ISSN 2712-8687

ПРОБЛЕМЫ УПРАВЛЕНИЯ

3/2022

CONTROL SCIENCES

CONTROL SCIENCES
Научно-технический журнал

6 номеров в год

ISSN 1819-3161 (Print)

ISSN 2712-8687 (Online)

Издается с 2003 года

УЧРЕДИТЕЛЬ и ИЗДАТЕЛЬ

Федеральное государственное бюджетное учреждение науки Институт проблем управления им. В.А. Трапезникова РАН

Адрес редакции
117997, ГСП-7, Москва,
ул. Профсоюзная, д. 65, к. 410

Тел./факс (495) 198-17-20, доб. 1410

E-mail: pu@ipu.ru

Интернет: http://pu.mtas.ru
http://controlsciences.org

Опубликовано: 15 июля 2022 г.

Свидетельство о регистрации
ПИ № ФС 77-49203 от 30 марта 2012 г.
выдано Министерством Российской Федерации по делам печати, телерадиовещания и средств массовых коммуникаций

Свидетельство о регистрации
Эл № ФС 77-80482 от 17 февраля 2021 г.
выдано Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций

Журнал входит в RSCI на платформе Web of Science и Перечень рецензируемых научных изданий ВАК

Журнал включен в Российский индекс научного цитирования (РИНЦ).
На сайте Научной электронной библиотеки (www.elibrary.ru) доступны полные тексты статей.

ПРОБЛЕМЫ УПРАВЛЕНИЯ

3.2022

СОДЕРЖАНИЕ

Анализ и синтез систем управления

Антипов А.С., Краснов Д.В. Синтез системы слежения для однозвенного бездатчикового манипулятора при воздействии негладких возмущений 3

Управление в социально-экономических системах

Москвичев В.В., Постникова У.С., Тасейко О.В. Управление техногенной безопасностью на основе риск-ориентированного подхода 16

Угольницкий Г.А. Методика сравнительного анализа эффективности способов организации активных агентов и методов управления 29

Информационные технологии в управлении

Промыслов В.Г., Семенков К.В., Менгазетдинов Н.Э. Исследование методов аутентификации операторов в промышленных системах управления 40

Стецюра Г.Г. Способ ускорения децентрализованного управления одновременным запуском действий в распределенной группе автоматических устройств с включением ретранслятора 55

CONTROL SCIENCES
Scientific Technical Journal

6 issues per year
ISSN 1819-3161 (Print)
ISSN 2712-8687 (Online)
Published since 2003
FOUNDER and PUBLISHER
V.A. Trapeznikov
Institute of Control Sciences
of Russian Academy of Sciences

Editor-in-Chief
D.A. Novikov, RAS Academician

Deputy Editor-in-Chief
F.F. Pashchenko

Executive Editor-in-Chief
N.E. Maximova

Editor
L.V. Petrakova

Editorial address
65 Profsoyuznaya st., office 410,
Moscow 117997, Russia

☎/🖷 +7(495) 198-17-20, ext. 1410

✉ pu@ipu.ru

URL: http://pu.mtas.ru
http://controlsciences.org

Published: July 15, 2022

Registration certificate of
ПИ № ФС 77-49203 от 30 March 2012
issued by the Ministry of Press,
Broadcasting, and Mass Media
of the Russian Federation

Registration certificate of
Эл № ФС 77-80482 of 17 February 2021
issued by the Federal Service
for Supervision of Communications,
Information Technology, and Mass Media

The Journal is indexed in RSCI (Russian Science Citation Index) on the platform Web of Science and in the list of peer-reviewed scientific publications of HAC

On the website of the Scientific electronic library (www.elibrary.ru) full texts of articles are available

CONTROL SCIENCES

3.2022

CONTENTS

Analysis and Design of Control Systems

Antipov, A.S. and Krasnov, D.V. Tracking System Design for a Single-Link Sensorless Manipulator under Nonsmooth Disturbances 3

Control in Social and Economic Systems

Moskvichev, V.V., Postnikova, U.S., and Taseiko, O.V. Management of Technogenic Safety Based on a Risk–Oriented Approach 16

Ougolnitsky, G.A. An Approach to Compare Organization Modes of Active Agents and Control Methods 29

Information Technology in Control

Promyslov, V.G., Semenkov, K.V. Mengazetdinov, N.E. Assessment of Operator Authentication Methods in Industrial Control Systems 40

Stetsyura, G.G. The Simultaneous Start of Actions in a Distributed Group of Automatic Devices: A Decentralized Control Method with a Signal Repeater 55

УДК 62–503.54 DOI: http://doi.org/10.25728/pu.2022.3.1

СИНТЕЗ СИСТЕМЫ СЛЕЖЕНИЯ ДЛЯ ОДНОЗВЕННОГО БЕЗДАТЧИКОВОГО МАНИПУЛЯТОРА ПРИ ВОЗДЕЙСТВИИ НЕГЛАДКИХ ВОЗМУЩЕНИЙ[1]

А.С. Антипов, Д.В. Краснов

Аннотация. В качестве объекта управления выступает однозвенный манипулятор, эластично сочлененный с двигателем постоянного тока и функционирующий в условиях неопределенности и неполных измерений переменных состояния. Поставлена задача синтеза разрывного закона управления в форме обратной связи, обеспечивающего отслеживание заданного сигнала угловым положением манипулятора. Особенности объекта таковы: угловое положение и скорость манипулятора недоступны для измерений, датчики расположены только на приводе; параметрические и внешние возмущения, воздействующие на манипулятор, являются негладкими и не могут быть непосредственно подавлены с помощью управления, воздействующего на исполнительное устройство. Для решения поставленной задачи применяется блочный подход, в рамках которого разработана декомпозиционная процедура синтеза нелинейных локальных связей, обеспечивающих инвариантность регулируемой переменной по отношению к неопределенностям, не согласованным с управляющим воздействием. Для оценивания углового положения и скорости манипулятора, необходимых для синтеза обратной связи, разработан редуцированный наблюдатель состояния. Для оценивания значений переменных состояния в этом наблюдателе реализован принцип восстановления внешних возмущений по их воздействию на объект управления, не требующий построения динамической модели внешних воздействий. И в задаче управления, и в задаче наблюдения были использованы *S*-образные ограниченные непрерывные локальные связи – гладкие (сигмоидальные) и негладкие (кусочно-линейные) соответственно, которые подавляли ограниченные возмущения, действующие с ними по одному каналу. Разработанные алгоритмы не требуют идентификации в реальном времени параметрических и внешних возмущений, но обеспечивают стабилизацию ошибок наблюдения и слежения с некоторой точностью. Эффективность разработанной динамической обратной связи подтверждена результатами численного моделирования.

Ключевые слова: электромеханическая система, слежение, инвариантность, блочный подход, редуцированный наблюдатель состояния, *S*-образные функции.

ВВЕДЕНИЕ

Рассматривается простейшая электромеханическая система – однозвенный бездатчиковый манипулятор, эластично сочлененный с двигателем постоянного тока (ДПТ) и функционирующий в условиях параметрических и внешних возмущений. Базовая задача состоит в управлении угловым положением манипулятора – стабилизации его на заданном уровне или отслеживании допустимого задающего воздействия. Несмотря на кажущуюся простоту, рассматриваемый объект имеет все признаки сложной системы автоматического управления. А именно: описывается динамической моделью пятого порядка с нелинейностью и неопределенными параметрами, имеет неполный комплект датчиков, находится под воздействием внешних возмущений. В настоящее время в рамках различных подходов разработано множество эффективных алгоритмов управления механическими и электромеханическими системами [см., например, работы 1–5]. Однако, как правило, при решении таких задач учитывается конкретный тип неопределенностей (либо параметрические неопределенности, либо внешние возмущения определенного класса, либо неполные измерения), а не их ком-

[1] Работа выполнена при частичной поддержке РФФИ (проект 20-01-00363-А).

плекс. Во многих исследованиях математическая модель состоит только из механической системы (динамика исполнительных устройств не учитывается), при этом проблема подавления несогласованных возмущений, действующих по разным каналам с управлением, остается открытой [6].

В предыдущей работе авторов [7] однозвенный бездатчиковый манипулятор, эластично сочлененный с ДПТ, рассматривался с учетом указанного комплекса неопределенностей в предположении, что задающее воздействие, параметрические и внешние возмущения являются гладкими функциями времени. Это позволило представить модель объекта управления в каноническом виде «вход – выход» относительно смешанных переменных (линейных комбинаций от переменных состояния, внешних воздействий и их производных) и решить на ее основе и задачу наблюдения, и задачу слежения. Проблема оценивания значения неизмеряемой регулируемой переменной, необходимого для синтеза обратной связи в наблюдателе смешанных переменных, решалась путем использования дополнительного контура подсистемы наблюдения. Однако в процессе эксплуатации на механический объект часто воздействуют негладкие возмущения – ударные нагрузки, силы сухого трения [8]. Эти возмущения нельзя дифференцировать и они не могут быть непосредственно подавлены или скомпенсированы посредством управления, действующего на электропривод. В данной работе рассматривается именно этот случай негладких и несогласованных внешних и параметрических возмущений, а также случай кусочно-непрерывных задающих воздействий, что является препятствием для применения типовых методов управления, в частности метода линеаризации обратной связью [9, 10]. Описание модели объекта управления и постановка задачи приведены в § 1.

Для синтеза системы слежения в указанных условиях представляется целесообразным применение блочного подхода, в рамках которого переменные состояния используются как фиктивные управления в виде функций определенного класса, к которым предъявляется требование гладкости [11, 12]. При этом возмущения будут согласованы с фиктивными управлениями и могут быть подавлены с заданной точностью. Исходная система преобразуется к системе, записанной относительно ошибки слежения и невязок между реальными и сформированными фиктивными управлениями (инвариантными локальными связями), дифференцирование внешних сигналов не выполняется. Истинное разрывное управление, действующее на исполнительное устройство, обеспечивает последовательную сходимость невязок в заданные окрестности нуля и, как следствие, выполнение цели управления – стабилизации ошибки слежения. Стабилизирующие фиктивные управления предлагается сформировать в виде гладких и ограниченных сигма-функций, чтобы избежать в начале переходных процессов всплесков, характерных для систем с линейными обратными связями с большими коэффициентами [11, 13], которые традиционно используются для подавления внешних возмущений. В статье [12] была разработана процедура синтеза сигмоидальных локальных связей для нелинейного одноканального объекта в предположении, что функции от переменных состояния в правых частях дифференциальных уравнений, описывающих динамику системы, всюду ограничены. Научная новизна данного исследования состоит в разработке процедуры блочного синтеза и выбора параметров сигмоидальных фиктивных управлений для почти линейной системы пятого порядка в условиях действия негладких внешних возмущений (с производными, терпящими разрыв). Особенность объекта состоит в том, что с теоретической точки зрения в уравнениях системы линейные комбинации переменных состояния не являются ограниченными. Для достижения цели управления требуется обеспечить, чтобы значения внутренних переменных в процессе регулирования принадлежали конкретным диапазонам. Процедура синтеза базового закона управления с учетом указанных особенностей объекта управления приведена в § 2.

В § 3 представлено решение задачи наблюдения для случая, когда угловое положение и скорость манипулятора, требуемые для синтеза обратной связи, не могут быть измерены (например, из-за агрессивной среды, вибрации и т. п. [14]), и датчики установлены только на приводе. Построен редуцированный наблюдатель состояния, в котором для оценивания переменных состояния реализован принцип восстановления внешних возмущений по их воздействию на объект управления, не требующий использования динамической модели восстанавливаемых сигналов [15, 16]. Согласно этому принципу оцениваемая переменная трактуется как внешнее возмущение. При этом получение ее оценки осуществляется с помощью обратной связи в наблюдателе (корректирующего воздействия). Данный подход позволил построить робастный наблюдатель состояния без использования уравнений системы с неопределенными параметрами. Разработана декомпозиционная процедура синтеза кусочно-линейных обратных связей, обеспечивающих решение задачи наблюдения с

заданной точностью в условиях действия на механическую подсистему параметрических и внешних возмущений. Благодаря использованию *S*-образных инвариантных обратных связей (гладких – в задаче слежения, кусочно-гладких – в задаче наблюдения) в процессах наблюдения и управления не требуется дополнительно идентифицировать неопределенные параметры и внешние возмущения, достаточно знать диапазоны их изменения. Параметры регулятора не требуют перенастройки при произвольном изменении неопределенностей в допустимых интервалах. Этот вывод проиллюстрирован результатами численного моделирования, приведенными в § 4.

1. ОПИСАНИЕ ОБЪЕКТА УПРАВЛЕНИЯ. ПОСТАНОВКА ЗАДАЧИ

Математическая модель однозвенного жесткого манипулятора с поворотным шарниром, упруго соединенного с валом ДПТ, описывается дифференциальными уравнениями [7, 17]

$$\dot{x}_1 = x_2,\ \dot{x}_2 = -a_{21}x_1 - a_2\sin(x_1) + b_2x_3 + f(t), \quad (1)$$

$$\begin{gathered}\dot{x}_3 = x_4,\ \dot{x}_4 = -a_{41}x_1 - a_{43}x_3 - a_{44}x_4 + b_4x_5,\\ \dot{x}_5 = -a_{54}x_4 - a_{55}x_5 + b_5u.\end{gathered} \quad (2)$$

Уравнениями (1) описывается динамика манипулятора, уравнениями (2) – динамика ДПТ с постоянными магнитами [6], $a_{41} = -a_{43} < 0$, значения остальных конструктивных коэффициентов положительные:

$$b_2 = a_{21} = k_l / J_l,\ a_2 = \bar{m}\bar{g}h / J_l,\ a_{43} = k_l / J_m,$$
$$a_{44} = d / J_m,\ b_4 = k_m / J_m,$$
$$a_{54} = c / L,\ a_{55} = R / L,\ b_5 = 1 / L.$$

Описание переменных $x = (x_1, ..., x_5)^{\mathrm{T}}$ и параметров системы (1), (2) приведено в табл. 1.

В системе (1), (2) выходной регулируемой переменной является угловое положение звена манипулятора $x_1(t)$, напряжение питания якорной цепи ДПТ u рассматривается как разрывное управление. Ставится задача синтеза динамической обратной связи, обеспечивающей отслеживание выходной переменной $x_1(t)$ заданного сигнала $g(t)$ в следующих предположениях:

- за точку отсчета $x_1(t) = 0$ принято нижнее вертикальное положение звена манипулятора, которое является устойчивым, максимальная угловая скорость звена манипулятора ограничена:

$$|x_1(t)| \le \pi,\ |x_2(t)| \le X_2,\ t \ge 0,\ X_2 = \mathrm{const} > 0; \quad (3)$$

- начальные значения переменных состояния находятся в известных диапазонах:

$$|x_i(0)| \le X_{i,0} = \mathrm{const} > 0, i = \overline{1,5}; \quad (4)$$

- датчики расположены только на исполнительном устройстве, значения переменных $x_1(t)$, $x_2(t)$ не измеряются, значения переменных $x_3(t)$, $x_4(t)$ $x_5(t)$ измеряются, шумы в измерениях отсутствуют;
- текущие значения задающего воздействия $g(t)$ известны, его производная $\dot{g}(t)$ полагается негладкой неизвестной функцией времени, ограниченной известной константой:

$$\begin{gathered}|g(t)| \le G_0 < \pi;\ |\dot{g}(t)| \le G_1,\ t \ge 0;\\ G_0, G_1 = \mathrm{const} > 0;\end{gathered} \quad (5)$$

- значения параметров k_l, J_m, d, k_m и, следовательно, a_{43}, a_{44}, b_4 известны, параметры $\bar{m}$, h, J_l, c, R, L и, следовательно, $b_2 = a_{21}$, a_2, a_{54}, a_{55}, b_5 точно не определены и могут изменяться в процессе эксплуатации в известных диапазонах:

$$\begin{gathered}a_{21,\min} \le a_{21}(t) \le a_{21,\max}, a_{2,\min} \le a_2(t) \le a_{2,\max};\\ a_{5j,\min} \le a_{5j}(t) \le a_{5j,\max}, j = 4,5;\\ b_{5,\min} \le b_5(t) \le b_{5,\max}, t \ge 0;\end{gathered} \quad (6)$$

Таблица 1

Описание переменных и параметров объекта управления

Обозначение	Описание, единица измерения	Обозначение	Описание, единица измерения
x_1	угловое положение манипулятора, рад	$\bar{g}$	ускорение свободного падения, 9,8 м/с^2
x_2	угловая скорость манипулятора, рад/с	k_l	жесткость передаточного механизма, Н·м/рад
x_3	угловое положение вала ДПТ, рад	J_l	момент инерции манипулятора, кг·м^2
x_4	угловая скорость вала ДПТ, рад/с	k_m	коэффициент передачи, Н·м/А
x_5	ток якоря ДПТ, А	J_m	момент инерции ДПТ, кг·м^2
$f(t)$	неконтролируемое возмущение, Н/(кг·м)	d	коэффициент демпфирования, кг·м^2/с
u	напряжение питания якорной цепи ДПТ, В	c	коэффициент противо-ЭДС ДПТ, В·с/рад
h	длина манипулятора, м	L	индуктивность якоря ДПТ, Гн
$\bar{m}$	масса манипулятора, кг	R	сопротивление якоря ДПТ, Ом

• $f(t)$ – неизвестная негладкая функция времени, ограниченная по модулю известной константой:

$$|f(t)| \le F = \text{const} > 0,\ t \ge 0. \qquad (7)$$

В контуре обратной связи предполагается использование только наблюдателя неизмеряемых переменных состояния, идентификаторы неизвестных параметров и генераторы внешних воздействий в построения не вводятся. В этих условиях стабилизация ошибки слежения $e_1(t) = x_1(t) - g(t) \in R$ возможна лишь с некоторой точностью. Цель управления – обеспечить в замкнутой системе выполнение условия

$$|e_1(t)| \le \Delta_1,\ t \ge t_1, \qquad (8)$$

где $\Delta_1 > 0$, $t_1 > 0$ – заданные точность стабилизации и время ее достижения соответственно.

2. БАЗОВЫЙ ЗАКОН УПРАВЛЕНИЯ

Вначале сформируем в системе (1), (2) закон управления, используя заданный сигнал $g(t)$ и все переменные состояния, а потом спроектируем наблюдатель для оценивания неизмеряемых переменных состояния. Для синтеза обратной связи применим блочный принцип управления [11, 12].

Система (1), (2) представляет собой блочную форму управляемости [11]. Это означает, что истинное управление входит аддитивно с ненулевым множителем только в последнее уравнение; в правой части каждого i-го уравнения (блока), $i = \overline{1,4}$, могут присутствовать функции только от переменных состояния $x_1,\ldots,x_i$, а переменная следующего i+1-го уравнения входит аддитивно с ненулевым множителем. Такой вид позволяет в каждом i-м уравнении рассматривать переменную x_{i+1} как фиктивное управление и последовательно (сверху вниз) формировать локальные связи в каждом уравнении, которые в последнем блоке будут обеспечены с помощью истинного управления. Тот факт, что первое уравнение записано относительно именно регулируемой переменной, позволяет рассматривать систему (1), (2) как треугольную (по составу аргументов функций в каждом уравнении за исключением фиктивных управлений) форму «вход – выход» и решать на ее основе задачу слежения.

Для того чтобы подавить параметрические и внешние возмущения, действующие по одним и тем же каналам с фиктивными управлениями, сформируем локальные связи в виде ограниченных S-образных сигма-функций с двумя настраиваемыми параметрами [12]:

$$x_i^* = -m_{i-1}\sigma(k_{i-1}e_{i-1}),\ k_{i-1}, m_{i-1} = \text{const} > 0,\ i = \overline{2,5}, \qquad (9)$$

где $\sigma(k_{i-1}e_{i-1}) = 2/(1+\exp(-k_{i-1}e_{i-1})) - 1$ – нечетная и ограниченная сигма–функция; $|\sigma(k_{i-1}e_{i-1})| < 1$, $e_i \in R$ $(i = \overline{2,5})$ – невязки между переменными x_i и желаемыми фиктивными управлениями x_i^* (9):

$$e_i = x_i - x_i^* = x_i + m_{i-1}\sigma(k_{i-1}e_{i-1}),\ i = \overline{2,5}. \qquad (10)$$

Истинное управление (напряжение питания ДПТ) естественно принять в виде разрывной функции [6]

$$u = -m_5\text{sign}(e_5),\ m_5 = \text{const} > 0,$$
$$\text{sign}(e_5) = \begin{cases} +1, & e_5 > 0, \\ -1, & e_5 < 0, \end{cases} \qquad (11)$$

при $e_5 = 0$ значение функции знака не определено, но ограничено отрезком $[-1; 1]$. Замкнутая система (1), (2), (11), записанная относительно ошибки слежения и невязок (10), имеет вид:

$$\begin{aligned} \dot e_1 &= e_2 - m_1\sigma(k_1e_1) - \dot g, \\ \dot e_i &= b_i(e_{i+1} - m_i\sigma(k_ie_i)) - \\ &-\sum_{j=1}^{i} a_{ij}e_j + f_i + \Lambda_{i-1}, i = 2,3,4, \\ \dot e_5 &= -a_{54}e_4 - a_{55}e_5 + f_5 + \Lambda_4 - b_5m_5\text{sign}(e_5), \end{aligned} \qquad (12)$$

где $b_3 = 1$, элементы a_{ij}, указанные в формуле (12), но отсутствующие в системе (1), (2), равны нулю, Λ_{i-1} – полные производные фиктивных управлений (9)

$$\begin{aligned} \Lambda_{i-1} &= \tfrac{d}{dt}m_{i-1}\sigma(k_{i-1}e_{i-1}) = \\ &= 0{,}5m_{i-1}k_{i-1} \times (1-\sigma^2(k_{i-1}e_{i-1}))\dot e_{i-1},\ i = \overline{2,5}; \\ f_2 &= -a_{21}g - a_2\sin(e_1+g) + f(t),\ f_3 = 0, \\ f_4 &= a_{43}(m_2\sigma(k_2e_2) + g) + a_{44}m_3\sigma(k_3e_3), \\ f_5 &= a_{54}m_3\sigma(k_3e_3) + a_{55}m_4\sigma(k_4e_4). \end{aligned} \qquad (13)$$

В силу формул (5)–(7) значения f_i ограничены, их оценки зависят от амплитуд фиктивных управлений:

$$\begin{aligned} |f_2(t)| &\le a_{21,\max}G_0 + a_{2,\max} + F = F_2, \\ |f_4(t)| &\le a_{43}(m_2 + G_0) + a_{44}m_3 = F_4, \\ |f_5(t)| &\le a_{54,\max}m_3 + a_{55,\max}m_4 = F_5. \end{aligned} \qquad (14)$$

Поставленная задача (8) сводится к задаче стабилизации системы (12). При этом задача синтеза управления одноканальной системой пятого порядка декомпозируется на пять последовательно решаемых элементарных подзадач синтеза – выбора параметров истинного и фиктивных управлений, обеспечивающих инвариантность с заданной точностью по отношению к имеющимся неопреде-

ленностям. Амплитуду разрывного управления (11) нужно выбрать так, чтобы обеспечить в системе (12) возникновение за конечное время $0 < t_5 < t_1$ скользящего режима на поверхности $e_5 = 0$. Согласно блочному принципу управления параметры фиктивных управлений (9) следует выбрать так, чтобы организовать последовательную сходимость невязок в некоторые окрестности нуля:

$$\begin{gathered}|e_5(t)| \le \Delta_5, t \ge t_5 > 0 \Rightarrow |e_4(t)| \le \Delta_4, \\ t \ge t_4 > t_5 \Rightarrow \ldots \Rightarrow |e_1(t)| \le \Delta_1,\ t \ge t_1 > t_2,\end{gathered} \tag{15}$$

где Δ_1 и t_1 заданы выражением (8) а $\Delta_i = \text{const} > 0$, $i = \overline{2,5}$, назначаются произвольно. В первом неравенстве (15) отражен тот факт, что в реальных системах из-за различного рода неидеальностей скользящий режим возникает в некотором пограничном слое поверхности переключения [6].

Сигма-функцию можно оценить снизу кусочно-линейной функцией

$$\begin{gathered}0{,}8|\text{sat}(k_i e_i)| \le |\sigma(k_i e_i)| < 1, \\ \text{sat}(k_i e_i) = \begin{cases}\text{sign}(e_i), |e_i| > 2{,}2 / k_i, \\ k_i e_i / 2{,}2, |e_i| \le 2{,}2 / k_i,\ i = \overline{1,\ 4},\end{cases}\end{gathered} \tag{16}$$

где $\sigma(\pm 2{,}2) \approx \pm 0{,}8$, $e_i = \pm 2{,}2 / k_i$ – точки разделения $\sigma(k_i e_i)$ на почти линейную и почти постоянную функции [12]. От выбора значения k_i – коэффициента усиления в аргументе сигма-функции – зависит точность стабилизации соответствующей невязки. Зафиксируем обратно пропорциональную зависимость между коэффициентами усиления и точностью стабилизации невязок: $|e_i| \le 2{,}2 / k_i = \Delta_i, i = \overline{1,4}$. Тогда при выбранных значениях коэффициентов усиления

$$k_i \ge 2{,}2 / \Delta_i, i = \overline{1,4}, \tag{17}$$

обеспечивающих желаемую точность стабилизации, задача синтеза сводится к выбору амплитуд m_i, $i = \overline{1,\ 5}$, посредством которого достигается последовательная сходимость невязок в соответствующие окрестности нуля (15). Достаточные условия, гарантирующие $|e_i| \le \Delta_i$, имеют вид: $e_i \dot{e}_i < 0$ при $|e_i| > \Delta_i, i = \overline{1,5}$ [6, 12]. Отсюда получим нижнюю оценку для выбора амплитуды в i-м ($i = \overline{1,4}$) блоке при условии, что во всех следующих блоках $j = i + 1,\ i + 2, \ldots, 5$, невязки уже сошлись в заданные окрестности нуля $|e_j| \le \Delta_j$ (15). С учетом формул (5), (14)–(17) имеем:

$$\begin{gathered}0{,}8m_1 > G_1 + \Delta_2 \Rightarrow e_1\dot{e}_1 = e_1(e_2 - m_1\sigma(k_1 e_1) - \dot{g}) \le \\ \le |e_1|(\Delta_2 + G_1 - 0{,}8m_1) < 0, \\ 0{,}8b_{i,\min}m_i > b_{i,\min}\Delta_{i+1} + \sum_{j=1}^{i-1} a_{ij,\max}|e_j| + \\ + F_i + |\Lambda_{i-1}| \Rightarrow e_i\dot{e}_i = e_i(b_i(e_{i+1} - m_i\sigma(k_i e_i)) - \\ - \sum_{j=1}^{i} a_{ij}e_j + f_i + \Lambda_{i-1}) \le \\ \le |e_i|(b_{i,\min}(\Delta_{i+1} - 0{,}8m_i) - a_{ij,\min}|e_i| + \\ \sum_{j=1}^{i-1} a_{ij,\max}|e_j| + F_i + |\Lambda_{i-1}|) < 0,\ i = 2,\ 3,\ 4; \\ b_{5,\min}m_5 > a_{54,\max}|e_4| + F_5 + |\Lambda_4| \Rightarrow e_5\dot{e}_5 = \\ = e_5(-a_{54}e_4 - a_{55}e_5 + f_5 + \Lambda_4 - b_5 m_5 \text{sign}(e_5)) \le \\ \le |e_5|(a_{54,\max}|e_4| - a_{55,\min}|e_5| + \\ + F_5 + |\Lambda_4| - b_{5,\min}m_5) < 0.\end{gathered} \tag{18}$$

Для реализации достаточных условий (18) требуется оценить диапазоны изменения значений переменных системы (12) и их производных в процессе регулирования с учетом заданного времени стабилизации ошибки слежения (8). Соответствующая процедура и итоговые неравенства для выбора амплитуд m_i ($i = \overline{1,5}$) представлены в Приложении. Процедура опирается на консервативные оценки и доказывает существование решений неравенств (18). Принимаемые значения коэффициентов усиления (17) и амплитуд можно скорректировать в меньшую сторону по результатам имитационного моделирования.

В системе с неполным комплектом датчиков в законе управления (11) вместе с измеряемыми переменными $g(t)$, $x_3(t)$, $x_4(t)$ $x_5(t)$ будут использованы оценки $\hat{x}_1(t)$, $\hat{x}_2(t)$ неизмеряемых переменных состояния $x_1(t)$, $x_2(t)$. В § 3 рассматривается задача синтеза наблюдателя состояния, который в условиях параметрической неопределенности объекта управления обеспечивает заданные точность и время оценивания:

$$|x_i(t) - \hat{x}_i(t)| \le \delta_i,\ i = 1,2,\ t \ge T,\ 0 < T < t_5. \tag{19}$$

В системе с динамической обратной связью закон управления (11) будет реализован в виде

$$u = -m_5 \text{sign}(\hat{e}_5), \tag{20}$$

где ошибка слежения и невязки (10) формируются по измеряемым и оценочным сигналам:

$$\hat{e}_1 = \hat{x}_1 - g,\ \hat{e}_2 = \hat{x}_2 + m_1\sigma(k_1\hat{e}_1),\ \hat{e}_3 = x_3 + m_2\sigma(k_2\hat{e}_2),$$
$$\hat{e}_4 = x_4 + m_3\sigma(k_3\hat{e}_3),\ \hat{e}_5 = x_5 + m_4\sigma(k_4\hat{e}_4).$$

В замкнутой системе (1), (2) с динамической обратной связью (20) в качестве неидеальностей выступают ошибки оценивания (19), что приводит к появлению в скользящем режиме пограничного слоя

$$\left|\hat{e}_5 - e_5\right| = m_4 \left|\sigma(k_4\hat{e}_4) - \sigma(k_4 e_4)\right| \le \Delta_5. \qquad (21)$$

Из (21) и *S*-образной формы сигма-функции следует, что наибольшее отклонение достигается в окрестности нуля, а на бесконечности влияние ошибок оценивания будет практически незаметно. С учетом первого приближения $\sigma(kx) \underset{x\to 0}{\sim} 0{,}5kx$ можно дать следующую оценку отклонению (21):

$$\begin{gathered}\left|\sigma(k_4\hat{e}_4) - \sigma(k_4 e_4)\right| \approx 0{,}5k_4\left|\hat{e}_4 - e_4\right| \approx \\ \approx 0{,}5k_4 m_3\left|\sigma(k_3\hat{e}_3) - \sigma(k_3 e_3)\right| \approx 0{,}5^2 k_4 m_3 k_3\left|\hat{e}_3 - e_3\right| \approx \\ \approx 0{,}5^2 k_4 m_3 k_3 m_2\left|\sigma(k_2\hat{e}_2) - \sigma(k_2 e_2)\right| \approx \\ \approx 0{,}5^3 k_4 m_3 k_3 m_2 k_2\left|\hat{e}_2 - e_2\right| \approx \\ \approx 0{,}5^3 k_4 m_3 k_3 m_2 k_2\left|\delta_2 + m_1\left|\sigma(k_1\hat{e}_1) - \sigma(k_1 e_1)\right|\right| \approx \\ \approx 0{,}5^3 k_4 m_3 k_3 m_2 k_2(\delta_2 + 0{,}5m_1 k_1\delta_1).\end{gathered}$$

Из данного выражения с учетом принятых значений параметров регулятора и величины пограничного слоя Δ_5, учитываемой при его настройке, следуют ограничения на ошибки оценивания, которые нужно обеспечить при решении задачи наблюдения:

$$\delta_2 + 0{,}5m_1 k_1\delta_1 \le \frac{8\Delta_5}{m_4 k_4 m_3 k_3 m_2 k_2}. \qquad (22)$$

3. НАБЛЮДАТЕЛЬ СОСТОЯНИЯ ДЛЯ ОЦЕНКИ ПЕРЕМЕННЫХ МЕХАНИЧЕСКОЙ ПОДСИСТЕМЫ

Система (1), (2) является наблюдаемой относительно измерений $x_3(t)$, $x_4(t)$ $x_5(t)$, однако наблюдатель состояния полного порядка невозможно синтезировать из-за наличия параметрических неопределенностей в модели и действия на объект неконтролируемых внешних возмущений. Для восстановления значений неизмеряемых переменных $x_1(t)$, $x_2(t)$ воспользуемся процедурой оценивания внешних возмущений без построения динамического генератора возмущений [7, 15, 16] и будем строить наблюдатель пониженного порядка (редуцированный наблюдатель). В этом случае искомые оценки $\hat{x}_1$, $\hat{x}_2$ могут быть получены только с заданной точностью (19), (22).

Согласно данной процедуре оценивания для построения редуцированного наблюдателя примем за основу четвертое и первое уравнения исходной системы (1), (2), которые не зависят от значений неопределенных параметров и включают в себя неизмеряемые переменные с ненулевыми множителями:

$$\dot{x}_4 = -a_{43}(x_3 - x_1) - a_{44}x_4 + a_{45}x_5,\ \dot{x}_1 = x_2. \qquad (23)$$

Редуцированный наблюдатель строится на основе системы (23) с учетом измеряемых сигналов:

$$\dot{z}_1 = -a_{43}(x_3 - z_2) - a_{44}x_4 + a_{45}x_5 + v_1,\ \dot{z}_2 = v_2, \qquad (24)$$

где z_1, z_2 – переменные состояния наблюдателя, v_1, v_2 – его корректирующие воздействия.

Введем ошибки наблюдения $\varepsilon_1 = x_4 - z_1$, $\varepsilon_2 = x_1 - z_2$, относительно которых с учетом формул (23), (24) получим систему

$$\dot{\varepsilon}_1 = a_{43}\varepsilon_2 - v_1,\ \dot{\varepsilon}_2 = x_2 - v_2. \qquad (25)$$

В силу имеющихся измерений значений параметра x_4 текущие значения ошибки $\varepsilon_1(t)$ известны, ошибки $\varepsilon_2(t)$ – неизвестны. Примем следующие начальные значения в наблюдателе (24) и, соответственно, в виртуальной системе (25):

$$\begin{gathered}z_1(0) = x_4(0) \Rightarrow \varepsilon_1(0) = 0; \\ z_2(0) = 0 \Rightarrow \varepsilon_2(0) = x_1(0),\ \left|\varepsilon_2(0)\right| \le \pi.\end{gathered} \qquad (26)$$

Цель – сформировать корректирующие воздействия v_1, v_2 так, чтобы обеспечить стабилизацию ошибок наблюдения и их производных с заданной точностью и за заданное время (19), (22). Для этого используем кусочно-линейные корректирующие воздействия [7, 15, 16]:

$$\begin{gathered}v_1 = p_1\,\mathrm{sat}(l_1\varepsilon_1),\ v_2 = p_2\,\mathrm{sat}(l_2 v_1),\ l_i,\ p_i = \mathrm{const} > 0, \\ \mathrm{sat}(l_1\varepsilon_1) = \begin{cases}\mathrm{sign}(\varepsilon_1),\ \left|\varepsilon_1\right| > 1/l_1, \\ l_1\varepsilon_1,\ \left|\varepsilon_1\right| \le 1/l_1.\end{cases}\end{gathered} \qquad (27)$$

Функции (27) так же, как и сигма-функции, имеют *S*-образную форму и по два настраиваемых параметра. Они более просты в реализации, но не являются гладкими. Однако последний факт не является критичным, так как в задаче наблюдения корректирующие воздействия не несут физического смысла и могут быть негладкими – в отличие от фиктивных управлений, в качестве которых принимаются переменные состояния (10) (а к ним, в свою очередь, предъявляется требование гладкости).

