается заштрихованным прямоугольником. Над прямоугольником представлен предикат, в скобках – аргумент предиката. Условием срабатывания перехода является не только наличие фишки во входных позициях (как классических, так и в z-позициях), но и истинность указанного предиката. При срабатывании предикатного перехода формируется классическая фишка в позициях в соответствии с выходной функцией инцидентности предикатного перехода. Прототипом предикатного перехода и z-позиции являются соответствующие элементы G-сетей, описанные в [11].

Подробно рассматривать формальный способ описания ограничений нет необходимости. Формальная модель ограничения соответствует по структуре кортежу (3) с соответствующими незначительными изменениями компонентов.

Адекватность модели технологического процесса

Формально адекватность модели устанавливается обратным формированием элементов кортежей (1) и (2) по содержимому элементов кортежей (3) и (4). Предлагается рассмотреть порядок вывода элементов Id_k, t_k и τ_k кортежа l_k для k-й операции из элементов кортежа $S = \langle P, T, F, B, H^+, H^-, M \rangle$, составленного для той же операции.

Как отмечалось при описании модели технологической операции, благодаря универсальности структура схем моделей различных операций различается только кратностью дуги:

$$F < \text{ОСВып}, \text{КонтрольВып} > = < \text{Длит} > .$$

Можно записать

$$\tau_k = < \text{Длит} > .$$

Момент t_k начала выполнения операции S_k процесса $\Re$ в единицах изменения состояний процесса в явном виде отсутствует в кортеже (3). Так как это только «планируемый» момент начала выполнения операции, контролировать адекватность модели спецификации по данному элементу кортежа (2) нет необходимости.

Булевы переменные, идентифицирующие условия начала и окончания выполнения операции, соответственно, $B_b^{(k)}$ и $B_f^{(k)}$, формируются путем анализа векторной функции инцидентности $\Im$ созданной k-й операции. При этом достаточно рассмотреть только входную функцию инцидентности $\Im_{in}$, так как составляющая $\Im_{out}$ предыдущей операции формируется автоматически при формировании составляющей $\Im_{in}$ очередной операции.

Анализируются аргументы $P_{out}^{(l)}$ и $P_{in}^{(k)}$ входной функции инцидентности $\Im_{in}$ в соответствии с выражениями

$$\Im_{in} : P_{out}^{(l)} \times P_{in}^{(k)} \to$$
$$\to N : (N > 0, P_{out}^{(l)} = \text{ИндЗакДлит}^{(l)}, P_{in}^{(k)} = \text{Старт}) \Rightarrow \quad (5)$$
$$\Rightarrow \Pr(B_b^{(k)}) = O(l);$$

$$\Im_{in} : P_{out}^{(l)} \times P_{in}^{(k)} \rightarrow$$
$$\rightarrow N : (N > 0, P_{out}^{(l)} = \text{ИндЗакДлит}^{(l)}, P_{in}^{(k)} = \text{Стоп}) \Rightarrow \quad (6)$$
$$\Rightarrow \Pr(B_f^{(k)}) = O(l);$$

$$\Im_{in} : P_{out}^{(l)} \times P_{in}^{(k)} \rightarrow N : (N > 0, P_{out}^{(l)} =$$
$$= \text{ИндНач}^{(l)}, P_{in}^{(k)} = \text{Старт}) \Rightarrow \quad (7)$$
$$\Rightarrow \Pr(B_b^{(k)}) = H(l);$$

$$\Im_{in} : P_{out}^{(l)} \times P_{in}^{(k)} \rightarrow$$
$$\rightarrow N : (N > 0, P_{out}^{(l)} = \text{ИндНач}^{(l)}, \quad (8)$$
$$P_{in}^{(k)} = \text{Стоп}) \Rightarrow \Pr(B_f^{(k)}) = H(l);$$

$$\Im_{in} : P_{out}^{(l)} \times P_{in}^{(k)} \rightarrow N : (N = 0, \forall P_{out}^{(l)}, P_{in}^{(k)} = \text{Стоп}) \Rightarrow$$
$$\Rightarrow \Pr(B_f^{(k)}) = \text{"По длит."}. \quad (9)$$

Выражение (5) показывает, что если входная функция инцидентности $\Im_{in}$ устанавливает связь между выходной позицией $\text{ИндЗакДлит}^{(l)}$ (или $\text{ИндЗак}^{(l)}$) l-й операции и входной позицией Старт k-й операции, то условием начала k-й операции в спецификации является окончание l-й операции. Выражение (6) показывает, что если входная функция инцидентности $\Im_{in}$ устанавливает связь между выходной позицией $\text{ИндЗакДлит}^{(l)}$ (или $\text{ИндЗак}^{(l)}$) l-й операции и входной позицией Стоп k-й операции, то условием окончания k-й операции в спецификации является окончание l-й операции. Выражение (7) показывает, что если входная функция инцидентности $\Im_{in}$ устанавливает связь между выходной позицией $\text{ИндНач}^{(l)}$ l-й операции и входной позицией Старт k-й операции, то условием начала k-й операции в спецификации является начало l-й операции. Выражение (8) показывает, что если входная функция инцидентности $\Im_{in}$ устанавливает связь между выходной позицией $\text{ИндНач}^{(l)}$ l-й операции и входной позицией Стоп k-й операции, то условием окончания k-й операции в спецификации является начало l-й операции. Выражение (9) показывает, что если входная функция инцидентности $\Im_{in}$ к входной позиции Стоп k-й операции отсутствует, то условием окончания k-й операции в спецификации является достижение длительности k-й операции τ_k =< Длит >. В последнем случае в спецификацию вносится запись «По длит.».

При равенстве полученных выражений $\Pr(B_b^{(k)})$ и $\Pr(B_f^{(k)})$, $k = \overline{1, card(I_S)}$ можно утверждать, что адекватность синтезированной модели своей спецификации соблюдена по элементу $L = \{l_k \mid k = \overline{1, card(I_S)}\}$ кортежа (1).

Верификация модели технологического процесса

Под ошибками в синтезированной модели понимаются критические прерывания (зацикливания) выполнения процесса (модели процесса) в не предусмотренные спецификацией моменты или этапы [12].

В качестве критических свойств, проверка которых обеспечит успешный результат формальной верификации синтезированной модели, следует назвать непротиворечивость, корректность и активность синтезированной модели технологического процесса.

Непротиворечивость модели технологического процесса

Значительное расширение моделирующей мощности структурно-логического подхода, особенно в области РКТ, достигается введением предикатных переходов.

В то время как на выполнение классических переходов не накладывается никаких ограничений, предикатные переходы выполняются (с одновременным занесением фишки в свою выходную позицию) лишь тогда, когда значение соответствующей предикатной функции $q_c^{(k)}(\cdot) = \text{"истина"}$, где $q_c^{(k)}(\cdot)$ – c-й вид ограничения операции S_k.

Множество значений аргументов $(\cdot)$ как предметных переменных предикатной функции для соответствующего предикатного перехода, при которых выполняется условие $q_c^{(k)}(\cdot) = \text{"истина"}$, определяет область применимости $D_{q_c^{(k)}(\cdot)}$ перехода $q_c^{(k)}(\cdot)$.

Используя обозначения областей применимости, условие выполнимости модели процесса $\hat{\Re}$ можно записать в виде

$$D_{\hat{\Re}} = \bigcap_{k=\overline{1, card(I_S)}} D_{S_k} = \varnothing. \quad (10)$$

Критическая ошибка возможна тогда, когда в модели процесса $\hat{\Re}$ существует, например, такая пара предикатов $q_1^{(\cdot)}(\cdot)$ и $q_2^{(\cdot)}(\cdot)$, которые на одном и том же подмножестве $D_{q_{1,2}^{(\cdot)}(\cdot)} = \left(D_{q_1^{(\cdot)}(\cdot)} \cap D_{q_2^{(\cdot)}(\cdot)} \right) \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}$ принимают значения и «истина», и «ложь».

При выявлении факта критической ошибки вследствие невыполнения выражения (10) следует дополнительно проанализировать наложенные ограничения $Q_k, k = \overline{1, card(I_S)}$. Смысл анализа должен заключаться в выявлении тех ограничений (предикатов) $q_c^{(k)}(\cdot)$, которые не обеспечивают выполнение равенства (10).

Корректность модели технологического процесса

Операция $S_k \left| k = \overline{1, card(I_S)} \right.$ процесса $\hat{\Re}$ считается корректной, если она одновременно корректна и по входу, и по выходу. Операция S_k является корректной по выходу, если для любой разметки индикаторных позиций $m(p_i) > 0$, $p_i \in P_{out}$ четко определен дальнейший порядок выбора каждой определяющей эту разметку фишки. Операция S_k является корректной по входу, если четко определено, каким способом была сформирована любая фишка, формирующая разметку $m(p_i) > 0$, $p_i \in P_{in}$ управляющих позиций P_{in} этой операции.

Приведенные определения понятий корректности операций не являются строгими и описывают рассматриваемое явление лишь на содержательном или интуитивном уровне. Точные определения корректности должны следовать из структуры входной и выходной функций инцидентности.

Операция, не корректная по входу, должна иметь следующий вид функции $\Im_{in}^{(k)}$:

$$\Im_{in}^{(k)} \left\langle P_{out}^{(\cdot)}, P_{in}^{(k)} \right\rangle = 1,$$

причем $card(P_{out}^{(\cdot)}) > 1$, $card(P_{in}^{(k)}) = 1$.

Данное выражение раскрывается следующим образом. Входная функция инцидентности $\Im_{in}^{(k)}$ операции S_k, некорректной по входу, имеет в качестве первого элемента кортежа множество позиций, по мощности большее 1, а в качестве второго элемента кортежа – только одну управляющую позицию операции S_k.

Операция, некорректная по выходу, должна иметь следующий вид функции $\Im_{out}^{(k)}$:

$$\Im_{out}^{(k)} \left\langle P_{out}^{(k)}, P_{in}^{(\cdot)} \right\rangle = 1,$$

причем $card(P_{out}^{(k)}) = 1$, $card(P_{in}^{(\cdot)}) > 1$.

Проверка корректности для каждой операции формирует корректную модель процесса в целом. Устранение некорректности по входу и выходу осуществляется добавлением фиктивных позиций и переходов, как описано, например, в [8, 11].

Тупиковые позиции в модели процесса (активность модели)

Непредусмотренная ситуация, когда не формируется разметка входных позиций, изменяющая состояние какой-либо операции, является ошибкой или тупиком в синтезированной модели. Для рассуждений будем рассматривать фрагмент схемы модели процесса, состоящий из двух операций, представленных на рис. 4.

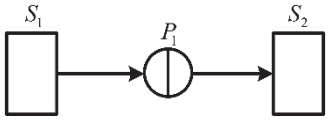


Рис. 4. Фрагмент схемы модели процесса

На рис. 4 позиция P_1 есть объединяющее множество $P_1 = \{P_{out}^{(1)}, P_{in}^{(2)}\}$.

Операция S_2 схемы модели процесса является тупиковой, если при выполнении фрагмента модели возможен случай, когда пришедшая в позицию P_1 фишка никогда не может быть выбрана оттуда.

Условие прихода (появления) фишки в позиции P_1 схемы модели процесса задается в виде $\Im_{out}^{(1)} : P_{out}^{(1)} \times P_{in}^{(2)} \to N$, где $N > 0$, а условие выхода (использования) фишки в этой позиции $\Im_{in}^{(2)} : P_{out}^{(1)} \times P_{in}^{(2)} \to N$, где $N > 0$.

Можно отметить, что операция S_2 тогда и только тогда не будет тупиковой, когда $N > 0$. Выполнение данного выражения является условием отсутствия тупиков для соответствующей операции.

Итак, после проверки всех трех условий формируется непротиворечивая, корректная, активная модель технологического процесса, что в совокупности позволяет говорить об успешной верификации синтезированной модели технологического процесса.

Мониторинг технологического процесса

Приложение синтезированной модели как предмета мониторинга технологического процесса поясняет рис. 5.

Штриховыми линиями на рис. 5 обозначены операции, выполнение которых может быть опущено. Представленная на рис. 5 информация известна и является максимально общей. Необходимо провести сопряжение мониторинга технологического процесса в общей постановке к использованию синтезированной модели, представленной кортежами (3) и (4).

Рис. 5. Схема мониторинга технологического процесса

Примем для разметок следующие обозначения:

- $m(p_i)$ – разметка позиции $p_i \in P_{out}$;
- $M_{out}^{(k)} = \{m(p_i) \,|\, p_i \in P_{out}^{(k)}\}$ – множество разметок $m(p_i)$ выходных позиций $p_i \in P_{out}^{(k)}$ операции $S_k \in \hat{\Re}$;
- $\mathrm{M}_{out} = \{M_{out}^{(k)} \,|\, k = \overline{1, card(I_S)}\}$ – множество разметок $M_{out}^{(k)}$ выходных позиций $p_i \in P_{out}^{(k)}$ операций $S_k \,|\, k = \overline{1, card(I_S)}$ процесса $\hat{\Re}$.

Таким образом, параметры процесса, представленного кортежем (4), измеряются путем фиксации разметок $m(p_i)$ позиций $p_i \in P_{out}$, $p_i \,|\, i \in I_P$ из множества P_{out} для каждой операции $S_k \,|\, k = \overline{1, card(I_S)}$ во множестве M_{out}. Для непрерывного наблюдения формируется кортеж X разметок M_{out}: $X = \left\langle \mathrm{M}_{\text{нач } out}, ..., \mathrm{M}_{i\ out}, ..., \mathrm{M}_{\text{кон } out} \right\rangle$, где $\mathrm{M}_{\text{нач } out}$ можно обозначить через x_1 – начальное состояние процесса; $\mathrm{M}_{i\ out} = x_i$ – i-е состояние процесса; $\mathrm{M}_{\text{кон } out} = x_f$ – конечное, или финальное, состояние процесса. Кортеж X формируется в требуемые (задаваемые) моменты или этапы (сечения) моделируемого процесса.

Операция вычисления характеристик состоит в применении при необходимости к элементу x_i кортежа X оператора преобразования с целью вычисления требуемой характеристики y_i.

Формально операция контроля характеристик процесса может быть описана следующим образом.

Введем следующие необходимые обозначения:

- $m_{\text{гр}}(p_i)$ – заданная (требуемая или ожидаемая) разметка позиции $p_i \in P_{out}$;
- $\mathrm{M}_{\text{гр } out} = \{M_{\text{гр } out}^{(k)} \,|\, k = \overline{1, card(I_S)}\}$ – множество заданных (требуемых или ожидаемых) разметок $M_{\text{гр } out}^{(k)}$ выходных позиций $p_i \in P_{out}^{(k)}$ операций $S_k \,|\, k = \overline{1, card(I_S)}$ процесса $\hat{\Re}$;
- $X_{\text{гр}} = \left\langle \mathrm{M}_{\text{гр нач } out}, ..., \mathrm{M}_{\text{гр } i\ out}, ..., \mathrm{M}_{\text{гр кон } out} \right\rangle$ – кортеж разметок $\mathrm{M}_{\text{гр } out}$, позволяющий определить упорядоченный перечень заданных (требуемых или ожидаемых) разметок $\mathrm{M}_{\text{гр } out}$ процесса $\hat{\Re}$ на интервале контроля;
- $\Delta m(p_i)$ – невязка разметок $m(p_i)$ и $m_{\text{гр}}(p_i)$;
- $\Delta\mathrm{M}_{out} = \{\Delta M_{out}^{(k)} \,|\, k = \overline{1, card(I_S)}\}$ – множество невязок разметок $M_{out}^{(k)}$ и $M_{\text{гр } out}^{(k)}$ выходных позиций $p_i \in P_{out}^{(k)}$ операций $S_k \,|\, k = \overline{1, card(I_S)}$ процесса $\hat{\Re}$;
- $\Delta X = \left\langle \Delta\mathrm{M}_{\text{нач } out}, ..., \Delta\mathrm{M}_{i\ out}, ..., \Delta\mathrm{M}_{\text{кон } out} \right\rangle$ – кортеж невязок разметок M_{out} и $\mathrm{M}_{\text{гр } out}$, позволяющий определить траекторию невязок на интервале контроля.

Вычисление невязки «нижнего уровня» заключается в операции вычитания:

$$\Delta m(p_i) = m(p_i) - m_{\text{тр}}(p_i).$$

Аналогичные выражения можно составить и для вычисления невязок $\Delta M_{out}^{(k)}$, $\Delta \mathrm{M}_{out}$ и ΔX.

Операция анализа (прогноза развития) процесса заключается в применении оператора

$$\Psi : \Delta \mathrm{M}_{i\,out} \times \mathrm{M}_{i\,out} \to \Delta \mathrm{M}_{(i+1)\,out}.$$

Таким образом, оператор прогноза Ψ заключается в «прогнозировании» невязки $\Delta \mathrm{M}_{(i+1)\,out}$ на следующем шаге выполнения процесса на основе текущего состояния $\mathrm{M}_{i\,out}$ и текущей невязки $\Delta \mathrm{M}_{i\,out}$ моделируемого процесса. Целью прогноза является определение степени приближения прогнозируемой невязки к критическому значению $\Delta \mathrm{M}_{\text{кр}\,out}$, которое потребует формирования корректирующих управляющих воздействий для ее компенсации.

При необходимости управляющих воздействий применяется соответствующая операция. Возможность их выполнения обусловлена наличием управляющих позиций – входных позиций в схеме модели операции (см. рис. 2). Рассмотрим порядок выбора управляющих воздействий.

Управление процессом – это целенаправленное изменение специальных (управляющих) параметров модели процесса, при которых достигается требуемое значение специальных (индикаторных) параметров. Последние являются показателями свойств модели процесса. В рамках СЛП управляющие параметры – разметки входных позиций, индикаторные параметры – разметки выходных позиций.

Для задания множества допустимых альтернатив выполнения модели процесса Δ_D может быть использовано отношение

$$\Delta_D : \Delta \times \mathrm{M}_{\text{нач}\,out} \times \mathrm{M}_{\text{кон}\,out} \times Q \to \Delta_D, \qquad (11)$$

где Δ – множество всех вариантов развития технологического процесса; $\mathrm{M}_{\text{нач}\,out}$ – множество начальных (исходных) состояний технологического процесса; $\mathrm{M}_{\text{кон}\,out}$ – множество требуемых состояний технологического процесса; Q – множество отношений, ограничивающих выбор.

Так как множество P состоит из трех непересекающихся подмножеств $P_{\text{вн}}$, P_{in} и P_{out}, правомерным будет записать

$$\mathrm{M} : \mathrm{M}_{\text{вн}} \times \mathrm{M}_{in} \times \mathrm{M}_{out},$$

причем $card(\mathrm{M}) = card(\mathrm{M}_{\text{вн}}) \cdot card(\mathrm{M}_{in}) \cdot card(\mathrm{M}_{out})$, где $\mathrm{M}_{\text{вн}}$, M_{in} и M_{out} – множества возможных разметок схем операций (рис. 1, 2), состоящих из, соответственно, только внутренних, входных и выходных позиций $P_{\text{вн}}$, P_{out} и P_{in}.

Из всей совокупности множества позиций $P = \{p_i \,|\, i \in I_P\} = \{P_{\text{вн}}, P_{\text{in}}, P_{out}\}$ необходимо выделить множество P_{out}, так как именно это множество отражает состояние операции, и по смене разметок только этих позиций будет приниматься решение о наблюдаемом (текущем) состоянии моделируемой операции. Среди элементов множества M_{out} должны находиться и некоторые элементы $\mathrm{M}_{\text{нач}\,out}$ и $\mathrm{M}_{\text{кон}\,out}$, обозначающие, соответственно, начальное и конечное (требуемое) состояние технологической операции. Данные разметки должны входить, как минимум, в один кортеж разметок сети. При наличии нескольких подобных кортежей операция должна допускать альтернативы выполнения.

Для всего технологического процесса

$$\mathrm{M}_{\text{нач}\,out} = \{M_{\text{нач}\,k\,out} \,|\, k = \overline{1, card(I_S)}\};$$

$$\mathrm{M}_{\text{кон}\,out} = \{M_{\text{кон}\,k\,out} \,|\, k = \overline{1, card(I_S)}\}.$$

Последние выражения обозначают начальные и конечные разметки выходных позиций обобщенных схем всех операций технологического процесса. Данные множества для каждого $k = \overline{1, card(I_S)}$ могут иметь как единичную мощность, так и мощность более единицы. В первом случае краевые условия задаются точечно, во втором случае краевые условия на состояния технологического процесса задаются в виде интервала значений.

Состояние технологической операции изменится после подачи управляющих сигналов на входные позиции P_{in} или формирования некоторой разметки $M_{t\,in} \in M_{in}$. Вследствие срабатывания разрешенных переходов сети будет сформирована новая разметка сети $M_{t'} : M_{t'\,\text{вн}} \times M_{t'\,in} \times M_{t'\,out}$ и технологическая операция перейдет в новое состояние, т. е. операция будет выполняться. Таким образом, элементарный кортеж $\langle M_t, M_{t'} \rangle$ описывает минимальный фрагмент траектории выполнения или развития технологической операции. Однако в выражении (11) для составления множества Δ целесообразно использовать только «управляющую» часть кортежа разметок $M_{t'} : M_{t'\,\text{вн}} \times M_{t'\,in} \times M_{t'\,out}$, а именно кортеж множеств разметок $M_{in} : P_{in} \to N$ входных позиций P_{in} по причине выбора именно среди них в некотором смысле оптимального управления моделируемым процессом.

В итоге именно кортеж множеств разметок $M_{in} : P_{in} \to N$ является кортежем управляющих воздействий Δ.

В рамках моделей (3) и (4) множество Δ_D будет содержать возможные кортежи разметок входных позиций обобщенной схемы операции применительно к каждому элементу множества $S = \{S_k \,|\, k = \overline{1, card(I_S)}\}$. В итоге можно записать

$$\Delta_D = \{\Delta_t = \langle M_{\text{нач}\,in\,t}, \ldots, M_{\text{кон}\,in\,t} \rangle_t,\ t = \overline{1, card(\Delta_D)}\}. \qquad (12)$$

Выражение (12) формализует управление моделью процесса через воздействие на входные позиции в каждый момент получения меток смены событий.

Таким образом, рассмотрена операция формирования управляющих воздействий (рис. 5).

Операция изменения состояния модели процесса на рис. 5 заключается в формировании очередной разметки выходных позиций M_{out} по результатам применения к модели процесса $\hat{\Re}$ очередной разметки входных позиций M_{in}, с помощью функции инцидентности $\Im$ входящей в кортеж (4).

Практическая апробация структурно-логического подхода

Для анализа эффективности применения СЛП для мониторинга технологических процессов при обработке и анализе измерительный информации РКТ была создана модель технологического процесса функционирования пневмогидравлической системы РН «Союз-2» на этапах подготовки к пуску, пуска и полета изделия. Спецификация такого технологиче-

ского процесса, согласно технической документации, содержала 176 операций. Для измерения физических процессов используется 59 телеметрируемых параметров.

В качестве эталона использовано штатное специальное программное обеспечение (СПО) мониторинга технологических процессов, в основе которого используется рекурсивная модель процесса [13]. Время мониторинга всех операций с использованием применяемой рекурсивной модели составляет примерно 3 часа. При этом полнота используемой информации крайне недостаточна из-за ограниченности моделирующей мощности рекурсивной модели: в синтезированной модели учитывалось в среднем 15 % (сигнального типа) доступных к использованию телеметрируемых параметров, технологических операций и возможных нештатных ситуаций. Синтезированная модель как инструмент мониторинга крайне слабо приспособлена для верификации и модификации.

Информационная технология мониторинга на основе СЛП позволила синтезировать модель рассматриваемого технологического процесса на качественно и количественно ином уровне. В 3 раза была повышена оперативность мониторинга, т. е. в 3 раза уменьшено время полного анализа всех операций согласно технической документации. Полнота используемой информации была повышена до 80 %, не использовалась лишь часть измерительной информации, формируемая наземной системой измерений. Благодаря повышению моделирующей мощности практически полностью учтены возможные нештатные ситуации (аварийные выключения двигателей), кроме того, достигнута большая глубина моделирования технологических операций. Реализованы алгоритмы автоматизированной верификации синтезированной модели. Значительно повышена модифицируемость синтезированной модели процесса, благодаря чему снижаются затраты на синтез новой модели при изменении прототипа заводом-изготовителем.

Применение процедур снижения ресурсной ресурсоемкости [14] позволило реализовать модель процесса функционирования рассматриваемой системы на ЭВМ с широко распространенными характеристиками.

Заключение

Структурно-логический подход заключается в представлении структуры технологического процесса мультиагентным комплексом операций на основе совокупности универсальных схем. Логика технологического процесса реализуется отношениями между универсальными схемами и системой ограничений.

Мониторинг технологического процесса, модель которого создана с помощью СЛП, заключается в выполнении задач формирования спецификации, синтеза модели, проверки ее адекватности спецификации, верификации модели и непосредственно мониторинга.

Приведенные краткие сведения о практической апробации технологии мониторинга в виде СПО на основе СЛП позволяют сделать вывод о повышении качества мониторинга по сравнению с используемой в настоящее время рекурсивной моделью технологического процесса.

Разработанный СЛП рекомендуется применять при создании СПО мониторинга сложных технологических процессов, содержащих взаимозависимые операции и использующих измерительную информацию для определения траектории своего развития, подлежащих одновременно и временно́му, и событийному контролю.

Литература

1. Майданович О. В. Теория и практика построения автоматизированных систем мониторинга технического состояния космических средств: моногр. / О. В. Майданович, В. А. Каргин, В. В. Мышко и др. СПб.: ВКА им. А. Ф. Можайского, 2011. 219 с.

2. Шмелев В. В. Сравнительный анализ структурно-логического подхода к моделированию технологических процессов функционирования ракетно-космической техники / В. В. Шмелев, М. Ю. Охтилев // Информационно-управляющие системы, 2016, № 5 (84). С. 35-44.

3. Шмелев В. В. Модели технологических процессов функционирования космических средств / В. В. Шмелев // Авиакосмическое приборостроение, 2015, № 4. С. 78-93.

4. Ахметов Р. Н. Концепция создания и применения перспективной АСУ подготовкой и пуском ракеты космического назначения «Союз-2»: новые подходы к интеграции, интеллектуализации, управлению / Р. Н. Ахметов, И. Е. Васильев, В. А. Капитонов и др. // Авиакосмическое приборостроение, 2015, № 4. С. 3-54.

5. Майданович О. В. Комплексная автоматизация мониторинга состояния космических средств на основе интеллектуальных информационных технологий / О. В. Майданович, М. Ю. Охтилев, Б. В. Соколов, Р. М. Юсупов // Прил. к журн. «Информационные технологии», 2011, № 10. 32 с.

6. Куренков В. И. Конструкция и проектирование изделий ракетно-космической техники. Ч. 2. Основы проектирования ракет-носителей / В. И. Куренков. – Самара: Самар. гос. аэрокосмич. ун-т им. С. П. Королева (нац. исслед. ун-т), 2012. 304 с.

7. Котов В. Е. Сети Петри / В. Е. Котов. – Л.: Наука, 1984. 160 с.

8. Westergaard M., Kristensen L. M. The Access/CPN Framework: A Tool for Interacting with the CPN Tools Simulator / M. Westergaard // Proc. of 30th Int. Conf. Appl. and Theory of Petri Nets (Petri Nets 2009). Lecture Notes in Comput. Sci. 5606. Berlin: Springer-Verlag, 2009. P. 313-322.

9. Jensen K. Coloured Petri Nets and CPN Tools for Modelling and Validation of Concurrent Systems / K. Jensen, L. M. Kristensen, L. Wells // Int. J. Software Tools for Technol. Transfer (STTT), 2007, № 9 (3-4). P. 213-254.

10. Ratzer A. V. CPN Tools for Editing, Simulating, and Analysing Coloured Petri Nets / A. V. Ratzer, L. Wells, H. M. Lassen, M. Laursen et al. // Proc. of 24th Int. Conf. Appl. and Theory of Petri Nets (Petri Nets 2003). Lecture Notes in Comput. Sci. 2679. Berlin: Springer-Verlag, 2003. P. 450-462.

11. Охтилев М. Ю. Основы теории автоматизированного анализа измерительной информации в реальном времени. Синтез системы анализа: моногр. / М. Ю. Охтилев. – СПб.: ВКА им. А. Ф. Можайского, 1999. 162 с.

12. Clarke E. M. Model Checking / E. M. Clarke, O. Grumberg, D. Peled // MIT Press, 1999. 314 p.

13. Лескин А. А. Сети Петри в моделировании и управлении / А. А. Лескин, П. А. Мальцев, А. М. Спиридонов. – Л.: Наука, 1989. 133 с.

14. Шмелев В. В. Вычислительная ресурсоемкость сетевой модели обработки и анализа измерительной информации ракеты-носителя «Союз-2» / В. В. Шмелев, Ю. С. Мануйлов // Информация и космос, 2016, № 1. С. 155-161.

Method for Monitoring the Technological Processes in the Aerospace Industry on the Basis of Structural and Logical Approach

Shmelev V. V.
Military Space Academy named Mozhaiskogo
St. Petersburg, Russia
valja1978@yandex.ru

Annotation. **This article contains the original structural and logical approach to modeling processes. As an initial description of the process used by its specification, to which are conventional ways of describing process. The approach comprises the steps of synthesis model adequacy test its prototype, the model verification and directly monitoring process using a synthetic model. The approach is different modeling capacity, fully corresponding domain processing and analysis of measurement information of missile technology. Brief information on the practical testing of the approach, showing its advantage over currently used in the practice approach based on recursive model.**

Keywords: **rocket and space technology, process monitoring, structural and logical approach, recursive process model, process modeling, Petri net, multiagent approach to modeling.**

References

1. Maidanovich O. V., Kargin V. A., Myshko V. V., Okhtilev M. Iu., Sokolov B. V. Theory and Practice of Building Automated Systems for Monitoring the Technical Condition of Space Vehicles [Teoriia i praktika postroeniia avtomatizirovannykh sistem monitoringa tekhnicheskogo sostoianiia kosmicheskikh sredstv]: monogr. St. Petersburg, Military Space Academy named Mozhaiskii, 2011. 219 p.

2. Shmelev V. V., Ohtilev M. Yu. Comparative Analysis of Structural and Logical Approach to the Modeling of Processes of Functioning of Rocket and Space Technology [Sravnitel'nyj analiz strukturno-logicheskogo podhoda k modelirovaniyu tekhnologicheskih processov funkcionirovaniya raketno-kosmicheskoj tekhniki], *Information and Control Systems [Informacionno-upravlyayushchie sistemy]*, 2016, no. 5 (84), pp. 35-44.

3. Shmelev V. V. Models of Processes of Functioning of Space Assets [Modeli tekhnologicheskih processov funkcionirovaniya kosmicheskih sredstv], *Aerospace Instrument [Aviakosmicheskoe priborostroenie]*, 2015, no. 4, pp. 78-93.

