DOI 10.17587/issn.1684-6400

ISSN 1684-6400

ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ

Том 26

2020

№ 4

ТЕОРЕТИЧЕСКИЙ И ПРИКЛАДНОЙ НАУЧНО-ТЕХНИЧЕСКИЙ ЖУРНАЛ

САПР

КОМПЬЮТЕРНАЯ ГРАФИКА

МЕТОДЫ ПРОГРАММИРОВАНИЯ

ОПЕРАЦИОННЫЕ СИСТЕМЫ И СРЕДЫ

ТЕЛЕКОММУНИКАЦИИ И ВЫЧИСЛИТЕЛЬНЫЕ СЕТИ

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

НЕЙРОСЕТИ И НЕЙРОКОМПЬЮТЕРЫ

СТРУКТУРНЫЙ СИНТЕЗ

ВЫЧИСЛИТЕЛЬНЫЕ СИСТЕМЫ

ПРИКЛАДНЫЕ ИНФОРМАЦИОННЫЕ СИСТЕМЫ

ИНТЕЛЛЕКТУАЛЬНЫЕ СИСТЕМЫ

ОПТИМИЗАЦИЯ И МОДЕЛИРОВАНИЕ

ИТ В ОБРАЗОВАНИИ

ГИС

Рисунки к статье И. Б. Зарубина, А. Д. Филинских, Т. И. Балашовой

«ОЦЕНКА ТЕСТОВОГО ПОКРЫТИЯ ИНТЕРФЕЙСА ПОЛЬЗОВАТЕЛЯ В МНОГОКОМПОНЕНТНЫХ ИНФОРМАЦИОННЫХ СИСТЕМАХ»

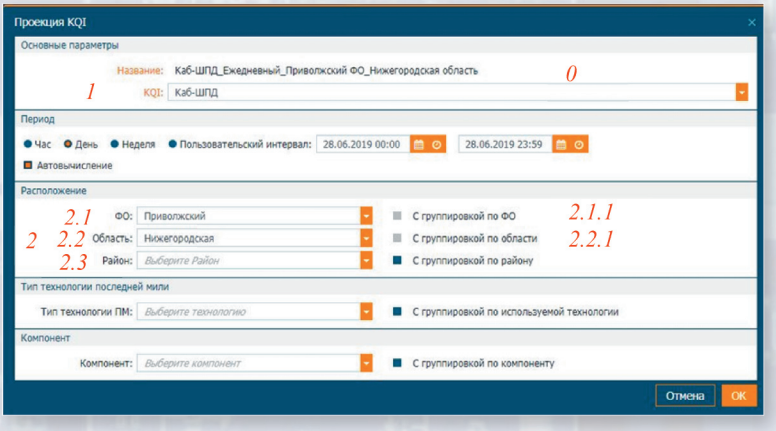

Рис. 4. Диалоговое окно вычисления качества сервиса с зависимыми взаимосвязями

Рисунки к статье В. И. Васильева, А. М. Вульфина, М. Б. Гузаирова, В. М. Картака, Л. Р. Черняховской

«ОЦЕНКА РИСКОВ КИБЕРБЕЗОПАСНОСТИ АСУ ТП ПРОМЫШЛЕННЫХ ОБЪЕКТОВ НА ОСНОВЕ ВЛОЖЕННЫХ НЕЧЕТКИХ КОГНИТИВНЫХ КАРТ»

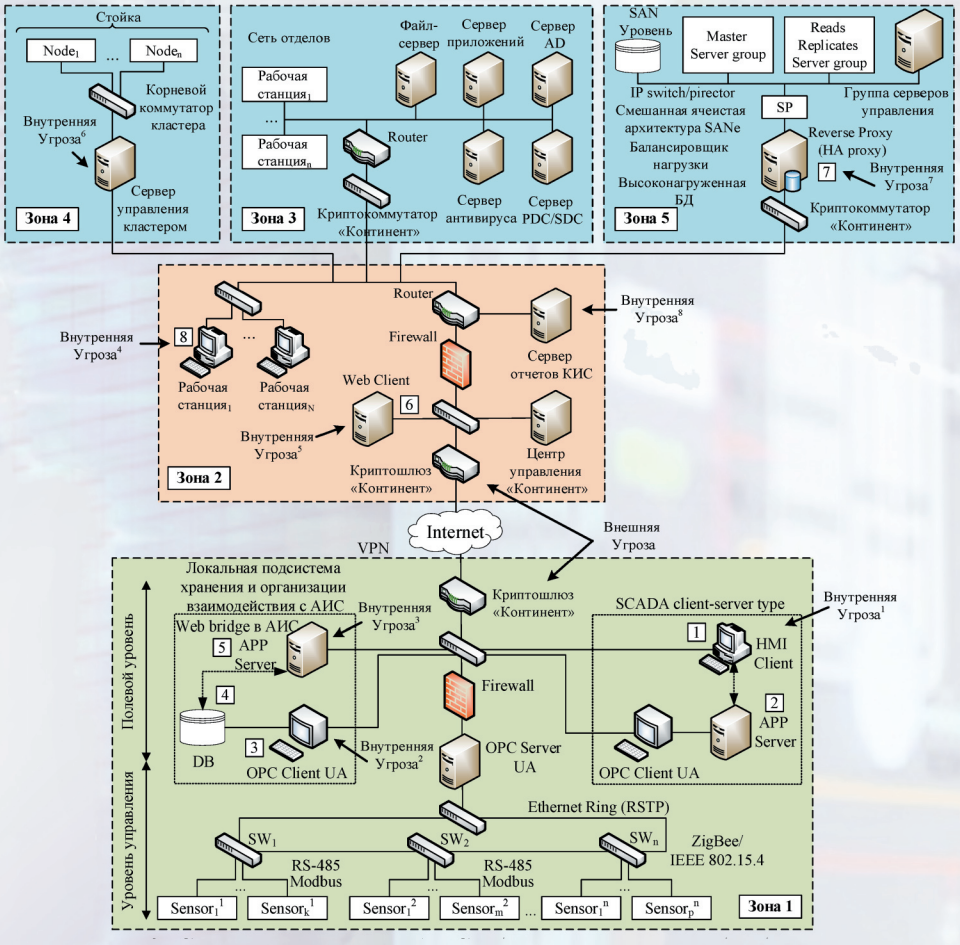

Рис. 2. Структурная схема АИС сбора, хранения и обработки ТМИ

ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ

Том 26
2020
№ 4

ТЕОРЕТИЧЕСКИЙ И ПРИКЛАДНОЙ НАУЧНО-ТЕХНИЧЕСКИЙ ЖУРНАЛ

Издается с ноября 1995 г. DOI 10.17587/issn.1684-6400

УЧРЕДИТЕЛЬ
Издательство "Новые технологии"

СОДЕРЖАНИЕ

ВЫЧИСЛИТЕЛЬНЫЕ СИСТЕМЫ И СЕТИ

Тарасов В. Н., Бахарева Н. Ф., Ахметшина Э. Г. Модели телетрафика на основе двойственных систем с запаздыванием с гиперэкспоненциальными и экспоненциальными распределениями 195

ПРОГРАММНАЯ ИНЖЕНЕРИЯ

Зарубин И. Б., Филинских А. Д., Балашова Т. И. Оценка тестового покрытия интерфейса пользователя в многокомпонентных информационных системах 203

БЕЗОПАСНОСТЬ ИНФОРМАЦИИ

Гурьянов Д. Ю., Костина А. А., Молдовян Н. А. Постквантовый протокол бесключевого шифрования 207

Васильев В. И., Вульфин А. М., Гузаиров М. Б., Картак В. М., Черняховская Л. Р. Оценка рисков кибербезопасности АСУ ТП промышленных объектов на основе вложенных нечетких когнитивных карт 213

Кабанов А. С. Оптимизация организационной структуры предприятия с учетом противодействия инсайдерской деятельности 222

ПРИКЛАДНЫЕ ИНФОРМАЦИОННЫЕ СИСТЕМЫ

Маничев В. Б., Митенкова Е. Ф., Фельдман Э. О., Кожевников Д. Ю., Соловьева Е. В. Достоверность и точность решения задач нуклидной кинетики 231

ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ В ЭКОНОМИКЕ И ПРОИЗВОДСТВЕ

Малахова А. И., Никулина Н. О., Черняховская Л. Р. Исследование содержания проблемы управления инновационными проектами в процессах стратегического планирования и развития производственно-экономических систем 239

Букалов Г. К., Бурыгин А. О., Панин И. Г. Применение методов построения сообществ для сегментации изображений текстильных строп 252

Информация о журнале доступна по сети Internet по адресу **http://novtex.ru/IT.**
Журнал включен в систему Российского индекса научного цитирования и базу данных RSCI на платформе Web of Science.
Журнал входит в Перечень научных журналов, в которых по рекомендации ВАК РФ должны быть опубликованы научные результаты диссертаций на соискание ученой степени доктора и кандидата наук.

INFORMATION TECHNOLOGIES
INFORMACIONNYE TEHNOLOGII

Vol. 26
2020
No. 4

THEORETICAL AND APPLIED SCIENTIFIC AND TECHNICAL JOURNAL

Published since November 1995

ISSN 1684-6400

CONTENTS

COMPUTING SYSTEMS AND NETWORKS

Tarasov V. N., Bakhareva N. F., Akhmetshina E. G. Teletrafic Models Based on Dual Systems with Delay with Hyperexponential and Exponential Distributions 195

SOFTWARE ENGINEERING

Zarubin I. B., Filinskih A. D., Balashova T. I. Evaluation of User Interface Test Coverage in Multicomponent Information Systems 203

INFORMATION SECURITY

Guryanov D. Yu., Kostina A. A., Moldovyan N. A. Post-Quantum Protocol for No-Key Encryption 207

Vasilyev V. I., Vulfin A. M., Guzairov M. B., Kartak V. M., Chernyakhovskaya L. R. Cybersecurity Risk Assessment of Industrial Objects' ACS of TP on the Basis of Nested Fuzzy Cognitive Maps Technology 213

Kabanov A. S. Optimization of the Organizational Structure of the Enterprise Taking into Account the Opposition of the Insider Activity 222

APPLICATION INFORMATION SYSTEMS

Manichev V. B., Mitenkova E. F., Feldman E. O., Kozhevnikov D. Ju., Solovjeva E. V. Reliability and calculation accuracy of nuclide kinetics problems 231

INFORMATION TECHNOLOGY IN THE ECONOMY AND PRODUCTION

Malakhova A. I., Nikulina N. O., Chernyakhovskaya L. R. Studding the Problem of Innovative Projects Management in Strategic Planning and Progress Processes of Production and Economic Systems 239

Bukalov G. K., Burygin A. O., Panin I. G. Application of Community Building Methods for Segmentation щf Textile Slings Images 252

Complete Internet version of the journal at site: **http://novtex.ru/IT.**
According to the decision of the Higher Certifying Commission of the Ministry of Education of Russian Federation, the journal is inscribed in "The List of the Leading Scientific Journals and Editions wherein Main Scientific Results of Theses for Doctor's or Candidate's Degrees Should Be Published"

УДК 621.391.1: 621.395 DOI: 10.17587/it.26.195-202

В. Н. Тарасов, д-р техн. наук, проф., зав. каф., e-mail: veniamin_tarasov@mail.ru,
Н. Ф. Бахарева, д-р техн. наук, проф., зав. каф., e-mail: nadin1956_04@inbox.ru,
Э. Г. Ахметшина, аспирант, e-mail: elyamalusha@mail.ru,
Поволжский государственный университет телекоммуникаций и информатики, г. Самара

Модели телетрафика на основе двойственных систем с запаздыванием с гиперэкспоненциальными и экспоненциальными распределениями

В теории массового обслуживания широко используются системы G/M/1 и M/G/1, при этом для первой системы до сих пор не существует решения в конечном виде в общем случае. Здесь G в первой системе по символике Кендалла означает произвольный закон распределения интервалов между требованиями входного потока, M — экспоненциальный закон времени обслуживания, а во второй системе — ровно наоборот. В статье рассматривается задача определения характеристик систем массового обслуживания (СМО) $H_2/M/1$ и $M/H_2/1$ с запаздыванием с гиперэкспоненциальным (H_2) и экспоненциальным (M) распределениями. Данная задача решается с использованием классического метода спектрального разложения решения интегрального уравнения Линдли. В качестве входных распределений для рассматриваемых систем выбраны вероятностные смеси сдвинутых вправо от нулевой точки экспоненциальных распределений и сдвинутые экспоненциальные распределения. Для таких законов распределений метод спектрального разложения позволяет получить решение в замкнутой форме. Показано, что в таких системах с запаздыванием среднее время ожидания требований в очереди меньше, чем в обычных системах. Это связано с тем, что операция сдвига во времени уменьшает коэффициенты вариаций интервалов между поступлениями и времени обслуживания, а как известно из теории массового обслуживания, среднее время ожидания требований связано с этими коэффициентами вариаций квадратичной зависимостью. СМО $H_2/M/1$ и $M/H_2/1$ с запаздыванием вполне могут быть использованы в качестве математической модели современного телетрафика.

Ключевые слова: *система с запаздыванием, двойственная пара $H_2/M/1$ и $M/H_2/1$, преобразование Лапласа, среднее время ожидания в очереди, интегральное уравнение Линдли*

Введение

Для моделирования работы каналов в системах передачи данных широко используют теорию массового обслуживания на основе законов распределений, преобразуемых по Лапласу. Однако в научной литературе нет данных по результатам исследований систем массового обслуживания (СМО) с запаздыванием, хотя в науке и технике вообще известны системы с запаздыванием. В работе [1] рассмотрен пример работы дилера по продаже автомобилей как системы с несколькими запаздываниями безотносительно к системам массового обслуживания. В статье [2] представлены результаты приближения очередей запросов к сети Интернет и мобильным сервисам в виде очередей с запаздыванием во времени. Показано, что если информация задерживается достаточно долго, может происходить бифуркация Хопфа, которая может вызвать нежелательные колебания в очередях.

В работе [3] впервые приведены результаты по исследованию классической системы M/M/1 со сдвинутыми экспоненциальными входными распределениями как системы с запаздыванием во времени, полученные классическим методом спектрального разложения решения интегрального уравнения Линдли (ИУЛ) [4]. В работе [3] показано, что среднее время ожидания требования в очереди в такой системе меньше, чем в классической системе M/M/1 при одинаковом коэффициенте загрузки, за счет того, что коэффициенты вариации времен поступления c_λ и обслуживания c_μ становятся меньше единицы при параметре запаздывания $t_0 > 0$. Таким образом, операция сдвига во времени трансформирует марков-

скую систему в немарковскую. За счет параметра сдвига $t_0 > 0$ законов распределений такое предположение о среднем времени ожидания можно сделать и для других систем массового обслуживания. Идея работы [3] развита для системы с запаздыванием во времени $H_2/H_2/1$ с гиперэкспоненциальными распределениями второго порядка в статье [5].

Другой подход к решению уравнения Линдли использован в работе [6]. Здесь вместо термина "спектральное разложение" [4] использована факторизация, а вместо функций $\psi_+(s)$ и $\psi_-(s)$ — компоненты факторизации $\omega_+(z, t)$ и $\omega_-(z, t)$ функции $1 - z\chi(t)$, где $\chi(t)$ — характеристическая функция случайной величины ξ с произвольной функцией распределения $C(t)$, а z — любое число из интервала $(-1, 1)$.

Постановка задачи

В работе ставится задача нахождения решения для среднего времени ожидания требований в очереди для двойственной пары СМО с гиперэкспоненциальными и экспоненциальными входными распределениями $H_2/M/1$ и $M/H_2/1$, а также для этих систем со сдвинутыми распределениями. Последние, в отличие от обычных систем, обозначим $H_2^-/M^-/1$ и $M^-/H_2^-/1$. Из теории массового обслуживания известно, что все остальные характеристики СМО являются производными от среднего времени ожидания. Для решения поставленной задачи выбираем классический метод спектрального разложения решения ИУЛ, в котором сохраним стандартные обозначения [4]. Таким образом, нам предстоит вначале найти закон распределения случайной величины — времени ожидания в системе — через спектральное разложение вида: $A^*(-s)B^*(s) - 1 = \psi_+(s)/\psi_-(s)$, где $\psi_+(s)$ и $\psi_-(s)$ — некоторые рациональные функции от s, которые возможно разложить на множители, $A^*(s)$ и $B^*(s)$ — преобразования Лапласа функций плотности $a(t)$ и $b(t)$, описывающих работу СМО. Функции $\psi_+(s)$ и $\psi_-(s)$ должны удовлетворять определенным условиям согласно работе [4]:

- для $\mathrm{Re}(s) > 0$ функция $\psi_+(s)$ является аналитической без нулей в этой полуплоскости;
- для $\mathrm{Re}(s) < D$ функция $\psi_-(s)$ является аналитической без нулей в этой полуплоскости, где D — некоторая положительная константа, определяемая из условия:

$$\lim_{t\to\infty} a(t)/\mathbf{e}^{-Dt} < \infty.$$

Кроме того, функции $\psi_+(s)$ и $\psi_-(s)$ должны удовлетворять следующим условиям:

$$\lim_{|s|\to\infty,\,\mathrm{Re}(s)>0} \frac{\psi_+(s)}{s} = 1; \quad \lim_{|s|\to\infty,\,\mathrm{Re}(s)<D} \frac{\psi_-(s)}{s} = -1.$$

Решение задачи для системы $H_2/M/1$ с запаздыванием

Рассмотрим СМО $H_2^-/M^-/1$, на вход которой поступают требования, случайные интервалы между которыми распределены с функцией плотности

$$a(t) = \begin{cases} p\lambda_1\mathbf{e}^{-\lambda_1(t-t_0)} + (1-p)\lambda_2\mathbf{e}^{-\lambda_2(t-t_0)}, & t > t_0; \\ 0, \quad 0 \leqslant t \leqslant t_0, \end{cases} \tag{1}$$

а время обслуживания

$$b(t) = \begin{cases} \mu\mathbf{e}^{-\mu(t-t_0)}, & t > t_0; \\ 0, \quad 0 \leqslant t \leqslant t_0. \end{cases} \tag{2}$$

В функции (1) вероятность $p \in (0, 1)$, так как это распределение представляет собой сдвинутую вправо от нулевой точки на величину t_0 вероятностную смесь экспоненциальных распределений с тремя параметрами (p, λ_1, λ_2). Теперь нужно решить задачу определения параметров распределений (1) и (2). Для этого определим числовые характеристики интервала между соседними требованиями входного потока для новой системы, воспользовавшись преобразованием Лапласа функции (1):

$$A^*(s) = \left[p\frac{\lambda_1}{s+\lambda_1} + (1-p)\frac{\lambda_2}{s+\lambda_2} \right] \mathbf{e}^{-t_0 s}.$$

Значение первой производной функции $A^*(s)$ со знаком минус в точке $s = 0$ равно:

$$-\frac{dA^*(s)}{ds}\Big|_{s=0} = p\lambda_1^{-1} + (1-p)\lambda_2^{-1} + t_0.$$

Отсюда среднее значение интервалов между соседними требованиями:

$$\overline{\tau}_\lambda = p\lambda_1^{-1} + (1-p)\lambda_2^{-1} + t_0.$$

Значение второй производной функции $A^*(s)$ в точке $s = 0$ дает второй начальный момент интервала поступления:

$$\overline{\tau_\lambda^2} = 2[p\lambda_1^{-2} + (1-p)\lambda_2^{-2}] + t_0^2 + 2t_0[p\lambda_1^{-1} + (1-p)\lambda_2^{-1}].$$

Используя полученные выражения для начальных моментов, определим значение квад-

рата коэффициента вариации интервала между поступлениями требований:

$$c_\lambda^2 = \frac{[(1-p^2)\lambda_1^2 - 2\lambda_1\lambda_2 p(1-p) + p(2-p)\lambda_2^2]}{[t_0\lambda_1\lambda_2 + (1-p)\lambda_1 + p\lambda_2]^2}.$$

Далее для определения неизвестных параметров распределения (1) λ_1, λ_2, p запишем следующую систему уравнений по известному методу моментов:

$$p\lambda_1^{-1} + (1-p)\lambda_2^{-1} + t_0 = \overline{\tau}_\lambda; \quad (3)$$

$$\frac{[(1-p^2)\lambda_1^2 - 2\lambda_1\lambda_2 p(1-p) + p(2-p)\lambda_2^2]}{[t_0\lambda_1\lambda_2 + (1-p)\lambda_1 + p\lambda_2]^2} = c_\lambda^2. \quad (4)$$

Исходя из вида уравнения (3) положим

$$\lambda_1 = 2p/(\overline{\tau}_\lambda - t_0); \quad \lambda_2 = 2(1-p)/(\overline{\tau}_\lambda - t_0) \quad (5)$$

и потребуем выполнения условия (4). Подставив решение (5) в равенство (4), получим уравнение четвертой степени относительно параметра p. Решив его с учетом условия $0 < p < 1$, отбросив тривиальные решения $p = 0$ и $p = 1$, определяем параметр p:

$$p = \frac{1}{2} \pm \sqrt{\frac{1}{4} - \frac{(\overline{\tau}_\lambda - t_0)^2}{2[(\overline{\tau}_\lambda - t_0)^2 + c_\lambda^2\overline{\tau}_\lambda^2]}}, \quad (6)$$

при этом можно воспользоваться любым из этих значений для p. Такой подход к аппроксимации законов распределения гиперэкспоненциальным распределением описан в работе [7]. Заметим, что в соотношении (4) коэффициент вариации $c_\lambda > 0$. Подобный подход к аппроксимации законов распределений применен в работах [8—15].

Для определения числовых характеристик времени обслуживания для распределения (2) воспользуемся полученными в работе [3] равенствами для среднего значения $\overline{\tau}_\mu$ и коэффициента вариации времени обслуживания c_μ:

$$\mu^{-1} + t_0 = \overline{\tau}_\mu; \quad (7)$$

$$(1 + \mu t_0)^{-1} = c_\mu. \quad (8)$$

Заметим, что здесь коэффициент вариации $c_\mu < 1$ [3]. Из выражения (7) выразим интенсивность обслуживания

$$\mu = (\overline{\tau}_\mu - t_0)^{-1} \quad (9)$$

и, подставив (9) в (8), найдем параметр сдвига t_0

$$t_0 = \overline{\tau}_\mu(1 - c_\mu). \quad (10)$$

Выражение (10) будет определять диапазон изменения параметра сдвига t_0 для данной системы.

Вывод решения для среднего времени ожидания в системе $H_2^-/M^-/1$

Запишем преобразования Лапласа для функций (1) и (2) при $t_0 = 0$, т.е. для обычных распределений без сдвига:

$$A^*(s) = p\frac{\lambda_1}{s+\lambda_1} + (1-p)\frac{\lambda_2}{s+\lambda_2}; \quad B^*(s) = \frac{\mu}{\mu+s}.$$

Тогда выражение для спектрального разложения решения ИУЛ $A^*(-s)B^*(s) - 1 = \psi_+(s)/\psi_-(s)$ для обычной системы $H_2/M/1$:

$$\frac{\psi_+(s)}{\psi_-(s)} = \left[p\frac{\lambda_1}{\lambda_1 - s} + (1-p)\frac{\lambda_2}{\lambda_2 - s}\right]\frac{\mu}{\mu+s} - 1 = \frac{-s(s+s_1)(s-s_2)}{(\lambda_1 - s)(\lambda_2 - s)(\mu+s)}, \quad (11)$$

где $-s_1 = -(\sqrt{c_1^2/4 + c_0} - c_1/2)$ — отрицательный корень; $s_2 = \sqrt{c_1^2/4 + c_0} + c_1/2$ — положительный корень многочлена $s^2 - c_1 s - c_0$ с коэффициентами $c_0 = \mu[\lambda_1(1-p) + \lambda_2 p] - \lambda_1\lambda_2$ и $c_1 = \lambda_1 + \lambda_2 - \mu$, которые выражаются через параметры распределений (1) и (2) при $t_0 = 0$.