Лемма. *Если в системе* (25)–(27) *внешний сигнал* $x_2(t)$ *ограничен условием* (3)*, то для любых* $\delta_1 > 0$, $\delta_2 > 0$, $T > 0$ *найдутся положительные*

действительные числа $\overline{p}_i$, $\overline{l}_i$ *такие, что при любых* $p_i > \overline{p}_i$, $l_i \ge \overline{l}_i$, $i = 1,2$, *будет обеспечено выполнение неравенств*

$$\begin{aligned} |\varepsilon_2(t)| = |x_1(t) - z_2(t)| \le \delta_1, \\ |x_2(t) - v_2(t)| \le \delta_2,\ t \ge T. \end{aligned} \tag{28}$$

Доказательство леммы приведено в Приложении. Из выражений (19), (28) следует, что в качестве искомых оценок неизмеряемых переменных принимаются переменная состояния и корректирующее воздействие второго уравнения редуцированного наблюдателя (24): $\hat{x}_1(t) = z_2(t)$, $\hat{x}_2(t) = v_2(t)$.

4. РЕЗУЛЬТАТЫ МОДЕЛИРОВАНИЯ

Для проверки работоспособности разработанного метода синтеза динамической обратной связи было проведено численное моделирование в среде MATLAB-Simulink замкнутой системы (1), (2), (20), (24) при начальных значениях $x_i(0) = 0$, $i = \overline{1,5}$. Ставилась задача обеспечения достижения следующих значений целевых показателей (8):

$$\Delta_1 = 0{,}04 \text{ рад},\ t_1 = 2 \text{ с}. \tag{29}$$

С учетом значений (29), а также значений и диапазонов изменения параметров и внешних воздействий

$$\begin{gathered} k_l = 0{,}2,\ J_m = 0{,}01,\ d = 0{,}045,\ k_m = 0{,}3; \\ \overline{m} \in [0{,}18;\ 0{,}25],\ h \in [0{,}2;\ 0{,}3], \\ J_l \in [0{,}0072;\ 0{,}0225],\ c \in [0{,}25;\ 0{,}33], \\ R \in [3{,}8;\ 4{,}2],\ L \in [0{,}006;\ 0{,}013]; \\ |g^{(i)}(t)| \le 0{,}2,\ i = \overline{0,1};\ |f(t)| \le 0{,}1 \end{gathered} \tag{30}$$

на основе неравенств (17), (П.9)–(П.13) (см. Приложение) были приняты следующие значения коэффициентов обратной связи:

$$\begin{gathered} k_1 = 80,\ k_2 = 25,\ k_3 = 5,\ k_4 = 8; \\ m_1 = 0{,}3,\ m_2 = 0{,}7,\ m_3 = 10,\ m_4 = 40,\ m_5 = 90. \end{gathered} \tag{31}$$

В силу выражений (19), (22) были определены значения целевых показателей для решения задачи наблюдения: $\delta_1 = 0{,}0008$ рад, $\delta_2 = 0{,}002$ рад/с, $T = 0{,}1$ с. В наблюдателе (24) с учетом ограничения $|x_2(t)| \le 5 = X_2$ рад/с (3) на основе неравенств (П.22), (П.26) (см. Приложение) приняты следующие значения коэффициентов коррекции (27):

$$l_1 = 155,\ l_2 = 150;\ p_1 = 60,\ p_2 = 40. \tag{32}$$

Проведено два численных эксперимента с одинаковыми коэффициентами регулятора (31) и наблюдателя (32), но с разными параметрами объекта и внешними воздействиями из диапазонов (30). В первом эксперименте в качестве значений неопределенных параметров объекта принимались левые границы отрезков (30) и внешние воздействия $g(t) = 0{,}05|\sin t| + 0{,}15\cos(0{,}5t)$, $f = 0{,}05$. Во втором эксперименте в качестве значений параметров объекта принимались правые границы отрезков (30) и внешние воздействия $g(t) = 0{,}18|\cos(t)|$, $f(t) = 0{,}05t$, $t \in [0;2)$ – пилообразная функция с главным периодом 2 с. Обратим внимание на то, что в обоих экспериментах задающие воздействия – кусочно-гладкие функции, производные которых имеют разрывы первого рода. В целях сравнения моделирование выполнялось и для системы со статической обратной связью (11) в предположении, что все переменные состояния измеряются, и для системы с динамической обратной связью (20), в которой оценки неизмеряемых переменных $\hat{x}_1(t)$, $\hat{x}_2(t)$ были получены с помощью наблюдателя (24), (27). При интегрировании использовался метод Эйлера с постоянным шагом 10^{-5}.

На рис. 1–4 представлены результаты моделирования первого эксперимента. Для системы (1), (2) с динамической обратной связью (20), (24), (27) представлены: на рис. 1 – графики заданного сигнала $g(t)$ и углового положения манипулятора $x_1(t)$; на рис. 2 – график ошибки слежения $e_{1д}(t) = x_1(t) - g(t)$; на рис. 3 – графики $\alpha_1(t) = x_1(t) - \hat{x}_1(t)$, $\alpha_2(t) = x_2(t) - \hat{x}_2(t)$ – отклонений оценок $\hat{x}_1(t) = z_2(t)$, $\hat{x}_2(t) = v_2(t)$, полученных с помощью наблюдателя (24), (27), от значений переменных $x_1(t)$, $x_2(t)$. На рис. 4 показан график $e_{1д}(t) - e_{1с}(t)$ – отклонения $e_{1д}(t)$ от ошибки слежения $e_{1с}(t)$ в системе со статической обратной связью (11). На рис. 5–8 показаны аналогичные графики для эксперимента 2.

В табл. 2 для обоих экспериментов и законов управления приведены показатели качества: время регулирования t^*: $|e_1(t)| \le 0{,}04$, $t \ge t^*$; перерегулирование $e_{1\max} \ge |e_1(t)|$, $t \ge 0$; достигаемая точность слежения $\overline{\Delta}_1 \ge |x_1(t) - g(t)|$ в установившемся режиме при $t \ge 10$ с.

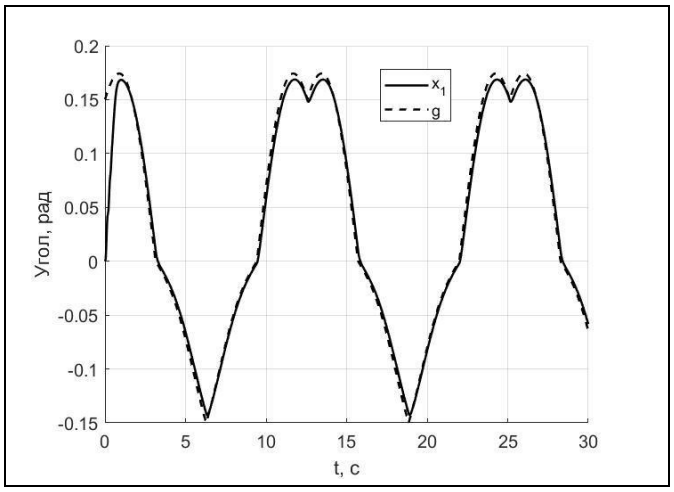


Рис. 1. Графики изменения значений переменных $g(t)$, $x_1(t)$ для эксперимента 1

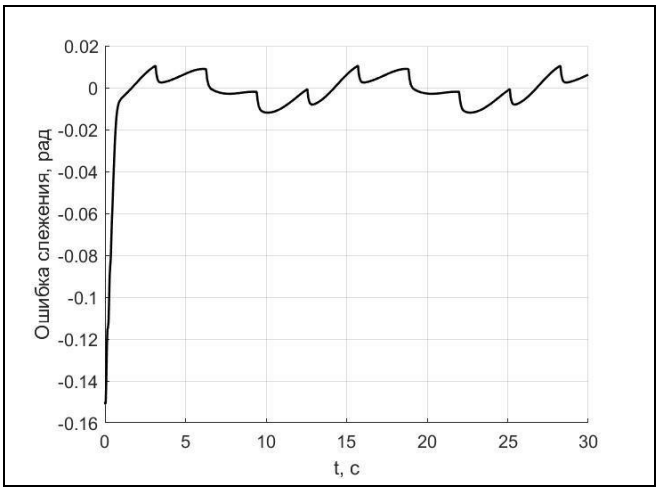


Рис. 2. График изменения ошибки слежения $e_{1д}(t)$ для эксперимента 1

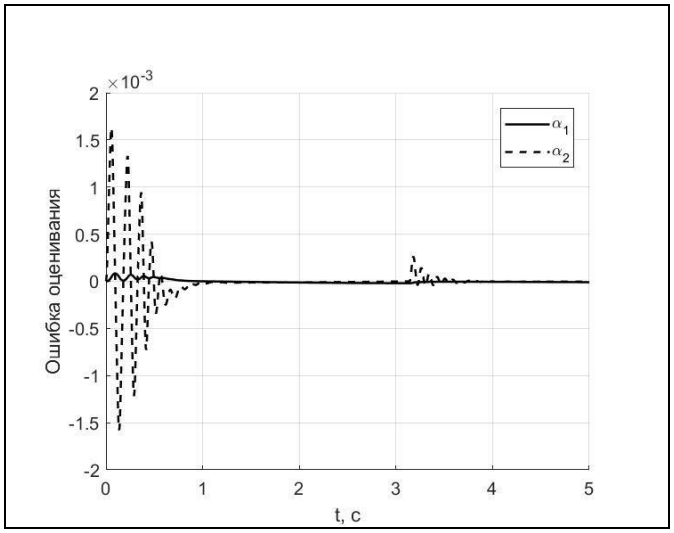


Рис. 3. Графики изменения отклонений $\alpha_1(t) = x_1(t) - \hat{x}_1(t)$, $\alpha_2(t) = x_2(t) - \hat{x}_2(t)$ для эксперимента 1

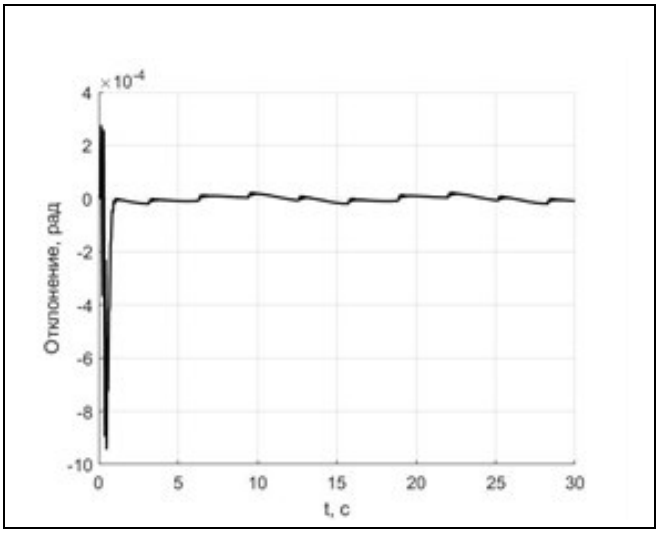


Рис. 4. График изменения отклонения e1д(t)–e1c(t) для эксперимента 1

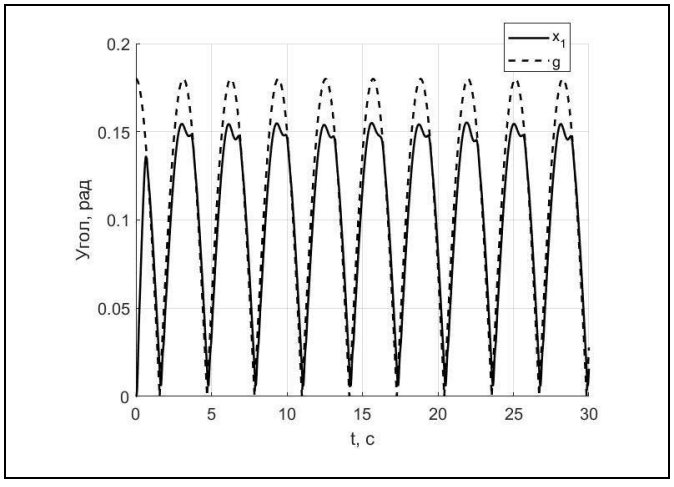


Рис. 5. Графики изменения значений переменных g(t), x_1(t) для эксперимента 2

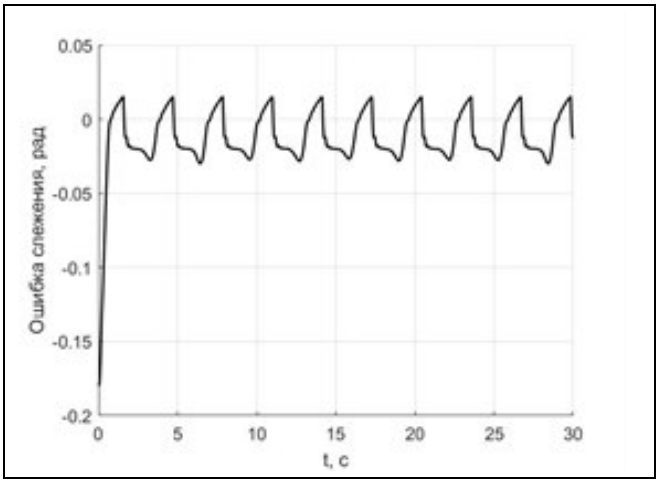


Рис. 6. График изменения ошибки $e_{1д}(t)$ для эксперимента 2

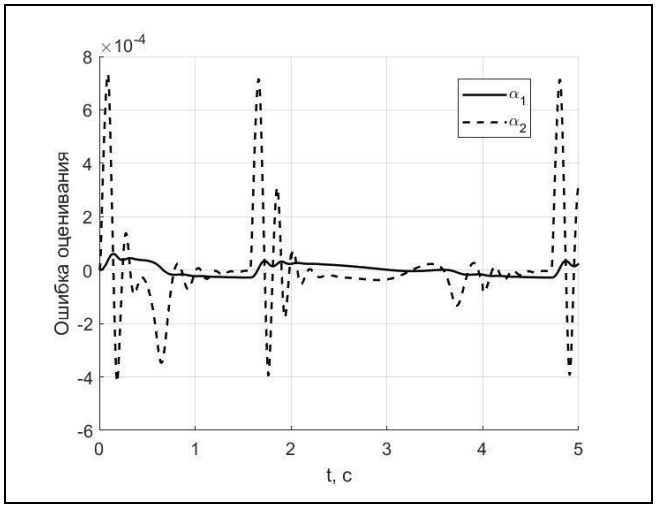


Рис. 7. Графики изменения отклонений $\alpha_1(t) = x_1(t) - \hat{x}_1(t)$, $\alpha_2(t) = x_2(t) - \hat{x}_2(t)$ для эксперимента 2

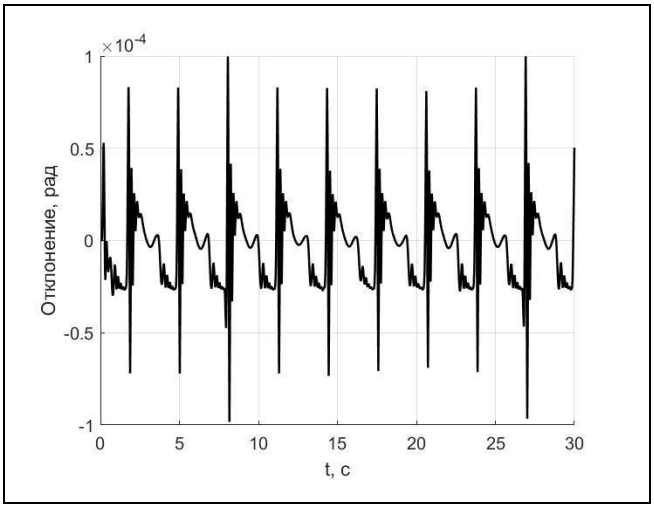


Рис. 8. График изменения ошибки $e_{1д}(t)$–$e_{1с}(t)$ для эксперимента 2

Таблица 2

Значения показателей качества регулирования

Наименование показателя, единица измерения	Статическая обратная связь (11)	Динамическая обратная связь (20), (24), (27)
Эксперимент 1		
t^*, с	0,5380	0,5408
e_{1max}, рад	0,1510	0,1510
$\overline{\Delta}_1$, рад	0,0119	0,0119
Эксперимент 2		
t^*, с	0,5146	0,5147
e_{1max}, рад	0,18	0,18
$\overline{\Delta}_1$, рад	0,0299	0,0299

Из рис. 1–8 и табл. 2 следует, что целевые значения показателей (29) достигаются во всех экспериментах. Ввод редуцированного наблюдателя (24), (27) в контур обратной связи не привел к существенному ухудшению качества регулирования.

ЗАКЛЮЧЕНИЕ

Цель настоящей работы заключалась в обеспечении отслеживания угловым положением однозвенного манипулятора заданного сигнала в условиях действия негладких внешних воздействий в случае, когда датчики установлены только на приводе. Эта цель была достигнута путем применения блочной процедуры синтеза обратной связи с сигмоидальными фиктивными управлениями, которые настраивались для «худших» допустимых значений неопределенных параметров и внешних возмущений. Для оценки углового положения и скорости манипулятора спроектирован редуцированный наблюдатель состояния, построение которого не требует точного знания параметров механической подсистемы. Результаты численного моделирования подтвердили работоспособность разработанных систем слежения и наблюдения. Показано, что при использовании динамической обратной связи с редуцированным наблюдателем значения показателей качества замкнутой системы сопоставимы со значениями показателей системы с полными измерениями.

В дальнейшем планируется распространить процедуру блочного синтеза сигмоидальных фиктивных управлений на линейные объекты со многими входами и выходами, а также исследовать работоспособность редуцированного наблюдателя при наличии шумов в измерениях.

ПРИЛОЖЕНИЕ

П р о ц е д у р а (выбора амплитуд истинного (11) и фиктивных (9) управлений). Вначале оценим значения переменных состояния системы (12). В силу формул (3)–(5) и (10) для области их начальных значений имеем оценки

$$|e_1(0)| \le X_{1,0} + G_0, |e_i(0)| \le X_{i,0} + m_{i-1}, i = \overline{2,5}. \quad (П.1)$$

В общем случае $|e_i(0)| > \Delta_i, i = \overline{1,5}$, в системе (12) монотонный переходный процесс гарантирован только для переменной последнего блока $e_5(t)$. В худшем расчетном случае значения переменных $e_i(t)$, $i = \overline{1,4}$ растут по модулю до тех пор, пока все переменные $e_j(t)$, $j = 5,4,\ldots,i+1$ не достигнут заданных окрестностей (15), т. е.

$$|e_5(t)| \le |e_5(0)| = e_{5,max}, |e_i(t)| \le |e_i(t_{i+1})| = e_{i,max}, i = \overline{4,1}. \quad (П.2)$$

С учетом того, что в системе (1), (2) и, следовательно, в системе (12) $a_{ii} = 0,\ i = \overline{1,3}$, $a_{44} > 0$, в силу выражений (18) и (П.1), (П.2) можно дать следующие оценки переменных состояния и их производных:

$$\begin{gathered} e_{1,\max} \le X_{1,0} + G_0 + (e_{2,\max} - \Delta_2)t_2, \\ e_{i,\max} \le X_{i,0} + m_{i-1} + b_{i,\max}(e_{i+1,\max} - \Delta_{i+1})t_{i+1}, i = 2,3, \\ e_{4,\max} \le X_{4,0} + m_3 + b_4(e_{5,\max} - \Delta_5)(1 - \exp(-a_{44}t_5))/a_{44}, \\ e_{5,\max} \le X_{5,0} + m_4; \end{gathered} \tag{П.3}$$

$$\begin{gathered} |\dot e_i(t)| < b_{i,\max}(2m_i + e_{i+1,\max} - \Delta_{i+1}), t \in [0; t_{i+1}), \\ |\dot e_i(t)| < 2b_{i,\max}m_i,\ t \ge t_{i+1},\ i = \overline{1,3},\ b_{1,\max} = b_{3,\max} = 1; \\ |\dot e_4(t)| < b_4(2m_4 + e_{5,\max} - \Delta_5) + a_{44}e_{4,\max},\ t \in [0;\ t_5), \\ |\dot e_4(t)| < 2b_4m_4 + a_{44}e_{4,\max},\ t \in [t_5;\ t_4), \\ |\dot e_4(t)| < 2b_4m_4 + a_{44}\Delta_4,\ t \ge t_4. \end{gathered} \tag{П.4}$$

С учетом введенного разделения сигма-функции (16) для ее производной $\sigma'(k_ie_i) = 0{,}5k_i(1 - \sigma^2(k_ie_i))$ имеем:

$$\begin{gathered} 0 < \sigma'(k_ie_i) < 0{,}18k_i,\ t \in [0; t_i),\ |e_i(t)| > 2{,}2/k_i, \\ 0{,}18k_i \le \sigma'(k_ie_i) \le 0{,}5k_i,\ t \ge t_i,\ |e_i(t)| \le 2{,}2/k_i, \\ i = \overline{1,4}. \end{gathered} \tag{П.5}$$

На максимальные по модулю значения невязок, зависящих от времени (П.3), введем ограничения

$$e_{1,\max} \le 2\pi, e_{i+1,\max} \le 3m_i + \Delta_{i+1}, i = \overline{1,3}, \tag{П.6}$$

тогда выражения (П.3) примут вид

$$\begin{gathered} e_{1,\max} \le X_{1,0} + G_0 + 3m_1t_2 \le 2\pi, \\ e_{i,\max} \le X_{i,0} + m_{i-1} + 3b_{i,\max}m_it_{i+1} \le 3m_{i-1} + \Delta_i,\ i = 2,\ 3, \\ e_{4,\max} \le X_{4,0} + m_3 + b_4(X_{5,0} + m_4 - \Delta_5)\times \\ \times(1 - \exp(-a_{44}t_5))/a_{44} \le 3m_3 + \Delta_4. \end{gathered} \tag{П.7}$$

В силу формул (П.4)–(П.7) для производных фиктивных управлений (13) получим следующие оценки:

$$\begin{gathered} |\Lambda_i(t)| = m_i\frac{k_i(1 - \sigma^2(k_ie_i))}{2}|\dot e_i| \le k_im_i^2b_{i,\max}, i = \overline{1,3}; \\ |\Lambda_4(t)| \le k_4m_4^2b_4 + 0{,}5k_4m_4a_{44}e_{4,\max}, t \ge 0. \end{gathered} \tag{П.8}$$

Для того чтобы обеспечить выполнение неравенств (П.6), амплитуды $m_i, i = \overline{1,4}$, должны быть ограничены сверху. Примем для удобства $0 < \Delta_i = X_{i,0},\ i = \overline{2,5}$, тогда из правых неравенств (П.7) получим

$$\begin{gathered} m_1 \le m_{1,\max} = \frac{2\pi - X_{1,0} + G_0}{3t_2},\ m_i \le m_{i,\max} = \frac{2m_{i-1}}{3b_{i,\max}t_{i+1}}, \\ i = 2,\ 3,\ m_4 \le m_{4,\max} = \frac{2m_3a_{44}}{b_4(1 - \exp(-a_{44}t_5))}. \end{gathered} \tag{П.9}$$

Очевидно, что верхние границы для выбора амплитуд (П.9) можно сделать сколь угодно большими путем уменьшения значений $t_i,\ i = \overline{2,5}$, с соблюдением иерархии $0 < t_5 < t_4 < \ldots < t_2 < t_1$.

Формализуем процедуру последовательного выбора амплитуд $m_i,\ i = \overline{1,5}$, которые обеспечат в замкнутой системе (12) выполнение условий (15) и, следовательно, цели управления (8) при заданных значениях Δ_1, t_1, принятых значениях $\Delta_i = X_{i,0},\ i = \overline{2,5}$, и выбранных на их основе значениях коэффициентов усиления (17). Амплитуды нужно выбрать так, чтобы обеспечить сходимость невязок $e_i(t),\ i = \overline{5,1}$, на интервалах $[t_{i+1};\ t_i]$, $t_6 = 0$, в заданные окрестности нуля с учетом выражений (18) и (П.7)–(П.9). Варьируемыми параметрами являются моменты времени $t_i,\ i = \overline{2,5}$.

Шаг 1. С учетом выражения (П.7) и интервала сходимости $[t_2;\ t_1]$ первое неравенство (18) можно представить в виде

$$\begin{gathered} 0{,}8m_1 \ge \frac{X_{1,0} + G_0 + 3m_1t_2 - \Delta_1}{t_1 - t_2} + G_1 + X_{2,0} \Rightarrow \\ \Rightarrow m_1 \ge m_{1,\min} = \frac{X_{1,0} + G_0 - \Delta_1 + (G_1 + X_{2,0})(t_1 - t_2)}{0{,}8t_1 - 3{,}8t_2}. \end{gathered} \tag{П.10}$$

Из неравенства (П.10) следует ограничение на выбор $0 < t_2 < t_1$: $0{,}8t_1 - 3{,}8t_2 > 0 \Rightarrow t_2 < 0{,}2t_1$. Фиксируем значения t_2^*, m_1^*:

$$\begin{gathered} 0 < t_2^* < 0{,}2t_1 : m_{1,\min}(t_2^*) < m_{1,\max}(t_2^*); \\ m_1^* \in [m_{1,\min}(t_2^*);\ m_{1,\max}(t_2^*)] \end{gathered}$$

и переходим на следующий шаг процедуры.

Шаг i (i = 2,3). С учетом выражений (П.7), (П.8) и интервала сходимости $[t_{i+1};\ t_i^*]$ i-е неравенство (18) примет вид

$$\begin{gathered} 0{,}8b_{i,\min}m_i \ge \frac{m_{i-1}^* + 3b_{i,\max}m_it_{i+1}}{t_i^* - t_{i+1}} + b_{i,\min}X_{i+1,0} + \\ + \sum_{j=1}^{i-1}a_{ij,\max}e_{j,\max}(m_j^*) + F_i + k_{i-1}(m_{i-1}^*)^2b_{i-1,\max} \Rightarrow \\ \Rightarrow m_i \ge m_{i,\min} = \frac{m_{i-1}^* + (b_{i,\min}X_{i+1,0} + \sum_{j=1}^{i-1}a_{ij,\max}e_{j,\max}(m_j^*)}{0{,}8b_{i,\min}t_i^* - (0{,}8b_{i,\min} + 3b_{i,\max})t_{i+1}} + \\ + \frac{F_i + k_{i-1}(m_{i-1}^*)^2b_{i-1,\max})(t_i^* - t_{i+1})}{0{,}8b_{i,\min}t_i^* - (0{,}8b_{i,\min} + 3b_{i,\max})t_{i+1}},\ i = 2,\ 3. \end{gathered} \tag{П.11}$$

Из неравенства (П.11) следует ограничение на выбор значения t_{i+1}: $0{,}8b_{i,\min}t_i^* - (0{,}8b_{i,\min} + 3b_{i,\max})t_{i+1} > 0 \Rightarrow$ $\Rightarrow t_{i+1} < 0{,}2b_{i,\min}t_i^*/b_{i,\max},\ i = 2,\ 3,\ b_{3,\min} = b_{3,\max} = 1$. Фиксируем значения t_{i+1}^*, m_i^*:

$$\begin{gathered} t_{i+1}^* < 0{,}2b_{i,\min}t_i^*/b_{i,\max} : m_{i,\min}(t_{i+1}^*) < m_{i,\max}(t_{i+1}^*); \\ m_i^* \in [m_{i,\min}(t_{i+1}^*); m_{i,\max}(t_{i+1}^*)] \end{gathered}$$

и переходим на следующий шаг процедуры.

Шаг 4. С учетом выражений (П.7), (П.8) и интервала сходимости $[t_5;t_4^*]$ четвертое неравенство (18) примет вид

$$0,8b_4m_4 \ge \frac{m_3^* + b_4m_4(1-\exp(-a_{44}t_5))/a_{44}}{t_4^* - t_5} + b_4X_{5,0} + a_{41}e_{1,\max} + a_{43}e_{3,\max} + F_4 + k_3(m_3^*)^2 \Rightarrow$$

$$\Rightarrow m_4 \ge m_{4,\min} = \frac{m_3^* + [b_4X_{5,0} + a_{41}(X_{1,0} + G_0 + 3m_1^*t_2^*)}{b_4(0,8(t_4^* - t_5) - (1-\exp(-a_{44}t_5))/a_{44})} + \frac{a_{43}(X_{3,0} + m_2^* + 3m_3t_4^*) + F_4 + k_3(m_3^*)^2](t_4^* - t_5)}{b_4(0,8(t_4^* - t_5) - (1-\exp(-a_{44}t_5))/a_{44})}. \quad (П.12)$$

Из неравенства (П.12) следует ограничение на выбор значения t_5: $0,8t_5 + (1-\exp(-a_{44}t_5))/a_{44} < 0,8t_4^*$. Фиксируем значения t_5^*, m_4^*:

$$t_5^* + 1,25(1-\exp(-a_{44}t_5^*))/a_{44} < t_4^* : m_{4,\min}(t_5^*) < m_{4,\max}(t_5^*);$$
$$m_4^* \in [m_{4,\min}(t_5^*); m_{4,\max}(t_5^*)]$$

и переходим на последний шаг процедуры.

Шаг 5. С учетом выражений (14), (П.7), (П.8) и интервала сходимости $[0;t_5^*]$ последнее неравенство (18) примет вид

$$b_{5,\min}m_5 \ge \frac{X_{5,0} + m_4^*}{t_5^*} + a_{54,\max}m_3^* + a_{55,\max}m_4^* + k_4(m_4^*)^2b_4 + (a_{54,\max} + 0,5k_4m_4^*a_{44}) \times (X_{4,0} + m_3^* + b_4m_4^*)(1-\exp(-a_{44}t_5^*))/a_{44}). \quad (П.13)$$

Процедура выбора амплитуд завершена. ♦

Доказательство леммы. При решении задачи управления переменные замкнутой системы (12) сходились в некоторую окрестность нуля последовательно «снизу вверх» (15), т. е. сначала обеспечивалась сходимость e_5, затем e_4 и так, пока не была достигнута цель управления – сходимость e_1. При решении задачи наблюдения в системе (25), напротив, устанавливается порядок сходимости ошибок наблюдения и их производных в окрестности нуля «сверху вниз», а именно

$$|\varepsilon_1(t)| \le 1/l_1,\ t \ge 0; \quad (П.14)$$

$$|a_{43}\varepsilon_2(t) - v_1(t)| = |\gamma_1(t)| \le a_{43}\beta_2,\ t \ge t_{01}; \quad (П.15)$$

$$|\varepsilon_2(t)| \le \beta_2 + 1/(a_{43}l_2),\ t \ge t_{02},\ \ 0 < t_{01} < t_{02} < T < t_5, \quad (П.16)$$

где $\beta_2 = \text{const} > 0$.

Неравенства (П.14), (П.16) и время попадания аргументов корректирующих воздействий (27) в окрестности нуля, где корректирующие воздействия описываются линейными функциями без насыщения (далее – линейные зоны), обеспечиваются выбором соответствующих значений амплитуд p_1, p_2. Неравенство (П.15), второе неравенство (28), а также заданная точность оценивания (19) достигаются путем выбора значений коэффициентов усиления l_1, l_2. Формализуем достаточные условия для выбора значений параметров корректирующих воздействий (27), обеспечивающих указанные требования.