4. Akhmetov R. N., Vasil'ev I. E., Kapitonov V. A., Okhtilev M. Iu., Sokolov B. V. Concept Creation and Application of Promising Automation Training and Start-up Space Purposes "Soyuz-2" Missiles, New Approaches to the Integration of Intellectualization, the Management [Kontseptsiia sozdaniia i primeneniia perspektivnoi ASU podgotovkoi i puskom rakety kosmicheskogo naznacheniia «Soiuz-2»: novye podkhody k integratsii, intellektualizatsii, upravleniiu]. *Aerospace Instrument [Aviakosmicheskoe priborostroenie]*, 2015, no. 4, pp. 3-54.

5. Maidanovich O. V., Okhtilev M. Iu., Sokolov B. V., Iusupov R. M. Integrated Automation of Monitoring the Status of Space Assets on the Basis of Intelligent Information Technologies [Kompleksnaia avtomatizatsiia monitoringa sostoianiia kosmicheskikh sredstv na osnove intellektual'nykh informatsionnykh tekhnologii], *Supplement to the Information Technology [Prilozhenie k zhurnalu Informatsionnye tekhnologii]*, 2011, no. 10, 32 p.

6. Kurenkov V. I. Design and Engineering Space Engineering. Part 2: Fundamentals of Rockets [Konstrukciya i proektirovanie izdelij raketno-kosmicheskoj tekhniki. Chast' 2. Osnovy proektirovaniya raket-nositelej], Samara, Samar. gos. aehrokosm. un-t im. S. P. Koroleva (nac. issled. un-t), 2012, 304 p.

7. Kotov V. E. Petri Nets [Seti Petri], Leningrad, Nauka, 1984, 160 p.

8. Westergaard M., Kristensen L. M. The Access/CPN Framework: A Tool for Interacting with the CPN Tools Simulator. *Proc. of 30th Int. Conf. Appl. and Theory of Petri Nets (Petri Nets 2009). Lecture Notes in Comput. Sci*. 5606, Berlin, Springer-Verlag, 2009, pp. 313-322.

9. Jensen K., Kristensen L. M., Wells L. Coloured Petri Nets and CPN Tools for Modelling and Validation of Concurrent Systems. *Int. J. Software Tools for Technol. Transfer* (STTT), 2007, no. 9 (3-4), pp. 213-254.

10. Ratzer A. V., Wells L., Lassen H. M., Laursen M., Qvortrup J. F., Stissing M. S., Westergaard M., Christensen S., Jensen K. CPN Tools for Editing, Simulating, and Analysing Coloured Petri Nets, *Proc. of 24th Int. Conf. Appl. and Theory of Petri Nets (Petri Nets 2003). Lecture Notes in Comput. Sci. 2679*, Berlin, Springer-Verlag, 2003, pp. 450-462.

11. Okhtilev M. Iu. Basic Theory of the Automated Analysis of the Measuring Data in Real Time. Synthesis Analysis [Osnovy teorii avtomatizirovannogo analiza izmeritel'noi informatsii v real'nom vremeni. Sintez sistemy analiza], St. Petersburg, Military Space Academy named Mozhaiskii, 1999, 162 p.

12. Clarke E. M., Grumberg O., Peled D. Model Checking, MIT Press, 1999. 314 p.

13. Leskin A. A., Mal'cev P. A., Spiridonov A. M. Petri Nets in Modeling and Management [Seti Petri v modelirovanii i upravlenii], Leningrad, Nauka, 1989, 133 p.

14. Shmelev V. V., Manuilov Iu. S. Computer Network Resource Consumption Model Measuring Data Processing and Analysis of Carrier Rocket "Soyuz-2" [Vychislitel'naia resursoemkost' setevoi modeli obrabotki i analiza izmeritel'noi informatsii rakety-nositelia «Soiuz-2»], *Information and Space [Informatsiia i kosmos]*, 2016, no. 1, pp. 155-161.

An Integrated Approach to Navigation of Mobile Devices Indoors Based on Wi-Fi and Image Objects

Erin A. A., Khomonenko A. D.
Emperor Alexander I Petersburg State Transport University
St. Petersburg, Russia
alexey.erin94@gmail.com, khomon@mail.ru

Abstract. **An approach to navigation of mobile devices indoors using artificial neural networks to determine location by comparing photographs of the premises taken by the user with images of the premises in the database is proposed. A comparison with existing models of indoor navigation is fulfilled. An example of a neural network for the chosen model and its complexity is given. An example of generation of an optimal route using algorithm Dijkstra, on the basis of the premises of the Department "Computing systems" of Emperor Alexander I Petersburg State Transport University is given.**

Keywords: **Artificial neural networks, indoor navigation, image moment invariants, Dijkstra's algorithm, Wi-Fi.**

Introduction

Currently, mobile devices are widely used for the various governmental purposes. One of the main features offered by mobile devices is navigation. The optimal route to your destination, the accommodation, the search for alternative paths – all this greatly facilitates modern life. However, many modern navigation methods are unsuitable for indoor navigation. Buildings have complex infrastructure, many buildings consist of several buildings, and often quite difficult to quickly navigate and find the right room. For these reasons, the development of navigation of mobile devices within the premises is an urgent task.

To date, the main technology used for navigation is the global navigation satellite system GPS/GLONASS [1]. Beacons GPS is built into nearly all mobile devices and with them in power is determined by the location of the device on the ground, laid the routes of long distances, etc. However, they will not be able to navigate inside, because the density and the materials from which made the building, greatly reduce the location accuracy that space is critical, and with their help it is impossible to determine on which floor the user device.

Therefore, for implementation of indoor navigation other technologies are used [2]. One of the technologies used to implement indoor navigation technology is a Wi-Fi wireless data transmission. With the help of trained Wi-Fi network can determine the location of the device on the floor plan and control movement along the route [3].

The main tasks that need to be addressed when implementing the navigation of mobile devices within the premises are: search device location on the plan of the building, a route from the start point to the end, follow-up monitoring device according to the route.

This article considers the existing methods of navigation for mobile devices indoors, as well as proposes an alternative method indoor navigation based on finding a location using photo comparison areas.

Existing navigation model of mobile devices indoor

Currently, there are several models of navigation of mobile devices indoors [4]. Consider two models that use Wi-Fi to determine the location of the mobile device.

The *first model* is based on measuring the signal strength from the source to the customer and its subsequent processing. The first stage of this model is to determine the signal strength RSSI from the source. The value of RSSI is defined as

$$RSSI = -10 \cdot n \cdot \log(d) + A,$$

where d is the distance, A is the transmitter power, n is the propagation constant of the signal. However, due to the physical properties of waves and other factors, this formula does not give sufficient accuracy, so, to calculate the distance according to the value of the force signal is used model of attenuation:

$$P(r)_{dBm} = P(r_0)_{dB} + 10 \cdot n \cdot \log \frac{r_0}{r},$$

where $P(r)_{dBm}$ is the value of RSSI on the distance r, n is the attenuation coefficient, r is the distance from the device to the transmitter, the distance from the device to the point where the measurement was carried out signal strength $P(r_0)_{dB}$ [5, 6].

After was produced by measuring distances, it becomes possible to build a geometric solution of the problem of positioning using triangulation graphs.

The *second model* is used artificial neural network to memorize the configuration of the premises and the subsequent recognition of the premises as visible in them signals [7–9]. At the training stage, a map of the room based on radio fingerprints, performed physical collecting radio fingerprint for each point. Then all the collected radio-prints and additional information about each point are combined into one file for training a neural network. After this occurs the training of the neural network.

The finished app works on the following principle: the user includes beacon Wi-Fi, collect radio fingerprints Wi-Fi hotspots to which the device can connect, the imprint is sent to the trained neural network, which determines where the user is located, by comparing the received data from the card and finding the closest values. Thus, determined by the most probable Wi-Fi access point, which is about the user.

Model indoor navigation, image-based and Wi-Fi network

Both models are considered based on the use of Wi-Fi networks to determine location of the device. However, the location accuracy via Wi-Fi network is affected by many factors, such as interference from devices operating on the same frequency; the obstacles that weaken signal strength and others. Therefore, alternatively, determining the initial location of the device we proposed to use the mechanism of comparison of photographs of the premises taken by the user.

The main idea of this method consists in using a mathematical model of an artificial neural network to determine the location of a mobile device made device pictures. It then executes the further building of the route from the starting location, on the photos to the end point selected by the user. To control the advance of the mobile device on the specified route uses a Wi-Fi network. Applied positioning method for assessing the signal strength of nearby access points Wi-Fi.

The software package consists of two components:

• a mobile application on the user's device, which carries out the survey of the premises, sends the image and the start location information about ending point of the route to the server, displays the constructed route to the user and monitors the progress on the route;

• the server where the database stores the image space, with their description and associated with PLA-us buildings and building plans in the form of graphs, and a server application that searches images using artificial neural network and builds the route.

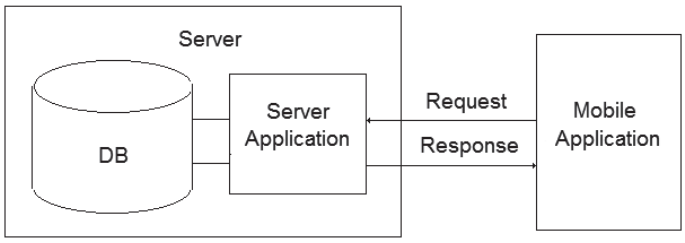


Fig. 1. Architecture of the software

The algorithm works mobile application

With the help of mobile applications having access to the device camera, the user photographs the room in which it is located and from which wants to route. The user then selects the end point of the route, a list with most places, the treatment, or noting the location on the floor plan, either by entering the room number or name in a search target row, then select. The resulting image and information about the endpoint sent to the server, where the processing and the construction of marsh root.

After a response received from server, building plan with marked on it the route displayed on the user's screen. Control of the movement route is via Wi-Fi module of the device. The Wi-Fi module in the background scans the network, receiving information about signal strength of Wi-Fi hotspots in the area which was hit by the device. Based on the information received, the application makes a conclusion in which the route point is a device and controls the correct route.

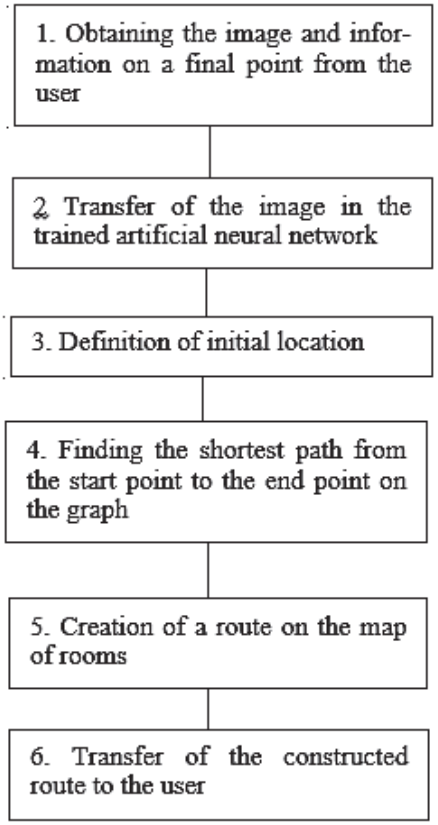


Fig. 2. The algorithm works mobile application

Using moment invariants of images

In many tasks of digital image processing has found a broad application of the torque characteristics of the images and counting them on the basis of moment invariants. The invariant is a value that remains unchanged under certain transformations. The invariant moments have become an essential tool for recognizing patterns irrespective of their particular position, orientation, viewing angle and other changes. The main advantage of moment invariants are insensitive to their rotation. This makes their use effective as features in the task of detection and recognition of image objects with an arbitrary orientation [10, 11].

In practice, recognizable images differ from each other appearance scale, rotation, and shear. For images of the same class in most of these cases come from the fact that a recognizable image was the result of a geometric transformation (scaling, rotation in the XY-plane and cyclic shift). If you consistently perform all the possible geometric transformation of the image and to compare the conversion result with a recognizable way, it is possible to register the parameters of the transformation, in which occurs the highest value of measures of similarity [11].

The invariant moments are the characteristics of the image based on exponential moments and describing the silhouette of an object. In accordance with its name, these features are invariant to affine transformations of the image. For processing digital images are discrete analogs of the torque characteristics. The formula for the moment of order (k, s) is written as follows [10]:

$$\mu_{ks} = \int_{-\infty}^{\infty}\int_{-\infty}^{\infty} m^k n^s x(m,n),\ k,s = 0,1,... \qquad (1)$$

Typically, in pattern recognition are used by the Central points having invariance to image shift. The corresponding Central moment is given by the formula:

$$\mu_{ks} = \int_{-\infty}^{\infty}\int_{-\infty}^{\infty} (m-\overline{m})^k (n-\overline{n})^s x(m,n)dmdn,\ k,s = 0,1,.. \qquad (2)$$

where: $\overline{m} = m_{10}/m_{00}; \overline{n} = m_{01}/m_{00}$ are the coordinates of the center of gravity of the image. Central moments (2) expressed via moments (1) using the ratio:

$$\mu_{ks} = \sum_{i=0}^{k}\sum_{j=0}^{s} (-1)^{i+j} C_k^i C_s^j \overline{m}^{k-i} \overline{n}^{s-j} t_{ij}, \qquad (3)$$

where C_k^i – binomial coefficients. For centered image values of the moments (1) and (2) coincide. Of Central moments (2) can be normalized to provide invariance to image scaling. Using the Central moments defined by features, invariant to image rotation (torque invariants). Having a set of characteristics, you can define the following seven invariant moments.

$$\varphi_1 = \mu_{20} + \mu_{02},$$

$$\varphi_2 = (\mu_{20} + \mu_{02})^2 + 4\mu_{11}^2,$$

$$\varphi_3 = (\mu_{30} + 3\mu_{12})^2 + (3\mu_{21} - \mu_{03})^2,$$

$$\varphi_4 = (\mu_{30} + 3\mu_{12})^2 + (\mu_{21} - \mu_{03})^2,$$

$$\varphi_5 = (\mu_{30} + 3\mu_{12})(\mu_{30} + \mu_{12})[(\mu_{30} + \mu_{12})^2 - 3(\mu_{21} + \mu_{03})^2] + (3\mu_{21} - \mu_{03})(\mu_{21} + \mu_{03}) \times [3(\mu_{30} + \mu_{12})^2 - (\mu_{21} + \mu_{03})^2],$$

$$\varphi_6 = (\mu_{20} + \mu_{02})[(\mu_{30} + \mu_{12})^2 - (\mu_{21} + \mu_{03})^2] + 4\mu_{11}(\mu_{30} - \mu_{12})(\mu_{21} + \mu_{03}),$$

$$\varphi_7 = (3\mu_{21} + \mu_{03})(\mu_{30} + \mu_{12})[(\mu_{30} + \mu_{12})^2 - 3(\mu_{21} + \mu_{03})^2] - (\mu_{30} - 3\mu_{12})(\mu_{21} + \mu_{03}) \times [3(\mu_{30} + \mu_{12})^2 - (\mu_{21} + \mu_{03})^2].$$

These seven moments are invariant to shifts, rotations, axial symmetries, and strains and compressions [11]. In General, they are nonlinear combinations of Central moments, which are, in turn, functions of the geometric (initial) moments.

To assess the computational complexity of the invariants it is necessary to calculate the number of operations multiplications and summations when computing the invariants [12]. Formula for calculation:

$$Q_{\text{ум}}(\varphi) = \sum_{j=1}^{J} Q_{\text{ум}}(\mu_{pjqj}) + \alpha + \beta + (\gamma - 1), \qquad (4)$$

$$Q_{\text{сл}}(\varphi) = \sum_{j=1}^{J} Q_{\text{сл}}(\mu_{pjqj}) + (\delta - 1), \qquad (5)$$

were $Q_{\text{ум}}(\mu_{pjqj})$, $Q_{\text{сл}}(\mu_{pjqj})$ is number of multiplications and additions at calculation of the moment entering functionality; J – amount of the moments entering functionality of an invariant φ; α – number of the multipliers which are subject to data in the second degree; β – number of the multiplications spent for multiplication of the moments (or their sums) on constant coefficient which module isn't equal to 1.

Calculation of computing complexity of invariants which results are taken out in table 1 is given in article [12].

Thus, it is possible to draw a conclusion that computing complexity increases in process of increase in an order of a moment invariant, computing complexity of an invariant depends on number of the moments entering functionality of an invariant and computing expenses are proportional to the image sizes.

Using of neural network for comparison of photos

For information search about the room in the image it is offered to use artificial neural network. As one of the main properties of the photo is quality and not each device is capable to take the high-quality picture of the room, in order that there was an opportunity to find the necessary room according to the taken picture of any quality, it is offered to use neural network of Hopfild [13, 14].

As the neural network of Hopfild is applied generally to recovery of noisy images, it has to level quality of the taken picture. The neural network of Hopfild consists of N artificial neurons; the axon of each neuron is tied with dendrites of other neurons, forming feedback. Each neuron can be in one of two states:

$$x(t) \in \{-1; 1\},$$

where $x(t)$ is a condition of neuron at the time of t. Corresponds to "excitement" of neuron +1, and to "braking"-1. Dynamics of a state in time i-oho of neuron in network from N neurons is described by discrete dynamic system:

$$x_i(t) = sign\left[\sum_{j=1, j\neq i}^{N} w_{ij} x_i(t-1)\right], i, j \in 1, ..., N,$$

Table 1

Computing complexity of invariants

Invariant	Number of multiplications $Q_{\text{ум}}(\varphi_i)$	Number additions $Q_{\text{сл}}(\varphi_i)$	Relative number of multiplications $\overline{Q}_{\text{ум}}(\varphi_i)$	Relative number of additions $\overline{Q}_{\text{сл}}(\varphi_i)$	Full expenses $Q(\varphi_i)$	Relative full expenses $\overline{Q}(\varphi_i)$
φ_1	24	5	1	1	29	1
φ_2	43	8	1,8	1,6	51	1,76
φ_3	104	19	4,33	3,8	123	4,24
φ_4	102	19	4,25	3,8	121	4,17
φ_5	112	27	4,66	5,4	139	4,79
φ_6	146	30	6,1	6	176	6,1
φ_7	112	27	4,66	5,4	139	4,79

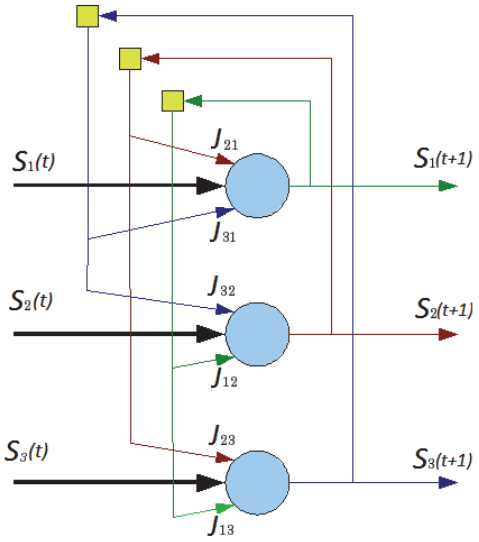


Fig. 3. Structure of Hopfield network

where w_{ij} is weight coefficient between neurons of i and j, $x_j(t-1)$ are values of exits of neuron of j in the previous time point [14].

Training of network of Hopfild in output images comes down to calculation of values of elements of a matrix w_{ij}. It is formally possible to describe training process as follows: let it is necessary to train neural network to distinguish the M images designated $\{X_\mu^{in}, \mu = 1,...,M\}$. The entrance image represents:

$$\overline{X_\mu^{in}} = X_\mu^{in} + \varepsilon,$$

where ε – the noise imposed on an initial image.

Calculation of a square matrix of scales is made by the Hebb rule:

$$W_{ij} = \frac{1}{N}\sum_{\mu=1}^{M}[x_{i\mu}^{in} \cdot x_{j\mu}^{in}].$$

Training of a neural network is made on the images which are stored in the database on the server that further the trained neural network could define to what image there corresponds the taken picture.

As an example the neural network of Hopfild capable to recognize to what image which is stored in memory of a network is realized there corresponds the image transferred to processing. At the moment the network is capable to work with black-and-white images of a format 50×50. In case of such format the one-layer network of Hopfild has 2500 neurons which accept one or the other values {–1; 1}. The realized network showed the following results provided in table 2.

Table 2

Temporary characteristics of neural network

	Time of processing of the image, s	Time of network training, s	Time of recognition of the normal image, s	Time of recognition of the noisy image, s
20 the training examples, 50×50 in size	4,8	96	5,2	5,8

At the same time if in the training set there were no strongly similar images, then the network recognized all usual images correctly, and noisy if they have been distorted less than for 35 % that all are distinguished correctly, at a strong noisiness the network could make a mistake. If in the training set there were several similar images, then the network could recognize the image incorrectly.

Creation of the route on the column

Having defined starting and ending point of a route, it is necessary to lay out a route. Building plans are stored in the database on the server in the form of a nonoriented graph. Trailing peaks are finite locations, remaining peaks are other locations, and edges of a graph – transitions and corridors between locations. Lengths of edges are lengths of the appropriate routes. As weight of edges – is non-negative, and throughput isn't important, for a route spacer that is search of the shortest way in the graph, Dijkstra's algorithm is used [15].

Dijkstra's algorithm finds the shortest ways from one of the count's tops to all others. The algorithm works only for counts without edges of negative weight. The algorithm works step by step – on each step he "visits" one top and tries to reduce tags. Work of an algorithm comes to the end when all tops are visited [15–17].

Initialization. The tag of the top of *a* necessary equal 0, tags of other tops – infinity. It reflects that distances from top *a* to other tops are still unknown. All tops of the count are marked as not visited.

Algorithm step. If all tops are visited, the algorithm comes to the end. Otherwise, u top having the minimum tag gets out of yet not visited tops. We consider various routes in which top *u* are penultimate point. We will call tops in which conduct edges from u neighbors of this top. For each neighbor of top of *u*, we will consider the new length of a way equal to the sum of values of the current tag of *u* and length of the edge connecting u to this neighbor. If the received value of length is less than value of a tag of the neighbor, we will replace value of a tag with the received value of length. Having considered all neighbors, we will mark *u* top as visited and we will repeat an algorithm step.

As an example of work of an algorithm the count corresponding to premises of "Information and Computing Systems" department of PGUPS, presented in fig. 4 has been constructed.

Lengths of routes of the count decide on the help of the following matrix of the weights.

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17
1	–	4	6	9	–	5	12	5	–	–	–	–	–	–	–	–	–
2	4	–	4	6	–	7	9	3	–	–	–	–	–	–	–	–	–
3	6	4	–	4	–	9	6	5	–	–	–	–	–	–	–	–	–
4	9	6	4	–	–	11	3	7	–	–	–	–	–	–	–	–	–
5	–	–	–	11	–	–	3	–	–	–	–	–	–	–	–	–	–
6	5	7	9	3	–	–	15	10	–	–	–	45	65	–	–	–	62
7	12	9	6	7	3	15	–	8	–	–	5	12	–	–	–	–	–
8	5	3	5	–	–	10	8	–	3	3	–	–	–	–	–	–	–
9	–	–	–	–	–	–	–	3	–	–	–	–	–	–	–	–	–
10	–	–	–	–	–	–	–	3	–	–	–	–	–	–	–	–	–

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17
11	–	–	–	–	–	–	5	–	–	–	–	8	–	–	–	–	–
12	–	–	–	–	–	45	12	–	–	–	8	–	15	–	–	–	–
13	–	–	–	–	–	65	–	–	–	–	–	15	–	10	8	10	10
14	–	–	–	–	–	–	–	–	–	–	–	–	10	–	4	6	–
15	–	–	–	–	–	–	–	–	–	–	–	–	8	4	–	4	–
16	–	–	–	–	–	–	–	–	–	–	–	–	10	6	4	–	–
17	–	–	–	–	–	62	–	–	–	–	–	–	10	–	–	–	–

Example of the algorithm: it is necessary to find all the shortest routes leading from vertex 1. The starting vertex from which the tree of shortest paths is constructed is vertex 1. Set the starting conditions: $d(1) = 0$, $d(x) = \infty$. We find the nearest vertex to the starting point, using the formula: $d(x) = \min\{d(x); D(y) + ay, x\}$:

$d(2) = \min\{–;0+4\} = 4$
$d(3) = \min\{–;0+6\} = 6$
$d(4) = \min\{–;0+9\} = 9$
$d(6) = \min\{–;0+5\} = 5$
$d(7) = \min\{–;0+12\} = 12$

Mark the corresponding vertices with new weights, select the nearest smallest vertex and add the corresponding arc, as the shortest path to this vertex. In this case, vertex 2 and arc (1,2).

Repeat the step of the algorithm, now for vertex 2.

$d(3) = \min\{6;4+4\} = 6$
$d(4) = \min\{9;4+6\} = 9$
$d(6) = \min\{5;4+7\} = 5$
$d(7) = \min\{12;4+9\} = 12$

The weights of the vertices have not changed, therefore, take the next smallest vertex 6 and write its arc (1.6).

Repeat the algorithm steps until all vertices are visited.

As a result, we obtain a table with all shortest routes from vertex 1.

Conclusion

In article the developed model for navigation of mobile devices in locations is provided, reasons for use of the selected technologies are given, information on the necessary software is provided.

On this basis the program complex realizing the developed navigation model is developed.

Table 3

Resulting table of the shortest routes

№ of tops	Shortest route	№ of tops	Shortest route
2	1–2	10	1–8-10
3	1–3	11	1–7-11
4	1–4	12	1–7-12
5	1–7-5	13	1–7-12–13
6	1–6	14	1–7-12–13–14
7	1–7	15	1–7-12–13–15
8	1–8	16	1–7-12–13–16
9	1–8-9	17	1–7-12–13–17

Further researches are supposed to be continued in the following directions on development of a program complex:

• improving of a neural network that the neural network could recognize color images of the big sizes;

• improving of system of a choice of finite location in the form of adding of an alternative possibility of an interactive choice of finite location on a building card;

• transfer of a mobile application on other operating systems, with the purpose to increase target audience.

• adding of a possibility of support of following along a route by means of network Wi-Fi.

References

1. Serapinas B. B. Global Positioning Systems: study guide [Global'nye sistemy positsionirovaniya: uchebnoye posobiye], Moscow, 2002. 106 p.

2. Yakovenko I. A. Indoor Navigation. Overview and Comparative Analysis of Technologies: GSM, Bluetooth, Wi-Fi, GPS, RFID, NFC [Navigatsiya vnutri pomeshcheniy. Obzor i sravnitelniy analiz tekhnologiy: GSM, Bluetooth, Wi-Fi, GPS, RFID, NFC], *Youth scientific and technical bulletin* [*Molodezhniy nauchno-tekhnicheskiy vestnik*], 2015, no. 6.

3. Evennou F., Marx F. Advanced Integration of WiFi and Inertial Navigation Systems for Indoor Mobile Positioning, *EURASIP J. on Applied Signal Proc*., 2006, Article ID 86706, pp. 1-11.

4. Ovsyannikov A. A., Novikov P. A. Implementation of the Indoor Navigation Algorithm Based on Bluetooth Low Energy 4.0. Technology [Modeli realizatsii navigatsii vnutri pomesh-

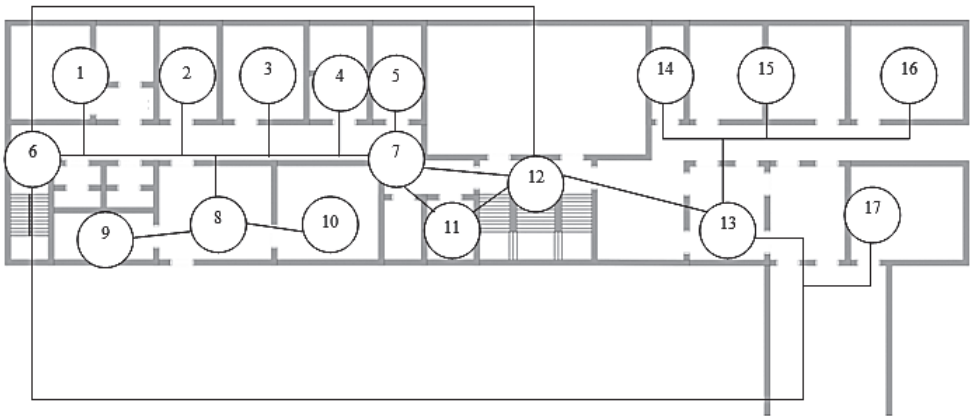


Fig. 4. The count corresponding to the map of rooms

cheniy pri pomoshchi analiza besprovodnikh istochnikov dannykh], *Computer Tools in Education* [*Kompyuternye instrumenty v obrazovanii*], 2015, no. 4, pp. 37-51.

5. Srinivasan K., Levis Ph. RSSI is Under Appre-ciated. Available at: https://sing.stanford.edu/pubs/rssi-emnets06.pdf (accessed 24 April 2017).

6. Park J. J., Yang L. T., Lee C. Future Information Technology, *6th Int. Conf. Future Inform. Technol.*, *FutureTech* 2011, Crete, Greece, June 28-30, 2011. Proc. Springer, 2011, pp. 89-90.

7. Mok E., Cheung Bernard K. S. An Improved Neural Network Training Algorithm for Wi-Fi Fingerprinting Positioning, *ISPRS Int. J. Geo-Inf*, 2013, no. 2, pp. 854-868.

8. Novikov P. A., Khomonenko A. D., Yakovlev E. L. Software for Mobile Indoor Navigation using Neural Networks [Kompleks programm dlya navigatsii mobilnikh ustroystv vnutri pomeshcheniy s pomoshchi neironnykh setey], *Information and Control Systems [Informatsionno-upravlyayushchie sistemy]*, 2016, no. 1 (80), pp. 32-39.

9. Novikov P. A., Khomonenko A. D., Yakovlev E. L. Justification of the choice of neural networks learning algorithms for indoor mobile positioning, *Proc. CEE-SECR '15 Proc. 11th Central & Eastern European Software Eng. Conf. Russia Article*, no. 9. NY, ACM, 2015.

10. Glumov N. I. The Construction and Application of Moment Invariants for Image Processing in a Sliding Window [Postroenie i primenenie momentnikh invariantov dlya obrabotki izobrazheniy v skolzyashchem okne], *KO*, 1995, no. 1, pp. 14-15. Available at: http://cyberleninka.ru/article/n/postroenie-i-primenenie-momentnyh-invariantov-dlya-obrabotki-izobrazheniy-v-skolzyaschem-okne (accessed 13 March 2017).

11. Gonzalez R. C., Woods R. E., Steven L. Eddins Digital Image Processing Using MATLAB [Tsifrovaya obrabotka izobrazheniy v srede Matlab], Moscow, Tekhnosfera, 2006, 616 p.