Теперь найдем преобразования Лапласа для сдвинутых функций (1) и (2). Для этого воспользуемся теоремой запаздывания как свойством преобразования Лапласа: для преобразуемой по Лапласу функции $f(t)$ при любом $t_0 > 0$ справедливо равенство $L[f(t-t_0)] = \mathbf{e}^{-st_0}F^*(s)$, где $\mathrm{Re}(s) > 0$. Тогда справедливы равенства

$$A^*(s) = \left[p\frac{\lambda_1}{s+\lambda_1} + (1-p)\frac{\lambda_2}{s+\lambda_2}\right]\mathbf{e}^{-t_0 s};$$

$$B^*(s) = \frac{\mu}{s+\mu}\mathbf{e}^{-t_0 s}.$$

Спектральное разложение решения ИУЛ $A^*(-s)B^*(s) - 1 = \psi_+(s)/\psi_-(s)$ для системы $H_2^-/M^-/1$ примет вид

$$\frac{\psi_+(s)}{\psi_-(s)} = \left[p\frac{\lambda_1}{\lambda_1 - s} + (1-p)\frac{\lambda_2}{\lambda_2 - s}\right] \times \mathbf{e}^{t_0 s}\left(\frac{\mu}{\mu+s}\right)\mathbf{e}^{-t_0 s} - 1 =$$

$$= \frac{s(s^2 - c_1 s - c_0)}{(\lambda_1 - s)(\lambda_2 - s)(\mu+s)} = \frac{-s(s+s_1)(s-s_2)}{(\lambda_1 - s)(\lambda_2 - s)(\mu+s)}.$$

Здесь показатели степени у экспонент в выражении для спектрального разложения обнуляются, и тем самым операция сдвига в спектральном разложении нивелируется. Таким образом, основное выражение $A^*(-s)B^*(s) - 1 = \psi_+(s)/\psi_-(s)$ для метода спектрального разложения для системы с запаздыванием $H_2^-/M^-/1$ имеет такой же вид (11), как и для обычной системы $H_2/M/1$, следовательно, спектральное разложение в этом случае инвариантно к операции сдвига во времени закона распределения.

В последнем выражении $-s_1 = c_1/2 - \sqrt{c_1^2/4 + c_0}$ — отрицательный корень, а $s_2 = c_1/2 + \sqrt{c_1^2/4 + c_0}$ — положительный корень многочлена $s^2 - c_1 s - c_0 = 0$ в числителе разложения с коэффициентами $c_0 = \mu[(1 - p)\lambda_1 + p\lambda_2] - \lambda_1\lambda_2$ и $c_1 = \lambda_1 + \lambda_2 - \mu$. Компоненты спектрального разложения $\psi_+(s)$ и $\psi_-(s)$ с учетом условий, которым они должны удовлетворять, в данном случае имеют вид: $\psi_+(s) = s(s + s_1)/(s + \mu)$, $\psi_-(s) = (s - \lambda_1)(\lambda_2 - s)/(s - s_2)$.

Далее по методике спектрального разложения найдем константу K:

$$K = \lim_{|s|\to 0} \frac{\psi_+(s)}{s} = \lim_{|s|\to 0} \frac{(s + s_1)}{(s + \mu)} = \frac{s_1}{\mu},$$

которая представляет собой вероятность того, что поступающее в систему требование застает ее свободной. Построим функцию $\Phi_+(s) = K/\psi_+(s)$, через которую найдем преобразование Лапласа функции плотности времени ожидания: $W^*(s) = s\Phi_+(s) = \dfrac{s_1(s + \mu)}{\mu(s + s_1)}$. Производная от функции $W^*(s)$ со знаком минус в точке $s = 0$ и даст среднее время ожидания:

$$-\left.\frac{dW^*(s)}{ds}\right|_{s=0} = -\left.\frac{d}{ds}\left[\frac{s_1(s + \mu)}{\mu(s + s_1)}\right]\right|_{s=0} = \frac{1}{s_1} - \frac{1}{\mu}.$$

Окончательно среднее время ожидания в системе в стационарном режиме, определяемом условием $0 < \rho = \overline{\tau}_\mu/\overline{\tau}_\lambda < 1$, где ρ — коэффициент загрузки системы, выражается формулой

$$\overline{W} = 1/s_1 - 1/\mu, \qquad (12)$$

где $s_1 = (\sqrt{c_1^2/4 + c_0} - c_1/2)$ — абсолютное значение отрицательного корня $-s_1$.

Тем самым, мы можем воспользоваться для системы с запаздыванием $H_2^-/M^-/1$ известным результатом по среднему времени ожидания для обычной системы $H_2/M/1$ (12), но уже с измененными вследствие операции сдвига параметрами согласно выражениям (5), (6), (9) и (10).

Тогда алгоритм определения среднего времени ожидания для системы $H_2^-/M^-/1$ при заданных входных параметрах $\overline{\tau}_\lambda, \overline{\tau}_\mu, c_\lambda, c_\mu$ сводится к последовательному нахождению неизвестных параметров распределений (1) и (2) $\lambda_1, \lambda_2, p, \mu$ из выражений (5), (6), (9), затем — к нахождению нужного корня $-s_1$ квадратного уравнения $s^2 - c_1 s - c_0 = 0$ и к применению расчетной формулы (12).

В табл. 1 приведены результаты расчетов времени ожидания для системы $H_2^-/M^-/1$ в пакете MathCAD при коэффициентах загрузки $\rho = 0{,}1$; 0,5 и 0,9 при нормированном времени обслуживания $\overline{\tau}_\mu = 1$ и коэффициентах вариаций $c_\lambda = 2$; 4; 8 и $c_\mu = 0{,}1$; 0,5, 0,9. В этом случае перечисленным значениям c_μ согласно (8) соответствуют значения параметра запаздывания $t_0 = 0{,}9$; 0,5 и 0,1. В правой колонке для сравнения приведены результаты для обычной системы $H_2/M/1$. Результаты расчетов полностью подтверждают справедливость нашего предположения о времени ожидания в системе с запаздыванием.

Как видно из табл. 1, с уменьшением значения параметра сдвига t_0 среднее время ожидания в системе с запаздыванием $H_2^-/M^-/1$ стремится к значению среднего времени ожидания в обычной системе $H_2/M/1$, что подтверждает полную адекватность построенной модели. Вместе с тем, операция сдвига в зависимости от параметра сдвига t_0 во много раз уменьшает среднее время ожидания в системе с запаздыванием $H_2^-/M^-/1$.

Таблица 1

Результаты вычислительных экспериментов для СМО $H_2^-/M^-/1$ и $H_2/M/1$

Входные параметры		Среднее время ожидания			
ρ	c_μ / c_λ	Для СМО $H_2^-/M^-/1$			Для СМО $H_2/M/1$
		$c_\mu = 0{,}1$ ($t_0 = 0{,}9$)	$c_\mu = 0{,}5$ ($t_0 = 0{,}5$)	$c_\mu = 0{,}9$ ($t_0 = 0{,}1$)	
0,1	2	0,001	0,05	0,15	0,19
	4	0,002	0,06	0,18	0,23
	8	0,002	0,06	0,20	0,25
0,5	2	0,02	0,60	1,82	2,16
	4	0,02	0,84	3,80	4,83
	8	0,02	0,95	7,02	10,40
0,9	2	0,92	15,46	21,12	22,41
	4	1,35	57,91	73,18	75,79
	8	1,64	227,6	281,2	289,1

Вывод решения для среднего времени ожидания в системе $M^-/H_2^-/1$

В двойственной системе $M^-/H_2^-/1$ распределения (1) и (2), а также их преобразования Лапласа поменяются местами. Закон распределения интервалов между соседними требованиями входного потока в виде функции плотности будет иметь вид

$$a(t) = \begin{cases} \lambda \mathbf{e}^{-\lambda(t-t_0)}, & t > t_0; \\ 0, & 0 \leqslant t \leqslant t_0, \end{cases} \qquad (13)$$

а время обслуживания задается функцией плотности

$$b(t) = \begin{cases} q\mu_1 \mathbf{e}^{-\mu_1(t-t_0)} + (1-q)\mu_2 \mathbf{e}^{-\mu_2(t-t_0)}, & t > t_0; \\ 0, & 0 \leqslant t \leqslant t_0. \end{cases} \qquad (14)$$

Преобразования Лапласа функций (13) и (14) будут соответственно равны

$$A^*(s) = \left(\frac{\lambda}{\lambda + s}\right)\mathbf{e}^{-t_0 s};$$

$$B^*(s) = \left[q\frac{\mu_1}{s+\mu_1} + (1-q)\frac{\mu_2}{s+\mu_2}\right]\mathbf{e}^{-t_0 s}.$$

Тогда спектральное разложение для решения ИУЛ для системы $M^-/H_2^-/1$ будет иметь вид

$$\frac{\psi_+(s)}{\psi_-(s)} =$$

$$= \left(\frac{\lambda}{\lambda - s}\right)\mathbf{e}^{t_0 s}\left[q\frac{\mu_1}{\mu_1 + s} + (1-q)\frac{\mu_2}{\mu_2 + s}\right]\mathbf{e}^{-t_0 s} - 1 =$$

$$= \frac{s(s^2 + l_1 s + l_0)}{(\lambda_1 - s)(\mu_1 + s)(\mu_2 + s)} = \frac{s(s+\sigma_1)(s+\sigma_2)}{(\lambda_1 - s)(\mu_1 + s)(\mu_2 + s)},$$

где $-\sigma_1 = -(l_1/2 - \sqrt{l_1^2/4 - l_0})$, $-\sigma_2 = -(l_1/2 + \sqrt{l_1^2/4 - l_0})$ — два различных действительных отрицательных корня квадратного уравнения $s^2 + l_1 s + l_0 = 0$ с коэффициентами $l_0 = \mu_1\mu_2 - \lambda[(1-q)\mu_1 + q\mu_2]$ и $l_1 = \mu_1 + \mu_2 - \lambda$.

Здесь опять показатели степени у экспонент в выражении обнуляются, и тем самым операция сдвига в спектральном разложении нивелируется. Таким образом, основное выражение $A^*(-s)B^*(s) - 1 = \psi_+(s)/\psi_-(s)$ для метода спектрального разложения для системы с запаздыванием $M^-/H_2^-/1$ будет иметь такой же вид, как и для обычной системы $M/H_2/1$. Окончательно спектральное разложение можно записать в виде

$$\frac{\psi_+(s)}{\psi_-(s)} = \frac{s(s+\sigma_1)(s+\sigma_2)}{(\lambda_1 - s)(\mu_1 + s)(\mu_2 + s)}. \qquad (15)$$

Наличие таких корней σ_1 и σ_2 следует из существования и единственности такого разложения [4] или же факторизации [6].

Компоненты спектрального разложения $\psi_+(s)$ и $\psi_-(s)$ в данном случае имеют вид $\psi_+(s) = \dfrac{s(s+\sigma_1)(s+\sigma_2)}{(s+\mu_1)(s+\mu_2)}$, $\psi_-(s) = \lambda - s$. Далее по методике спектрального разложения найдем константу K:

$$K = \lim_{|s|\to 0}\frac{\psi_+(s)}{s} = \lim_{|s|\to 0}\frac{(s+\sigma_1)(s+\sigma_2)}{(s+\mu_1)(s+\mu_2)} = \frac{\sigma_1\sigma_2}{\mu_1\mu_2}.$$

Через константу K найдем преобразование Лапласа функции плотности времени ожидания:

$$W^*(s) = s\frac{K}{\psi_+(s)} = \frac{\sigma_1\sigma_2(s+\mu_1)(s+\mu_2)}{\mu_1\mu_2(s+\sigma_1)(s+\sigma_2)}.$$

Производная от функции $W^*(s)$ со знаком минус в точке $s = 0$ и даст среднее время ожидания:

$$-\frac{dW^*(s)}{ds}\bigg|_{s=0} = -\frac{d}{ds}\left[\frac{\sigma_1\sigma_2(s+\mu_1)(s+\mu_2)}{\mu_1\mu_2(s+\sigma_1)(s+\sigma_2)}\right]\bigg|_{s=0} =$$

$$= \frac{\sigma_1 + \sigma_2}{\sigma_1\sigma_2} - \frac{\mu_1 + \mu_2}{\mu_1\mu_2}.$$

Окончательно среднее время ожидания в стационарном режиме в этом случае примет вид

$$\bar{W} = \frac{\sigma_1 + \sigma_2}{\sigma_1\sigma_2} - \frac{\mu_1 + \mu_2}{\mu_1\mu_2}. \qquad (16)$$

Для практического применения расчетной формулы (16) требуется записать выражения для определения неизвестных параметров (13) и (14). Для среднего значения интервала входного потока требований $\bar{\tau}_\lambda$ и коэффициента вариации c_λ имеем:

$$\lambda^{-1} + t_0 = \bar{\tau}_\lambda; \qquad (17)$$

$$(1 + \lambda t_0)^{-1} = c_\lambda. \qquad (18)$$

Заметим, что здесь коэффициент вариации $c_\lambda < 1$ при $t_0 > 0$ [2]. Из выражения (17) выразим интенсивность входного потока:

$$\lambda = (\bar{\tau}_\lambda - t_0)^{-1}. \qquad (19)$$

Неизвестные параметры распределения (14) μ_1, μ_2, q определяются аналогично для системы $H_2^-/M^-/1$ заменой символа λ на μ:

$$\mu_1 = 2q/(\overline{\tau}_\mu - t_0);$$
$$\mu_2 = 2(1-q)/(\overline{\tau}_\mu - t_0); \qquad (20)$$
$$q = \frac{1}{2} \pm \sqrt{\frac{1}{4} - \frac{(\overline{\tau}_\mu - t_0)^2}{2[(\overline{\tau}_\mu - t_0)^2 + c_\mu^2 \overline{\tau}_\mu^2]}}.$$

Запишем квадрат коэффициента вариации времени обслуживания:

$$\frac{[(1-q^2)\mu_1^2 - 2\mu_1\mu_2 q(1-q) + q(2-q)\mu_2^2]}{[t_0\mu_1\mu_2 + (1-q)\mu_1 + q\mu_2]^2} = c_\mu^2$$

и оценим влияние на него параметра сдвига $t_0 > 0$. Сравнение с квадратом коэффициента вариации времени обслуживания при $t_0 = 0$, т.е. в случае несдвинутого распределения, показывает, что c_μ уменьшается в $1 + t_0\mu_1\mu_2/[\mu_1(1-q) + q\mu_2]$ раз.

Тогда алгоритм определения времени ожидания для системы с запаздыванием $M^-/H_2^-/1$ сводится к последовательному решению уравнений (20), (19), (18) при заданных входных параметрах: $\overline{\tau}_\lambda$, $\overline{\tau}_\mu$, c_λ, c_μ, t_0, а затем к нахождению отрицательных корней σ_1, σ_2 многочлена $s^2 + h_1 s + h_0$ и использованию расчетной формулы (16). В табл. 2 приведены результаты расчетов времени ожидания в пакете MathCAD при коэффициентах загрузки $\rho = 0{,}1$; 0,5 и 0,9 при нормированном времени обслуживания $\overline{\tau}_\mu = 1$ и коэффициенте вариации $c_\mu = 2$; 4; 8 для обычной системы $M/H_2/1$. Согласно равенству (18) при таких значениях коэффициента загрузки ρ и параметре сдвига $t_0 = 0{,}9$ коэффициент вариации c_λ примет значения $c_\lambda = 0{,}91$; 0,55; 0,19 соответственно. Согласно тому факту, что коэффициент вариации c_μ при таких входных данных уменьшается в $1 + t_0\mu_1\mu_2/[\mu_1(1-q) + q\mu_2] = 1{,}9$ раза, для системы $M^-/H_2^-/1$ коэффициенты вариации будут равны $c_\mu = 1{,}05$; 2,11; 4,21. В правой колонке для сравнения приведены результаты для обычной системы $M/H_2/1$. Результаты расчетов полностью подтверждают справедливость нашего предположения о времени ожидания в системе с запаздыванием.

Таблица 2

Результаты экспериментов для СМО $M^-/H_2^-/1$ и $M/H_2/1$

Входные параметры		Среднее время ожидания					
ρ	c_λ \ c_μ	Для системы $M^-/H_2^-/1$			Для системы $M/H_2/1$		
		$c_\mu = 1{,}05$	$c_\mu = 2{,}11$	$c_\mu = 4{,}21$	$c_\mu = 2$	$c_\mu = 4$	$c_\mu = 8$
0,1	0,91 ($t_0 = 0{,}9$)	0,06	0,25	0,99	0,28	0,94	3,61
0,5	0,55 ($t_0 = 0{,}9$)	0,56	2,23	8,87	2,50	8,50	32,50
0,9	0,15 ($t_0 = 0{,}9$)	5,01	20,08	79,80	22,50	76,50	292,50

Заключение

Полученные результаты приводят к следующим выводам. Операция сдвига во времени в законах распределений уменьшает коэффициенты вариаций интервала между поступлениями и времени обслуживания требований. В связи с тем, что среднее время ожидания в системе G/G/1 связано с коэффициентами вариаций интервалов поступления и обслуживания квадратичной зависимостью, среднее время ожидания в системе с запаздыванием будет меньше, чем в обычной системе при одинаковом коэффициенте загрузки. Например, для системы $H_2^-/M^-/1$ при параметре сдвига $t_0 = 0{,}9$ (северо-западная клетка табл. 1) коэффициент вариации времени обслуживания уменьшается с 1 для обычной системы до 0,1 для системы с запаздыванием, а время ожидания уменьшается с 0,19 до 0,001 единицы времени. Для системы $M^-/H_2^-/1$ коэффициент вариации времени обслуживания уменьшается с 8 для обычной системы до 4,21 для системы с запаздыванием, а время ожидания уменьшается с 292,5 до 79,8 единицы времени (табл. 2), т.е. почти в четыре раза.

Практическое применение полученных результатов при анализе современного телетрафика просматривается следующим образом: при коэффициентах вариации c, больших 1, закон распределения можно аппроксимировать гиперэкспоненциальным распределением 2-го порядка H_2 либо H_2^-. При этом необходимо учесть уникальное свойство гиперэкспоненциального распределения, состоящее в том, что оно может определяться как двумя первыми моментами, так и тремя моментами [7, 8]. С точки зрения теории вероятностей описание закона распределения на уровне трех моментов все же точнее, но в таком случае применение изложенных результатов потребует большего объема вычислений из-за необходимости решения систем трех уравнений с использованием известного метода моментов.

Изложенные результаты справедливы только для одинаковых параметров сдвига t_0 для распределения времени между поступлениями требований и времени их обслуживания.

Список литературы

1. **Медоуз Д. Х.** Азбука системного мышления. М.: БИНОМ. Лаборатория знаний, 2011. 343 с.

2. **Novitzky S., Pender J., Rand J., R. H., Wesson E.** Nonlinear Dynamics in Queueing Theory: Determining the Size of Oscillations in Queues with Delay // SIAM J. Appl. Dyn. Syst. 2019. Vol. 18, N. 1. P. 279—311. DOI: https://doi.org/10.1137/18M1170637.

3. **Тарасов В. Н., Бахарева Н. Ф., Блатов И. А.** Анализ и расчет системы массового обслуживания с запаздыванием // Автоматика и телемеханика. 2015. № 11. С. 51—59. DOI: 10.1134/S0005117915110041.

4. **Клейнрок Л.** Теория массового обслуживания. М.: Машиностроение, 1979. 432 с.

5. **Тарасов В. Н., Ахметшина Э. Г.** Среднее время ожидания в системе массового обслуживания $H_2/H_2/1$ с запаздыванием // Вестн. Сам. гос. техн. ун-та. Сер. физ.-мат. науки. 2018. № 4. С. 702—713. DOI: 10.14498/vsgtu1607.

6. **Бочаров П. П., Печинкин А. В.** Теория массового обслуживания. М.: Изд-во РУДН, 1995. 529 с.

7. **Тарасов В. Н., Бахарева Н. Ф., Липилина Л. В.** Математическая модель телетрафика на основе системы G/M/1 и результаты вычислительных экспериментов // Информационные технологии. 2016. Т.22, № 2. С. 121—126.

8. **Тарасов В. Н., Карташевский И. В.** Способы аппроксимации входных распределений для системы G/G/1 и анализ полученных результатов // Системы управления и информационные технологии. 2015. № 3. С. 182—185.

9. **Алиев Т. И.** Основы моделирования дискретных систем. СПб: СПбГУ ИТМО, 2009. 363 с.

10. **Алиев Т. И.** Аппроксимация вероятностных распределений в моделях массового обслуживания // Научно-технический вестник информационных технологий, механики и оптики. 2013. № 2(84). С. 88—93.

11. **Whitt W.** Approximating a point process by a renewal process: two basic methods // Operation Research. 1982. N. 1. P. 125—147.

12. **Myskja A.** An improved heuristic approximation for the GI/GI/1 queue with bursty arrivals // Teletraffic and datatraffic in a Period of Change, ITC-13. Elsevier Science Publishers. 1991. P. 683—688.

13. **Jennings O. B., Pender J.** Comparisons of ticket and standard queues. Queueing Systems. 2016. Vol. 84, N. 1. P. 145—202.

14. **Тарасов В. Н., Горелов Г. А., Ушаков Ю. А.** Восстановление моментных характеристик распределения интервалов между пакетами входящего трафика // Инфокоммуникационные технологии. 2014. № 2. С. 40—44.

15. **Legros B.** M/G/1 queue with event-dependent arrival rates // Queueing Systems. 2018. Vol. 89, N. 3. P. 269—301. DOI: https://doi.org/10.1007 /s11134-017-9557-7.

16. **Тарасов В. Н.** Вероятностное компьютерное моделирование сложных систем. Самара: СНЦ РАН, 2002. 194 с.

V. N. Tarasov, D. Sc., Professor, Head of Chair, e-mail: veniamin_tarasov@mail.ru,
N. F. Bakhareva, D. Sc., Professor, Head of Chair, e-mail: nadin1956_04@inbox.ru,
E. G. Akhmetshina, Postgraduate,
Povolzhsky State University of Telecommunications and Informatics, Samara, 443010, Russian Federation

Teletrafic Models Based on Dual Systems with Delay with Hyperexponential and Exponential Distributions

In queuing theory, the G/M/1 and M/G/1 systems are widely used, while for the first system there is still no final solution in the general case. Here G in the first system according to Kendall symbolism means an arbitrary law of the distribution of intervals between the requirements of the input flow, M is the exponential law of service time, and in the second system, it is exactly the opposite. The article considers the problem of determining the characteristics of queuing systems (QS) $H_2/M/1$ and $M/H_2/1$ with delay with hyperexponential (H_2) and exponential (M) distributions. This problem is solved using the classical method of spectral decomposition of the solution of the Lindley integral equation. As input distributions for the systems under consideration, probabilistic mixtures of exponential distributions shifted to the right from the zero point and shifted exponential distributions are selected. For such distribution laws, the spectral decomposition method allows one to obtain a closed-form solution. It is shown that in such systems with delay, the average waiting time for requirements in the queue is shorter than in conventional systems. This is because the time shift operation reduces the coefficient of variation of the intervals between receipts and the service time, and as is known from the queuing theory, the average waiting time for requirements is associated with these coefficients of variation by a quadratic dependence. QS $H_2/M/1$ and $M/H_2/1$ with delay can very well be used as a mathematical model of modern teletraffic.

Keywords: *Delayed system, dual pair $H_2/M/1$ and $M/H_2/1$, Laplace transform, average waiting time in a queue, Lindley integral equation*

DOI: 10.17587/it.26.195-202

References

1. **Meadows D. Kh.** The ABC of systemic thinking, Moscow, BINOM. Laboratory of Knowledge, 2011, 343 p. (in Russian).

2. **Novitzky S., Pender J., Rand J. R. H., Wesson E.** Nonlinear Dynamics in Queuing Theory: Determining the Size of Oscillations in Queues with Delay**,** *SIAM J. Appl. Dyn. Syst.*, 2019, vol. 18, no. 1, pp. 279—311, doi: https://doi.org/10.1137/18M1170637.

3. **Tarasov V. N., Bakhareva N. F., Blatov I. A.** Analysis and calculation of queuing systems with delay, *Automation and Telemechanics*, 2015, no. 11, pp. 51—59, doi: 10.1134 / S0005117915110041 (in Russian).

4. **Kleinrock L.** Theory of queuing, Moscow, Mechanical Engineering, 1979, 432 p. (in Russian).

5. **Tarasov V. N., Akhmetshina E. G.** The average waiting time in the queuing system H2 / H2 / 1 with delay, *Vestn. Itself. state tech. un-that. Ser. Phys.-mat. Science*, 2018, no. 4, pp. 702—713, doi: 10.14498 / vsgtu1607 (in Russian).

6. **Bocharov P. P., Pechinkin A. V.** Queuing theory, Moscow, Publishing House of RUDN, 1995, 529 p. (in Russian).

7. **Tarasov V. N., Bakhareva N. F., Lipilina L. V.** The mathematical model of teletraffic based on the G/M/1 system and the results of computational experiments, *Informacionnye Technologii*, 2016, vol. 22, no. 2, pp. 121—126 (in Russian).

8. **Tarasov V. N., Kartashevsky I. V.** Methods for approximating input distributions for the G/G/1 system and analysis of the results, *Control Systems And Information Technology*, 2015, no. 3, pp. 182—185 (in Russian).