Сначала рассмотрим настройку амплитуд. В силу выражения (26) $\varepsilon_1(0) = 0 \le 1/l_1$, т. е. переменная $\varepsilon_1(t)$ изначально находится в линейной зоне. В ней первое уравнение системы (25), (27) имеет вид $\dot{\varepsilon}_1 = a_{43}\varepsilon_2 - p_1l_1\varepsilon_1$. На основе того вида, который оно принимает вне линейной зоны, $\dot{\varepsilon}_1 = a_{43}\varepsilon_2 - p_1\text{sign}(\varepsilon_1)$, получим достаточные условия для выбора значения p_1, обеспечивающие выполнение неравенства (П.14):

$$p_1 > a_{43}|\varepsilon_2| \Rightarrow \varepsilon_1\dot{\varepsilon}_1 = \varepsilon_1(a_{43}\varepsilon_2 - p_1\text{sign}(\varepsilon_1)) \le \le |\varepsilon_1|(a_{43}|\varepsilon_2| - p_1) < 0. \quad (П.17)$$

Во втором уравнении системы (25), (27) равенство $\text{sign}(v_2(t)) = \text{sign}(\varepsilon_2(t))$ гарантировано вне области $|\varepsilon_2(t)| \le \beta_2$ при $t \ge t_{01}$ после выполнения условия (П.15). Для худшего расчетного случая согласно выражениям (П.15), (П.16) имеем:

$$\dot{\varepsilon}_2 = \begin{cases} x_2 + p_2\text{sign}(\varepsilon_2),\ t \in [0;t_{01}), \\ x_2 - p_2\text{sign}(\varepsilon_2),\ t \in [t_{01};t_{02}), \\ x_2 - p_2l_2(a_{43}\varepsilon_2(t) \pm \gamma_1),\ t \ge t_{02}. \end{cases} \quad (П.18)$$

С учетом выражения (3) максимальное по модулю значение переменной $\varepsilon_2(t)$ достигается при $t = t_{01}$, а именно:

$$|\varepsilon_2(t)| \le |\varepsilon_2(t_1)| \le \pi + (X_2 + p_2)t_{01} = E_2,\ t \ge 0. \quad (П.19)$$

Достаточные условия выбора значения p_2 аналогичны (П.17). В силу (П.19) получим неравенство для выбора значения p_2, обеспечивающего сходимость в линейную зону (П.16) на интервале $[t_{01}; t_{02})$:

$$p_2 \ge \frac{\pi + (X_2 + p_2)t_{01} - \delta_1}{t_{02} - t_{01}} + X_2 \Rightarrow \Rightarrow p_2 \ge \frac{\pi + X_2t_{02} - \delta_1}{t_{02} - 2t_{01}}. \quad (П.20)$$

Из выражения (П.20) следует ограничение $t_{02} > 2t_{01}$, которое нужно учитывать при назначении интервалов времени. Примем, например,

$$t_{02} - 2t_{01} = T - t_{02} = t_{01} \Rightarrow t_{01} = T/4. \quad (П.21)$$

Объединяя выражения (П.17), (П.19)–(П.21), получим итоговые неравенства для последовательного выбора амплитуд корректирующих воздействий (27), обеспечивающих выполнение условий (П.14), (П.16) за заданное время:

$$p_2 \ge \overline{p}_2 = \frac{4(\pi - \delta_1)}{T} + 3X_2, \quad p_1 > \overline{p}_1 = a_{43}(\pi + (X_2 + p_2)T/4). \quad (П.22)$$

Далее рассмотрим настройку коэффициентов усиления корректирующих воздействий (27), гарантирующих выполнение условий (П.15), (28). Для этого составим и проанализируем оценки решений системы (25), (27) в линейных зонах (первого уравнения – на интервале

$[0; t_{01}]$; второго уравнения – на интервале $[t_{02}; t_{02} + t_{01} = T]$). На основе третьего уравнения (П.18), а также выражений (П.19), (П.21) имеем:

$$|\varepsilon_1(t_1)| \le \frac{a_{43}E_2}{p_1 l_1} + \frac{p_1 - a_{43}E_2}{p_1 l_1} e^{-p_1 l_1 t_{01}} \Rightarrow$$
$$\Rightarrow p_1 l_1 |\varepsilon_1(t_1)| - a_{43}E_2 \le (p_1 - a_{43}E_2) e^{-p_1 l_1 t_{01}}, \quad (\text{П.23})$$
$$|a_{43}\varepsilon_2(t) - v_1(t)| \le a_{43}\beta_2, \ t \ge t_{01} \Leftrightarrow$$
$$\Leftrightarrow (p_1 - a_{43}E_2) e^{-p_1 l_1 T/4} \le a_{43}\beta_2;$$

$$|\varepsilon_2(T)| \le \frac{X_2}{p_2 l_2 a_{43}} + \beta_2 + \frac{p_2 - X_2}{p_2 l_2 a_{43}} e^{-p_2 l_2 a_{43} t_{01}} \le \delta_1,$$
$$p_2 l_2 a_{43} (|\varepsilon_2(T)| - \beta_2) - X_2 \le (p_2 - X_2) e^{-p_2 l_2 a_{43} t_{01}}, \quad (\text{П.24})$$
$$|x_2(t) - v_2(t)| \le \delta_2, t \ge T \Leftrightarrow (p_2 - X_2) e^{-p_2 l_2 a_{43} T/4} \le \delta_2.$$

Из выражений (П.23), (П.24) следует, что ошибки наблюдения при $t \ge T$ сходятся в следующие окрестности нуля:

$$|\varepsilon_1(t)| \le \frac{a_{43}(E_2 + \beta_2)}{p_1 l_1}; \ |\varepsilon_2(t)| \le \frac{X_2 + \delta_2}{p_2 l_2 a_{43}} + \beta_2 \le \delta_1. \quad (\text{П.25})$$

Примем, например, $\beta_2 = \delta_1 / 2$. Из (П.23)–(П.25) заключаем, что заданная точность (19) обеспечивается, если при зафиксированных амплитудах (П.22) коэффициенты усиления удовлетворяют условиям

$$l_1 \ge \overline{l}_1 = \frac{4}{p_1 T} \ln \frac{2(p_1 - a_{43}E_2)}{a_{43}\delta_1};$$
$$l_2 \ge \overline{l}_2 = \frac{1}{p_2 a_{43}} \max \left\{ \frac{2(X_2 + \delta_2)}{\delta_1}; \ \frac{4}{T} \ln \frac{p_2 - X_2}{\delta_2} \right\}. \quad (\text{П.26})$$

Таким образом, существуют такие $\overline{p}_i > 0$ (П.22), $\overline{l}_i > 0$ (П.26), что при любых $p_i > \overline{p}_i$, $l_i \ge \overline{l}_i$, $i = 1, 2$, условия леммы (28) выполняются. ♦

ЛИТЕРАТУРА

1. *Spong, M., Hutchinson S., Vidyasagar M.* Robot Modeling and Control. – New York: Wiley, 2005. – 496 p.
2. *Angeles, J.* Fundamentals of Robotic Mechanical Systems: Theory, Methods and Algorithms. Third Edition. – New York: Springer, 2007. – 573 p.
3. *Голубев А.Е.* Стабилизация однозвенного манипулятора при неполном измерении состояния: обратная связь по угловой координате звена манипулятора // Научное издание МГТУ им. Н.Э. Баумана. Наука и образование. – 2012. – № 11. – С. 395–412. [*Golubev, A.E.* Single-Link Manipulator Output Feedback Control: Manipulator Link Angular Coordinate Feedback // Scientific Periodical of the Bauman MSTU. Science and Education. –2020. – No. 11. – P. 395–412. (In Russian)]
4. *Ананьевский И.М.* Управление механическими системами с неопределенными параметрами посредством малых сил // ПММ. 2010. – Т. 74, вып. 1. – С. 133–150. [*Anan'evskii, I.M.* Control of Mechanical Systems with Uncertain Parameters by Means of Small Forces // Journal of Applied Mathematics and Mechanics. – 2010. – No. 74. – P. 95–107.]
5. *Varghese E.S., Vincent A.K., Bagyaveereswaran V.* Optimal Control of Inverted Pendulum System Using PID Controller, LQR and MPC // IOP Conference Series Materials Science and Engineering. – 2017. – Vol. 263, no. 5. – 15 p.
6. *Utkin, V.I., Guldner, J., Shi, J.* Sliding Mode Control in Electromechanical Systems. – New York: CRC Press, 2009. – 485 p.
7. *Краснов Д.В., Антипов А.С.* Синтез двухконтурного наблюдателя в задаче управления однозвенным манипулятором в условиях неопределенности // Проблемы управления. – 2021. – № 4. – С. 27–39. [*Krasnov, D.V., Antipov, A.S.* Designing a Double-Loop Observer to Control a Single-Link Manipulator under Uncertainty // Control Sciences. –2021. – No. 4. – P. 23–33.]
8. *Feng, H., Qiao, W., Yin, C.,* et al. Identification and Compensation of Nonlinear Friction for a Electro-Hydraulic system // Mechanism and Machine Theory. – 2019. – Vol. 141. – P. 1–13.
9. *Пестерев А.В., Рапопорт Л.Б., Ткачев С.Б.* Каноническое представление нестационарной задачи путевой стабилизации // Известия РАН. Теория и системы управления. – 2015. – Т. 54, № 4. – С. 160–176. [*Pesterev, A.V., Rapoport, L.B., Tkachev, S.B.* Canonical Representation of a Nonstationary Path Following Problem // Journal of Computer and Systems Sciences International. – 2015. – Vol. 54, no. 4. – P. 656–670.]
10. *Уткин В.А., Уткин А.В.* Задача слежения в линейных системах с параметрическими неопределенностями при неустойчивой нулевой динамике // Автоматика и телемеханика. – 2014. – № 9. – С. 62–81. [*Utkin, V.A., Utkin, A.V.* Problem of Tracking in Linear Systems with Parametric Uncertainties under Unstable Zero Dynamics // Automation and Remote Control. – 2014. – Vol. 75, no. 9. – P. 1577–1592.]
11. *Краснова С.А., Сиротина Т.Г., Уткин В.А.* Структурный подход к робастному управлению // Автоматика и телемеханика. – 2011. – № 8. – С. 65–95. [*Krasnova, S.A., Sirotina, T.G., Utkin, V.A.* A Structural Approach to Robust Control // Automation and Remote Control. – 2011. – Vol. 72, no. 8. – P. 1639–1666.]
12. *Антипов А.С., Краснова С.А., Уткин В.А.* Синтез инвариантных нелинейных одноканальных систем слежения с сигмоидальными обратными связями с обеспечением заданной точности слежения // Автоматика и телемеханика. – 2022. – № 1. – С. 40–66. [*Antipov, A.S., Krasnova, S.A., Utkin, V.A.* Synthesis of Invariant Nonlinear Single-Channel Sigmoid Feedback Tracking Systems Ensuring Given Tracking Accuracy // Automation and Remote Control. – 2022. – Vol. 83, iss. 1. – P. 32–53.]
13. *Tsypkin Y., Polyak B.* High-Gain Robust Control // European J. Control. – 1999. – Vol. 5. – P. 3–9.
14. *Бусурин В.И., Йин Н.В., Жеглов М.А.* Анализ влияния линейного ускорения на характеристики кольцевого оптоэлектронного преобразователя угловой скорости и его компенсация // Автометрия. – 2019. – № 3. – С. 120–128. [*Busurin, V.I., Win, Y.N., Zheglov, M.A.* Effect of Linear Acceleration on the Characteristics of an Optoelectronic Ring Transducer of Angular Velocity and its Compensation // Optoelectronics, Instrumentation and Data Processing. – 2019. – Vol. 55, no. 3. – P. 309–316.]
15. *Краснова С.А.* Оценивание внешних возмущений на основе виртуальных динамических моделей // Управление

большими системами. – 2018. – Вып. 76. – С. 6–25. [*Krasnova, S.A*. Estimating the Derivatives of External Perturbations Based on Virtual Dynamic Models // Automation and Remote Control. – 2020. – Vol. 81, no, 5. – P. 897–910.]
16. *Кокунько Ю.Г., Краснов Д.В., Уткин А.В*. Два метода синтеза наблюдателей состояния и возмущений для беспилотного летательного аппарата // Проблемы управления. – 2020. – № 1. – С. 3–16. [*Kokunko, Yu.G., Krasnov, D.V., Utkin, A.V*. Two Methods for Synthesis of State and Disturbance Observers for an Unmanned Aerial Vehicle // Automation and Remote Control. – 2021. – Vol. 82, no. 8. – P. 1426–1441.]
17. *Spong, M*. Modeling and control of elastic joint robots // ASME Journal of Dynamic Systems, Measurement and Control. – 1987. – Vol. 109. – P. 310–319.

Статья представлена к публикации членом редколлегии Л.Б. Рапопортом.

Поступила в редакцию 05.05.2022,
после доработки 28.06.2022.
Принята к публикации 29.06.2022.

Антипов Алексей Семенович – канд. техн. наук, ✉ scholess18@mail.ru,

Краснов Дмитрий Валентинович – научн. сотрудник, ✉ dim93kr@mail.ru,

Институт проблем управления им. В.А. Трапезникова РАН, г. Москва.

TRACKING SYSTEM DESIGN FOR A SINGLE-LINK SENSORLESS MANIPULATOR UNDER NONSMOOTH DISTURBANCES

A.S. Antipov[1] and D.V. Krasnov[2]

Trapeznikov Institute of Control Sciences, Russian Academy of Sciences, Moscow, Russia

[1]✉ scholess18@mail.ru, [2]✉ dim93kr@mail.ru

Abstract. The controlled plant is a single-link manipulator having an elastic connection to a DC motor and operating under uncertainty and incomplete measurements. The problem is to design a discontinuous feedback control for tracking a given reference signal of the plant's angular position. The angular position and velocity of the manipulator are not available for measurements; the sensors are located only on the drive; parametric and exogenous disturbances affecting the manipulator are nonsmooth and cannot be directly suppressed by control applied to the actuator. Within the block approach, a decomposition procedure is developed to design a nonlinear local feedback control. This control ensures the controlled variable's invariance with respect to uncertainties unmatched with the control action. A state observer of reduced order is constructed to estimate the angular position and velocity of the manipulator required for feedback design. The state variables in this observer are estimated using the principle of restoring exogenous disturbances by their action on the controlled plant. With this principle, a dynamic model of exogenous disturbances is not needed. In both problems (control and observation), *S*-shaped bounded continuous local feedbacks are used (smooth (sigmoidal) and nonsmooth (piecewise linear) local feedbacks, respectively). These local feedbacks suppress bounded disturbances acting with them through the same channel. The algorithms developed below do not require real-time identification of parametric and exogenous disturbances. However, they stabilize the observation and tracking errors with some accuracy. The effectiveness of the dynamic feedback is validated by the results of numerical simulation.

Keywords: electromechanical system, tracking, invariance, block approach, state observer of reduced order, *S*-shaped functions.

Funding. This work was supported in part by the Russian Foundation for Basic Research, project no. 20-01-00363-A.

УДК 519.23 DOI: http://doi.org/10.25728/pu.2022.3.2

УПРАВЛЕНИЕ ТЕХНОГЕННОЙ БЕЗОПАСНОСТЬЮ НА ОСНОВЕ РИСК-ОРИЕНТИРОВАННОГО ПОДХОДА[1]

В.В. Москвичев, У.С. Постникова, О.В. Тасейко

Аннотация. Предложен алгоритм принятия управленческих решений на основе разработанной методики оценки рисков с применением методов многомерного статистического анализа. Предложенная методика позволяет получить расчетные значения приемлемого уровня риска, которые могут быть использованы при разработке нормативных документов. Алгоритм принятия решений интегрирован в информационную систему территориального управления рисками и безопасностью. В качестве объекта исследования выбраны промышленные агломерации Сибири, для которых были проанализированы основные виды техногенных опасностей. Для получения количественной оценки комплексного техногенного территориального риска использовались данные о числе техногенных опасных событий, чрезвычайных ситуациях и гибели людей из официальной базы данных МЧС России. В результате анализа факторов риска было определено, что основная техногенная нагрузка на рассматриваемых территориальных образованиях связана с пожаровзрывоопасными событиями. Решение обратной задачи позволило выявить необходимость выработки мер в отношении факторов риска для достижения его приемлемого уровня. Задача минимизации комплексного техногенного территориального риска связана с двухкритериальной задачей управления: необходимо минимизировать количество летальных исходов и сумму ущерба. Для решения указанной задачи по результатам применения рассматриваемого подхода комплексной оценки рисков предложены превентивные мероприятия по повышению безопасности территории.

Ключевые слова: социально-природно-техногенная система, территориальный риск, управление.

ВВЕДЕНИЕ

Устойчивое развитие территорий основывается на соблюдении баланса между экономическим ростом, безопасностью, социальной ответственностью и экологической обстановкой. Для осуществления эффективного управления территориальные образования целесообразно анализировать с точки зрения концепции социально-природно-техногенной (СПТ) системы [1–5], которая представляется единым комплексом взаимосвязанных элементов социо-эко-техносферы и характеризуется наличием различных групп рисков [2, 6, 7]. При наличии опасных природных процессов и росте числа сложных техногенных систем условия развития территориальных образований связаны с реализацией, выявлением и минимизацией рисков[2]. Требования по идентификации, оценке и управлению рисками закреплены в федеральных законах [8–10], а необходимость противостояния факторам, создающим прямую или косвенную возможность причинения ущерба национальным интересам отражена в указах Президента РФ [11, 12].

Для комплексного решения задач управления на разных уровнях и в различных областях создаются интеллектуальные системы, позволяющие интегрировать, хранить и обрабатывать значительные потоки информации. За последние годы в России и за рубежом создано множество программных комплексов и систем, позволяющих обрабатывать поступающую в ходе мониторинга информацию [13–28], однако такие системы имеют узкоспециа-

[1] Работа выполнена при поддержке гранта Президента РФ НШ-421.2022.4.

[2] Риск – количественная мера опасности, характеризующая одновременно процессы возникновения неблагоприятных явлений, событий или процессов в сложной социально-природно-техногенной системе и тяжесть их последствий [29].

лизированную направленность. В условиях быстрорастущих объемов и потоков информации комплексная оценка состояния СПТ систем представляет собой сложную научно-прикладную задачу, решить которую можно путем создания информационно-аналитических систем с реализацией возможности оценки рисков.

Наибольшую опасность[3] для жизни и здоровья человека представляют техногенные аварии и катастрофы, характеризующие такую компоненту СПТ системы, как техносфера. Нарушения технологических, управленческих и организационных процессов в промышленной и административной деятельности приводят к появлению широкого спектра техногенных опасных событий: аварии на транспорте, взрывы и крупные пожары, обрушения несущих конструкций, аварии с выбросом аварийно-химически опасных и радиационно-опасных веществ (АХОВ и РВ), разрушения магистральных трубопроводов, аварии на системах жизнеобеспечения (электроэнергетические системы, коммунальные системы и тепловые сети).

1. АНАЛИЗ И ПОСТАНОВКА ЗАДАЧИ

Предметом исследования является анализ состояния и оценка уровня техногенной нагрузки в крупных промышленных центрах Сибирского федерального округа – Красноярске, Новосибирске, Омске. Наибольшую опасность на рассматриваемых территориях представляют все виды пожаров, крупные ДТП и аварии на системах жизнеобеспечения.

Процессы урбанизации и рост промышленности в городах оказывают негативное влияние на экологическую и социальную безопасность, под их влиянием формируется ряд проблем, требующих постоянного внимания органов государственной власти и местного самоуправления:

– высокая концентрация источников потенциальной опасности на ограниченных территориях (предприятия ядерного цикла, военно-промышленный комплекс, трубопроводы, нефте- и газохранилища, гидроэлектростанции, химические и металлургические производства и др.);

– повышение вероятности возникновения аварийных ситуаций из-за высокой изношенности основных производственных фондов;

– факторы, связанные с низкой культурой безопасности.

На сегодняшний день одной из основных задач является повышение устойчивости развития и функционирования территориальных образований посредством эффективного управления. Для решения данной задачи предлагается использовать информационную систему территориального управления рисками и безопасностью (ИСТУ РБ) [1], которая предназначена для выявления территориальных рисков и минимизации их до научно обоснованных приемлемых уровней[4]. Система позволяет интегрировать накопленный опыт в области сетевого мониторинга состояния окружающей среды и техносферы, технологий анализа больших объемов информации, теории безопасности и риска, механизмов территориального управления и методов прогнозирования социально-экономического развития.

2. МЕТОДОЛОГИЯ ОЦЕНКИ КОМПЛЕКСНОГО ТЕХНОГЕННОГО ТЕРРИТОРИАЛЬНОГО РИСКА

Оценка комплексного техногенного территориального риска и предельного состояния объектов техносферы как элемента СПТ системы проводилась с помощью метода иерархического кластерного анализа [5, 31], который позволил разбить территории СФО на группы кластеров и выбрать для сравнения эталонную группу с последующим определением приемлемого уровня риска.

Иерархический кластерный анализ позволяет объединять в группы объекты, имеющие схожие характеристики. На первом шаге каждый объект (территориальное образование) выборки рассматривается как отдельный кластер. Процесс объединения кластеров происходит последовательно: объединяются наиболее близкие объекты. Классификация объектов проводится на основе сходства между ними, которое, в свою очередь, устанавливаются в зависимости от метрического расстояния между классифицируемыми объектами. Каждый объект описывается k признаками и представляется как точка в k-мерном пространстве, его сход-

[3] *Опасность* – объективно существующая возможность негативного воздействия на объект или процесс, в результате которого может быть причинен какой-либо ущерб, вред, ухудшающий состояние, придающий развитию нежелательные динамику или параметры (характер, темпы, формы и т.д.) [30].

[4] *Приемлемый уровень риска* – научно обоснованное количественное значение риска, которое может быть принято человеком, обществом и государством на данном отрезке времени [29].

ство с другими объектами будет определяться как соответствующее расстояние (метрика). Если матрица сходства первоначально имеет размерность $m \times m$, то полностью процесс кластеризации завершается за m–1 шагов, в итоге все объекты будут объединены в один кластер.

Метод оценки риска на основе кластерного анализа состоит из восьми этапов.

Этап 1 – формулировка проблемы. Стоит задача анализа техногенной безопасности городов СФО с численностью населения более 70 тыс. чел. согласно классификации муниципальных образований [32].

Этап 2. Выбираются количественные показатели, на основании которых проводится анализ (статистические данные официальной базы автоматизированной информационно-управляющей системы предупреждения и ликвидации чрезвычайных ситуаций (АИУС РСЧС) за период 1999–2020 гг.).

Этап 3. Исходные показатели представляются в виде количественных значений уязвимости[5], имеющих вероятностную природу, которые изменяются в диапазоне от нуля до единицы, что позволяет проводить деление на городов на группы кластеров:

$$\vartheta = \{p_a; p_f; p_e\}, \qquad (1)$$

где ϑ – уязвимость территории; p_a – вероятность возникновения опасного события; p_f – вероятность гибели при определенном опасном событии; p_e – вероятность возникновения ЧС.

Этап 4 связан с определением расстояния между объектами в условном многомерном пространстве. В качестве меры расстояния между двумя точками (характеризующего близость или подобие (схожесть) объектов), образованными координатными осями x и y, наиболее часто используются Евклидово расстояние, квадрат Евклидового расстояния, расстояние городских кварталов (Манхэттенское) и расстояние Чебышева. Для обоснования корректности деления на кластеры применяют разные меры расстояния. Однотипное распределение кластеров, полученное с использованием различных методов определения расстояния, подтверждает обоснованность выбранного метода классификации.

Этап 5. Выбирается метод кластеризации (способ вычисления расстояний между кластерами). Для объектов, имеющих «размытую» структуру с нечетко выраженными «сгущениями», наилучшим образом подходит метод Варда. В результате применения данного метода формируются небольшие по размеру и компактные кластеры. Данный метод кластеризации предполагает, что на первом шаге каждый кластер состоит из одного объекта. Далее объединяются два ближайших кластера. Для них определяются средние значения каждого признака и рассчитывается сумма квадратов отклонений V_k

$$V_k = \sum_{i=1}^{n_k}\sum_{j=1}^{p}\left(x_{ij} - \overline{x}_{jk}\right)^2,$$

где k – номер кластера; i – номер объекта; j – номер признака; p – количество признаков, характеризующих каждый объект; n_k – количество объектов в k-м кластере; $\overline{x}_{jk}$ – среднее значение j-го признака в k-м кластере; x_{ij} – значение j-го признака для i-го объекта.

В одну группу объединяются те кластеры, которые дают наименьший прирост общей суммы расстояний.

Этап 6 – определение количества кластеров иерархического дерева. В настоящей работе для определения числа кластеров использовался метод k-means. Он позволяет задавать количество кластеров (2, 3, 4 и т. д.) и последовательно проверять деление иерархического дерева.

Этап 7 связан с количественной оценкой техногенных рисков для каждой группы кластеров. Оценка комплексного техногенного территориального риска определяется по формуле (2) и учитывает весь перечень опасностей на рассматриваемой территории и размеры ущерба, связанные с данными опасными событиями:

$$R_c = \sum_{i=1}^{n} N_i\left(Q_i\right) P_i\left(Q_i\right) U_i\left(N_i, Q_i\right),$$

$$R_c \le [R], \qquad (2)$$

где R_c – комплексный техногенный территориальный риск (далее по тексту значение риска); n – число видов опасностей; $N_i\left(Q_i\right)$ – вероятность гибели людей (число погибших, деленное на численность населения) из-за реализации различных видов опасностей; $P_i\left(Q_i\right)$ – вероятность наступления опасного события на рассматриваемой терри-

[5] *Уязвимость* – системный параметр, характеризующий возможность нанесения описываемой системе повреждений любой природы [33], для территориальных образований уязвимость, характеризуется степенью возможных потерь, которые могут произойти при воздействии какого-либо негативного процесса или явления определенной величины [30].

тории в единицу времени; $U_i(N_i, Q_i)$ – материальный ущерб от источника опасностей и числа человеческих жертв, руб; $[R]$ – приемлемый уровень риска, руб./год.

Этап 8. Выбирается эталонная группа кластеров, имеющая наименьшее значение риска. Расчетный приемлемый уровень риска определялся как доверительный интервал по эталонной группе [5, 31]. Для крупных городов Сибири с численностью населения более 70 тыс. чел. расчетный приемлемый уровень риска соответствует интервальному значению [0; 2,1].

При выявлении высокого значения риска требуется дополнительный анализ данных. Для этого наилучшим образом подходит метод решения обратных задач, который позволяет определить доминирующие факторы, влияющие на значение риска, и выявить параметры, которые нуждаются в управлении. В оптимальных условиях в рамках концепции ненулевого риска суммарное значение комплексного техногенного территориального риска по различным видам техногенных событий не должно превышать приемлемого:

$$R_c = \sum_{i=1}^{n} R_{c_i} = R_{c_1} + R_{c_2} \ldots + R_{c_n}$$

$$R_{c_1} \ll [R];\ R_{c_2} \ll [R]; \ldots R_{c_n} \ll [R], \qquad (3)$$

где R_{c_i} – комплексный техногенный территориальный риск, возникающий из-за реализации событий определенного вида.

Определив доминирующие факторы, необходимо проводить мероприятия, направленные на минимизацию значения выявленного вида риска. Методы риск-менеджмента представляют собой направленные действия по снижению опасностей и их последствий. Минимизация значения риска в соответствии с формулой (2) связана с двухкритериальной задачей управления – необходимо минимизировать количество фатальных исходов $F(N_i)$ и ущерб $F(U_i)$:

$$\begin{cases} F_1(N_i) \to \min, \\ F_2(U_i) \to \min. \end{cases}$$

Накладывая на один из критериев ограничение C, получаем две задачи оптимизации:

$$\begin{cases} F_1(N_i) \to \min, \\ F_2(U_i) \le C_1, \end{cases} \quad \begin{cases} F_2(U_i) \to \min, \\ F_1(N_i) \le C_2. \end{cases} \qquad (4)$$

Быстрое реагирование на аварийную ситуацию, позволяющее снизить материальные потери, напрямую зависит от числа пожарно-спасательных формирований, а наличие достаточного количества медицинских учреждений позволяет уменьшить количество летальных исходов. Одной из задач, которую необходимо решить в целях разработки мер по повышению защищенности, является количественная оценка обеспеченности территориального образования необходимым числом медицинских учреждений и пожарно-спасательных формирований $Z_{(\tau)}$:

$$Z_{(\tau)} = \left(\frac{N^{\Phi}_{\text{ПЧ}} + N^{\Phi}_{\text{МУ}}}{N^{\text{Н}}_{\text{ПЧ}} + N^{\text{Н}}_{\text{МУ}}} \right) \cdot 100 \ge 100\ \%, \qquad (5)$$

где $N^{\Phi}_{\text{ПЧ}}$ – фактическое количество пожарно-спасательных формирований на рассматриваемой территории; $N^{\text{Н}}_{\text{ПЧ}}$ – нормативное количество пожарно-спасательных формирований на рассматриваемой территории; $N^{\Phi}_{\text{МУ}}$ – фактическое количество медицинских учреждений на рассматриваемой территории; $N^{\text{Н}}_{\text{МУ}}$ – нормативное количество медицинских учреждений на рассматриваемой территории.

Территория является защищенной, когда фактические и нормативные значения количества медицинских учреждений и пожарно-спасательных формирований равны или фактическое количество больше нормативного, при таких условиях $Z_{(\tau)}$ принимается ≥ 100 %. Расчет нормативного значения пожарно-спасательных формирований основывается на определении нормативной численности личного состава подразделений пожарной охраны, привлекаемых к спасательным работам, и типовой штатной структуре:

$$N^{\text{Н}}_{\text{ПЧ}} = \frac{N_{\text{нас}}}{N_{\text{ПФ}} N_{\text{шт}}}, \qquad (6)$$

где $N_{\text{нас}}$ – численность населения на рассматриваемой территории; $N_{\text{ПФ}}$ – численность населения, приходящегося на одного сотрудника пожарно-спасательного формирования (ПФ); $N_{\text{шт}}$ – типовое штатное количество спасателей в ПФ.

Для определения численности населения, приходящегося на одного сотрудника ПФ, применяется формула [34]

$$N_{\text{ПФ}} = 0,036757 \cdot P\left(0,036648 + 98,781 \cdot P^{-0,44823}\right)^2, \qquad (7)$$

где P – плотность населения на рассматриваемой территории.

Определение нормативного количества медицинских учреждений основывается на нормативном документе Министерства здравоохранения [35].

Таким образом, кластеризация территориальных образований по показателям техногенной опасности (формула (1)), кластерная оценка рисков (формулы (2) и (3)) и защищенности (формулы (5)–(7)) дают возможность проведения комплексного анализа техногенной безопасности территориальных образований с позиции риск-ориентированного подхода [31].

3. ПРОГРАММНО-ТЕХНИЧЕСКАЯ РЕАЛИЗАЦИЯ

Определение значения комплексного техногенного территориального риска является одной из основных функций информационной системы территориального управления рисками и безопасностью (ИСТУ РБ). Общая блок-схема ИСТУ РБ построена на базе Docker-контейнеров, которые представляют собой систему управления контейнерами (модулями), где каждый отдельный модуль размещен как независимый компонент-программа на расчетном сервере, имеет свой порт доступа и набор библиотек. Он позволяет «упаковать» приложение или веб-сайт со всем его окружением и зависимостями в контейнер, которым в дальнейшем можно легко и просто управлять: переносить на другой сервер, масштабировать, обновлять. Графический интерфейс системы разработан на базе библиотек ReactJS + Redux. Система использует комплексную кризисную базу данных (на базе СУБД PostgreSQL) [36].

В работе предложен алгоритм поддержки принятия управленческих решений, встроенный в информационную систему территориального управления рисками и безопасностью (рис. 1) [1, 31].

Рис. 1. Алгоритм принятия управленческих решений на основе риск-ориентированного подхода

В ИСТУ РБ поступают статистические данные, характеризующие СПТ систему (территорию). ИСТУ РБ состоит из двух подсистем:

- Информационная подсистема «Мониторинг». В данной подсистеме происходит сбор и систематизация информационных потоков систем мониторинга с последующей обработкой, анализом и организацией хранения исходных и обработанных данных.
- Информационная подсистема «Риск-анализ». Данная подсистема имеет три блока: кризисные базы данных СПТ системы; картографическая база геоинформационной системы и блок, в который входят модели и вычислительные технологии анализа базовых рисков. Решается задача количественной оценки риска, происходит идентификация риска (выявление, классификация, оценка и определение приемлемого уровня).

После прохождения информации через указанные подсистемы данные обрабатываются до получения количественных значений риска, рассчитываемых на основе представленного выше методического подхода.

В зависимости от полученного расчетного значения риска формируется заключение, в котором прописываются мероприятия по управлению территорией и планированию. В случае, если значение риска соответствует приемлемому уровню, формируется заключение о том, что дополнительных мероприятий по уменьшению риска на рассматриваемой территории не требуется. При выявлении высокого уровня риска проводится дополнительный анализ данных для выявления доминирующего фактора риска.

На основе полученной информации формируется промежуточный продукт – заключение о мероприятиях, направленных на минимизацию значения риска для конкретного фактора путем повышения защищенности, снижения техногенной опасности и повышения устойчивости защищаемых объектов (табл. 1), а также осуществляется контроль уровня риска.

Заключение направляется лицу, принимающему решение, которое анализирует полученную информацию и согласовывает мероприятия в рамках имеющегося бюджета. Результатом работы данной системы будут нормативные документы (приказы или постановления), в которых прописываются методы управления рисками. В зависимости от вида опасного фактора (техногенного события) и возможностей финансирования превентивные мероприятия будут различны (табл. 2).

Территориальные образования являются динамическими системами, поэтому с течением времени расчетное значение риска будет изменяться. Таким образом, для эффективного управления необходимо ежегодно проводить корректировку результатов.

Таблица 1

Основные виды превентивных мероприятий для повышения техногенной безопасности территории

Цели превентивных мероприятий	Технологические решения, превентивные мероприятия
Снижение вероятности реализации опасных событий	– ремонт, реконструкция объектов техносферы; – строительство всех видов объектов по новым технологиям с учетом требований безопасности; – непрерывный мониторинг негативных процессов; – автоматизация процессов (уменьшение роли человеческого фактора)
Повышение устойчивости защищаемых объектов	– зонирование территорий, прилегающих к объектам техносферы; – развитие систем здравоохранения и охраны труда; – инженерные решения по повышению устойчивости городской среды; – развитие систем оповещения и информирования; – страхование имущества; – контроль, надзор, профилактика, обучение населения
Повышение защищенности	– создание и модернизация аварийно-спасательных формирований, служб экстренного реагирования; – создание, пополнение, замена резервов на случай ЧС; – увеличение финансовых резервов; – совершенствование межведомственного взаимодействия, работа с волонтерами

Таблица 2

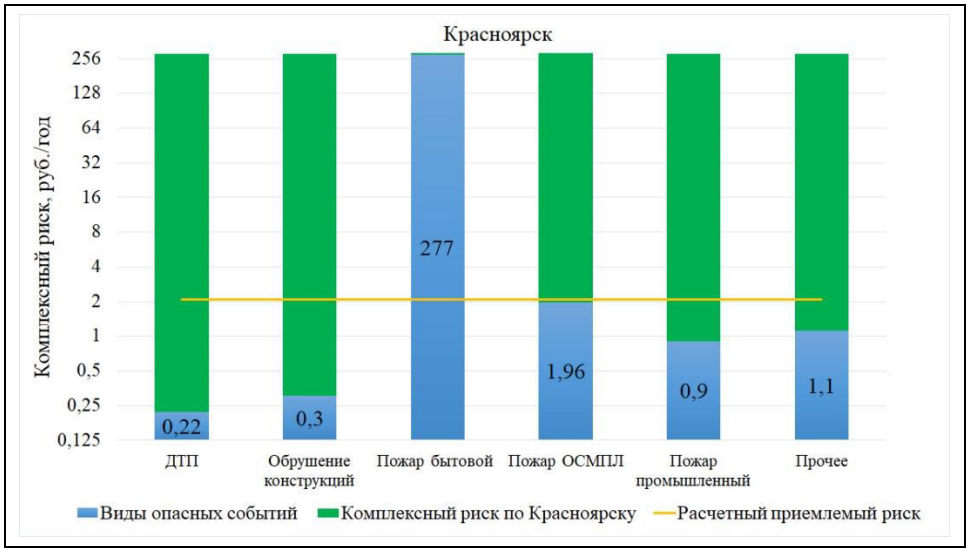
Мероприятия по предупреждению или снижению последствий основных опасных техногенных событий

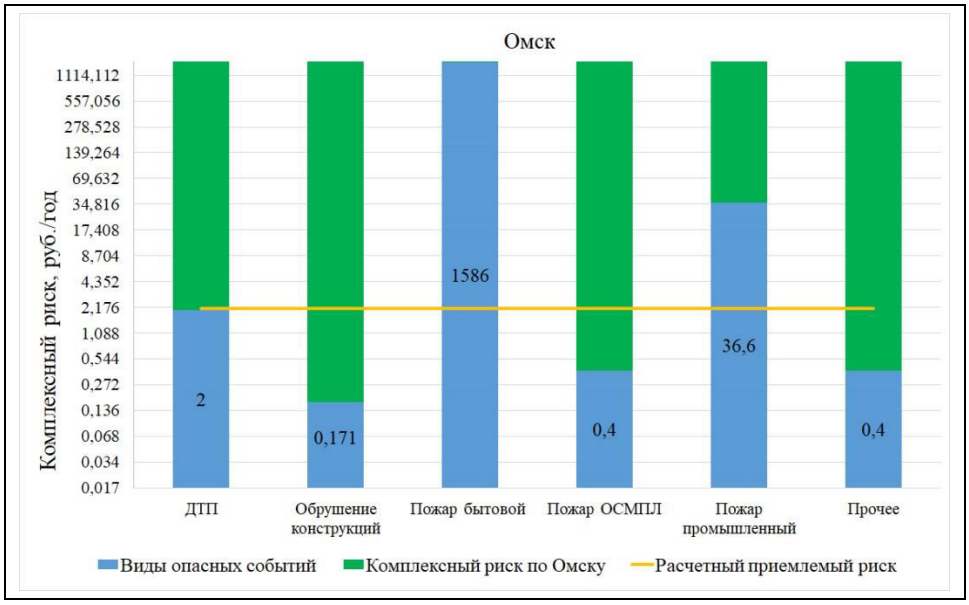
Вид опасного события	Превентивные мероприятия		
	Снижение вероятности возникновения	Снижение масштабов ЧС	Действия при отсутствии ограничений ресурсов
Аварии на потенциально опасных объектах	Повышение «чувствительности» АСУ ТП к идентификации аварий и инцидентов. Проверки Ростехнадзора	Повышение готовности объектовых формирований. Совершенствование планов действий по ликвидации ЧС	Переход на альтернативные технологии. Снижение объемов (полный отказ от использования) опасных веществ и материалов
Пожары промышленные	Усиление пожарного надзора. Контроль знания правил пожарной безопасности	Установка современного противопожарного оборудования. Повышение готовности объектовых формирований. Совершенствование планов действий по ликвидации ЧС	Переход на альтернативные технологии производства и строительства
Пожары бытовые и на объектах массового пребывания людей	Усиление пожарного надзора. Обучение населения правилам пожарной безопасности	Увеличение количества и статуса противопожарных формирований. Создание ресурсов для тушения пожаров	Переход на альтернативные технологии строительства. Отказ от печного отопления
Аварии в сфере ЖКХ	Увеличение объемов и качества капитальных ремонтов	Повышение готовности формирований. Совершенствование планов действий по ликвидации ЧС	Переход на альтернативные технологии и материалы при замене коммуникаций
Автотранспортные аварии	Законодательное регулирование вопросов безопасности	Обучение навыкам оказания первой помощи. Повышение готовности спасательных формирований	Строительство и реконструкция дорог по современным стандартам (четыре полосы, развязки)

4. ПРАКТИЧЕСКИЕ РЕЗУЛЬТАТЫ

На основе предложенной методологии было проанализировано 31 территориальное образование СФО с численностью более 70 тыс. чел. Выявлено, что в Красноярске, Новосибирске и Омске значение комплексного техногенного территориального риска в сотни раз превышает предельно-допустимый уровень. На рис. 2 представлен график распределения значений комплексного техногенного территориального риска по каждому виду опасных событий для рассматриваемых городов Сибири.

Основная техногенная нагрузка в городских формированиях приходится на различные пожаро-взрывоопасные ситуации и крупные дорожно-транспортные происшествия. Наименьшее значение риска получено для показателей «Обрушение конструкций» и «Прочее» (куда входят аварии на воздушном, ж/д и речном транспорте, аварии на промышленных объектах, аварии с выбросом РВ / ХОВ, взрывы бытовые и промышленные, аварии на системах жизнеобеспечения).