12. Medvedik A. D., Verchenko V. A., Babak P. E. Evaluation of the Computational Complexity of Moment Invariants Used in Pattern Recognition Problems [Otsenka vichislitelnoy slozhnosti momentnikh invariantov, ispolzuemykh v zadachakh raspoznavaniya], *Radioelectronic and Computer Systems* [*Radioelektronnye i comp'yuternye sistemy*], 2015, no. 4 (74), pp. 124-130.

13. Kruglov V. V., Borisov V. V. Artificial Neural Networks. Theory and Practice [Iskusstvennye neyronnye seti. Teoriya i praktika], Moscow, Goryachaya Liniya Telekom, 2002, 382 p.

14. Wasserman Ph. D. Neural Computing. Theory and Practice [Neirokompyuternaya tekhnika: teoriya i praktika], Moscow, Mir, 1992, 240 p.

15. Cormen T. H., Leiserson Ch. E., Rivest R. L., Stein C. Introduction to Algorithms [Algoritmy: postroyenie i analiz], Moscow, Vilyams, 2006, 1296 p.

16. Levitin A. V. Algoritmy. Algorithms. Introduction to Development and Analysis [Vvedenie v razrabotku i analiz], Moscow, Vilyams, 2006, 576 p.

17. Asanov M. O., Baranskiy V. A., Rasin V. V. Discrete Mathematics: Graphs, Matroids, Algorithms [Diskretnaya matematika: grafy, matroidy, algoritmy], Izhevsk, NITS "Regularnaya i khaoticheskaya dinamika", 2001, 288 p.

Комплексный подход к навигации мобильных устройств внутри помещений на основе Wi-Fi и изображений объектов

Ерин А. А., Хомоненко А. Д.
Петербургский государственный университет путей сообщения Императора Александра I
Санкт-Петербург, Россия
alexey.erin94@gmail.com, khomon@mail.ru

Аннотация. **Предлагается подход к навигации мобильных устройств внутри помещений с использованием искусственной нейронной сети для определения местоположения путем сравнения фотографий помещения, сделанных пользователем с изображениями помещений в базе данных. Проводится их сравнение с существующими моделями навигации внутри помещений. Рассматривается пример нейронной сети для выбранной модели и его трудоемкость. Приводится пример построения оптимального маршрута с помощью алгоритма Дейкстры на основе помещений кафедры «Информационно вычислительные системы» Петербургского государственного университета путей сообщения Императора Александра I.**

Ключевые слова: **искусственные нейронные сети, навигация внутри помещений, инварианты моментов изображений, алгоритм Дейкстры, Wi-Fi.**

Литература

1. Серапинас Б. Б. Глобальные системы позиционирования: учеб. пособие / Б. Б. Серапинас. М.: Каталог, 2002. 106 с.

2. Яковенко И. А. Навигация внутри помещений. Обзор и сравнительный анализ технологий: GSM, Bluetooth, Wi-Fi, GPS, RFID, NFC / И. А. Яковенко // Молодеж. науч.-технич. вестн., 2015, № 6.

3. Evennou F. Advanced Integration of WiFi and Inertial Navigation Systems for Indoor Mobile Positioning / F. Evennou, F. Marx // EURASIP J. on Applied Signal Proc., 2006. Article ID 86706, p. 1-11.

4. Овсянников А. А. Модели реализации навигации внутри помещения при помощи анализа беспроводных источников данных / А. А. Овсянников, П. А. Новиков // Компьютерные инструменты в образовании, 2015, № 4.

5. Srinivasan K. RSSI is Under Appreciated / K. Srinivasan, Ph. Levis. URL: https://sing.stanford.edu/pubs/rssi-emnets06.pdf (дата обращения 24.04.2017).

6. Park J. J. Future Information Technology / J. J. Park, L. T. Yang, C. Lee // 6th Int. Conf. on Future Inform. Technol., Future Tech 2011, Crete, Greece, June 28-30, 2011. Proc. Springer, 2011, pp. 89-90.

7. Mok E. An Improved Neural Network Training Algorithm for Wi-Fi Fingerprinting Positioning / E. Mok, B. K. S. Cheung // ISPRS Int. J. Geo-Inf, 2013, № 2. P. 854-868.

8. Новиков П. А. Комплекс программ для навигации мобильных устройств внутри помещений с помощью нейронных сетей / П. А. Новиков, А. Д. Хомоненко, Е. Л. Яковлев // Информационно-управляющие системы, 2016, № 1 (80). С. 32-39.

9. Novikov P. A. Justification of the choice of neural networks learning algorithms for indoor mobile positioning / P. A. Novikov, A. D. Khomonenko, E. L. Yakovlev // Proc. CEE-SECR '15 Proc. 11th Central & Eastern European Software Eng. Conf. in Russia Article № 9. NY: ACM, 2015.

10. Глумов Н. И. Построение и применение моментных инвариантов для обработки изображений в скользящем окне / Н. И. Глумов // КО, 1995, № 1. С. 14-15.

11. Гонсалес Р. Цифровая обработка изображений в среде Matlab / Р. Гонсалес, Р. Вудс, Р. Эддинс. М.: Техносфера, 2006. 616 с.

12. Медведик А. Д. Оценка вычислительной сложности моментных инвариантов, используемых в задачах распознавания / А. Д. Медведик, В. А. Верченко, П. Е. Бабак // Радиоэлектронные и компьютерные системы, 2015, № 4(74). С. 124-130.

13. Круглов В. В. Искусственные нейронные сети. Теория и практика / В. В. Круглов, В. В. Борисов. М.: Горячая линия-Телеком, 2002. 382 с.

14. Уоссермен Ф. Нейрокомпьютерная техника: Теория и практика / Ф. Уоссермен. М.: Мир, 1992. 240 с.

15. Кормен Т. Х. Алгоритмы: построение и анализ / Т. Х. Кормен, Ч. И. Лейзерсон, Р. Л. Ривест, К. Штайн. 2-е изд. М.: Вильямс, 2006. 1296 с.

16. Левитин А. В. Алгоритмы. Введение в разработку и анализ / А. В. Левитин. М.: Вильямс, 2006. 576 с.

17. Асанов М. О. Дискретная математика: графы, матроиды, алгоритмы / М. О. Асанов, В. А. Баранский, В. В. Расин. Ижевск: НИЦ «Регулярная и хаотическая динамика», 2001. 288 с.

Сравнение протоколов динамической маршрутизации IS-IS и OSPF

Шардаков К. С., Корбаков А. И., Красновидов А. В.
Петербургский государственный университет путей сообщения Императора Александра I
Санкт-Петербург, Россия
k.shardakov@gmail.com, alexvalet@list.ru, alexkrasnovidow@mail.ru

Аннотация. **В данной статье рассмотрены два протокола динамической маршрутизации: IS-IS (Intermediate-System-to-Intermediate-System) и OSPF (Open Shortest Path First). Выявлены сходства и различия между ними. Описана используемая протоколами терминология, различия в дизайне сети. Смоделирована инфокоммуникационная сеть для измерения объёма генерируемого служебного трафика протоколов.**

Ключевые слова: **OSPF, IS-IS, сеть, топология, динамическая маршрутизация, архитектура сети, трафик, алгоритм Дейкстры.**

Введение

В настоящее время широко используются различные протоколы динамической маршрутизации: BGP (Border Gateway Protocol), OSPF, IS-IS и другие. Все они делятся на две большие группы: протоколы внешней маршрутизации EGP (Exterior Gateway Protocol) и внутренней маршрутизации IGP (Interior Gateway Protocol).

Основная задача протоколов динамической маршрутизации – автоматический поиск лучшего маршрута на основании некоторых атрибутов для передачи трафика по сети [1]. Например, протоколы динамической маршрутизации помогают эффективно использовать резервные каналы связи, избегая петель маршрутизации.

В статье рассматриваются несколько IGP, такие как OSPF и IS-IS, представлена их сравнительная характеристика, предложены рекомендации по выбору протокола. Оба протокола основаны на технологии отслеживания состояния канала и используют алгоритм Дейкстры для поиска кратчайшего пути.

OSPF (Open Shortest Path First) – иерархический протокол, был разработан организацией IETF (Internet Engineering Task Force, инженерный совет Интернета). Разработка протокола OSPF началась в 1987 г., сегодня используются две версии:

• OSPFv2: OSPF для сетей IPv4 (RFC 1247 и RFC 2328) [2];
• OSPFv3: OSPF для сетей IPv6 (RFC 2740) [2].

IS-IS (Intermediate-System-to-Intermediate-System) – иерархический протокол, был разработан в 1978 г. ISO в качестве протокола маршрутизации для собственного Connectionless Network Protocol (CLNP), являвшегося частью стека протоколов, призванного заменить TCP/IP. Протокол IS-IS описывается в ISO 10589. Имеет двухуровневую иерархическую архитектуру.

Сравниваемые протоколы используют различную терминологию (табл. 1).

Таблица 1

Соответствие терминов в протоколах

OSPF	IS-IS
Host	End System (ES)
Router	Intermediate System (IS)
Link	Circuit
Packet	Protocol Data Unit (PDU)
Designated router (DR)	Designated IS (DIS)
Backup DR (BDR)	Нет аналога, не используется
Link-State Advertisement	Link-State PDU (LSP)
Hello packet	Hello PDU
Area	Sub domain (area)
Non-backbone area	Level-1 area
Backbone area	Level-2 Sub domain (backbone)
Area Border Router (ABR)	L1L2 router
Autonomous System Boundary Router (ASBR)	Любая IS

Исследование сходств и различий

Несмотря на то, что OSPF и IS-IS – это различные протоколы, они имеют некоторые общие черты, например:

• являются IGP, распространяют маршрутную информацию между маршрутизаторами только внутри одной AS (Autonomous system);

• использован алгоритм Дейкстры для поиска кратчайшего пути на основе состояния каналов связи;

• поддержка Bidirectional Forwarding Detection (BFD) и возможность обеспечивать обнаружение потери связи с соседом за 50 мс в зависимости от аппаратной реализации оборудования. Время сходимости протоколов исследовалось в работах [3, 4];

• поддержка CIDR (Classless Inter-Domain-Routing) – бесклассовая маршрутизация;

• поддержка VLSM (Variable Subnet Length Masking) – маски подсетей переменной длины;

• поддержка QoS (Quality of Service) – качество обслуживания;

• поддержка аутентификации.

Дизайн домена

В первую очередь, стоит рассмотреть возможности дизайна домена при создании сети. Правильно построенный домен является одним из ключевых моментов при выборе архитектуры сети, поскольку позволяет решить сразу несколько возможных проблем в будущем:

- предусмотреть возможности масштабирования;
- снизить нагрузку на аппаратные ресурсы роутеров;
- уменьшить время восстановления сети при аварии;
- увеличить отказоустойчивость сети в целом.

Протоколы OSPF и IS-IS идеологически по-разному относятся к вопросу дизайна домена.

OSPF – протокол иерархический. Это значит, что весь домен маршрутизации протокола OSPF можно разделить на отдельные области (area). Разделение на области не должно быть произвольным. Если топология действительно разбивается на области, в обязательном порядке должна присутствовать область с номером 0 (так называемая нулевая область), а все другие области подключаются к нулевой с помощью маршрутизаторов ABR (Area Border Router). Любое взаимодействие между периферийными областями будет обеспечиваться через нулевую область [5]. То есть протокол OSPF собирает топологию «звезда» с нулевой зоной в её центре. Такое построение логики сети обеспечивает защиту от петель маршрутизации на сетевом уровне. В нулевую область обычно выделяют ядро сети, в остальные области попадает периферия. При этом граница между областями проходит внутри маршрутизатора, т. е. фактически области принадлежит не маршрутизатор целиком, а его отдельный интерфейс, и области разграничиваются внутри роутера. На рис. 1 представлена классическая структура домена протокола OSPF.

Протокол IS-IS также является иерархическим протоколом с возможностью разделения топологии на области. Но принципы этого разделения совершенно другие:

- маршрутизаторы IS-IS-домена целиком и полностью принадлежат какой-то одной зоне, т. е. граница между областями проходит по каналу связи между маршрутизаторами, а не внутри маршрутизатора;
- нет специального номера зоны (как нулевая зона в протоколе OSPF). То есть области, на которые разбита топология, могут иметь произвольные номера и объединяться между собой произвольным образом.

В основе иерархичности протокола лежат уровни взаимодействия маршрутизаторов друг с другом. Пара IS-IS-маршрутизаторов, подключенных друг к другу, могут сформировать два уровня взаимодействий: Level 1 и Level 2 (L1 и L2). При этом соседство уровня 1 (L1) формируется только между маршрутизаторами одной области, а соседство уровня 2 (L2) может быть сформировано между маршрутизаторами как одной, так и разных областей [6]. Также существуют маршрутизаторы уровня L1/L2 для взаимодействия между маршрутизаторами различных уровней, обычно они находятся на границе области [7]. Пример формирования дизайна топологии протокола IS-IS приведен на рис. 2. В данном случае маршрутизаторы в зоне 49.0001 будут владеть полным объемом маршрутной информации в сети, а маршрутизаторы в зоне 49.0002 и зоне 49.0003 не будут знать ничего друг о друге, все обязанности по маршрутизации между ними возьмет на себя зона 49.0001. Данная схема очень похожа на топологию протокола OSPF, и зона 49.0001 является аналогом нулевой области, таким образом обычно обосабливается ядро сети и разграничивается взаимодействие зон между собой.

Транспорт

Протокол OSPF изначально был ориентирован на IP-сети, поэтому свои пакеты он инкапсулирует в пакеты протокола IP. Протокол IS-IS инкапсулирует служебные пакеты непосредственно во фреймы канального уровня, тем самым поддерживая сразу несколько протоколов сетевого уровня (например, IP, IPX и AppleTalk) [8]. Вдобавок это предоставляет дополнительную защиту от атак на сетевом уровне, направленных на этот протокол, что, несомненно, является большим плюсом в его пользу.

Служебный трафик, моделирование топологии и тестирование

Ещё одним критерием для сравнения является объём служебного трафика, генерируемый протоколами, поскольку это влияет на общую пропускную способность канала связи. В рамках статьи собран тестовый стенд с топологией из четырёх роутеров, изображённой на рис. 3. В качестве среды использовался программный продукт GNS3 (графический симулятор сети, который позволяет моделировать сложные сети [9]). В качестве маршрутизаторов использо-

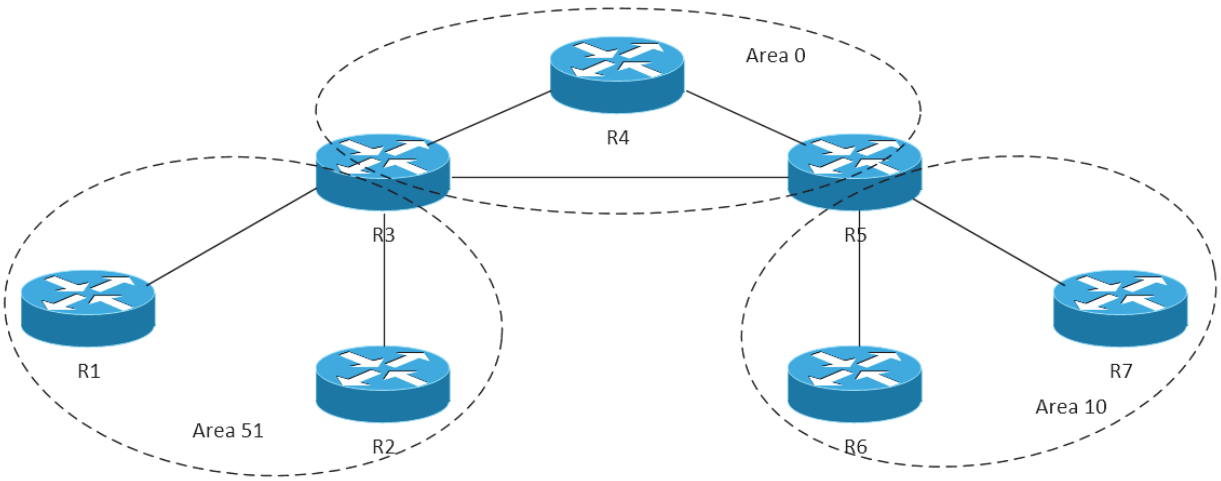


Рис. 1. Дизайн домена OSPF

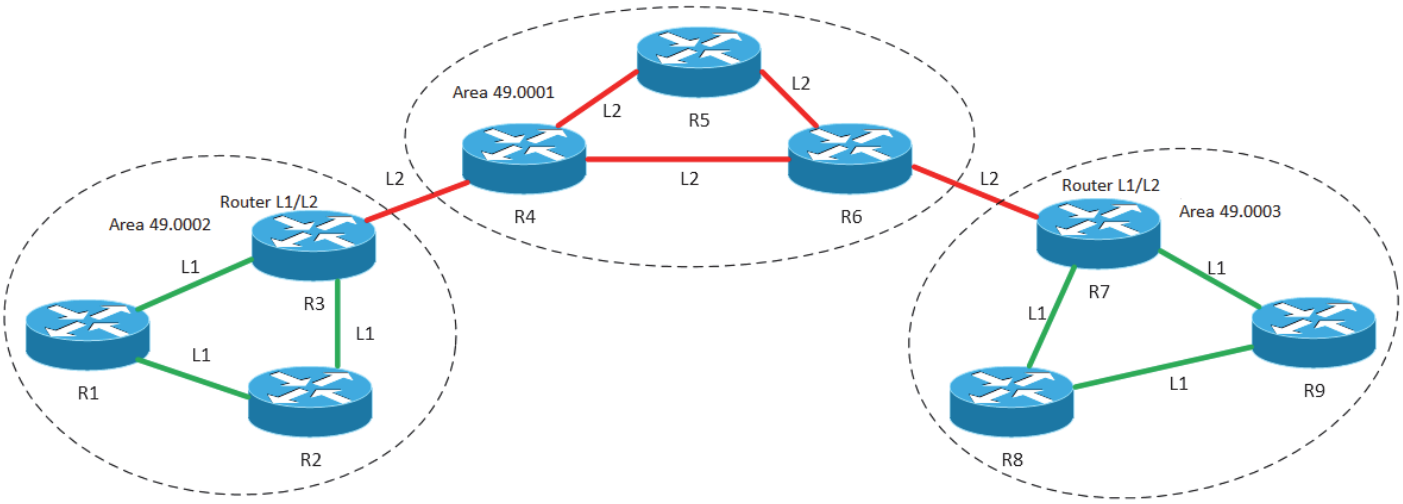


Рис. 2. Дизайн домена IS-IS

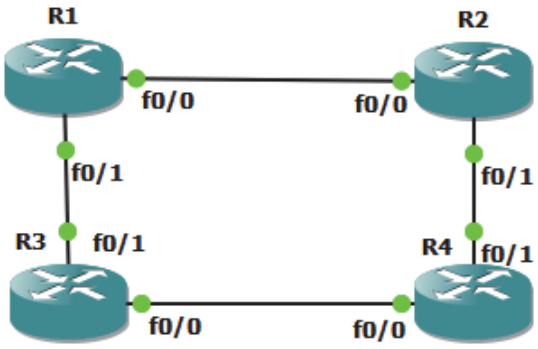


Рис. 3. Тестовая топология

ваны образы платформ Cisco 2691. На каждом канале связи между маршрутизаторами установлено отношение соседства по протоколу OSPF в нулевой области, а также отношение соседства по протоколу IS-IS уровня L2 со стандартными таймерами для эмуляции одного домена с распространением всей маршрутной информации между всеми маршрутизаторами, что означает присутствие всех маршрутных данных на каждом из физических каналов связи.

Цель эксперимента – измерить объём служебного трафика в стабильной сети, для этого используется утилита WireShark – программа-анализатор трафика для компьютерных сетей Ethernet и некоторых других [10].

Сам захват трафика всегда производится на канале связи между маршрутизаторами R1 и R2.

Тест 1. На указанной топологии захватывается трафик. Результат его анализа показан на рис. 4. Как видно из рис. 4, протокол IS-IS шлёт 74,2 % всех пакетов на этом канале связи, но их объем занимает 96,1 % всего переданного трафика, на долю протокола OSPF приходится только 1,6 %.

Анализируя статистику размеров пакетов, приведённую на рис. 5, можно заметить, что присутствуют 583 пакета объёмом 1514 байт. Согласно рис. 4, это пакеты IS-IS Hello. Обратив внимание на содержимое пакета, мы увидим, что большую часть его объема составляет поле Padding, предназначенное для обнаружения проблем с MTU в канале связи до установления соседства.

Тест 2. На всех интерфейсах маршрутизаторов, где запущен процесс протокола IS-IS, прописывается команда ‘no isis hello padding’. Она предлагает не заполнять поле Padding в IS-IS Hello PDU при уже установившемся отношении соседства. Результат показан на рис. 6. Протокол IS-IS шлёт 74 % всех пакетов, но теперь их суммарный объём составляет 60,6 %, доля пакетов OSPF составляет только 16,4 %. Соотношение изменилось в 10 раз. Объём трафика протокола IS-IS без учета накладных расходов на транспорт – 897 579 байт в первом тесте и 56 838 байт во втором тесте – уменьшился в 15,8 раза. Поле padding в IS-IS PDU значительно влияет на объём служебного трафика протокола IS-IS.

Protocol	Percent Packets	Packets	Percent Bytes	Bytes	Bits/s
Frame	100.0	1000	100.0	934377	5887
Ethernet	100.0	1000	1.5	14000	88
Logical-Link Control	74.2	742	96.3	899805	5669
ISO 10589 ISIS InTRA Domain Routeing Information Exchange Protocol	74.2	742	96.1	897579	5655
ISO 10589 ISIS Link State Protocol Data Unit	1.3	13	0.1	926	5
ISO 10589 ISIS Complete Sequence Numbers Protocol Data Unit	14.6	146	2.4	22630	142
ISIS HELLO	58.3	583	92.9	868087	5469
Internet Protocol Version 4	25.4	254	0.5	5080	32
Open Shortest Path First	25.4	254	1.6	15240	96
Data	0.4	4	0.0	252	1

Рис. 4. Результаты анализа трафика

Topic / Item	Count	Average	Min val	Max val	Rate (ms)	Percent
Packet Lengths	1000	934.38	69	1514	0.0008	100%
0-19	0	-	-	-	0.0000	0.00%
20-39	0	-	-	-	0.0000	0.00%
40-79	11	71.91	69	77	0.0000	1.10%
80-159	260	94.78	94	138	0.0002	26.00%
160-319	146	180.00	180	180	0.0001	14.60%
320-639	0	-	-	-	0.0000	0.00%
640-1279	0	-	-	-	0.0000	0.00%
1280-2559	583	1514.00	1514	1514	0.0005	58.30%
2560-5119	0	-	-	-	0.0000	0.00%
5120 and greater	0	-	-	-	0.0000	0.00%

Рис. 5. Статистика размеров пакетов

Protocol	Percent Packets	Packets	Percent Bytes	Bytes	Bits/s
Frame	100.0	1001	100.0	93807	588
Ethernet	100.0	1001	14.9	14014	87
Logical-Link Control	74.0	741	63.0	59061	370
ISO 10589 ISIS InTRA Domain Routeing Inform...	74.0	741	60.6	56838	356
ISO 10589 ISIS Link State Protocol Data Unit	1.1	11	0.8	724	4
ISO 10589 ISIS Complete Sequence Numb...	14.7	147	24.3	22785	142
ISIS HELLO	58.2	583	29.2	27401	171
Internet Protocol Version 4	25.6	256	5.5	5120	32
Open Shortest Path First	25.6	256	16.4	15360	96
Data	0.4	4	0.3	252	1

Рис. 6. Результаты анализа трафика без поля Padding

Тест 3. Сеть увеличивается в два раза и состоит теперь из 8 маршрутизаторов, строящих топологию, как указано на рис. 7. По-прежнему на каждом канале связи установлено отношение соседства по протоколам OSPF и IS-IS. Настройки интерфейсов совпадают с настройками во втором тесте.

Результат изображен на рис. 8. Процентное соотношение количества переданных пакетов прежнее. Процентное соотношение объёма переданного трафика изменилось: доля IS-IS выросла с 60,6 % до 68,7 %, доля OSPF же, наоборот, уменьшилась с 16,4 % до 12,9 %. Передано 252 пакета протокола OSPF общей сложностью 15 120 байт, иными словами, объём трафика не изменился по сравнению с предыдущим тестом. На долю протокола IS-IS теперь вместо 56 838 байт приходится 80 342 байт, фигурирует прирост служебных данных на 41 %.

Результаты теста говорят о независимости объёма служебного трафика протокола OSPF от количества связей и маршрутизаторов в стабильной сети в рамках одного отношения соседства, это обусловлено тем, что при стабильной сети протокол OSPF производит только обмен Hello-пакетами.

Количество данных протокола IS-IS, наоборот, увеличивается. Исходя из статистики, видно, что по сравнению со вторым тестом суммарный объем пакетов IS-IS CSNP (Complete Sequence Number PDU) вырос в 2 раза при их прежнем количестве. С помощью этих PDU IS-IS-маршрутизаторы синхронизируют известную им информацию о топологии, PDU содержат список всех LSP (Link-State PDU). Из этого следует, что объём пакета IS-IS CSNP напрямую зависит от количества роутеров в сети и от её связности, что подразумевает прямую зависимость объёма служебного трафика IS-IS

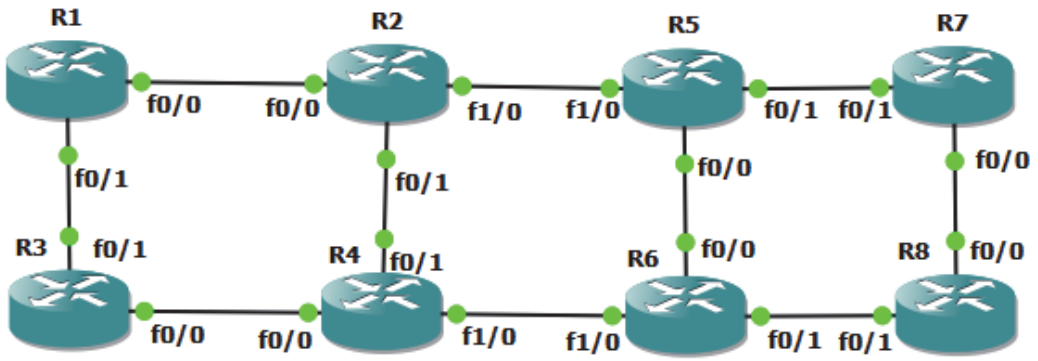
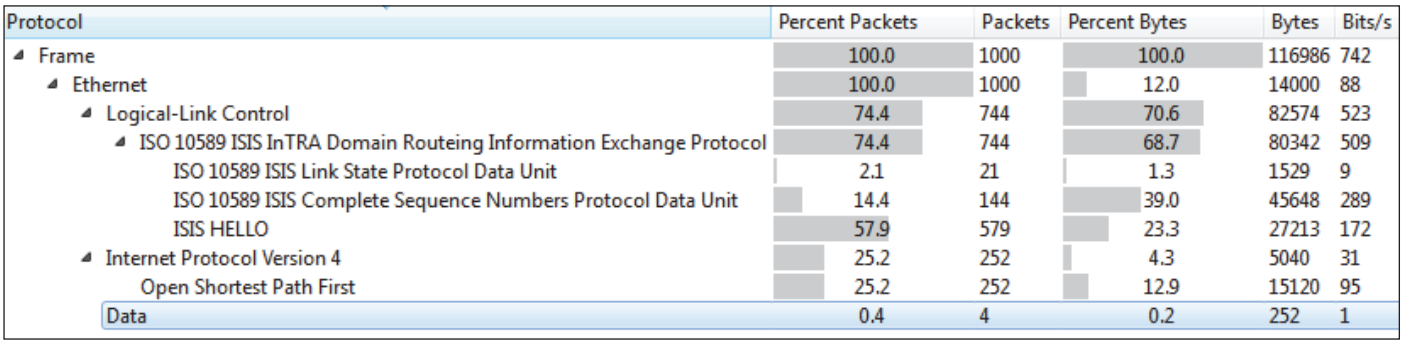


Рис. 7. Расширенная тестовая топология



Protocol	Percent Packets	Packets	Percent Bytes	Bytes	Bits/s
Frame	100.0	1000	100.0	116986	742
Ethernet	100.0	1000	12.0	14000	88
Logical-Link Control	74.4	744	70.6	82574	523
ISO 10589 ISIS InTRA Domain Routeing Information Exchange Protocol	74.4	744	68.7	80342	509
ISO 10589 ISIS Link State Protocol Data Unit	2.1	21	1.3	1529	9
ISO 10589 ISIS Complete Sequence Numbers Protocol Data Unit	14.4	144	39.0	45648	289
ISIS HELLO	57.9	579	23.3	27213	172
Internet Protocol Version 4	25.2	252	4.3	5040	31
Open Shortest Path First	25.2	252	12.9	15120	95
Data	0.4	4	0.2	252	1

Рис. 8. Результаты анализа трафика для топологии из 8 роутеров

Таблица 2

Результаты тестов

№ теста	Время захвата, с	Кол-во пакетов, шт.	Кол-во связей, шт.	Кол-во роутеров, шт.	Протокол	Объём трафика, байт	Занятая п/с, бит/с
1	1240	1000	4	4	OSPF	15240	5655
					IS-IS	897579	96
2	1235	1001	4	4	OSPF	15360	356
					IS-IS	56838	96
3	1260	1000	10	8	OSPF	15120	509
					IS-IS	80342	95

от объёма пакета IS-IS CSNP. Также здесь применимо правило транзитивности, объём служебного трафика напрямую зависит от количества роутеров в сети и от её связности.

В табл. 2 представлены обобщённые результаты тестов. Протокол OSPF показывает явную стабильность вне зависимости от количества роутеров и связей между ними. Объём служебного трафика протокола IS-IS меняется в зависимости от присутствия поля Padding в пакетах протокола, имеет прямую зависимость от количества роутеров и связей между ними. Даже после оптимизации (отключения поля Padding в Hello PDU для установленного соседства) этот протокол генерирует больший объём служебного трафика.

Выводы

1. Сравниваемые протоколы в некоторой мере схожи: являются IGP, используют один и тот же алгоритм расчета кратчайшего пути, в совокупности с протоколом BFD показывают практически одинаковое время сходимости.