9. **Aliev T. I.** Fundamentals of modeling discrete systems, St. Petersburg, Publishing House of St. Petersburg State University ITMO, 2009, 363 p. (in Russian).

10. **Aliev T. I.** Approximation of probability distributions in queuing models, *Scientific and Technical Bulletin of Information Technologies, Mechanics and Optics*. 2013, no. 2 (84), pp. 88—93 (in Russian).

11. **Whitt W.** Approximating a point process by a renewal process: two basic methods, *Operation Research*, 1982, no. 1, pp. 125—147.

12. **Myskja A.** An improved heuristic approximation for the GI/GI/1 queue with bursty arrivals*, Teletraffic and datatraffic in a Period of Change, ITC-13*, Elsevier Science Publishers, 1991, pp. 683—688.

13. **Jennings O. B., Pender J.** Comparisons of ticket and standard queues, *Queueing Systems,* 2016, vol. 84, no. 1, pp. 145—202.

14. **Tarasov V. N., Gorelov G. A., Ushakov Yu. A.** Recovery of moment characteristics of the distribution of intervals between packets of incoming traffic, *Infocommunication Technologies*, 2014, no. 2, pp. 40—44 (in Russian).

15. **Legros B.** M / G / 1 queue with event-dependent arrival rates, *Queueing Systems*, 2018, vol. 89, no. 3, pp. 269—301, doi: https://doi.org/10.1007/s11134-017-9557-7.

16. **Tarasov V. N.** Probabilistic computer modeling of complex systems, Samara, SSC RAS, 2002, 194 p. (in Russian).

УДК 004.054 DOI: 10.17587/it.26.203-206

И. Б. Зарубин, ст. преподаватель, e-mail: simarglz@yandex.ru,
А. Д. Филинских, канд. техн. наук, доц., зав. кафедрой, e-mail: alexfil@yandex.ru,
Т. И. Балашова, канд. техн. наук, доц., e-mail: tibalashova@mail.ru,
Нижегородский Государственный Технический Университет, г. Нижний Новгород

Оценка тестового покрытия интерфейса пользователя в многокомпонентных информационных системах

Рассмотрен метод оценки полноты покрытия проверочными сценариями графического интерфейса пользователя в информационных системах, которые состоят из множества взаимосвязанных модулей, путем построения ориентированного графа возможных взаимосвязей элементов информационной системы с приданием веса каждой связи и нормировкой по числу взаимосвязей. Описаны достоинства и недостатки рассмотренного метода, условия успешного использования рассмотренного метода для проверки качества графического интерфейса пользователя (ГИП) в многомодульных информационных системах.

Ключевые слова: *проверка качества ГИП, тестовое покрытие, метод ориентированного графа возможных взаимодействий, регрессионное тестирование*

Введение

Стремительное развитие рынка информационных технологий и, как следствие этого, возникшая высокая конкуренция на этом рынке привели к острой необходимости резкого сокращения сроков разработки информационных систем (ИС). Стали применяться более гибкие и быстрые процессы реализации проектов — Agile [1] вместо Waterfall [2], и в рамках парадигмы сокращения затрачиваемых на разработку проекта ресурсов возникла необходимость в оперативной оценке качества ИС в целом [3], а особенно — графического интерфейса пользователя (ГИП). При этом необходимо учитывать, что ГИП является важнейшей составляющей неспециализированной ИС и вносит значимый вклад в ее успешность. Именно поэтому корректности работы ГИП необходимо уделять особое внимание.

ГИП современной ИС представляет собой, как правило, весьма обширный набор взаимосвязанных между собой элементов — кнопки, поля для ввода текста, списки, метки, переключатели и пр. При оценке качества ГИП [4] одним из ключевых вопросов является вопрос покрытия возможностей и элементов системы проверочным сценариями (тестами), иным словами, вопрос "а все ли мы проверили?". В настоящее время существует несколько методик, которые позволяют с некоторой степенью достоверности понять покрытие ИС тестами. Наиболее распространенные среди них — матрица трассировки [5], а также тестирование по "пользовательским историям" (userstories) [6].

Использование матрицы трассировки требует четко сформулированных и достаточно полных требований к ИС, что в современных реалиях, как правило, невозможно. Полное покрытие матрицы трассировки проверочными сценариями требует значительных тестовых ресурсов, что также трудно реализуемо в процессе создания относительно небольших ИС.

Тестирование на основе "пользовательских историй", напротив, позволяет оперативно оценить качество ИС с точки зрения основных пользовательских сценариев использования, но не способно доподлинно оценить качество всех компонентов, возможностей и сценариев использования системы, состоящей из нескольких взаимосвязанных компонентов.

Кроме того, случаются ситуации, когда процесс проверки качества выполняется для существующих ИС, которые переданы в экс-

плуатацию. В этой ситуации вопрос о полноте покрытия тестовыми сценариями встает наиболее остро и требует оперативного ответа. В качестве быстрого ответа на вышеуказанный вопрос предлагается реализовать граф [7] взаимодействий для элементов ГИП.

Граф взаимодействий элементов ГИП

Методика оценки покрытия ИС проверочными сценариями на основе построения графа взаимодействий основана на том, что каждый элемент ГИП представляется в виде узла графа, а ребра графа — это возможные связи между элементами.

На рис. 1 показано диалоговое окно, в котором наполнение групп элементов *2*, *3* и *4* зависит от значения поля со списком *1*.

Представим элементы ГИП *1*, *2*, *3* и *4* в виде узлов графа и определим взаимодействия между узлами, где Obj1 — это поле со списком KQI, Obj2, Obj3 и Obj4 — соответственно группы элементов *2*, *3* и *4* на рис. 1 (рис. 2)

На основании данного графа хорошо видно, что необходимо разработать как минимум, три проверки на группы элементов Obj2, Obj3 и Obj4 — по зависимости этих элементов на выбранное пользователем значение поля со списком KQI. В данной методике необходимо учитывать только те элементы ГИП, которые оказывают друг на друга влияние. Иными словами, нет необходимости создавать проверочный сценарий для совместного взаимодействия элементов Obj2, Obj3 и Obj4.

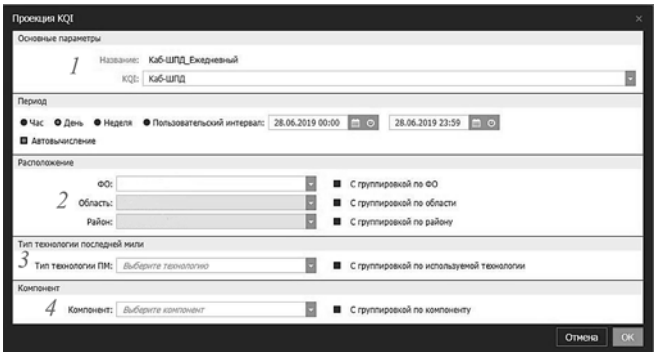

Рис. 1. Диалоговое окно создания проекции

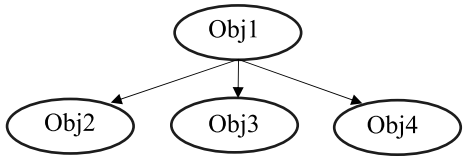

Рис. 2. Схема 1 — простой граф взаимосвязи элементов ГИП

Таким образом, представив элементы ГИП в виде графа, можно оценить число необходимых проверочных сценариев для всех ИС в целом, а также определить области, не покрытые тестами (gaps).

Приоритет тестов при использовании методики графа взаимодействий

Как уже говорилось выше, современная ИС — это, как правило, очень обширный набор объектов графического интерфейса. Очевидно, что в этом случае при использовании метода графов для оценки покрытия функционала ИС проверочными сценариями может возникнуть ситуация, когда будет необходимо разработать и выполнить большое число тестов, что очень сложно в ситуации, когда существует недостаток тестовых ресурсов и/или времени для проведения проверки ИС. В этих случаях предлагается использовать приоритезацию взаимосвязей между элементами (рис. 3).

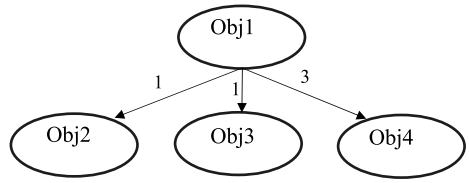

Рис. 3. Схема 2 — граф взаимосвязи элементов ГИП с приоритетами

На схеме 2 взаимосвязям элементов ГИП был назначен приоритет (1 — высокий, 2 — средний, 3 — низкий). Под приоритетом понимается важность взаимосвязи с точки зрения бизнес-процесса/важности для конечного пользователя. При наличии разделения всех проверочных сценариев по приоритетам появляется возможность более гибко подходить к отбору тестов для первоочередного запуска и, соответственно, находить приоритетные ошибки в ИС раньше, нежели при простом, поочередном запуске тестов, что сделает тестирование более эффективным [8].

Нормировка суммарной приоритетности связей по длине взаимодействия

Для оптимизации числа необходимых проверок, а также для сокращения необходимых для корректного запуска тестов предварительных настроек ИС применяют несколько последовательных действий, после каждого из которых

проверяется корректность реакции системы. Кроме того, действия пользователя, как правило, представляют собой последовательность действий из нескольких шагов, не ограничиваясь единичным воздействием на систему.

В качестве примера на рис. 4 (см. вторую сторону обложки) представлено диалоговое окно вычисления качества сервиса. Предположим, что после выбора в поле со списком *1* значения Каб-ШПД в группе 2 становятся доступны возможные опции ограничения вычисления по расположению сервиса. От значения поля со списком *2.1* зависит доступность флага *2.1.1* и набор значений в поле со списком *2.2*. Значение поля со списком *2.2*, в свою очередь, влияет на доступность флага *2.2.1* и на доступные значения поля со списком *2.3*. При этом выбранные значения элементов графического интерфейса *2.1*, *2.2* и *2.3* формируют значение поля 0.

В виде графа взаимодействие этих элементов интерфейса ИС можно представить так, как показано на рис. 5

Используя схему 3, также можно оценивать полноту покрытия тестовыми сценариями элементов и взаимодействий ИС, но оценка приоритетности проверочного сценария с несколькими последовательными действиями нуждается в уточнении. Для корректной оценки приоритета сценария из нескольких действий, имеющих различный приоритет, необходима нормировка по числу действий.

$$\text{Приоритет сценария} = \frac{\sum w}{N},$$

где w — приоритет взаимодействия; N — число взаимодействий.

Таким образом, приоритет сценария равен отношению суммы приоритетов всех взаимодействий к числу взаимодействий.

Данная методика позволяет оперативно оценить тестовое покрытие ИС с учетом приоритетов и выявить области, которые не покрыты или недостаточно покрыты проверочными сценариями, а также выявить наиболее важные с точки зрения бизнес-процессов сценарии, что позволит сосредоточиться на их первоочередной проверке.

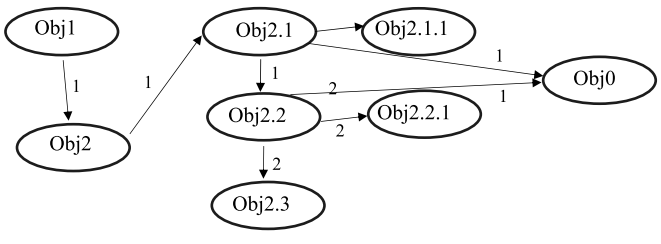

Рис. 5. Схема 3 — граф взаимодействия элементов окна вычисления качества

Из недостатков данной методики следует отметить необходимость в высокой квалификации тестовых инженеров, которые будут использовать данную методику и широкие знания взаимодействий всех компонентов системы. Кроме того, возможны такие цепочки взаимодействий, приоритет которых может быть некорректно оценен с помощью нормировки, например, у цепочки 1-1-3-3 приоритет равен 2, но в этой цепочке присутствуют два взаимодействия первого приоритета — для таких ситуаций необходимо использовать другие методики.

Заключение

Методика применения графов взаимодействия элементов ГИП позволяет оперативно определить недостаточность тестового покрытия и восполнить его впоследствии, с учетом приоритетов бизнес-процесса при сравнительно малых затратах тестовых ресурсов. Использовать данную методику для формирования перечня тестов для регрессионного тестирования [9] не представляется возможным, так как указанная методика не учитывает "новизну" взаимодействий элементов и возможные влияния на приоритетность взаимодействий [10] новых компонентов.

Список литературы

1. **Mitasiunas A., Rout T., O'Connor R. V.** Software Process Improvement and Capability Determination // 14th International Conference, SPICE 2014, Vilnius, Lithuania, November 4—6, 2014. Proceedings. 2014. P. 190—201. doi:10.1007/978-3-319-13036-1_17.

2. **Ensmenger N.** The Computer Boys Take Over. Massachusetts. England: The MIT press, 2010. 42 p.

3. **Зарубин И. Б., Филинских А. Д.** Способы оперативного выбора тестовых сценариев для регрессионного тестирования при внесении изменения в комплексные информационные системы // Матер. 29-й Всерос. науч.-практ. конф. по графическим информационным технологиям и системам. 2019. С. 198—201.

4. **Филинских А. Д., Мерзляков И. Н.** Оценка геометрических моделей на основании структуры их параметров // Информационно-измерительные и управляющие системы. 2015. Т. 13, № 3. С. 69—74.

5. **Gotel O., Cleland-Huang J., Hayes J. H., Zisman A., Egyed A., Grünbacher P., Dekhtyar A., Antoniol G., Maletic J.** Software and Systems Traceability. London: Springer, 2012. P. 3—22. doi:10.1007/978-1-4471-2239-5_1.

6. **Майк Кон.** Пользовательские истории. Гибкая разработка программного обеспечения. М.: Вильямс, 2012. 256 с.

7. **Волченская Т. В., Князьков В. С.** Компьютерная математика: Часть 2. Теория графов / Учеб. пособ. Пенза: Изд-во Пенз. ун-та, 2002. 101 с.

8. **Golze A., Sarbiewski M., Zahm A.** Оптимизация качества для достижения высоких бизнес-результатов. Wiley Publishing, Inc., Indianapolis, IN. 2008. 290 с.

9. **Yoo S., Harman M.** Regression testing minimization, selection and prioritization: A survey // Software Testing Verification and Reliability 22(2). March 2012 С. 67-120. DOI: 10.1002/stvr.430.

10. **Зарубин И. Б., Филинских А. Д.** Методика оценки полноты регрессионного тестирования с нормировкой по весовым коэффициентам // Тр. НГТУ им. Р. Е. Алексеева. 2019. № 4 (127). С. 9—17.

I. B. Zarubin, e-mail: simarglz@yandex.ru, **A. D. Filinskih,** e-mail: alexfil@yandex.ru,
T. I. Balashova, e-mail: tibalashova@mail.ru,
Nizhny Novgorod State Technical University n. a. R. E. Alexeyev,
Nizhny Novgorod, 603155, Russian Federation

Evaluation of User Interface Test Coverage in Multicomponent Information Systems

The method of estimation of completeness of a cover by test scenarios of the graphic user interface in complex information systems by construction of the directed graph of possible interrelations of elements with giving weight to each communication and normalization on quantity of interrelations is considered. Given the advantages and disadvantages of the considered method, the conditions for the successful use of the considered method for checking the quality of the UI in integrated complex information systems.

Keywords: *UI quality assurance, test coverage, the test coverage method of directed graph of possible interactions*

DOI: 10.17587/it.26.203-206

References

1. **Mitasiunas A., Rout T., O'Connor R. V.** Software Process Improvement and Capability Determination, *14th International Conference, SPICE 2014, Vilnius, Lithuania, November 4-6, 2014, Proceedings*, 2014, pp. 190—201, doi:10.1007/978-3-319-13036-1_17.

2. **Ensmenger N.** The Computer Boys Take Over. Massachusetts, *England, The MIT press*, 2010, p. 42.

3. **Zarubin I. B., Filinskikh F. D.** Fast ways to select test scenarios for regression testing when making changes in complex information systems, *Collection of materials of the 29th all-Russian scientific and practical conference on graphic information technologies and systems,* 2019, pp. 198—201 (in Russian).

4. **Filinskikh F. D., Merzliakov I. N.** Evaluation of geometric models based on the structure of their parameters, *Informacionno-Izmeritelniye i Upravliayushchie Sistemy*, 2015, vol. 13, no. 3, pp. 69—74 (in Russian).

5. **Gotel O., Cleland-Huang J., Hayes J. H., Zisman A., Egyed A., Grünbacher P., Dekhtyar A., Antoniol G., Maletic J.** Software and Systems Traceability, London, Springer, 2012, pp. 3—22, doi:10.1007/978-1-4471-2239-5_1.

6. **Mike Cohn.** User Stories Applied: For Agile Software Development, Moscow, Williams, 2012, 256 p. (in Russian).

7. **Volchenskaia T. V., Kniazkov V. S.** Computer mathematics: Part 2. Graph Theory, Penza, *Izdatelstvo Penzenskogo universiteta*, 2002, p. 8 (in Russian).

8. **Golze A., Sarbiewski M., Zahm A.** Quality optimization to achieve high business results, Wiley Publishing, Inc., Indianapolis, IN. 2008, 290 p.

9. **Yoo S., Harman M.** Regression testing minimization, selection and prioritization: A survey *Software Testing Verification and Reliability,* 22(2), March 2012, pp. 67—120, doi:10.1002/stvr.430.

10. **Zarubin I. B., Filinskikh F. D.** Methodology for evaluating the completeness of regression testing with normalization by weight coefficients, *78 Proceedings of the NSTU R. E. Alekseeva*, 2019, no. 4 (127), pp. 9—17.

УДК 003.26 DOI: 10.17587/it.26.207-213

Д. Ю. Гурьянов, канд. техн. наук, доц., e-mail: guryanov.dyu@yandex.ru,
Государственный университет морского и речного флота имени адмирала С. О. Макарова, Санкт-Петербург,
А. А. Костина, науч. сотр., e-mail: to.ann@inbox.ru,
Н. А. Молдовян, д-р техн. наук, проф., e-mail: nmold@mail.ru,
Санкт-Петербургский институт информатики и автоматизации Российской академии наук, Санкт-Петербург

Постквантовый протокол бесключевого шифрования[1]

Существенный прогресс в развитии квантовых вычислителей, для которых известны полиномиальные алгоритмы факторизации целых чисел и нахождения дискретного логарифма, выдвинул на передний план проблему построения постквантовых алгоритмов и протоколов, т.е. криптосхем, которые были бы стойкими к атакам с использованием квантовых компьютеров. В работе рассматривается протокол бесключевого шифрования, стойкий к атакам с использованием квантовых компьютеров, на основе вычислительной трудности задачи дискретного логарифмирования на эллиптической кривой. В результате предложено новое построение протокола бесключевого шифрования, стойкого к квантовым атакам. Предложенный протокол отличается использованием коммутативного шифрования на эллиптической кривой и расщеплением передаваемого значения на две части, каждая из которых преобразуется на независимом локальном ключе.

Ключевые слова: *постквантовые криптосхемы, защита информации, бесключевое шифрование, коммутативное шифрование, локальные ключи, разовые ключи, стойкость, эллиптическая кривая, вычислительно сложная задача*

Введение

Криптографические методы защиты информации играют важную роль для обеспечения информационной безопасности информационно-телекоммуникационных систем [1, 2]. В частности, протоколы электронной цифровой подписи, основанные на вычислительно трудных задачах факторизации и дискретного логарифмирования, нашли широкое применение в современных информационных технологиях [3, 4], однако в случае появления в будущем квантовых компьютеров, для которых известны полиномиальные алгоритмы решения задачи дискретного логарифмирования (ЗДЛ) и задачи факторизации [5—7], потребуется заменить указанные протоколы на протоколы, основанные на вычислительно трудных задачах других типов, решение которых с использованием квантовых вычислителей будет иметь сверхполиномиальную сложность. Актуальность данной проблемы подтверждается проведением тематических конференций [8] и объявлением Национальным институтом стандартов и технологий США (НИСТ, National Institute of Standards and Technology, NIST) конкурса по разработке протоколов и алгоритмов постквантовой криптографии [9].

В качестве примитивов постквантовых криптосхем были предложены следующие вычислительные задачи: 1) поиска сопрягающего элемента в некоммутативных группах кос [10, 11] и 2) дискретного логарифмирования в скрытой циклической группе конечной некоммутативной алгебры [12—14]. Однако в первом случае имеются принципиальные трудности, обусловленные тем, что задача поиска сопрягающего элемента сводится к решению систем линейных уравнений [15]. Указанная сводимость ставит под сомнение стойкость многочисленных двухключевых криптосхем, основанных на вычислениях в группах кос [16, 17].

[1]Работа выполнена при финансовой поддержке РФФИ в рамках проекта № 18-07-00932-а.

Второй случай представляется более перспективным, однако при использовании в качестве носителей задачи дискретного логарифмирования в скрытой группе предложенных конечных некоммутативных алгебр найдены полиномиальные способы сведения этой задачи к задаче дискретного логарифмирования в конечном поле [18, 19]. Последнее определяет необходимость поиска новых типов конечных алгебр, пригодных для использования при построении постквантовых криптосхем на основе задачи дискретного логарифмирования в скрытой циклической группе.

Известные коммутативные шифры, используемые в протоколах бесключевого шифрования, основаны на вычислительной трудности задачи дискретного логарифмирования. Они также могут быть построены на основе задачи дискретного логарифмирования в скрытой циклической группе [13]. Однако в настоящее время не предложены подходящие конечные алгебры и представляет интерес рассмотрение возможности обеспечения стойкости протокола бесключевого шифрования за счет увеличения числа используемых интерактивных шагов, выполняемых абонентами сеанса секретной связи (отправителем и получателем сообщения), при использовании коммутативного шифра, основанного на вычислительной трудности задачи дискретного логарифмирования на эллиптической кривой (ЭК). Для этого может быть использован способ коммутативного шифрования на ЭК, представленный в работе [20].

В настоящей статье обсуждается построение постквантового протокола бесключевого шифрования, основанного на вычислениях на ЭК и применении разовых вспомогательных локальных ключей. Рассматриваются типовые операции на ЭК, реализация алгоритма коммутативного шифрования Похлига—Хеллмана на ЭК и его использование в стандартном трехпроходном протоколе бесключевого шифрования. Описывается предложенный постквантовый протокол бесключевого шифрования. В заключении формулируются основные выводы по выполненному исследованию.

Коммутативные шифры и протокол бесключевого шифрования

Некоторый шифр (алгоритм шифрования) E называется коммутативным, если зашифровывание некоторого сообщения M на двух разных ключах A и B приводит к формированию одного и того же шифртекста независимо от порядка использования ключей:

$$E_A(E_B(M)) = E_B(E_A(M)),$$

где A и B — произвольно выбираемые ключи, например, принадлежащие абонентам A и B соответственно. Протокол, известный как трехпроходный протокол Шамира или протокол бесключевого шифрования [21], позволяет безопасно передать секретное сообщение по открытому каналу без того, чтобы отправитель и получатель использовали заранее выполняемую процедуру согласования ключей (открытых ключей или разделяемых секретных ключей). Протокол бесключевого шифрования требует использования коммутативного шифра, который является стойким к атакам на основе известного исходного текста, в которых предполагается, что потенциальному нарушителю известно исходное сообщение и шифртекст. Последнему требованию удовлетворяет алгоритм шифрования Похлига—Хеллмана, известный как экспоненциальный шифр [21]. В нем в качестве процедуры шифрования используется операция возведения в большую натуральную степень по модулю большого простого числа p. При этом зашифровывание и расшифровывание осуществляются как возведение в степень e и d соответственно. Пара натуральных чисел (e, d), удовлетворяющих условию $ed = 1(\mathrm{mod}\ p - 1)$, представляет собой секретный ключ.

Передача секретного сообщения M, удовлетворяющего условию $M < p$, по открытому каналу связи в соответствии с протоколом бесключевого шифрования осуществляется следующим образом.

1. Алиса (отправитель сообщения) генерирует свой локальный ключ в виде пары чисел (e_A, d_A), вычисляет шифртекст $C_1 = Me_A \mathrm{mod} p$ и высылает Бобу (получателю сообщения).

2. Боб генерирует свой локальный ключ в виде пары чисел (e_B, d_B), зашифровывает шифртекст C_1 (теперь сообщение M зашифровано дважды с использованием двух различных ключей), получает шифртекст $C_2 = C_1 e_B \mathrm{mod} p = Me_A e_B \mathrm{mod} p$ и направляет C_2 Алисе.

3. Алиса расшифровывает C_2, получает шифртекст $C_3 = C_2 d_A \mathrm{mod} p = Me_A e_B d_A = Me_B \mathrm{mod} p$ (теперь сообщение M зашифровано только на ключе Боба) и направляет C_3 Бобу.