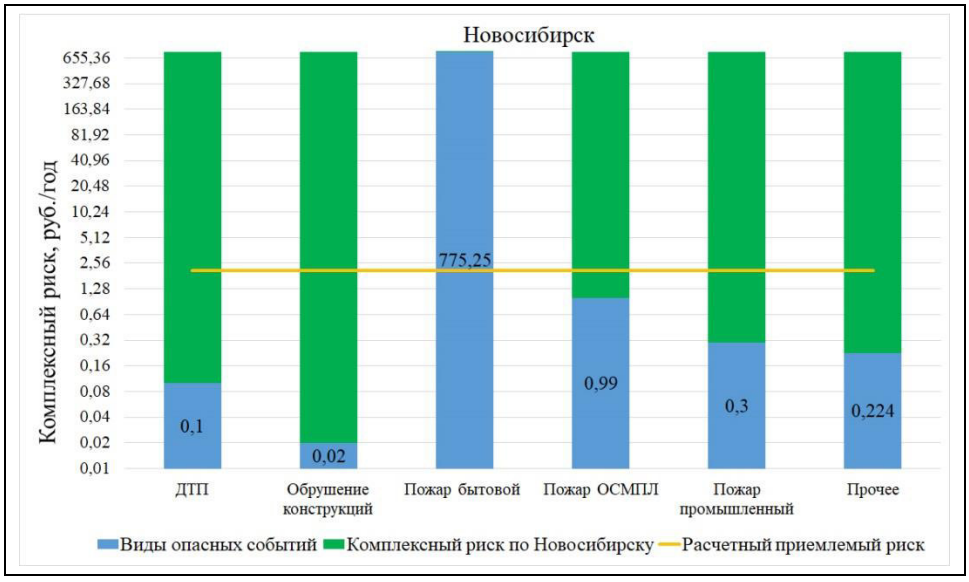


Рис. 2. Распределение значений комплексного техногенного территориального риска по видам опасностей для крупнейших городов Сибири

Для трех городов методом решения обратных задач были определены доминирующие виды опасных событий. Для г. Красноярска и г. Новосибирска основная опасность связана с пожарами (бытовые и на объектах с массовым пребыванием людей), для г. Омска – пожары (бытовые и на объектах с массовым пребыванием людей) и крупные ДТП. Основная проблема, характерная для всех рассматриваемых городов, требующая минимизации и управления, связана с бытовыми пожарами. На рис. 3 представлены графики изменения комплексного территориального техногенного риска при управлении двумя показателями – ущерб и количество смертельных исходов (уравнения (4) и (5)).

Снижение значения одного из показателей – количества летальных исходов или суммы ущерба – позволяет уменьшить значение риска, поэтому основные рекомендации по минимизации риска должны быть направлены на повышение культуры и общего уровня безопасности и, как следствие, снижение количества летальных исходов, а также на страхование имущества, которое позволит компенсировать ущерб в случае наступления опасного техногенного события. Для достижения приемлемого уровня риска на рассматриваемых территориях необходимо уменьшение ущерба или числа погибших в для г. Новосибирска 8 раз, для г. Красноярска в 6 раз, для г. Омска в 10 раз.

Для поддержания необходимого уровня устойчивости к негативному воздействию проведен расчет количественных значений защищенности по формулам (5)–(7) и выполнен анализ количества спасательных формирований и медицинских учреждений для рассматриваемых городов (табл. 3).

Самая низкая защищенность выявлена в г. Новосибирске, где наблюдается недостаток пожарно-спасательных формирований и медицинских учреждений. Таким образом, для своевременного

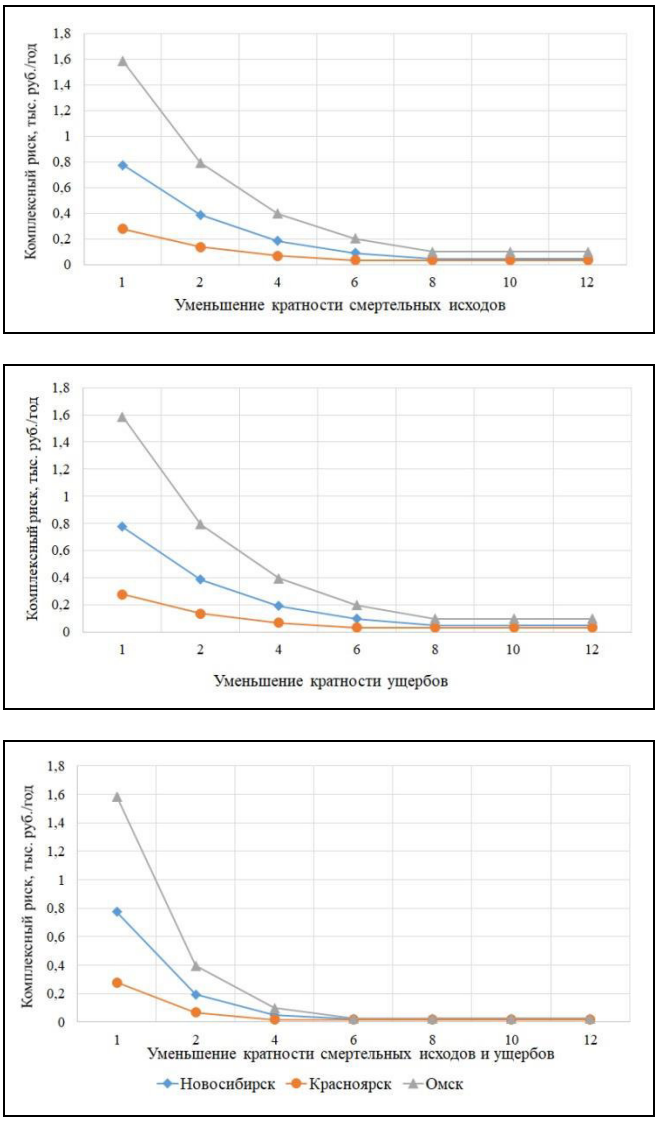


Рис. 3. Графики изменения риска при снижении размеров ущерба и смертности населения

предупреждения аварий и катастроф и минимизации последствий от реализованных событий необходимо увеличивать защищенность территории путем увеличения числа аварийно-спасательных формирований и служб экстренного реагирования, а также их модернизации.

Таблица 3

Количественные значения показателя защищенности и данные для его расчета

Наименование территории	Защищенность, %	Фактическое кол-во ПФ	Нормативное кол-во ПФ	Фактическое кол-во мед. уч.	Нормативное кол-во мед. уч.
г. Новосибирск	84,5	25	30	68	80
г. Омск	135	22	22	85	57
г. Красноярск	98,5	10	18	55	48

5. ОБСУЖДЕНИЕ

Основная цель территориального управления сводится к достижению приемлемого уровня риска. Однако анализ нормативно-технических документов по оценке техногенного территориального риска выявил ряд методических проблем и противоречий в их применении вследствие различного правового статуса и несогласованности норм. Ключевая проблема действующей нормативно-технической базы в области безопасности и оценки рисков заключается в том, что приемлемые уровни рисков не являются научно обоснованными. Математический аппарат оценки рисков требует доработок, учитываются только чрезвычайные ситуации, но для анализа безопасности территориального образования необходимо анализировать все происшествия, которые возникают на территории и в дальнейшем могут привести к крупным авариям и катастрофам. Разработанная методика оценки рисков, основанная на методах многомерного статистического анализа, позволяет снизить остроту обозначенных проблем и противоречий.

Обеспечение территориальной техногенной безопасности возложено на территориальные Агентства по делам ГО и ЧС субъектов РФ и территориальные управления МЧС России. Для эффективного управления целесообразно использовать информационные системы поддержки принятия решений, которые должны объединять и анализировать данные мониторинга, имеющиеся в распоряжении различных ведомств, и оценивать риски по основным сферам жизнедеятельности. Управление техногенным риском включает в себя разработку и реализацию программ деятельности по предотвращению опасных событий, снижению их возможных последствий, обеспечение мониторинга и повышение эффективности затрат, направленных на снижение значений рисков до приемлемых уровней. Идентификация основных факторов высокого техногенного риска с использованием соответствующей информационной системы территориального управления рисками и безопасностью позволяет конкретизировать эту работу и предупредительные мероприятия.

Оценка эффективности и экономической целесообразности управленческих решений по минимизации рисков является отдельной практической задачей, для решения которой необходима исходная информация о стоимости реконструкции конкретных технических объектов, развития системы мониторинга объектов, систем здравоохранения и охраны труда, создании и модернизации аварийно-спасательных формирований и т. д. Реализация этих мероприятий находится в ведении различных министерств и ведомств РФ, органов исполнительной власти регионов и производственных структур.

ЗАКЛЮЧЕНИЕ

При анализе полученных значений комплексного техногенного территориального риска для крупных промышленных центров СФО были выявлены причины, которые в наибольшей степени влияют на уровень риска. Основными из них являются пожары на объектах промышленного и социального значения, аварии в жилищно-коммуналь-ной сфере (теплосети, электросети, водоснабжение и пр.) и аварии на транспорте. Наибольшее число погибших наблюдается при возникновении бытовых пожаров. Наибольший материальный ущерб обусловлен промышленными пожарами, что связано с большим числом пострадавших, экономическими потерями при ликвидации ЧС и аварийно-восстановительными работами.

Преимущество разработанной методики оценки рисков заключается в возможности получения расчетного приемлемого уровня риска, который может быть использован при разработке нормативных документов. Существующие в настоящее время численные значения приемлемых уровней рисков относятся к индивидуальным рискам, в то время как для нормирования комплексного риска применяются преимущественно качественные показатели (балльные оценки). Оценка защищенности территории также выполняется с помощью качественных методов, в то время как предложенная методика позволила впервые получить численные значения.

Оценка комплексной безопасности территориальных образований должна базироваться на разработке и применении критериев и методов анализа рисков. С ростом антропогенной нагрузки, использования технологий, угрожающих воспроизводству природных ресурсов, ростом угроз для жизни и здоровья граждан необходимы механизмы эффективного территориального управления, базирующиеся на использовании системы поддержки принятия решений в составе ИСТУ РБ, в основе которой лежит комплексная оценка техногенных территориальных рисков.

ЛИТЕРАТУРА

1. *Москвичев В.В., Бычков И.В., Потапов В.П.* и др. Информационная система территориального управления рисками развития и безопасностью // Вестник Российской академии наук. – 2017. – № 8. – С. 696–705. [*Moskvichev, V.V., By-*

chkov, I.V., Potapov, V.P., et al. Information System for Territorial Risk and Safety Management Development// Herald of the Russian Academy of Sciences. – 2017. – No. 8. – P. 696–705. (In Russian)].

2. *Махутов Н.А., Кузык Б.Н., Абросимов Н.В*. и др Научные основы прогнозирования и прогнозные показатели социально-экономического и научно-технического развития России до 2030 года с использованием критериев стратегических рисков. – М.: ИНЭС, 2011. – 136 с. [*Makhutov, N.A., Kuzyk, B.N., Abrosimov, N.V.,* et al. Scientific Bases of Forecasting and Forecast Indicators of Socio-Economic and Scientific-Technical Development of Russia until 2030 Using Criteria of Strategic Risks. – Moscow: INES, 2011. – 136 s. (In Russian)]
3. *Махутов Н.А, Кузык Б.Н.*, *Абросимов Н.В.* Системные стратегические риски и приоритеты прогнозного социально-экономического и научно-технологического развития России до 2030 года. – М: ИНЭС, 2012. 78 с. [*Makhutov, N.A., Kuzyk, B.N.,Abrosimov, N.V.* Systemic Strategic Risks and Priorities of the Forecast Socio-Economic, Scientific and Technological Development of Russia until 2030. – Moscow: INES, 2012. – 78 s. (In Russian)]
4. *Москвичев В.В., Тасейко О.В., Иванова У.С., Черных Д.А.* Базовые региональные риски развития территорий Сибирского федерального округа // Вычислительные технологии. – 2018. – Т. 23. – № 4. – С. 95–109. [*Moskvichev, V.V., Taseiko, O.V., Ivanova, U.S., Chernykh, D.A.* Basic Regional Risks of the Development of the Territories of the Siberian Federal District // Computational Technologies. – 2018. – Vol. 23, no. 4. – P. 95–109. (In Russian)]
5. *Moskvichev V.V., Postnikova U.S., Taseiko O.V.* Cluster Analysis and Individual Anthropogenic Risk // CEUR Workshop Proceedings. SDM 2021 – Proceedings of the All-Russian Conference with International Participation «Spatial Data Processing for Monitoring of Natural and Anthropogenic Processes»». – 2021. – С. 526–532.
6. *Управление* риском: Риск. Устойчивое развитие. Синергетика / *Владимиров В.А., Воробьев Ю.Л., Салов С.С.* и др. – М.: Федеральное государственное унитарное предприятие «Академический научно-издательский, производственно-полиграфический и книгораспространительский центр «Наука», 2000. – 431 с. – (Кибернетика: неограниченные возможности и возможные ограничения). [*Risk* management: Risk. Sustainable Development. Synergetics / *Vladimirov, V.A., Vorobyev, Yu.L. Salov, S.S.,* et al. – Moscow : Federal State Unitary Enterprise «Academic Scientific Publishing, Production, Printing and Book Distribution Center «Nauka», 2000. – 431 p. – (Cybernetics: unlimited possibilities and possible limitations) (In Russian)]
7. *Кононов Д.А.* Исследование безопасности систем управленияна основе анализа их системных параметров // Проблемы управления безопасностью сложных систем: Материалы XXVIII международной конференции, Москва, 16 декабря 2020 года / Под общей редакцией А.О. Калашникова, В.В. Кульбы. – Москва: Институт проблем управления им. В.А. Трапезникова РАН, 2020. – С. 102–108. [*Kononov, D.A.* Safety Research of Control Systems Based on the Analysis of Their System Parameters // Problems of security management of complex systems : Proceedings of the XXVIII International Conference, Moscow, December 16, 2020 / Eds. A.O. Kalashnikov, V.V. Kulba. – Moscow: V.A. Trapeznikov Institute of Management Problems of the Russian Academy of Sciences, 2020. – pp. 102–108. (In Russian)]
8. *Федеральный* закон «О техническом регулировании» от 27.12.2002 N 184-ФЗ [Электронный ресурс]. – Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_40241/ [*Federal* Law «On Technical Regulation» dated December 27, 2002 N 184-FZ (In Russian)]
9. *Федеральный* закон «О безопасности» от 28.12.2010 N 390-ФЗ [Электронный ресурс]. – Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_108546/ [Federal Law «On Safety» dated December 28, 2010 N 390-FZ. (In Russian)]
10. *Федеральный* закон «О защите населения и территорий от чрезвычайных ситуаций природного и техногенного характера» от 21.12.1994 N 68-ФЗ [Электронный ресурс]. – Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_5295/ [Federal Law «On the Protection of the Population and Territories from Natural and Man-Made Emergencies» dated December 21, 1994 N 68-FZ. (In Russian)]
11. *Указ* Президента Российской Федерации от 02.07.2021 № 400 «О Стратегии национальной безопасности Российской Федерации» [Электронный ресурс]. – Режим доступа: http://publication.pravo.gov.ru/Document/View/0001202107030001 [*Decree* of the President of the Russian Federation of February 7, 2021 No. 400 «On the National Safety Strategy of the Russian Federation» (In Russian)]
12. *Указ* Президента РФ от 19.04.2017 N 176 «О Стратегии экологической безопасности Российской Федерации на период до 2025 года» [Электронный ресурс]. – Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_215668/ [*Decree* of the President of the Russian Federation of April 19, 2017 N 176 «On the Strategy for Environmental Safety of the Russian Federation for the period up to 2025» (In Russian)]
13. *Большаков Б.Е., Шевенина Е.В.* Методологические принципы бездефектного управления безопасностью и развитием территориальных и производственных систем // Науковедение. – 2016. – Т. 8. – № 2. – С. 1–18. [*Bolshakov, B.E., Shevenina, E.V.* Methodological Principles of defect-free Management of Safety and Development of Territorial and Production Systems // Naukovedenie. – 2016. – Vol. 8, no. 2. – P. 1–18. (In Russian)]
14. *Состояние* окружающей среды: Постановление Правительства РФ № 477 от 6 июня 2013 г. «Об осуществлении государственного мониторинга состояния и загрязнения окружающей среды» [Электронный ресурс]. – Режим доступа: http://www.meteorf.ru/upload/iblock/30b/PPRF-477-20130606.pdf [State of the Environment: Decree of the Government of the Russian Federation No. 477 of June 6, 2013 «On the Implementation of State Monitoring of the State and Pollution of the Environment» (In Russian)]
15. *Приказ* Федерального агентства по недропользованию «Об утверждении Положения о функциональной подсистеме мониторинга состояния недр единой государственной системы предупреждения и ликвидации чрезвычайных ситуаций» от 24.11.2005 № 1197: [Электронный ресурс]. – Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_224058/ [Order of the Federal Agency for Subsoil Use «On approval of the Regulations on the Functional Subsystem for Monitoring the State of the Subsoil of the Unified State System for the Prevention and Liquidation of Emergency Situations» dated 11/24/2005 No. 1197: (In Russian)]
16. *Немтинов В.А*. Информационные технологии принятия решений по обеспечению экологической безопасности

промышленных объектов // Вестник ТГТУ. – 2008. – № 14. – С. 13–19. [*Nemtinov, V.A.* Information Technologies for Decision-Making in Maintenance of Ecological Safety of Industrial Enterprises // Vestnik TGTU. – 2008. – No. 14. – P. 13–19. (In Russian)]

17. *Neirotti, P.* Current Trends in Smart City Initiatives: Some Stylized Facts // Cities 38. – 2014. – P. 25–36.
18. *Fraker, H.* The Hidden Potential of Sustainable Neighborhoods: Lessons for Low-Carbon Communities. – Washington, DC: Island Press, 2013. 248 p.
19. *La Greca,P., Barbarossa, L., Ignaccolo, M.,* et al. The Density Dilemma. A Proposal for Introducing Smart Growth Principles in a Sprawling Settlement within Catania Metropolitan Area // Cities, 28. – 2011. – Vol. 6. – P. 527–535.
20. *Барановский В.Ю.* Интеллектуально-информационные системы как источник повышения рационализации процедуры управления промышленного предприятия в условиях неопределенности // Евразийский союз ученых. – 2021. – № 4-3 (85). – С. 17–20. [*Baranovskiy, V.Yu.* Intellectual Information Systems as a Source of Increasing the Rationalization of the Management Procedure of an Industrial Enterprise under Uncertainty // Eurasian Union of Scientists. – 2021. – No. 4-3 (85). – P. 17–20. (In Russian)]
21. *Кретова А.В.* Экономические информационные системы как основа повышения качества управления организацией // Менеджер. – 2020. – № 3 (93). – С. 84–90. [*Kretova, A.V.* Economic Information Systems as a Basis for Improving the Quality of Organization Management // Менеджер. – 2020. – No. 3 (93). – P. 84–90. (In Russian)]
22. *Вожаков А.В., Столбов В.Ю., Федосеев С.А.* Интеллектуальные информационные системы управления предприятием: модели и практики: – М: Университетская книга. – 2021. – 304 с. [*Vozhakov, A.V., Stolbov, V.Yu., Fedoseev, S.A.* Intelligent Information Systems of Enterprise Management: Models and Practices: – M: University Book. – 2021. – 304 s. (In Russian)]
23. *Киселев В.М., Данько Т.П., Афанасьев М.А.* Географические информационные системы для обеспечения экономической безопасности страны во время эпидемиологических кризисов // Инновации и инвестиции. – 2020. – № 10. – С. 249–253. [*Kiselev, V.M., Danko, T.P., Afanasyev, M.A.* Geographic Information Systems to Ensure the Economic Security of the Country During Epidemiological Crises. – 2020. – No. 10. – P. 249–253. (In Russian)]
24. *Oliveira da Silva, A., Souza Fernandes, R.A.* Smart Governance Based on Multipurpose Territorial Cadastre and Geographic Information System: An Analysis of Geoinformation, Transparency and Collaborative Participation for Brazilian Capitals // Land Use Policy, – 2020, – Vol. 97. 104752.
25. *Béjar, R., Latre, M.Á., Lopez-Pellicer, F.J.,* et al. SDI-Based Business Processes: A Territorial Analysis Web Information System in Spain // Computers & Geosciences. – 2012. – Vol. 46. – P. 66–72.
26. *Lee, B.S., Alexander, M.E., Hawkes, B.C.,* et al. Information Systems in Support of Wildland Fire Management Decision Making in Canada // Computers and Electronics in Agriculture. – 2002. – Vol. 37. – P. 185–198.
27. *Green, B., Chen, Y.* The Principles and Limits of Algorithm-in-the-Loop Decision Making // Proceedings of the ACM on Human-Computer Interaction . – 2019. – Vol. 3,– no. CSCW. – P. 1–24.
28. *Alkhatib, A., Bernstein, M.* Street-Level Algorithms: A theory at the Gaps Between Policy and Decisions // Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems. – 2019. – P. 1–13.
29. *Махутов Н.А.* Научные основы анализа стратегических приоритетов и рисков развития России: Информационно-аналитическая справка по проблемам стратегического прогнозирования, планирования и программирования в целях устойчивого социально-экономического развития и обеспечения национальной безопасности – Москва : МГОФ «Знание», 2018. – 96 с. [*Makhutov, N.A.* Scientific Basis for the Analysis of Strategic Priorities and Risks of Russia's Development: Information and Analytical Reference on the Problems of Strategic Forecasting, Planning and Programming for Sustainable Socio-Economic Development and Ensuring National Security – Moscow: MGOF «Znanie», 2018. – 96 p. (In Russian)]
30. *Махутов Н.А., Урсул А.Д., Проценко А.Н.* и др. Безопасность России. Правовые, социально-экономические и научно- технические аспекты. Словарь терминов и определений. – М.: МГФ «Знание», 1999. – 368 с. [*Makhutov, N.A., Ursul, A.D., Protsenko, A.N.,* et al. Security of Russia. Legal, Socio-Economic and Scientific and Technical Aspects. Dictionary of Terms and Definitions. - M.: MGF «Znanie», 1999. – 368 p. (In Russian)]
31. *Taseiko, O.V., Postnikovaa, U.S., Georgieva, M.,* et al. Methods for Analyzing Heterogeneous Data in the Tasks of Assessing Territorial Risks // CEUR Workshop Proceedings. – 2021. – 2930. – P. 124–128.
32. *Градостроительный* кодекс РФ от 7 мая 1998 г. N 73-ФЗ. Принят Государственной Думой 8 апреля 1998 г. 46 с. [*Town-planning* Code of the Russian Federation of May 7, 1998 N 73-FZ. Adopted by the State Duma on April 8, 1998. 46 p. (In Russian)]
33. *Кононов Д.А., Пономарев Н.О., Пономарев Р.О., Барбашев М.П.* Региональные системы:моделирование кризисных явлений и уязвимость // Управление развитием крупномасштабных систем MLSD'2015: Материалы Восьмой международной конференции: В 2 томах. / Под общей редакцией С.Н. Васильева, А.Д. Цвиркуна. – Москва: Институт проблем управления им. В.А. Трапезникова РАН, 2015. – С. 147–149. [*Kononov, D.A., Ponomarev, N.O., Ponomarev, R.O. M. P. Barbashev, M.P.* Regional Systems: Modeling of Crisis Phenomena and Vulnerability // Management of Large-Scale Syatem Development MLSD'2015 : Proceedings of the Eighth International Conference: In 2 volumes. / Eds. S.N. Vasiliev, A.D. Tsvirkun. – Moscow: V.A. Trapeznikov Institute of Control Sciences of the Russian Academy of Sciences, 2015. – p. 147–149. (In Russian)]
34. *Организационно-методические* рекомендации по определению численности противопожарной службы субъекта Российской Федерации и ее технической оснащенности. [Электронный ресурс]. – Режим доступа https://www.mchs.gov.ru/dokumenty/metodicheskie-materialy/metodicheskie-rekomendacii/prochee/organizacionno-metodicheskie-rekomendacii-po-opredeleniyu-chislennosti-protivopozharnoy-sluzhby-subekta-rossiyskoy-federacii-i-ee-tehnicheskoy-osnashchennosti. [*Organizational* and Methodological Recommendations for Determining the Size of the Fire Service of the Subject of the Russian Federation and Its Technical Equipment. (In Russian)]
35. *Приказ* Министерства здравоохранения Российской Федерации от 27.02.2016 № 132н «О Требованиях к размещению медицинских организаций государственной

системы здравоохранения и муниципальной системы здравоохранения исходя из потребностей населения» (Зарегистрирован 22.03.2016 № 41485). 8 с. [*Order* of the Ministry of Health of the Russian Federation No. 132n dated 27.02.2016 «On the Requirements for the Placement of Medical Organizations of the State Health System and Municipal Health System Based on the Needs of the Population» (Registered 22.03.2016 No. 41485). – 8 p. (In Russian)]

36. *Попов С.Е., Потапов В.П., Замараев Р.Ю.* и др. Информационно-вычислительная система «Риски»: № 2020660032: заявл. 04.09.2020: опубл. 17.09.2020. Свидетельство о гос. регистрации программы для ЭВМ № 2020661041 РФ. [*Popov, S.E., Potapov, V.P., Zamaraev, R.Yu.,* et al. Information and computing system «Risks»: No. 2020660032: application 04.09.2020: publ. 17.09.2020. Sertificate of state registration of the computer program No. 2020661041 Russian Federation. (In Russian)]

Статья представлена к публикации членом редколлегии В.В. Кульбой.

Поступила в редакцию 29.04.2022,
после доработки 4.07.2022.
Принята к публикации 11.07.2022.

Москвичев Владимир Викторович – д-р техн. наук, Красноярский филиал ФИЦ ИВТ, г. Красноярск, ✉ e-mail: krasn@ict.nsc.ru,

Постникова Ульяна Сергеевна – мл. науч. сотрудник, Красноярский филиал ФИЦ ИВТ, г. Красноярск, ✉ e-mail: ulyana-ivanova@inbox.ru,

Тасейко Ольга Викторовна – канд. физ.-мат. наук, СибГУ им. М.Ф. Решетнева, г. Красноярск, ✉ e-mail: taseiko@gmail.com.

MANAGEMENT OF TECHNOGENIC SAFETY BASED ON A RISK-ORIENTED APPROACH

V.V. Moskvichev[1], U.S. Postnikova[1], and O.V. Taseiko[2]

[1]Federal Research Center for Information and Computational Technologies,
Krasnoyarsk Branch, Krasnoyarsk, Russia
[2]Reshetnev Siberian State University of Science and Technology, Krasnoyarsk, Russia

✉ krasn@ict.nsc.ru, ✉ ulyana-ivanova@inbox.ru, ✉ taseiko@gmail.com

Abstract. This paper proposes a managerial decision algorithm based on the developed risk assessment methodology with multidimensional statistical analysis. The methodology allows calculating an acceptable level of risk, which can be used in regulatory documents. The decision algorithm is integrated into the information system of territorial risk and security management. The industrial agglomerations of Siberia are chosen as the object of research, and their main types of technogenic hazards are analyzed. The complex risk is assessed using statistical data on man-made dangerous events, emergencies, material damage, and fatal outcomes from the official database (the Emercom of Russia). According to risk factor analysis, the main technogenic load in territorial units is due to fire and explosive events. The inverse problem is solved, showing the need to reduce the main risk factors for achieving an acceptable level. Minimizing the complex technogenic territorial risk is a management problem with two criteria: the minimum number of fatal outcomes and the minimum amount of damage. Within the complex risk assessment approach, the problem is solved by proposing preventive measures to improve territorial security.

Keywords: socio-natural-technogenic system, territorial risk, management.

Funding. This work was supported by the Russian Federation President grant no. NSh-421.2022.4.

УДК 519.83+519.86

DOI: http://doi.org/10.25728/pu.2022.3.3

МЕТОДИКА СРАВНИТЕЛЬНОГО АНАЛИЗА ЭФФЕКТИВНОСТИ СПОСОБОВ ОРГАНИЗАЦИИ АКТИВНЫХ АГЕНТОВ И МЕТОДОВ УПРАВЛЕНИЯ

Г.А. Угольницкий

Аннотация. При взаимодействии активные агенты могут действовать независимо, вступать в кооперацию или быть связанными отношениями иерархии. В свою очередь, иерархическое воздействие может осуществляться с помощью административных или экономических методов с обратной связью или без неё. Приведено систематическое описание этих способов организации и методов управления посредством теоретико-игровых моделей конфликтного управления без учёта неопределённости с разными информационными регламентами. Представляется чрезвычайно важным количественное сравнение выигрышей отдельных агентов и всего их множества (общественного благосостояния) при указанных способах организации и методах управления. Предложена методика построения систем общественных и индивидуальных предпочтений на основе выигрышей агентов в играх в нормальной форме и долей в распределении общего выигрыша в кооперативных играх. Для более детальной количественной оценки разработана система индексов относительной эффективности. Предложенная методика проиллюстрирована на примере моделей олигополии Курно.

Ключевые слова: методы управления и распределения дохода, неэффективность равновесий, способы организации активных агентов.

ВВЕДЕНИЕ

На первый взгляд кажется очевидным, что кооперация лучше конфронтации. Объединение усилий активных агентов позволяет добиться лучших результатов, чем их независимое эгоистичное поведение и тем более вражда, а полученный дополнительный выигрыш коалиции всех агентов можно каким-то образом разделить между всеми ними.

К сожалению, здесь не всё так просто. Для общества в целом действительно выигрыш при кооперации всегда по крайней мере не меньше, чем при независимом поведении составляющих общество активных агентов или при наличии отношений иерархии между ними. Но вот для каждого агента в отдельности это уже совсем не обязательно так. Например, выигрыш агента верхнего уровня иерархии может оказаться больше, чем его доля в равномерном распределении при кооперации даже с учётом дополнительного эффекта. Не так легко и договориться о том, как именно делить прибавку даже при наличии принципиального соглашения о сотрудничестве и как обеспечить устойчивость этого соглашения. Возможно, отчасти в силу этих соображений известно множество примеров отказа от кооперации в пользу конфликта и борьбы за лидерство в экономике, общественной жизни, международных отношениях и иных областях.

Поэтому чрезвычайно актуальным представляется математический анализ условий выгодности кооперации и сравнение эффективности различных способов организации активных агентов, методов управления ими и распределения полученного кооперативного дохода. Фундаментальные основы такого анализа предоставляют теории активных систем и управления организационными системами [1, 2], информационная теория иерархических систем [3–7], теория контрактов и дизайн механизмов [8]. Концепция управления устойчивым развитием активных систем на основе учёта и согласования интересов активных агентов предложена в работах [9, 10]. Основным математическим инструментом анализа служит теория игр [11–15]. Для решения сложных динамических задач конфликтного управления целесообразно использовать имитационное моделирование [16].

Детальный анализ так называемой проблемы неэффективности равновесий приведён в работах [17–20]. Исход рационального поведения независимых эгоистичных экономических агентов обычно оказывается для общества хуже исхода, полученного при централизованном управлении или добровольной кооперации. Возникает важный вопрос: насколько именно хуже? Обычно для количественной оценки неэффективности равновесий используется цена анархии, которая определяется как отношение наихудшего из равновесных значений выбранной функции выигрыша общества к её значению на оптимальном исходе [21]. Более широкий набор показателей для динамических игр предложен в работе [22]. Сравнение выигрышей при различных способах организации агентов проводится в очень многих работах по теории игр [23–25].

Однако, проблему (не)эффективности равновесий целесообразно формулировать в более общем виде. Прежде всего, сравнению подлежат выигрыши не только при базовых способах организации активных экономических агентов (равноправие, иерархия, кооперация), но и с учётом различных методов управления, определяющих регламент взаимодействия агентов. Кроме того, что ещё более важно, сравнение необходимо проводить с точки зрения не только общественного благосостояния, но и интересов отдельных агентов. Ещё раз подчеркнём, что исход игры, более выгодный для общества в целом при некотором способе организации, не обязательно окажется таким же для каждого из агентов.

Главные способы организации взаимодействия активных агентов – это их равноправие, иерархия и кооперация. При равноправии агенты (игроки) выбирают свои действия одновременно и независимо, а решением возникающей игры в нормальной форме считается равновесие Нэша. При иерархической организации возможны два основных варианта управления. При первом из них ведущий игрок выбирает и сообщает одному или нескольким остальным игрокам своё предполагаемое действие, а они оптимально реагируют на него. Тогда возникает игра Гермейера Γ_1 (игра Штакельберга в англоязычной литературе), решением которой считается равновесие Штакельберга. Во втором варианте ведущий выбирает и сообщает ведомым свою стратегию как функцию от их ожидаемых действий, а они оптимально реагируют на эту стратегию. Тогда возникает игра Гермейера Γ_2 (обратная игра Штакельберга в англоязычной литературе), решение которой ищется на основе принципа гарантированного результата Ю.Б. Гермейера [4]. Целесообразно также различать административные (принуждение) и экономические (побуждение) методы управления, которые соответственно заключаются в воздействии на множества допустимых стратегий или функции выигрыша агентов [9, 10]. Другой вариант формализации иерархических отношений – игры в развёрнутой форме, когда игроки делают ходы последовательно. Этот вариант в статье не рассматривается. Наконец, при кооперации все игроки объединяются и совместно максимизируют суммарную функцию выигрыша по всем управляющим переменным. Эта трактовка отвечает утилитаристскому подходу, в отличие от эгалитаристского, когда максимизируется наименьший из выигрышей агентов [26].Тогда исходная игра сводится к задаче оптимизации, кооперативное решение которой оптимально по Парето. Динамические постановки задач конфликтного управления (дифференциальные или разностные игры) в обсуждаемом смысле принципиально не отличаются от статических [11–15].

Кроме функций выигрыша, которые характеризуют эффективность действий активных агентов, теоретико-игровые модели могут содержать дополнительные ограничения, характеризуемые как условия координации [7] или условия устойчивого развития [9, 10]. Эти условия означают, что состояние управляемой динамической системы должно принадлежать определённой области фазового пространства. В статических моделях данные условия формулируются как ограничения на управляющие переменные.

Вклад настоящей статьи состоит в следующем:

- дано систематическое описание способов взаимодействия активных агентов и методов управления ими посредством теоретико-игровых моделей без учёта неопределённости;
- предложена методика сравнительного анализа общественной и индивидуальной эффективности указанных способов и методов на основе выигрышей агентов в играх в нормальной форме и их долей в кооперативном распределении общего выигрыша в играх в форме характеристической функции;
- для более детальной количественной оценки сравнительной эффективности разработана система индексов;
- предложенная методика проиллюстрирована на примере статических и динамических моделей олигополии Курно.

В § 1 описывается теоретико-игровая формализация способов организации взаимодействия активных агентов и методов управления ими. Сравнение выигрышей агентов позволяет построить

системы общественных и индивидуальных предпочтений. При этом для более детальной количественной характеристики можно использовать индексы сравнительной эффективности. В § 2 рассматривается методика сравнительного анализа эффективности, основанная на построении и исследовании теоретико-игровых моделей конфликтного управления. В § 3 предложенная методика иллюстрируется на примере различных моделей олигополии Курно. Результаты настоящей работы и перспективы дальнейших исследований обсуждаются в заключении.

1. СПОСОБЫ ОРГАНИЗАЦИИ, МЕТОДЫ УПРАВЛЕНИЯ И СИСТЕМЫ ПРЕДПОЧТЕНИЙ

1.1. Способы организации и методы управления

Базовые способы организации взаимодействия активных агентов – это их равноправие, иерархия и кооперация. При иерархической организации возможны два основных метода управления: принуждение (административные механизмы) и побуждение (экономические механизмы). Эти механизмы могут быть реализованы с обратной связью по управлению или без неё.