2. Сравниваемые протоколы различаются подходом к дизайну. Протокол OSPF строит топологию типа «звезда» с нулевой областью в центре и не разрешает всем остальным областям взаимодействовать между собой в обход нулевой области, что, в свою очередь, является отличным защитным механизмом от петель маршрутизации. В настоящее время такой подход практикуется в большинстве сетей различных размеров. Архитектура дизайна домена протокола IS-IS иная. Области внутри AS могут быть связаны в каком угодно порядке, что затрудняет понимание топологии человеком при сети крупных размеров и создает дополнительные возможности для появления петель, также увеличивается вероятность человеческой ошибки при конфигурировании. С другой стороны, протокол IS-IS имеет гибкую двухуровневую архитектуру и позволяет из роутеров второго уровня создать аналог нулевой области протокола OSPF при правильном дизайне домена, но это вызывает дополнительные трудозатраты.

3. Сравниваемые протоколы используют транспорт для своих пакетов на разных уровнях по модели OSI. Пакеты протокола OSPF используют сетевой уровень и инкапсулируют свои данные в пакеты протокола IP. Протокол IS-IS передает служебные данные на канальном уровне, это освобождает протокол от возможных атак на сетевом уровне, что говорит в пользу этого протокола.

4. Сравниваемые протоколы генерируют различный объём служебного трафика. При стандартных настройках протокол OSPF генерирует в разы меньше служебных данных на стабильной сети, чем протокол IS-IS. Из табл. 2 видно, что увеличение объёма служебного трафика протокола IS-IS прямо пропорционально количеству узлов в сети и связей между ними. Малый объём служебного трафика протокола OSPF позволяет разворачивать маршрутизацию в крупных сетях с проблемой «бутылочного горлышка» (проблемой медленного обмена информацией из-за низкой пропускной способности одного из каналов связи в сети) без большой потери пропускной способности. Если данной проблемы нет, применение протокола IS-IS не повредит сети. При современных скоростях передачи данных генерируемый протоколом объём служебной информации ничтожно мал и не влияет на работоспособность канала.

Литература

1. Олифер В. Г. Компьютерные сети. Принципы, технологии, протоколы: учеб. для вузов / В. Г. Олифер, Н. А. Олифер. 4-е изд. СПб.: Питер, 2010. 944 с.

2. База данных RFC-документов. URL: http://www.rfc-editor.org (дата обращения 15.03.2017).

3. Макаренко С. И. Время сходимости протоколов маршрутизации при отказах в сети / С. И. Макаренко // Системы управления, связи и безопасности, 2015, № 2. С. 45-98.

4. Tsegaye Y. OSPF Convergence Times. Master of Science Thesis in the Programme Networks and Distributed Systems / Y. Tsegaye, T. Geberehana. Göteborg (Sweden): Chalmers Univ. Technol., 2012. 77 c. URL: http://publications.lib.chalmers.se/records/fulltext/184363/184363.pdf (дата обращения 17.03.2017).

5. Odom W., Hogg S. CCNA Routing and Switching ICND2 200-105 Official Cert Guide / W. Odom, S. Hogg. Indianapolis: Cisco Press, 2016. 2557 c.

6. Официальный сайт компании Cisco Systems. URL: http://cisco.com (дата обращения 19.03.2017).

7. Martey A. IS-IS Network Design Solutions / A. Martey. Indianapolis: Cisco Press, 2002. 405 c.

8. Таненбаум Э. Компьютерные сети / Э. Таненбаум, Д. Уэзеролл. 5-е изд. СПб.: Питер, 2012. 960 с.

9. Документация к GNS3. URL: http://docs.gns3.com (дата обращения 23.03.2017).

10. Документация к Wireshark. URL: https://www.wireshark.org/docs (дата обращения 23.03.2017).

Comparison of IS-IS and OSPF Dynamic Routing Protocols

Shardakov K. S., Korbakov A. I., Krasnovidov A. V.
Emperor Alexander I Petersburg State Transport University
St. Petersburg, Russia
shardakov@gmail.com, alexpvb111@yandex.ru, alexkrasnovidow@mail.ru

Abstract. **This article discusses two dynamic routing protocols – IS-IS (Intermediate-System-to-Intermediate-System) and OSPF (Open Shortest Path First). Similarities and differences between them are revealed. Describes the terminology used by the protocols, the differences in network design. An infocommunication network is being modeled to measure the amount of generated protocol overhead.**

Keywords: OSPF, **IS-IS, network, topology, dynamic routing, network architecture, traffic, Dijkstra's algorithm.**

References

1. Olifer V. G., Olifer N. A. Computer Networks. Principles, Technologies, Protocols: Textbook for high schools [Komp'juternye seti. Principy, tehnologii, protokoly: Uchebnik dlja vuzov]. 4th ed. St. Petersburg, Piter, 2010, 944 p.

2. RFC-editor (2017). Available at: http://www.rfc-editor.org (accessed 15 March 2017).

3. Makarenko S. I. The Convergence Time of Routing Protocols in Case of Network Failures [Vremja shodimosti protokolov marshrutizacii pri otkazah v seti] *Sistemy upravlenija*, *svjazi i bezopasnosti*, 2015, no. 2, pp. 45-98.

4. Tsegaye Y., Geberehana T. OSPF Convergence Times. Master of Science Thesis in the Programme Networks and Distributed Systems. Göteborg (Sweden), Chalmers Univ. Technol., 2012, 77 p. Available at: http://publications.lib.chalmers.se/records/fulltext/184363/184363.pdf (accessed 17 March 2017).

5. Odom W., Hogg S. CCNA Routing and Switching ICND2 200-105 Official Cert Guide. Indianapolis, Cisco Press, 2016, 2557 p.

6. Cisco Systems (2017). Available at: http://cisco.com (accessed 19 March 2017).

7. Martey A. IS-IS Network Design Solutions. Indianapolis, Cisco Press, 2002, 405 p.

8. Tanenbaum A., Wetherall D. Computer Networks. 5th ed. St. Petersburg, Piter, 2012, 960 p.

9. GNS3 documentation (2017). Available at: http://docs.gns3.com (accessed 23 March 2017).

10. Wireshark documentation (2017). Available at: https://www.wireshark.org/docs (accessed 23 March 2017).

Применение технологии энергосберегающих параллельных вычислений в автономных вычислительных системах на отечественной элементной базе

Басыров А. Г., Шульгин А. Н.
Военно-космическая академия имени А. Ф. Можайского
Санкт-Петербург, Россия
shulgin_albert@mail.ru

Аннотация. **Рассматривается использование архитектуры SPARC в качестве технологической основы реализации новых подходов к организации энергосберегающей параллельной обработки информации. Результаты моделирования показали, что построение автономной высокопроизводительной вычислительной системы на базе процессорного модуля «МЦСТ МВС/С» помимо высокой оперативности при малых массо-габаритных характеристиках обеспечивает эффективные энергосберегающие параллельные вычисления.**

Ключевые слова: **параллельные вычислительные процессы, энергосбережение, диспетчирование, мобильные вычислительные системы.**

Введение

При построении современных мобильных вычислительных систем (ВС) явно просматривается тенденция к применению многомодульной архитектуры, обеспечивающей требуемые производительность и надежность функционирования ВС за счет внедрения технологий параллельных вычислений и возможностей резервирования аппаратных средств.

Возможности параллельной обработки информации обеспечивают повышение производительности функционирования таких ВС и как следствие – способность решить все большее количество целевых задач в реальном времени. Вместе с тем организация параллельных вычислений в мобильных ВС, с одной стороны, и требования к повышению автономности функционирования таких ВС – с другой, порождают ряд проблем, одной из которых является необходимость снижения энергоемкости параллельных вычислительных процессов (ПВП).

Микропроцессоры МЦСТ как основа для построения автономных высокопроизводительных автономных вычислительных систем

Выбор элементной базы для построения автономных ВС основывается на соответствии определяемых для них характеристик базовых аппаратных средств требованиям, предъявляемым к этим ВС. В частности, к таким требованиям относятся:

• защищенность от внешних ионизирующих излучений (что позволяет сделать реальным использование таких ВС в условиях космического пространства);

• использование преимущественно отечественной элементной базы вместо импортной с целью исключения аппаратно-программных «закладок».

Исходя из сказанного, в качестве элементной базы для построения высокоэффективных автономных ВС могут уверенно выступать микропроцессорные средства, реализованные на базе архитектуры SPARC (Scalable Processor ARChitecture – масштабируемая архитектура процессора) специфицированной компанией Sun Microsystems, обладающие всеми чертами RISC-процессоров, сочетая простоту набора команд и высокую скорость исполнения кода [1]. Разработчиком данной элементной базы в России является ЗАО «МЦСТ» (Московский центр SPARC-технологий).

Масштабируемость SPARC-архитектуры дала возможность создать на базе системы на кристалле «МЦСТ-R500S» процессорный модуль «МВС/С», который представляет собой восьмипроцессорную (восьмиядерную) одноплатную универсальную вычислительную систему с оперативной памятью до 8 Гбайт и набором периферийных контроллеров [2]. Основные технические характеристики процессорного модуля «МВС/С» представлены в табл. 1 [3].

Очевидно, что отечественная элементная база не уступает, а по отдельным показателям даже превосходит зарубежные аналоги.

Структурная схема БВС на базе процессорного модуля «МВС/С» показана на рис. 1.

Подход к организации энергосберегающей параллельной обработке информации

Решение проблемы повышения автономности функционирования мобильных ВС может быть основано на управлении энергопотреблением отдельных компонентов параллельной вычислительной системы (ПВС), учитывающим их энерго-временные характеристики и стохастический характер параллельных вычислений.

В этом случае рассматриваются энергосберегающие ПВП, под которыми понимают процессы одновременного выполнения частей программы несколькими вычислительными модулями ПВС при номинальном качестве и минимальном энергопотреблении ВС [4].

Концепция энергосберегающих вычислений воплотилась в управлении вычислительной нагрузкой посредством ее распределенного выполнения на множестве вычислительных модулей (ВМ) в соответствии с некоторым планом вы-

Таблица 1

Основные технические характеристики процессорного модуля «МВС/С»

Характеристика	Значение
Количество машин	4
Количество процессоров	в модуле – 8; в машине –2
Производительность	модуля – 4400 MIPS/1600 MFLOPS машины – 1190 MIPS/400 MFLOPS
Память	Объем: модуля – до 8 Гбайт; машины – до 2 Гбайт Пропускная способность канала обмена 4 × 2,664 Гбайт/с
Флэш-память	512 Кбайт (OpenBoot PROM, стандарт IEEE-1275-1994)
Периферийная шина PCI	Количество слотов 8 Пропускная способность шины 264 Мбайт/с
SCSI-2	Пропускная способность шины 10 Мбайт/с
Ethernet 100	Количество каналов 4 Пропускная способность канала 100 Мбит/с
RS-232	Количество каналов 2 Пропускная способность канала 115 Кбит/с
IDE	Пропускная способность канала 33/66 МБайт/с

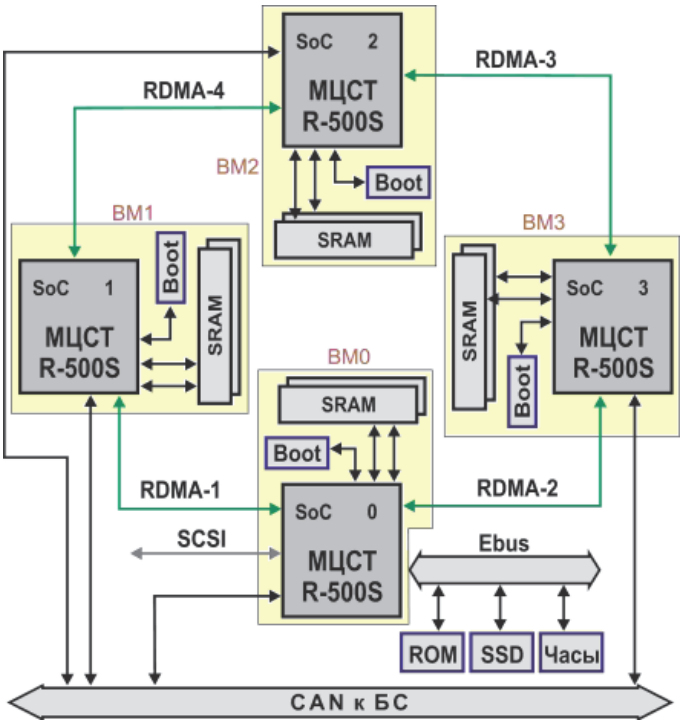


Рис. 1. Структурная схема автономной ВС на базе процессорного модуля «МВС/С»

числительного процесса. Решение этой задачи возлагается на диспетчер вычислительных процессов [5].

При этом основным инструментом решения задачи энергосбережения при диспетчировании энергосберегающих ПВП является совокупность энергосберегающих состояний, в которых ВМ могут находиться определенное время. В табл. 2 показаны основные энергосберегающие состояния ВМ процессорного модуля «МВС/С».

При планировании ПВП используется функция приоритетов TRM, в соответствии с которой наивысший приоритет присваивается задаче, имеющей наименьший резерв времени. На рис. 2 в качестве примера дано графическое представление плана ПВП в виде временной диаграммы реализации параллельного алгоритма комплекса задач автономной ВС для трех ВМ. На рис. 2 видно, как распределены энергосберегающие *С*-состояния по периодам простоев ВМ.

Таблица 2

Содержание и характеристики энергосберегающих состояний ВМ перспективной бортовой вычислительной системы (БВС) на базе процессорного модуля «МВС/С»

С – состояние	Потреб. мощность, Вт	$T_{\text{ППВык}}$, с	$T_{\text{ППВкл}}$, с	$T_{\text{перев}}$, с	Содержание состояний
C0	4,8	0	0	0	Активный режим работы всех устройств ВМ
C1	1,8	0,00005	0,00025	0,0003	SoC переводится в режим пониженного энергопотребления
C2	0,6	0,0005	0,0015	0,0020	Внутренние устройства SoC отключены. Boot отключено. Состояние SoC сохраняется в SRAM
C3	0,01	1,5360	3,0720	4,6080	SRAM отключено. Состояние SRAM сохраняется в SSD

Результаты моделирования процессов диспетчирования энергосберегающих параллельных вычислительных процессов для вычислительных систем на базе процессорного модуля МЦСТ «МВС/С»

Моделирование процесса диспетчирования энергосберегающих ПВП позволило объективно оценить эффективность различных подходов к управлению состояниями ВМ в процессе вычислений. В качестве объекта моделирования рассматривалась бортовая ВС на базе процессорного модуля «МЦСТ МВС/С».

Диспетчирование моделировалось для вариантов реализации алгоритма решения комплекса целевых задач на 2, 3 и 4 ВМ. На рис. 3а изображена графовая модель алгоритма комплекса задач для 3-модульной реализации БВС.

В качестве веса данного взвешенного графа [6] указаны значения двух первых начальных моментов случайных величин времени завершения каждой задачи (вершины).

В качестве исходных данных при моделировании выступали: граф целевых задач в форме матрицы смежности $\|H\|_{N.N}$ и множество энергосберегающих *С*-состояний вычислительных модулей с соответствующими каждому состоянию энерго-временными характеристиками (см. табл. 1).

На рис. 3б показана матрица смежности графа комплекса целевых задач перспективной БВС для трех ВМ.

При моделировании отрабатывались алгоритмы условных и безусловных переводов ВМ в энергосберегающие

Рис. 2. Временная диаграмма реализации параллельного алгоритма комплекса целевых задач перспективной БВС для трех ВМ

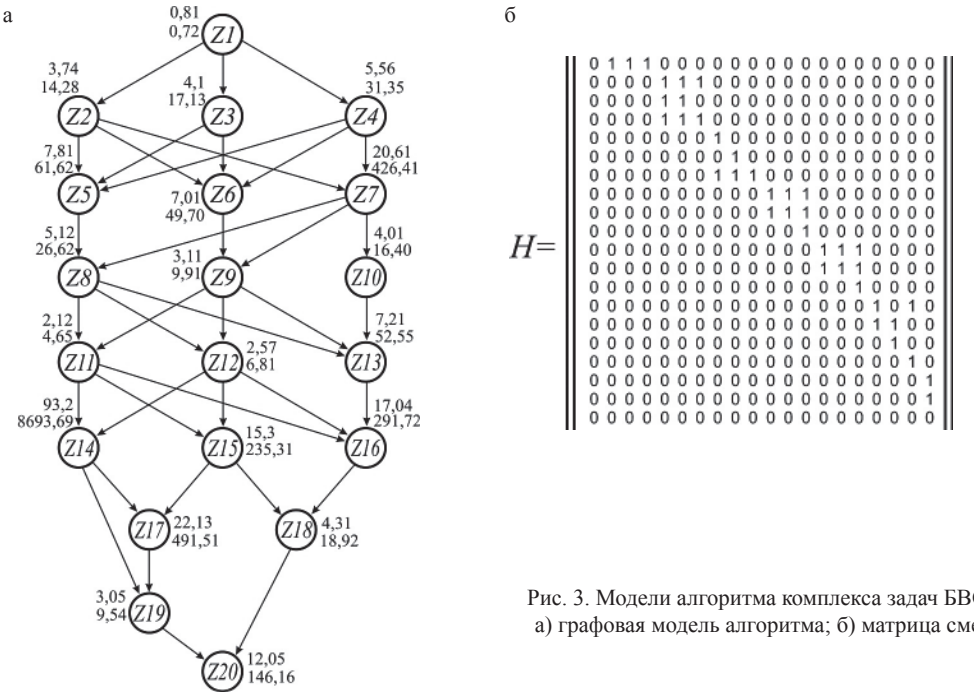


Рис. 3. Модели алгоритма комплекса задач БВС для трех ВМ:
а) графовая модель алгоритма; б) матрица смежности графа

C-состояния. В каждом испытании случайным образом генерировались 1-е и 2-е моменты случайной величины времени завершения каждого задания, распределенной по закону Вейбулла – Гнеденко [7].

При сравнительной оценке эффективности функционирования ПВС различной конфигурации важна оценка ее функционирования за определенный период времени ΔT. В качестве такой оценки может выступать возможное количество циклов L выполнения ПВП за период ΔT, которое находится из соотношения

$$L = \frac{\Delta T}{T_{\text{ПВП}}}, \qquad (1)$$

где ΔT – период функционирования ПВС; $T_{\text{ПВП}}$ – время выполнения ПВП.

Тогда энергоемкость ПВП за период ΔT может быть найдена из выражения

$$E_{\text{ПВП}} = (T_{\Sigma\text{ВМ}} \cdot P_{\text{АР}} + T_{\Sigma\text{пр}} \cdot P_{\text{С*}})L, \qquad (2)$$

где L – количество циклов выполнения ПВП за ΔT; $T_{\Sigma\text{ВМ}}$ – суммарное время работы всех ВМ; $T_{\Sigma\text{пр}}$ – суммарное время простоев всех ВМ; $P_{\text{АР}}$ – мощность, потребляемая ВМ в активном режиме; $P_{\text{С*}}$ – мощность, потребляемая ВМ в энергосберегающем состоянии.

Результаты расчетов энергоемкости при диспетчировании энергосберегающих ПВП в БВС малых космических аппаратов для разного количества ВМ и способов управления энергопотреблением ВМ за период функционирования в течение 1 ч (3600 с) с учетом параметров энергосберегающих состояний, представленных в табл. 1, показаны в табл. 3.

На рис. 4 показаны соотношения величин энергоемкости функционирования БВС при выполнении ПВП при различных способах управления энергопотреблением ВМ (для 1, 2, 3 и 4 ВМ) за 1 ч функционирования.

Рис. 5 иллюстрирует величину эффекта, представленного в виде процента снижения энергопотребления функционирования БВС при реализации ПВП по методике с условным отключением ВМ за 1 ч функционирования:

Таблица 3

Результаты расчетов параметров энергосберегающих ПВП для ПВС с различным числом ВМ и способов управления энергопотреблением

Количество ВМ	$T_{ПВП}$, с	$T_{\Sigma ВМ}$, с	$T_{\Sigma пр}$, с	L	$E_{ПВП}$, Вт·ч		
					Без откл. ВМ	С безусл. откл. ВМ	С условн. откл. ВМ
1 ВМ	240,29	240,29	0,0	14,8	5,8	–	–
2 ВМ	177,20	240,29	106,90	20,3	11,7	8,1	7,8
3 ВМ	164,70	240,29	253,81	22,1	17,6	9,5	8,5
4 ВМ	159,54	240,29	397,87	23,1	23,4	10,2	8,8

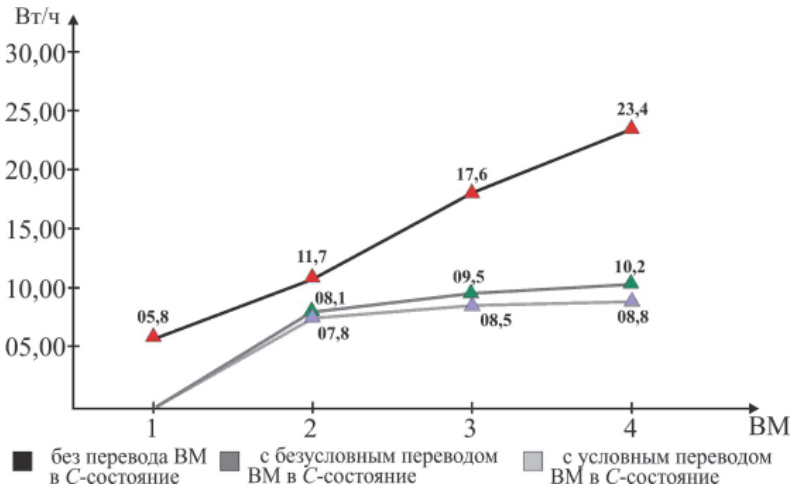


Рис. 4. Соотношение величин энергоемкости функционирования БВС при различных способах управления энергопотреблением ВМ

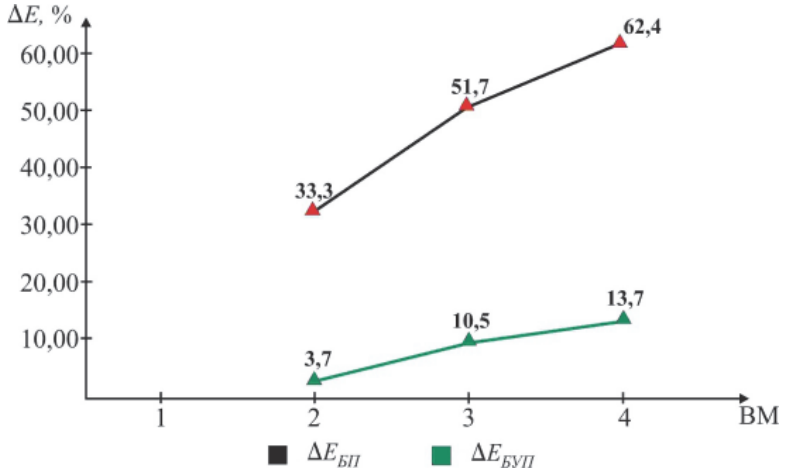


Рис. 5. Энергосберегающий эффект при реализации ПВП по методике с условным отключением ВМ за 1 час работы

• по отношению к способу управления энергопотреблением ВМ без перевода ВМ в пассивный режим работы ($\Delta E_{БП}$);

• по отношению к способу с безусловным переводом в пассивный режим функционирования ($\Delta E_{БУП}$).

Заключение

Технологии энергосберегающих параллельных вычислений в автономных вычислительных системах активно исследуются и широко применяются при решении различных целевых задач [8–11].

Исходя из анализа результатов моделирования, можно сделать выводы, что:

• при увеличении связности графа алгоритма целевых задач и их количества эффективность диспетчирования энергосберегающих ПВП с использованием условных переходов ВМ в энергосберегающие состояния растет на 10–42 % по сравнению с функционированием ВМ без отключения и от 6 до 20 % – по сравнению с методом безусловного отключения ВМ;

• элементная база МЦСТ, реализующая архитектуру SPARC, соответствует требованиям, предъявляемым к ап-

паратным составляющим перспективных БВС и обеспечивает построение высокопроизводительных универсальных бортовых вычислительных комплексов. Предлагаемое построение перспективной БВС на базе процессорного модуля «МЦСТ МВС/С» помимо высокой оперативности при малых массово-габаритных характеристиках обеспечивает эффективную реализацию энергосберегающих параллельных вычислений.

Литература

1. Ким А. К. Развитие и реализация архитектуры вычислительных комплексов серии «Эльбрус» для решения задач ракетно-космической обороны / А. К. Ким, В. И. Перекатов, Ю. Х. Сахин // Вопр. радиоэлектроники. Сер. ЭВТ, 2010, вып. 3. С. 5–17.

2. Ким А. К. Современные российские микропроцессоры / А. К. Ким // МЦСТ Вычислительные технологии, 2012. С. 10–17.

3. Ким А. К. Микропроцессоры и вычислительные комплексы семейства «Эльбрус / А. К. Ким, В. И. Перекатов, С. Г. Ермаков. СПб.: Питер, 2013. С. 68-77.

4. Басыров А. Г. Методика организации энергосберегающего функционирования бортовой вычислительной системы космического аппарата / А. Г. Басыров // Тр. ВКА им. А. Ф. Можайского, 2009, вып. 627. С. 243-252.

5. Басыров А. Г. Диспетчер энергосберегающего параллельного вычислительного процесса / А. Г. Басыров, А. В. Данеев, А. Б. Мастин // Современные технологии. Системный анализ. Моделирование, 2010, № 3 (27). С. 157-162.

6. Кустов В. Н. Основы теории ограниченного структурного параллелизма / В. Н. Кустов. СПб.: МО РФ, 1992. 246 с.

7. Вадзинский Р. Н. Справочник по вероятностным распределениям / Р. Н. Вадзинский. СПб.: Наука, 2001. 158 с.

8. Кулешов С. В.Технология удаленного мониторинга пространственного положения пилотируемого летательного аппарата и состояния его бортовых систем в режиме реального времени / С. В. Кулешов, А. А. Зайцева, А. Ю. Аксенов // Интеллектуальные технологии на транспорте, 2016, вып. 6. С. 43-49.

9. Advanced Configuration and Power Interface Specification. Hewlett-Packard/Intel/Microsoft/Phoenix/Toshiba, Revision 3.0b, 2006. 606 p.

10. Wang S. Application Configuration Selection for Energy-efficient Execution on Multicore Systems / S. Wang, B. Luo, W. Shi, D. Tiwari // J. Parallel and Distributed Computing, 2016, vol. 87, pp. 43-54.

11. Bui D.-M. Energy Efficiency for Cloud Computing System Based on Predictive Optimization / D.-M. Bui, Y. Yoon, E.-N. Huh, S. Jun, S. Lee / J. Parallel and Distributed Computing, 2017, vol. 102, pp. 103-114.

Application of Energy Saving Technology of Parallel Computation in the Autonomous Computing Systems in the Domestic Element Base

Basyrov A. G., Shulgin A. N.
Military Space Academy named A. F. Mozhaisky
St. Petersburg, Russia
shulgin_albert@mail.ru

Abstract. **The article discusses the use of architecture-SPARC as a technological basis for the implementation of new approaches to energy saving parallel processing of information. The results of modeling showed that the construction of an Autonomous, high-performance computing system based on the processor module "MCST MVS/C", in addition to high efficiency at small mass-dimensional characteristics, ensures effective implementation of energy-saving parallel computing.**

Keywords: **parallel computing processes, energy saving, dispatching, mobile computing system.**

References

1. Kim A. K., Perekatov V. I., Sahin Yu. H. The Development and Implementation of Architecture, Computer Systems Series "Elbrus" for Solving Problems of Rocket-space Defense [Razvitie i realizaciya arhitektury vychislitel'nyh kompleksov serii "EHl'brus" dlya resheniya zadach raketno-kosmicheskoj oborony], *Questions of radio electronics [Voprosy radioehlektroniki]*, 2010, vol. 3, pp. 5-17.

2. Kim A. K. Modern Russian Microprocessors [Sovremennye rossijskie mikroprocessory], *MCST Computing technology [MCST Vychislitel'nye tekhnologii]*, 2012, pp.10-17.

3. Kim A. K., Perekatov V. I., Ermakov S. G. Microprocessors and Computer Systems of the Family "Elbrus" [Mikroprocessory i vychislitel'nye kompleksy semejstva "EHl'brus"], St. Petersburg, Piter, 2013, pp. 68-77.

4. Basyrov A. G. The Methods of Organization of Energy Saving Functioning of the Onboard Computer System Spacecraft [Metodika organizacii ehnergosberegayushchego funkcionirovaniya bortovoj vychislitel'noj sistemy kosmicheskogo apparata], *Works MSA named after A. F. Mozhaisky Works MSA named after A. F. Mozhaisky [Trudy VKA imeni A. F. Mozhajskogo]*, 2009, vol. 627, pp. 243-252.

5. Basyrov A. G., Daneev A. V., Mastin A. B. Energy Saving Manager of Parallel Computing Process [Dispetcher ehnergosberegayushchego parallel'nogo vychislitel'nogo processa], *Modern technology. System analysis. Modeling [Sovremennye tekhnologii. Sistemnyj analiz. Modelirovanie]*, 2010, vol. 3 (27), pp. 157-162.

6. Kustov V. N. Fundamentals of the Theory of Limited Structural Parallelism [Osnovy teorii ogranichennogo strukturnogo parallelizma], St. Petersburg, MO RF, 1992, 246 p.

7. Vadzinskij R. N. The Reference Probability Distributions [Spravochnik po veroyatnostnym raspredeleniyam], St. Petersburg, Nauka, 2001, 158 p.

8. Kuleshov S. V., Zaytseva A. A., Aksenov A. Yu. The Technology of Remote Monitoring of the Spatial Position of the Aircraft and the State of Its Onboard Systems in Real Time [Tehnologiya udalennogo monitoringa prostranstvennogo polozheniya pilotiruemogo letatelnogo apparata i sostoyaniya ego bortovyih sistem v rezhime realnogo vremeni], *Intellektualnyie tehnologii na transporte [Intellectual technologies on transport]*, 2016, vol. 6, pp. 43-49.

9. Advanced Configuration and Power Interface Specification. Hewlett-Packard/Intel/Microsoft/Phoenix/Toshiba, Revision 3.0b, 2006. 606 p.

10. Wang S., Luo B., Shi W., Tiwari D. Application Configuration Selection for Energy-efficient Execution on Multicore Systems. J. Parallel and Distributed Computing, 2016, vol. 87, pp. 43-54.

11. Bui D.-M., Yoon Y., Huh E.-N., Jun S., Lee S. Energy Efficiency for Cloud Computing System Based on Predictive Optimization. J. of Parallel and Distributed Computing, 2017, vol. 102, pp. 103-114.