Получив шифртекст C_3, Боб легко расшифровывает сообщение: $M = C_3 d_B \mathrm{mod} p$.Потенциальный нарушитель для восстановления секретного сообщения может попытаться вычислить значе-

ние d_A из уравнения $C_3 = C_2 d_A \mathrm{mod} p$ или e_B из уравнения $C_2 = C_1 e_B \mathrm{mod} p$, однако обе последние задачи представляют собой нахождение значения дискретного логарифма по простому модулю — задачу, вычислительная сложность которой является сверхполиномиальной для современных практически реализуемых алгоритмов.

Аналогичный алгоритм коммутативного шифрования и протокол бесключевого шифрования могут быть реализованы с использованием вычислений на ЭК [20]. Для построения криптосхем используются ЭК, заданные над конечными полями [22]. В этом случае ЭК представляет собой конечные множества пар элементов (x, y) конечного поля $GF(p^s)$, где s — степень расширения ($s \geqslant 1$); p — характеристика поля ($p \geqslant 2$), удовлетворяющих уравнению третьей степени. Над таким множеством пар (x, y), называемых точками ЭК, определена операция сложения (+), обладающая свойствами коммутативности и ассоциативности. Значение суммы точек $A = (x_A, y_A)$ и $B = (x_B, y_B)$ представляет собой точку $C = (x_C, y_C)$, координаты которой вычисляются по сравнительно простым формулам, в которые входят координаты точек-операндов: $x_A, y_A, x_B, y_B \in GF(p^s)$. Вид этих формул и вид уравнения ЭК зависят от вида поля $GF(p^s)$. Например, стандарты цифровой подписи ГОСТ Р 34.10—2001 и ГОСТ Р 34.10—2012 [23] рекомендуют использование ЭК над простым полем $GF(p)$ и уравнение ЭК вида

$$y^2 = x^3 + ax + b,$$

где $a, b \in GF(p)$.

В этом случае сумма точек A и B вычисляется по формулам

$$x_c = k^2 - x_A - x_B \mathrm{mod} p,$$
$$y_c = k(x_A - x_C) - y_A \mathrm{mod} p,$$

где $k = \dfrac{y_B - y_A}{x_B - x_A} \bmod p$, если точки A и B не равны, и $k = \dfrac{3x_A + a}{2y_A} \bmod p$, если точки A и B равны. Точки $A = (x_A, y_A)$ и $-A = (x_A, -y_A)$ называются противоположными, их сумма по определению равна бесконечно удаленной точке, обозначаемой буквой O, которая считается принадлежащей ЭК. Умножение точки A на натуральное число n определяется как n-кратное сложение точки A:

$$nA = A + A + \ldots + A \ (n \text{ раз}).$$

Результат умножения любой точки ЭК на нуль определяется как точка O. Умножение на целое отрицательное число $-n$ определяется по формуле $(-n)A = n(-A)$. При задании ЭК над конечным полем она представляет собой конечную коммутативную группу. При этом групповой операцией является операция сложения точек, а нейтральным элементом — бесконечно удаленная точка O. Вычисление неизвестного $k \in GF(p)$ в уравнении $P = kG$, где P и G — известные точки ЭК, называется ЗДЛ на ЭК. Число точек на ЭК называется ее порядком и обозначается $\#E$. Известны общие методы вычисления порядка кривой по значениям p, a и b. Примеры ЭК, пригодных для построения криптосхем, приведены в стандарте [22].

В методе коммутативного шифрования на ЭК [20] используется вероятностное отображение сообщения в точку (присоединение к сообщению случайного 8-битового значения, при котором полученное значение является абсциссой некоторой точки M), лежащую на ЭК, и последующее шифрование, осуществляемое путем выполнения операции умножения сообщения-точки на число, являющееся элементом секретного ключа. Ключом является пара чисел (e, d), удовлетворяющих условию $ed = 1 \bmod \Omega$, где $\Omega = \#E$. Протокол бесключевого шифрования при использовании вычислений на ЭК описывается следующим образом.

1. Алиса (отправитель сообщения) генерирует свой локальный ключ в виде пары чисел (e_A, d_A), кодирует сообщение точкой M, вычисляет шифртекст в виде точки $C_1 = e_A M$ и высылает Бобу координаты точки C_1.

2. Боб генерирует свой локальный ключ в виде пары чисел (e_B, d_B), преобразует шифртекст C_1 в шифртекст $C_2 = e_B C_1 = e_B e_A M$ и направляет C_2 Алисе.

3. Алиса преобразует C_2 в шифртекст $C_3 = d_A C_2 = e_B M$ и направляет точку C_3 Бобу.

Получив шифртекст C_3, Боб легко расшифровывает точку-сообщение: $M = d_B C_3$. Потенциальный нарушитель для восстановления секретного сообщения может попытаться вычислить значение d_A из уравнения $C_3 = d_A C_2$ или e_B из $C_2 = e_B C_1$. Решение этих уравнений называется ЗДЛ на ЭК, которая имеет экспоненциальную сложность при правильно выбранных параметрах используемой ЭК. Однако при наличии возможности использования квантового компьютера ЗДЛ в любой циклической группе, в том числе и ЗДЛ на ЭК, имеет полиномиальную сложность. В следующем разделе представлена постквантовая версия протокола бесключевого шифрования.

Постквантовый протокол бесключевого шифрования

В качестве основной операции шифрования в описанном ниже протоколе также используется операция умножения точек ЭК, однако в процедуру шифрования дополнительно включена операция сложения с точками, представляющими собой разовые ключи. Используемая операция сложения не позволяет свести взлом протокола к решению ЗДЛ на ЭК, благодаря чему обеспечивается стойкость к атакам с использованием квантовых компьютеров. Для того чтобы внесение дополнительной шифрующей операции сохранило свойство коммутативности шифрования по ключам отправителя и получателя сообщения, в разработанном протоколе использован механизм расщепления шифруемых данных, который в рассматриваемом случае состоит в представлении шифруемой точки ЭК в виде суммы двух случайных точек и в выполнении над последними дальнейших шифрующих преобразований. Предлагаемый постквантовый протокол бесключевого шифрования описывается следующим образом.

1. Алиса (отправитель сообщения) генерирует два локальных ключа в виде пар чисел (e_{A1}, d_{A1}) и (e_{A2}, d_{A2}), кодирует сообщение точкой M (путем присоединения справа к сообщению 8 битов и получения значения абсциссы x_M), формирует пару случайных точек ЭК R_1 и R_2, таких что $R_1 + R_2 = M$. Затем преобразует точки R_1 и R_2 по формулам $C_1' = e_{A1}R_1$ и $C_1'' = e_A R_2$ и направляет точки C_1' и C_1'' Бобу.

2. Боб генерирует два своих локальных ключа в виде пар чисел (e_{B1}, d_{B1}) и (e_{B2}, d_{B2}), представляет каждую из точек C_1' и C_1'' в виде суммы двух случайных точек R_{11}, R_{12} и R_{21}, R_{22}: $R_1 = R_{11} + R_{12}$; $R_2 = R_{21} + R_{22}$. Затем генерирует две случайные точки L_1 и L_2 и преобразует точки R_{11}, R_{12}, R_{21} и R_{22} по следующим формулам:

$$C_2' = e_{B1}R_{11} + d_{B2}L_1;\ \ C_2''' = e_{B1}R_{21} + d_{B2}L_2;$$
$$C_2'' = e_{B2}R_{12} + d_{B1}L_1;\ \ \overline{C_2} = e_{B2}R_{22} + d_{B1}L_2.$$

После этого Боб направляет точки C_2', C_2'', C_2''' и $\overline{C}_2$ Алисе.

3. Алиса генерирует случайные точки N_1 и N_2 и преобразует точки C_2', C_2'', C_2''' и $\overline{C}_2$ по следующим формулам:

$$C_3' = d_{A1}C_2' + N_1;\ \ C_3''' = d_{A2}C_2''' - N_1;$$
$$C_3'' = d_{A1}C_2'' + N_2;\ \ \overline{C}_3 = d_{A2}\overline{C}_2 - N_2.$$

Затем Алиса направляет точки C_3', C_3'', C_3''' и $\overline{C}_3$ Бобу.

Боб восстанавливает точку-сообщение из точек C_3', C_3'', C_3''' и $\overline{C}_3$ путем вычисления и сложения точек S', S'', S''' и $\overline{S}$:

$$S' = d_{B1}C_3';\ S'' = d_{B2}C_3''';\ S''' = d_{B1}C_3''';\ \overline{S} = d_{B2}\overline{C}_3;$$
$$M = S' + S'' + S''' + \overline{S} = (x_M, y_M).$$

Затем он удаляет правые 8 битов в значении абсциссы x_M точки M и получает значение секретного сообщения, переданного ему Алисой.

Приведем доказательство корректности протокола. Рассмотрим следующие значения:

$$S' = d_{B1}C_3' = d_{B1}d_{A1}C_2' + d_{B1}N_1 =$$
$$= d_{B1}d_{A1}e_{B1}R_{11} + d_{B1}d_{A1}d_{B2}L_1 + d_{B1}N1 =$$
$$= d_{A1}R_{11} + d_{B1}d_{A1}d_{B2}L_1 + d_{B1}N_1;$$
$$S'' = d_{B2}C_3'' = d_{B2}d_{A1}C_2'' + d_{B2}N_2 =$$
$$= d_{B2}d_{A1}e_{B2}R_{12} - d_{B2}d_{A1}d_{B1}L_1 + d_{B2}N_2 =$$
$$= d_{A1}R_{12} - d_{B2}d_{A1}d_{B1}L_1 + d_{B2}N_2;$$
$$S''' = d_{B1}C_3''' = d_{B1}d_{A2}C_2''' - d_{B1}N_1 =$$
$$= d_{B1}d_{A2}e_{B1}R_{21} + d_{B1}d_{A2}d_{B2}L_2 - d_{B1}N_1 =$$
$$= d_{A2}R_{21} + d_{B1}d_{A2}d_{B2}L_2 - d_{B1}N_1;$$
$$\overline{S} = d_{B2}\overline{C}_3 = d_{B2}d_{A2}\overline{C}_2 - d_{B2}N_2 =$$
$$= d_{B2}d_{A2}e_{B2}R_{22} - d_{B2}d_{A2}d_{B1}L_2 - d_{B2}N_2 =$$
$$= d_{A2}R_{22} + d_{B2}d_{A2}d_{B1}L_2 - d_{B2}N_2.$$

Складывая точки S' и S'', получаем:

$$S' + S'' = d_{A1}R_{11} + d_{B1}d_{A1}d_{B2}L_1 + d_{B1}N_1 +$$
$$+ d_{A1}R_{12} - d_{B2}d_{A1}d_{B1}L_1 + d_{B2}N_2 =$$
$$= d_{A1}(R_{11} + R_{12}) + d_{B1}N_1 + d_{B2}N_2 =$$
$$= d_{A1}C_1' + d_{B1}N_1 + d_{B2}N_2 =$$
$$= d_{A1}e_{A1}R_1 + d_{B1}N_1 + d_{B2}N_2 = R_1 + d_{B1}N_1 + d_{B2}N_2.$$

Складывая точки S''' и $\overline{S}$, получаем:

$$S''' + \overline{S} = d_{A2}R_{21} + d_{B1}d_{A2}d_{B2}L_2 - d_{B1}N_1 +$$
$$+ d_{A2}R_{22} - d_{B2}d_{A2}d_{B1}L_2 - d_{B2}N_2 =$$
$$= d_{A2}(R_{21} + R_{22}) - d_{B1}N_1 - d_{B2}N_2 =$$
$$= d_{A2}C_1'' - d_{B1}N_1 - d_{B2}N_2 =$$
$$= d_{A2}e_{A2}R_2 - d_{B1}N_1 - d_{B2}N_2 = R_2 - d_{B1}N_1 - d_{B2}N_2.$$

Имеем:

$$S' + S'' + S''' + \overline{S} =$$
$$= R_1 + d_{B1}N_1 + d_{B2}N_2 + R_2 - d_{B1}N_1 - d_{B2}N_2 =$$
$$= R_1 + R_2 = M.$$

Таким образом, получатель сообщения восстанавливает точку-сообщение $M = (x_M, y_M)$,

из которой, удаляя правые 8 битов в значении абсциссы x_M, он получает значение переданного ему сообщения.

Заключение

Предложен новый вариант реализации протокола бесключевого шифрования, использующий вычислительную трудность ЗДЛ на ЭК и обеспечивающий стойкость к атакам с использованием квантового вычислителя. Последнее достигнуто благодаря тому, что в результате преобразований по перехваченным шифртекстам потенциальный нарушитель не имеет возможности в явном виде записать уравнение ЗДЛ на ЭК, поскольку дополнительно к операции умножения точки на многоразрядное число выполняется также и операция сложения со случайно выбранной точкой. При этом, для того чтобы сохранить свойство коммутативности преобразований, выполняемых отправителем сообщения и получателем, случайные точки-слагаемые входят в преобразования дважды, причем с противоположными знаками. Для того чтобы потенциальный нарушитель не смог воспользоваться последним, преобразуемые точки "расщепляются" в сумму двух точек, каждая из которых преобразуется на различных локальных ключах текущего пользователя. Такое расщепление выполняется в ходе выполнения протокола один раз отправителем. Другая сторона (получатель), получая два шифртекста, выполняет расщепление каждого из них, поэтому на первом шаге шифртекст передается в виде двух точек ЭК, а на втором и третьем — в виде четырех точек.

Производительность предложенного протокола определяется, главным образом, вычислительной сложностью операции умножения точки ЭК на многоразрядное число аналогично реализации на ЭК стандартного трехпроходного протокола бесключевого шифрования, хотя первый из протоколов требует выполнения в два раза большего числа таких операций. Однако снижение производительности в два раза является приемлемой издержкой для обеспечения стойкости к квантовым атакам. Программная и аппаратная реализации операции умножения точки ЭК являются хорошо апробированными. В целом с практической точки зрения предложенный постквантовый протокол обладает достаточной производительностью при программной и аппаратной его реализации.

Следует отметить, что протоколы бесключевого шифрования обеспечивают высокий уровень секретности к атакам пассивного нарушителя. Для обеспечения защиты от активных атак требуется встроить механизм взаимной аутентификации участников протокола. Например, это может быть сделано с использованием коротких ключей малого размера (от 16 до 56 бит) по аналогии с криптосхемой [24].

Постквантовый протокол бесключевого шифрования может быть построен по аналогии с предложенной криптосхемой также и при использовании вычислений в конечных полях, например, в простых полях $GF(p)$ или двоичных полях $GF(2^s)$. При этом реализация протокола над полями $GF(2^s)$ со степенью расширения, равной степени Мерсенна, представляет особый интерес, поскольку мультипликативная группа таких полей имеет порядок, равный простому числу Мерсенна [25]. Предложенная схема построения постквантового протокола может быть реализована и с использованием вычислительной трудности скрытой ЗДЛ [13]. Детальное рассмотрение указанных вариантов реализации протокола представляет самостоятельный интерес.

Список литературы

1. **Yiteng Feng, Guomin Yang, Joseph K. Liu.** A new public remote integrity checking scheme with user and data privacy // International Journal of Applied Cryptography. 2017. Vol. 3, N. 3. P. 196—209.
2. **Sirwan A., Majeed N.** New Algorithm for Wireless Network Communication Security // International Journal on Cryptography and Information Security. 2016. Vol. 6, N. 3/4. P. 1—8.
3. **Chiou S. Y.** Novel Digital Signature Schemes based on Factoring and Discrete Logarithms // International Journal of Security and Its Applications. 2016. Vol. 10, N. 3. P. 295—310.
4. **Poulakis D.** A variant of Digital Signature Algorithm // Designs, Codes and Cryptography. 2009. Vol. 51, N. 1. P. 99—104.
5. **Yan S. Y.** Quantum Computational Number Theory. Springer, 2015. 252 p.
6. **Yan S. Y.** Quantum Attacks on Public-Key Cryptosystems. Springer, 2014. 207 p.
7. **Smolin J. A., Smith G., Vargo A.** Oversimplifying quantum factoring // Nature. 2013. Vol. 499, N. 7457. P. 163—165.
8. **Proceedings** of the 7th International Workshop on Post-Quantum Cryptography, PQCrypto 2016. Fukuoka, Japan, February 24—26, 2016 // Lecture Notes in Computer Science (LNCS) series. Springer, 2016. Vol. 9606. 270 p.
9. **Federal** Register:: Announcing Request for Nominations for Public-Key Post-Quantum Cryptographic Algorithms // Federal Register. The Daily journal of the United States Government. URL: https://www.gpo.gov/fdsys/pkg/FR-2016-12-20/pdf/2016-30615.pdf (дата обращения 07.11.2019).
10. **Verma G. K.** A Proxy Blind Signature Scheme over Braid Groups // International Journal of Network Security. 2009. V.9, N. 3. P. 214–217.
11. **Hiranvanichakorn P.** Provably Authenticated Group Key Agreement based on Braid Groups — The Dynamic Case // International Journal of Network Security. 2017. V. 19, N. 4. P. 517—527.
12. **Sakalauskas E., Tvarijonas P., Raulynaitis A.** Key Agreement Protocol (KAP) Using Conjugacy and Discrete Logarithm

Problems in Group Representation Level // Informatica. 2007. Vol. 18, N. 1. P. 115—124.

13. **Moldovyan D. N.** Non-Commutative Finite Groups as Primitive of Public-Key Cryptoschemes // Quasigroups and Related Systems. 2010. Vol. 18. P. 165—176.

14. **Kuzmin A. S., Markov V. T., Mikhalev A. A., Mikhalev A. V., Nechaev A. A.** Cryptographic Algorithms on Groups and Algebras // Journal of Mathematical Sciences. 2017. Vol. 223, N. 5. P. 629—641.

15. **Myasnikov A., Shpilrain V., Ushakov A.** A Practical Attack on a Braid Group Based Cryptographic Protocol // In: Advances in Cryptology — CRYPTO'05 / Lecture Notes in Computer Science. Springer-Verlag, 2005. Vol. 3621. P. 86—96.

16. **Chaturvedi A., Lal S.** An Authenticated Key Agreement Protocol Using Conjugacy Problem in Braid Groups // International Journal of Network Security. 2008. V.6, N. 2. P. 181—184.

17. **Verma G. K.** Probable Security Proof of a Blind Signature Scheme over Braid Groups // International Journal of Network Security. 2011. Vol. 12, N. 2. P. 118—120.

18. **Кузьмин А. С., Марков В. Т., Михалев А. А., Михалев А. В., Нечаев А. А.** Криптографические алгоритмы на группах и алгебрах // Фундаментальная и прикладная математика. 2015. Т. 20, № 1. С. 205—222.

19. **Глухов М. М.** К анализу некоторых систем открытого распределения ключей, основанных на неабелевых группах // Математические вопросы криптографии. 2010. Т. 1, № 4. С. 5—22.

20. **Молдовян Н. А., Рыжков А. В.** Способ коммутативного шифрования на основе вероятностного кодирования // Вопросы защиты информации. 2013. № 3. С. 3—10.

21. **Menezes A. J., Van Oorschot P. C., Vanstone S. A.** Handbook of Applied Cryptography. Boca Raton, FL: CRC Press, 1997. 780 p.

22. **National** Institute of Standards and Technology, Digital Signature Standard, FIPS Publication 186-3, 2009.

23. **Информационная** технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи. Национальный стандарт Российской Федерации ГОСТ Р 34.10—2012. М., Стандартинформ. 32 с.

24. **Молдовян Н. А., Горячев А. А., Муравьев А. В.** Протокол стойкого шифрования по ключу малого размера // Вопросы защиты информации. 2015. № 1. С. 3—8.

25. **Moldovyan N. A., Moldovyan A. A., Berezin A. N.** On Using Mersenne Primes in Designing Cryptoschemes // Int. Journal of Network Security. 2016. Vol. 18, N. 2. P. 369—373.

D. Yu. Guryanov, PhD, Tech., Associate Professor, e-mail: guryanov.dyu@yandex.ru,
Admiral Makarov State University Maritime and Inland Shipping,
Saint-Petersburg, 198035, Russian Federation,
A. A. Kostina, Research Fellow of Laboratory of Information Systems Security, e-mail: to.ann@inbox.ru,
N. A. Moldovyan, Dr. Sc., Tech., Professor, Chief Researcher of Laboratory
of Information Systems Security, e-mail: nmold@mail.ru,
St. Petersburg Institute for Informatics and Automation of the Russian Academy of Sciences,
Saint-Petersburg, 199178, Russian Federation

Post-Quantum Protocol for No-Key Encryption

The most widely used cryptoschemes with public key are based on computational difficulty of the factorization problem and on the discrete logarithm problem. The known no-key protocols are base on the second problem. Significant progress in the development of quantum computers for which there is known polynomial algorithm for integer factoring and for finding discrete logarithm have put forward problem of construction of the post-quantum algorithms and protocols, i.e. cryptoschemes that are secure to potential attacks using quantum computers. The paper considers a protocol no-key encryption, which is secure to attacks using quantum computers, on the base of the discrete logarithm on elliptic curve. As a method, at the first step of the protocol the sender divides the sent message into two values and encrypts each of them on independent local keys. At the second step analogous procedure is performed by the receiver over each of two received ciphertexts. As a result, it is proposed a new design of the no-key encryption protocol based on commutative encryption function, which is secure against quantum attacks. The proposed protocol is characterized in using commutative encryption on elliptic curve and dividing the encrypted value into two parts followed by encryption of each part using independent local key. The proposed protocol possesses sufficiently high performance and suites well for software and hardware implementations.

Keywords: *post-quantum cryptoschemes, information protection, no-key encryption, commutative encryption, local keys, single-use keys, security, elliptic curve, computationally difficult problem*

DOI: 10.17587/it.26.207-213

References

1. **Yiteng Feng, Guomin Yang, Joseph K. Liu.** A new public remote integrity checking scheme with user and data privacy, *International Journal of Applied Cryptography*, 2017, vol. 3, no. 3, pp. 196—209.

2. **Sirwan A., Majeed N.** New Algorithm for Wireless Network Communication Security, *International Journal on Cryptography and Information Security,* 2016, vol. 6, no. 3/4, pp. 1—8.

3. **Chiou S. Y.** Novel Digital Signature Schemes based on Factoring and Discrete Logarithms, *International Journal of Security and Its Applications,* 2016, vol. 10, no. 3, pp. 295—310.

4. **Poulakis D.** A variant of Digital Signature Algorithm, *Designs, Codes and Cryptography*, 2009, vol. 51, no. 1, pp. 99—104.

5. **Yan S. Y.** Quantum Computational Number Theory, Springer, 2015, 252 p.

6. **Yan S. Y.** Quantum Attacks on Public-Key Cryptosystems, Springer, 2014, 207 p.

7. **Smolin J. A., Smith G., Vargo A.** Oversimplifying quantum factoring, *Nature*, 2013, vol. 499, no. 7457, pp. 163—165.

8. **Proceedings** of the 7th International Workshop on Post-Quantum Cryptography, PQCrypto 2016. Fukuoka, Japan, Feb-

ruary 24—26, 2016, *Lecture Notes in Computer Science (LNCS) series*, Springer, 2016, vol. 9606, 270 p.

9. **Federal** Register:: Announcing Request for Nominations for Public-Key Post-Quantum Cryptographic Algorithms, *Federal Register. The Daily journal of the United States Government,* available at: https://www.gpo.gov/fdsys/pkg/FR-2016-12-20/pdf/2016-30615.pdf (date of the application 07.11.2019).

10. **Verma G. K.** A Proxy Blind Signature Scheme over Braid Groups, *International Journal of Network Security*, 2009, vol. 9, no. 3, pp. 214—217.

11. **Hiranvanichakorn P.** Provably Authenticated Group Key Agreement based on Braid Groups — The Dynamic Case, *International Journal of Network Security*, 2017, vol. 19, no. 4, pp. 517—527.

12. **Sakalauskas E., Tvarijonas P., Raulynaitis A.** Key Agreement Protocol (KAP) Using Conjugacy and Discrete Logarithm Problems in Group Representation Level, *Informatica*, 2007, vol. 18, no. 1, pp. 115—124.

13. **Moldovyan D. N.** Non-Commutative Finite Groups as Primitive of Public-Key Cryptoschemes, *Quasigroups and Related Systems*, 2010, vol. 18, pp. 165—176.

14. **Kuzmin A. S., Markov V. T., Mikhalev A. A., Mikhalev A. V., Nechaev A. A.** Cryptographic Algorithms on Groups and Algebras, *Journal of Mathematical Sciences*, 2017, vol. 223, no. 5, pp. 629—641.