При кооперации возникают два вопроса: как определить выигрыш каждой коалиции (построение характеристической функции) и как распределить общий выигрыш между игроками (выбор принципа оптимальности). Распределение выигрыша также естественно трактовать как задачу управления.

В данном разделе даётся систематическое описание указанных способов взаимодействия и методов управления посредством статических теоретико-игровых моделей.

Взаимодействие равноправных агентов отражает модель игры *n* лиц в нормальной форме

$$u_i(x_1,...,x_n) \to \max,\ x_i \in X_i,\ i \in N. \qquad (1.1)$$

Здесь $N = \{1,..., n\}$ – множество игроков (активных агентов); X_i – множество допустимых действий игрока *i*; x_i – конкретное выбранное действие игрока *i*; $u_i : X \to R$ – функция выигрыша игрока *i*. Игроки из множества N одновременно и независимо выбирают свои действия x_i, в результате чего возникает исход игры $x = (x_1,...,x_n) \in X = X_1 \times ... \times X_n$. Игроки могут иметь различную природу. В экономике это отдельные предприниматели, домохозяйства, фирмы, регионы, страны. В политике – отдельные избиратели, политические партии, движения и объединения, органы исполнительной и законодательной власти. В организационном управлении – отдельные сотрудники, подразделения и целые организации. Важно, что интересы каждого игрока целиком и полностью описываются стремлением к максимизации выигрыша u_i (постулат экономической рациональности).

Решением игры (1.1) считается множество равновесий Нэша

$$\mathrm{NE} = \{x^{\mathrm{NE}} \in X : \forall i \in N$$
$$\forall x_i \in X_i\ u_i(x^{\mathrm{NE}}) \ge u_i(x_i, x_{-i}^{\mathrm{NE}})\},$$
$$x_{-i} = (x_1,...,x_{i-1},x_{i+1},...,x_n). \qquad (1.2)$$

При кооперации игроки объединяются и вместе максимизируют суммарный выигрыш (утилитаристскую функцию общественного благосостояния) [26]

$$u(x) = \sum_{i \in N} u_i(x). \qquad (1.3)$$

Кооперативное решение есть

$$x^C \in X : u^C = u(x^C) = \max_{x \in X} u(x). \qquad (1.4)$$

При иерархическом управлении ко множеству игроков N добавляется выделенный игрок (Центр в теории активных систем), обозначаемый индексом 0. При управлении без обратной связи Центр выбирает и сообщает остальным игрокам своё действие $x_0 \in X_0$. Зная действие x_0, игроки выбирают оптимальные ответы. Предвидя такое поведение, Центр на самом деле выбирает действие $x_0 \in X_0$ так, чтобы максимизировать свой выигрыш на множестве оптимальных ответов. Здесь различают два случая.

- Если Центр рассчитывает на благожелательность остальных агентов, то его выигрыш определяется значением

$$u_0^B = \sup_{x_0 \in X_0}\ \sup_{x \in R(x_0)} u_0(x_0, x), \qquad (1.5)$$

где $R(x_0)$ – множество оптимальных ответов агентов на действие Центра x_0. Ответ на вопрос о том, как определить это множество при связанных агентах, неочевиден. Обычно считают, что $R(x_0) = \mathrm{NE}(x_0)$, предполагая $\forall x_0\ \mathrm{NE}(x_0) \ne \varnothing$, иначе определение множества $R(x_0)$ нужно давать отдельно для конкретной модели. В широко известной монографии [13] даётся следующее определение равновесия Штакельберга для конечных игр трёх лиц, которое легко обобщить для произвольного $n > 3$.

Пусть в игре трёх лиц первый игрок ведущий, второй и третий ведомые. Обозначим через x_i стратегии игроков, X_i – множества их допусти-

мых стратегий, $J_1(x_1, x_2, x_3)$ – выигрыши при исходе (x_1, x_2, x_3), $i = 1, 2, 3$. Тогда x_1^* – иерархическая равновесная стратегия ведущего, если

$$\min_{(x_2, x_3) \in R(x_1^*)} J_1(x_1^*, x_2, x_3) = \max_{x_1 \in X_1} \min_{(x_2, x_3) \in R(x_1)} J_1(x_1, x_2, x_3),$$

где $R(x_1)$ – множество оптимальных ответов группы ведомых, которое определяется для каждой стратегии ведущего $x_1 \in X_1$ условиями

$$R(x_1) = \{(y_2, y_3) \in X_2 \times X_3 : J_2(x_1, y_2, y_3) \geq \geq J_2(x_1, x_2, x_3) \wedge J_3(x_1, y_2, y_3) \geq J_3(x_1, x_2, x_3), \forall x_2 \in X_2, x_3 \in X_3\}.$$

Любая тройка (x_1^*, x_2^*, x_3^*), $(x_2^*, x_3^*) \in R(x_1^*)$, есть равновесие Штакельберга [13, *с. 145, 146*].

- В противном случае (при сознательной или невольной неблагожелательности агентов) выигрыш Центра определяется значением

$$u_0^{\mathrm{NB}} = \sup_{x_0 \in X_0} \inf_{x \in R(x_0)} u_0(x_0, x). \qquad (1.6)$$

Обозначим через ST множество равновесий Штакельберга (решений иерархической игры Центра и агентов).

Замечание 1. Часто считается, что равновесие Штакельберга определяется только формулой (1.5), в то время как формула (1.6) относится лишь к принципу гарантированного результата Ю.Б. Гермейера, однако это не так. В широко известной монографии [13] равновесие Штакельберга определяется формулой (1.6).

Замечание 2. Во многих представляющих практический интерес прикладных моделях существует единственный оптимальный ответ агентов (например, единственное равновесие Нэша). Тогда вопрос о благожелательности или неблагожелательности агентов вообще не возникает.

При иерархическом управлении с обратной связью Центр выбирает и сообщает остальным игрокам свою стратегию $\tilde{x}_0 \in \tilde{X}_0 = X_0^X$, т. е. $\tilde{x} : X \to X_0$. Далее регламент игры аналогичен предыдущему случаю с естественной модификацией. Зная стратегию $\tilde{x}_0$, игроки выбирают оптимальный ответ. Предвидя такое поведение, Центр на самом деле выбирает стратегию $\tilde{x}_0 \in \tilde{X}_0$ так, чтобы максимизировать свой выигрыш на множестве оптимальных ответов. Если Центр рассчитывает на благожелательность агентов, то его выигрыш определяется значением

$$\tilde{u}_0^B = \sup_{\tilde{x}_0 \in \tilde{X}_0} \sup_{x \in R(\tilde{x}_0)} u_0(\tilde{x}_0(x), x). \qquad (1.7)$$

В противном случае (при сознательной или невольной неблагожелательности агентов) выигрыш Центра определяется значением

$$\tilde{u}_0^{\mathrm{NB}} = \sup_{\tilde{x}_0 \in \tilde{X}_0} \inf_{x \in R(\tilde{x}_0)} u_0(\tilde{x}_0(x), x). \qquad (1.8)$$

Обозначим через IST множество решений иерархической игры Центра и агентов при управлении с обратной связью.

При иерархическом управлении различают административные методы (принуждение) и экономические методы (побуждение) [9, 10]. Проведём формализацию на примере управления без обратной связи при неблагожелательных агентах. Иерархическая игра имеет вид

$$u_0(p, q, x) \to \max, \; p \in P, \; q \in Q; \qquad (1.9)$$

$$u_i(p_i, x) \to \max, \; x_i \in X_i(q_i), \; i \in N. \qquad (1.10)$$

Здесь $p = (p_1, ..., p_n)$ – вектор экономических управлений Центра, с помощью которых он воздействует на функции выигрыша агентов; $q = (q_1, ..., q_n)$ – вектор административных управлений Центра, посредством которых он воздействует на множества допустимых действий агентов.

Множество равновесий принуждения в игре (1.9), (1.10) есть множество исходов $\mathrm{COMP} = \{(x_0^{\mathrm{COMP}}, x^{\mathrm{COMP}}) : u_0(x_0^{\mathrm{COMP}}, x^{\mathrm{COMP}}) = u_0^{\mathrm{COMP}}\}$, где

$$u_0^{\mathrm{COMP}} = \sup_{q \in Q} \inf_{x \in R(q)} u_0(q, x), \qquad (1.11)$$

при этом значение p считается фиксированным.

Множество равновесий побуждения в игре (1.9), (1.10) есть множество исходов $\mathrm{IMP} = \{(x_0^{\mathrm{IMP}}, x^{\mathrm{IMP}}) : u_0(x_0^{\mathrm{IMP}}, x^{\mathrm{IMP}}) = u_0^{\mathrm{IMP}}\}$, где

$$u_0^{\mathrm{IMP}} = \sup_{p \in P} \inf_{x \in R(p)} u_0(p, x), \qquad (1.12)$$

при этом значение q считается фиксированным. Случай управления с обратной связью формализуется аналогично.

Замечание 3. Известны и другие информационные регламенты, например, игра Гермейера Γ_3 [7]. Поэтому предложенная классификация не претендует на исчерпывающую полноту. Однако она охватывает основные способы организации активных агентов.

Для описания распределения кооперативного дохода (1.4) целесообразно использовать теорию игр в форме характеристической функции (кооперативных игр) [11, 12]. Характеристическая функция есть отображение $v : 2^N \to R$, её значение $v(K)$ характеризует выигрыш коалиции $K \subseteq N$. Наиболее распространена характеристическая функция фон Неймана – Моргенштерна [27]

$$v^{\mathrm{NM}}(K) = \mathrm{val}(K,\, N\setminus K) = \\ = \sup_{x_i,\, i\in K} \inf_{x_j\, j\in N\setminus K} \sum_{i\in K} u_i(x_1,..., x_n). \qquad (1.13)$$

Предложены также характеристические функции Петросяна – Заккура [28]

$$v^{\mathrm{PZ}}(K) = \sup_{x_i,\, i\in K} \sum_{i\in K} u_i(x_K,\, x^{\mathrm{NE}}_{N\setminus K}) \qquad (1.14)$$

и Громовой – Петросяна [29]

$$v^{\mathrm{PG}}(K) = \inf_{x_j\, ,j\in N\setminus K} \sum_{i\in K} u_i(x^C_K,\, x_{N\setminus K}), \qquad (1.15)$$

где x_K – набор стратегий игроков из коалиции K, $x_{N\setminus K}$ – набор стратегий игроков из анти-коалиции $N\setminus K$, верхний индекс NE или C обозначает равновесие Нэша или кооперативное решение соответственно. Заметим, что для всех характеристических функций (1.13)–(1.15)

$$v^{\mathrm{NM}}(N) = v^{\mathrm{PZ}}(N) = v^{\mathrm{PG}}(N) = \sup_{x_1,...,x_n} \sum_{i\in N} u_i(x_1,..., x_n) = u^C,$$

т. е. выигрыш максимальной коалиции всегда совпадает с выигрышем при кооперации (1.4). В качестве решения кооперативной игры удобно взять вектор Шепли, который всегда существует и единствен. Компоненты вектора Шепли вычисляются по формуле [30]

$$\Phi_i(v) = \sum_{i\in K} \gamma_n(k)[v(K) - v(K\setminus\{i\})],\ \ i\in N,$$

$$\gamma_n(k) = \frac{(n-k)!(k-1)!}{n!},\ k = |K|,\ n = |N|. \qquad (1.16)$$

В соответствии с формулой (1.16), доля игрока при распределении кооперативного выигрыша согласно вектору Шепли показывает его вклад во все коалиции с его участием с учётом их мощности.

1.2. Системы предпочтений и индексы сравнительной эффективности

Эффективность различных способов организации активных агентов, методов управления и распределения кооперативного выигрыша принципиально необходимо сравнивать с двух разных позиций: общества в целом и отдельных агентов. Показателями для системы общественных предпочтений служат величины суммарного выигрыша (1.3). Для удобства сравнения предположим, что всегда $N = \{0, 1,..., n\}$, при этом в случаях равноправного и кооперативного поведения игрок с номером 0 ничем не отличается от остальных игроков.

Выигрыш общества при равноправии есть

$$u^{\mathrm{NE}} = \min_{x\in \mathrm{NE}} u(x), \qquad (1.17)$$

при кооперации

$$u^C = \max_{x\in X} u(x), \qquad (1.18)$$

при управлении без обратной связи

$$u^{\mathrm{ST}} = \sum_{i\in N} u_i(x^{\mathrm{ST}}), \qquad (1.19)$$

при управлении с обратной связью

$$u^{\mathrm{IST}} = \sum_{i\in N} u_i(x^{\mathrm{IST}}). \qquad (1.20)$$

Для вычисления общественного выигрыша (1.19) могут использоваться как определение (1.5), так и (1.6), а для вычисления выигрыша (1.20) – как (1.7), так и (1.8) в зависимости от того, какие сделаны предположения о благожелательности/неблагожелательности агентов. Также в качестве решения иерархической игры вместо ST можно брать множество COMP на основе формулы (1.11) или множество IMP на основе формулы (1.12) либо их аналоги при управлении с обратной связью на основе формул (1.7), (1.8) вместо IST. Соответственно, получим общественные выигрыши u^{COMP}, u^{IMP}, u^{ICOMP}, u^{IIMP}.

Согласно определению (1.4), выигрыш общества при кооперации всегда не меньше, чем при любом другом способе организации или методе управления. Для оценки потерь (неэффективности равновесий) можно использовать индексы общественной эффективности

$$K^{\mathrm{NE}} = \frac{u^{\mathrm{NE}}}{u^C},\ K^{\mathrm{ST}} = \frac{u^{\mathrm{ST}}}{u^C},\ K^{\mathrm{IST}} = \frac{u^{\mathrm{IST}}}{u^C},\ K^{\mathrm{COMP}} = \frac{u^{\mathrm{COMP}}}{u^C},$$

$$K^{\mathrm{IMP}} = \frac{u^{\mathrm{IMP}}}{u^C},\ K^{\mathrm{ICOMP}} = \frac{u^{\mathrm{ICOMP}}}{u^C},$$

$$K^{\mathrm{IIMP}} = \frac{u^{\mathrm{IIMP}}}{u^C}. \qquad (1.21)$$

Замечание 4. Использование индексов (1.21) предполагает положительность всех выигрышей, и тогда значения всех дробей не превышают единицу. Хотя это предположение считается стандартным в теории (не)эффективности равновесий [17, *с. 444*], оно ограничивает универсальность подхода. На самом деле, для сравнительного анализа эффективности можно использовать исходные значения выигрышей. Индексы (1.21) дают дополнительную количественную характеристику в тех случаях, когда это удобно.

Показателями для системы индивидуальных предпочтений агентов $i\in N$ служат величины:

- при равноправии –

$$u_i^{\mathrm{NE}} = \min_{x\in \mathrm{NE}} u_i(x), \qquad (1.22)$$

т. е. значение выигрыша игрока в наихудшем из равновесий Нэша (принципа оптимальности для данного способа организации);

- при кооперации –

$$u_i^C = \frac{u^C}{|N|} \qquad (1.23)$$

либо значение вектора Шепли $\Phi_i(v)$ для одной из характеристических функций (1.13), (1.14) или (1.15);

- при иерархии без обратной связи u_i^{ST};
- при иерархии с обратной связью u_i^{IST}.

В качестве множеств ST или IST можно также брать их аналоги при принуждении COMP, ICOMP или при побуждении IMP, IIMP. Для более детальной количественной сравнительной оценки подходят индексы индивидуальной эффективности

$$K_i^{\mathrm{NE}} = \frac{u_i^{\mathrm{NE}}}{u_i^C},\ K_i^{\mathrm{ST}} = \frac{u_i^{\mathrm{ST}}}{u_i^C},\ K_i^{\mathrm{IST}} = \frac{u_i^{\mathrm{IST}}}{u_i^C},$$

$$K_i^{\mathrm{NM}} = \frac{\Phi_i^{\mathrm{NM}}}{u_i^C}\ K_i^{\mathrm{PZ}} = \frac{\Phi_i^{\mathrm{PZ}}}{u_i^C},\ K_i^{\mathrm{PG}} = \frac{\Phi_i^{\mathrm{PG}}}{u_i^C},$$

$$K_i^{\mathrm{COMP}} = \frac{u_i^{\mathrm{COMP}}}{u_i^C}, K_i^{\mathrm{IMP}} = \frac{u_i^{\mathrm{IMP}}}{u_i^C},\ K_i^{\mathrm{ICOMP}} = \frac{u_i^{\mathrm{ICOMP}}}{u_i^C},$$

$$K_i^{\mathrm{IIMP}} = \frac{u_i^{\mathrm{IIMP}}}{u_i^C}, i \in N. \qquad (1.24)$$

Показатели общественной и индивидуальной эффективности и соответствующие индексы собраны в табл. 1.

Условия координации (устойчивого развития) имеют вид

$$u \in U^*, \qquad (1.25)$$

где U^* – некоторое заданное множество. Эти условия могут дополнять любую из рассмотренных моделей.

2. МЕТОДИКА СРАВНИТЕЛЬНОГО АНАЛИЗА ЭФФЕКТИВНОСТИ

Сравнительный анализ эффективности способов организации активных агентов и методов управления и распределения кооперативного выигрыша включает в себя следующие этапы.

1. Ввести множество активных агентов (игроков) $N = \{0, 1, ..., n\}$.

2. При равноправии агент с номером 0 не отличается от остальных. Построить игру в нормальной форме (1.1). Найти множество равновесий Нэша (1.2). Вычислить значения показателей (1.17) и (1.22).

3. При кооперации агент с номером 0 также не отличается от остальных. Найти решение задачи оптимизации (1.4). Вычислить значения показателей (1.18) и (1.23).

4. При иерархии агент с номером 0 выполняет роль Центра (на эту роль может претендовать любой из исходно равноправных игроков). Для регламента управления без обратной связи вычислить значения выигрышей (1.5) и (1.6) и найти соответствующие множества ST. Вычислить значения показателя (1.19) и u_i^{ST}.

5. Для регламента управления с обратной связью вычислить значения (1.7) и (1.8) и найти соответствующие множества IST. Вычислить значения показателей (1.20) и u_i^{IST}.

Таблица 1

Показатели и индексы общественной и индивидуальной эффективности

	Равноправие	Кооперация	Иерархия без обратной связи	Иерархия с обратной связью
Показатели общественной эффективности	u^{NE}	$u^C = v(N)$	$u^{\mathrm{ST}}, u^{\mathrm{COMP}}, u^{\mathrm{IMP}}$	$u^{\mathrm{IST}}, u^{\mathrm{ICOMP}}, u^{\mathrm{IIMP}}$
Показатели индивидуальной эффективности, $i \in N$	u_i^{NE}	$u_i^C, \Phi_i^{\mathrm{NM}}, \Phi_i^{\mathrm{PZ}}, \Phi_i^{\mathrm{PG}}$	$u_i^{\mathrm{ST}}, u_i^{\mathrm{COMP}}, u_i^{\mathrm{IMP}}$	$u_i^{\mathrm{IST}}, u_i^{\mathrm{ICOMP}}, u_i^{\mathrm{IIMP}}$
Индексы общественной эффективности	$K^{\mathrm{NE}} = \frac{u^{\mathrm{NE}}}{u^C}$	–	$K^{\mathrm{ST}} = \frac{u^{\mathrm{ST}}}{u^C}$	$K^{\mathrm{IST}} = \frac{u^{\mathrm{IST}}}{u^C}$
Индексы индивидуальной эффективности, $i \in N$	$K_i^{\mathrm{NE}} = \frac{u_i^{\mathrm{NE}}}{u_i^C}$	$K_i^{\mathrm{NM}} = \frac{\Phi_i^{\mathrm{NM}}}{u_i^C}$, $K_i^{\mathrm{PZ}} = \frac{\Phi_i^{\mathrm{PZ}}}{u_i^C}$, $K_i^{\mathrm{PG}} = \frac{\Phi_i^{\mathrm{PG}}}{u_i^C}$	$K_i^{\mathrm{ST}} = \frac{u_i^{\mathrm{ST}}}{u_i^C}$, $K_i^{\mathrm{COMP}} = \frac{u_i^{\mathrm{COMP}}}{u_i^C}$, $K_i^{\mathrm{IMP}} = \frac{u_i^{\mathrm{IMP}}}{u_i^C}$	$K_i^{\mathrm{IST}} = \frac{u_i^{\mathrm{IST}}}{u_i^C}$, $K_i^{\mathrm{ICOMP}} = \frac{u_i^{\mathrm{ICOMP}}}{u_i^C}$, $K_i^{\mathrm{IIMP}} = \frac{u_i^{\mathrm{IIMP}}}{u_i^C}$

6. Для регламента принуждения в иерархической игре (1.9), (1.10) найти множество COMP согласно формуле (1.11). Вычислить аналоги показателей (1.19) и u_i^{ST}.

7. Для регламента побуждения в иерархической игре (1.9), (1.10) найти множество IMP согласно формуле (1.12). Вычислить аналоги показателей (1.20) и u_i^{IST}.

8. На основе игры в нормальной форме (1.1) построить игру в форме каждой из характеристических функций (1.13)–(1.15). Для этих игр вычислить вектор Шепли (1.16).

9. На основе иерархической игры с управлением при отсутствии или наличии обратной связи построить игру в форме каждой из характеристических функций (1.13)–(1.15). В этом случае возможны три различных типа коалиций: только агенты; только Центр; Центр и хотя бы один агент (включая максимальную коалицию). Для построенных кооперативных игр вычислить вектор Шепли (1.16).

10. Учесть дополнительно ограничения вида (1.25).

11. Построить систему общественных предпочтений путём упорядочения показателей (1.17), (1.19), (1.20), а также величин $u^{\mathrm{COMP}}, u^{\mathrm{IMP}}, u^{\mathrm{ICOMP}}, u^{\mathrm{IIMP}}$. Дополнительно оценить потери от неэффективности равновесий с помощью индексов (1.21).

12. Построить систему индивидуальных предпочтений путём упорядочения показателей (1.22), (1.23). Для более детальной оценки сравнительной эффективности использовать индексы (1.24).

Замечание 5. Разумеется, что в большинстве случаев решения теоретико-игровых задач конфликтного управления могут быть найдены только численно. Тогда при сравнении используются средние значения всех введённых показателей по множеству вычислительных экспериментов для различных наборов входных данных.

Замечание 6. В зависимости от постановки задачи и возможностей исследования некоторые этапы могут быть опущены.

3. МОДЕЛИ ОЛИГОПОЛИИ КУРНО

В качестве иллюстративного примера проведём сравнительный анализ эффективности нескольких моделей олигополии Курно.

Пример 1. Олигополия Курно с симметричными агентами.

Пусть $N=\{1,...,n\}$ – множество равноправных симметричных агентов (фирм). Для случая постоянных затрат с учётом налога модель имеет вид

$$u_i(x)=(1-p)[(D-\bar{x})x_i-cx_i]\to\max,$$
$$0\le x_i\le 1/n,\ i\in N.$$

Здесь x_i – объём выпуска продукции i-й фирмы; D – объём спроса; c – удельные затраты каждой фирмы; $p\in[0,1]$ – фиксированная ставка налога; $\bar{x}=x_1+...+x_n$. Положим для определённости $D=1$, $c=1/n$ (в работе [31] эта параметризация использована для $n=2$). Тогда

$$u_i(x)=(1-p)\left(\frac{n-1}{n}-\bar{x}\right)x_i\to\max,\qquad(3.1)$$
$$0\le x_i\le 1/n,\ i\in N.$$

Обозначим также $\bar{u}(x)=u_1(x)+...+u_n(x)$. Имеем

$$\frac{\partial u_i}{\partial x_i}=0=\frac{n-1}{n}-2x_i-\sum_{j\ne i}x_j,\ i\in N;$$

$$2x_i+\sum_{j\ne i}x_j=\frac{n-1}{n},\ i\in N.$$

Значит, в равновесии Нэша

$$x_i^{\mathrm{NE}}=x^{NE}=\frac{n-1}{n(n+1)};\ \bar{x}^{\mathrm{NE}}=\frac{n-1}{n+1};$$
$$u_i^{\mathrm{NE}}=u^{\mathrm{NE}}=\frac{(1-p)(n-1)^2}{n^2(n+1)^2};\qquad(3.2)$$
$$\bar{u}^{\mathrm{NE}}=\frac{(1-p)(n-1)^2}{n(n+1)^2}.$$

Пусть теперь агенты из множества N вступают в кооперацию. Модель принимает вид

$$\bar{u}(x)=(1-p)\left(\frac{n-1}{n}-\bar{x}\right)\bar{x}\to\max,$$
$$0\le x_i\le 1/n,\ i\in N.$$

Очевидно, что в этом случае $\forall i\in N\ x_i=x$, откуда

$$\bar{u}(x)=(1-p)\left(\frac{n-1}{n}-nx\right)nx,$$

и условие максимума имеет вид

$$\frac{\partial\bar{u}}{\partial x}=0=n-1-2nx,$$

откуда получаются решение кооперативной задачи оптимизации и значения выигрышей

$$x_i^C=x^C=\frac{n-1}{2n^2};\ \bar{x}^C=\frac{n-1}{2n};$$
$$u_i^C=u^C=\frac{(1-p)(n-1)^2}{4n^3};$$
$$\bar{u}^C=\frac{(1-p)(n-1)^2}{4n^2}.$$

Далее пусть агент с номером 1 становится Центром, первым выбирает значение x_1 и сообщает его остальным агентам. Тогда задача каждого из этих агентов такова:

$$u_i = (1-p)\left(\frac{n-1}{n} - x_1 - \sum_{j=2}^{n} x_j\right)x_i \to \max,$$

$$0 \le x_i \le 1/n, \;\; i = 2,..., n.$$

Условия максимума

$$\frac{\partial u_i}{\partial x_i} = 0 = \frac{n-1}{n} - x_1 - 2x_i - \sum_{j=2, j\ne i}^{n} x_j \;,\; i = 2,..., n \;,$$

дают оптимальный ответ каждого агента (индекс BR обозначает *best response*)

$$x_i^{\mathrm{BR}} = x^{\mathrm{BR}} = \frac{n-1-nx_1}{n^2}, i = 2,...,n \;.$$

Задача Центра принимает вид

$$u_1(x_1) = (1-p)\left(\frac{n-1}{n} - x_1 - \frac{(n-1)(n-1-nx_1)}{n^2}\right)x_1 =$$

$$= \frac{1-p}{n^2}(n-1-nx_1)x_1 \to max, \; 0 \le x_1 \le 1/n.$$

Условия максимума

$$\frac{\partial u_1}{\partial x_1} = 0 = n-1-2nx_1$$

приводят к равновесию Штакельберга

$$x_1^{\mathrm{ST}} = \frac{n-1}{2n}; \; x_i^{\mathrm{ST}} = \frac{n-1}{2n^2}, \; i = 2,..., \; n,$$

суммарному выпуску $\bar{x}^{\mathrm{ST}} = \dfrac{(n-1)(2n-1)}{2n^2}$ и выигрышам

$$u_1^{\mathrm{ST}} = \frac{(1-p)(n-1)^2}{4n^3};$$

$$u_i^{\mathrm{ST}} = \frac{(1-p)(n-1)^2}{4n^4}, i = 2,...,n \;;$$

$$\bar{u}^{\mathrm{ST}} = \frac{(1-p)(n-1)(n^2-n+1)}{4n^4}.$$

Предположим теперь, что Центр – это дополнительный агент с индексом 0, который сам ничего не производит, но назначает ставку налога p. Тогда его задачу можно записать в виде

$$u_0 = \left(\frac{n-1}{n} - \bar{x}\right)\bar{x}p - ap^2 \to \max, \; 0 \le p \le 1 \;, \quad (3.3)$$

где $a > 0$ – коэффициент затрат на сбор налогов.

Оптимальный ответ агентов есть равновесие Нэша в их игре, которое задаётся формулой (3.2). Задача Центра принимает вид

$$u_0 = \frac{(n-1)^2}{n(n+1)^2}\,p - ap^2 \to \max, \; 0 \le p \le 1 \;, \quad (3.4)$$

откуда $p^{\mathrm{ST}} = \dfrac{(n-1)^2}{2an(n+1)^2}$, а равновесие Штакельберга (здесь равновесие побуждения) есть

$$\mathrm{ST{=}IMP} = \left(\frac{(n-1)^2}{2an(n+1)^2}, \frac{n-1}{n(n+1)}, ..., \frac{n-1}{n(n+1)}\right).$$

Выигрыши Центра и агентов задаются формулами

$$u_0^{\mathrm{IMP}} = \frac{(n-1)^2[(n-1)^2 - an(n+1)^2]}{2an^2(n+1)^2};$$

$$u_i^{\mathrm{IMP}} = \frac{(n-1)^2[2an(n+1)^2 - (n-1)^2]}{2an^2(n+1)^4}, \; i = 1,..., \; n \;;$$

$$\bar{u}^{\mathrm{IMP}} = \frac{(n-1)^2[2an(n+1)^2 - (n-1)^2]}{2an(n+1)^4}.$$

Рассмотрим теперь экологическое ограничение (условие устойчивого развития)

$$d\bar{x} \le P_{\max} \;, \quad (3.5)$$

за выполнение которого отвечает Центр (т. е. это дополнительное ограничение в его задаче оптимизации (3.4)), где d – коэффициент, характеризующий отношение объёма выбросов загрязняющих веществ к суммарному выпуску продукции; $P_{\max}$ – предельно допустимая величина выбросов. Тогда в равновесии Нэша это условие принимает вид

$$\frac{n-1}{n+1} \le \frac{P_{\max}}{d} \;, \quad (3.6)$$

а при кооперации

$$\frac{n-1}{2n} \le \frac{P_{\max}}{d} \;. \quad (3.7)$$

При выполнении условий (3.6) или (3.7) соответственно равноправное или кооперативное поведение агентов совместимо с условиями устойчивого развития.

В противном случае Центр может использовать механизм побуждения равноправных агентов к устойчивому развитию вида

$$\tilde{p}(x) = \begin{cases} p^{+}, \; x \le \dfrac{P_{\max}}{dn}, \\ p^{-}, \; \text{иначе.} \end{cases}$$

Для исследования распределения кооперативного выигрыша построим сначала характеристическую функцию фон Неймана – Моргенштерна (1.13). Очевидно, что для любой коалиции K имеем $x_i = 1/n, \; i \in N \setminus K.$ Тогда

$$v^{\mathrm{NM}}(i) = (1-p)\max_{x_i}\left(\frac{n-1}{n} - \frac{n-1}{n} - x_i\right)x_i = 0, \; i \in N \;;$$

$$v^{\mathrm{NM}}(K) = (1-p)\max_{x_i, i\in K}\left(\frac{n-1}{n} - \frac{n-k}{n} - \bar{x}_K\right)\bar{x}_K, \; k = |K| \;.$$

Поскольку, очевидно, $\forall i \in K \; x_i = x$, то

$$v^{\mathrm{NM}}(K) = k(1-p)\max_{x}\left(\frac{k-1}{n} - kx\right)x \;.$$

Условие максимума $\dfrac{k-1}{n} - 2kx = 0$ даёт

$$x^* = \frac{k-1}{2kn}, \; \bar{x}^* = \frac{k-1}{2n} \;,$$

откуда окончательно

$$v^{\mathrm{NM}}(K) = k(1-p)\left(\frac{k-1}{n} - \frac{k(k-1)}{2kn}\right)\frac{k-1}{2kn} = (1-p)\frac{(k-1)^2}{4n^2}.$$

Соответственно,

$$v^{\mathrm{NM}}(N) = \frac{(1-p)(n-1)^2}{4n^2} = \bar{u}^{C}.$$

По определению характеристическая функция Петросяна – Заккура (1.14) здесь совпадает с функцией фон

Неймана – Моргенштерна. Построим характеристическую функцию Громовой – Петросяна (1.15):

$$v^{\mathrm{GP}}(i)=(1-p)\left(\frac{n-1}{n}-\frac{n-1}{n}-\frac{n-1}{2n^2}\right)\frac{n-1}{2n^2}=$$

$$=-\frac{(1-p)(n-1)^2}{4n^4},\ i\in N;$$

$$v^{\mathrm{GP}}(K)=(1-p)\left(\frac{n-1}{n}-\frac{n-k}{n}-\frac{k(n-1)}{2n^2}\right)\frac{k(n-1)}{2n^2}=$$

$$=(1-p)\frac{k(n-1)(kn-2n+k)}{4n^4};$$

$$v^{\mathrm{GP}}(N)=\frac{(1-p)(n-1)^2}{4n^2}=\bar{u}^C.$$

В силу симметрии кооперативных игр для всех характеристических функций

$$\Phi^{\mathrm{NM}}=\Phi^{\mathrm{PZ}}=\Phi^{\mathrm{GP}}=\left(\frac{(1-p)(n-1)^2}{4n^3},...,\frac{(1-p)(n-1)^2}{4n^3}\right).$$

Очевидно, что в моделях с симметричными агентами для равноправия и кооперации общественные и индивидуальные предпочтения совпадают, а распределения кооперативного выигрыша согласно вектору Шепли всегда одинаковы для всех характеристических функций.

Заметим, что в рассмотренной модели $u^C=u_1^{\mathrm{ST}}>u_i^{\mathrm{ST}}$, $i=2,...,n$. Таким образом, кооперация строго выгоднее иерархии для всех агентов, кроме Центра, которому всё равно. При этом

$$\bar{u}^C-\bar{u}^{\mathrm{ST}}=\frac{(1-p)(n-1)}{4n^2}\left(n-1-\frac{n^2-n+1}{n^2}\right)=$$

$$=\frac{(1-p)(n-1)}{4n^4}(n^2(n-2)+n-1)>0,$$

т. е. для общества в целом кооперация строго выгоднее иерархии. Значения индексов

$$K^{\mathrm{NE}}=\frac{4n}{(n+1)^2}\underset{n\to\infty}{\to}0,\ K^{\mathrm{ST}}=\frac{n^2-n+1}{n^2(n-1)}\underset{n\to\infty}{\to}0$$

показывают, что с ростом числа агентов выгодность кооперации по сравнению с равноправием и иерархией увеличивается.

Пример 2. Дуополия Курно с несимметричными агентами.

Модель имеет вид

$$u_i=(1-p)(1-c_i-x_1-x_2)x_i\to\max,$$

$$0\le x_i\le 1/2,\ \ i=1,\ 2.$$

Теперь по сравнению с формулой (3.1) $c_i\in(0,\ 1/2)$ – затраты i-й фирмы. При равноправном поведении агентов равновесие Нэша находится как решение системы

$$\frac{\partial u_i}{\partial x_i}=0,\ i=1,2,\ \text{откуда}$$

$$x_i^{\mathrm{NE}}=(1+c_j-2c_i)/3,\ \ i,\ j=1,\ 2;$$

$$\bar{u}^{\mathrm{NE}}=(2-c_1-c_2)/3, \qquad (3.8)$$

а выигрыши равны

$$u_i^{\mathrm{NE}}=(1-p)(1+c_j-2c_i)^2/9,\ i=1,2;$$

$$\bar{u}^{\mathrm{NE}}=(1-p)(2-2c_1-2c_2+5c_1^2+5c_2^2-8c_1c_2)/9.$$

Кооперация агентов приводит к задаче оптимизации

$$\bar{u}=(1-p)[(1-\bar{x})\bar{x}-c_1x_1-c_2x_2]\to\max,$$

$$0\le x_i\le 1/2,\ \ i=1,\ 2.$$

Система $\partial\bar{u}/\partial x_i=0,\ \ i=1,\ 2$—∘, приводится к виду

$$\begin{cases}x_1+x_2=(1-c_1)/2,\\ x_1+x_2=(1-c_2)/2,\end{cases}$$

т. е. при сделанном предположении $c_1\ne c_2$ она не имеет решений. Значения суммарной функции выигрыша на границе области допустимых управлений равны

$$\bar{u}(0,\ 0)=0;\ \bar{u}(1/2,\ 1/2)=-(1-p)(c_1+c_2)<0;$$

$$\bar{u}(1/2,\ 0)=(1-p)(1/4-c_1/2);$$

$$\bar{u}(0,\ 1/2)=(1-p)(1/4-c_2/2).$$

Таким образом, решение кооперативной задачи и соответствующие выигрыши таковы:

$$x^C=\begin{cases}(1/2,\ 0),\ \ c_1<c_2\Rightarrow\bar{u}^C=(1-p)(1-2c_1)/4,\\ \qquad u_i^C=(1-p)(1-2c_1)/8,\ i=1,\ 2;\\ (0,\ 1/2),\ \ c_1>c_2\Rightarrow\bar{u}^C=(1-p)(1-2c_2)/4,\\ \qquad u_i^C=(1-p)(1-2c_2)/8,\ \ i=1,\ 2.\end{cases}$$

В обоих случаях суммарный кооперативный выпуск $\bar{x}^C=1/2$.