Новая угроза безопасной эксплуатации информационно-управляющих комплексов электроподвижного состава

Белов В. П.
Военно-космическая академия им. А. Ф. Можайского
Санкт-Петербург, Россия
arsenal_belov@mail.ru

Штагер Е. А.
Крыловский государственный научный центр
Санкт-Петербург, Россия
shtager.e@mail.ru

Аннотация. **Проанализированы портативные средства электромагнитного излучения, способные нарушить функционирование автоматизированных систем управления движением поездов, в том числе поездов метрополитена. Рассмотрена одна из возможностей защиты персонала, радиоэлектронной аппаратуры систем управления и обеспечения безопасности перевозок с помощью защитных стекол отечественного производства. Проанализированы частотные характеристики эффективности экранирования энергосберегающими стеклами и стеклами, задерживающими преднамеренное электромагнитное излучение. Обоснована эффективность противодействия проникновению электромагнитного импульса через окна заданий путем замены обычных стекол на стекла с металлическим покрытием.**

Ключевые слова: **эффективность экранирования, электромагнитный терроризм.**

1. Электромагнитный терроризм

Научно-технический прорыв в области исследований неидеальной плазмы, взрывного преобразования энергии в электромагнитные импульсы привёл к созданию генераторов мощного электромагнитного излучения (ЭМИ). Стала актуальной защита радиоэлектронных систем (РЭС) и обслуживающего персонала. Это подтверждают результаты локальных конфликтов, где впервые велось широкое применение средств электромагнитного воздействия [1]. ЭМИ как природного, так и техногенного происхождения оказывают решающее влияние на безопасность работы радиоэлектронных средств, средств обеспечения безопасности функционирования [2–4]. В зоне риска оказываются в том числе интеллектуальные системы автоведения поездов различного целевого назначения, оснащённых бортовыми вычислительными устройствами на основе контроллеров. Создаётся угроза безопасной работы городских центров диспетчерского управления (ЦДУ) перевозками, объектов управления городским транспортом и городским хозяйством [5]. Основной принцип действия созданных генераторов заключается в излучении мощных одиночных импульсов или в формировании их последовательности. В результате таких воздействий происходят сбои программ, а иногда и выгорания *p-n*-переходов во входных транзисторах. В последнее время появились мощные портативные генераторы электромагнитных волн, используемые в системе электромагнитного терроризма. Эти генераторы могут размещаться в кейсах, багажниках автомашин и в других средствах передвижения. На рис. 1 и 2 показаны такого рода генераторы, которые излучают короткие электромагнитные импульсы длительностью в единицы наносекунд и мощностью более 100 кВ [2].

Рис. 1. Малогабаритный источник ЭМИ разового действия

Рис. 2. Малогабаритный источник ЭМИ

Генератор на рис. 1 может быть включен дистанционно и его не обязательно заносить внутрь помещения.

Другая компания [3] разработала генератор многоразового действия (рис. 2). Малогабаритный генератор (20×16×8 дюй-

мов, масса 62 фунта, включая передающую антенну) имеет следующие характеристики:

• частота излучения 350 МГц;

• напряженность поля 120 кВ/м в ближней зоне от всенаправленной антенны;

• продолжительность работы 30 мин в непрерывном режиме (5 импульсов в секунду) или 3 часа с перерывами.

Мощный генератор ЭМИ может быть расположен и в багажнике легкового автомобиля (рис. 3). При этом стёкла такого автомобиля не должны пропускать электромагнитное излучение внутрь салона. Такие же стёкла должны иметь здания с высокочувствительной аппаратурой и работающими на ней операторами.

Рис. 3. Генератор мощного ЭМИ в багажнике автомобиля

Современные малогабаритные генераторы ЭМИ, включая показанные на рис. 1–3, способны вывести из строя высокочувствительные электронные приборы и системы (аппаратуру управления и централизации, видеокамеры наружного и внутреннего наблюдения, компьютеры и серверы локальных сетей в объеме малоэтажного здания). Попавший под облучение ЭМИ персонал получает сбои сознания, люди перестают понимать свои задачи, совершают неразумные поступки и действия, которые могут приводить к еще более тяжелым технологическим последствиям [2–5]. Один из возможных путей защиты РЭС и персонала от воздействия ЭМИ – применение специализированных стёкол на окнах кабин поездов и рамах зданий ЦДУ [6].

Для оценки эффективности экранирования стеклами используется соотношение

$$SE = 20\lg\frac{E_o}{E_{tr}}, \qquad (1)$$

где E_o – напряженность падающего по нормали на стекло поля; E_{tr} – напряженность прошедшего через экран поля.

Типичная конструкция применяемого защитного стекла показана на рис. 4.

Защитные стекла производят промышленным способом: на поверхность оконного стекла наносят тонкую металлическую пленку или сетку. Различают «мягкую» и «жесткую» форму нанесения металлической пленки [4, 7]. В первом случае из коллоидного раствора, например серебра, осаждают нанопленку толщиной несколько десятков нанометров на одну из сторон стекла. Во втором случае при нанесении используется химическое паровое осаждение, в результате которого создается пленка, например из диоксида олова толщиной в сотни нанометров [8]. Эти же способы используются для создания энергосберегающего стекла. Интересно выяснить частотную зависимость SE защитного стекла, к чему мы и переходим.

2. Частотные зависимости эффективности экранирования зарубежных защитных стекол

Электромагнитное оружие работает в диапазоне от 1 до 100 ГГц, что определяет рабочий диапазон защитных стекол, которые должны задерживать до 99 % ЭМИ [2–4]. Эффективность экранирования защитным стеклом измерялась в полубезэховой камере Крыловского государственного научного центра [9]. На рис. 5 представлены результаты измерений для разных стекол, характерной особенностью которых были регулярные изменения величины SE. Согласно теории парциальных волн, эти регулярные измерения SE вызваны многократными отражениями между внешней поверхностью стекла и слоем металла [8, 10]. В отсутствие затухания, как в обычном оконном стекле 5, изменения SE с увеличением частоты практически исчезают. По той же причине отсутствует тренд для частотной зависимости SE сводчатого стекла 4.

Характерно, что «толстая» пленка (зависимость 3) приводит к более низкому уровню экранирования по сравнению с нанопленками серебра (зависимости 1 и 2). В сравниваемых случаях действуют различные механизмы затухания электромагнитных волн. В нанопленках внешнее поле взаимодействует с локальным внутренним полем по законам микроэлектродинамики [2, 5, 11]. Увеличение толщины нанопленки вдвое не ведет к пропорциональному увеличению затухания. Однако в том и в другом случае эффективность экранирования оказывается выше, чем у пленки, которая в несколько раз толще. Причина в том, что в толстых пленках действуют уже законы макроэлектродинамики, поскольку в них отсутствуют локальные поля. Этот вопрос подробно рассмотрен в [2].

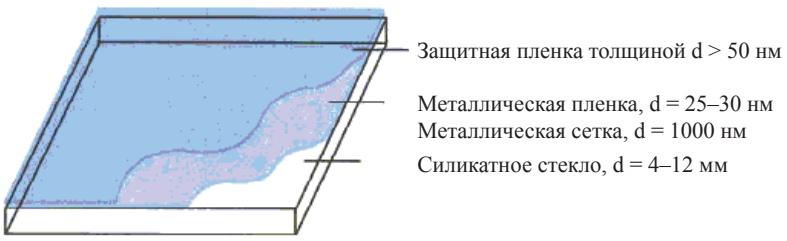


Рис. 4. Конструкция стекла, защищающего от ЭМИ

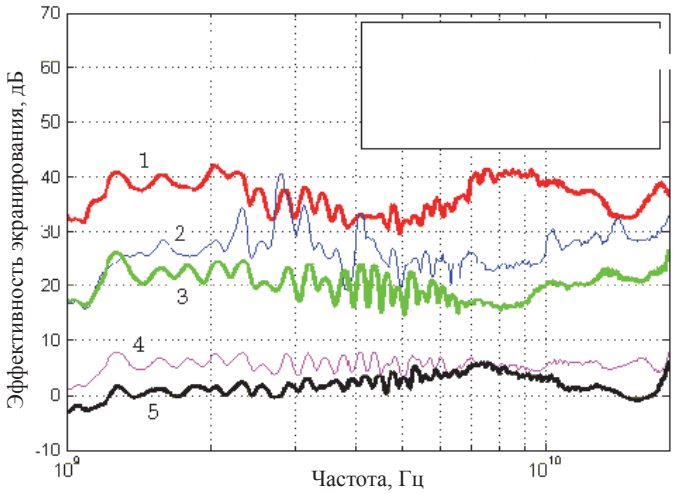


Рис. 5. Измеренные частотные зависимости SE различных стекол при падении волны по нормали к их поверхности:
1 – 2Ag, двойное серебряное покрытие; 2 – 1Ag, одинарное серебряное покрытие; 3 – HC, твердое покрытие; 4 – сводчатое стекло; 5 – чистое стекло

Авторы [9] не смогли полностью объяснить пологие подъемы зависимости SE простого стекла в области частот от 4 до 10 ГГц (см. рис. 5). Действительно, на основе повсеместно используемой модели длинных линий такое объяснение невозможно. Напротив, теория парциальных волн дает однозначное объяснение этого подъема SE. Подъем связан с ростом коэффициента многократных отражений в области указанных частот, что непременно ведет к росту SE [2, 8, 9].

В зарубежной литературе можно найти сведения о более сложных конструкциях из защитных стекол. Одиночные стекла можно соединять в триплексы, когда два одиночных защитных стекла соединены друг с другом, или в стеклопакеты из двух защитных стекол, помещенных рядом, или создавать другие конструкции [2, 8, 11]. В работе [8] приводятся результаты измерений эффективности экранирования некоторых конструкций (см. рис. 6).

Частотные зависимости SE энергосберегающих конструкций (рис. 6, нижняя кривая) имеет характерные максимумы.

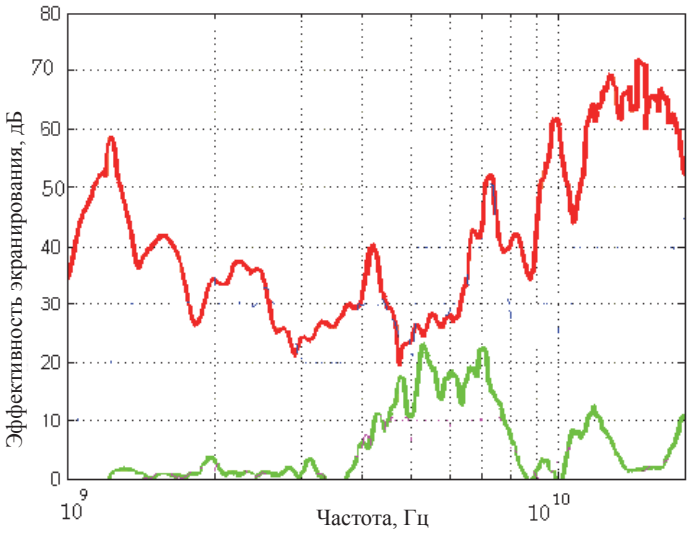


Рис. 6. Частотная зависимость эффективности экранирования защитного триплекса

Первый из них обязан своим появлением росту коэффициента отражения на частотах, обеспечивающих сложение сигналов, отраженных от верхней поверхности и от металлического слоя [7]. Понятно, что рост коэффициента отражения сопровождается падением коэффициента прохождения ЭМИ через конструкцию стекла. В свою очередь, на этих частотах поднимается эффективность экранирования. Следующий максимум SE будет при двукратном увеличении частоты, т. е. в районе частот 12 ГГц, что мы и наблюдаем в эксперименте (см. рис. 6). Этот максимум оказывается ниже предыдущего, что имеет свое объяснение. Действительно, с ростом частоты уменьшается глубина скин-эффекта, поэтому в «толстом» металлическом покрытии на частотах второго максимума в пленке укладывается вдвое больше величин скин-эффекта, а на глубине каждое поле спадает в 2,4 раза. Тогда понятно, почему второй максимум верхней кривой меньше первого, а третий меньше второго.

3. Частотные зависимости эффективности экранирования отечественных защитных стекол

Защитное стекло разработано совместными усилиями авторов публикации и стекольной компании ОАО «АКМА» (Санкт-Петербург) [8, 9, 11]. Промышленная линия этой компании производит защищенный триплекс, образованный двумя защитными стеклами пленками внутрь. Частотные характеристики SE одиночного стекла с серебряной нанопленкой (дуплекса) показаны на рис. 7.

Исходя из физических понятий, эффективность экранирования дуплексов должна быть одинакова с любой стороны наблюдения [2]. Это положение подтверждается экспериментально (рис. 7), что косвенно свидетельствует о правильности измерений.

На этой же измерительной установке определены частотные зависимости коэффициента прохождения через триплекс, образованного двумя дуплексами, обращенными нанопленками внутрь (рис. 8).

Измерения выполнялись в пяти точках листа триплекса размером 500×700 мм, что представлялось эквивалентным пяти образцам триплекса. Мы видим, что результаты измере-

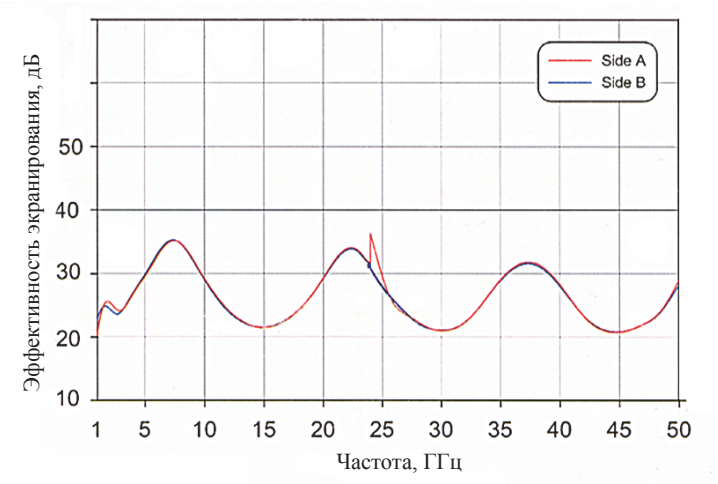


Рис. 7. Результаты измерений эффективности экранирования дуплексом со стороны серебряной пленки (side A) и с противоположной стороны (side B)

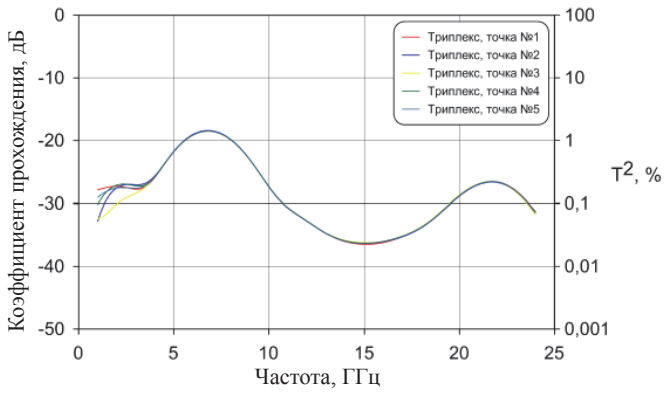


Рис. 8. Результаты измерений коэффициента прохождения через триплекс на каждом из пяти его участков при нормальном падении поля

ний совпали друг с другом, это свидетельствует как о равномерной толщине пленки на обеих сторонах дуплекса, так и о точности измерений.

Постановка защитного стекла в обычную раму не создает надлежащего эффекта защиты помещения из-за проникновения ЭМИ через рамы и щели, снижающие SE до 10 дБ [11]. Этот недостаток ликвидируется постановкой защитных материалов на сами рамы и щели между ними и стеной. Эти вопросы подробно исследовались в работах [8–11], куда мы и отсылаем заинтересованных читателей.

Заключение

Сравнение электродинамических характеристик зарубежных и отечественных триплексов показало их идентичность в части эффективности экранирования в широком диапазоне частот. Можно надеяться, что и другие характеристики сравниваемых устройств будут на одном уровне.

Вместе с тем, номенклатура защитных стекол не ограничивается дуплексами и триплексами. Большое значение могут иметь частотно селективные защитные стекла. Тому есть примеры из области защитных ограждений антенн и других экранов. Существует и целая область знаний в проектировании частотно селективных экранов [4]. Эти знания могут быть использованы при создании частотно селективных стекол. Тогда будет решена проблема защиты радиоэлектронной аппаратуры, персонала и энергосберегающих стекол, которыми оснащаются окна поездов и зданий, рубки кораблей, но которые препятствуют каналам мобильной связи.

Литература

1. Wilson C. High Altitude Electromagnetic Pulse (HEMP) and High Power Microwave (HPM) Devices: Threat Assessments / C. Wilson // Congr. Res. Serv. Report for Congress. 21 July 2008. P. 13. URL: at https://fas.org/sgp/crs/natsec/RL32544.pdf (дата обращения 9 ноября 2010).

2. Фортов В.Е. Взрывные генераторы мощных импульсов электрического тока / В.Е. Фортов. М.: Наука, 2002. 399 с.

3. Threat of Radio Frequency Weapons to Critical Infrastructure Facilities. URL: http://emprimus.com/lit/NavyReportRF-Weapons.pdf.

4. Tong X.C. Advanced Materials and Design for Electromagnetic Interference Shielding / X.C. Tong. CRC Press, 2010. 325 p.

5. Celozzi S. Electromagnetic Shielding / S. Celozzi, R. Araneo, G. Lovat. NY: IEEE Press, 2014. 355 p.

6. Ängskog P. Measurement of Radio Signal Protaction through Windows / P. Ängskog, M. Bäckström, B. Vallhagen // IEEE Int. Symp., 2015. P. 74-79. URL: http://dx.doi.org/10.1109/ISEMC.2015.7256135.

7. Carafano J.J. Attacks – What the U.S. Must Do Now / J.J. Carafano, R. Weitz // Backgrounder, 2010, Nov. 17, № 2491. P. 1-12. URL: http://thf_media.s3.amazonaws.com/2010/pdf/bg2491.pdf.

8. Штагер Е.А. Физические основы стелс-технологии / Е.А. Штагер. СПб.: ВВМ, 2014. 271 с.

9. Белов В.П., Штагер Е.А., Седов А.Н. Заявка на изобретение № 201628687/28 (044746) от 14.12.2016 г. Защитный прозрачный триплекс. СПб., 2015.

10. Белов В.П. Безопасность и экономичность – главные черты системы управления Казанского метрополитена / В.П. Белов, А.П. Голынский, К.Б. Потапов и др. СПб., 2006.

11. Штагер Е.А. Защита помещения с окнами от электромагнитных излучений: докл. на XVIII Всерос. науч.-практ. конф. «Актуальные проблемы защиты и безопасности / Е.А. Штагер. СПб., 2015.

A New Threat to the Safe Operation of Information-Control Systems of Electric Rolling Stock

Belov V. P.
Military Space Academy named after A. F. Mozhaysky
St. Petersburg, Russia
arsenal_belov@mail.ru

Shtager E. A.
Krylov state scientific center
St. Petersburg, Russia
shtager.e@mail.ru

Abstract. **Analysis of existing portable means of electromagnetic radiation, which can disrupt the functioning of the automated control systems of movement of trains, including underground trains. Considered one of the possibilities for the protection of personnel, electronic equipment control systems and security traffic –use of safety glasses domestic production. Analyzes frequency characteristics of shielding effectiveness, energy-efficient windows and glass, whuch may check the intentional electromagnetic radiation. Are proved Efficiency of resistance to penetration of an electromagnetic pulse through window jobs by replacing conventional glass on glass with a metallic coating.**

Keywords: **the shielding efficiency, electromagnetic terrorism.**

Reference

1. Wilson C. High Altitude Electromagnetic Pulse (HEMP) and High Power Microwave (HPM) Devices: Threat Assessments, *Congr. Res. Serv. Report for Congress*, 21 July 2008, pp. 13. Available at: https://fas.org/sgp/crs/natsec/RL32544.pdf (November 9, 2010).

2. Fortov V. E. Explosive Generators of Powerful Pulses of Electric Current [Vzryvnye generatori moshchnyh impulsov ehlektricheskogo toka]. Moscow, Nauka, 2002, 399 p.

3. Threat of Radio Frequency Weapons to Critical Infrastructure Facilities. Available at: http://emprimus.com/lit/NavyReportRFWeapons.pdf.

4. Tong X. C. Advanced Materials and Design for Electromagnetic Interference Shielding. CRC Press, 2010, 325 p.

5. Celozzi S., Araneo R., Lovat G. Electromagnetic Shielding. NY, IEEE Press, 2014, 355 p.

6. Ängskog P., Bäckström M., Vallhagen B. Measurement of Radio Signal Protaction through Windows. *IEEE Int. Symp. 2015*, pp. 74–79. Available at: http://dx.doi.org/10.1109/ISEMC.2015.7256135.

7. Carafano J. J., Weitz R. Attacks – What the U. S. Must Do Now. Backgrounder, 2010. 17 Nov., no. 2491, pp. 1-12. Available at: http://thf_media.s3.amazonaws.com/2010/pdf/bg2491.pdf.

8. Shtager E. A. Physical Bases of Stealth Technology. [Fizicheskie osnovy stels-tekhnologii]. St. Petersburg, VVM, 2014, 271 s.

9. Belov V. P., Shtager E. A., Sedov A. N. Application for Invention № 201628687/28 (044746) from 14.12.2016 “Protective transparent triplex”. St. Petersburg, 2015.

10. Belov V. P., Golynsky A. P., Potapov K. B., Garkusha M. I., Korenev L. Y. Safety and Cost Effectiveness-basic Features of the Control System of Kazan Metropolitan [Bezopasnost i ehkonomichnost glavnye-cherty sistemy upravleniya kazanskogo metropolitena]. St. Petersburg, 2006.

11. Shtager E. A. Protection of the Premises from Electromagnetic Radiation in the Space with Windows [Zashchita pomeshcheniya s oknami ot ehlektromagnitnyh izluchenij. Report on the XVIII all-Russian scientific-practical conference “Actual problems of protection and security”. St. Petersburg, 2015.

Проблемы защиты информации в приложениях для мобильных систем

Зубков К. Н., Диасамидзе С. В.
Петербургский государственный университет путей сообщения Императора Александра I
Санкт-Петербург, Россия
kirillzubkoff@gmail.com, sv.diass99@yandex.ru

Аннотация. **Мобильные телефоны в современном мире являются не просто средством связи, а устройством, которое содержит уязвимые персональные данные, несанкционированный доступ к которым может привести к непредсказуемым результатам. В настоящий момент современные средства защиты не позволяют в полной мере решить вопросы безопасности мобильных систем и оценить возможные риски потенциальных злоумышленных действий. В связи с этим возникает задача систематизировать основные угрозы и уязвимости мобильных приложений для последующего формирования методики по оцениванию угроз информационной безопасности в приложениях для мобильных систем.**

Ключевые слова: **мобильная операционная система, приложение, уязвимость, анализ защищенности, мобильная платформа, мобильное устройство.**

Введение

В соответствии с последними данными исследовательской компании eMarketer [1], специализирующейся на анализе рынка высоких технологий, смартфонами уже пользуется четверть мирового населения. Это около 2 млрд человек. И тенденция роста пользователей мобильных устройств продолжается. На рис. 1 представлена динамика роста числа пользователей смартфонов в период с 2013 по 2016 г. с прогнозом на 2017–2018 г.

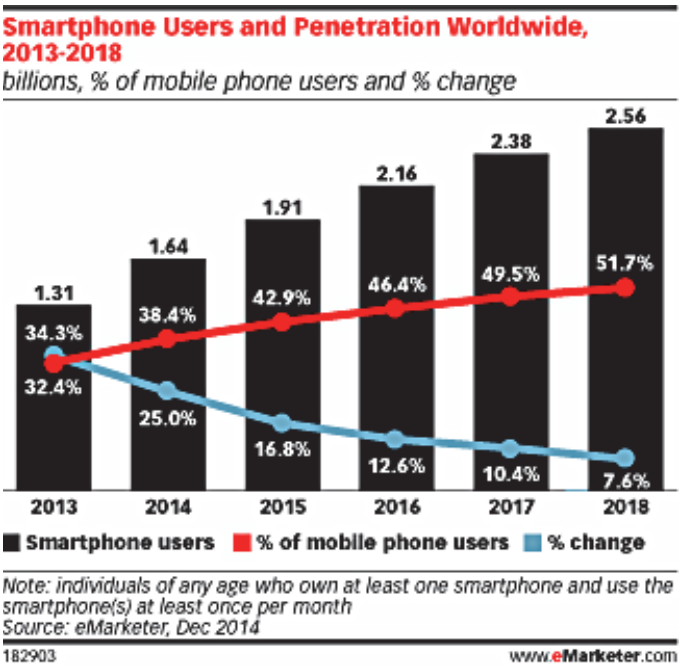


Рис. 1. Прогноз роста числа пользователей смартфонов

В настоящий момент Россия занимает пятое место в списке из 25 стран по числу пользователей мобильных устройств (рис. 2).

Мобильные телефоны в современном мире являются не просто средством связи, а устройством, которое содержит уязвимые персональные данные: номера кредитных карт, электронную почту, геолокационные сведения [2], профили в социальных сетях, средства удалённого доступа и управления предприятием, фотографии, видео и т. д. Несанкционированный доступ к таким чувствительным данным может привести к критической ситуации. Между тем, рынок мобильных

Top 25 Countries, Ranked by Smartphone Users, 2013-2018
millions

	2013	2014	2015	2016	2017	2018
1. China*	436.1	519.7	574.2	624.7	672.1	704.1
2. US**	143.9	165.3	184.2	198.5	211.5	220.0
3. India	76.0	123.3	167.9	204.1	243.8	279.2
4. Japan	40.5	50.8	57.4	61.2	63.9	65.5
5. Russia	35.8	49.0	58.2	65.1	71.9	76.4
6. Brazil	27.1	38.8	48.6	58.5	66.6	71.9
7. Indonesia	27.4	38.3	52.2	69.4	86.6	103.0
8. Germany	29.6	36.4	44.5	50.8	56.1	59.2
9. UK**	33.2	36.4	39.4	42.4	44.9	46.4
10. South Korea	29.3	32.8	33.9	34.5	35.1	35.6
11. Mexico	22.9	28.7	34.2	39.4	44.7	49.9
12. France	21.0	26.7	32.9	37.8	41.5	43.7
13. Italy	19.5	24.1	28.6	32.2	33.7	37.0
14. Turkey	15.3	22.6	27.8	32.4	37.2	40.7
15. Spain	18.9	22.0	25.0	26.9	28.4	29.5
16. Philippines	14.8	20.0	24.8	29.7	34.8	39.4
17. Nigeria	15.9	19.5	23.1	26.8	30.5	34.0
18. Canada	15.2	17.8	20.0	21.7	23.0	23.9
19. Thailand	14.4	17.5	20.4	22.8	25.0	26.8
20. Vietnam	12.4	16.6	20.7	24.6	28.6	32.0
21. Egypt	12.6	15.5	18.2	21.0	23.6	25.8
22. Colombia	11.7	14.4	16.3	18.2	19.7	20.9
23. Australia	11.4	13.2	13.8	14.3	14.7	15.1
24. Poland	9.4	12.7	15.4	17.4	19.4	20.8
25. Argentina	8.8	10.8	12.6	14.1	15.6	17.0
Worldwide* **	**1,311.2**	**1,639.0**	**1,914.6**	**2,155.0**	**2,380.2**	**2,561.8**

*Note: individuals of any age who own at least one smartphone and use the smartphone(s) at least once per month; *excludes Hong Kong; **forecast from Aug 2014; ***includes countries not listed*
Source: eMarketer, Dec 2014
182905 www.eMarketer.com

Рис. 2. Топ 25 стран по количеству пользователей мобильных устройств

приложений растёт с большой скоростью, а пользователи особенно не задумываются о том, какие разрешения они предоставляют приложениям, устанавливая их на свой смартфон, а также о последствиях, которые могут наступить.

Последний отчёт компании Digital Secuirty об исследовании российских приложений мобильного банкинга показал, что все они содержат, по крайней мере, одну уязвимость, позволяющую либо перехватить данные, передающиеся между клиентом и сервером, либо напрямую эксплуатировать уязвимости устройства и самого мобильного приложения [3].

Проблемы безопасности касаются не только банковского сектора. Игры на мобильных устройствах, множество других популярных приложений могут быть потенциально опасными. Например, популярное приложение «Музыка ВКонтакте», размещённое на площадке Google Play и имеющее довольно высокий рейтинг (4,5 из 5), а также более 500 тысяч скачиваний, вовсе похищало идентификационные данные пользователей, что приводило к потере доступа к профилю в социальной сети.

Всё это говорит о том, что существует реальная необходимость оценить текущее состояние информационной безопасности наиболее распространённых мобильных операционных систем, систематизировать основные угрозы и уязвимости мобильных приложений и составить детальный подход к разработке методики по оцениванию угроз информационной безопасности в приложениях для мобильных систем.

Популярные мобильные операционные системы

Сегодня наиболее распространёнными мобильными операционными системами являются ОС Android, iOS и ОС Windows Phone.

По последним данным, 8 из 10 современных мобильных устройств работают на базе операционной системы с открытым кодом Android. На рис. 3 приведена статистика с сайта https://www.statista.com. На графиках продемонстрированы доли рынка мобильных операционных систем в соответствии с продажами устройств конечным пользователям в период с 2009 по 2016 г. В третьем квартале 2015 г. 84,7 % от количества всех проданных смартфонов базировались на операционной системе Android.

По последним статистическим сведениям, ОС Android получила статус самой уязвимой. В 2016 г. на ОС Android специалисты по информационной безопасности нашли 523 уязвимости. На рис. 4 приведена статистика 2016 г., демонстрирующая количество уязвимостей на различных мобильных операционных системах.

Классификация приложений для мобильных устройств

Существует множество классификаций приложений для мобильных устройств, но в контексте информационной безопасности приложений следует выделить две большие группы:

• web-приложения, представляющие собой специальную версию web-сайта;

• мобильные приложения, разработанные под определённую мобильную операционную систему с использованием специализированного API.

Перед тем как рассматривать методологии анализа защищенности мобильных приложений, следует определить типовые уязвимости приложений и потенциальные угрозы несанкционированных действий для пользователя.