15. **Myasnikov A., Shpilrain V., Ushakov A.** A Practical Attack on a Braid Group Based Cryptographic Protocol, *In: Advances in Cryptology — CRYPTO'05 / Lecture Notes in Computer Science*, Springer-Verlag, 2005, vol. 3621, pp. 86—96.

16. **Chaturvedi A., Lal S.** An Authenticated Key Agreement Protocol Using Conjugacy Problem in Braid Groups, *International Journal of Network Security*, 2008, vol. 6, no. 2, pp. 181—184.

17. **Verma G. K.** Probable Security Proof of a Blind Signature Scheme over Braid Groups, *International Journal of Network Security*, 2011, vol. 12, no. 2, pp. 118—120.

18. **Kuzmin A. S., Markov V. T., Mikhalev A. A., Mikhalev A. V., Nechaev A. A.** Cryptographic Algorithms on Groups and Algebras, *Fundamentalinaya i Prikladnaya Matematika*, 2015, vol. 20, no. 1, pp. 205—222 (in Russian).

19. **Glukhov M. M.** On analysis of some public key distribution systems based on non-abelian groups, *Matematicheskie Voprosy Kriptografii*, 2010, vol. 1, no. 4, pp. 5—22 (in Russian).

20. **Moldovyan N. A., Rizkov A. V.** Method for Commutative Encryption Based on Probabilistic Coding, *Information Security Issues*, 2013, vol. 3, pp. 3—10 (in Russian).

21. **Menezes A. J., Van Oorschot P. C., Vanstone S. A.** Handbook of Applied Cryptography, Boca Raton, FL, CRC Press, 1997, 780 p.

22. **National** Institute of Standards and Technology, Digital Signature Standard, FIPS Publication 186-3, 2009.

23. **Information** technology. Cryptographic protection of the information. Processes for generation and verification of the electronic digital signature. National standard of Russian Federation GOST R 34.10-2012, Moscow, Standartinform, 32 p. (in Russian).

24. **Moldovyan N. A., Goryachev A. A., Muravev A. V.** Protocol Strong Encryption Employing Key of Small Size, *Information security issues*, 2015, vol. 1, pp. 3—8 (in Russian).

25. **Moldovyan N. A., Moldovyan A. A., Berezin A. N.** On Using Mersenne Primes in Designing Cryptoschemes, *Int. Journal of Network Security*, 2016, vol. 18, no. 2, pp. 369—373.

УДК 004.89 DOI: 10.17587/it.26.213-221

В. И. Васильев, д-р техн. наук, проф., e-mail: vasilyev@ugatu.ac.ru,
А. М. Вульфин, канд. техн. наук, доц., e-mail: vulfin.alexey@gmail.com,
М. Б. Гузаиров, д-р техн. наук, проф., e-mail: guzairov@ugatu.su,
В. М. Картак, д-р физ.-мат. наук, доц., e-mail: kvmail@mail.ru,
Л. Р. Черняховская, д-р техн. наук, проф., e-mail: lrchern@yandex.ru,
Уфимский государственный авиационный технический университет

Оценка рисков кибербезопасности АСУ ТП промышленных объектов на основе вложенных нечетких когнитивных карт[1]

Рассмотрены методические аспекты количественной оценки рисков кибербезопасности АСУ ТП промышленных предприятий. В качестве базового подхода предлагается использование риск-ориентированного подхода, заложенного в основу стандартов серии ГОСТ Р 62443. Применение вложенных нечетких серых когнитивных карт при этом обеспечивает возможность получить более обоснованные и достоверные количественные оценки показателей рисков кибербезопасности АСУ ТП. Рассмотрен пример применения данной технологии для оценки защищенности телеметрической информации о состоянии бортовых авиационных систем.

Ключевые слова: *кибербезопасность, оценка рисков, когнитивное моделирование, нечеткая серая когнитивная карта*

Введение

В последние годы в нашу жизнь все более прочно входят новые термины и понятия: "цифровизация экономики", "промышленный интернет вещей", "киберфизические системы", "киберпространство", "кибербезопасность". Неизбежным следствием промышленной революции 4.0 при этом является не только ожидаемый рост эффективности, качества и производительности производства, но и все

[1]Исследование выполнено при финансовой поддержке РФФИ в рамках научного проекта № 18-00-00238 КОМФИ.

возрастающая зависимость от безопасности и надежности функционирования инфраструктуры промышленных систем автоматизации и контроля.

Согласно данным, приведенным в отчете "Лаборатории Касперского" [1], промышленные предприятия все чаще становятся мишенью и жертвами целевых кибератак (Advanced Persistent Threats, APT). По итогам 2018 г. общий процент атакованных АСУ ТП, на которых были обнаружены вредоносные объекты, вырос по сравнению с 2017 г. на 3,2 % и составил 47,2 %. В России в течение второго полугодия 2018 г. хотя бы один раз вредоносные объекты были зафиксированы на 45,3 % компьютеров АСУ. На сайте "Лаборатории Касперского" (US ICS-CERT) опубликовано 415 уязвимостей, выявленных в 2018 г. в различных компонентах АСУ ТП, что на 28,9 % превышает уровень 2017 г. Более половины выявленных в системах АСУ ТП уязвимостей получили при этом более 7 баллов по шкале CVSS версии 3.0, что соответствует высокой и критической степени риска.

Отметим еще одно важное обстоятельство, накладывающее свой отпечаток на задачи обеспечения безопасности АСУ ТП. Современные технологические сети предприятий находятся в тесном взаимодействии с многочисленными организациями-смежниками (подрядчики, разработчики, системные интеграторы, поставщики облачных решений и т.д.). Очевидно, что это открывает возможности подключения компьютеров сотрудников указанных организаций к технологической сети обслуживаемого предприятия извне (напрямую или удаленно через сеть Интернет) и может являться одним из каналов проникновения вредоносного ПО в технологические сети.

Задачи обеспечения кибербезопасности промышленных автоматизированных систем при этом принципиально отличаются от классических задач обеспечения информационной безопасности [2, 3]. С точки зрения кибербезопасности главным защищаемым ресурсом в АСУ ТП является сам технологический процесс, и основная цель — это обеспечить его непрерывность (т.е. доступность всех узлов) и целостность (в том числе передаваемой между узлами информации). В корпоративных информационно-вычислительных системах главный ресурс — это информация, которая обрабатывается, передается и хранится в системе, а основная цель — обеспечение ее конфиденциальности. Таким образом, поле потенциальных рисков и угроз для АСУ ТП по сравнению с корпоративными информационными системами расширяется за счет рисков потенциального ущерба жизни и здоровью персонала, населения и окружающей среде.

Отсюда понятен особый интерес к решению проблемы обеспечения кибербезопасности АСУ ТП, включая создание нормативно-правовой и методической базы (краткую характеристику современного состояния и полученных результатов в этой области можно найти в работе [4]). Одним из перспективных путей решения данной проблемы является разработка и поэтапное принятие серии международных стандартов ISA/IEC 62443 [5]. Всего в этой серии запланирован выпуск 13 руководящих документов, три из которых уже переведены на русский язык и утверждены в России (ГОСТ Р 62443). В основе развиваемого в этих стандартах риск-ориентированного подхода используется методология формирования требований по обеспечению кибербезопасности АСУ ТП в зависимости от уровня рисков предприятия подвергнуться кибератакам. В стандартах подчеркивается необходимость применения для этих целей не только критериев качественной оценки уровня безопасности АСУ ТП, но и разработки количественных методов оценки безопасности на основе математических моделей риска, угроз и инцидентов безопасности.

Рассмотрению одного из возможных подходов к решению данной задачи с использованием технологии когнитивного моделирования (и, в частности, математического аппарата "вложенных" нечетких серых когнитивных карт) посвящена данная статья.

1. Нечеткие когнитивные карты и принцип вложения

Технологии когнитивного моделирования, основанные на построении нечетких когнитивных карт, сегодня успешно используются при изучении поведения сложных социально-экономических и организационно-технических систем. Преимуществами нечетких когнитивных карт (Fuzzy Cognitive Maps, FCM), предложенных в 1986 г. Б. Коско [6], являются их наглядность, возможность выявления структуры причинно-следственных связей между элементами сложной системы, трудно поддающейся количественному анализу традиционными методами, использование знаний и опыта экспертов в исследуемой предметной области. Известны примеры применения нечетких когнитивных

карт при решении задач оценки рисков информационной безопасности [7—12].

Вместе с тем, на практике изучение реального сложного объекта (системы, проблемы) с помощью нечеткого когнитивного моделирования встречается с рядом труднопреодолимых факторов (высокая размерность пространства состояний исследуемой системы, неоднозначность выбора состава концептов и выявления наиболее существенных (значимых) связей между ними, неопределенность в оценке силы этих связей и т.д. — т.е. все то, что составляет "проклятие размерности"). Попытки разрешить эту ситуацию, как правило, связаны с представлением исходной нечеткой когнитивной карты (НКК) системы в виде совокупности из нескольких, более простых с точки зрения анализа, НКК, взаимодействующих между собой по вертикали или по горизонтали. В качестве инструмента для исследования сложных систем сегодня эффективно применяются такие модификации НКК, как иерархические НКК [13], многоагентные НКК [14], многослойные (вложенные) НКК [15—17].

Отметим, что в отличие от иерархических и многоагентных НКК основной упор при построении вложенных НКК (Nested FCM) делается на последовательном раскрытии неопределенностей — каждый последующий (нижележащий) слой содержит более детальную (локальную) информацию о внутренней структуре (топологии) базовых концептов исходной НКК. Ниже нами будет рассматриваться именно этот класс нечетких когнитивных моделей, в основе которых используется принцип вложения (nesting principle).

В качестве базового подхода к построению вложенных НКК можно воспользоваться предложенной в работе [18] теорией декомпозиции больших НКК. Согласно этой теории процедура когнитивного моделирования начинается с построения подробной (развернутой) НКК исследуемой системы, которая принимается в качестве исходной. Затем проводится разбиение множества вершин (концептов) данной НКК на ряд отдельных блоков в соответствии с отношением эквивалентности. Каждый из этих блоков содержит локальную информацию о взаимодействиях и внутренних зависимостях между концептами в пределах данного блока. Рассматривая полученные блоки в качестве вершин укрупненной (обобщенной) НКК (которую авторы [18] назвали Quotient Fuzzy Cognitive Map), получим новое блочное представление НКК.

На рис. 1 показан пример подобной декомпозиции НКК (слева — исходная НКК, состоящая из шести индивидуальных блоков (частных НКК), определенным образом связанных между собой; справа — укрупненная НКК, каждая из вершин (концептов) которой отражает множество вершин (концептов) соответствующей частной НКК.

Заметим, что в отличие от описанной выше процедуры преобразования НКК [18] путем ее "сворачивания" (т.е. от частного к общему) мы ниже, наоборот, будем строить вложенную НКК путем ее "развертывания", детализации (от общего к частному). Будем полагать, что рассматриваемая вложенная НКК строится в классе нечетких серых когнитивных карт (Fuzzy Grey Cognitive Maps, FGCM), предложенных в 2010 г. Хосе Салмероном [19]. Основное отличие нечетких серых когнитивных карт (НСКК) от других классов НКК — использование интервальных значений переменных состояния концептов и весов связей между концептами вместо нечетких чисел или термов лингвистических переменных, как это традиционно делается в НКК. Считается, что НСКК лучше соответствуют представлениям экспертов, обладают большей интерпретируемостью и предоставляют больше степеней свободы лицу, принимающему решение (ЛПР), по результатам моделирования.

Согласно работе [19] НСКК — это когнитивная модель системы в виде ориентированного графа, заданного с помощью следующей тройки множеств:

$$\text{НСКК} = \{C,\ F,\ W\}, \qquad (1)$$

где $C = \{C_i\}$ — множество концептов (вершин графа), $i = 1, 2, ..., n$; $F = \{F_{ij}\}$ — множество связей между концептами (дуг графа); $W = \{W_{ij}\}$ — множество отношений межу концептами, задан-

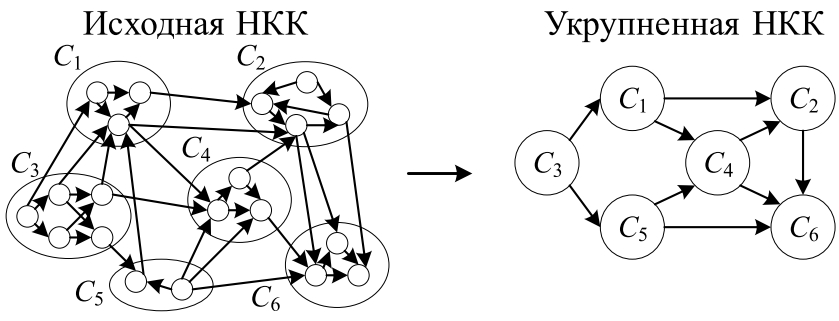

Рис. 1. Пример декомпозиции НКК

ных в виде весов соответствующих связей (дуг графа), $(i, j) \in \Omega$. Здесь $\Omega = \{(i_1, i_2), ..., (i_L, j_L)\}$ — множество индексов вершин, связанных между собой; L — число связей (дуг графа), $L \leqslant n(n-1)$.

В отличие от традиционного способа задания НКК, веса связей НСКК задаются с помощью "серых" (интервальных) чисел, которые обозначаются $\otimes W_{ij}$ и определяются следующим образом:

$$\otimes W_{i,j} \in [\underline{W}_{ij}, \overline{W}_{ij}], \qquad (2)$$

где $\underline{W}_{ij} < \overline{W}_{ij}$; $[\underline{W}_{ij}, \overline{W}_{ij}] \in [-1, 1]$; $\underline{W}_{ij}, \overline{W}_{ij}$ — соответственно нижняя и верхняя границы серого числа $\otimes W_{ij}$. В частном случае, когда $\underline{W}_{ij} = \overline{W}_{ij}$, получаем $\otimes W_{ij} \in [\underline{W}_{ij}, \underline{W}_{ij}]$ — "белое" (обычное) число.

Изменение состояния концептов во времени при этом описывается уравнениями

$$\otimes X_i(k+1) = f\left(\otimes X_i(k) + \sum_{\substack{j=1 \\ (j \neq i)}}^{n} \otimes W_{ji} \otimes X_j(k)\right), \qquad (3)$$

$i = 1, 2, \ldots, n,$

где $\otimes X_i(k)$ — "серая" (интервальная) переменная состояния i-го концепта НСКК, в каждый момент времени $k = 0, 1, 2, ...$ принимающая значение внутри некоторого интервала $[\underline{X}_i(k), \overline{X}_i(k)]$ из интервала $[-1, 1]$; $f(\cdot)$ — нелинейная функция активации i-го концепта, отображающая значения аргумента в интервал $[-1, 1]$. Для определенности будем полагать, что в качестве функции активации принимается двухполярная сигмоида (гиперболический тангенс):

$$f(x) = (1 - \mathbf{e}^{-x})/(1 + \mathbf{e}^{-x}) = \mathrm{th}(x/2). \qquad (4)$$

Для решения уравнений (3) необходимо задать начальные условия для переменных состояния $\otimes X_i(0)$, которые также представляют собой серые числа $\otimes X_i(0) \in [\underline{X}_i(0), \overline{X}_i(0)]$, $i = 1, 2, \ldots, n$.

2. Методика анализа рисков с помощью нечетких серых когнитивных карт

Рассмотрим методику анализа рисков обеспечения кибербезопасности АСУ ТП с использованием вложенных нечетких когнитивных карт на следующем примере. В качестве объекта защиты будем рассматривать автоматизированную информационную систему (АИС) сбора, хранения и обработки телеметрической информации (ТМИ) предприятия-изготовителя изделий авиационной техники. Текущая информация о параметрах состояния бортовых систем собирается в течение всего периода их эксплуатации наземными службами технического обслуживания. Детальный анализ этой информации позволяет в последующем принимать правильные управленческие и конструкторские решения о дальнейшей эксплуатации и модификации бортовых систем летательного аппарата. Поэтому задача обеспечения целостности ТМИ в условиях воздействия на нее внешних и внутренних угроз имеет важное значение.

Обобщенная структура перспективной территориально распределенной АИС сбора, хранения и обработки ТМИ на станциях технического обслуживания приведена на рис. 2 (см. вторую сторону обложки).

В составе АИС при этом можно выделить следующие подсистемы (зоны), объединяемые по принципу единства выполняемых функций и требований к безопасности их реализации:

1) *подсистема сбора и хранения первичных данных на станциях технического обслуживания* (зона 1), в состав которой входят:

- элемент 1 — клиентская часть Web-base SCADA системы;
- элемент 2 — серверная часть Web-base SCADA системы;
- элемент 3 — OPC UA клиент;
- элемент 4 — временное хранилище для размещения оперативных данных телеметрии, накапливаемых на объекте;
- элемент 5 — серверная часть системы передачи накопленных данных в хранилище предприятия-изготовителя (ПИ) авиационной техники;

2) *ядро корпоративной информационной сети (КИС)* ПИ (зона 2), где

- элемент 6 — клиентская часть для организации доступа к серверу станции обслуживания в целях передачи накопленных оперативных данных ТМИ в хранилище ПИ;
- элемент 8 — АРМ администратора и обслуживающего персонала ядра КИС ПИ;

3) *подсистема хранения ТМИ с функциями обеспечения отказоустойчивости* (зона 3), где:

- элемент 7 — узел доступа к хранилищу данных ТМИ на ПИ;
- Cluster management server — сервер управления вычислительным кластером и консоль управления системой мониторинга целостности;
- Core switch — базовый коммутатор вычислительного кластера;

4) *подсистема обработки данных ТМИ с помощью иерархии математических моделей* изделий авиационной техники (зона 4);

5) *подсистема поддержки и реализации бизнес-процессов ПИ* (зона 5).

Соответствующие подсистемы (зоны безопасности) связаны между собой на рис. 2 (см. вторую сторону обложки) с помощью каналов телекоммуникаций (трактов).

Используя в качестве инструмента моделирования аппарат НСКК, обратимся к задаче анализа рисков, связанных с обеспечением целостности ТМИ в рассмотренной выше АИС с учетом воздействия на систему внешних и внутренних угроз. Укрупненная НСКК для оценки рисков АИС, выступающая в данном случае как когнитивная модель АИС начального приближения (нулевой уровень декомпозиции), представлена на рис. 3.

Здесь используются следующие обозначения: верхний индекс (маркер "*") обозначает принадлежность концепта C_p^* укрупненной НСКК, нижний индекс p обозначает номер концепта текущего уровня.

Выбор серых значений весов связей $\otimes W_{ij}$ для НСКК на рис. 3 должен проводиться экспертом с учетом его опыта и субъективных оценок вероятностей использования уязвимостей АИС (табл. 1), что на практике весьма затруднительно. Учитывая, что каждое из указанных событий представляет собой сложное событие, состоящее из цепочки следующих друг за другом элементарных событий, целесообразно декомпозировать изображенную на рис. 3 НСКК, представив ее в виде набора вложенных НСКК для отдельных концептов (т.е. зон безопасности, содержащих целевые объекты атаки на ТМИ через соответствующие уязвимости АИС).

Первый уровень декомпозиции исходной (укрупненной) НСКК представлен на рис. 4

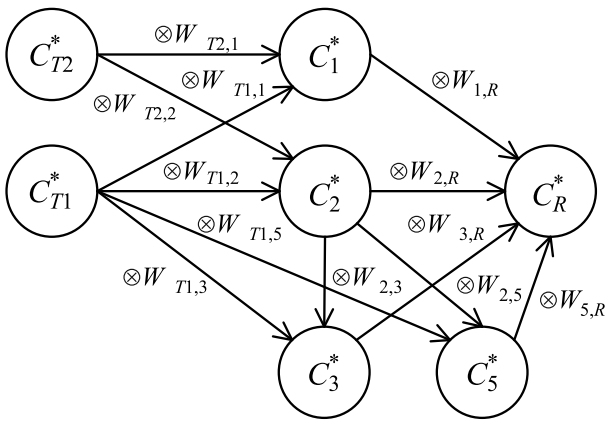

Рис. 3. Укрупненная (исходная) НСКК для оценки рисков АИС

Таблица 1

Список концептов укрупненной НСКК

Концепт	Наименование концепта
$C^*_{T_1}$	Внутренняя угроза целостности ТМИ (вследствие сбоев или ошибочных действий персонала)
$C^*_{T_2}$	Внешняя угроза целостности ТМИ (вследствие попытки несанкционированного доступа извне к информации)
C^*_1	Модификация данных ТМИ в Зоне 1
C^*_2	Модификация данных ТМИ в Зоне 2
C^*_3	Модификация данных ТМИ в Зоне 3
C^*_5	Модификация данных ТМИ в Зоне 5
C^*_R	Риск (потенциальный ущерб), вызванный нарушением целостности ТМИ в АИС

(см. третью сторону обложки). Здесь используются следующие обозначения: верхний индекс q концепта C_p^q указывает на его принадлежность к концепту C_q^* укрупненной НСКК; нижний индекс p — номер концепта в НСКК первого уровня декомпозиции. Список концептов первого уровня декомпозиции НСКК приведен в табл. 2.

На рис. 5 представлен второй уровень декомпозиции для концепта C_1^*, позволяющий уточнить воздействие угроз на рассматриваемый концепт.

На схеме используются следующие обозначения концептов $C_r^{q,p}$ второго уровня декомпозиции НСКК: верхний индекс q — номер концепта (родительский концепт нулевого уровня декомпозиции) укрупненной НСКК, в состав которого входит данный элемент; индекс p — номер родительского концепта первого уровня декомпозиции; нижний индекс r — номер концепта текущего уровня. Список концептов второго уровня декомпозиции НСКК для зоны 1 приведен в табл. 3.

Дальнейшая декомпозиция второго уровня позволяет перейти к еще более детальной НСКК, позволяющей учитывать влияние отдельных уязвимостей на потенциальное нарушение целостности ТМИ в промежуточных элементах обработки информации.

Рассмотрим численный пример оценки рисков для концепта C_1^* (рис. 5). Будем полагать, что при выборе серых значений весов НСКК необходимо ориентироваться на некоторую нечеткую шкалу, определяющую силу связей между собой различных концептов (табл. 4).

Допустим далее, что эксперт оценил значения весов связей НСКК на рис. 5 (табл. 5).