Далее пусть агент с номером 1 становится Центром, первым выбирает значение x_1 и сообщает его второму агенту. Аналогично предыдущему разделу получаем равновесие Штакельберга в виде

$$x_1^{\mathrm{ST}}=(1-2c_1+c_2)/2;\ x_2^{\mathrm{ST}}=(1+2c_1-3c_2)/4.$$

При этом суммарный выпуск и выигрыши равны

$$\bar{x}^{\mathrm{ST}}=(3-2c_1-c_2)/4;$$

$$u_1^{\mathrm{ST}}=(1-p)(1-2c_1+c_2)/8;$$

$$u_2^{\mathrm{ST}}=(1-p)(1+2c_1-3c_2)/16;$$

$$\bar{u}^{\mathrm{ST}}=(1-p)(3-4c_1-2c_2+12c_1^2-20c_1c_2+11c_2^2)/16.$$

Предположим теперь, что Центр – это дополнительный агент с индексом 0, который сам ничего не производит, но назначает ставку налога p. Тогда его задачу по аналогии с формулой (3.3) можно записать в виде

$$u_0=(1-c_1-c_2-\bar{x})\bar{x}p-ap^2\to\max,\ 0\le p\le 1.$$

Оптимальный ответ агентов на стратегию Центра p есть равновесие Нэша в их игре (3.8). Аналогично предыдущему разделу получаем стратегию побуждения Центра

$$p^{\mathrm{IMP}}=\frac{(1-2c_1-2c_2)(2-c_1-c_2)}{18a}$$

и равновесие побуждения $\mathrm{IMP}=(p^{\mathrm{IMP}},\ x_1^{\mathrm{NE}},\ x_2^{\mathrm{NE}})$.

Наконец, рассмотрим экологическое ограничение (условие устойчивого развития) (3.5). Тогда в равновесии Нэша это условие принимает вид

$$d(2-c_1-c_2)\le 3P_{\max},$$

а при кооперации

$$d\le 2P_{max}.$$

Построение игры в форме характеристической функции при $n=2$ нецелесообразно.

ЗАКЛЮЧЕНИЕ

Очевидный общий результат заключается в том, что в детерминированных моделях для общества в целом кооперация оказывается не хуже, чем любой другой способ организации взаимодействия активных агентов, поскольку она приводит к неотрицательному кооперативному эффекту. Возникающие при отказе от сотрудничества коллективные потери можно оценить с помощью различных индексов (классическая проблема неэффективности равновесий).

Однако для отдельных агентов вполне может оказаться выгоднее захватить лидерство или просто сохранять независимость. Неочевидны и правила распределения кооперативного выигрыша между агентами. Поэтому наряду с общественными нужно учитывать индивидуальные предпочтения, которые к тому же в общем случае неодинаковы для разных агентов. Здесь также можно использовать индексы сравнительной эффективности.

Даже в достаточно простых моделях вычислить выигрыши отдельных агентов и общества в целом и провести их аналитическое сравнение нелегко. В настоящей работе получены простые иллюстрации предложенной методики сравнительного анализа для случая симметричных агентов. В дальнейшем предполагается выполнить численное исследование сравнительной эффективности способов организации, методов управления и распределения кооперативного выигрыша для ряда статических и динамических моделей олигополии Курно.

ЛИТЕРАТУРА

1. *Бурков В.Н., Новиков Д.А.* Теория активных систем: состояние и перспективы. – М.: СИНТЕГ, 1999. – 128 с. [*Burkov, V.N., Novikov, D.A*. Teoriya aktivny hsistem: sostoyanie i perspektivy. – M.: SINTEG, 1999. – 128 s. (In Russian)]
2. *Новиков Д.А.* Теория управления организационными системами. – М.: Изд-во физ.-мат. лит., 2007. – 584 с. [*Novikov, D.A*. Teoriya upravleniya organizacionnymi sistemami. – M.: Izd-vofiz.-mat. lit., 2007. – 584 s. (In Russian)]
3. *Гермейер Ю.Б*. Введение в теорию исследования операций. – М.: Наука, 1971. – 384 с. [*Germejer, Yu.B.* Vvedenie v teoriyu issledovaniya operacij. – M.: Nauka, 1971. – 384 s. (In Russian)]
4. *Гермейер Ю.Б*. Игры с непротивоположными интересами. – М.: Наука, 1976. – 328 с. [*Germejer, Yu.B.* Igry s neprotivopolozhnymi interesami. – M.: Nauka, 1976. – 328 s. (In Russian)]
5. *Моисеев Н.Н*. Элементы теории оптимальных систем. – М.: Наука, 1975. – 528 с. [*Moiseev, N.N.* Elementy teorii optimal'nyh sistem. – M.: Nauka, 1975. – 528 s. (In Russian)]
6. *Кукушкин Н.С., Морозов В.В.* Теория неантагонистических игр. – М.: МГУ, 1984. – 106 с. [*Kukushkin, N.S., Morozov, V.V*. Teoriya neantagonisticheskih igr. – M.: MGU, 1984. – 106 s. (In Russian)]
7. *Горелик В.А., Горелов М.А., Кононенко А.Ф.* Анализ конфликтных ситуаций в системах управления. – М.: Радио и связь, 1991. – 288 с. [*Gorelik, V.A., Gorelov, M.A., Kononenko, A.F.* Analiz konfliktnyh situacij v sistemah upravleniya. – M.: Radio i svyaz', 1991. – 288 s. (InRussian)]
8. *Laffont, J.-J., Martimort, D.* The Theory of Incentives: The Principal-Agent Model. – Princeton University Press, 2002. – 421 p.
9. *Угольницкий Г.А.* Управление устойчивым развитием активных систем. – Ростов-на-Дону: Изд-во Южного федерального ун-та, 2016. – 940 с. [*Ugol'nickij, G.A.* Upravlenie ustojchivym razvitiem aktivnyh sistem. – Rostov-na-Donu: Izd-vo Yuzhnogo federal'nogo un-ta, 2016. – 940 s. (In Russian)]
10. *Угольницкий Г.А.* Методология и прикладные задачи управления устойчивым развитием активных систем // Проблемы управления. – 2019. – № 2. – С. 19–29. [*Ougolnitsky, G.A*. Methodology and Applied Problems of the Sustainable Management in Active Systems / Control Sciences. – 2019. – No. 2. – P. 19–29. (In Rusian)]
11. *Мазалов В.В.*Математическая теория игр и приложения. – СПб.:Лань, 2010. – 448 с. [*Mazalov, V.V.* Matematicheskaya teoriya igr i prilozheniya. – SPb.: Lan', 2010. – 448 s. (In Russian)]
12. *Петросян Л.А., Зенкевич Н.А., Шевкопляс Е.В*. Теория игр. – СПб.:БХВ-Петербург, 2011. – 432 с. [*Petrosyan, L.A., Zenkevich, N.A., Shevkoplyas, E.V*. Teoriya igr. – SPb.: BHV-Peterburg, 2011. – 432 s. (In Russian)]
13. *Basar, T., Olsder, G.Y*. Dynamic Non-Cooperative Game Theory. – SIAM, 1999. – 506 p.
14. *Differential* Games in Economics and Management Science / Dockner E., Jorgensen S., Long N.V., Sorger G. – Cambridge: Cambridge University Press, 2000. – 382 p.
15. *Gorelov, M.A., Kononenko, A.F.* Dynamic models of conflicts. III. Hierarchical games // Automation and Remote Control. – 2015. – Vol. 76, no. 2. – P. 264–277.
16. *Ougolnitsky, G.A., Usov, A.B.* Computer Simulations as a Solution Method for Differential Games // Computer Simulations: Advances in Research and Applications. Eds. M.D. Pfeffer and E. Bachmaier. – N.-Y.: Nova Science Publishers, 2018. – P. 63–106.
17. *Algorithmic* Game Theory. Ed. by N. Nisan, T. Roughgarden, E. Tardos, V. Vazirany. – Cambridge University Press, 2007. – 754 p.
18. *Dubey, P*. Inefficiency of Nash equilibria // Math. Operations Research. – 1986. – No. 11(1). – P. 1–8.
19. *Johari, R., Tsitsiklis, J.N*. Efficiency loss in a network resource allocation game // Math. Oper. Res. – 2004. – No. 29(3). – P. 407–435.
20. *Roughgarden, T.* Selfish Routing and the Price of Anarchy. – MIT Press, 2005. – 240 p.
21. *Papadimitriou, C.H*. Algorithms, games, and the Internet // Proc. 33rd Symp. Theory of Computing, 2001. – P. 749–753.
22. *Basar, T., Zhu,Q*. Prices of Anarchy, Information, and Cooperation in Differential Games // Dynamic Games and Applications. – 2011. – No. 1(1). – P. 50–73.
23. *Dahmouni, I., Vardar, B., Zaccour, G.* A fair and time-consistent sharing of the joint exploitation payoff of a fishery // Natural Resource Modeling. - 2019. - 32(2). -e12216.

24.*Zhang, W., Zhao, S., Wan, X.* Industrial digital transformation strategies based on differential games // Applied Mathematical Modeling. - 2021. - Vol.98. - P.90-108.
25.*Sharma, A., Jain, D*. Game-Theoretic Analysis of Green Supply Chain Under Cost-Sharing Contract with Fairness Concerns // International Game Theory Review. - 2021. - Vol. 23. - No.2. - 2050017. (32 p.)
26.*Мулен Э.* Кооперативное принятие решений: Аксиомы и модели. – М.: Мир, 1991. – 464 с. [*Mulen, E.* Kooperativnoe prinyatie reshenij: Aksiomy i modeli. – M.: Mir, 1991. – 464 s. (In Russian)]
27.*von Neumann, J., Morgenstern, O*. Theory of Games and Economic Behavior. – Princeton University Press, 1953. – 625 p.
28.*Petrosjan, L., Zaccour, G*. Time-consistent Shapley value allocation of pollution cost reduction // J. of Economic Dynamics and Control. – 2003. – Vol. 27, no. 3. – P. 381–398.
29.*Gromova, E.V., Petrosyan L.A*. On an approach to constructing a characteristic function in cooperative differential games // Automation and Remote Control. – 2017. – Vol. 78. – P. 1680–1692.
30.*Shapley, L*. A Value for *n*-person Games. Santa Monica, CA: The RAND Corporation, 1952.
31.*Мулен Э.* Теория игр с примерами из математической экономики. – М.:Мир, 1985. – 200 с. [*Mulen, E*. Teoriya igr s primerami iz matematicheskoj ekonomiki. – M.: Mir, 1985. – 200 s. (In Russian)]

Статья представлена к публикации членом редколлегии академиком РАН Д.А. Новиковым.

Поступила в редакцию 31.03.2022,
после доработки 29.06.2022.
Принята к публикации 1.07.2022.

Угольницкий Геннадий Анатольевич – д-р физ.-мат. наук, Южный федеральный университет, г. Ростов-на-Дону, ✉ gaugolnickiy@sfedu.ru.

AN APPROACH TO COMPARE ORGANIZATION MODES OF ACTIVE AGENTS AND CONTROL METHODS

G.A. Ougolnitsky

Southern Federal University, Rostov-on-Don, Russia

✉ gaugolnickiy@sfedu.ru

Abstract. When interacting, active agents can behave independently, cooperate, or have hierarchical relations. In turn, a hierarchical impact may be exerted by administrative or economic methods with or without feedback. These organizational modes and control methods are systematically described based on game-theoretic models with different information structures without uncertainty. It seems crucial to compare the payoffs of separate agents quantitatively with social welfare under the organization modes and control methods. A methodology is proposed to build the systems of social and individual preferences in normal form games and determine shares when allocating the cooperative payoff. A system of relative efficiency indices is developed for detailed quantitative assessment. This methodology is illustrated by several Cournot oligopoly models.

Keywords: inefficient equilibria, control and resource allocation methods, organization modes for active agents.

УДК 004.056.5

DOI: http://doi.org/10.25728/pu.2022.3.4

ИССЛЕДОВАНИЕ МЕТОДОВ АУТЕНТИФИКАЦИИ ОПЕРАТОРОВ В ПРОМЫШЛЕННЫХ СИСТЕМАХ УПРАВЛЕНИЯ[1]

В.Г. Промыслов, К.В. Семенков, Н.Э. Менгазетдинов

Аннотация. Рассматривается проблема аутентификации операторов в автоматизированных системах управления технологическими процессами (АСУ ТП) промышленными объектами критической информационной инфраструктуры на примере АСУ ТП атомных электростанций (АЭС). Проведен обзор применяемых в информационных системах общего назначения методов аутентификации – парольного, токена и биометрических – и анализируется их применимость для типовых условий работы оператора АСУ ТП. Анализ включает как экспериментальное тестирование парольного и биометрического методов аутентификации, так и экспертную оценку преимуществ и недостатков методов аутентификации в АСУ ТП. В ходе тестирования все исследуемые методы показали несколько худшие значения ошибок первого рода по сравнению с характеристиками, известными из доступных источников. Наилучшие результаты показал метод биометрической аутентификации по овалу лица. Однако и для него процент ошибок первого рода значителен, что может повлиять на доступность функции управления для легитимного пользователя. Сделан вывод о перспективности реализации в АСУ ТП многофакторной аутентификации на основе токена или парольной защиты в качестве блокирующего метода аутентификации с дополнительным биометрическим методом аутентификации по овалу лица с неблокирующей политикой безопасности.

Ключевые слова: аутентификация, биометрия, токен, пароль, АСУ ТП, оператор.

ВВЕДЕНИЕ

Для современных производств, в том числе опасных, например, атомных станций, транспорта, предприятий химической промышленности и т. д., характерна зависимость от цифровых автоматизированных систем управления. В контуре управления таких систем чаще всего присутствует человек (оператор), который воздействует как на сам объект управления, так и на систему управления через компьютеры, входящие в состав АСУ ТП.

В промышленных системах при решении задачи допуска доверенного оператора к управлению технологическим объектом возникают вопросы аутентификации. В частности, задачу аутентификации необходимо решать при наделении оператора правами на выполнение определенных действий с объектом управления, что в информационных технологиях принято называть авторизацией. Аутентификацию можно определить как «действия по проверке подлинности субъекта доступа и/или объекта доступа, а также по проверке принадлежности субъекту доступа и/или объекту доступа предъявленного идентификатора доступа и аутентификационной информации» [1].

Аутентифицирующий субъект выполняет проверку, сопоставляя некоторый идентификатор личности – например, общий секрет, который был заранее оговорен во время регистрации пользователя. Это может осуществляться с целью создания доверенных коммуникаций между сторонами или для наделения правами доступа к коммуникационным и вычислительным ресурсам системы в ходе авторизации.

Неавторизованные действия оператора могут не только к нарушить основные свойства информационной безопасности (целостность, доступность и конфиденциальность), но нанести экономический ущерб или вред здоровью людей. Дополнительно существует проблема отслеживания решений по управлению объектом, т. е. обеспечение неотказуемости от совершенных ранее действий. В целом данные проблемы вынуждают использовать более формальные методы аутентифи-

[1] Исследование (п. 2.3–2.5) выполнено при частичной финансовой поддержке РФФИ в рамках научного проекта № 19-29-06044.

кации даже в рутинных операциях в цифровых системах управления.

Решение задачи аутентификации операторов АСУ ТП критических объектов имеет особенности, связанные как с объектом управления, так и с политикой информационной безопасности [2]. Это отличает аутентификацию операторов АСУ ТП от аутентификации в информационных системах общего пользования. Перечислим основные из этих особенностей:

- наличие контролируемой физической зоны безопасности для доступа на объект снижает угрозу со стороны внешнего нарушителя в задаче аутентификации персонала; однако это не устраняет опасность, связанную с действиями внутреннего нарушителя, когда человек, допущенный в зону безопасности, но не имеющий полномочий оператора, пытается получить доступ к функциям операторского управления;
- приоритет доступности над другими свойствами информационной безопасности приводит к тому, что в задаче аутентификации ставятся жесткие ограничения на длительность процесса аутентификации и на вероятность ошибки первого рода (ошибочной негативной аутентификации объекта);
- в работе оператора могут возникнуть стрессовые ситуации (например, техногенная авария), отчего человек может забыть очевидные вещи, у него могут поменяться функциональные и внешние характеристики (задрожать руки, измениться тембр голоса, он может вспотеть и т. д.);
- из-за изменений внешней среды могут появиться помехи аутентификации; помеха – это некоторое изменение внешней среды, которое не приводит к разрушению объекта и немедленному отказу функций в АСУ ТП или на самом объекте, но вызывает неудобство для оператора, например, частичный выход из строя системы освещения, задымление, срабатывание системы пожаротушения, землетрясение и т. д.

Задачи аутентификации для промышленных систем, как и для обычных информационных систем, включают в себя и аутентификацию оператора (пользователя) на компьютере (цифровом устройстве), и аутентификацию самих компьютеров. Для информационных систем общего пользования задача аутентификации между компьютерами хорошо проработана [3, 4], но для промышленных систем, где применяются контроллеры и промышленные компьютеры, часто используются протоколы со слабыми механизмами аутентификации или даже вообще без аутентификации. Однако проблема обеспечения надежной аутентификации «компьютер – компьютер» в промышленных системах является скорее проблемой конкретных реализаций, чем научного исследования.

Протоколы, используемые для задачи аутентификации пользователей, гораздо менее безопасны, чем протоколы аутентификации между компьютерами, так как имеют дело с людьми и их лимитированными возможностями и слабостями [5]. В области информационной безопасности люди часто являются слабым звеном в защите.

Целью настоящей работы является выбор и обоснование методов и протокола аутентификации для применения их в задаче аутентификации операторов АСУ ТП. В работе анализируются основные методы и протоколы аутентификации пользователей и проводится их экспериментальное тестирование и анализ с учетом особенностей функционирования промышленных объектов и используемых политик информационной безопасности. В качестве примера промышленной системы управления для исследований выбрана разработанная в ИПУ РАН система верхнего блочного уровня АСУ ТП АЭС [6].

При проведении экспериментальных исследований предполагалось, что условия работы оператора на объекте и степень воздействия физических полей на людей и оборудование близки к нормальной офисной среде. Данное предположение для части промышленных объектов может нарушаться, но учет этих факторов лежит за рамками данной работы.

1. ПРОТОКОЛЫ И МЕТОДЫ АУТЕНТИФИКАЦИИ В АСУ ТП

Рассмотрим основные методы аутентификации пользователей и сравним их эффективность с точки зрения применимости для АСУ ТП.

Методы аутентификации пользователей можно разделить на классы, основываясь на трех основных вопросах [7]:

– Что вы знаете?

– Что у вас есть?

– Кто вы?

Часто три метода аутентификации ассоциируются с их характерными представителями: паролем, токеном и биометрическим признаком. Поэтому, описывая каждый из методов, мы будем приводить ссылку на их конкретные реализации. Во всех случаях объектом аутентификации является человек.

1.1. Парольные методы аутентификации

Пароль – это секретное слово, которое знает пользователь и, возможно, компьютер, на котором пользователь аутентифицируется. Это слово связано с ключом, по которому происходит аутентификация. В теории парольный метод аутентификации может быть весьма стойким: например, в случае применения расширенного стандарта шифрования [8] максимальная длина ключа составляет 256 бит, и чтобы угадать ключ, злоумышленнику в среднем потребуется более 10^{76} попыток, что займет слишком много времени и сейчас, и в обозримом будущем. В случае непосредственной зависимости пароля и ключа, используемого для аутентификации, для обеспечения высокой стойкости ключа необходим пароль сравнимой длины, а такое количество символов слишком велико для запоминания человеком. Поэтому на практике этот ключ хранится, например, в файле, защищенном более запоминающимся (то есть коротким) паролем. Основная уязвимость парольной защиты состоит в том, что запоминающийся пароль может быть угадан или найден злоумышленником [5, 9], а длинный, случайный, меняющийся пароль трудно запомнить, и тогда его могут записать и хранить в открытом виде. Считается [10, 11], что около 20 % пользователей из всех возможных сочетаний паролей используют не более пяти тысяч. Следовательно, пространство поиска для взлома системы снижается, и злоумышленник часто может сосредоточиться на этих пяти тысячах сочетаний.

Недостатков парольного метода аутентификации можно избежать, используя методы иных классов, в соответствии с которым в процессе аутентификации человек становится не субъектом, а объектом. Это методы на основе токенов и биометрические методы.

1.2. Методы аутентификации с применением токенов

Токен – это физическое устройство, которое выполняет или помогает провести аутентификацию. Также этот термин может относиться и к программным токенам, которые выдаются пользователю после успешной авторизации и являются ключом для доступа к службам. Токены могут быть как пассивными, так и активными (например, предоставляющими одноразовые коды доступа либо изменяющимися синхронно с мастером на хосте и т. д.) Безопасность токена обеспечивают различные средства защиты, например, футляр или специальное аппаратное обеспечение, которое отключает токен, если он скомпрометирован или если количество неудачных попыток аутентификации превысит выбранный порог.

В общем случае токен можно рассматривать как секрет, аналогичный паролю, за исключением того, что он сгенерирован машиной или сохранен машиной, поэтому он может быть длиннее, более случайным и, возможно, меняться во времени.

1.3. Биометрические методы

Для человека как пользователя биометрия – наиболее удобный и простой способ аутентификации, поскольку она является продолжением естественных способов установления личности.

Биометрия, или биометрические персональные данные, – это некоторая измеримая индивидуальная характеристика человеческого тела, достаточная для того, чтобы ее можно было использовать для аутентификации пользователя. Стандарт [1] определяет биометрические персональные данные как сведения, характеризующие физиологические и биологические особенности человека, на основании которых можно установить его личность.

Биометрия призвана неразрывно связать аутентификатор (признак) и владельца аутентификационного признака, что в случае пароля и токена принципиально сделать нельзя, так как их можно одолжить или украсть. Такая неразрывная связка признака аутентификации с носителем признака позволила бы обеспечить свойство неотказуемости. Напомним, что неотказуемость – это свойство, которое обеспечивает такие доказательства выполнения определенных действий, что вовлеченные стороны не могут впоследствии отклонить транзакцию как несанкционированную или заявить, что не выполняли этих действий. Однако биометрические характеристики, как и пароли, можно скопировать или подделать с бо́льшим или меньшим уровнем затрат и использовать для получения несанкционированного доступа. В целом, биометрия на текущем техническом уровне не может гарантировать свойство неотказуемости.

Биометрические данные, используемые для аутентификации, обычно классифицируются на физические и поведенческие типы. К физическому типу относят биометрию, основанную на стабильных характеристиках тела: отпечатках пальцев,

лице, радужной оболочке глаза, форме руки и др. К поведенческому типу относятся умения, приобретенные в процессе обучения, такие как рукописная подпись, динамика работы с клавиатурой, походка. Речь обычно классифицируется как поведенческий тип данных, потому что она является продуктом усвоенного поведения [12–14].

Биометрический метод аутентификации, как и прочие методы, может приводить к ошибкам [15], однако отношение пользователя к ошибкам при разных методах аутентификации различается. Пользователь может забыть или неправильно ввести пароль, может потерять токен. Эти ошибки неудобны, но пользователь осознает, что виноват он сам. В случае ошибки биометрической аутентификации пользователь не виноват и не может сам устранить проблему.

Биометрическая ошибка может возникнуть по разным причинам, например:

– грязный сканер,

– плохое освещение,

– система изначально запомнила неправильный шаблон для сравнения,

– система может плохо приспосабливаться к изменению окружающей среды (холод, дождь, солнечные блики, сухость и т. д.) или к естественному изменению биометрических характеристик пользователя (прическа, борода, порезанный палец и т. п.).

Один из последних примеров проблем биометрии связан с необходимостью носить маски в связи с пандемией.

Детальные требования к биометрическим методам аутентификации приведены в различных нормативных документах, например, в стандарте [16].

1.4. Протоколы аутентификации и их применение в АСУ ТП

В контексте задачи аутентификации пользователя мы будем рассматривать самый общий протокол аутентификации [17], устанавливающий правила обмена, которые необходимо применять для обеспечения аутентификации на основе двусторонне согласованной секретной информации.

Для информационных систем общего пользования популярными вариантами протокола аутентификации являются протокол «оклик – отзыв» [18]. Варианты протокола «оклик – отзыв» лежат в основе протоколов аутентификации Unix с модулями PAM [19] и MS Windows [20] и в их составе могут использоваться для аутентификации оператора АСУ ТП. Опыт авторов показывает, что применение протокола для парольного метода аутентификации ограничено из-за требований обеспечения доступности и сценариев работы оператора при выполнении критичных функций системы. Тем не менее, применение протокола возможно, например, для доступа к функции перепрограммирования цифрового устройства.

В реальных системах протоколы аутентификации для достижения высокого уровня защиты и обеспечения ее эшелонирования могут объединять несколько разных методов аутентификации [21]. Такая аутентификация называется многофакторной. Многофакторная аутентификация реализует алгоритм логического «И», когда для успешной аутентификации необходимо, чтобы аутентификация всеми методами прошла успешно. В настоящее время в подавляющем большинстве случаев при многофакторной аутентификации используется связка «физический токен – пароль» [22, 23]. Совместное применение пароля и биометрического идентификатора используют редко, потому что биометрию обычно применяют для удобства, чтобы не запоминать пароль.

Многофакторная аутентификация, сочетающая все три фактора, не нашла широкого применения, хотя такая реализация может потребоваться для доступа к функциям, где необходим высокий уровень защиты. В табл. 1 сведены основные преимущества и недостатки некоторых методов многофакторной аутентификации, а также экспертная оценка их пригодности для задач аутентификации оператора АСУ ТП по качественной шкале «плохо» – «удовлетворительно» – «хорошо».

Основные протоколы аутентификации легко модифицируются для применения в многофакторной аутентификации. Однако для реализации политики безопасности с высокими требованиями к доступности, характерными для АСУ ТП, введение дополнительной транзакции и сложности в протокол может привести к негативным последствиям.

Для АСУ ТП и других объектов с приоритетом доступности может быть реализована многофакторная аутентификация по сценарию логического «ИЛИ». В этом случае аутентификация считается выполненной, если хотя бы один из методов многофакторной аутентификации дал утвердительный ответ.

2. АНАЛИЗ И СРАВНЕНИЕ МЕТОДОВ АУТЕНТИФИКАЦИИ

2.1. Принципы сравнения

Сравним три основных метода аутентификации с точки зрения их применимости в АСУ ТП на примере их характерных представителей. Сравнение будем проводить по следующим признакам: стойкость, достоинства (удобство) и недостатки, качество распознавания. Сравнение будет в большинстве случаев качественным и в значительной мере основанным на практическом (экспертном) опыте, который может иметь субъективный характер; набор показателей для сравнения взят из работы [7].

В табл. 2 приведены основные атрибуты трех методов аутентификации.

Таблица 1

Сравнение методов многофакторной сильной защиты аутентификации пользователя для получения более сильной защиты в АСУ ТП

Комбинация методов аутентификации	Преимущества	Недостатки	Пример	Оценка применимости для АСУ ТП
«Что вы знаете?» + «Что у вас есть?»	Потеря токена не приводит к его немедленной компрометации, так как он защищен паролем	Необходимо иметь токен и помнить пароль	Банковская карта + ПИН	Удовлетворительно
«Что у вас есть?» + «Кто вы?»	Потеря токена не приводит к его немедленной компрометации, так как он защищен уникальностью его владельца	Необходимо иметь токен. Может приводить к ложному отказу при аутентификации из-за несовершенства биометрических методов	Пропуск с чипом и фотографией	Хорошо
«Что вы знаете?» + «Кто вы?»	Подмена идентификатора пользователя (использование двойника) не приведет к ложной аутентификации	Может приводить к ложному отказу при аутентификации из-за несовершенства биометрических методов	Пароль + датчик отпечатка пальца на компьютере	Удовлетворительно
«Что вы знаете?» + «Что у вас есть?» + «Кто вы?»	Все три метода работают последовательно	Нужно иметь токен и помнить пароль. Может приводить к ложному отказу при аутентификации из-за несовершенства биометрических методов	Аутентификация для доступа на критически важный объект, включающая пропуск с чипом и фотографией, на входе в объект, биометрический сканер по отпечатку пальца для доступа в помещение и пароль для доступа к компьютеру	Плохо

Таблица 2

Три основных метода аутентификации пользователя и их атрибуты

Методы аутентификации	Что вы знаете?	Что у вас есть?	Кто вы?
Реализация метода	Пароль	Токен	Биометрия
На чем основана аутентификация	Знание секрета	Владение нужным объектом	Характерные признаки субъекта
Вид защиты	Сохранение тайны	Физическая безопасность	Уникальность субъекта
Примеры уязвимости	Можно подсмотреть или угадать	Можно потерять, может быть украден	Можно подделать; трудно сменить, в случае компрометации

2.2. Практическая энтропия ключа

Сравнение стойкости различных методов аутентификации – непростая задача, так как в зависимости от реализации метода аутентификации используемый в протоколе ключ может иметь различную связь с исходными данными, предоставляемыми методом. Например, для парольного метода ключ может просто представлять собой хранимую копию пароля, или его хеш-код, или проверочные значения, которые зависят от паролей, но не могут быть непосредственно использованы злоумышленником для аутентификации. Для других методов аутентификации вместо пароля может использоваться некоторое значение, полученное от токена или устройства биометрии.

Поэтому для оценки стойкости методов аутентификации воспользуемся метрикой, основанной на энтропии ключа, который может быть непосредственно получен из исходных данных (пароля, информации хранимой в токене, или биометрических данных). Исследования энтропии ключей, полученных на основе паролей, проведенные в крупных IT-компаниях, имеющих большой объем персональных данных (Yahoo, Google) [5], показывают, что энтропия ключа составляет 10–20 бит. Причем отмечается, что применение хеш-кода уменьшает энтропию ключа, который скорее ближе к левой границе (т. е. к 10 битам), так как хеш-код оптимизирован для обеспечения быстродействия, что уменьшает стойкость ключа. Хотя, например, реализации алгоритмов хеширования SHA1 (*Secure Hash Algorithm* 1) [24] являются настраиваемыми и могут быть весьма стойкими.

Ранние исследования [5] показывали, что энтропия ключа и, следовательно, стойкость метода для биометрического и парольного видов защиты примерно одинакова, но более поздние работы свидетельствуют о том, что биометрические методы позволяют получить степень защиты в два-три раза лучшую, чем парольные [25].

Специальные исследования по стойкости парольного метода для операторов АСУ ТП авторам неизвестны. Однако представляется целесообразным принять значение стойкости используемых паролей ближе к нижней границе (простые пароли). Хотя политика безопасности промышленного объекта может и должна содержать требования к стойкости паролей и процедуру управления ими, применение слишком сложного (стойкого) пароля невозможно из-за требований к доступности системы и наличия стрессовых ситуаций в работе оператора.

Энтропия ключа, получаемого на основе данных и содержащегося в токене, может быть весьма большой при использовании алгоритмов, аналогичных методам аутентификации «компьютер – компьютер». Например, в работе [26] приведены значения энтропии ключа до 128 бит. Однако нужно учитывать вероятность кражи токена, которая может оказаться значительной, особенно при наличии злого умысла.

2.3. Основные характеристики качества распознавания

Для оценки качества распознавания традиционно используются две основные характеристики: ошибки первого и второго рода, часто обозначаемые английскими аббревиатурами FRR (*False Rejection Rate*) и FAR (*False Acceptance Rate*).

Первое число характеризует вероятность отказа в доступе человеку, имеющему допуск. Второе – это вероятность принятия ложного решении о положительной аутентификации. Чем лучше система, тем при одинаковых значениях FAR меньше значение FRR. Параметр FAR имеет смысл приводить только для биометрического метода аутентификации, так как для остальных методов аутентификации значение отражает способности человека (набор и запоминание парольной фразы) или надежность аппаратной реализации.

У любого метода аутентификации есть некоторая доля ошибок, связанная с отказом аппаратуры, например, считывателя токена или клавиатуры, однако, как показывает практика, она пренебрежимо мала. Качество биометрической аутентификации является наиболее неустойчивой характеристикой, так как существенно зависит от конкретного человека. В табл. 3 содержатся типовые характеристики различных способов биометрического метода аутентификации, найденные авторами в литературе. Типовые характеристики демонстрируют только тенденцию, сравнение реализаций и алгоритмов для биометрического метода выходит за рамки настоящей работы.

Таблица 3

Типовые параметры ошибок для биометрического метода

Тип биометрии	FAR	FRR	Размер выборки (согласно работе [27])	Источник
Распознавание по отпечатку пальца	10^{-3}	10^{-2}	$5 \cdot 10^6$	[27]
Распознавание по овалу лица	0,058		$12 \cdot 10^6$	[27]
Распознавание по сетчатке глаза	0,059		$500 \cdot 10^3$	[27]

Чтобы исследовать практические аспекты применимости коммерчески доступных устройств для биометрической аутентификации операторов АСУ ТП, мы провели дополнительное тестирование, в ходе которого имитировались некоторые характерные условия работы оператора АСУ ТП. Результаты приведены в п. 3.4.

2.4. Практическое тестирование пригодности методов аутентификации для операторов АСУ ТП

Авторами были проведены испытания парольных и некоторых реализаций биометрических методов аутентификации в типичных сценариях работы оператора АСУ ТП на промышленном объекте. Тестирование метода аутентификации с токеном не проводилось, так как предполагалось, что его свойства определяются возможностями, заложенными при проектировании и изготовлении токена, и они стабильны в процессе эксплуатации.

В табл. 4 приведены используемые коммерческие устройства и тип биометрической аутентификации, доступный на устройстве. Использовались устройства, официально поставляемые в Российскую Федерацию и не имеющие лицензионных ограничений на момент написания статьи. Для тестирования биометрических методов аутентификации выбирались устройства и алгоритмы, доступные массовому потребителю, применяемые для аутентификации в мобильных устройствах. Для тестов парольной аутентификации использовались типовые клавиатуры для персональных компьютеров, которые также используются на рабочих местах операторов АСУ ТП. Как показывает опыт авторов, именно массовые продукты в основном применяются в реализации технических мер защиты для промышленных систем.

Для каждого из методов проводилось не менее 50 тестов. Каждый тест проводила группа из двух испытателей, один (оператор) по команде другого испытателя делал попытку аутентифицироваться с применением одного из методов аутентификации.

Таблица 4

Устройства, используемые в ходе тестирования

Устройство	Тип аутентификации
HONOR 10. Android version 10	Распознавание по отпечатку пальца; распознавание по овалу лица
MI 5S Plus. Android version 8. MIUI Global 10.2	Распознавание по отпечатку пальца
Персональный компьютер с мембранной клавиатурой	Парольная защита

В ходе тестирования испытатели в группе периодически менялись ролями. В каждом тесте измерялось время, за которое была проведена аутентификация, и число затраченных попыток до удачной аутентификации. Тесты проводились как в обычных, нормальных внешних условиях, так и при наличии помех, осложняющих аутентификацию (табл. 5).