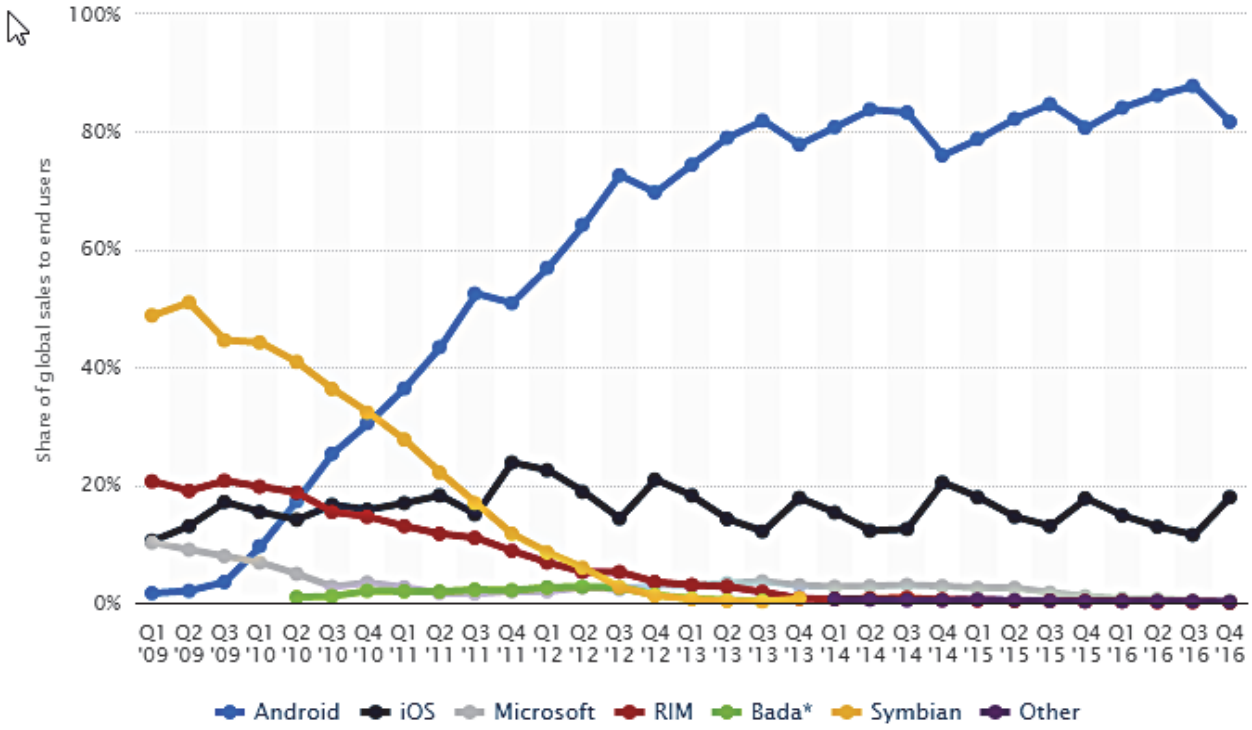


Рис. 3. Доли рынка мобильных операционных систем в соответствии с продажами мобильных устройств конечным пользователям в 2009–2016 гг.

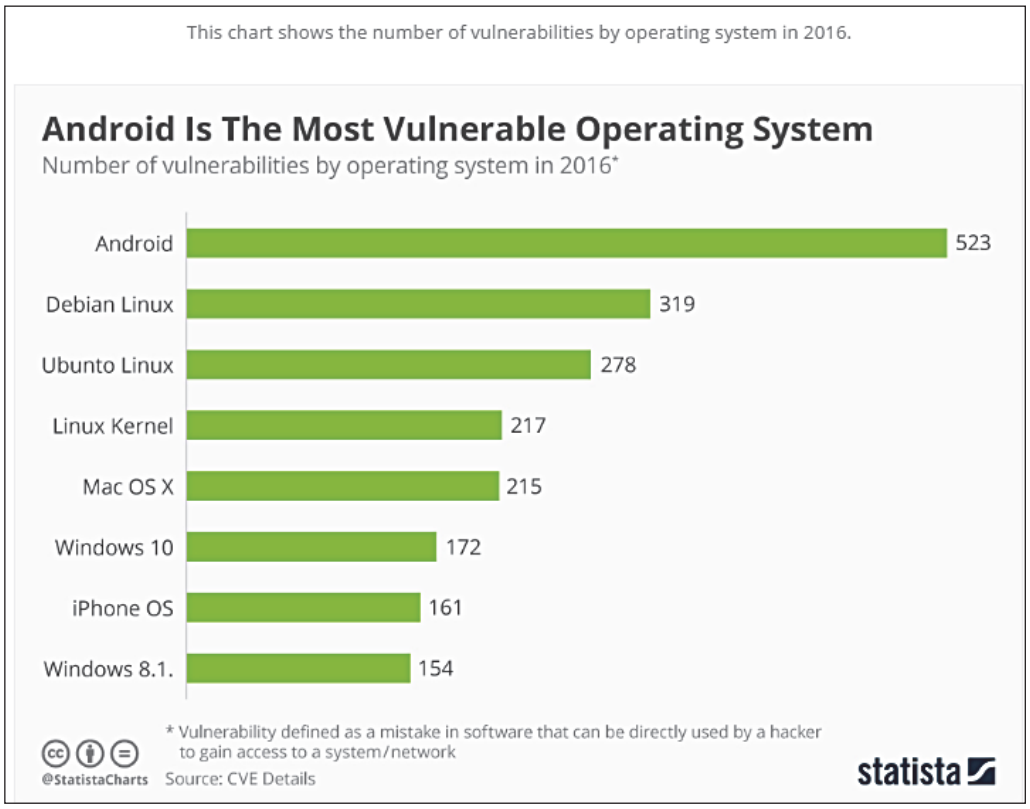


Рис. 4. Количество уязвимостей, найденных в мобильных операционных системах, 2016 г.

Типовые уязвимости

В соответствии с классификацией открытого проекта обеспечения безопасности web-приложений OWASP [4] (Open Web Application Security Project), к основным уязвимостям, которым подвержены мобильные устройства, относятся:

1) системные уязвимости (архитектурных решений мобильной платформы);

2) небезопасное хранение данных;

3) недостаточная защищенность протоколов передачи данных;

4) уязвимости системы авторизации и аутентификации;

5) слабая криптостойкость;

6) уязвимости кода приложения;

7) скрытый функционал приложений;

8) ненадлежащий контроль за клиентскими приложениями.

Остановимся на каждом из пунктов более подробно, акцентируя внимание на особенностях наиболее популярных мобильных операционных систем.

1. Уязвимости архитектурных решений мобильной платформы

Основная причина, по которой операционная система Android является наиболее слабо защищенной, – это отсутствие технологии подписывания ядра на уровне архитектуры платформы [5]. Суть подписи кода заключается в том, что она не позволяет выполняться в системе стороннему коду, не подписанному компанией, выпустившей мобильную операционную систему. Благодаря тесной взаимосвязи программного и аппаратного обеспечения в устройствах, например, под управлением iOS или Windows Phone, каждый шаг, начиная с нагрузки системы и заканчивая установкой приложений, анализируется с точки зрения безопасности и эффективности использования ресурсов. Целостность системы безопасности напрямую зависит от целостности и надежности ядра iOS. На рис. 5 схематично показана архитектура системы безопасности iOS, на рис. 6 – структурная схема операционной системы Android.

2. Небезопасное хранение данных

Этот раздел включает в себя следующие проблемы информационной безопасности:

• уязвимость «Hardcoded and Forgotten».

Это уязвимости, случайно созданные разработчиками при проектировании программного продукта.

Android-приложение представляет собой apk-файл (англ. Android Package – формат архивных исполняемых файлов-приложений для Android), т. е. архив, в котором хранятся исполняемые файлы, конфигурационные файлы, ресурсы приложения и т. д. Если распаковать архив apk и проанализировать конфигурационные файлы, то часто можно обнаружить строки кода, которые разработчики забыли убрать из финальной версии продукта. Эти строки кода чаще всего используются для отладки в течение периода разработки приложения, и они могут значительно облегчить злоумышленнику задачу получения данных конфиденциального характера или реализацию других несанкционированных действий;

• некорректное назначение прав доступа для файлов, которое создаёт приложение.

На этапе тестирования разработчики часто некорректно назначают права доступа и забывают редактировать их при финальном выпуске программного продукта, в связи с чем у злоумышленников появляется ещё больше возможностей для несанкционированного доступа;

• хранение важных данных на SD-карте.

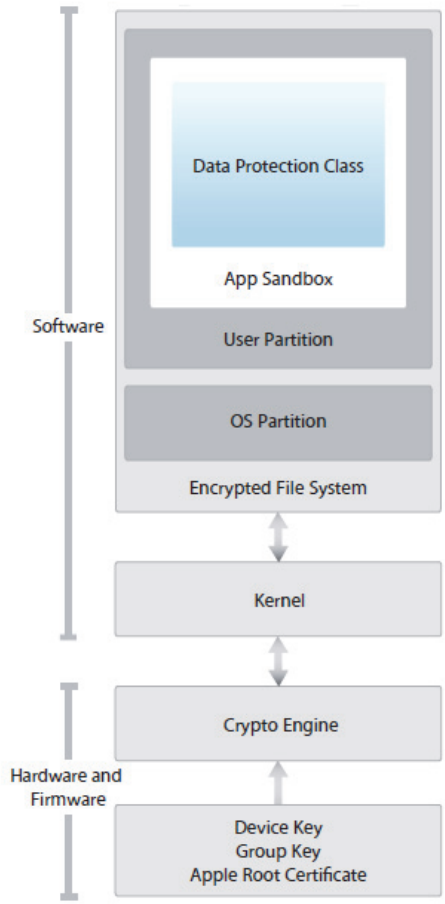


Рис. 5. Архитектура безопасности операционной системы iOS

Часто пользователи хранят важные данные на SD-карте, забывая, что эти данные доступны для всех приложений по умолчанию. Некоторые приложения могут хранить даже cookie-файлы (небольшой фрагмент данных, отправленный сервером для хранения браузером пользователя) и ISDN-токены на SD-картах;

• логирование [6].

Логи представляют собой файлы регистрации, содержащие записи обо всех событиях, происходящих в мобильной операционной системе, с высокой степенью детализации. В Android любое приложение при установке может запросить права доступа на чтение логов. Многие пользователи не обращают внимания на этот запрос, но опасность заключается в том, что любое устанавливаемое приложение, которое запросило доступ к чтению логов, и при этом получило одобрение со стороны пользователя, получит право чтения всей информации, которое приложение заносит в логи, если логирование не выключено пользователем. Зачастую в логи попадает вся отладочная информация и персональные данные без шифрования;

• получение прав суперпользователя.

Часто пользователи смартфонов стремятся к получению полного доступа к файловой системе устройства, чтобы обеспечить возможность установки сторонних приложений (не из официальных магазинов AppStore или Google Play Market). На мобильных устройствах компании Apple эта процедура называется Jail Break, а на Android-смартфонах – получение Root-прав (или прав суперпользователя). Стоит отметить, что jail-break или root – это компрометация всей системы безопасности устройства, а не просто опция, расширяющая возможности смартфона.

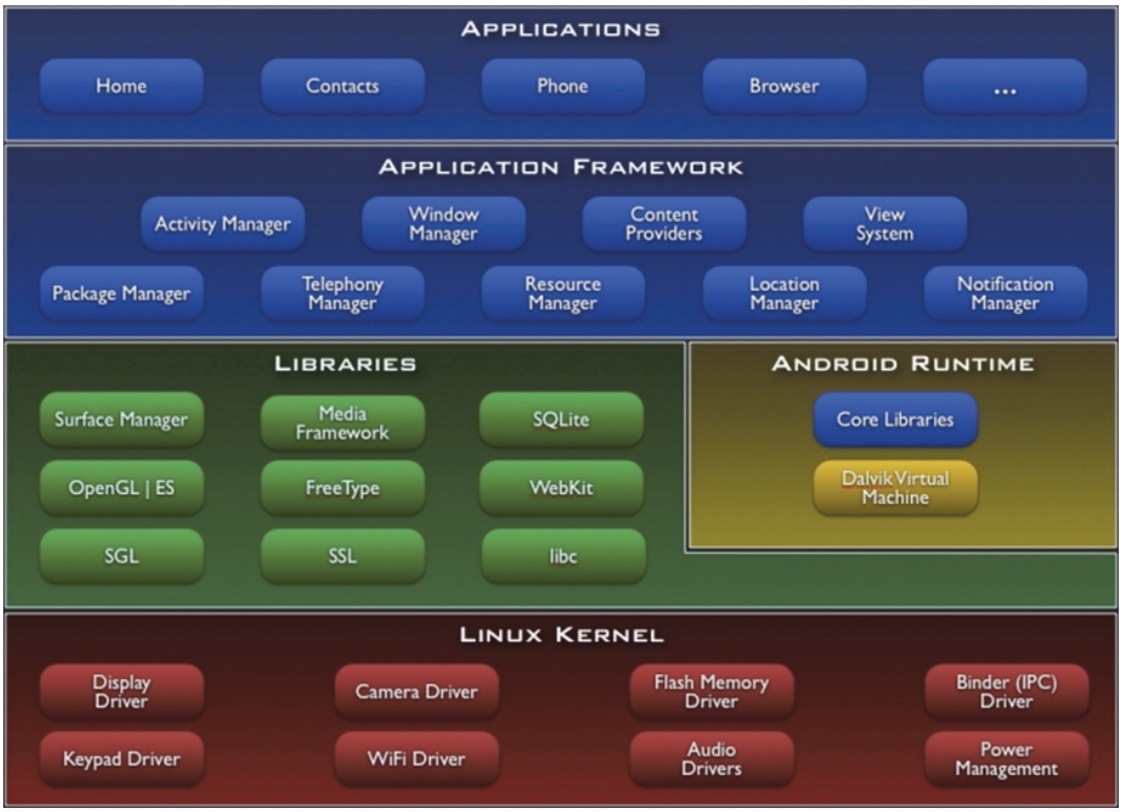


Рис. 6. Архитектура операционной системы Android

Меры, которые следует предпринимать для защиты персональных данных мобильного устройства от несанкционированного доступа:

• не допускать хранения важных данных на SD-карте;

• отключить логирование перед установкой приложений;

• при разработке приложений необходимо настроить права доступа с учетом того, что мобильное устройство пользователя может быть скомпрометировано root-правами;

• периодически просматривать конфигурационные файлы на предмет забытых отладочных строк кода, позволяющих получить несанкционированный доступ к персональным данным.

3. Недостаточная защищенность протоколов передачи данных

Основные проблемы:

• не используется шифрование при передаче данных (например, использование протокола http вместо https);

• при передаче данных используются самоподписанные сертификаты;

Меры по обеспечению информационной безопасности:

• проверка трафика мобильного приложения;

• использование web-сниффера, который будет анализировать трафик мобильных приложений и проверять, чтобы важные данные уходили в зашифрованном виде по протоколу https;

• использование сертификатов, подписанных доверенными центрами;

• при использовании контент-провайдеров (предоставляющих доступ к файлам или базам данных для других приложений) проверка и прописывание прав доступа.

4. Слабая авторизация [7]:

• анонимная работа с приложением.

Требования к защищенности мобильных приложений не такие, как к web-приложениям. Предполагается, что пользователь может работать оффлайн, поэтому часто используется онлайн-авторизация с последующим хранением данных в сессионных cookie-файлах.

После того как были введены идентификационные данные (логин и пароль) и приложение авторизовало пользователя, оно сохраняет специальный идентификатор, который в дальнейшем предъявляется серверу при каждом запросе, поступающем от приложения.

Если злоумышленник получил идентификатор пользователя и при этом в системе не были реализованы процедуры проверки IP-адреса сессии или наличия более одного соединения в пределах сессии, злоумышленник сможет получить доступ в систему с правами аккаунта пользователя. Если это приложения, связанные с интернет-банкингом или с личным кабинетом платежной системы, то о последствиях несанкционированного доступа в таком случае догадаться нетрудно;

• слабые пароли.

Считается, что в мобильных приложениях пароли не должны быть длинными, и большинство приложений разрешает создавать пароли от четырех символов. При этом пароли в большинстве случаев не шифруются и помещаются в базу в хешированном виде. Если злоумышленник получил доступ к базе данных, то с помощью готовых хэш-таблиц расшифровать пароли из четырех символов для него – тривиальная задача, требующая незначительных временны́х затрат.

Меры защиты при данном типе уязвимости:

• аутентификация в мобильном приложении должна соответствовать таковой в web-версии;

• локальная аутентификация должна работать через cookie-файлы только после авторизации на сервере;

• создание сложных паролей длиной более 6 символов.

5. Ненадлежащий контроль за клиентскими приложениями

Это процесс верификации загружаемого в магазины Appstore программного обеспечения. Перед тем как попасть на площадку App Store, iOS-приложения детально проверяются на наличие уязвимостей и на соответствие стандартам разработки Apple. Каждое приложение, устанавливаемое на iOS, должно быть подписано специальным сертификатом «iOS Developer Program», выдаваемым компанией Apple только после целого ряда необходимых проверок. Такие меры безопасности обеспечивают отсутствие вредоносного программного обеспечения в магазине приложений App Store.

К тому же в операционной системе iOS реализована политика «песочницы» (sandbox) для всех сторонних приложений. У каждого приложения есть строго определённая директория, создаваемая во время его установки на мобильное устройство, в которую помещаются файлы приложения. При необходимости доступ к системной информации приложение может получить посредством API или системных служб.

Если говорить об операционной системе Android, то перед загрузкой приложений на площадку Google Play приложения не проверяются на наличие вредоносного кода. Вместо процедуры предварительной проверки компанией Google реализован механизм регулярного автоматического сканирования магазина приложений на предмет потенциально вредоносного программного обеспечения. Как показывает практика, этот метод анализа информационной безопасности повышает процент проникновения вредоносных приложений и их дальнейшего распространения на конечные устройства пользователей.

При установке нового приложения на мобильное устройство на операционной системе Android пользователю предоставляется полный перечень прав доступа, запрашиваемых приложением. Внимательно изучив этот перечень, пользователь может самостоятельно определить потенциально вредоносное программное обеспечение и отменить его установку. Например, если приложение, базовое функциональное предназначение которого – фонарь, запрашивает доступ к контактным данным либо подключение к Интернету, то данное приложение с высокой долей вероятности можно отнести к вредоносному программному обеспечению.

В iOS раздача прав доступа приложениям реализована более гибко. Каждая категория доступа, будь то доступ к камере или к GPS, должна быть либо подтверждена, либо отклонена пользователем.

Таким образом, обязательная подпись кода приложений и корректное исполнение политики безопасности расширяет рамки действия принципа доверия с уровня операционной системы на уровень приложений и препятствует выполнению вредоносного или самомодифицирующегося кода.

Методы анализа защищённости мобильных приложений

Существуют различные методы оценивания угроз информационной безопасности в приложениях для мобильных систем, которые применяются как в отдельности, так и в совокупности. Разделить их можно на две большие категории: статистические и динамические.

В качестве методов динамического анализа используются:

- стресс-тестирование;
- анализ сетевого трафика мобильного приложения;
- анализ памяти приложения;
- анализ взаимодействия приложения с файловой системой.

К методам статистического анализа относятся [9]:

- аудит безопасности кода приложения;
- Reverse Engineering;
- дизассемблирование;
- декомпиляция.

Для комплексной оценки состояния защищенности мобильной системы необходимо исследовать три составляющих: клиентскую часть, серверную часть и непосредственно канал связи. Для этого применяют такие методы:

- комплексный анализ архитектуры клиентской и серверной части приложения;
- моделирование угроз в соответствии с логикой приложения;
- проектирование модели нарушителя.

Заключение

Несмотря на большое количество методов обеспечения безопасности информации, хранящейся на мобильных устройствах, уровень распространения вредоносных приложений в мобильном сегменте растёт высокими темпами. Угрозы безопасности создают риски персональным данным пользователя, риски компрометации критичных данных вплоть до хищения денежных средств. К тому же разработчики мобильных приложений не всегда уделяют достаточного внимания проблемам безопасности или просто не следуют руководствам по безопасной разработке.

На настоящий момент ни высокие рейтинги приложения, ни большое количество скачиваний, ни список ресурсов, доступ к которым пользователь предоставляет приложению перед его установкой, не позволяют оценить возможные риски персональным данным и последствия потенциальных злоумышленных действий. Современные средства защиты (антивирусы, снифферы) могут помочь предотвратить определенный спектр угроз, но их применение не позволит решить проблему безопасности комплексно. В связи с этим возникает задача разработки комплексной методики по оцениванию угроз информационной безопасности в приложениях для мобильных систем, а также методики анализа приложений на предмет их соответствия требованиям информационной безопасности.

Литература

1. Аналитический центр InfoWatch. Глобальное исследование утечек корпоративной информации и конфиденциальных данных, 2016. URL: https://www.infowatch.ru/report2016 (дата обращения 01.05.2017).

2. Михайлов Д. М. Исследование уязвимости мобильных устройств систем Apple и Google / Д. М. Михайлов, А. В. Зуйков, И. Ю. Жуков и др. // Спецтехника и связь, 2011, № 6. С. 38-40. URL: http://cyberleninka.ru/article/n/issledovanie-uyazvimosti-mobilnyh-ustroystv-sistem-apple-i-google#ixzz4hjVQGz9w.

3. Корниенко А. А. Информационная безопасность и защита информации на железнодорожном транспорте: в 2 ч. Ч. 1: Методология и система обеспечения информационной безопасности на железнодорожном транспорте / А. А. Корниенко, С. Е. Ададуров, А. П. Глухов. М.: УМЦ ЖДТ, 2014. 440 с.

4. Anton K. OWASP Top-10 Proactive Controls 2016 / K. Anton, J. Bird, J. Manico // The OWASP Foundation. 2016 February. URL: https://www.owasp.org/images/5/57/OWASP_Proactive_Controls_2.pdf.

5. Rovelli P. Developing a Next-generation Mobile Security Solution for Android. April 2014 School of Computer Science Reykjavík University / P. Rovelli. URL: http://skemman.is/stream/get/1946/19500/43671/1/Developing_a_next-generation_Mobile_Security_solution_for_Android_-_Paolo_Rovelli.pdf.

6. Сафин Л. К. Исследование информационной защищенности мобильных приложений / Л. К. Сафин, А. В. Чернов, Я. А. Александров, К. Н. Трошина // Вопр. кибербезопасности, 2015, № 4 (12). С. 28-37. URL: http://cyberleninka.ru/article/n/issledovanie-informatsionnoy-zaschischennosti-mobilnyh-prilozheniy.

7. Diasamidze S. V. Implementation of the Role Based Access Control in Application for Mobile Device on the Android OS Platform / S. V. Diasamidze, E. Yu. Kuzmenkova, D. A. Kuznetsov, A. R. Sarkisyan // Интеллектуальные технологии на транспорте, 2016, № 1. С. 21-26.

8. Толюпа Е. А. Метод обеспечения безопасности пользователей интернет-магазинов мобильных приложений / Е. А. Толюпа // Прикладная дискретная математика. Приложение, 2014, № 7. С. 101-103. URL: http://cyberleninka.ru/article/n/metod-obespecheniya-bezopasnosti-polzovateley-internet-magazinov-mobilnyh-prilozheniy.

9. Цыганенко Н. П. Статический анализ кода мобильных приложений как средство выявления его уязвимостей / Н. П. Цыганенко // Тр. БГТУ. Сер. 6: Физико-математические науки и информатика, 2015, № 6. С. 200-203. URL: http://cyberleninka.ru/article/n/staticheskiy-analiz-koda-mobilnyh-prilozheniy-kak-sredstvo-vyyavleniya-ego-uyazvimostey.

Formation Security Problems in Applications for Mobile Systems

Zubkov K. N.,
Diasamidze S. V.
Emperor Alexander I Petersburg State Transport University
St. Petersburg, Russia
e-mail: kirillzubkoff@gmail.com,
sv.diass99@yandex.ru

Abstract. **Mobile phones are not just communications facilities nowadays, but the devices which are the storage of sensitive personal data and unauthorized access to them can lead to unpredictable results. Nowadays modern information security solutions don't allow to resolve the security issues of mobile systems and to assess the possible risks of potential malicious acts. So the problem of systematization of the main mobile applications threats and vulnerabilities becomes important for the following developing of methodology connected with evaluation of information security threats in applications for mobile systems.**

Keywords: **mobile operation system, application, vulnerability, security analysis, mobile platform, mobile device.**

References

1. InfoWatch Analytical Centre. Global research of corporate information leaks and confidential data, 2016 [Analiticheskii Tsentr InfoWatch. Global'noe issledovanie utechek korporativnoi informatsii i konfidentsial'nykh dannykh, 2016]. Available at: https://www.infowatch.ru/report2016 (accessed 1 May 2017).

2. Mikhailov D. M., Zuikov A. V., Zhukov I.Iu., Bel'tov A. G., Starikovskii A. V., Froimson M. I., Tolstaia A. M. Study of the Vulnerability of Mobile Devices of Apple and Google Systems [Issledovanie uiazvimosti mobil'nykh ustroistv sistem Apple i Google], *Special Technics and Communication [Spetstekhnika i sviaz']*, 2011, no. 6, pp. 38-40.

3. Kornienko A. A., Adadurov S. E., Glukhov A. P. Information Security and Information Protection in Rrailway Transport [Informatsionnaia bezopasnost' i zashchita informatsii na zheleznodorozhnom transporte]: in 2 is. – Is. 1: Methodology and system for ensuring information security in railway transport [Metodologiia i sistema obespecheniia informatsionnoi bezopasnosti na zheleznodorozhnom transporte]. Moscow, UM ZhDT, 2014. 440 p.

4. Anton K., Bird J., Manico J. OWASP Top-10 Proactive Controls 2016. *The OWASP Foundation*, February, 2016. Available at: https://www.owasp.org/images/5/57/OWASP_Proactive_Controls_2.pdf.

5. Rovelli P. Developing a Next-generation Mobile Security Solution for Android. April 2014 School of Computer Science Reykjavík University. Available at: http://skemman.is/stream/get/1946/19500/43671/1/Developing_a_next-generation_Mobile_Security_solution_for_Android_-_Paolo_Rovelli.pdf.

6. Safin L. K., Chernov A. V., Aleksandrov Ia. A., Troshina K. N. A Study of Mobile Application Security. [Issledovanie informatsionnoi zashchishchennosti mobil'nykh prilozhenii]. *Cybersecurity issues* [*Voprosy kiberbezopasnosti*], 2015, № 4 (12), pp. 28-37. Availble at: http://cyberleninka.ru/article/n/issledovanie-informatsionnoy-zaschischennosti-mobilnyh-prilozheniy.

7. Diasamidze S. V., Kuzmenkova E. Yu., Kuznetsov D. A., Sarkisyan A. R. Implementation of the Role Based Access Control in Application for Mobile Device on the Android OS Platform // Intelligent technologies in transport [Intellektual'nye tehnologii na transporte], 2016, no. 1, pp. 21-26.

8. Toliupa E. A. Method to Provide Safety for Customer of Application's Store [Metod obespecheniia bezopasnosti pol'zovatelei internet-magazinov mobil'nykh prilozhenii], *Applied Discrete Mathematics. Application [Prikladnaia diskretnaia matematika. Prilozhenie]*, 2014, no. 7, pp. 101-103. Available at: http://cyberleninka.ru/article/n/metod-obespecheniya-bezopasnosti-polzovateley-internet-magazinov-mobilnyh-prilozheniy.

9. Tsyganenko N. P. The Static Analysis of Mobile Applications Code as Vulnerabilities Detection Method [Staticheskii analiz koda mobil'nykh prilozhenii kak sredstvo vyiavleniia ego uiazvimostei], *Proceedings of BGTU. Series 6: Physics and Mathematics and Computer Science [Trudy BGTU. Seriia 6: Fiziko-matematicheskie nauki i informatika]*, 2015, no. 6, pp. 200-203. Available at: http://cyberleninka.ru/article/n/staticheskiy-analiz-koda-mobilnyh-prilozheniy-kak-sredstvo-vyyavleniya-ego-uyazvimostey.

Преимущество гиперконвергентных систем над облачными технологиями

Носкова А. И., Токранова М. В.
Петербургский государственный университет путей сообщения Императора Александра I
Санкт-Петербург, Россия
magistrpgups@rambler.ru

Аннотация. **Статья посвящена актуальности облачных технологий и гиперконвергентных систем, что вызвано популярностью их использования как крупными, так и небольшими компаниями. Большинство предприятий переводят свои сервисы и приложения в облака, в первую очередь, по причине снижения затрат на приобретение собственной ИТ-инфраструктуры. Однако облачные вычисления не являются в полной мере идеальным решением. Такие недостатки, как жесткая зависимость от поставщиков, хранение конфиденциальной информации на чужих ресурсах, невозможность полного контроля безопасности данных, вынуждают искать другие, более надежные, варианты. Конвергентные и гиперконвергентные системы являются альтернативой аренды облаков у сторонних компаний. С их помощью стало возможным развертывание частных облаков, которыми полностью распоряжаются предприятия.**

Ключевые слова: **гиперконвергентные системы, облачные вычисления, IaaS, PaaS, SaaS.**

Введение

Новые технологии и модели обслуживания способны изменить деятельность компаний и стать важнейшими стимулами инноваций и сокращения текущих расходов. Многие ИТ-поставщики переносят свои продукты в облако. Под облачными вычислениями понимается модель обеспечения удобного доступа по сети к конфигурируемым вычислительным ресурсам [1]. Например, к сетям передачи данных, серверам, устройствам хранения данных, приложениям и сервисам – как вместе, так и по отдельности. Основные причины нарастающей популярности облаков – быстрое и простое развертывание, непосредственный доступ к ресурсам, мгновенная масштабируемость, разработка и тестирование ПО по запросу, оплата фактического использования. Благодаря этому облачная модель распространяется все шире и представляет собой жизнеспособную альтернативу решениям с использованием собственной площадки [2].

Основные варианты построения облачной архитектуры (рис. 1):

- инфраструктура по требованию (Infrastructure as a Service, IaaS);
- платформа по требованию (Platform as a Service, PaaS);
- программа по требованию (Software as a Service, SaaS).