Таблица 2

Список концептов первого уровня декомпозиции НСКК

Концепт	Наименование концепта	Родительский концепт
$T_1^1, \ldots, T_1^8$	Внутренние угрозы целостности ТМИ (т.е. точки потенциальной реализации угрозы нарушения целостности ТМИ внутренним субъектом)	T_1^*
T_2^1, T_2^2	Внешние угрозы целостности ТМИ (декомпозиция концепта T_2^*)	T_2^*
C_1^1	Доступ к данным ТМИ в клиент-серверной SCADA web-base до внесения в БД оперативного хранилища ТМИ	C_1^* (Зона 1)
C_2^1	Доступ к БД оперативного хранения данных ТМИ	
C_3^1	Доступ к сетевому оборудованию	
C_4^1	Доступ к модулю Web-сервера отправки данных ТМИ в долгосрочное хранилище ПИ	
C_5^2	Доступ к сетевой инфраструктуре	C_2^* (Зона 2)
C_6^2	Доступ к модулю Web-клиента, реализующего прием ТМИ на ПИ с удаленных станций обслуживания	
C_8^2	Несанкционированный доступ к рабочей станции ядра КИС ПИ	
C_{10}^2	Доступ к серверу отчетов о состоянии оборудования, формируемых для пользователей Зоны 4	
C_7^3	Получение доступа к ТМИ в долгосрочном хранилище	C_3^* (Зона 3)
C_9^5	Доступ к серверу управления вычислительным кластером Зоны 5	C_5^* (Зона 5)
IST^5	Модуль контроля целостности ТМИ	

Таблица 3

Список концептов второго уровня декомпозиции НСКК для зоны 1

Концепт	Наименование концепта	Родительский концепт
$C_1^{1,1}$	Доступ к HMI client SCADA	C_1^1
$C_2^{1,1}$	Доступ к оперативным данным ТМИ на client-server части SCADA до внесения в оперативное хранилище	
$C_3^{1,2}$	Доступ к клиенту для взаимодействия с сервером OPC UA	C_2^1
$C_4^{1,2}$	Доступ к БД хранения оперативных данных ТМИ	

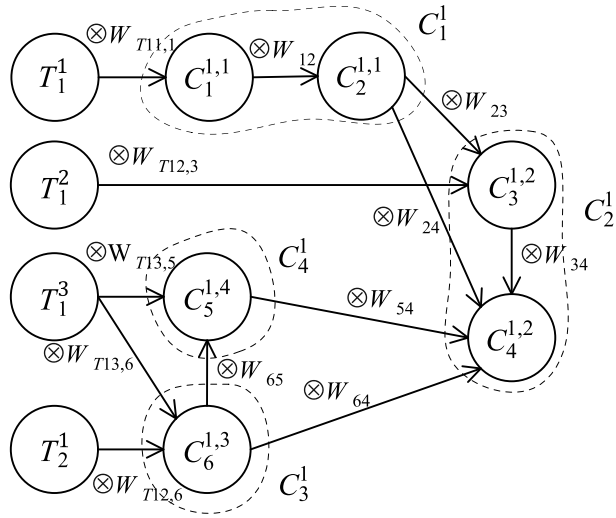

Рис. 5. Второй уровень декомпозиции НСКК для оценки рисков АИС в зоне 1

Таблица 4

Оценка силы связи между концептами

Лингвистическое значение силы связи	Числовой диапазон
Не влияет	0
Очень слабая	(0; 0,15]
Слабая	(0,15; 0,35]
Средняя	(0,35; 0,6]
Сильная	(0,6; 0,85]
Очень сильная	(0,85; 1]

Таблица 5

Значения весов связей НСКК

Вес связи	Значение веса связи	Серость (разброс оценки)
$\otimes W_{T11,1}$	[0,6; 0,75]	0,075
$\otimes W_{T12,3}$	[0,5; 0,7]	0,1
$\otimes W_{T13,5}$	[0,5; 0,7]	0,1
$\otimes W_{T13,6}$	[0,15; 0,3]	0,075
$\otimes W_{T21,6}$	[0,55; 0,65]	0,05
$\otimes W_{12}$	[0,35; 0,55]	0,1
$\otimes W_{23}$	[0,55; 0,65]	0,05
$\otimes W_{24}$	[0,3; 0,5]	0,1
$\otimes W_{34}$	[0,15; 0,3]	0,075
$\otimes W_{54}$	[0,2; 0,45]	0,125
$\otimes W_{64}$	[0,24; 0,35]	0,055
$\otimes W_{65}$	[0,22; 0,37]	0,075

Используя для расчетов программное средство "Cognitive Map Constructor" (см. раздел 3 настоящей статьи), выполним оценку изменения верхней и нижней границ переменной состояния концептов НСКК во времени $k = 1, 2, 3, ...$ (табл. 6, 7). Состояния входных концептов T_1^1, T_1^2, T_1^3, T_2^1 при этом были заданы как [0,8; 1] для всех $k = 0, 1, 2, ...$; начальные условия для переменных состояния других концептов приняты нулевыми, т.е. равны [0; 0].

В результате установившееся значение серого вектора состояния $\otimes X$ для НСКК на рис. 5 (т.е. для декомпозиции концепта C_1^*) находится как

$$\otimes X = \{[0,42;0,58],[0,14;0,30],[0,42;0,65],$$
$$[0,36;0,71],[0,36;0,56],[0,48;0,67]\},$$

а искомое значение для состояния целевого концепта $C_4^{1,2}$ определяется серым числом [0,36; 0,71].

Рассмотрим состояние целевого концепта C_R^* (см. рис. 3), т.е. ущерба, вызванного потенциальным нарушением целостности ТМИ в АИС, после уточнения значений всех весовых коэффициентов по уровням декомпозиции исходной НСКК. Предположим, что активной является внутренняя угроза T_1^* нарушения целостности ТМИ, уровень которой определяется серым числом $\otimes X_{T_1}^* \in [0,6;0,95]$. Тогда получаем установившееся значение для оценки рисков вследствие нарушения целостности информации ТМИ: $\otimes X_R^* \in [0,19;0,28]$.

Допустим далее, что в качестве возможной контрмеры для снижения ущерба от нарушения целостности ТМИ применяется дополнительная система мониторинга, развернутая в виде защищенного контейнера в зоне 5. На рис. 4 данная система обозначена как модуль контроля целостности ТМИ — концепт IST^5. Защищенный контейнер обеспечивает мониторинг целостности ТМИ в режиме онлайн и офлайн путем анализа оперативных данных и данных, собранных в хранилище (зона 3).

Как показали расчеты, оценка рисков вследствие нарушения целостности информации ТМИ после применения дополнительной контрмеры составляет $\otimes X_R^*\big|_A \in [0,07;0,15]$, т.е. риск снижается в среднем в 2,3 раза.

Таблица 6

Верхние границы оценок состояния концептов

$\bar{X}_i$	k								
	1	2	3	4	5	6	7	8	9
$\bar{X}_1^{1,1}$	0,36	0,50	0,56	0,57	0,58	0,58	0,58	0,58	0,58
$\bar{X}_2^{1,1}$	0	0,10	0,19	0,24	0,27	0,29	0,29	0,30	0,30
$\bar{X}_3^{1,2}$	0,34	0,48	0,55	0,60	0,62	0,63	0,64	0,64	0,65
$\bar{X}_4^{1,2}$	0	0,10	0,19	0,26	0,31	0,33	0,35	0,36	0,36
$\bar{X}_5^{1,4}$	0,20	0,29	0,33	0,35	0,36	0,36	0,36	0,36	0,36
$\bar{X}_6^{1,3}$	0,27	0,39	0,44	0,46	0,47	0,47	0,48	0,48	0,48

Таблица 7

Нижние границы оценок состояния концептов

$\underline{X}_i$	k								
	1	2	3	4	5	6	7	8	9
$\underline{X}_1^{1,1}$	0,24	0,34	0,39	0,41	0,42	0,42	0,42	0,42	0,42
$\underline{X}_2^{1,1}$	0	0,04	0,08	0,11	0,13	0,13	0,14	0,14	0,14
$\underline{X}_3^{1,2}$	0,20	0,29	0,34	0,37	0,39	0,41	0,41	0,42	0,42
$\underline{X}_4^{1,2}$	0	0,28	0,51	0,63	0,68	0,70	0,71	0,71	0,71
$\underline{X}_5^{1,4}$	0,34	0,48	0,53	0,55	0,55	0,56	0,56	0,56	0,56
$\underline{X}_6^{1,3}$	0,44	0,60	0,65	0,66	0,67	0,67	0,67	0,67	0,67

3. Автоматизация процедуры анализа и управления рисками на основе технологии когнитивного моделирования

В целях повышения эффективности анализа и управления рисками с использованием НСКК было разработано специальное программное средство "Cognitive Map Constructor". Данное программное средство позволяет строить и редактировать НСКК, проводить с их помощью анализ рисков и обосновывать выбор необходимых контрмер из заданного пользователем набора. В результате строится диаграмма оценки рисков при различных сценариях внедрения контрмер и реализации угроз.

Помимо поддержки НСКК с установкой весов связей в виде верхних и нижних границ программа допускает использование лингвистических термов нечеткой логики, а также задание весов в виде "белых" (четких) чисел. Программа имеет интерфейс, реализованный на языке гипертекстовой разметки HTML с применением CSS, позволяющий отображать НСКК и необходимую сопроводительную информацию по концептам и связям, а также способна работать на любой графической операционной системе, в которой имеется актуальный веб-браузер.

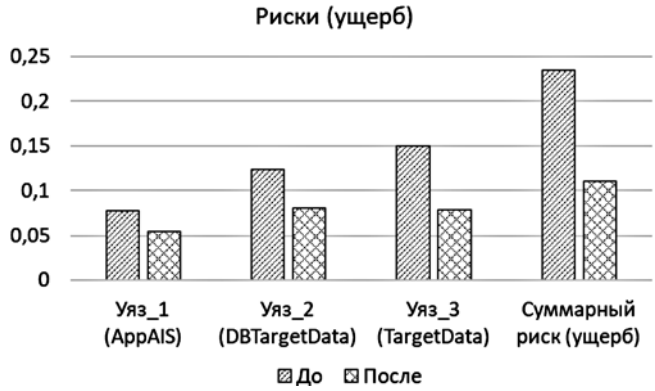

Рис. 7. Оценка рисков для целевых концептов и суммарного риска до и после реализации контрмер

На рис. 6 (см. третью сторону обложки) приведен пример НСКК оценки рисков подсистемы сбора и хранения данных АИС, построенной в "Cognitive Map Constructor".

Оценка рисков для целевых концептов и оценка суммарного риска до и после реализации контрмер и состояние целевых концептов НСКК приведены на рис. 7. Здесь: AppAIS — эксплуатация уязвимости Web-приложения для запуска модуля доступа к БД оперативного хранения ТМИ на станциях обслуживания ЛА; DBTargetData — модификация оперативных данных ТМИ в БД хранения; TargetData — модификация ТМИ в долгосрочном хранилище.

Заключение

Перспективным способом решения задачи оценки рисков кибербезопасности промышленных автоматизированных систем является моделирование сценариев реализации угроз с помощью когнитивного моделирования с применением нечетких серых когнитивных карт.

В основе данного подхода используется построение укрупненной НСКК для оценки рисков автоматизированной информационной системы, с последующей ее декомпозицией на ряд вложенных когнитивных карт следующих уровней детализации. Особенности построения данной процедуры рассмотрены на примере задачи обеспечения целостности ТМИ в промышленной автоматизированной системе сбора, хранения и обработки информации о состоянии авиационных бортовых систем. Использование НСКК позволяет при этом получить более достоверные оценки факторов риска с учетом возможного разброса фактически располагаемых данных и мнений экспертов.

Список литературы

1. **Ландшафт** угроз для систем промышленной автоматизации. Второе полугодие 2018. URL: https://ics-cert.kaspersky.ru/reports/2019/03/27/threat-landscape-for-industrial-automation-systems-h2-2018/ (дата обращения 17.08.2019).

2. **Ярушевский Д.** Кибербезопасность АСУ ТП — что это и зачем? Пресс-центр "ДиалогНаука". URL: https://www.dialognauka.ru/press-center/article/13226/ (дата обращения 17.08.2019).

3. **Андреев Ю. С., Дергачев А. М., Жаров Ф. А., Садырин Д. С.** Информационная безопасность автоматизированных систем управления технологическими процессами // Известия вузов. Приборостроение. 2019. Т. 62, № 4. С. 331—339.

4. **Васильев В. И., Кириллова А. Д., Кухарев С. Н.** Кибербезопасность автоматизированных систем управления промышленных объектов (современное состояние, тенденции) // Вестник УрФО. Безопасность в информационной сфере. 2018. № 4(30). С. 66—74.

5. **Ярушевский Д.** Обеспечение безопасности АСУ ТП — краткий обзор семейства стандартов IEC 62443 // Information Security/ Информационная безопасность. 2014. № 3. URL: http://lib.itsec.ru/articles2/ (дата обращения 17.08.2019).

6. **Kosko B.** Fuzzy Cognitive Maps // Intern. Journal of Man-Machine Studies. 1986. Vol. 1. P. 65—75.

7. **Гузаиров М. Б., Васильев В. И., Кудрявцева Р. Т.** Системный анализ информационных рисков с применением нечетких когнитивных карт // Инфокоммуникационные технологии. 2007. Т. 5, № 4. С. 42—48.

8. **Ажмухамедов И. М.** Динамическая нечеткая когнитивная модель влияния угроз на информационную безопасность системы // Безопасность информационных технологий. 2010. № 2. С. 68—72.

9. **Yeboah-Boateng E. O.** Using Fuzzy Cognitive Maps (FCMs) to Evaluate the Vulnerabilities with ICT Assets Disposal Policies // Intern. Journal on Electrical & Computer Sciences IJECS-IJENS. Oct. 2012. Vol. 12, N. 05. P. 20—31.

10. **Szwed P., Skrzynski P. A.** New Lightweight method for security risk assessment based on Fuzzy Cognitive Maps // Intern. Journal on Appl. Math. Comput. Sci. 2014. Vol. 24, N. 1. P. 213—225.

11. **Васильев В. И., Вульфин А. М., Гузаиров М. Б.** Оценка рисков информационной безопасности с использованием нечетких продукционных когнитивных карт // Информационные технологии. 2018. Т. 24, № 4. С. 266—273.

12. **Васильев В. И., Вульфин А. М., Гузаиров М. Б., Кириллова А. Д.** Интервальное оценивание информационных рисков с помощью нечетких серых когнитивных карт // Информационные технологии. 2018. № 10(24). С. 657—664.

13. **Stylios C. D., Groumpos P. P.** Fuzzy Cognitive Maps Multi-Model for Complex Manufacturing Systems // IFAC Large Scale Systems: Theory and Applications. Bucharest, Romania, 2001. P. 61—66.

14. **Stula M., Stipanicev D., Bodrozic L.** Intelligent Modeling with Agent-based Fuzzy Cognitive Map // Intern. Journal on Intell. Systems. 2010. Vol. 25, N. 10. P. 981—1004.

15. **Mohr S.** Modelling Approaches for Multilayer Fuzzy Cognitive Maps. URL: https://www.researchgate.net/publication/332158518_Modelling_Approaches_for_Multilayer_Fuzzy_Cognitive_Maps (дата обращения 17.08.2019).

16. **Mohagheghi S.** Fuzzy Cognitive Maps for Identifying Fault Activation Patterns in Automation Systems. URL: https://www.intechopen.com/books/ (дата обращения 17.08.2019).

17. **Motlagh O., Papageorgiou E. I., Tang S. H., Jamaludin Z.** Multivariate Relationship Modeling Using Nested Fuzzy Cognitive Map // Sains Malaysiana. 2014. N. 43(11). P. 1781—1790.

18. **Zhang J. Y., Liu Z. Q., Zhou S.** Quotient FCMs — A Decomposition Theory for Fuzzy Cognitive Maps // IEEE Transactions on Fuzzy Systems. Oct. 2003. Vol. 11, N. 5. P. 593— 604.

19. **Salmeron J. L.** Modelling grey uncertainty with Fuzzy Grey Cognitive Maps // Expert Systems with Applications. 2010. Vol. 37. N. 12. P. 7581—7588.

V. I. Vasilyev, Professor, e-mail: vasilyev@ugatu.ac.ru,
A. M. Vulfin, Associate Professor, e-mail: vulfin.alexey@gmail.com,
M. B. Guzairov, Professor, e-mail: guzairov@ugatu.su, **V. M. Kartak,** Professor, e-mail: kvmail@mail.ru,
L. R. Chernyakhovskaya, Professor, e-mail: lrchern@yandex.ru,
Ufa State Aviation Technical University, Ufa, 450077, Russian Federation

Cybersecurity Risk Assessment of Industrial Objects' ACS of TP on the Basis of Nested Fuzzy Cognitive Maps Technology

The paper is devoted to methodical aspects of quantitative assessment of cybersecurity risks for automated systems of control and checking the technological processes (ACS of TP) of modern industrial companies which are at present more often the objects of targeted attacks leading to widescale losses. As the basic approach to obtain the quantitative risk estimates, it is offered to use the system risk-oriented approach laid down in the series of international and national standards IEC 62443 and GOST R 62443. As the development of this approach, the authors offer the technique of ACS cybersecurity risks analysis consisting in formation on the basis of preliminary comprehensive examination of protected object its detailed cognitive model, reflecting the main factors leading to these risks, their interdependencies (cause-effect links) and final effects caused by these risks. The peculiarity of this cognitive model is its creation in the class of nested fuzzy grey cognitive maps, accumulating generally the information about both the global nature of risks character and the local mechanisms of their occurrence and propagation in the explored object. The application of mathematical apparatus of Fuzzy Grey Cognitive Maps (FGCM) here provides a possibility to obtain more reliable quantitative (interval) estimates of risks indices with account of disposable real statistical data. The example of using the offered technique of risks analysis for quantitative assessment of security level (integrity) of telemetric information used for monitoring and checking the parameters of onboard aviation systems condition at the stations of ground technical service is considered. The software tool "Cognitive Map Constructor" allowing to automate the main stages of applying this technique is developed.

Keywords: *cybersecurity, risk assessment, cognitive modeling, Fuzzy Grey Cognitive Map*

DOI: 10.17587/it.26...

References

1. **Threat landscape** for industrial automation systems. H2 2018, availible at: https://ics-cert.kaspersky.com/reports/2019/03/27/threat-landscape-for-industrial-automation-systems-h2-2018/ (accessed 17 August 2019).

2. **Yarushevskij D.** ICS cybersecurity — what is it and why?, available at: https://www.dialognauka.ru/press-center/article/13226/ (accessed 17 August 2019) (in Russian).

3. **Andreev Yu. S., Dergachev A. M., Zharov F. A., Sadyrin D. S.** Information Security of Automated Process Control Systems, *Izvestiya Vuzov. Priborostroenie*, 2019. vol. 62, no. 4. pp. 331—339 (in Russian).

4. **Vasilyev V. I., Kirillova A. D., Kukharev S. N.** Cybersecurity of automated control systems of industrial objects: modern trends and approaches (current state, trends), *Vestnik UrFO. Bezopasnost' v Informacionnoj Sfere,* 2018, vol. 4(30), pp. 66—74 (in Russian).

5. **Yarushevskij D.** Security of ACS of TP — Overview of the IEC 62443 Family of Standards, *Information Security/Informacionnaya bezopasnost'*, 2014, no. 3, available at: http://lib.itsec.ru/articles2/ (accessed 17 August 2019) (in Russian).

6. **Kosko B.** Fuzzy Cognitive Maps, *Intern. Journal of Man-Machine Studies*, 1986, vol. 1, pp. 65—75.

7. **Guzairov M. B., Vasilyev V. I., Kudryavtseva R. T.** The system analysis of information risks with application of fuzzy cognitive maps, *Infokommunikatsionnye Tekhnologii*, 2007, vol. 5, no. 4, pp. 42—48 (in Russian).

8. **Azhmuhamedov I. M.** Dynamic fuzzy cognitive model of the threat influence on information security of the system, *Bezopasnost' Informacionnyh Tekhnologij.* 2010, no. 2, pp. 68—72 (in Russian).

9. **Yeboah-Boateng E. O.** Using Fuzzy Cognitive Maps (FCMs) to Evaluate the Vulnerabilities with ICT Assets Disposal Policies, *Intern. Journal on Electrical & Computer Sciences IJECS-IJENS.* Oct. 2012, vol. 12, no. 5, pp. 20—31.

10. **Szwed P., Skrzynski P. A.** New lightweight method for security risk assessment based on Fuzzy Cognitive Maps, *Intern. Journal on Appl. Math. Comput. Sci.* 2014, vol. 24, no. 1, pp. 213—225.

11. **Vasilyev V. I., Vulfin A. M., Guzairov M. B.** Information security risk assessment using fuzzy production cognitive maps, *Informatcionnye Tekhnologii.* 2018, vol. 24, no. 4, pp. 266—273 (in Russian).

12. **Vasilyev V. I., Vulfin A. M., Guzairov M. B., Kirillova A. D.** Interval estimation of information risks with use of Fuzzy Grey Cognitive Maps*, Informatcionnye Tehnologii*, 2018, 10(24), pp. 657—664 (in Russian).

13. **Stylios C. D., Groumpos P. P.** Fuzzy Cognitive Maps Multi-Model for Complex Manufacturing Systems, *IFAC Large Scale Systems: Theory and Applications.* Bucharest, Romania, 2001, pp. 61—66.

14. **Stula M., Stipanicev D., Bodrozic L.** Intelligent Modeling with Agent-based Fuzzy Cognitive Map, *Intern. Journal on Intell. Systems.* 2010, 25(10), pp. 981—1004.

15. **Mohr S.** Modelling Approaches for Multilayer Fuzzy Cognitive Maps, available at: https://www.researchgate.net/publication/332158518_Modelling_Approaches_for_Multilayer_Fuzzy_Cognitive_Maps (accessed 17 August 2019).

16. **Mohagheghi S.** Fuzzy Cognitive Maps for Identifying Fault Activation Patterns in Automation Systems, available at: https://www.intechopen.com/books/ (accessed 17 August 2019).

17. **Motlagh O., Papageorgiou E. I., Tang S. H., Jamaludin Z.** Multivariate Relationship Modeling Using Nested Fuzzy Cognitive Map, *Sains Malaysiana*. 2014, no. 43(11), pp. 1781—1790.

18. **Zhang J. Y., Liu Z. Q., Zhou S.** Quotient FCMs — A Decomposition Theory for Fuzzy Cognitive Maps, *IEEE Transactions on Fuzzy Systems.* Oct. 2003, vol. 11, no. 5, pp. 593— 604.

19. **Salmeron J. L.** Modelling grey uncertainty with Fuzzy Grey Cognitive Maps, *Expert Systems with Applications*, 2010, vol. 37, no. 12, pp. 7581—7588.

УДК 004.056 DOI: 10.17587/it.26.222-230

А. С. Кабанов, канд. техн. наук, доц., e-mail: kabanov_as@mail.ru,
Московский институт электроники и математики имени А. Н. Тихонова
Национального исследовательского университета "Высшая школа экономики"

Оптимизация организационной структуры предприятия с учетом противодействия инсайдерской деятельности

Рассматриваются различные подходы к оптимизации организационной структуры предприятия и обоснована актуальность данной задачи с точки зрения защиты от инсайдерской деятельности. Предложен алгоритм определения места подразделения противодействия инсайдерской деятельности в организационной структуре предприятия. Показан прагматичный подход к оценке необходимости и стоимости внедрения средств противодействия инсайдерской деятельности. Приведено условие экономической целесообразности внедрения средств противодействия инсайдерской деятельности, а также предложены подходы к оценке инсайдерской информации и сформулированы основные выводы. Статья носит аналитический характер и может быть полезна руководителям служб информационной безопасности, преподавателям, аспирантам и студентам вузов.

Ключевые слова: *организационная структура предприятия, инсайдер, инсайдерская деятельность, ценность инсайдерской информации*

Введение

Все предприятия обладают организационной структурой, разработанной на этапе их создания и откорректированной в процессе функционирования. Всякая организационная структура может быть представлена в виде схемы, отдельными блоками которой будут выступать директор или руководитель предприятия, структурные подразделения предприятия, отдельные управленческие единицы и связи между ними.

Американский ученый Питер Друкер показал, что не может быть одной "единственно правильной" организационной структуры. Для каждого предприятия существует своя, оптимальная именно для него организационная структура. Оптимальна только та организационная структура, которая обеспечивает наиболее эффективную реализацию стратегии предприятия по достижению поставленной перед ним цели [1].

Следует отметить, что с точки зрения экономистов организационная структура должна быть оптимальна для достижения экономических целей предприятия. Данный подход не дает информации о том, как должна быть построена организационная структура, поскольку экономическая цель не отражает процессы, протекающие на предприятии. Но именно продукция и процессы, связанные с ее созданием, производством и реализацией, приносящие предприятию экономический эффект, обеспечивают достижение поставленной экономической цели и определяют организационную структуру. А сама продукция и все связанные с ней процессы, в свою очередь, определяются стратегией предприятия. Таким образом, "стратегия определяет структуру" [2]. Очевидно, что в свете современных угроз информационной безопасности становится актуальной задача противодействия инсайдерской деятельности, причем данная задача непосредственно влияет на процессы, протекающие на предприятии по достижению, в том числе, экономических целей.

Вопросы организационной структуры начинаются с разработки стратегии предприятия. Если стратегия изменяется, возможно, потребуется оптимизация организационной структуры под новую стратегию. Очевидно, что с точки зрения защиты от инсайдерской деятельности целесообразно оценить ценность данной информации (ее влияние на стратегию предприятия). После оценки ценности информации и принятия решения по противодействию возникает задача поиска оптимальной организационной структуры предприятия с учетом обеспечения защиты от инсайдерской деятельности.

В классическом понимании целесообразность проведения оптимизации определяется на основе отраслевых показателей, внутренней информации или внешней оценки. Очевидно, что целесообразность проведения оптимизации организационной структуры предприятия с точки зрения защиты от инсайдерской деятельности имеет смысл, только если эта оптимизация не приводит к нарушению стратегических целей (например, ухудшению экономических показателей).

Актуальным вопросом, рассмотренным в данной статье, является определение места подразделения противодействия инсайдерской деятельности (ПИД) в организационной структуре предприятия. В настоящее время

имеется несколько распространенных схем размещения подразделения ПИД в организационной структуре, но, по мнению автора, для некоторых типов предприятий пул вариантов можно значительно сократить (полагаясь на здравый смысл), при этом, безусловно, каждое предприятие индивидуально и может иметь свою специфику.