Таблица 5

Типы вводимых при тестировании помех

Обозначение помехи	Описание
Помеха 1	Нагретые руки
Помеха 2	Чехол на сенсоре
Помеха 3	Вода тонким слоем на пальце
Помеха 4	Охлаждение пальца
Помеха 5	Маска на лице
Помеха 6	Изменение угла между камерой и лицом объекта
Помеха 7	Изменение освещенности
Помеха 10	Ввод пароля стоя
Помеха 11	Ввод пароля в перчатках
Помеха 12	Ввод пароля «вслепую»
Помеха 13	Ввод пароля при физической помехе (один из испытателей подталкивал другого)

Для парольных методов аутентификации после каждых десяти тестов менялся пароль в соответствии с выбранным уровнем сложности.

Результаты испытаний приведены в табл. 6.

Таблица 6

Тестирование методов аутентификации

Тест (Условия)	Результат	
	Время максимальное, минимальное и среднее, с	Максимальное число попыток для успешной аутентификации
Простой пароль (5 символов; базирующийся на словарном слове; нормальные условия)	2,63; 1,82; 2,1	1
Простой пароль (5 символов; базирующийся на словарном слове; помеха 8)	6,34; 2,1; 2,3	2
Простой пароль (5 символов; базирующийся на словарном слове; помеха 9)	9,29; 1,68; 4,2	3
Простой пароль (5 символов; базирующийся на словарном слове; помеха 10)	12,64; 2,37; 5,62	4
Простой пароль (5 символов; базирующийся на словарном слове; помеха 11)	20,33; 2;06; 6,12	6
Сложный пароль (не менее 9 символов; большие и маленькие буквы, цифры; нормальные условия)	24,5; 5,33; 9,1	3
Сложный пароль (не менее 9 символов; большие и маленькие буквы, цифры; помеха 10)	11,59; 5,98; 6,6	1
Сложный пароль (не менее 9 символов; большие и маленькие буквы, цифры; помеха 11)	49,03; 9,1; 12;6	3
Сложный пароль (не менее 9 символов; большие и маленькие буквы, цифры; помеха 12)	95,31; 7,8; 23,4	11
Сложный пароль (не менее 9 символов; большие и маленькие буквы, цифры; помеха 13)	46,39; 8,1; 24,3	4
Отпечаток пальцев (нормальные условия)	3,92; 0,99; 1,44	2
Отпечаток пальцев (помеха 1)	1,23; 1,09; 1,2	1
Отпечаток пальцев (помеха 2)	2,69; 1,09; 1,82	3
Отпечаток пальцев (помеха 3)	9,48; 1,05; 3,61	6
Отпечаток пальцев (помеха 4)	3,59; ,2,1; 1,7	3
Овал лица (нормальные условия)	2,87; 1,85; 1,91	1
Овал лица (помеха 5)	4,23; 1,7; 2,64	2
Овал лица (помеха 6)	5,42; 1,64; 3,26	2
Овал лица (помеха 7)	2,09; 0,99; 1,2	1

Для парольного метода получена относительно высокая ($\sim 10^{-1}$) вероятность отказа в доступе человеку, имеющему право доступа, при наличии помех. Вероятность ошибки первого рода возрастает при увеличении сложности пароля. Большая вероятность ошибки оператора при вводе пароля, особенно сложного, при наличии помехи приводит к тому, что оператор вынужден неоднократно (в тестах это значение достигало 11 раз) вводить пароль для успешной аутентификации. Время аутентификации в этом случае вырастает на порядок при типовом значении около двух-трех секунд для простого пароля и около пяти секунд для сложного пароля.

В АСУ ТП такие задержки могут быть критическими. Это может стать основанием для отказа от парольной защиты в пользу токенов, биометрических методов или организационных и физических мер аутентификации и их комбинации.

Среди биометрических методов идентификации наилучшие результаты во время тестирования были получены для идентификации по овалу лица. Для биометрических методов аутентификации проводилось дополнительное тестирование с це-

лью выявить возможность ложной аутентификации. Ни по одному из используемых биометрических методов не удалось добиться ложной аутентификации в пределах средств, доступных обычному пользователю ($FAR = 0$). Это не означает, что биометрическая аутентификация в условиях работы оператора АСУ ТП свободна от ошибок второго рода и что полученные данные противоречат типовым значениям, приведенным в предыдущем разделе. Причинами могут быть как ограниченность используемой выборки, так и то, что обход систем защиты требует знания как особенностей реализаций используемых алгоритмов для сравнения биометрического шаблона, так и, возможно, специального реквизита.

Полученная в практических условиях ошибка первого рода для биометрического метода приблизительно на порядок превышает типовые значения, что в основном связано с наличием помех. Данные результаты следует учитывать при использовании биометрических методов для АСУ ТП.

2.5. Анализ применимости методов аутентификации в АСУ ТП

Проанализируем основные проблемы, связанные с применением каждого метода для типовых условий работы оператора промышленной системы управления.

- Аутентификаторы, основанные на знаниях («Что вы знаете?»), включают в себя секретную информацию (пароль), но такая информация является не столько секретной, сколько «неизвестной». Данной информации можно дать приблизительно такое определение – «скрытая от большинства людей». Недостатком секретов является то, что при каждом их использовании для аутентификации они становятся все менее секретными. К тому же «большинство людей» часто означает «большинство честных людей», а для злоумышленника при некотором усилии (например, путем применения средств социальной инженерии) такая информация перестает быть закрытой. Для систем управления АСУ ТП характерен высокий уровень доверия между пользователями, возникающего как в результате отбора персонала, так и в ходе производственной деятельности, когда люди выполняют в течении долгого времени общую работу. Поэтому у злоумышленника, проникшего в изолированный коллектив, упрощается задача получения знаний, включая секретные (пароли), от других членов этого коллектива.

- Аутентификаторы-объекты («Что у вас есть?») – это материальные объекты, наиболее характерный пример – токен. Основной недостаток аутентификатора-объекта тот же, что и у предметов, которые непосредственно им предшествовали – физических ключей. Если ключ утерян, то любой, кто его нашел, может обойти систему защиты. В этом смысле слабости объектных аутентификаторов аналогичны парольной защите: злоумышленник может использовать потерянный или украденный токен. Как и при парольной защите, пользователи АСУ ТП склонны доверять друг другу. Однако, в отличие от парольной защиты, при утере физического объекта владелец узнает об этом при первом обращении к нему и сможет принять меры для скорейшей нейтрализации угрозы.

- Аутентификаторы на основе идентификаторов («Кто вы?») привязаны к одному человеку, они уникальны. Данная категория включает в себя все биометрические методы аутентификации, такие как отпечаток пальца, сканирование глаз и радужной оболочки, голосовой отпечаток или подпись. Биометрический метод аутентификации имеет сравнительно высокую степень защиты в части копирования и подделки и очевидно не может быть утерян [28].

Суммируя вышесказанное, можно заключить, что ни один из этих методов аутентификации не идеален, они имеют некоторый набор «врожденных» недостатков. В табл. 7 приведены характерные уязвимости различных методов аутентификации применительно к задачам АСУ ТП.

Легко заметить, что в контексте политики безопасности АСУ ТП возможности для атак на систему аутентификации неравнозначны. Если на предприятии имеется постоянно действующая система обнаружения вторжений и есть должностные лица, ответственные за компьютерную безопасность, то атаки перебором должны легко обнаруживаться, после чего должны приниматься соответствующие меры. В то же время, атаки, связанные с кражей токена или пароля, особенно последние, весьма вероятны, учитывая высокую степень доверия, которая обычно устанавливается между пользователями, допущенными в зону безопасности на промышленном объекте. Для АСУ ТП, по мнению авторов, желательно применение неблокирующих методов защиты от многих атак, связанных с попытками обойти процедуру аутентификации. Неблокирующие методы защиты прежде всего призваны привлечь внимание офицера по безопасности к нештатной ситуации, оставляя на усмотрение человека принятие мер в ответ на событие безопасности.

Таблица 7

Компрометация свойств безопасности при различных методах аутентификации

Компрометируемое свойство безопасности	Метод аутентификации	Пример атаки	Типовые методы защиты
Неопровержимость	Пароль, токен	Потеря или кража токена	Персональная ответственность пользователя за потерю (административная мера защиты)
	Биометрия	Подделка	Многофакторная аутентификация
Обнаружение компрометации	Пароль, биометрия	Подделка, кража	Информирование пользователя об использовании аутентификатора (*last login*)
	Токен		Обнаружение пропажи пользователем
Подмена пользователя при начальной идентификации пользователя	Пароль	Передача данных неавторизованному лицу. Пароль по умолчанию	Личная явка пользователя. Политика управления паролями
	Токен	Передача токена неавторизованному лицу	Личная явка пользователя
	Биометрия	Замена пользовательских биометрических данных	
Утечка данных при обновлении идентификатора	Пароль	Передача данных неавторизованному лицу. Пароль по умолчанию	Политика управления паролями. Многофакторная аутентификация
	Токен	Передача токена неавторизованному лицу	Личная явка пользователя и сдача токена если он сломан, а не утерян
	Биометрия	Замена пользовательских биометрических данных при компрометации	Политика управления персональной информацией
Отказ в обслуживании	Пароль, токен, биометрия	Многократные неудачные попытки для блокирования доступа	Неблокирующая политика безопасности с нотификацией офицера по безопасности
Ложная аутентификация	Пароль, токен, биометрия	Атака с повторной передачей сообщений	Протокол «оклик – отзыв»
	Пароль	Атака перебором	Блокирующая политика безопасности при некотором числе неудачных попыток аутентификации

2.6. Качественный анализ и сравнение методов аутентификации для АСУ ТП

Для сравнения методов аутентификации можно предложить различные показатели. Рассмотрим три высокоуровневых показателя, которые традиционно используются для сравнения методов аутентификации [5]:

– удобство использования,

– удобство развертывания,

– безопасность.

В каждом из наборов высокоуровневых показателей выделим набор показателей более низкого уровня. Значения всех показателей в наборе будут оцениваться по ранговой шкале: «хорошо» – 2, «удовлетворительно» – 1, «плохо» – 0. Значение высокоуровневого показателя вычислим как сумму отдельных показателей в наборе.

Рассмотрим группы показателей «удобство использования» (табл. 8) и «удобство развертывания» (табл. 9). В табл. 10, в свою очередь, представлен набор показателей из группы «безопасность» в контексте того, какие виды атак может предотвратить метод аутентификации.

Таблица 8

Показатели из группы «удобство использования» для различных методов аутентификации для применения в АСУ ТП

Показатель	Пароль	Токен	Биометрия
Легкость взаимодействия со схемой аутентификации для пользователя	Удовлетворительно	Хорошо	Удовлетворительно
Простота обучения: пользователи, не знакомые с методом, могут понять его и освоить без особых проблем	Хорошо	Хорошо	Удовлетворительно
Нечастые ошибки: задача, которую пользователи должны выполнить для аутентификации, обычно завершается успешно, если ее выполняет законный и честный пользователь	Удовлетворительно. Пользователи обычно успешно справляются, но при условии слабого пароля	Хорошо	Удовлетворительно
Масштабируемость для пользователей: использование схемы для сотен учетных записей не увеличивает нагрузку на пользователя	Плохо. Люди часто повторно используют пароли или создают простую схему уникальности для каждого сайта для базового пароля	Удовлетворительно. Проблема выбора одного токена из множества имеющихся в наличии не всегда тривиальна	Хорошо
Простое восстановление после компрометации	Хорошо. Преимущество паролей – их легко сбросить	Удовлетворительно	Плохо
Необходимость что-то иметь при себе	Хорошо	Плохо	Хорошо
Сумма	8	8	7

Таблица 9

Показатели группы «удобство развертывания» для различных методов аутентификации для применения в АСУ ТП

Показатель	Пароль	Токен	Биометрия
Простота внедрения метода аутентификации в реальные системы	Хорошо	Хорошо	Удовлетворительно
Совместимость с сервером аутентификации	Хорошо. Серверы аутентификации изначально разработаны для парольных методов аутентификации	Хорошо. С точки зрения сервера, ключ, полученный от токена, не отличим от ключа, полученного через пароль	Удовлетворительно. Возможно, необходимо внедрить защиту биометрической информации, если того требует законодательство
Совместимость с клиентским компьютером	Хорошо. Клиенты аутентификации изначально разработаны для парольных методов аутентификации	Удовлетворительно. Требуется поддержка со стороны специальных устройств	Удовлетворительно. Требуется поддержка со стороны специальных устройств

См. окончание табл. 9

Окончание табл. 9

Показатель	Пароль	Токен	Биометрия
Доступность. Наличие ограничений на использование в зависимости от конкретного индивидуума	Хорошо	Хорошо	Плохо Доступность метода может меняться в зависимости от состояния здоровья, наличия травм. Люди с ограниченными возможностями могут быть не способны использовать определенные методы биометрической аутентификации. Для операторов АСУ ТП это может быть актуально если в смене присутствует временный персонал, не прошедший медицинский отбор, аналогичный тому, который проходят операторы
Возможность обновления	Удовлетворительно	Хорошо. При условии административной поддержки	Плохо. Биометрия меняется очень медленно (голос, лицо) или не меняется совсем (отпечатки пальцев)
Сумма	9	9	3

Таблица 10

Показатели группы «безопасность» для различных методов аутентификации для применения в АСУ ТП

Показатель	Пароль	Токен	Биометрия
Сопротивляемость наблюдению со стороны	Плохо. Злоумышленник может выдавать себя за пользователя после того, как он один или несколько раз наблюдает за его аутентификацией путем повторения наблюдения более, допустим, 10–20 раз. Атаки включают в себя серфинг через плечо, видеосъемку клавиатуры, запись звуков нажатия клавиш или телевизионное изображение клавиатуры и т. д.	Хорошо	Хорошо
Сопротивляемость методам социальной инженерии	Хорошо. Знакомому (или опытному хакеру) невозможно выдать себя за конкретного пользователя, используя знание личных данных (дата рождения, имена родственников и т. д.).	Хорошо	Хорошо
Сопротивляемость простому угадыванию	Удовлетворительно. Зависит от длины пароля	Хорошо	Хорошо
Сопротивляемость атакам со стороны субъектов внутри компьютерной системы	Удовлетворительно. Зависит от длины пароля	Хорошо	Удовлетворительно. Биометрические методы, как и пароль, имеют невысокую энтропию и длину ключа
Сумма	4	8	7

В табл. 11 приведены суммарные оценки методов аутентификации по всем группам показателей. Результаты проведенного анализа демонстрируют, что токен может быть наиболее сбалансированным методом, если он используется в качестве единственного метода аутентификации.

Таблица 11

Суммарная оценка каждого из методов по всем группам показателей

	Пароль	Токен	Биометрия
Сумма	21	25	17

ЗАКЛЮЧЕНИЕ. ОБСУЖДЕНИЕ РЕЗУЛЬТАТОВ

Подчеркнем, что в задачу данной работы входило не собственно исследование известных на сегодняшний момент методов аутентификации, а рассмотрение особенностей их применения для решения задачи аутентификации оператора АСУ ТП.

Был учтен накопленный опыт использования методов аутентификации для информационных систем общего назначения. Обзор доступных источников показывает, что на данный момент степени защиты, предоставляемые каждым из методов, сравнимы. Общая проблема заключается в том, что, если аутентификатор неудобен, им либо не пользуются, либо пользуются недолжным образом, что может привести к уязвимости. На практике это означает, что если для доступа к разным рабочим местам или для выполнения разных операций операторам АСУ ТП будет нужно запоминать несколько паролей, то они будут выбирать простые пароли или пароли, связанные простой зависимостью. В политике безопасности предприятия могут предъявляться определенные требования к паролям (например, длина, использование специальных символов) для увеличения энтропии. Однако мы полагаем, что такие требования к паролям редко приводят к увеличению энтропии ключа. Компетентный взломщик может учесть ограничения паролей, накладываемые политикой безопасности, при составлении таблиц хеш-кодов, используемых для взлома системы, либо, что еще проще, может просто подсмотреть пароль, так как сложный пароль оператор будет записывать на бумаге и носить с собой.

Проведенные опыты показали достаточно высокий процент ошибок первого рода (неправильный набор пароля) при наличии помехи даже при достаточно простом пароле. Поэтому при определении политики безопасности парольной защиты должно учитываться влияние ошибок первого рода на свойство доступности в системе, что автоматически ограничивает как частоту смены пароля, так и его сложность.

Биометрические методы аутентификации на практике при типовых условиях и помехах для работы оператора показали значения ошибок первого рода в несколько раз хуже теоретических ($\leq 10^{-2}$). Основываясь на результатах приведенного тестирования, наиболее перспективным из исследованных биометрических методов представляется контроль по овалу лица. Однако даже он имеет высокий процент ошибок, поэтому его не рекомендуется объединять с блокирующей политикой безопасности. Предлагается использовать его при многофакторной аутентификации вместе с парольным методом или токеном. Выбирая методы многофакторной аутентификации, стоит принимать во внимание то, что энтропия ключа для биометрической и парольной защиты приблизительно одинакова, но для пароля энтропия ограничена возможностями человеческой памяти, а для биометрии – текущей аппаратной реализацией сканеров и датчиков биометрии.

Применение токена устраняет проблему запоминания паролей, но пользователь должен иметь с собой физический носитель, что иногда неудобно, так как токен можно украсть, скопировать или потерять.

Можно сделать вывод, что для аутентификации оператора АСУ ТП возможно построить систему защиты, использующую различные методы и их комбинации. Операторы АСУ ТП, как правило, работают в помещении с контролируемым физическим доступом. Исходя из этого, в пределах контролируемой зоны безопасности можно установить процедуру доступа на основе токенов с дополнительным видеоконтролем со стороны службы безопасности. По мнению авторов, перспективной является двухфакторная аутентификация с блокирующей политикой безопасности для токена и неблокирующей для биометрического метода распознавания по овалу лица.

ЛИТЕРАТУРА

1. *ГОСТ* Р 58833-2020. Защита информации. Идентификация и аутентификация. Общие положения. [*GOST* R 58833-2020. Zashchita informacii. Identifikaciya i autentifikaciya. Obshchie polozheniya. (In Russian)]
2. *Исхаков С.Ю.,* Шелупанов А.А., Исхаков А.Ю. Имитационная модель комплексной сети систем безопасности // Доклады Томского государственного университета систем управления и радиоэлектроники. – 2014. – № 2(32). – С. 82–86. – EDN SEBGNR. [*Iskhakov, S.Yu., Shelupanov, A.A., Iskhakov, A.Yu.* Imitacionnaya model' kompleksnoj seti sistem bezopasnosti // Doklady Tomskogo gosudarstvennogo universiteta sistem upravleniya i radioelektroniki. – 2014. – No. 2(32). – P. 82–86. – EDN SEBGNR.
3. *Dierks, T. and Rescorla, E.* The Transport Layer Security (TLS) Protocol Version 1.1. – RFC 4346, 2006.
4. *Conte de Leon, D., Makrakis, G.M., Kolias, C.* "Cybersecurity," in Resilient Control Architectures and Power Systems. – IEEE, 2022. – P. 89–111. – DOI: 10.1002/9781119660446.ch7.
5. *Hu, G.* On Password Strength: A Survey and Analysis. – Springer International Publishing, 2018. – DOI: 10.1007/978-3-319-62048-0_12.
6. *Менгазетдинов Н.Э., Полетыкин А.Г., Промыслов В.Г.* и др. Комплекс работ по созданию первой управляющей системы верхнего блочного уровня АСУ ТП ДЛЯ АЭС

«БУШЕР» на основе отечественных технологий. – М.: ИПУ РАН. – 2013. – 95 с. [*Mengazetdinov, N.E., Poletykin, A.G., Promyslov, V.G.* i dr. Kompleks rabot po sozdaniyu pervoj upravlya-yushchej sistemy verhnego blochnogo urovnya ASUTP DLYA AES «BUSHER» na osnove otechestvennyh tekhnolo-gij. – M.: IPU RAN. – 2013. – 95 s. (In Russian)]

7. *O'Gorman, L.* Comparing Passwords, Tokens, and Biometrics for User Authentication / Proceedings of the IEEE. – 2003. – Vol. 91, no. 12. – P. 2021–2040. – DOI: 10.1109/JPROC.2003.819611.
8. *Dworkin, M., Barker, E., Nechvatal, J.,* et al. Advanced Encryption Standard (AES). – Federal Inf. Process. Stds. (NIST FIPS), National Institute of Standards and Technology, Gaithersburg, MD, 2001. – DOI: 10.6028/NIST.FIPS.197.
9. *Jobusch, D.L., Oldehoeft, A.E.* A Survey of Password Mechanisms: Weaknesses and Potential Improvements. Part 1 // Computers & Security. – 1989. – Vol. 8, iss. 7. – P. 587–604. – DOI: 10.1016/0167-4048(89)90051-5.
10. *The 200 Worst* Passwords of 2021 Are Here and Oh My God. – https://gizmodo.com/the-200-worst-passwords-of-2021-are-here-and-oh-my-god-1848073946 (дата обращения 7.03.2022).
11. *Most* Common Passwords of 2021. – https://nordpass.com/most-common-passwords-list/ (дата обращения 7.03.2022).
12. *Köhler, D., Klieme, E., Kreuseler, M.,* et al. Assessment of Remote Biometric Authentication Systems: Another Take on the Quest to Replace Passwords / 2021 IEEE 5th International Conference on Cryptography, Security and Privacy (CSP). – 2021. – P. 22–31. – DOI: 10.1109/CSP51677.2021.9357504.
13. *Alanezi, N.A., Alharbi, N.H., Alharthi, Z.S., and Alhazmi, O.H.* POSTER: A Brief Overview of Biometrics in Cybersecurity: A Comparative Analysis / 2020 First International Conference of Smart Systems and Emerging Technologies (SMARTTECH). – 2020. – P. 257–258. – DOI: 10.1109/SMART-TECH49988.2020.00067.
14. *Антонова В.М., Балакин К.А., Гречишкина Н.А., Кузнецов Н.А.* Разработка системы аутентификации с использованием верификации диктора по голосу / Информационные процессы. – 2020. – Т. 20, № 1. – С. 10–21. [*Antonova, V.M., Balakin, K.A., Grechishkina, N.A., Kuznetsov, N.A.* Development of an authentication system using voice announcer verification / Informacionnye processy. – 2020. – Vol. 20, no. 1. – P. 10–21. (In Russian)]
15. Machine Learning Masters the Fingerprint to Fool Biometric Systems: https://engineering.nyu.edu/news/machine-learning-masters-fingerprint-fool-biometric-systems (дата обращения 12.07.2022)
16. *ГОСТ* Р 52633.0-2006. Требования к средствам высоконадежной биометрической аутентификации. [*GOST* R 52633.0-2006. Trebovaniya k sredstvam vysokonadezhnoj biometricheskoj autentifikacii. (In Russian)]
17. *Mao B.* Современная криптография: теория и практика. Пер. с англ. – М.: Издательский дом «Вильямс». – 2005. – 768 с. [*Mao, V.* Sovremennaya kriptografiya: teoriya i praktika. Per. s angl. – M.: Izdatel'skij dom «Vil'yams». – 2005. – 768 s. (In Russian)]
18. *Burrows, M., Abadi, M., and Needham, R.M*. A Logic for Authentication / DEC System Research Center Technical Report. – 1989. – No. 39.
19. *Krawczyk, H., Bellare, M., Canetti, R.* HMAC: Keyed-Hashing for Message Authentication. – RFC 2104, 1997.
20. *Agorithms* for Challenge/Response Authentication. – https://docs.microsoft.com/en-us/openspecs/windows_protocols/ms-cifs/4d1a2cb0-0951-462a-8582-121fd1afe28e (дата обращения 7.03.2022).
21. *Исхаков А.Ю.* Система двухфакторной аутентификации на основе QR-кодов / Безопасность информационных технологий. – 2014. – Т. 21. – № 3. – С. 97–101. – EDN TRZJLN. [*Iskhakov, A.Y.* Two-Factor Authentication System Based on QR-Codes / IT Security (Russia). – 2014. – Vol. 21, no. 3. – P. 97–101. (In Russian)]
22. *Giri, D., Sherratt, R.S., Maitra, T., and Amin, R.* Efficient Biometric and Password Based Mutual Authentication for Consumer USB Mass Storage Devices / IEEE Transactions on Consumer Electronics. – 2015. – Vol. 61, no. 4. – P. 491–499. – DOI: 10.1109/TCE.2015.7389804.
23. *Razaque, K.K. Myrzabekovna, S.Y. Magbatkyzy, M.*, et al. Secure Password-Driven Fingerprint Biometrics Authentication / 2020 Seventh International Conference on Software Defined Systems (SDS). – 2020. – P. 95–99. –DOI: 10.1109/SDS49854.2020.9143881.
24. *Eastlake, D., Jones, P.* US Secure Hash Algorithm 1 (SHA1). – RFC 3174, 2001.
25. *Dinca, L. and Hancke, G.* User-Centric Key Entropy: Study of Biometric Key Derivation Subject to Spoofing Attacks // Entropy. – 2017. – Vol. 19, no. 2. – DOI: 10.3390/e19020070.
26. *Fouque, P.-A., Pointcheval, D., Zimmer, S.* HMAC is a Randomness Extractor and Applications to TLS / Proceedings of the 3rd ACM Symposium on Information, Computer and Communications Security (ASIACCS '08). – Tokyo, Japan, 2008. – P. 21–32.
27. *Jain, A.K., Deb, D., and Engelsma, J.J.* Biometrics: Trust, but Verify / IEEE Transactions on Biometrics, Behavior, and Identity Science. – 2021. – DOI: 10.1109/TBIOM.2021.3115465.
28. *Alsellami, B., Deshmukh, P.D., Ahmed, Z.A.T.* Overview of Biometric Traits / 2021 Third International Conference on Inventive Research in Computing Applications (ICIRCA). – 2021. – P. 807–813. DOI: 10.1109/ICIRCA51532.2021.9545069.

Статья представлена к публикации членом редколлегии А.О. Калашниковым.

Поступила в редакцию 6.05.2022,
после доработки 30.06.2022.
Принята к публикации 11.07.2022.

Промыслов Виталий Георгиевич – канд. физ.-мат. наук,
✉ vp@ipu.ru,

Семенков Кирилл Валерьевич – канд. физ.-мат. наук,
✉ semenkovk@ipu.ru,

Менгазетдинов Надыр Энверович – ст. науч. сотрудник,
✉ mengazne@mail.ru,

Институт проблем управления им. В.А. Трапезникова РАН,
г. Москва.

ASSESSMENT OF OPERATOR AUTHENTICATION METHODS IN INDUSTRIAL CONTROL SYSTEMS

V.G. Promyslov[1], K.V. Semenkov[2], N.E. Mengazetdinov[3]

Trapeznikov Institute of Control Sciences, Russian Academy of Sciences, Moscow, Russia

[1]✉ vp@ipu.ru, [2]✉ semenkovk@mail.ru, [3]✉ mengazne@mail.ru

Abstract. This paper considers the authentication of operators in instrumentation and control (I&C) systems for industrial facilities. The main emphasis is on such systems for critical facilities, on an example of nuclear power plants (NPPs). Authentication methods known for public information systems (password, token, and biometrics) are surveyed, and their applicability in typical operating conditions of an I&C operator is analyzed. The analysis includes experimental testing of password and biometric authentication methods and an expert assessment of their advantages and disadvantages for I&C systems. According to the testing results, all the methods under consideration have somewhat worse values of the false rejection rate (FRR) compared with the known characteristics from available sources. The best results are shown by biometric identification by the face oval. However, the percentage of FRR for this method is significant, which can affect the availability of the control function for a legitimate operator. As concluded, a promising approach for industrial control systems is to implement multi-factor authentication: token or password protection for blocking authentication jointly with biometric authentication by the face oval with a non-blocking security policy.

Keywords: authentication, biometrics, token, password, industrial control system, I&C, operator.

Funding. This work (Sections 2.3–2.5) was supported in part by the Russian Foundation for Basic Research, project no. 19-29-06044.

УДК 004.75

DOI: http://doi.org/10.25728/pu.2022.3.5

СПОСОБ УСКОРЕНИЯ ДЕЦЕНТРАЛИЗОВАННОГО УПРАВЛЕНИЯ ОДНОВРЕМЕННЫМ ЗАПУСКОМ ДЕЙСТВИЙ В РАСПРЕДЕЛЕННОЙ ГРУППЕ АВТОМАТИЧЕСКИХ УСТРОЙСТВ С ВКЛЮЧЕНИЕМ РЕТРАНСЛЯТОРА

Г.Г. Стецюра

Аннотация. Предлагается способ ускорения децентрализованных процессов синхронизации для распределенного управления группой стационарных или мобильных автоматических объектов, позволяющий объектам в заранее неизвестный момент одновременно переходить в заданные состояния. Действия объектов зависят от их текущего состояния и внешней среды и должны начаться согласованно во времени с как можно меньшей задержкой после обнаружения всеми объектами возможности их выполнения. Такими объектами могут быть компьютеры вычислительного кластера, распределенные средства обработки данных в суперкомпьютерах, мобильные роботы, исполнительные механизмы, действующие на внешнюю среду. Синхронизация произвольно расположенных источников исполнительных команд и их приемников осуществляется путем обмена сигналами и сообщениями между объектами через посредника, в качестве которого выступает ретранслятор сигналов. Используются средства точного измерения временны*х* интервалов передачи сигналов между каждым объектом и ретранслятором. Для ускорения процессов синхронизации применяются групповые операции, обладающие следующими общими свойствами. В них одновременно участвует большое количество объектов. Данные, которые они доставляют в сообщениях, используются в операциях одновременно. Обработка данных происходит в процессе их передачи, без увеличения этого времени. Операции выполняются сетевыми устройствами объектов и не содержащим вычислительных средств общим сетевым устройством – ретранслятором.

Ключевые слова: одновременный запуск групповых операций, децентрализованное управление, синхронизация движущихся объектов, быстрые распределенные внутрисетевые вычисления, многослойная синхронизация.

ВВЕДЕНИЕ

В статье решается задача ускорения децентрализованного управления запуском совместного действия распределенной группы цифровых объектов: компьютеров компьютерного кластера, распределенных средств обработки данных в суперкомпьютерах, мобильных роботов, исполнительных механизмов, действующих на внешнюю среду.

Задача следующая. Имеется распределенная группа источников общей команды, которая создается совместно этими источниками и направляется распределенной группе объектов-приемников – исполнителей команды. Объекты в группах расположены произвольно, могут изменять свое расположение и объединены сетью связи. Получив команду, все приемники должны выполнить указанные в команде действия одновременно или с заданными в команде для каждого приемника временными задержками. Момент отправки команды заранее неизвестен и зависит от текущего состояния объектов и внешней среды. Действия объектов должны начаться с возможно меньшей задержкой после отправки источниками частей общей команды. При работе объектов в распределенной системе управления также важно уменьшать задержку формирования всеми объектами общей команды, которая создается группой объектов системы. Все

объекты, источники и приемники, должны действовать без выделенного центра управления работой объектов.

Решение задачи состоит из двух частей, соответственно для источников и приемников команды. Действия источников были представлены в предыдущих публикациях автора и кратко изложены в § 3 настоящей статьи. Вводится дополнительное звено связи между объектами – ретранслятор сигналов *RS*, простое, не содержащее вычислительных средств и даже логических элементов устройство. Оно только принимает сигналы объектов на одних частотах и ретранслирует их объектам на других частотах, но не может выдавать по собственной инициативе команды и поэтому не служит центром управления. Объекты-приемники принимают сигналы только от *RS*. Использование *RS* дает следующие центральные для статьи результаты.

Предложенная синхронизация действий объектов позволяет источникам посылать сообщения в *RS* с одновременным приходом к нему одноименных двоичных разрядов всех сообщений. Для приемников *RS* действует как единственный источник, заменяющий всю предыдущую группу источников. Теперь объекты должны учитывать только изменения в удаленности объектов относительно *RS*. Источники посылают сообщения единственному приемнику – *RS*. Приемники получают сообщение только от *RS*. Это упрощает сетевые технические средства и уменьшает время исполнения команды. Добавление *RS* исключает помехи от поступления в приемники сигналов источников. Без *RS* сигналы группы источников, даже посылаемые одновременно, поступят в приемники в виде помех в разные, практически не контролируемые моменты времени.

В статье применены групповые операции и команды, которые выполняют распределенные управляющие и вычислительные операции за время, не зависящее от количества объектов – одновременных участников операции. Как будет показано, только наличие *RS* позволяет компьютерам распределенных объектов выполнять групповые операции на высоких скоростях.

Для решения поставленной задачи необходимо определять время переноса сигналов между объектами и *RS*. В разных технических областях для этого разработано много решений. Наиболее полезны для целей статьи результаты двух стандартизированных решений по синхронизации часов распределенных объектов и высокоточному измерению расстояний между объектами. В промышленности широко применяется стандарт IEEE 1588-2008 Precise Time Protocol (PTP) [1]. В PTP измерение времени переноса сигнала использовано для синхронизации показаний часов объектов. В зависимости от особенностей конкретного применения, точность изменяется в диапазоне от десятков микросекунд до восьми наносекунд. Для проведения точных физических экспериментов в ЦЕРН в рамках проекта White Rabbit (WR) [2, 3] были разработаны способы измерения времени переноса сигнала между объектами, обеспечивающие пикосекундную точность. В настоящее время создан стандарт, объединяющий оба решения, – IEEE 1588-2019 High Accuracy Default PTP Profile (HA) [4]. В PTP и WR взаимодействие объектов выполняется в режиме «ведущий – ведомый». И PTP, и WR могут работать на сетях большой протяженности.

Ниже применены решения PTP и WR, но с учетом поставленной в настоящей работе задачи внесены дополнения. В статье рассматривается интенсивный обмен данными между объектами для управления действиями объектов и выполнения распределенных вычислений, требующий уменьшения задержек в доставке данных. Поэтому далее речь пойдет только о системах, в которых объекты взаимно удалены на расстояние от долей метра до нескольких сотен метров.

Решения, предлагаемые в статье, ориентированы на задачи с непредсказуемым заранее временем исполнения приемниками команды, поэтому часы не применяются. Отсутствует ведущий объект, все объекты равноправны.

Наличие *RS* – дополнительного устройства между объектами – вызывает естественный вопрос о снижении отказоустойчивости системы. Но благодаря простоте *RS* их количество может быть увеличено и использовано для замены отказавших *RS*. Кроме этого, функции *RS* могут быть переданы любому объекту. Настоящая статья не рассматривает вопросы отказоустойчивости.

В начале данного раздела приведены существенно различные по организации цифровые объекты, к которым должны быть применимы способы, предлагаемые в статье. Это выполняется, но для конкретного вида объектов требуется уточнять многие технические детали. Например, для многих видов мобильных объектов связь должна выполняться только путем обмена ненаправленными радиосигналами через единственный *RS*. В суперкомпьютере целесообразно применить направленные оптические связи с коммутацией сигналов через тысячи одновременно доступных *RS*. Но в

каждом из этих случаев способы, изложенные в статье, не требуют изменений.

Материал статьи следующим образом распределен между ее разделами. В § 1 рассмотрены принципы измерения времени в PTP и WR, полезные для дальнейших разделов статьи. В § 2 приведена структура связей, используемая далее для синхронизации действий источников и приемников команд. В § 3 дан способ выполнения приемниками команд источников одновременно или с заданными в команде для каждого приемника временными задержками. В § 4 приведен способ распределенного управления взаимодействием источников. В § 5 рассмотрена многослойная синхронизация выполнения команд приемниками. Здесь приемники слоя, выполнив команду, становятся источниками команды для следующего слоя приемников и т. д. В § 6 дана краткая сводка групповых операций. В § 7 показана связь предлагаемых в статье сетевых операций с операциями ассоциативных вычислительных средств.