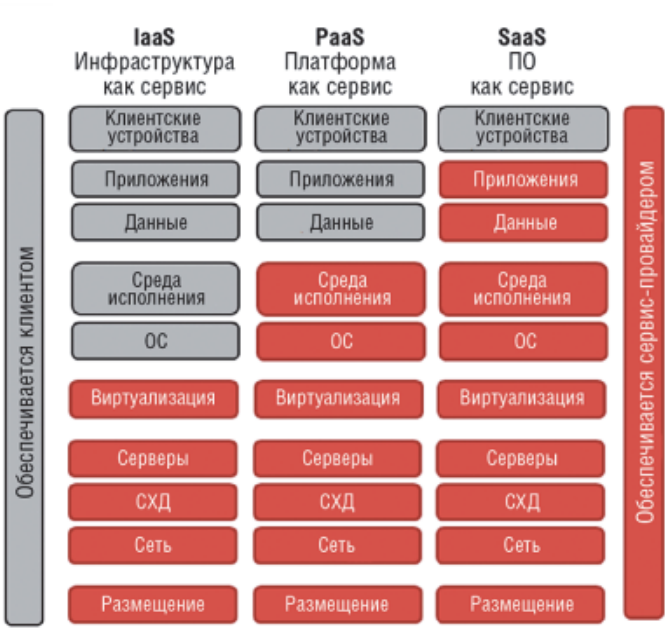


Рис. 1. Основные варианты построения облачной архитектуры IaaS

IaaS

IaaS (Infrastructure as a Service) – модель обслуживания, в которой заказчики арендуют вычислительные мощности для развертывания и использования виртуализованных экземпляров операционных систем и программных продуктов [3] (рис. 2). Компании любого масштаба могут получить

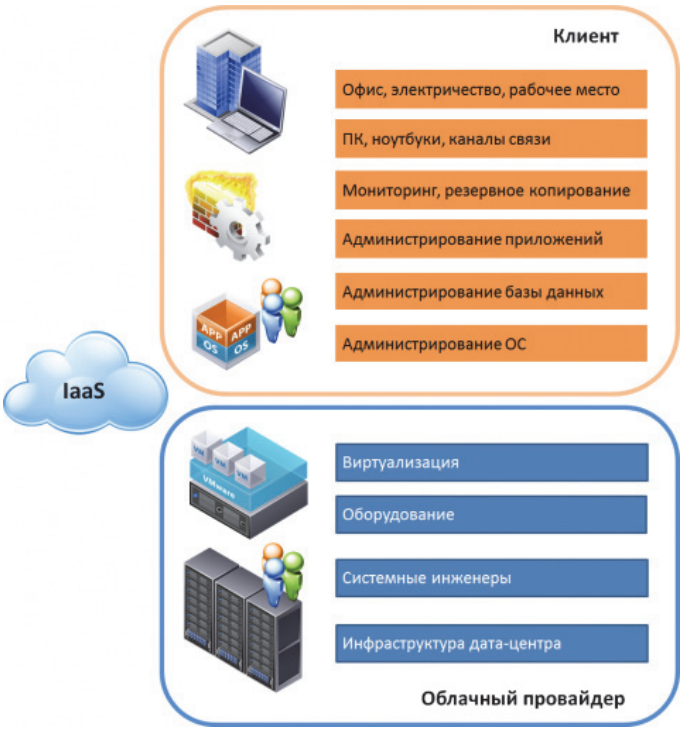


Рис. 2. IaaS (Infrastructure as a Service)

доступ к самым современным центрам обработки данных (ЦОД), защищенным серверам и высокопроизводительным системам хранения.

В соответствии с IaaS, серверы и другие ресурсы предоставляются заказчику по мере необходимости через облако. Данная модель обеспечивает самообслуживание и доступ к ИТ-ресурсам по запросу. Это означает, что на создание необходимых инструментов разработчикам потребуется минимальное количество временных затрат без приобретения собственных мощностей.

Потребителю отраслевых решений предоставляется базовая инфраструктура, в частности, необходимое оборудование и каналы передачи данных. Потребитель должен сам настроить платформу и приложения, например, установить операционную систему и необходимые программные компоненты. При аренде виртуальной инфраструктуры можно воспользоваться услугами разного масштаба: виртуальным сервером и виртуальной сетью. В первом случае арендуется единственный виртуальный сервер, во втором – пул виртуальных серверов с возможностью их объединения в виртуальную сеть [4].

Оборудование, на котором построена виртуальная инфраструктура, находится в специализированных ЦОД. В этих центрах обеспечивается резервирование каналов связи, защита от перебоев с электричеством и всё, что непосредственно связано с работоспособностью и доступностью оборудования.

При использовании модели IAAS возможны два варианта тарификации:

• продажа ресурсов сервис-провайдера, лимитированных только производительностью хоста. Оплата производится строго за потребленный объем мощностей, который ежечасно мониторится. Такая система резервирования ресурсов наиболее оптимальна для компаний с сезонными пиками нагрузки, когда вычислительные мощности требуются периодически или скачкообразно. Потребность в вычислительных мощностях значительно колеблется;

• гарантированное выделение ресурсов. В этом случае резервируется определенный объем ресурсов, который используется заказчиком, с ежемесячным фиксированным платежом. Данный вариант предоставления ресурсов менее гибкий в части оплаты, однако более стабильный в части выделения ресурсов и работы систем заказчика. Ресурсы всегда зарезервированы вне зависимости от загрузки ресурсов другими клиентами. Такая система резервирования ресурсов идеально подходит для компаний с нормированной нагрузкой.

Подводя итог, можно сказать, что при использовании IAAS заказчик получает полные административные права внутри арендованных виртуальных серверов, в зоне ответственности провайдера лежит только организация доступа к серверу по сети и обеспечение работоспособности оборудования и базового инфраструктурного ПО. Недостаток данной модели – то, что обслуживание ориентировано на предоставление услуг ИТ-компаниям, которые самостоятельно занимаются разработкой ПО.

PaaS

PaaS (Platform as a Service) – модель предоставления облачных вычислений, при которой потребитель получает доступ к использованию информационно-технологических платформ: операционных систем, систем управления базами данных, связующему программному обеспечению, средствам разработки и тестирования, размещённым у облачного провайдера [5] (рис. 3). В этой модели всей информационно-технологической инфраструктурой, включая вычислительные сети, серверы, системы хранения, целиком управляет провайдер. Также он определяет наборы доступных для потребителей видов платформ и управляемых параметров платформ, а потребителю предоставляется возможность использовать платформы, создавать их виртуальные экземпляры, устанавливать, разрабатывать, тестировать, эксплуатировать на них прикладное ПО, при этом динамически изменяя количество потребляемых вычислительных ресурсов.

Рис. 3. PaaS (Platform as a Service)

PaaS дает возможность выполнять весь перечень операций разработки, тестирования и разворачивания веб-приложений в одной интегрированной среде, тем самым исключая затраты на поддержку отдельных сред для отдельных этапов [6].

Оплата облачной платформы может взиматься в зависимости от уровня потребления. Ценообразование облачных сервисов складывается из следующих элементов:

• плата за вычислительные мощности;

• плата за лицензии используемого ПО (программ виртуализации, операционных систем, приложений);

• надбавка сервис-провайдера.

Большинство существующих PaaS-платформ направлено в первую очередь на удовлетворение интересов разработчиков. Они позволяют создавать масштабируемые веб-приложения с более низкими затратами по сравнению с моделью IaaS, но наряду с этим имеются существенные недостатки: отсутствуют свободный выбор технологий и контроль над низкоуровневыми компонентами системы, также система недостаточно производительна, так как при обмене

данными с провайдерами PaaS рекомендуется использовать шифрование данных, а это требует дополнительных процессорных мощностей.

SaaS

SaaS (Software as a Service) – модель обслуживания, при которой подписчикам предоставляется готовое прикладное программное обеспечение, полностью обслуживаемое провайдером [7] (рис. 4). Поставщик в этой модели самостоятельно управляет приложением, предоставляя заказчикам доступ к функциям с клиентских устройств, как правило, через мобильное приложение или веб-браузер.

Как и во всех формах облачных вычислений, заказчики платят не за владение программным обеспечением, а за его аренду (пользователю не нужно инсталлировать программу на свой компьютер). Таким образом, в отличие от классической схемы лицензирования ПО, заказчик несет сравнительно небольшие периодические затраты, и ему не требуется инвестировать значительные средства в приобретение прикладной программы [8, 9].

Рис. 4. SaaS (Software as a Service)

При использовании SaaS схема периодической оплаты предполагает, что при временном отсутствии необходимости в ПО заказчик может приостановить его использование и заморозить выплаты разработчику. Контракт на аренду SaaS включает в себя плату не только за использование ПО, но и за все затраты, связанные с поддержкой его работоспособности, обновлением и защитой данных [10].

Основное достоинство модели SaaS для потребителя услуги – отсутствие затрат, связанных с установкой, обновлением и поддержкой работоспособности оборудования и работающего на нём программного обеспечения. Несмотря на очевидное преимущество данной модели, имеется ряд сдерживающих факторов, ограничивающих её использование. Во-первых, концепция SaaS применима далеко не для всех функциональных классов систем. Во-вторых, поскольку основная экономия ресурсов SaaS-провайдера достигается за счёт масштаба, SaaS-модели неэффективны для систем, требующих адаптации под каждого заказчика, а также инновационных решений.

Проведя обзор моделей облачных вычислений, можно выделить ряд общих проблем:

- для получения доступа к услугам облака необходимо постоянное подключение к сети Интернет;
- использование облачных вычислений ограничивает заказчика в выборе ПО, а также не дает возможности настраивать его под собственные цели;
- безопасность конфиденциальной информации не гарантируется, поскольку сегодня нет технологий, которые обеспечивают это в полной мере.

Одним из вариантов решений данных проблем являются гиперконвергентные системы, которые имеют ряд преимуществ перед основными моделями представлений.

Гиперконвергентные системы

Гиперконвергенция позволяет упростить архитектуру вычислительных систем за счет отказа от отдельного уровня хранения. Гиперконвергентные системы пользуются всё большей популярностью. В отличие от прежних архитектур, гиперконвергентная не приводит к образованию изолированных ресурсов хранения, чтобы каждый сервер мог воспользоваться ими на других системах, она опирается на программно-определяемые решения в области хранения [11]. Гиперконвергентная система представляет собой объединённые в одном корпусе сервер, систему хранения данных и сетевой коммутатор (рис. 5). Однако самой главной частью является адаптированное ПО, включая программные контроллеры – некие массовые устройства, не требующие наладки и доводки, обладающие широчайшей совместимостью и универсальные в применении. Именно на уровне программного контролера гиперконвергентные системы выделяются за счет их легкого масштабирования. Для увеличения емкости и производительности нужно добавить новый блок. Вместо усиления мощности за счет увеличения числа дисков, количества памяти или процессоров производительность увеличивается за счет добавления большего числа модулей [12].

Рис. 5. Архитектура гиперконвергентных систем

Таким образом, гиперконвергентная инфраструктура – это инфраструктура, в которой вычислительные мощности, хранилища, серверы, сети объединяются с помощью программных средств и управляются через общую консоль администрирования. По этой причине вместо команды IT-специалистов для управления хранилищами данных и серверным оборудованием порой достаточно одного системного администратора.

Гиперконвергентные системы обычно состоят из нескольких физических модулей, объединяемых в горизонтально масштабируемый кластер. Каждый из них содержит вычислительное ядро, ресурсы хранения, сетевые компоненты и гипервизор. Наличие гипервизора не обязательно, но он имеется во всех основных продуктах известных производителей, причем часто можно выбрать из двух и более гипервизоров [13].

Отдельное устройство имеет от одного до четырех узлов, каждый из которых представляет собой самостоятельный сервер с процессором и памятью в общем шасси. Гиперконвергентные кластеры обычно содержат от 4 до 64 узлов, хотя некоторые производители не указывают конкретных пределов масштабируемости. Чтобы узлы могли совместно использовать ресурсы хранения, применяется ПО для создания виртуальной сети хранения или кластерная файловая система. Программное обеспечение для реализации гиперконвергентной инфраструктуры может предлагаться как отдельно, так и предустановленным на физические устройства.

В основном на рынке предлагаются полностью готовые самодостаточные вычислительные системы. Поставщики разрабатывают собственное ПО для реализации функций хранения и управления, либо эти функции выполняются на используемом гипервизоре [14]. Во многих продуктах используется виртуальное устройство хранения (Virtual Storage Appliance, VSA) для объединения ресурсов хранения в общий пул. Другой подход состоит в использовании платформы VMware EVO: RAIL, в которой функции хранения и управления интегрированы в соответствующий гипервизор.

Преимущества конвергентных систем проистекают из суммы двух компонентов: аппаратной части и программного обеспечения:

• простота архитектуры и управления. Благодаря интеграции всех компонентов в одном корпусе с общей системой управления не требуется привлекать целую команду специалистов, обладающих знаниями и опытом в области виртуализации, систем хранения данных, серверов и сетей;

• упрощенное взаимодействие с пользователями в условиях среды с высоким уровнем визуализации;

• низкая стоимость. Гиперконвергентная система не приводит к существенному увеличению капитальных затрат. При необходимости масштабирования вы можете точно оценить будущие затраты, поскольку соотношение ресурсов хранения данных и вычислительных ресурсов всегда постоянное;

• высокая автоматизация и управление на основе заданных правил позволяют гибко и легко управлять распределением ресурсов и рабочей нагрузки;

• сокращение числа управляемых систем. Один гиперконвергентный узел объединяет вычислительные ресурсы и ресурсы хранения данных, что ведет к уменьшению числа отдельных устройств и как следствие – к уменьшению количества объектов, которые надо покупать, устанавливать и обслуживать. Также более легкому развертыванию и обслуживанию гиперконвергентных устройств способствует то, что они базируются на стандартных серверных компонентах. Наконец, наличие во многих решениях интегрированных инструментов управления упрощает задачи администрирования;

• упрощение масштабирования. Гиперконвергентные системы рассчитаны не на вертикальное, а на горизонтальное масштабирование. Гиперконвергентная архитектура интегрирует ПО для распределенных вычислений, которое автоматически обнаруживает новые узлы и добавляет их в кластер, предоставляя дополнительные вычислительные ресурсы и ресурсы хранения при добавлении каждого нового модуля.

Среди минусов, присущих гиперконвергенции, отметим невозможность гранулярного обновления или настройки системы. Рост хранилища данных и повышение производительности являются критически важными показателями для любой компании. Если емкость системы хранения данных кластера практически закончилась, однако по вычислительным ресурсам еще имеется хороший резерв, то пользователь будет вынужден увеличить общую вычислительную мощность путем добавления новых устройств. Точно так же возникновение потребности в настройке конфигурации дисков хранилища для определенного приложения может повлечь за собой похожую проблему. Исключение состоит в построении собственной платформы. Имеется возможность добавлять только системы хранения данных или только вычислительную мощность при выборе подхода VSA.

Заключение

После обзора моделей представления облачных вычислений выделены их основные недостатки: безопасность хранения данных, необходимость постоянного подключения к Интернету, ограничения в используемом ПО. Было предложено альтернативное решение – гиперконвергентные системы, которые имеют преимущества над облачными вычислениями: единый программный интерфейс управления вычислительными ресурсами, легкость масштабирования, а также снижение затрат на общую стоимость владения IT-инфраструктурой за счет глубокой автоматизации и самообслуживания.

Литература

1. https://en.wikipedia.org/wiki (дата обращения 15.04.2017).

2. Amrhein D. Cloud Computing for the Enterprise: Part 1: Capturing the Cloud / D. Amrhein, S. Quint. URL: http://www.ibm.com/developerworks/websphere/techjournal/0904_amrhein/0904_amrhein.html (дата обращения 16.04.2017).

3. Орландо Д. Модели сервисов облачных вычислений: инфраструктура как сервис / Д. Орландо. URL: http://www.ibm.com/developerworks/ru/library/cloudservices1iaas (дата обращения: 16.04.2017).

4. Sheu P.C.-Y. Semantic Computing, Cloud Computing, and Semantic Search Engine / P.C.-Y. Sheu, S. Wang, Q. Wang et al. // IEEE Int. Conf. Semantic Comput., 2009. P. 654-657.

5. Doddavula S.K. Implementation of a Secure Genome Sequence Search Platform on Public Cloud / S.K. Doddavula, V. Saxena // Third IEEE Int. Conf. Cloud Computing Technol. and Sci., 2011. P. 205-212.

6. Chen J. Research about Spam Page Identification Based on Cloud Computing in Search Service / J. Chen, Y. Xu, Y. Li // 4th IEEE Int. Conf. Intelligent Human-Machine Systems and Cybernetics, 2012. P. 77-80.

7. Новиков И. Облачные вычисления: на пороге перемен / И. Новиков. URL: http://www.pcmag.ru/solutions/sub_detail.php?ID=44441& SUB_PAGE=1 (дата обращения 17.04.2017).

8. O'Brien N. S. Exploiting Cloud Computing for Algorithm Development / N. S. O'Brien, S. J. Johnston, E. E. Hart, et al. // IEEE Int. Conf. Cyber-Enabled Distributed Comput. and Knowledge Discovery, 2011. P. 336-342.

9. Khazaei H. Modelling of Cloud Computing Centers Using M/G/m Queues / H. Khazaei, J. Misic, V. B. Misic // Proc. 2011 31st Int. Conf. Distributed Comput. Workshops. P. 87-92.

10. Calheiros R. N. Virtual Machine Provisioning Based on Analytical Performance and QoS in Cloud Computing Environments / R. N. Calheiros, R. Ranjan, R. Buyya // Proc. Int. Conf. Parallel Proc. (ICPP), Sept 2011. P. 295-304.

11. CRN ИТ-Бизнес. Десять лучших гиперконвергентных решений 2016 года. URL: https://www.crn.ru/news/detail.php?ID=112462 (дата обращения 16.04.2017).

12. ChannelForIT. Гиперконвергентные системы: что нужно знать. URL: http://channel4it.com/publications/Giperkonvergentnye-sistemy-chto-nuzhno-znat –2140.html (дата обращения 16.04.2017).

13. https://www.hpe.com (дата обращения 15.04.2017).

14. Гиперконвергентные системы. URL: https://habrahabr.ru (дата обращения 15.04.2017).

Advantage of Hyperconvergent Systems over Cloud Technologies

Noskova A. I., Tokranova M. V.
Emperor Alexander I Petersburg State Transport University
St. Petersburg, Russia
magistrpgups@rambler.ru

Abstract. **The article is devoted to the relevance of cloud computing and hyperconvergent systems, that is caused by the popularity of their use by large and small scale companies. Most enterprises transfer their services and applications to "clouds", first of all, because of lower prices on buying it's own IT infrastructure. However, cloud computing is not an ideal solution in full measure. Such shortcomings as strict dependence on suppliers, the storage of confidential information on others resources, the inability to fully control the security of data, forces us to look for other more reliable options. Converged and hyperconvergent systems are an alternative to renting "clouds" from outside companies. Due to their help, it became possible to deploy private "clouds", which disposal is entirely in the hands of the enterprise.**

Keywords: **Hyperconvergent systems, cloud computing, IaaS, PaaS, SaaS.**

References

1. https://en.wikipedia.org/wiki (accessed: 15.04.2017).

2. Amrhein D., Quint S. Cloud Computing for the Enterprise: Part 1: Capturing the Cloud. Available at: http://www.ibm.com/developerworks/websphere/techjournal/0904_amrhein/0904_amrhein.html (accessed: 16.04.2017).

3. Orlando D. Models of Cloud Computing Services: Infrastructure as a Service. Available at: http://www.ibm.com/developerworks/ru/library/cloudservices1iaas (accessed: 16.04.2017).

4. Sheu P. C.-Y., Wang S., Wang Q., Hao K., Paul R. Semantic Computing, Cloud Computing, and Semantic Search Engine. *IEEE Int. Conf. Semantic Comput.*, 2009, pp. 654-657.

5. Doddavula S. K., Saxena V. Implementation of a Secure Genome Sequence Search Platform on Public Cloud. *Third IEEE Int. Conf. Cloud Comput. Technol. and Sci.*, 2011, pp. 205-212.

6. Chen J., Xu Y., Li Y. Research about Spam Page Identification Based on Cloud Computing in Search Service. *4th IEEE Int. Conf. Intelligent Human-Machine Systems and Cybernetics*, 2012, pp. 77-80.

7. Novikov I. Cloud Computing: on the Verge of Change. Available at: http://www.pcmag.ru/solutions/sub_detail.php?ID=44441& SUB_PAGE=1 (accessed: 17.04.2017).

8. O'Brien N. S., Johnston S. J., Hart E. E., Djidjeli K., Cox S. J. Exploiting Cloud Computing for Algorithm Development. *IEEE Int. Conf. Cyber-Enabled Distributed Comput. and Knowledge Discovery*, 2011, pp. 336-342.

9. Khazaei H., Misic J., Misic V. B. Modelling of Cloud Computing Centers Using M/G/m Queues, *Proc. 2011 31st Int. Conf. Distributed Comput. Workshops*, pp. 87-92.

10. Calheiros R. N., Ranjan R., Buyya R. Virtual Machine Provisioning Based on Analytical Performance and QoS in Cloud Computing Environments, *Proc. Int. Conf. Parallel Proc. (ICPP)*, Sept 2011, pp. 295-304.

11. CRN IT Business, Top Ten Hyperconvergent Soltions 2016. Available at: https://www.crn.ru/news/detail.php?ID=112462 (accessed: 16.04.2017).

12. ChannelForIT, Hyperconvergent Systems: what You Need to Know. Available at: http://channel4it.com/publications/Giperkonvergentnye-sistemy-chto-nuzhno-znat –2140.html (accessed: 16.04.2017).

13. https://www.hpe.com (accessed: 15.04.2017).

14. Hyperconvergent systems. Available at: https://habrahabr.ru (accessed: 15.04.2017).

Имитационное моделирование в AnyLogic многоканальных немарковских систем массового обслуживания с «разогревом», «охлаждением» и распределениями фазового типа

Максимов Е. В.
Петербургский государственный университет путей сообщения Императора Александра I
Санкт-Петербург, Россия
maksimov.eugene69@gmail.com

Аннотация. **Рассматривается имитационное моделирование в AnyLogic многоканальных немарковских систем массового обслуживания (СМО) с «разогревом», «охлаждением» и распределениями фазового типа. При реализации модели используется распределение Эрланга второго порядка. Указаны основные расчетные соотношения для определения параметров этого распределения. Обсуждаются возможные варианты интерпретации понятий «разогрев» и «охлаждение» применительно в информационно-вычислительным системам. Приводится схема модели немарковской системы массового обслуживания с «разогревом», «охлаждением» и распределениями Эрланга 2-го порядка в среде AnyLogic. Приведены результаты расчета основных вероятностно-временных характеристик модели СМО (плотности и функции распределения времени ожидания заявки в очереди и времени пребывания в системе), обсуждаются возможности применения результатов.**

Ключевые слова**: имитационное моделирование, AnyLogic, системы массового обслуживания, «разогрев», «охлаждение», вероятностно-временные характеристики, распределения фазового типа, распределение Эрланга.**

Введение

В ряде систем массового обслуживания (СМО), особенно при относительно малой загрузке, целесообразно вводить порог включения, когда обслуживание начинается при скоплении в системе некоторого количества заявок и заканчивается при полном освобождении системы. Такой режим увеличивает как период непрерывной занятости, так и время, в течение которого обслуживание не ведется. Это позволяет на довольно длительные периоды переводить автоматическую аппаратуру в облегченный (дежурный) режим в целях экономии ресурса и электроэнергии. В системах с участием человека появляется возможность полностью выключать значительную часть техники и переводить оператора на решение других задач.

Очевидно, что обслуживание первой заявки в этих условиях сопряжено с выполнением некоторых дополнительных операций («разогрев» системы) и в среднем будет продолжаться дольше, чем обслуживание прочих заявок. СМО с «разогревом» рассматриваются в работах [1–6].

Возможен и другой случай, когда после полного освобождения системы требуются мероприятия, связанные с восстановлением работоспособности, проведением технического обслуживания, перерывами в работе и т. д. В этом случае уместно говорить, что СМО переходит в режим «охлаждения». Начало обслуживания вновь прибывшей заявки не начнется, пока не завершатся все операции «охлаждения». В отличие от «разогрева», процесс «охлаждения» системы не зависит от прибытия первой заявки периода занятости. Если система успеет «охладиться» до прихода заявки, обслуживание начнется без дополнительных задержек. Исследованию систем с охлаждением посвящены работы [7, 8].

В статье [9] рассматриваются системы с «разогревом», с «охлаждением», также предложена диаграмма переходов между состояниями модели многоканальной системы массового обслуживания типа $M / E_2 / E_2 / M / n$ – с «разогревом», с «охлаждением» и распределением Эрланга 2-го порядка.

Вопросы прикладного применения моделей систем массового обслуживания для прогнозного оценивания оперативности функционирования облачных систем, систем распределенной обработки данных рассматриваются в [6, 10–13]. В частности, в [6, 13] рассматриваются вопросы оценивания оперативности распределенной обработки данных с учетом затрат на обеспечение информационной безопасности на основе использования «разогрева».

Далее представлено моделирование узла дата-центра с несколькими одинаковыми серверами, поддерживающими возможность «разогрева» и «охлаждения», также в среде AnyLogic разработана имитационная модель.

Моделирование многопроцессорного сервера с «разогревом» и «охлаждением»

В центре обработки данных имеется машинный зал, в котором расположено серверное оборудование. В качестве примера исследуемого узла центра обработки данных рассмотрим несколько одинаковых серверов (рис. 1).

Конечный пользователь (клиент) отправляет запросы на сервер посредством сети Интернет. Сервер, получив заявки, подготавливает оборудование, происходит «разогрев» системы для дальнейшей обработки. Заявки, заставшие вычислительные ресурсы занятыми, встают в очередь и ожидают. По окончании обслуживания запросов, если в систему не поступило новых запросов, система переходит в режим «охлаждения».

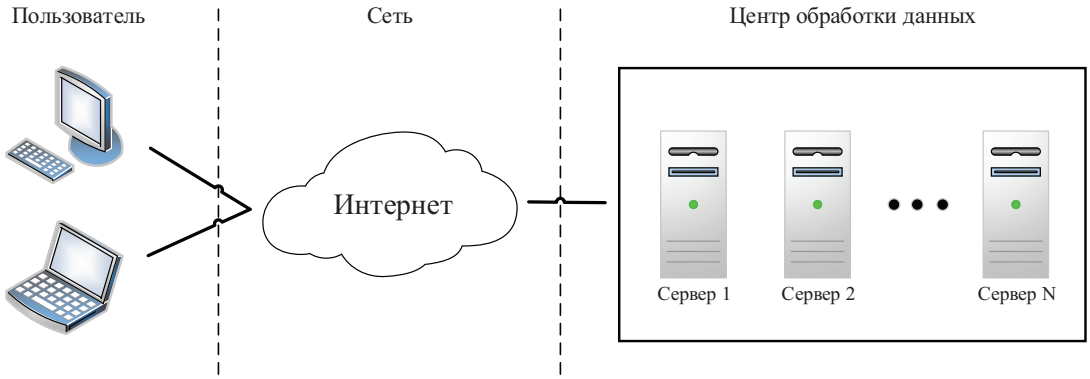


Рис. 1. Схема узлов центра обработки данных

В качестве «разогрева» системы будем рассматривать процесс подготовки необходимых данных для обработки поступающих запросов, которые помещаются в оперативную память. «Охлаждение» системы будем рассматривать как процесс освобождения занятой оперативной памяти.

Методы построения имитационных моделей систематически изложены в работе Ю. И. Рыжикова [14]. В качестве оценки оперативности функционирования рассмотренного узла дата-центра будет применен метод имитационного моделирования в среде AnyLogic. Технология работы в указанной среде подробно изложена в [15].

Для изучения сервера с описанным «разогревом/охлаждением» полезно ввести усовершенствованную запись A/B/C/D/n, которая по сравнению с оригинальной записью Кендалла содержит дополнительные C и D, обозначающие распределение времени «разогрева» и «охлаждения», соответственно.

Диаграмма процесса обработки запросов

На рис. 2 изображена основная диаграмма процесса обработки запроса системой массового обслуживания с «разогревом» и «охлаждением».

Последовательность блоков, которая начинается с source, задает основной поток запросов на серверы в дата-центре. Последовательность блоков, которая начинается с sourceWarmUp, отвечает за «разогрев» системы. Последовательность блоков, которая начинается с sourceCooling, начинает процесс «охлаждения» системы.

Распределения фазового типа

Д. Р. Кокс показал, что произвольное распределение длительности некоторой случайной величины можно представить смесью экспоненциальных фаз или распределением фазового типа (гиперэкспоненциальным, Эрланга или Кокса) [16]. Достоинства такого представления – удобство сведения случайного процесса к Марковскому и легкость составления и решения системы уравнений, описывающей поведение соответствующей модели. Такой подход получил широкое применение при исследовании немарковских многоканальных систем массового обслуживания, см. например [17]. Параметры аппроксимирующего распределения могут быть вещественными или комплексно-сопряженными, при этом вероятности состояний исследуемой системы являются вещественными.

Схема двухэтапного неоднородного распределения Эрланга приведена на рис. 3. Оно представляет собой смесь двух экспоненциальных фаз с интенсивностями λ_1, λ_2.

Чтобы найти параметры двухэтапного неоднородного распределения Эрланга, нужно потребовать равенства первых двух начальных моментов распределений аппроксимирующего и исходного распределения. При этом уравнение имеет вид

$$\begin{cases} \dfrac{1}{\lambda_1}+\dfrac{1}{\lambda_2}=f_1, \\ \dfrac{1}{\lambda_1^2}+\dfrac{1}{\lambda_1\lambda_2}+\dfrac{1}{\lambda_2^2}=f_2. \end{cases} \quad (1)$$

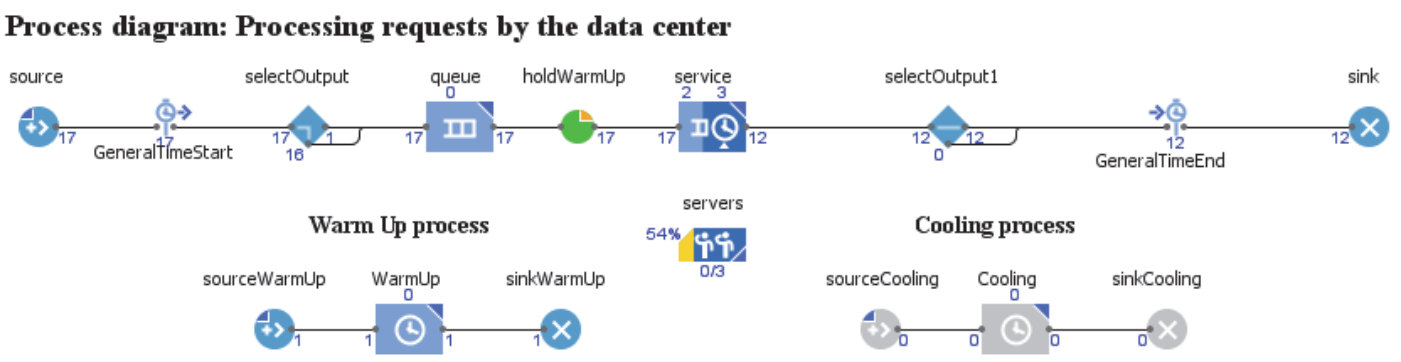


Рис. 2. Диаграмма процесса обработки заявки многоканальной СМО с «разогревом/охлаждением»

Рис. 3. Схема неоднородного распределения Эрланга

Из (1) следует:

$$\lambda_{1,2} = \frac{f_1 \pm \sqrt{4f_2 - 3f_1^2}}{2(f_1^2 - f_2)}. \quad (2)$$

Из (2) следует, что параметры являются вещественными при аппроксимации исходной плотности с коэффициентом вариации

$$\frac{1}{\sqrt{2}} \le \eta < 1. \quad (3)$$

При использовании аппроксимации в диапазоне

$$0 \le \eta < \frac{1}{\sqrt{2}} \quad (4)$$

целесообразно использовать комплексно-сопряженные параметры:

$$\lambda_1 = \alpha + j\beta;$$

$$\lambda_2 = \alpha - j\beta.$$

Из (2) получается:

$$\alpha = \frac{f_1}{2(f_1^2 - f_2)};$$

$$\beta = \frac{\sqrt{3f_1^2 - 4f_2}}{2(f_1^2 - f_2)}.$$

В качестве времени на «разогрев» и «охлаждение» системы используется распределение фазного типа, а именно распределение Эрланга 2-го порядка.