Следует отметить, что, несмотря на большое число иностранных и отечественных публикаций по проблемам ПИД, все они преимущественно сводятся к анализу средств противодействия (SIEM и т.д.) и разработкам подходов к классификации инсайдеров в целях более эффективного противодействия (например, работы [3, 4]). Вопросы изменения организационной структуры предприятия для противодействия инсайду практически не затрагиваются в отечественной и зарубежной литературе, а лишь изредка упоминаются. В некоторых работах рассматривают различные по размеру предприятия с точки зрения внедрения тех или иных средств противодействия (например, [5]). И это несмотря на то, что нередко оптимизация структуры предприятия может привести к отсутствию необходимости внедрения средств защиты от инсайдерской деятельности. Определение ценности инсайдерской информации редко встречается в публикациях и носит преимущественно очень формальный характер.

Учитывая актуальность данной проблемы, настоящая статья посвящена следующим основным вопросам.

1. Оптимизация организационной структуры предприятия с точки зрения защиты от инсайдерской деятельности.

2. Определение места подразделения ПИД в организационной структуре предприятия.

3. Оценка ценности инсайдерской информации.

1. Построение системы противодействия инсайдерской деятельности с учетом стратегических целей предприятия

После определения стратегических целей и формирования организационной структуры предприятия первостепенной задачей (с точки зрения оптимизации по противодействию инсайду) лиц, ответственных за ПИД, является создание реестра соответствующей информации с оценкой ее стоимости (места в организационной структуре), а также выбор средств ПИД и определение стоимости их внедрения. Следует отметить, что тип информации (ограниченного и неограниченного распространения) достаточно часто не влияет на ценность информации. Нередко открытая информация представляет собой значительно больший "интерес" и ценность для инсайдера, чем информация ограниченного распространения. Например, открытая информация о компаниях партнерах и условиях сделок для организации-конкурента намного "интереснее", чем защищаемые законом и обрабатываемые специальным образом с использованием средств защиты персональные данные.

После создания соответствующего реестра для предприятия возможны три стратегии, выбор которых зависит от внутренней структуры организации (возможности оптимизации), а также специфики реализации технологических и бизнес-процессов, а именно:

1. Для небольших организаций либо организаций, в которых инсайдерская информация достаточно компактно сосредоточена (в силу внутренней структуры и реализации технологических/бизнес-процессов), защита от инсайдерской деятельности может быть сведена к оптимизации структуры в части обработки данной информации. Например, если инсайдерской информации немного, и ее концентрация в одном месте не приводит к нарушению технологических и бизнес-процессов организации, то целесообразно поместить ее в одно помещение одного подразделения с доступом узкого круга доверенных лиц, а также в случае необходимости реализовать достаточно недорогие организационно-технические меры защиты. Кроме того, необходима разработка и утверждение порядка доступа к инсайдерской информации, правил соблюдения ее конфиденциальности, а также создание (определение, назначение) структурного подразделения (должностного лица), в обязанности которого входит осуществление контроля. Данная стратегия, как правило, не требует значительных финансовых затрат (в основном затраты организационные), и реализация систем ПИД достаточно широко описана в различных трудах, например [6—9].

2. Для инфраструктурно сложных предприятий необходимо провести оценку на предмет возможности оптимизации с точки зрения защиты от инсайдерской деятельности, например, свести все звенья, обрабатывающие инсайдерскую информацию, в одном защищенном месте. Очевидно, что если стоимость изменения организационной структуры превышает стоимость ущерба от инсайдерской деятельности, то реорганизация не имеет смысла. Следовательно, если инфраструктурно сложное предприятие нельзя свести к первому типу, то данное предприятие принадлежит к следующему типу.

3. Для больших, инфраструктурно сложных, разветвленных организаций, в которых инсайдерская информация сильно рассредоточена (в силу специфики реализации технологических/бизнес-процессов), целесообразность внедрения различных средств ПИД необходимо предварительно сопоставить со стоимостью утечки инсайдерской информации и стоимостью средств ПИД. Внедрение средств ПИД имеет экономический смысл при выполнении принципа разумной достаточности [10], а именно следующего условия:

$$C_{\text{СПИ}} < C_{\text{риск}},$$

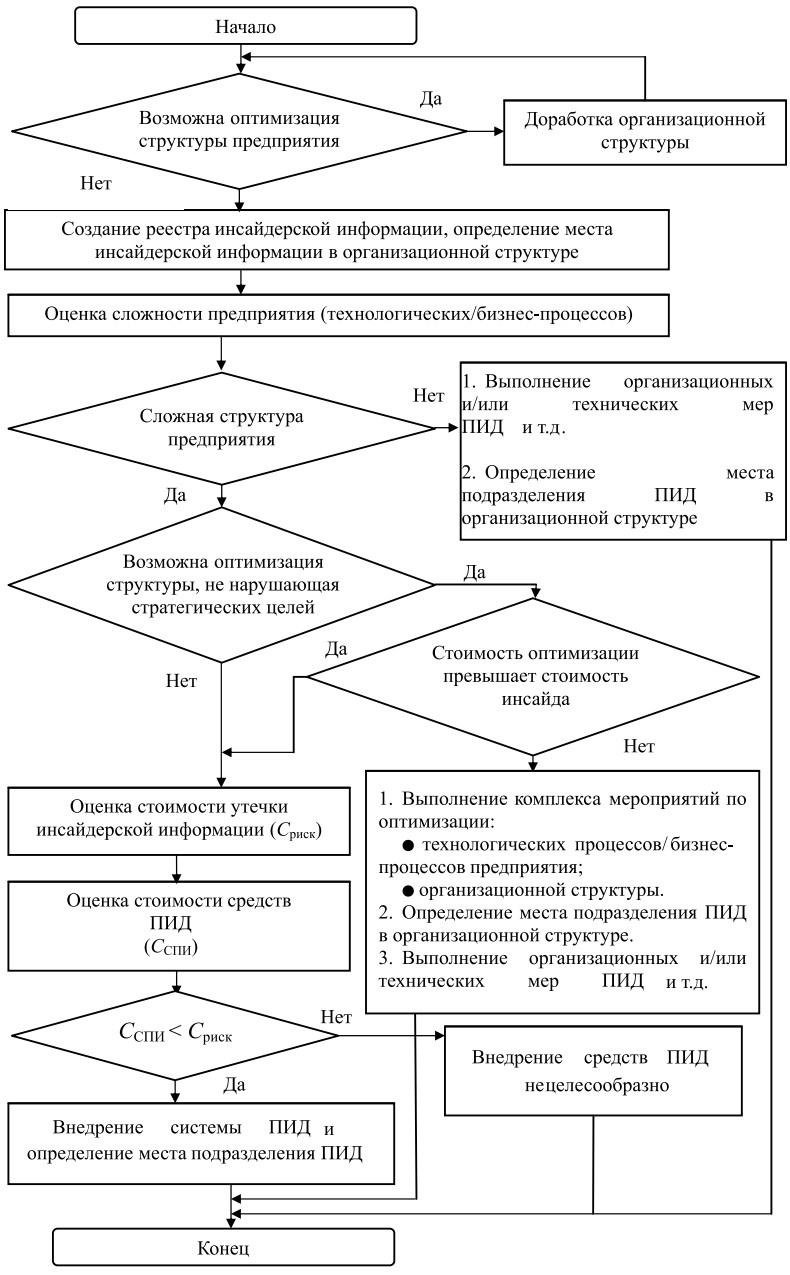

Рис. 1. Алгоритм внедрения средств противодействия инсайду

где $C_{\text{СПИ}}$ — стоимость внедрения средств ПИД; $C_{\text{риск}}$ — стоимость утечки инсайдерской информации для организации.

Следует отметить, что в процессе расчета $C_{\text{риск}}$ в его стоимость (помимо стоимости закупки и внедрения средств ПИД) нередко необходимо включить так называемые репутационные риски организации.

При условии $C_{\text{СПИ}} \geqslant C_{\text{риск}}$ внедрение средств ПИД бессмысленно с точки зрения экономического эффекта. В этом случае, как вариант, возможно построение графа передачи инсайдерской информации между средствами обработки в целях проведения его оптимизации для уменьшения стоимости $C_{\text{СПИ}}$ либо приведения к организации первого типа.

Алгоритм выбора средств противодействия отображен на рис. 1.

Далее рассмотрим подход к определению сложности организации. Для сложных организаций характерна разветвленная структура с большим числом элементов (средств обработки информации, филиалов и т.д.). Точечные решения для таких организаций не всегда применимы и эффективны. При этом сетевые программно-аппаратные средства защиты (в первую очередь SIEM-системы, а также DLP и т.д.) являются более дорогими в части закупки и внедрения. Поскольку интерес представляет только инсайдерская информация, которая хранится, обрабатывается и передается в/между средствами обработки, следовательно, оценка сложности организации тождественна инфраструктурной сложности совокупности данных систем и связей между ними. Таким образом, сложность организации (инфраструктуры) можно оценить, используя теорию графов, где вершины соответствуют отдельным средствам обработки инсайдерской информации, а ребра определяют информационное взаимодействие между ними [11]. Веса ребер графа определяют объем и частоту передаваемой инсайдерской информации. Наличие разных типов взаимодействия определяет множество инфраструктурных графов $G_k = \langle V_k, E_k, W_k \rangle$, где V_k — множество вершин графа; E_k — множество ребер графа; W_k — вес ребер графа; k — тип взаимодействия.

Объединенный граф инфраструктуры имеет вид

$$G = \bigcup_{k=1}^{K} G_k = \langle V, E, W \rangle,$$

где $V = \bigcup_{k=1}^{K} V_k$; $E = \bigcup_{k=1}^{K} E_k$; K — число типов взаимодействия.

Вес объединенного графа для каждого $v_{ij} \in V$ ребра определяется суммой весов исходных графов $w_{ij} = \sum_{k=1}^{K} w_{ij}^k$.

Таким образом, получив граф средств обработки инсайдерской информации и связей между ними, необходимо провести оценку сложности предприятия. Создание указанного графа для некоторых небольших организаций первого типа позволит решить оптимизационные задачи, например, для сосредоточения инсайдерской информации в одном месте и т.д. Под структурной сложностью инфраструктуры предприятия будем понимать свойство, оценивающее размерность такого объединенного графа, многообразие маршрутов между его вершинами, число циклов, близость между вершинами и др.

Необходимо сформулировать требования, которым должен удовлетворять объединенный граф инфраструктуры, чтобы организацию можно было отнести к одному из типов.

На этапе создания реестра инсайдерской информации необходима идентификация всех вершин графа, являющихся средствами обработки инсайдерской информации ($N_{\text{СОИИ}}$). Также должна быть определена максимальная вместимость кластеров средств обработки инсайдерской информации, требующих выполнения недорогостоящих организационно-технических мер защиты информации ($N_{\text{мест}}$), а также число кластеров в конкретной организации (L).

Таким образом, для определения инфраструктурной сложности организации необходимо проверить три условия:

1. $N_{\text{СОИИ}} \leqslant \sum_{i=1}^{L} N_{\text{мест}\,i}$.
2. Размещение всех $N_{\text{СОИИ}}$ во всех $\sum_{i=1}^{L} N_{\text{мест}\,i}$ не влечет нарушения технологических и бизнес-процессов организации.
3. Отсутствие удаленных частей организации с каналами связи, по которым циркулирует инсайдерская информация.

По мнению автора, выполнение всех трех условий характерно для предприятий первого типа (как правило, небольших). Невыполнение хотя бы одного условия влечет идентификацию предприятия как предприятия второго либо третьего типов. Наличие третьего условия обусловлено относительной дороговизной сетевых средств защиты (особенно сертифицированных) и более разветвленной структурой процесса обработки инсайдерской информации со всеми вытекающими последствиями.

Следует отметить, что предложенный подход к построению графа сложности предприятия позволит наглядно увидеть все информационные потоки инсайдерской информации, оценить объем и частоту передаваемой инсайдерской информации для принятия решений по внедрению систем сетевой защиты, а также объективно оценить $C_{\text{СПИ}}$ конкретной организации.

2. Определение места подразделения противодействия инсайдерской деятельности в организационной структуре предприятия

Место подразделения информационной безопасности и проблема подчиненности обсуждаются достаточно давно. Следует отметить, что единого мнения в сообществе специалистов по данному вопросу нет, различные авторы [12] отстаивают часто противоположные точки зрения, приводя разумные аргументы. В рамках данной статьи рассматривается место и подчиненность только подразделения ПИД без учета остальных составляющих подразделения информационной безопасности, службы безопасности и т.д. Небольшие предприятия (ИП и т.д.), в которых функцию подразделения ПИД может выполнить один человек или небольшая группа лиц, также не рассматриваются в данной статье.

В настоящее время наиболее распространены следующие схемы организации подразделения ПИД.

1. Подчинение службе безопасности (экономической, собственной и т.д.). Одна из наиболее часто встречающихся схем. Недостатком является то, что если ПИД осуществляется преимущественно программно-техническими методами, то данный функционал слабо пересекается со службой безопасности, что часто приводит к недопониманиям между руководством службы безопасности и подразделением ПИД. Положительным является тот факт, что полномочия у службы безопасности, как правило, очень высокие, что существенно упрощает работу подразделения ПИД.

2. Подчинение подразделению информационных технологий (ИТ). В данной схеме налицо конфликт интересов, поскольку работа подразделения ПИД подразумевает в том числе контроль исполнения сотрудниками ИТ-подразделения правил, предписаний и регламентов. Кроме того, значительная часть функций подразделения ИТ не совсем коррелируется с деятельностью подразделения ПИД. Достоинством является то, что подразделению ПИД значительно проще внедрять программно-технические системы.

3. Создание самостоятельного подразделения. Данная схема требует существенных финансовых издержек, обладает достоинствами первой схемы (подчиненности службе безопасности) и лишена недостатков второй схемы.

Поскольку основополагающим критерием оценки решений для подавляющего большинства руководителей предприятий является экономическая целесообразность, то предлагается следующая схема определения места подразделения ПИД (рис. 2).

Указанная схема не является единственно возможной, но позволяет аргументированно принимать решение о месте подразделения ПИД преимущественно с точки зрения экономической целесообразности.

Очевидно, что для предприятий первого и второго типа схема циркуляции инсайдерской информации минимизируется и может быть защищена в основном организационно-техническими мерами, управление которыми находится, как правило, в ведении службы безопасности.

В указанной схеме в случае трудоемкости в сфере ИТ, большей 50 %, предлагается создание отдельного подразделения ПИД, поскольку функции преимущественно не относятся к службе безопасности, а значительная трудоемкость приходится на ИТ. Включение подразделения ПИД в подразделение ИТ не даст существенного эффекта, но приведет к недостаткам второй схемы.

Рис. 2. Схема определения места подразделения ПИД

При трудоемкости подразделения ПИД в сфере ИТ, меньшей 50 %, возможны следующие варианты в порядке предпочтения:

- включение подразделения ПИД в службу безопасности, поскольку функций ИТ не очень много;
- создание обособленного подразделения ПИД.

По мнению автора, предлагаемая схема отражает основные тенденции подчиненности подразделения ПИД. Отсутствие на рис. 2 подчиненности подразделения ПИД подразделению ИТ объясняется чрезмерными рисками конфликта интересов и отсутствием в том числе существенного экономического эффекта. Для большой и малой трудоемкости ИТ по противодействию инсайдерской деятельности нет существенного экономического эффекта по следующим причинам: большая трудоемкость потребует значительных ресурсов параллельно классическим функциям ИТ, а малая приведет к наличию в ИТ-подразделении значительного штата сотрудников с другими функциями.

3. Определение ценности инсайдерской информации

Далее рассмотрим возможные подходы к оценке ценности инсайдерской информации, например, для создания реестра инсайдерской информации.

Под ценностью инсайдерской информации, как правило, понимается широкий круг свойств информации, которые определяют степень влияния и воздействия на деятельность организации в случае ее утечки к организации-конкуренту. Если информация касается незначительных вопросов и утечка такой информации не ведет к значительному ущербу, то фактом утечки такой информации можно в определенной мере пренебречь. В то же время информация о ситуации, которая чревата банкротством организации, требует повышенного внимания и привлечения значительных ресурсов даже в том случае, если риск маловероятен.

Несмотря на то что ценность инсайдерской информации включает в себя комплекс показателей, главным критерием значимости является потенциальный ущерб для организации, измеряемый в натуральных или денежных показателях.

Ценность инсайдерской информации может быть ранжирована в соот-

ветствии с определенным заданным критерием. Как правило, им является уровень потенциальных негативных эффектов для организации. Рейтинг может присваиваться как самой инсайдерской информации, так и ее источникам [13]. Для оценки ценности инсайдерской информации может быть применена шкала, представленная в табл. 1.

Представленная шкала не претендует на истину в последней инстанции, но, по мнению автора, может успешно применяться для ранжирования ценности инсайдерской информации (например, в реестре инсайдерской информации организации). Наиболее очевидным для ранжирования ценности инсайдерской информации и вероятности ее утечки в соответствии с табл. 1 является использование экспертного оценивания. Однако для оценки выполнения критерия $C_{\text{СПИ}} < C_{\text{риск}}$, кроме ранжирования, необходима стоимостная оценка инсайдерской информации. Следует отметить, что не всю инсайдерскую информацию можно достаточно легко оценить в денежном выражении (например, репутационный ущерб и т.д.). В этом случае, по мнению автора, целесообразно воспользоваться методом непосредственной оценки (балльным методом). Он позволяет определить, насколько один фактор более значим, чем другие. В этом случае диапазон изменения характеристик объекта разбивается на отдельные интервалы, каждому из которых приписывается определенная оценка (балл), например, от 0 до 10. Следует отметить,

Таблица 1

Шкала оценки ценности инсайдерской информации

Рейтинг	Оценка инсайдерской информации	Вероятность утечки	Последствия утечки для организации
5	Имеет решающее значение для деятельности организации	Высокая	Катастрофические
		Средняя	
		Низкая	
4	Высокая значимость	Высокая	Значительные
		Средняя	
		Низкая	
3	Средняя значимость	Высокая	Умеренные
		Средняя	
		Низкая	
2	Низкая значимость	Высокая	Малозначительные
		Средняя	
		Низкая	
1	Незначительный риск	Высокая	Несущественные
		Средняя	
		Низкая	

что экспертное оценивание не является темой данной статьи, поэтому определение степени согласованности мнений экспертов и другие вопросы оценки адекватности и качества экспертного оценивания выходят за рамки данного материала.

Для определения стоимости инсайдерской информации (на основе полученных балльных оценок) можно воспользоваться аддитивной моделью. При использовании данной модели определение ценности базируется на экспертных оценках компонентов данной информации, и при объективности стоимостных оценок ее компонентов подсчитывается искомая величина — их сумма в стоимостном эквиваленте [13]. Основная проблема заключается в том, что количественная оценка компонентов информации часто оценивается необъективно, даже если оценка выполняется высококвалифицированными специалистами, причина заключается в неоднородности компоненов в целом. Для решения этой проблемы принято использовать иерархическую относительную шкалу, которая представляет собой линейный порядок, с помощью которого сравниваются отдельные компоненты по ценности один относительно другого. Случай единой шкалы равносилен тому, что все компоненты, имеющие равную порядковую оценку, равноценны.

Рассмотрим следующий пример. Пусть даны n объектов инсайдерской информации O_1, O_2, ..., O_n, оценка проводится по десятибалльной шкале; результат оценки экспертами — вектор ценностей объектов каждого относительно другого: (3, 5, ..., 8). Предположим, что изначально определена цена одного из объектов, например $O_2 = 150$ тыс. руб.

Вычисляем стоимость одного балла: $O_2/k = 150/5 = 30$ тыс. руб., где k — оценка объекта в баллах.

Аналогичным образом выполняется оценка других объектов. Сумма стоимостей объектов инсайдерской информации дает полную стоимость всей инсайдерской информации.

Рассмотрим обратную ситуацию. Если известна конечная стоимость инсайдерской информации, то исходя из нее можно обратным преобразованием определить стоимость каждого объекта инсайдерской информации.

С учетом применения метода непосредственного оценивания и аддитивной модели табл. 1, например, принимает числовой вид, который можно с успехом применять для проверки критерия $C_{\text{СПИ}} < C_{\text{риск}}$.

Рассмотрим два подхода для оценки ценности инсайдерской информации с точки зрения ее пользы для организации-конкурента. Следует отметить, что при зеркальном рас-

смотрении (с позиции оценки инсайдерской информации организацией) данные подходы справедливы для определения $C_{риск}$.

Прагматичный подход к оценке информации (в нашем случае — инсайдерской информации) предложен А. А. Харкевичем [14, 15]. Мерой ценности информации является изменение вероятности достижения цели при получении этой информации. В нашем случае количественная мера ценности инсайдерской информации $I_ц$ выражена следующим образом:

$$I_ц = \log P_1 - \log P_0 = \log P_1/P_0,$$

где P_0 — начальная, до получения инсайдерской информации, вероятность достижения цели организацией-конкурентом; P_1 — вероятность достижения цели организацией-конкурентом после получения информации.

Возможны следующие три случая. В первом случае полученная инсайдерская информация является ценной, увеличивающей вероятность достижения цели организацией-конкурентом, т.е. $P_1 > P_0$. Следовательно, информация является ценной, полезной, и количественная мера ценности информации $I_ц > 0$.

Во втором случае информация не изменяет вероятность достижения цели организацией-конкурентом. Она является бесполезной. При этом $P_1 = P_0$ и $I_ц = 0$.

В третьем случае вероятность достижения цели уменьшается, поскольку полученная информация является ложной, ошибочной. При этом $P_1 < P_0$ и $I_ц < 0$.

Данный подход можно успешно применять совместно с методами экспертного оценивания, представленными ранее.

Рассмотрим подход, *основанный на изменении экономической эффективности принятых решений* организацией-конкурентом после получения инсайдерской информации.

Например, некоторая организация-конкурент является одним из лидеров отрасли. Ей необходимо провести модернизацию своих производственных мощностей. На рынке также имеется другая организация, которая в силу своей значительности обладает информацией о перспективах развития рынка. Данная информация, несомненно, представляет интерес для организации-конкурента, поскольку позволяет выработать оптимальную стратегию развития. Цель организации-конкурента — определить ценность инсайдерской информации организации.

Допустим, руководство организации-конкурента рассматривает три варианта действий:

- вложить средства в собственную разработку производственных мощностей на новом технологическом уровне, не имеющих аналогов у конкурентов;
- вложить средства в закупку имеющихся на рынке технологий;
- не проводить модернизацию производств (бездействие).

Размер выигрыша или потерь организации-конкурента зависит от благоприятного или неблагоприятного состояния рынка [16].

Первоначально информация о состоянии рынка отсутствует, но экономисты могут рассчитать выигрыши/потери организации-конкурента от реализации стратегий при благоприятных и неблагоприятных условиях. В соответствии с принципом Байеса состояние рынка (благоприятное или неблагоприятное) принимают равновероятным и равным 0,5.

Средний ожидаемый выигрыш рассчитывается по формуле:

$$W = P_б W_в + P_н W_п,$$

где $P_б$ и $P_н$ — вероятности благоприятных и неблагоприятных состояний соответственно; $W_в$ и $W_п$ — выигрыши и потери организации-конкурента соответственно.

Результаты расчетов до и после получения инсайдерской информации от организации представлены в табл. 2 и 3.

Результаты расчетов показывают, что наилучшим решением при отсутствии инсайдерской информации является закупка технологий, так как при этом средний выигрыш максимален и равен $W_0 = 10$ млн руб.

Допустим, покупка инсайдерской информации обойдется организации-конкуренту в 1 млн руб. Инсайдерская информация указы-

Таблица 2

Средний выигрыш до получения инсайдерской информации

№	Действия организации-конкурента	Выигрыш/потери в зависимости от конъюнктуры рынка		Средний выигрыш до получения инсайдерской информации
		Благоприятный $P_б = 0,5$	Неблагоприятный $P_н = 0,5$	
1	Собственная разработка	130 млн руб.	−120 млн руб.	5 млн руб.
2	Покупка технологий	30 млн руб.	−10 млн руб.	10 млн руб.
3	Бездействие	10 млн руб.	−20 млн руб.	−5 млн руб.

Таблица 3

Средний выигрыш после получения инсайдерской информации

№	Действия организации-конкурента	Выигрыш/потери в зависимости от конъюнктуры рынка		Средний выигрыш после получения инсайдерской информации
		Благоприятный $P_б = 0,7$	Неблагоприятный $P_н = 0,3$	
1	Собственная разработка	130 млн руб.	−120 млн руб.	55 млн руб.
2	Покупка технологий	30 млн руб..	−10 млн руб.	18 млн руб.
3	Бездействие	10 млн руб.	−20 млн руб.	1 млн руб.

вает на то, что прогнозируется благоприятное состояние рынка с вероятностью 0,7 и неблагоприятное с вероятностью 0,3. В этом случае максимальный средний выигрыш (W_1 = = 55 млн руб.) организация-конкурент получит при выборе стратегии по собственной разработке производственных мощностей на новом технологическом уровне.