1. ОСОБЕННОСТИ ИЗМЕРЕНИЯ ИНТЕРВАЛОВ ВРЕМЕНИ в PTP и WR

Основная схема измерения в PTP интервалов времени показана на рис. 1, *а*.

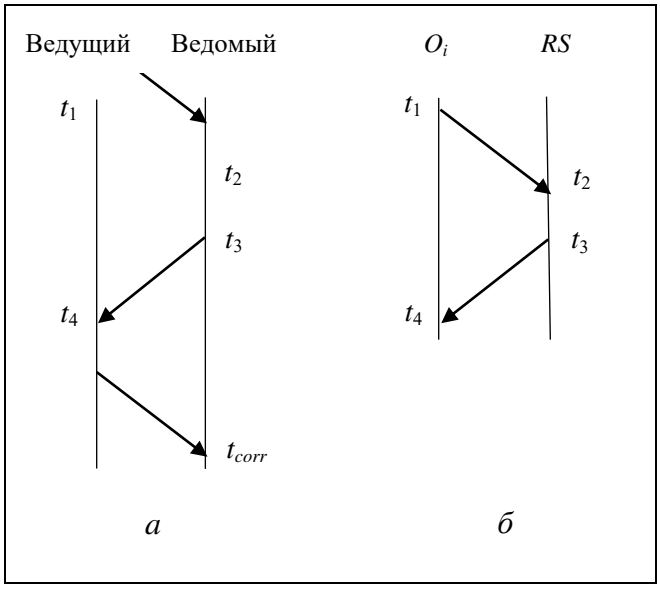


Рис. 1. Измерение времени в PTP и вариант его использования

Здесь взаимодействуют два объекта – ведущий и ведомый (“master–slave” по распространенной терминологии). В момент времени t_1 ведущий посылает ведомому сигнал начала синхронизации и показание своих часов. Сообщение поступает в момент t_2. Ведомый в момент t_3 посылает ведущему ответный сигнал и новое показание своих часов. Ведущий в момент t_4 получает ответ ведомого, определяет расстояние между этой парой объектов, определяет расстояние (удаленность) от ведомого и сообщает его ведомому. Ведомый корректирует часы. За исключением ряда важных деталей в этом состоит основа корректировки времени в PTP.

Для целей настоящей статьи потребуется упрощенный вариант измерения, показанный на рис. 1, *б*. Часы не используются. Имеется объект *RS* – ретранслятор сигналов. Для оптических сигналов в качестве *RS* можно использовать пассивный ретрорефлектор. Произвольный объект O_i включает свой таймер и в момент t_1 посылает в *RS* сигнал. Сигнал поступает в *RS* в момент t_2. С задержкой срабатывания *RS* в момент t_3 сигнал будет отправлен в *RS* и в момент t_4 объект O_i определяет время переноса сигнала между O_i и *RS* как $T_{OiRS} = t_4 - t_1 - (t_3 - t_2)$.

В WR используется более точный фазовый способ измерения интервалов времени. В работе [5] для этого предложено электронное устройство, измеряющее время передачи сигнала между объектами достаточно простыми средствами. Достигнута точность в фемтосекундном диапазоне. В настоящей статье этот способ можно применять непосредственно или как средство контроля стабильности участвующих в измерениях устройств объектов.

2. СВЯЗИ МЕЖДУ ИСТОЧНИКАМИ И ПРИЕМНИКАМИ КОМАНД

На рис. 2 показана структура связей, использованная в настоящей работе для обмена сигналами и сообщениями между источниками и приемниками команд.

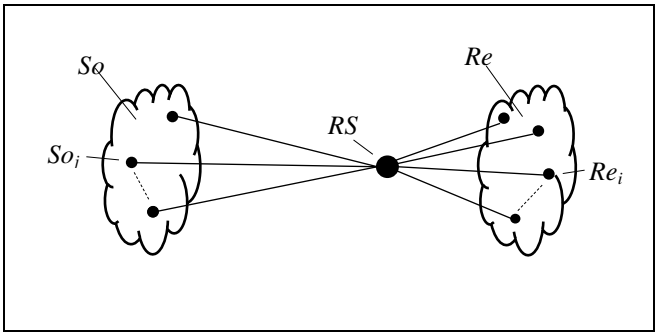


Рис. 2. Связи между источниками и приемниками команд

Система объектов имеет группу *Re* приемников команд $\{Re_i\}$, группу *So* источников команд $\{So_j\}$,

ретранслятор *RS* сигналов источников и приемников. До § 4 будем считать, что только один произвольный источник из *So* посылает команду приемникам из *Re*. Источник посылает команду не непосредственно *Re*, а через *RS*. При этом двоичный разряд «1» кода команды источник посылает в *RS* сигналом несущей частоты f_1, двоичный разряд «0» посылается сигналом другой частоты f_0. Ретранслятор переводит эти сигналы соответственно в другие сигналы $^*f_1$ и $^*f_0$ и посылает приемникам. Сигналы не изменяются при операциях WR. Как отмечено во введении, объекты принимают только сигналы, ретранслируемые *RS* объектам.

Из изложенного следует, что *RS* действительно простое, не содержащее логических элементов устройство и активно не участвует в управлении действиями объектов.

Наличие *RS* – основа использованной в статье синхронизации действий объектов. При этом *RS* уменьшает объем передаваемых данных и времени, необходимых Re_i для организации синхронного выполнения задания. Без сбора сообщений в одну точку – *RS* – решение задач статьи, как отмечено во введении, требует больших затрат времени. Эти возможности детально рассмотрены в следующих разделах статьи.

Связи между объектами могут быть беспроводными и проводными. Беспроводные связи предоставляют дополнительные возможности. К примеру, для мобильных объектов допустимы только беспроводные связи. В стационарных суперкомпьютерах беспроводные связи между группой объектов и группой *RS* позволяют быстро перестраивать структуру системы в пределах решения одной задачи. Также упрощается восстановление системы при отказах *RS*. Они избавляют от дублирования и троирования состава ретрансляторов. Так, если есть хотя бы один запасной ретранслятор, то при отказе какого-либо из ретрансляторов объекты без промежуточных коммутаторов переключатся на резервный ретранслятор. Обнаружить отказ помогает широковещательная передача логической шкалы, доступной одновременно всем объектам (см. § 4).

3. СИНХРОНИЗАЦИЯ ПРОЦЕССА ВЫПОЛНЕНИЯ КОМАНД ПРИЕМНИКАМИ

В данном разделе изложен способ выполнения точной синхронизации приемников – исполнителей команд, объединенных в соответствии с рис. 2. Каждый приемник до получения исполнительной команды, запускающей процесс синхронного выполнения исполнительных действий, получает описание его действия в предварительной команде. Эти команды могут быть посланы разными источниками в произвольном порядке или в виде единого сообщения, состоящего из сообщений отдельных источников. Такой способ показан в § 4.

До реализации исполнительной команды каждый приемник должен измерить время прохода сигнала (оптического или радиосигнала, имеющих скорость света *c*) между приемником и *RS* (удаленность от *RS*). Здесь предлагается вариант измерения, который требует введения дополнительных частотных каналов, но позволяет проводить измерения независимо и одновременно с другими процессами обмена сообщениями между объектами.

Первая задача приемников в процессе измерения времени состоит в его запуске без привлечения специального центра управления, задающего объектам порядок измерения. Для этого приемники из *Re*, которым требуется определить удаленность от *RS*, посылают в *RS* специальный синхросигнал *S*. Длительность его должна быть не меньше *T* – наибольшего интервала времени переноса сигнала между *RS* и любым приемником. Приемник посылает сигнал *S*, если он не получил до этого момента возвращенный от *RS* сигнал *S*, посланный другими источниками. При длительности сигнала $S \geq T$ общий сигнал *S* создается наложением отдельных сигналов *S* объектов в единственный общий сигнал *S* переменной длительности. Ретранслятор преобразует *S* в единственный сигнал S_{rs} и широковещательно рассылает его приемникам *Re*.

Момент прекращения приема сигнала S_{rs} приемник воспринимает как сигнал $^*S_{rs}$ начала синхронизации, созданный без привлечения центра управления (см. также работу [6]). Далее предполагается, что приемники из *Re* имеют порядковые номера. Объект Re_i с известным наименьшим номером *i*, например, с $i = 1$, проводит измерение его удаленности от *RS*. Так поступают все приемники. Этот процесс может выполняться непрерывно, одновременно с другими процессами взаимодействия объектов. Некоторые варианты данного действия объектов приведены в статье [6]. В частности, если не требуется высокая точность синхронизации (не требуется различать временные интервалы $\leq T$), то в соответствии с работой [6] объектам достаточно обмениваться между собой сигналами непосредственно, без наличия *RS*.

После завершения измерения приемниками Re_i их удаленности T_i от *RS* начинается процесс синхронного выполнения всеми приемниками команды источника. Для этого каждый приемник выполняет следующую последовательность действий.

Шаг 1. Приемник Re_i вычисляет значение задержки $d_i = C - T_i + a_i$. Здесь $C \geq T$, a_i – не обязательная для Re_i дополнительная задержка во времени; $a_i \geq 0$. Используется $C \geq 0$, если требуется учесть затраты времени на дополнительные действия объектов.

Шаг 2. Каждый Re_i, получив команду, в момент ее завершения выполняет задержку d_i и после этого выполняет требуемые командой действия.

Команда после выхода из *RS* поступает в Re_i через интервал времени T_i. Следовательно, при задержке d_i любой Re_i выполнит действия в момент времени $\tau = T_i + C - T_i + a_i = C + a_i$. Все Re_i выполнят команду одновременно в момент C после выхода команды из *RS* или с задержками a_i, что и требовалось.

Таким образом, после выхода команды из *RS* для всех объектов переход в синхронное выполнение команды произойдет через время доставки команды к наиболее удаленному от *RS* объекту. Если всем объектам известно $T_{\max}$ (время переноса сигнала между *RS* и наиболее удаленным от него объектом) и допустима замена C на $T_{\max}$, то будет выполнен переход в синхронное состояние за наименьшее возможное время.

Необходимо определиться с моментом отбора измерений T_i приемниками Re_i. Так как предполагается непрерывный процесс измерения приемниками значений T_i, то можно брать последнее из измерений, выполненных до получения команды объектом. Но можно выполнить измерение при получении команды приемником. Если Re_i известно время определения Re_i значений T_i и d_i, то достаточно задать всем Re_i верхнюю границу времени определения T_i и d_i, чтобы приемники откорректировали возможный разброс времени в определении этих значений.

Точность измерения T_i существенно улучшается приведенным ниже способом, ориентированным на жесткие временные требования, что необходимо для согласования действий компьютеров, находящихся в приемниках Re_i. В этом способе Re_i будет по-прежнему проводить новое измерение расстояния до *RS* после завершения измерений остальных приемников, но все эти измерения теперь проводятся в пределах одного общего для всех приемников сообщения. В нем измерению каждого Re_i отводится очень короткий временной интервал Δt.

Полагаем, что до применения предлагаемого способа приемники Re_i определили интервалы времени T_i, задана константа C, в лучшем случае $C = T$ [6]. Приемники Re_i также вычислили значения d_i. Каждому Re_i для нового определения T_i выделен интервал времени Δt_i одинаковой длительности Δt. Способ предполагает следующую последовательность действий.

Шаг 1. Приемники Re_i, как изложено выше, посылают в *RS* сигнал *S*, получают от *RS* сигнал S_{rs}. По сигналу ${}^*S_{rs}$ завершения сигнала S_{rs} каждый Re_i поочередно по i в своем интервале Δt_i посылает в *RS* тест-сигнал δt длительности, меньшей длительности Δt, располагая δt в центре Δt_i.

Шаг 2. Так как всем Re_i известно значение Δt, то все Re_i отправят свои Δt_i в одном общем сообщении *SC* длительности $n\Delta t$, где n – количество приемников.

Шаг 3. Сигналы δt сообщения *SC* поступят в *RS*, преобразуются в ${}^*\delta t$ и возвратятся приемникам. По смещению δt в пределах Δt_i приемник Re_i определит новое T_i.

Для того, ч тобы способ был работоспособен и полезен, требуется выполнение двух условий. Во-первых, сигнал δt при любом перемещении Re_i не должен выходить за пределы Δt_i. Во-вторых, длительность $n\Delta t$ должна быть меньше длительности предыдущего способа определения T_i, использующего группу отдельных сообщений. Покажем, что это достигается.

При неподвижных и не подверженных внешним воздействиям Re_i при любом количестве измерений T_i сигнал δt будет находиться в центре Δt. Иначе δt смещается.

Пусть максимальное расстояние между *RS* и любым Re_i равно L, максимальная скорость перемещения Re_i равна v. Тогда за время измерения T_i приемник сместится не более чем на расстояние ${}^*L = T_i v$. При этом сигнал δt сместится в пределах Δt не более чем на интервал времени ${}^*\Delta t = {}^*L / c = T_i v/c$. Интервал Δt должен быть не меньше $2{}^*\Delta t$, чтобы δt не перешел в соседний интервал Δt. Весь цикл измерений для n приемников будет выполнен за интервал времени $2nT_i v/c << nT_i$. Выделение отдельного частотного канала для сигналов каждого Re_i устранит зависимость от n и уменьшит допустимое время измерения удаленности от *RS* для всей группы *Re*.

Изложенные решения обеспечивают минимальную задержку в исполнении направляемой приемникам команды. Действительно, при наличии *RS* он действует как единственный источник команды. Приемник измеряет удаленность от *RS* до получения команды и задержка в начале ее выполнения отсутствует. Далее каждый приемник должен начинать выполнять команду только при получении команды всеми приемниками, задерживая выполнение с учетом своей удаленности от *RS*. Как показано выше в этом разделе, вся информация для этого приемникам доступна заранее и, получив команду, приемник с соответствующим ему

сдвигом во времени начинает ее выполнение. Таким образом, наличие *RS* устраняет задержки в выполнении команды. При отсутствии *RS* задержка возникает обязательно.

Если общую команду формирует группа источников и отсутствует *RS*, то одновременность действий приемников достигается только при замене *RS* одним из источников – лидером. Лидер будет действовать как *RS*. Такой процесс неприемлемо длительный.

В следующем § 4 источники отправляют сообщения приемникам только через *RS*, регулируя время прихода сообщения в *RS* с учетом удаленности источника от *RS*. При этом источники, действуя подобно приемникам, определяют удаленность до *RS* и затем посылают сообщения так, чтобы они достигли *RS* одновременно или в заданном порядке. Удаленность до *RS* источники определяют заранее и формирование общей команды будет выполнено без задержек, например, следуя решениям § 6.

Способ измерения переноса сигнала (PTP, WR) без изменения решений статьи можно заменить другим известным способом. Таким образом, во всех случаях наличие *RS* минимизирует задержку начала выполнения общего действия приемников.

Изложенным завершен процесс синхронизации выполнения команд для структуры с единственным *RS*, посылающим сигналы всем приемникам группы *Re*. В § 5 будет рассмотрена более общая задача. Но вначале в § 4 рассмотрим совместные синхронные действия группы источников.

4. СИНХРОННЫЕ ДЕЙСТВИЯ ГРУППЫ ИСТОЧНИКОВ

Синхронные действия группы источников были рассмотрены в статье [6], но они многократно используются в настоящей статье и здесь дано более соответствующее § 3 краткое изложение действий группы источников.

Подобно действиям приемников, в § 3 источники организуют действия следующим образом. Источники So_j из группы источников *So*, упорядоченные по *j*, посылают в *RS* сигнал *S*, в ответ получают от *RS* сигнал S_{rs} и сигнал ${}^*S_{rs}$ – признак завершения *S*. После этого So_j поочередно определяют удаленность от *RS* и вычисляют задержки $D_j = C - t_j + a_j$, подобные d_i, C, T_i, a_i из § 3. Теперь источники могут без использования выделенного центра посылать синхронно сообщения (и команды приемникам) в *RS*.

Для описания дальнейших действий источников вводится логическая шкала *LS* – последовательность двоичных разрядов в количестве, равном количеству источников в *So*. Источник So_j, которому требуется передать сообщение в *RS*, вносит в соответствующий ему разряд *j* шкалы *LS* единицу, которая передается в *RS* сигналом с несущей частотой f_1. Остальные разряды *LS* могут не содержать двоичных значений или So_j вносит в них ноль, который передается сигналом f_0. Во втором случае при одновременном приходе в *RS* и далее в Re_i от нескольких источников сигналов f_1 и f_0 они в некоторых операциях Re_i воспринимаются как пара сигналов, но в большинстве операций считаются сигналом f_1.

Для начала взаимодействия с *RS* источники посылают в *RS* сигнал *S*, получают в ответ S_{rs} и ${}^*S_{rs}$. После этого с задержками D_j источники посылают в *RS* свои шкалы *LS* и получают объединенную шкалу ${}^*LS$, в которой совмещены одноименные разряды всех полученных *RS* шкал. Теперь So_j могут послать упорядоченно свои сообщения в *RS*, не задерживаясь на источниках, не затребовавших передачу сообщений.

Таким образом, получен полезный результат. Источники упорядочивают свои сообщения, посылая их в *RS*. Теперь *RS* действует как единственный источник, рассылающий от *RS* приемникам сообщения-команды. Источники одновременно могут быть приемниками, что позволяет им согласовывать совместные действия. В частности, So_j могут подтвердить согласие всей группы *So* на выполнение команды, отправленной в *Re*. В § 6 будет показано, что *RS* может не только действовать как ретранслятор сигналов, но для ряда распределенных между членами *So* операций может их выполнять без включения в состав *RS* логических элементов.

В отличие от синхронных действий объектов, при асинхронных действиях отсутствует возможность указать время занятия *RS* объектом. В этом случае применим барьерную синхронизацию в виде, приведенном в работе [7]. В ней один или несколько выполняющих общую операцию объектов на время выполнения операции посылают доступный всем объектам сигнал *B*, отличающийся от всех других сигналов. При работе нескольких объектов и завершении каким-либо объектом его работы этот объект прекращает передавать сигнал *B*. При завершении работы всех участников операции передача сигнала *B* прекращается. Его отсутствие разрешает другим объектам начать следующую операцию. Если не применить эти действия, то при асинхронных действиях объектов значение *C* придется выбирать неоправданно большим. Операции источников § 4 использованы в следующем § 5 при многослойной синхронизации действий в *Re*.

5. МНОГОСЛОЙНАЯ СИНХРОНИЗАЦИЯ ГРУПП ПРИЕМНИКОВ

В отличие от § 3, здесь общая группа объектов разделена на подгруппы (слои) Le_1, Le_2, …, Le_n. (рис. 3). В пределах слоя объекты действуют, как показано в предыдущих разделах. Сигналы, которыми они обмениваются, недоступны объектам других слоев. Но ретрансляторы *RS* слоя под управлением объектов слоя могут объединяться с *RS* следующего слоя. Первый слой приемников получает команды источников в соответствии с § 3 непосредственно от *So* слоя. Затем группа *Re* приемников первого слоя через свой ретранслятор действует как группа источников для приемников второго слоя, согласовав свои действия в соответствии с § 4. Для этого *RS* этих слоев действуют совместно – ретранслятор второго слоя транслирует объектам второго слоя сигналы первого слоя, а также посылает сигналы второго слоя первому. Аналогично будут действовать приемники следующих слоев. В простейшем случае требуется, чтобы приемники последнего слоя синхронно выполнили действия по отношению к внешним объектам. В более сложном случае компьютеры приемников и компьютеры источников слоя при выполнении совместных действий будут через свой *RS* обмениваться сообщениями, которые будут одновременно доступны всем этим объектам и должны использоваться для корректировки их действий, что потребует дополнительного времени. Начнем с простейшего процесса 1.

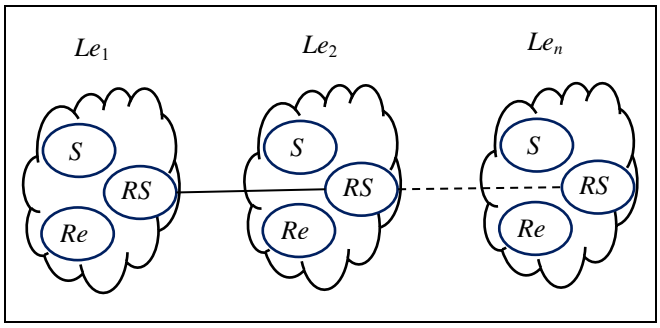


Рис. 3. Многослойная синхронизация групп приемников

Процесс 1. Объекты разделены на k слоев, $k = 0, \ldots, n$. Объекты-приемники слоя k для взаимодействия с приемниками слоя $k + 1$ переходят в режим работы источниками. Новые источники слоя k действуют в соответствии с положениями § 3, синхронизуя приемники слоя $k + 1$. Перемещаясь от слоя к слою, этот процесс достигает слоя, действия приемников которого требуется синхронизовать. Синхронизация будет выполнена. При этом промежуточным слоям запрещено выполнять какие-либо внешние действия.

Если требуется, чтобы приемники всех слоев с одинаковым для всех слоев временем выполнения действий C одновременно выполнили внешние действия, не требующие обращения к *RS*, то для этого используем процесс 2, дополняющий действия процесса 1.

Процесс 2. Приемники произвольного слоя $k \le n$ после получения команды многократно вычисляют значение $F = n - k$, увеличивая k на единицу. При каждом вычислении F формируется задержка времени C, после достижения которой вычисляется следующее значение F.

При получении $F = 0$ приемники слоя выполнят внешнее действие. При первом вычислении для слоя $k = 0$ получим $F = n$, для слоя $k = 1$ получим $F = n - 1$ и т. д. В результате в момент получения команды в последнем слое приемники во всех слоях получат $F = 0$ и одновременно выполнят внешнее действие.

Кроме внешних действий компьютерам объектов слоя k может потребоваться обмен данными, командами и выполнение распределенных вычислений, занимающие для этого их общий ресурс RS_k. Если можно указать верхнюю границу ${}^*C$ занятия этого RS_k объектами слоя, то при поочередной работе слоев время занятия учитывается выбором соответствующего значения ${}^*C$ вместо C.

При наличии асинхронно действующих объектов лучший временной результат дает применение следующего двухфазного процесса синхронизации.

Фаза подготовки к синхронизации. В ней для первого слоя асинхронно выполняется подготовка данных источниками для передачи их приемникам первого слоя. Все действия выполняются с применением барьерной синхронизации (§ 4). Приемники первого слоя при необходимости также асинхронно формируют дополнительные данные для подготовки действий в качестве источников второго слоя. Переход к действиям второго слоя выполняется по сигналу барьерной синхронизации. Так поочередно выполняется работа всех слоев. Пока не требуется одновременное выполнение всеми слоями внешних действий, они будут выполнены на следующей фазе.

Фаза синхронизации. Процесс подобен процессу 2, но теперь все слои перенумерованы в обратном порядке, последний слой n имеет номер 0. Для синхронизации объекты слоя с новой нумерацией $k = 0$ действуют как источники и начинают синхронизацию приемников всех слоев. После получения команды объекты многократно вычисляют значение ${}^*F = n - k$, увеличивая k на единицу, с

задержкой после каждого вычисления $^{**}C$. При получении $F = 0$ во всех слоях приемники одновременно выполнят внешнее действие.

Фаза синхронизации выполняется быстрее, так как объекты здесь не выполняют никаких действий, кроме передачи команды в предшествующий слой. Поэтому $^{**}C < C$. В фазе синхронизации в дополнение к предыдущим процессам введена обратная связь, позволяющая также передавать результаты вычислений следующих слоев предыдущим.

Таким образом, получен следующий результат. Объекты, не используя общий центр управления, синхронизуют свои действия и выполнят их одновременно во всех слоях рассмотренной многослойной структуры объектов.

6. ОБЗОР ВЫПОЛНЯЕМЫХ В СЕТИ ГРУППОВЫХ ОПЕРАЦИЙ

В этом разделе приведем краткую сводку рассматриваемых в статье групповых операций как средства группового взаимодействия объектов. Ряд операций разработан для настоящей работы, другие были созданы автором раньше и адаптированы для целей статьи. Перечисленные ниже операции в разное время были разработаны в Институте проблем управления им. В.А. Трапезникова РАН (ИПУ РАН). Дальнейший текст достаточно полно излагает основные принципы действия групповых операций и не требует обращения к первоисточникам.

Основные свойства операций следующие. Данные для обработки операцией одновременно поступают от группы распределенных объектов – хранителей данных. Эти данные операции обрабатывают одновременно, причем обработка идет во время передачи данных, не увеличивая это время. Операции выполняются в сетевых средствах системы объектов без использования в них компьютеров и других вычислительных устройств. Время получения результата операции не зависит от количества обрабатываемых данных.

Эти результаты – следствие согласования действий объектов при помощи процессов синхронизации сообщений. Основное средство достижения синхронности действий объектов, не зависящее от расположения объектов в текущий момент времени, состоит в выделении для группы объектов одного объекта – ретранслятора сигналов *RS*. Синхронная доставка группы сообщений одному объекту *RS* с последующей пересылкой их группе приемников в виде одного общего для всех источников сообщения выполняется достаточно просто и быстро. Но это сообщение поступает к группе произвольно расположенных приемников в разное время. Используя *RS*, приемники вносят соответствующие задержки и одновременно выполняют требуемое от них групповое действие. Возвращаясь к предыдущим разделам статьи, легко проверить, что приведенные свойства выполняются во всех следующих **операциях управления действиями объектов**: синхронизация источников, синхронизация приемников, многослойная синхронизация, устранение конфликтов доступа, барьерная синхронизация.

Перечислим также распределенные **вычислительные операции**: поиск максимума и минимума, поразрядные логические операции И и ИЛИ, аналого-цифровые операции счета, сложения, вычитания. Эти операции в настоящей статье не использованы, но они ускоряют управление системой при поиске объектов с заданным набором свойств и для оценки состояния системы в целом. Описание их есть, например, в работе [7]. Кратко изложим принцип их работы.

Для определения максимума объекты посылают числа, представленные в двоичном коде, и на первом шаге передают старший разряд числа. В передаче следующего разряда участвуют только объекты, передавшие перед этим единицу, и т. д. Остается максимальное из переданных чисел. С заменой единиц на нули определяется минимум. От двоичного представления чисел можно перейти к другим системам счисления, если цифры числа представлять шкалой, в которой все разряды содержат нули, кроме разряда, соответствующего значению цифры.

Поразрядные операции И и ИЛИ позволяют быстро оценить состояние всех объектов системы. Для этого состояние объекта описывается шкалой – последовательностью двоичных разрядов, каждый из них равен единице при наличии соответствующего признака и равен нулю при его отсутствии и передается соответственно сигналами частот f_1 и f_0. Оценка состояния всех объектов выполняется при одновременной передаче шкал в *RS* с совмещением в *RS* одноименных разрядов последовательностей объектов. При выполнении операции И наличие в *RS* в разряде шкалы f_0 означает отсутствие соответствующего признака хотя бы у одного объекта. Иначе признак присутствует у всех объектов. Для операции ИЛИ в этих же условиях наличие f_1 означает наличие признака хотя бы у одного объекта. Иначе признак отсутствует у всех объектов.

Для выполнения аналого-цифровых операций *RS* содержит аналого-цифровой преобразователь (АЦП). Пусть объекты также характеризуют свое состояние шкалой – последовательностью признаков, представленных нулями и единицами. Если объекты пошлют свои шкалы в *RS* с совмещением одноименных разрядов, то АЦП оценит суммарную энергию принятых сигналов, выдаст численное значение присутствия признака во всех объектах. Его получат одновременно все объекты. Объединение таких операций с поразрядными И и ИЛИ позволяет получить более точную оценку состояния системы объектов. Выполнение сложения и вычитания чисел в системе счисления, отличной от двоичной, дано в работе [7]. В этих операциях цифры чисел представлены шкалами с единицей только в разряде шкалы, соответствующем значению цифры. Результат операций также не зависит от количества участвующих в ней объектов.

Для операций с АЦП требуются источники оптических сигналов со стабильным значением энергии сигналов. Современные технологии позволяют получать точное цифровое значение при одновременном суммировании нескольких тысяч сигналов. В работе [8] приведен простой светодиодный источник со стабильностью выходной мощности лучше 50×10^{-6} ºC^{-1}.

7. ОБЩИЙ ВЗГЛЯД НА СПЕЦИФИКУ ПРЕДЛОЖЕНОГО СПОСОБА

Основные результаты статьи получены путем применения распределенных групповых операций, не используемых в известных системах с сетевыми связями. Их аналог – ассоциативные операции, предложенные в 1960-х гг. для сосредоточенных ассоциативных компьютеров (АК). Укрупненно ассоциативные операции выполнялись по следующей схеме.

В АК центр управления одновременно посылал общую команду группе ассоциативных узлов компьютера, содержащих ассоциативную память. В узлах выполнялись требуемые действия. Результат действий узлов мог быть доступен другим узлам и одновременно поступал в центр, который на основе полученных результатов формировал следующую команду, и т. д. Основным применением АК были системы управления, работающие в режиме жесткого реального времени. Пример – ассоциативный суперкомпьютер серии STARAN, управляющий движениям самолетов в аэропорту им. Дж. Кеннеди в Нью-Йорке. Групповые операции статьи можно рассматривать как вариант ассоциативных операций, имеющий следующие дополнительные отличия. Операции распределенные и выполняются непосредственно в простом сетевом средстве – ретрансляторе. Ретранслятор не имеет вычислительных средств, тем не менее все приведенные в статье групповые операции в нем выполняются и позволяют управлять взаимодействием объектов и одновременно оценивать состояние всей совокупности объектов. Все приведенные в статье виды взаимодействия объектов выполняются децентрализованно, без применения управляющего центра. Таким образом, предложенные в статье структуры имеют одновременно сетевые и ассоциативные возможности.

Отметим, что в настоящее время проводится много исследований, направленных на выполнение в сетях не только переноса сообщений, но и других функций – управления транспортировкой данных, распределенных вычислений [9–12]. Однако эти важные направления работ отличаются от выполненных в ИПУ РАН тем, что в них новые функции выполняют компьютеры сетевых средств, групповые операции не используются.

ЗАКЛЮЧЕНИЕ

В статье предложен способ децентрализованного управления одновременным запуском действий в распределенной группе стационарных или мобильных автоматических объектов. Способ позволяет этим объектам начинать действия с минимальной задержкой после возникновения заранее неизвестного момента запуска.

Задачу одновременного запуска действий группы объектов при возможности указать заранее время действия успешно решает стандарт IEEE 1588-2019. Область применения стандарта расширяется на работающие в реальном времени управляющие системы путем добавления к этим возможностям запуска в заранее неизвестный момент времени

Предложенный способ обладает быстрой реакцией на возникающие события благодаря использованию сетевых групповых операций.

ЛИТЕРАТУРА

1. *IEEE* Standard for a Precision Clock Synchronization Protocol for Networked Measurement and Control Systems / In IEEE Std 1588-2008 (Revision of IEEE Std 1588-2002), 2008. – P. 1–269. – DOI: 10.1109/IEEESTD.2008.4579760.
2. *IEEE* Standard for a Precision Clock Synchronization Protocol for Networked Measurement and Control Systems / In IEEE Std 1588-2019 (Revision ofIEEE Std 1588-2008), 2020. – P. 1–499. – DOI: 10.1109/IEEESTD.2020.9120376.

3. *Girela-López, F., López-Jiménez, J., Jiménez-López, M.,* et al. IEEE 1588 High Accuracy Default Profile: Applications and Challenges // IEEE Access, 2020. – Vol. 8. – P. 45211 – 45220.
4. *Sliwczynski, Ł., Krehlik, P., Buczek, Ł., Schnatz, H.* Picoseconds-Accurate Fiber-Optic Time Transfer with Relative Stabilization of Lasers Wavelengths // Journal of Lightwave Technology. – 2020. – Vol. 38, no. 18. – P. 5056 – 5063.
5. *Moreira, P.* Timing Signals and Radio Frequency Distribution Using Ethernet Networks for High Energy Physics Applications: A thesis submitted for the degree of Doctor of Philosophy (PhD). – University College of London, 2014. – 302 p. https://discovery.ucl.ac.uk/id/eprint/1461109/1/PMmoreira_PhD_Final-signed[1].pdf
6. *Стецюра Г.Г.* Децентрализованная автономная синхронизация процессов взаимодействия мобильных объектов // Проблемы управления. – 2020. – № 6. – С.47–56. DOI: http://doi.org/10.25728/pu.2020.6.5. [*Stetsyura, G.G.* Decentralized Autonomic Synchronization of Interaction Processes of Mobile Objects// Control Sciences. – 2020. – No. 6. – P. 47 – 56. (In Russian)]
7. *Стецюра Г.Г.* Сетевая информационно-вычислительная поддержка взаимодействия подвижных роботов // Проблемы управления. – 2018. – № 5. – С. 56 – 65. DOI: http://doi.org/10.25728/pu.2018.5.6. [*Stetsyura, G.G.* Network Information-Computing Support of Automatic Mobile Objects Interaction // Automation and Remote Control. – 2019. – Vol. 80, no. 6. – P. 1134 – 1147. DOI: 10.1134/S0005117919060110].
8. *Bosiljevac, M., Babić, D., Sipus, Z.* Temperature-Stable LED-Based Light Source without Temperature Control // Proceedings of SPIE OPTO. – San Francisco, CA, USA, 2016. – Vol. 9754. – P. 1–6. – DOI: 10.1117/12.2211576.
9. *Tennenhouse, D.L.* Towards an Active Network Architecture // SIGCOMM Comput. Commun. Rev. – 1996. – Vol. 26, no. 2. http://ccr.sigcomm.org/archive/1996/apr96/ccr-9604-tennenhouse.pdf .
10. *Zilberman, N., Watts, P.M., Rotsos, C., Moore, A.W.* Reconfigurable Network Systems and Software-Defined Networking // Proc. of the IEEE. – 2015. – Vol. 103, no. 7. – P. 1102 – 1124.
11. *In-Network* Computing. – ACM SIGARCH, 2019. https://www.sigarch.org/in-network-computing-draft/
12. *Kim, D.* Towards Elastic and Resilient In-Network Computing: PhD Thesis. – Carnegie Mellon University, 2021. http://reports-archive.adm.cs.cmu.edu/anon/2021/CMU-CS-21-143.pdf .

Статья представлена к публикации членом редколлегии В.Г. Лебедевым.

Поступила в редакцию 28.11.2021,
после доработки 5.05.2022.
Принята к публикации 19.05.2022.

Стецюра Геннадий Георгиевич – д-р техн. наук, Институт проблем управления им. В.А. Трапезникова РАН, г. Москва, ✉ gstetsura@mail.ru.

THE SIMULTANEOUS START OF ACTIONS IN A DISTRIBUTED GROUP OF AUTOMATIC DEVICES: A DECENTRALIZED CONTROL METHOD WITH A SIGNAL REPEATER

G.G. Stetsyura

Trapeznikov Institute of Control Sciences, Russian Academy of Sciences, Moscow, Russia

✉ gstetsura@mail.ru

Abstract. This paper proposes a method for accelerating decentralized synchronization processes in the distributed control of a group of stationary or mobile automatic objects. With this method, the objects pass to specified states or affect the environment simultaneously or with required time delays. Some examples of such objects include actuators, computers in a computing cluster, distributed data processing facilities in supercomputers, and mobile robots. The object's action depends on the current state of all objects and the environment. The actions should start with minimum delay after detecting the possibility to perform them. Arbitrarily located sources of executive commands and their receivers are synchronized by exchanging signals and messages between objects through an intermediary (a signal repeater). Means are used to accurately measure the time intervals of signal transfer between each object and the repeater. Group operations are used to accelerate synchronization processes. These operations involve a large number of objects simultaneously. The object's data are used in operations simultaneously. Data are processed during their transmission without extra time. Operations are executed by network devices of the system objects and the common network device without any computing facilities (the repeater).

Keywords: simultaneous start of group operations, decentralized control, synchronization of mobile objects, fast distributed intranet computing, multilayer synchronization.