Практические результаты

Построенная модель имитирует работу одного узла датацентра, в состав которого входят три одинаковых по техническим характеристикам сервера. Эти сервера выступают как система с возможностью «разогрева» и «охлаждения».

Разработанная имитационная модель позволяет определить:

- среднее число заявок в системе;
- среднее число каналов, занятых обслуживанием;
- среднюю длину очереди;
- среднее время нахождения заявки в очереди;
- среднее время нахождения заявки в системе;
- коэффициент загрузки.

Было проведено несколько экспериментов. Различия экспериментов заключаются в количестве заявок. В качестве исходных данных приняты значения из статьи [3]. Поскольку в [3] время, необходимое для «охлаждения», изменяется от 0,5 до 3,5 с, решено использовать среднее значение.

Исходные данные:

- интенсивность входного потока – 4;
- интенсивность обслуживания – 1,8 с;
- время «разогрева» и «охлаждения» – 2 с;
- число каналов – 3.

В таблице 1 приведены полученные результаты.

Таблица 1

Результаты имитационного моделирования

Параметр	Число заявок		
	100	1000	10 000
Среднее число каналов, занятых обслуживанием	1,94	2,131	2,192
Коэффициент загрузки	0,628	0,711	0,744
Среднее число заявок в очереди (длина очереди)	3,085	1,662	1,641
Среднее число заявок в системе	4,86	3,544	3,606
Среднее время ожидания заявки в очереди	0,458	0,216	0,214
Среднее время пребывания заявки в системе	1,273	0,797	0,772

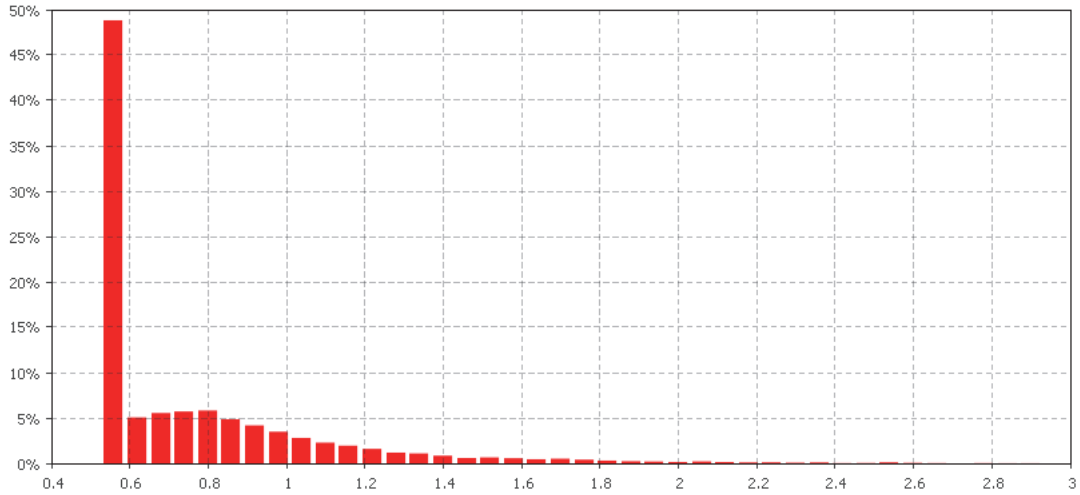


Рис. 4. Плотность распределения времени пребывания заявки в системе

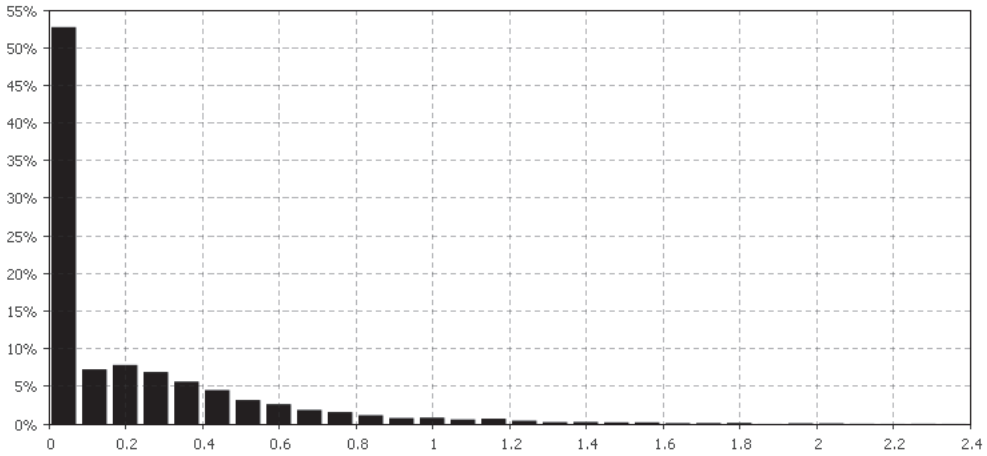


Рис. 5. Плотность распределения времени ожидания в очереди

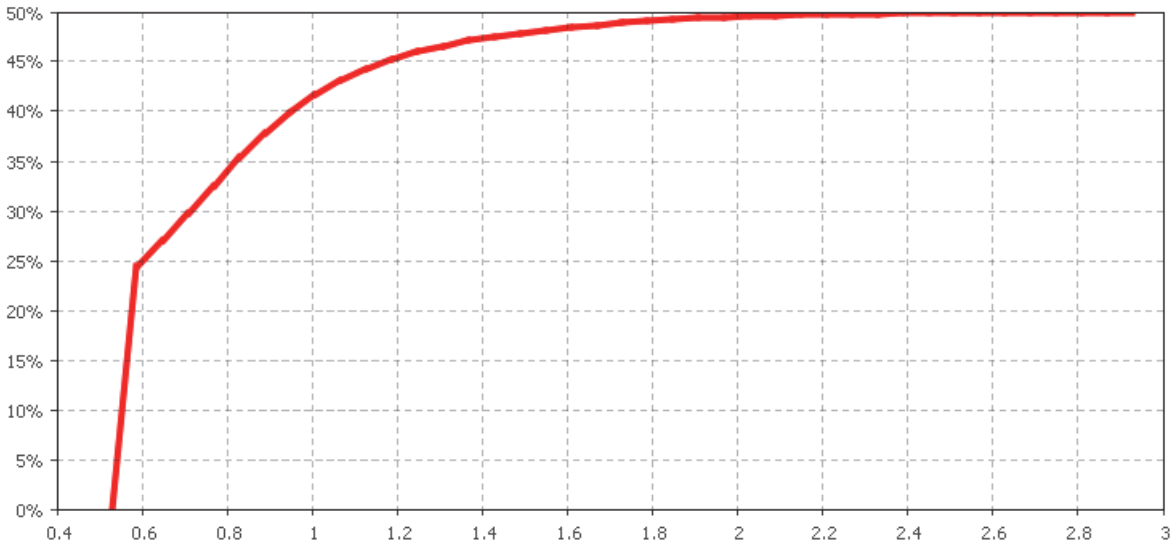


Рис. 6. Функция распределения времени пребывания заявки в системе

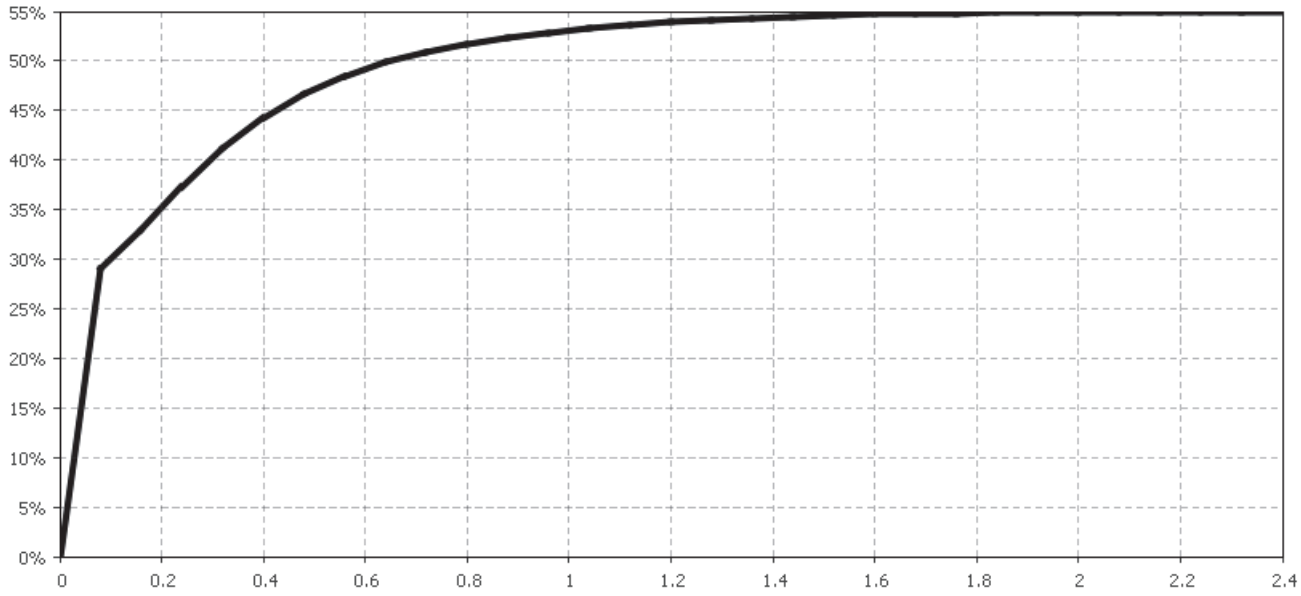


Рис. 7. Функция распределения времени ожидания в очереди

Как видно из таблицы, при малом количестве заявок сложно оценить работу системы, поскольку значения получаются больше, чем при другом количестве заявок. При увеличении числа заявок можно более точно оценить работу системы.

На рис. 4–7 представлены графики функции распределения и плотности распределения для временных параметров, таких как время пребывания заявки в системе и время ожидания.

Из рис. 4 видно, что заявки пребывают в системе в основном столько времени, сколько необходимо на их обслуживание. Это обусловлено невысоким значением удельной загрузки системы массового обслуживания.

Из рис. 5 видно, что большинство заявок поступают на обслуживание без дополнительного времени. Это также обусловлено невысоким значением удельной загрузки моделируемой системы массового обслуживания.

Приведенные графики позволяют оценить оперативность процессов обслуживания заявок в узлах информационно-вычислительных систем и сетей и на этой базе обосновать характеристики их производительности.

Выводы

Реализованная в среде AnyLogic модель многоканальной немарковской систем обслуживания «разогревом» и «охлаждением» и распределениями фазового типа может использоваться, прежде всего, в качестве средства обоснования достоверности вновь разрабатываемых численных моделей аналогичных классов СМО. Кроме того, модель может найти применение при оценивании и обосновании производительности узлов центров обработки данных, облачных систем и других, в которых требуется учитывать затраты на проведение подготовительных («разогрева») и завершающих («охлаждения») работ.

Литература

1. Kreinin Ya. Single-channel Queuing System with Warm up / Ya. Kreinin // Automation and Remote Control, 1980 41. 6. P. 771-776.

2. Grassmann W. K. Warm-up Periods in Simulation Can Be Detrimental / W. K. Grassmann // Probab. Engrg. Inform. Sci., 2008, № 22 (3). P. 415-429.

3. Kolahi S. S. Simulation Model, Warm-up Period, and Simulation Length of Cellular Systems / S. S. Kolahi // Second Int. Conf. Intelligent Systems, Modelling and Simulation (ISMS), 2011. P. 375-379.

4. Гиндин С. И. Численный расчет многоканальной системы массового обслуживания с рекуррентным входящим потоком и «разогревом» / С. И. Гиндин, А. Д. Хомоненко, С. Е. Ададуров // Изв. ПГУПС, 2013, № 4 (37). С. 92-101.

5. Eremin A. S. A Queuing System with Determined Delay in Starting the Service / A. S. Eremin // Интеллектуальные технологии на транспорте, 2015, № 4. С. 23-26.

6. Khomonenko A. Performance Evaluation of Cloud Computing Accounting for Expenses on Information Security / A. Khomonenko, S. Gindin // 18th Conf. Open Innovations Association and Seminar on Information Security and Protection of Information Technology (FRUCT-ISPIT), 18-22 Apr. 2016. P. 100-105.

7. Лохвитский В. А. Численный анализ системы массового обслуживания с гиперэкспоненциальным «охлаждением» / В. А. Лохвитский, А. В. Уланов // Вестн. Томского гос. ун-та. Управление, вычислительная техника и информатика, 2016, № 4 (37). С. 36-43.

8. Khalil M. M. Testing of Software for Calculating a Multichannel Queuing System with “Cooling” and E2-approximation / M. M. Khalil, A. A. Andruk // Интеллектуальные технологии на транспорте, 2016, № 4 (8). С. 22-28.

9. Khomonenko A. D. A Cloud Computing Model Using Multi-channel Queuing System with Cooling / A. D. Khomonenko, S. I. Gindin, M. M. Khalil // XIX IEEE Int. Conf. Soft Comput. and Measurements (SCM), 2016. P. 103-106. DOI: 10.1109/SCM.2016.7519697.

10. Mao M. A Performance Study on the VM Startup Time in the Cloud / M. Mao, M. Humphrey // IEEE 5th Int. Conf. Cloud Computing (CLOUD). IEEE Press, 2012. P. 423-430.

11. Bruneo D. A Stochastic Model to Investigate Data Center Performance and QoS in IaaS Cloud Computing Systems / D. Bruneo // IEEE Transactions on Parallel and Distributed Systems, 2014. P. 560-569.

12. Gong C. The characteristics of cloud computing / C. Gong et al. // 39th Int. Conf. Parallel Processing Workshops (ICPPW). IEEE Press, 2010. P. 275-279.

13. Гиндин С. И. Модель оценивания оперативности распределенной обработки данных с учетом затрат на обеспечение информационной безопасности / С. И. Гиндин, А. Д. Хомоненко, В. В. Яковлев, С. В. Матвеев // Проблемы информационной безопасности. Компьютерные системы, 2013, № 4. С. 59-67.

14. Рыжиков Ю. И. Имитационное моделирование. Теория и технологии / Ю. И. Рыжиков. СПб.: КОРОНА принт; М.: Альтекс-А, 2010. 384 с.

15. Карпов Ю. Г. Имитационное моделирование систем. Введение в моделирование с AnyLogic 5 / Ю. Г. Карпов. СПб.: БХВ-Петербург, 2006. 400 с.

16. Cox D. R. A Use of Complex Probabilities in the Theory of Stochastic Processes / D. R. Cox // Proc. Cambr. Phil. Soc., 1955, vol. 51, № 2. P. 313-319.

17. Bubnov V. P. Software Reliability Model with Coxian Distribution of Length of Intervals Between Errors Detection and Fixing Moments / V. P. Bubnov, A. D. Khomonenko, A. V. Tyrva // Proceedings – 35th Annual IEEE Int. Computer Software and Appl. Conf. Workshops, COMPSACW 2011. 2011. P. 310-314.

Simulation Modeling in AnyLogic of Multi-Channel non-Markov Queuing Systems with «Heat-up», «Cooling» and Distributions of Phase Type

Maksimov E. V.
Emperor Alexander I Petersburg State Transport University
St. Petersburg, Russia
maksimov.eugene69@gmail.com

Abstract. **Simulation modeling in AnyLogic of multi-channel non-Markov queuing systems with "heat-up", "cooling" and distributions of phase type is considered. In case of implementation of model distribution of the Erlang 2 orders is used. The main estimated ratios for determination of parameters of this distribution are specified. Possible options of interpretation of concepts "heat-up" and "cooling" applicable in information systems are discussed. The diagram of model of non-Markov queuing system with "heat-up", "cooling" and distributions of the Erlang of the 2nd order in the environment of AnyLogic is provided. Results of calculation of the main probable time response characteristics of the SMO model are given (density and distribution functions of wait time of the request in queue and time of stay in system), possibilities of use of results are discussed.**

Keywords**: simulation modeling, AnyLogic, queuing systems, "heat-up", "cooling", probable time response characteristics, distributions of phase type, distribution of the Erlang.**

References

1. Kreinin Ya. Single-channel Queuing System with Warm up. *Automation and Remote Control*, 1980, no. 41, 6, pp. 771-776.

2. Grassmann W. K. Warm-up Periods in Simulation Can Be Detrimental. *Probab. Engrg. Inform. Sci.*, 2008, no. 22 (3), pp. 415-429.

3. Kolahi S. S. Simulation Model, Warm-up Period, and Simulation Length of Cellular Systems. *Second Int. Conf. Intelligent Systems*, *Modelling and Simulation (ISMS)*, 2011, pp. 375-379.

4. Gindin S. I., Khomonenko A. D., Adadurov S. E. Numerical Calculation of Multi-channel Queuing System with the Recurrent Entering Flow and «Heat-up» [Chislennyy raschet mnogokanal'noy sistemy massovogo obsluzhivaniya s rekurrentnym vkhodyashchim potokom i „razogrevom"], *Proc. of Petersburg Transport University [Izvestiya Peterburgskogo universiteta putey soobshcheniya]*, 2013, no. 4 (37), pp. 92-101.

5. Eremin A. S. A Queuing System with Determined Delay in Starting the Service. *Intellectual Technologies on Transport*, 2015, no. 4, pp. 23-26.

6. Khomonenko A., Gindin S. Performance Evaluation of Cloud Computing Accounting for Expenses on Information Security. *18th Conf. Open Innovations Association and Seminar on Information Security and Protection of Information Technology (FRUCT-ISPIT)*, 18-22 Apr. 2016, pp. 100-105.

7. Lokhvitsky V.A., Ulanov A. V. The Numerical Analyses of Queuing System with Hyperexponential Distribution of Cooling Time [Chislennyy analiz sistemy massovogo obsluzhivaniya s gipereksponentsial'nym „okhlazhdeniem"], *Tomsk State Univ. J. of Control and Computer Sci. [Vestnik Tomskogo gosudarstvennogo universiteta. Upravlenie*, *vychislitel'naya tekhnika i informatika]*, 2016, no. 4 (37), pp. 36-43.

8. Khalil M. M., Andruk A. A. Testing of Software for Calculating a Multichannel Queuing System with "Cooling" and E2-approximation. *Intellectual Technologies on Transport*, 2016, № 4 (8), pp. 22-28.

9. Khomonenko A. D., Gindin S. I., Khalil M. M. A Cloud Computing Model Using Multi-channel Queuing System with Cooling. *XIX IEEE Int. Conf. Soft Computing and Measurements (SCM)*, 2016, pp. 103-106. DOI: 10.1109/SCM.2016.7519697.

10. Mao M., Humphrey M. A Performance Study on the VM Startup Time in the Cloud. *IEEE 5th Int. Conf. Cloud Computing (CLOUD)*, IEEE Press, 2012, pp. 423-430.

11. Bruneo D. A Stochastic Model to Investigate Data Center Performance and QoS in IaaS Cloud Computing Systems. *IEEE Transactions on Parallel and Distributed Systems*, 2014, pp. 560-569.

12. Gong C. et al. The Characteristics of Cloud Computing. *39th Int. Conf. Parallel Processing Workshops (ICPPW)*, IEEE Press. 2010, pp. 275-279.

13. Gindin S. I., Khomonenko A. D., Jakovlev V. V., Matveev S. V. Model Evaluation of Efficiency Distributed Data Processing Including the Spending of Ensuring the Information Security [Model' otsenivaniya operativnosti raspredelennoy obrabotki dannykh s uchetom zatrat na obespechenie informatsionnoy bezopasnosti], *Information Security Problems. Comput. Systems [Problemy informatsionnoy bezopasnosti. Komp'yuternye sistemy]*, 2013, no. 4, pp. 59-67.

14. Ryzhikov Y. I. Simulation Modeling. Theory and Technologies [Imitatsionnoe modelirovanie. Teoriya i tekhnologii]. St. Petersburg, KORONA print; Moscow, Alteks-A, 2010, 384 p.

15. Karpov Y. G. Simulation Modeling of Systems. Introduction to Simulation with AnyLogic 5 [Imitatsionnoe modelirovanie sistem. Vvedenie v modelirovanie s AnyLogic 5]. St. Petersburg, BHV-Petersburg, 2006, 400 p.

16. Cox D. R. A Use of Complex Probabilities in the Theory of Stochastic Processes. *Proc. Cambr. Phil. Soc*., 1955, vol. 51, no. 2, pp. 313-319.

17. Bubnov V. P., Khomonenko A. D., Tyrva A. V. Software Reliability Model with Coxian Distribution of Length of Intervals Between Errors Detection and Fixing Moments. *Proc. – 35th Annual IEEE Int. Computer Software and Applications Conf. Workshops*, *COMPSACW 2011*, 2011, pp. 310, 314.

Список авторов статей, опубликованных в № 2 журнала «Интеллектуальные технологии на транспорте» за 2017 год

Басыров Александр Геннадьевич
д.т.н., профессор
Должность: начальник кафедры информационно-вычислительных систем и сетей Военно-космической академии имени А. Ф. Можайского
Область научных интересов: параллельные вычислительные процессы, энергосберегающие технологии в вычислительной технике, высокопроизводительные вычислительные системы
e-mail: alexanderbas@mail.ru

Белов Виктор Петрович
к.т.н., доцент
Должность: доцент кафедры «Автоматизированные системы» Военно-космической академии имени А. Ф. Можайского
Область научных интересов: методы защиты от мощных электромагнитных излучений, безопасность систем
e-mail: arsenal_belov@mail.ru

Диасамидзе Светлана Владимировна
к.т.н.
Должность: доцент кафедры «Информатика и информационная безопасность» ФГБОУ ВО «Петербургский государственный университет путей сообщения Императора Александра I»
Область научных интересов: анализ и управление информационной безопасностью автоматизированных систем и информационных сетей, программного обеспечения средств железнодорожного транспорта. Разработка программных средств обеспечения информационной безопасности
e-mail: sv.diass99@yandex.ru

Ерин Алексей Андреевич
Магистрант кафедры «Информационные и вычислительные системы» ФГБОУ ВПО «Петербургский государственный университет путей сообщения Императора Александра I»
e-mail: alexey.erin94@gmail.com

Зубков Кирилл Николаевич
аспирант кафедры «Информатика и информационная безопасность» ФГБОУ ВО «Петербургский государственный университет путей сообщения Императора Александра I»
Область научных интересов: мобильные приложения, голосовые сетевые технологии, разработка и развитие методов анализа защищенности, аудит информационной безопасности
e-mail: kirillzubkoff@gmail.com

Корбаков Александр Игоревич
Магистрант кафедры «Информационные и вычислительные системы» ФГБОУ ВПО «Петербургский государственный университет путей сообщения Императора Александра I»
Область научных интересов: информационные системы и технологии на транспорте
e-mail: alexpvb111@yandex.ru

Красновидов Александр Владленович
к.т.н.
Должность: доцент кафедры «Информационные и вычислительные системы» ФГБОУ ВО «Петербургский государственный университет путей сообщения Императора Александра I»
Область научных интересов: моделирование систем, теория языков программирования
e-mail: alexkrasnovidow@mail.ru

Максимов Евгений Владимирович
Магистрант кафедры «Информационные и вычислительные системы» ФГБОУ ВПО «Петербургский государственный университет путей сообщения Императора Александра I»
e-mail: maksimov.eugene69@gmail.com

Носкова Александра Игоревна
Магистрант кафедры «Информационные и вычислительные системы» ФГБОУ ВПО «Петербургский государственный университет путей сообщения Императора Александра I»
Область научных интересов: информационные системы, базы данных
e-mail: alexandranskv@mail.ru

Токранова Мария Вадимовна
Магистрант кафедры «Информационные и вычислительные системы» ФГБОУ ВПО «Петербургский государственный университет путей сообщения Императора Александра I»
Область научных интересов: информационные системы, базы данных
e-mail: mari_tn@mail.ru

Шардаков Кирилл Сергеевич
Магистрант кафедры «Информационные и вычислительные системы» ФГБОУ ВПО «Петербургский государственный университет путей сообщения Императора Александра I»
Область научных интересов: информационные системы и технологии на транспорте, сети передачи данных
e-mail: k.shardakov@gmail.com

Шмелев Валентин Валерьевич
к.т.н.
Должность: докторант Военно-космической академии имени А. Ф. Можайского
Область научных интересов: автоматизированные системы управления в ракетно-космической отрасли, обработка и анализ телеметрической информации
e-mail: valja1978@yandex.ru

Штагер Евгений Анатольевич
д.ф.-м.н.
Должность: главный специалист Крыловского государственного научного центра
Область научных интересов: методы защиты от мощного электромагнитного излучения
e-mail: shtager.e@mail.ru

Шульгин Альберт Николаевич
к.т.н.
Должность: преподаватель кафедры информационно-вычислительных систем и сетей Военно-космической академии имени А. Ф. Можайского
Область научных интересов: параллельные вычисления, энергосберегающие вычислительные процессы, высокопроизводительные вычислительные системы
e-mail: shulgin_albert@mail.ru

The list of authors of articles published in the journal number 2 „Intellectual Technologies on Transport“ for 2017

Basyrov Aleksandr Gennadevich
Doct. Eng., professor
Appointment: the head of the Department of information computing systems and networks Military Space Academy name A. F. Mozhaisky
Academic interests: parallel computing processes, energy-saving technologies in computing, high-performance computing systems
e-mail: alexanderbas@mail.ru

Belov Viktor Petrovich
Cand. Eng., assist. professor
Appointment: assist. professor of the Department “Avtomatic sistem” Military Space Academy named after A. F. Mozhaysky
Academic interests: methods protection against high-power microwaves, security of sistem
e-mail: arsenal_belov@mail.ru

Diasamidze Svetlana Vladimirovna
Cand. Eng.
Appointment: Associate Professor of Informatics and Information Technology Department
Security » of the Emperor Alexander I St. Petersburg State Transport University
Academic interests: analysis and management of information security for automated systems and information networks, development software of railway transport tools. Development of software tools to ensure information security.
e-mail: sv.diass99@yandex.ru

Erin Alexey Andreevich
Master’s Degree of Department Information and Computing Systems of Emperor Alexander I Petersburg State Transport University
e-mail: alexey.erin94@gmail.com

Korbakov Aleksandr Igorevich
Master’s Degree of Department Information and Computing Systems of Emperor Alexander I Petersburg State Transport University
Academic interests: information systems and technologies on railway transport
e-mail: alexpvb111@yandex.ru

Krasnovidov Alexander Vladlenovich
Ph. D.
Appointment: Associate Professor, Information and Computing Systems Department, Emperor Alexander I Petersburg State Transport University
Academic interests: modeling of systems, theory of programming languages
e-mail: alexkrasnovidow@mail.ru

Maksimov Evgeniy Vladimirovich
Master’s Degree of Department Information and Computing Systems of Emperor Alexander I Petersburg State Transport University
e-mail: maksimov.eugene69@gmail.com

Noskova Aleksandra Igorevna
Master’s Degree of Department Information and Computing Systems of Emperor Alexander I Petersburg State Transport University
Academic interests: information systems, databases
e-mail: alexandranskv@mail.ru

Shardakov Kirill Setgeevich
Master’s Degree of Department Information and Computing Systems of Emperor Alexander I Petersburg State Transport University
Academic interests: information systems and technologies on railway transport, data transmission network
e-mail: shardakov@gmail.com

Shmelev Valentin Valerievich
Cand. Eng.
Appointment: doctoral student of the A. F. Mozhaisky Military Space Academy
Academic interests: Automated control systems in the rocket and space industry, processing and analysis of telemetric information
e-mail: valja1978@yandex.ru

Shtager Evgeniy Anatolievich
Doct. f.-m.sci.
Appointment: mains scientific recercher Krylov State scientific center Saint-Petersburg
Academic interests: methods of protection against high-power microwaves
e-mail: shtager.e@mail.ru

Shulgin Albert Nikolaevich
Cand. Eng.
Appointment: teacher of the Department of information computing systems and networks Military Space Academy named after A. F. Mozhaisky
Academic interests: parallel computing processes, energy-saving technologies in computing
e-mail: shulgin_albert@mail.ru

Tokranova Maria Vadimovna
Master's Degree of Department Information and Computing Systems of Emperor Alexander I Petersburg State Transport University
Academic interests: information systems, databases
e-mail: mari_tn@mail.ru

Zubkov Kirill Nikolayevich
Post-graduate student of the department «Informatics and Information Security»,Emperor Alexander I Petersburg State Transport University
Academic interests: mobile applications, voice network technologies, development and development of security analysis methods, information security audit
e-mail: kirillzubkoff@gmail.com

К 50-летию Санкт-Петербургского ИВЦ

В Санкт-Петербургском ИВЦ
Увлеченный коллектив.
Им выбран правильный мотив –
Здесь каждый трудится, как бог,
На благо всей сети дорог.

Глубокоуважаемый Андрей Николаевич!

Поздравляем коллектив Санкт-Петербургского информационно-вычислительного центра с замечательным юбилеем – 50-летием со дня основания.

Ваш центр является примером удачного сочетания оснащенности высокопроизводительной вычислительной техникой, применения современных информационных технологий, с работой высококвалифицированного коллектива специалистов, преданных своему делу.

Вам, безусловно, есть чем гордиться: Вы добились весомых результатов в обеспечении эффективной и оперативной обработки информации в интересах качественного функционирования сети железных дорог нашей страны.

Надеемся, что и в дальнейшем наше взаимодействие будет продуктивным и взаимно полезным. Верим в перспективу развития и процветания Вашего центра.

Желаем всему коллективу ИВЦ доброго здоровья, дальнейших весомых творческих успехов, семейного благополучия и всего наилучшего.

Редакция журнала «Интеллектуальные технологии на транспорте»

For the 50th Anniversary of St. Petersburg Computer Center

In St. Petersburg computer center
An enthusiastic collective.
They chose the right motive –
Here every one works, as God,
For good of the road network.

Dear Andrey Nickolaevich!

Congratulations to the team of Saint-Petersburg information and computing center with a remarkable jubilee – the 50th anniversary of the founding of.

Your center is an example of a successful combination of equipment, high-performance computing technology, application of modern information technologies work with highly qualified collective of specialists dedicated to their work.

You certainly have something to be proud of: You have achieved significant results in ensuring efficient and operative processing of information in the interests of the good functioning of the railway network in our country.

We hope that in the future our cooperation will be productive and mutually beneficial. We believe in the future development and prosperity of Your center.

We wish all the staff of center good health, the continued significant creative success, family wellbeing and all the best.

Editorial Board of Journal "Intellectual technologies on transport"