Таким образом, полученная дополнительная информация изменяет представление о целесообразности стратегии организации-конкурента и, соответственно, изменяет экономический эффект с 10 млн руб. до 55 млн руб.

Ценность дополнительной информации равна разности максимальных средних выигрышей организации-конкурента до и после получения инсайдерской информации с учетом стоимости самой информации:

$$I_ц = (W_1 - W_0) - S_п,$$

где $S_п$ — стоимость получения инсайдерской информации.

Для рассмотренного примера $I_ц = (55 - 10) - 1 = 44$ млн руб.

Таким образом, ценность инсайдерской информации определяется выгодой от ее использования. Ценность инсайдерской информации может существенно превысить стоимость ее получения. Платить за инсайдерскую информацию имеет смысл, если $(W_1 - W_0) > S_п$, т. е. $I_ц > 0$.

В рассмотренном примере инсайдерская информация указывает на прогноз благоприятного и неблагоприятного состояния рынка, что на практике, например, можно определить по числу выпускаемых в продажу средств производства с определенными характеристиками, которые влияют на конкуренцию в определенном сегменте и объеме рынка.

Очевидно, что $I_ц$ входит в $C_{риск}$, а в некоторых случаях полностью тождественно $C_{риск}$.

Заключение

Предложенные подходы к оптимизации организационной структуры предприятия и определению места подразделения противодействия инсайдерской деятельности позволяют на интуитивно понятном уровне, используя здравый смысл, противодействовать инсайду. Развитие предложенных подходов позволит выявить схожие по характеристикам предприятия и объединить их в кластеры в целях повышения качества оценок, возможности оптимизации, а также повышения объективности и точности принятия решений.

Описанный экономический критерий целесообразности внедрения средств ПИД (взятый из классической теории информационной безопасности) во многих трудах незаслуженно отсутствует, что с точки зрения практической реализации некорректно ввиду его ключевой роли (например, для руководителей организации).

Рассмотренные подходы к внедрению средств ПИД для различных предприятий, по мнению автора, являются наиболее логичными и позволяют быстро определиться сквозь призму экономической целесообразности с методами, формами и средствами противодействия инсайдерской деятельности. Дальнейшими направлениями развития являются разработка типовых моделей предприятий с детализацией условий классификации и характеристик для сложных организаций.

Представленные подходы к оценке и ранжированию инсайдерской информации могут с успехом применяться на практике, поскольку достаточно просты и интуитивно понятны. Выбор используемого подхода должен определяться удобством и наличием исходных данных для конкретной организации.

Список литературы

1. **Жемчугов А. М., Жемчугов М. К.** Организационная структура и стратегия предприятия // Проблемы экономики и менеджмента. 2011. № 2.

2. **Шершнева З. Е.** Стратегическое управление. К.: КНЭУ, 2004. 394 с.

3. **Ахмедов Т. Ч.** Междисциплинарный подход к вопросу выявления недобросовестного инсайдера в организации // Вестник Московского университета МВД России. 2014. № 2.

4. **Карпычев В. Ю., Сычев В. М.** Применение байесовских сетей в задачах анализа внутренних угроз информационной безопасности // Вестник Воронежского института МВД России. 2015. № 1.

5. **Matthew L. Collins's, Randall F. Trzeciak** et al. Common Sense Guide to Mitigating Insider Threats, Fifth Edition. Software Engineering Institute Carnegie Mellon University. Technical Report. December 2016.

6. **Кабанов А. С., Лось А. Б.** Причины, профилактика и методы противодействия инсайдерской деятельности // Безопасность бизнеса. 2016. № 3.

7. **Кабанов А. С., Суроев А. В., Лось А. Б.** Методы социальной инженерии в сфере информационной безопасности и противодействие им // Российский следователь. 2015. № 18.

8. **Веденеев В. С., Бычков И. В.** Системы выявления инсайдеров // Математические структуры и моделирование. 2014. № 4(32).

9. **Сычев В. М.** Формализация модели внутреннего нарушителя информационной безопасности // Вестник МГТУ им. Н. Э. Баумана. 2015. № 2.

10. **Гайкович В. Ю., Ершов Д. В.** Основы безопасности информационных технологий. М.: МИФИ, 1995. 96 с.

11. **Наумов В. Н., Кучеренко Д. В.** Исследование структурной сложности инфраструктуры государственных информационных систем методами анализа социальных графов // Современные наукоемкие технологии. 2019. № 2. С. 114—122.

12. **Директор** по информационной безопасности // Государство. Бизнес. ИТ, 2017. URL: http://www.tadviser.ru/index.php/Статья:Директор_по_информационной_безопасности_(Chief_information_security_officer,_CISO).

13. **Шарамко М. М.** Внутренний контроль: методология, система и процессы. М.: Русайнс, 2016. 228 с.

14. **Грушо А. А., Тимонина Е. Е.** Теоретические основы защиты информации. М.: Яхсмен, 1996.

15. **Волкова В. Н.** Теория информационных процессов и систем: учебник и практикум для академического бакалавриата. М.: Издательство Юрайт, 2016. 502 с.

16. **Лазебник В. М.** Экономическая кибернетика. URL: https://studfiles.net/preview/1100363/.

A. S. Kabanov, Candidate of Science (PhD) in technology,
Associate Professor of the Department, e-mail: kabanov_as@mail.ru,
Moscow Institute of Electronics and Mathematics, National Research University
"Higher School of Economics", Moscow, 123458, Russian Federation

Optimization of the Organizational Structure of the Enterprise Taking into Account the Opposition of the Insider Activity

Various approaches to optimizing the organizational structure of the enterprise are considered and the relevance of this task in terms of protection from insider activity is substantiated. An algorithm is proposed for determining the location of the anti-insider unit in the organizational structure of the enterprise. A pragmatic approach to assessing the need and cost of introducing counter measures to insider activities is shown. The condition of economic feasibility of introducing means of counteracting insider activities is given, and approaches to assessing insider information are proposed and the main conclusions are formulated. The article is analytical in nature and may be useful to heads of information security services, teachers, graduate students and university students.

Keywords: *organizational structure of the enterprise, insider, insider activity, value of insider information*

DOI: 10.17587/it.26.222-230

References

1. **Zhemchugov A. M., Zhemchugov M. K.** Organizational structure and strategy of the enterprise, *Problems of Economics and Management*, 2011, no. 2.

2. **Shershneva Z. E.** Strategic management, Kyiv, National University of Economics, 2004, 394 p.

3. **Akhmedov T. Ch.** Interdisciplinary approach to the issue of identifying an unfair insider in an organization, *Bulletin of the Moscow University of the Ministry of internal Affairs of Russia,* 2014, no. 2.

4. **Karpychev V. Yu., Sychev V. M.** Application of Bayesian networks in the analysis of internal threats to information security, *Bulletin of the Voronezh Institute of the Ministry of internal Affairs of Russia*, 2015, no. 1.

5. **Collins's M. L., Trzeciak R. F.** et al. Common Sense Guide to Mitigating Insider Threats, Fifth Edition, Software Engineering Institute Of Carnegie Mellon University, Technical Report, December 2016.

6. **Kabanov A. S., Los A. B.** Reasons, prevention and methods of countering insider activity, *Business Security*, 2016, no. 3.

7. **Kabanov A. S., Suroev A. V., Los A. B.** Methods of social engineering in the field of information security and counteraction to them, *Russian Investigator*, 2015, no. 18.

8. **Vedeneev V. S., Bychkov I. V.** Systems for identifying insiders, *Mathematical Structures knd Modeling,* 2014, no. 4(32).

9. **Sychev V. M.** Formalization of the model of internal intruder information security, *Bulletin of the Bauman Moscow state technical University*, 2015, no. 2.

10. **Gaikovich V. Yu., Ershov D. V.** Fundamentals of information technology security, Moscow, Moscow Institute of engineering and physics, 1995, 96 p.

11. **Naumov V. N., Kucherenko D. V.** Study of the structural complexity of the infrastructure of state information systems by methods of analysis of social graphs, *Modern Science-Intensive Technologies*, 2019, no. 2, pp. 114—122.

12. **Chief** Information Security Officer, *State. Business. IT*, 2017, available at: http://www.tadviser.ru/index.php/Статья:Директор_по_информационной безопасности_(Chief_information_security_officer,_CISO).

13. **Shramko M. M.** Internal control: methodology, system, and processes, Moscow, Rusyns, 2016, 228 p.

14. **Grusho A. A., Timonina E. E.** Theoretical bases of information protection, Moscow, Jahsman, 1996.

15. **Volkova V. N.** Theory of information processes and systems: textbook and workshop for academic undergraduate studies, Moscow, Yurayt Publishing House, 2016, 502 p.

16. **Lazebnik V. M.** Economic Cybernetics, available at: https://studfiles.net/preview/1100363/.

УДК 621.382.82.001 DOI: 10.17587/it.26.231-238

В. Б. Маничев[1], канд. тех. наук, доц., manichev@bmstu.ru,
Е. Ф. Митенкова[2], канд. физ.-мат. наук, зав. лабораторией,
Э. О. Фельдман[1], бакалавр, **Д. Ю. Кожевников**[1], вед. инженер,
Е. В. Соловьева[2], канд. физ.-мат. наук, ст. науч. сотр., sol@ibrae.ac.ru,
[1]Московский государственный технический университет им. Н. Э. Баумана,
[2]Институт проблем безопасного развития атомной энергетики Российской академии наук

Достоверность и точность решения задач нуклидной кинетики

Современные требования при разработке реакторов нового поколения инициируют совершенствование расчетной базы, в том числе и повышение точности решения задач нуклидной кинетики. Это особенно актуально при максимально полном использовании ядерно-физических данных ввиду объективной сложности получения аналитических решений и экспериментальных данных для большей части нуклидов облучаемого топлива. Показано, что при решении жестких систем обыкновенных дифференциальных уравнений (ОДУ) большой и сверхбольшой размерности следует учитывать влияние погрешностей округления чисел на достоверность и точность получения конечного результата вычислений. Для гарантированно точного решения систем линейных алгебраических уравнений (СЛАУ) с приемлемыми затратами счета следует использовать алгоритм итерационного уточнения с вычислением правой части с повышенной разрядностью. Это особенно актуально для задач высокой размерности с разреженными матрицами. Для получения решения с гарантированной достоверностью и точностью для всех элементов ОДУ большой размерности в пакете MZK реализован одностадийный неявный метод Эйлера с представленным алгоритмом решения СЛАУ с удвоенной и повышенной точностью вычислений. Пакет MZK может использоваться для получения реперных значений в прецизионных расчетах задач нуклидной кинетики.

Ключевые слова: *математическое моделирование, обыкновенные дифференциальные уравнения (ОДУ), линейные алгебраические уравнения (ЛАУ), жесткие системы, нуклидная кинетика, гарантированная точность, погрешность округления*

Введение

Для решения задач нуклидной кинетики разработано достаточно много программ с разными допущениями и ограничениями математической модели [1]. Математическая модель нуклидной кинетики базируется на системе обыкновенных дифференциальных уравнений (ОДУ) первого порядка, представляемых уравнениями вида $d\mathbf{X}(t)/dt = \mathbf{A}\mathbf{X}(t)$, где $\mathbf{A}$ — матрица эффективных скоростей реакций накопления и увода элементов вектора $\mathbf{X}$, размерность которого определяется числом рассматриваемых элементов (нуклидов). Элементы матрицы определяются как $a_{ij} = \sum_{j=1}^{N} p_{ij}\lambda_j + \phi\sum_{k=1}^{N} q_{ik}\sigma_k \quad (i \neq j)$ и $a_{ii} = -(\lambda_i + \phi\sigma_i + r_i) + f_i$, где N — число нуклидов; p_{ij} — доля радиоактивного распада j-го нуклида в образовании i-го нуклида; λ_j — коэффициент радиоактивного распада i-го нуклида; ϕ — нейтронный поток; q_{ik} — доля поглощения нейтрона k-ми нуклидами, приводящими к образованию i-го нуклида; σ_k — сечение поглощения k-го нуклида; r_i — скорость увода из системы i-го нуклида; f_i — скорость внешней подпитки i-го нуклида. В существующих программах нуклидной кинетики ограничения касаются числа рассматриваемых нуклидов, структуры цепочек переходов, представляемых значениями a_{ij} и λ. Отдельные программы ориентированы на использование только линейных переходов без ветвлений и циклов со строго различающимися коэффициентами с сохранением начальных значений $\mathbf{X}_0$ для каждой цепочки. В других программах ветвления и циклы реализуются с помощью специальных процедур с искусственно введенными элементами [2].

Современные требования при разработке реакторов нового поколения инициируют со-

вершенствование расчетной базы, в том числе и повышение точности решения задач нуклидной кинетики. При отсутствии экспериментальных данных и аналитических решений особую актуальность приобретает решение задач нуклидной кинетики с максимально полным использованием современных ядерно-физических данных [3, 4]. Для решения задач нуклидной кинетики программы семейства ORIGEN на протяжении более 30 лет остаются наиболее востребованными. В программе ORIGEN2, формально не имеющей ограничений на число элементов и структуру переходов, для вычисления элементов $\mathbf{X}$ используются разные подходы — для короткоживущих применяется метод Гаусса—Зейделя, для остальных решение $\mathbf{X}(t) = \mathbf{e}^{\mathbf{A}t}\mathbf{X}_0$ находится с помощью вычисления матричной экспоненты в виде ряда Тейлора $\mathbf{e}^{\mathbf{A}t} = \sum_{k=0}^{\infty} \frac{(\mathbf{A}t)^k}{k!}$ [5]. Возникающие при этом сложности изложены во многих работах [1, 6, 7].

Постановка задачи

Для задач нуклидной кинетики требуется получение достоверных решений с гарантированной точностью для всех элементов при использовании:

1) полного набора элементов (~1800) продуктов деления с независимыми выходами;

2) матрицы (коэффициентов), сформированной на основе переходов с ветвлениями и циклами, обеспечивающими превращения нуклидов $(Z, A) \to (Z^*, A^*)$ в соответствии с распадом и реакциями (n, γ), (n, f), $(n, 2n)$, $(n, 3n)$, (n, p), (n, α) с возможностью включения дополнительных реакций (n, d), (n, t), $(n, n\,\alpha)$ и др. без изменений алгоритма решения;

3) короткоживущих и долгоживущих нуклидов с коэффициентами от $\sim 10^{-27}$ до $\sim 10^{6}$.

При такой постановке формируемая матрица коэффициентов размерности ~3000 × 3000 оказывается несимметричной с числом обусловленности $\mu(\mathbf{A})$ до 10^{27}, что приводит к принципиальным математическим сложностям получения решений. Даже применение наиболее продвинутых итерационных методов в подпространствах Крылова [7] и аппроксимации решений дробно-рациональными чебышевскими полиномами (CRAM) с коэффициентами высокой точности [8] не могут гарантировать достоверность получаемых решений. При этом ни один из существующих матричных методов не обеспечивает устойчивость решений подобных систем [9] и тем более гарантированную точность для каждой компоненты вектора решений. Метод RADAU5, реализованный в работе [10] для решения задач нуклидной кинетики, базируется на трехстадийном неявном методе Рунге—Кутты, реализованном по классическим алгоритмам без учета влияния погрешностей округления на конечный результат решения системы ОДУ. Также следует отметить, что коэффициенты метода в виде иррациональных чисел не имеют абсолютно точного представления в двоичной арифметике. Кроме того, с увеличением размера решаемых систем ОДУ возрастание влияния погрешностей округления на результаты вычислений связано с вычислительными сложностями определения числа верных значащих цифр в каждой компоненте вектора решений. Поэтому можно ожидать, что для систем ОДУ большой размерности метод RADAU5 даст достоверную траекторию компонент вектора решений, но без гарантии требуемой компьютерной точности для каждой компоненты. Под компьютерной точностью подразумевается гарантированное получение заданного числа верных значащих цифр в каждой компоненте вектора решения.

Трудности получения точного решения

С точки зрения численного интегрирования поставленная задача нуклидной кинетики имеет ряд ключевых особенностей:

- плохая обусловленность матрицы, переводящая задачу в разряд сверхжесткой для большинства основных методов численного расчета;
- отсутствие точного аналитического (контрольного) решения;
- значительный разброс коэффициентов, обусловленный спецификой используемых (ядерных) данных;
- большая размерность задачи (более 1000) и рост $\mu(\mathbf{A})$ способствуют накоплению ошибок округления при использовании численных методов, причем оба фактора действуют независимо друг от друга.

Поскольку для конкретных значений $\mu(\mathbf{A})$ и размерности задачи численная оценка применимости используемого метода весьма затруднительна, получение гарантированно точного решения принципиально важно в отсутствие контрольной тестовой задачи с точным аналитическим решением. Следует отметить, что на решение известных контрольных тестовых задач, имеющих невысокую размерность, влияние погрешностей округления незначитель-

но. Процесс получения численного решения вне зависимости от способа должен обеспечивать достоверность и компьютерную точность решения.

Для решения поставленной задачи предлагается адаптированный для решения жестких систем пакет MZK [11], в котором реализованы AL-устойчивые неявные методы с переменным шагом интегрирования и алгоритмы вычислений с гарантированной точностью [12, 13], учитывающие влияние погрешностей округления.

Методы численного решения системы ОДУ в пакете MZK

Задача нуклидной кинетики представляется системой ОДУ в общем виде $F(x, \dot{x}, t) = 0$ с начальными условиями $x(t_0) = \boldsymbol{X}_0$, что позволяет проводить ее решение пошаговыми методами. Траектория решения для каждой вычисляемой компоненты имеет не колебательный и не периодический характер.

Прямое пошаговое интегрирование исходной системы ОДУ позволяет управлять вычислительным процессом для обеспечения заданной точности, изменяя значение шага по результатам контроля точности решения на текущем шаге.

Требование достоверности решения обеспечивается использованием A- и AL-устойчивых методов интегрирования, что гарантирует устойчивость численного решения при любых значениях шага интегрирования.

Для получения количественно верного тестового контрольного решения метод интегрирования должен обладать свойством абсолютной устойчивости в области мнимых значений области устойчивости этого метода. Неявный метод Эйлера обладает этим свойством, а также свойством "фильтрования" колебательных процессов, возникающих при интегрировании из-за возможных комплексных собственных значений матрицы **A** большой размерности. При этом полученное решение оказывается достоверным для задач нуклидной кинетики и при увеличении числа шагов всегда будет стремиться к истинному решению.

Требование компьютерной точности подразумевает получение заданного числа верных десятичных знаков мантиссы для каждой компоненты вектора решения, представленного нормализованным числом. Универсальным способом контроля достоверности n верных десятичных значащих цифр является применение следующего алгоритма.

1. Интегрирование с исходными параметрами достижения точности (например, с выбранной относительной погрешностью).

2. Повторное интегрирование с более жесткими параметрами (например, с увеличенной относительной точностью).

3. Сравнение полученных результатов пп. 1 и 2 на совпадение первых n знаков во всех компонентах вектора решения и выполнение пп. 1, 2 до совпадения требуемых n десятичных знаков.

4. Для контроля отсутствия влияния на формирование n знаков результата погрешностей округления, обусловленных размерностью и (или) жесткостью системы, расчет с параметрами интегрирования п. 3 повторяется с повышенной разрядностью и последующим сравнением с результатом п. 3. При расхождении в пределах n десятичных знаков расчеты пп. 1 и 2 выполняются с повышенной разрядностью.

Важно отметить невозможность выполнения п. 4 в стандартных вычислительных пакетах из-за отсутствия в них поддержки интегрирования с повышенной разрядностью.

В подтверждение необходимости учета влияния погрешностей округления и вычислений с повышенной разрядностью для получения точного численного решения в работе [16] представлен пример вычисления числа **e:** $\exp(1) = \lim_{n\to\infty}(1 + 1/n)^n$. В табл. 1 представлены результаты расчета exp(1) при увеличении параметра точности n с одинарной точностью $6 \cdot 10^{-8}$. При возведении $(1 + 1/n)$ в степень только несколько значащих цифр от $1/n$ сохраняются в сумме, и любое последующее возведение в степень будет давать неточное приближение к значению **e**. Решение с двойной точностью дает правильный результат. Аналогичный результат будет и при увеличении числа шагов в численных методах решения систем ОДУ.

Очевидно, что минимальное влияние погрешностей округления на конечный результат дадут явные методы интегрирования, но они

Таблица 1

Численное вычисление с одинарной точностью e = 2,71828

n	exp(1)	abs(**e** − exp(1))
10^1	2,593743	$1{,}25 \cdot 10^{-1}$
10^2	2,704811	$1{,}35 \cdot 10^{-2}$
10^3	2,717051	$1{,}23 \cdot 10^{-3}$
10^4	2,718597	$3{,}15 \cdot 10^{-4}$
10^5	2,721962	$3{,}68 \cdot 10^{-3}$
10^6	2,595227	$1{,}23 \cdot 10^{-1}$
10^7	3,293968	$5{,}76 \cdot 10^{-1}$

непригодны для решения жестких систем ОДУ. Среди неявных методов интегрирования минимальное влияние погрешностей округления имеют одностадийные неявные методы Рунге—Кутты — методы Эйлера и трапеций, коэффициенты которых абсолютно точно представляются в двоичной арифметике с плавающей точкой. Для получения гарантированно точного решения задач нуклидной кинетики в пакете MZK реализован одностадийный (в реализации неявных методов Рунге—Кутты) неявный метод Эйлера с удвоенной и учетверенной точностью вычислений. В связи с этим MZK обеспечивает интегрирование с различной разрядностью вычислений, в частности, с обычной (double precision) и повышенной (quadruple precision) разрядностью, позволяющей реализовать единственно возможный способ оценки влияния на результат погрешностей округления при выполнении машинных вычислений. В пакете MATLAB интегрирование можно выполнять только с обычной разрядностью (double precision), принятой в этом пакете по умолчанию, но решение систем линейных алгебраических равнений (СЛАУ) можно выполнять и с повышенной разрядностью, что было использовано для исследования алгоритмов гарантированно точного решения СЛАУ и разработки модуля решения СЛАУ в пакете MZK.

Численное решение жестких и сверхжестких систем ОДУ неявными методами интегрирования сводится к численному решению плохо обусловленных СЛАУ на каждом шаге интегрирования, при этом уменьшение шага интегрирования уменьшает обусловленность СЛАУ, поэтому необходимо реализовать алгоритмы решения СЛАУ, которые гарантируют точное решение для максимально возможного числа обусловленности СЛАУ.

Для плохо обусловленных СЛАУ точное решение можно получить с помощью символьных вычислений, например, в MATLAB с помощью функции vpa. Недостатком такого подхода является резкое увеличение времени счета при увеличении размерности задачи. Аналогичные проблемы должны возникать и в методе RADAU5 [10] при использовании трехстадийного неявного метода Рунге—Кутты, приводящего к тройному увеличению размера решаемой СЛАУ на каждом шаге интегрирования (по сравнению с одностадийными методами) и заметно возрастающему влиянию погрешностей округления.

Наши исследования показали, что итерационное уточнение с обычной для MATLAB точностью решает эту проблему, но правая часть СЛАУ должна быть вычислена с повышенной разрядностью. Опишем алгоритм итерационного уточнения решения для СЛАУ вида $\mathbf{A}x = b$.

Пусть $X_р$ — приближенное решение, R — соответствующая невязка. В работе [17] показано, что точность решения можно существенно повысить, итерационно улучшая его следующим образом:

- вычисляем c повышенной разрядностью невязку: $R = b - AX_р$;
- вычисляем приращение dX для СЛАУ $AdX = R$;
- $X = X + dX$.

Итерационный процесс продолжается до достижения требуемой точности — относительного значения dX либо до указанного априори числа итераций.

Вычисление dX можно значительно ускорить при использовании LU-разложения матрицы **A**. Реализованный в MATLAB алгоритм обеспечивает достижение требуемой точности с помощью итерационного процесса "уточнения". Число итераций улучшения достаточно ограничить семью [18].

На тестовых задачах с известным решением оценить точность полученного результата можно, вычислив порядок относительной погрешности. Для получения точного (аналитического) решения в MATLAB использовалась функция vpa:

```
function [XA] = vpa_solver(A,B)
    digits n
    AVPA = vpa(A);
    BVPA = vpa(B);
    XVPA = vpa(X);
    XAVPA = AVPA\BVPA;
    XA = double(XAVPA);
End
```

Тестирование алгоритма решения СЛАУ

Разработанный алгоритм решения СЛАУ протестирован на задачах с плотными матрицами с максимальным размером 1000×1000. Формируется случайная матрица заданного размера с заданным числом обусловленности:

```
function A = randmatgen(logcond,n)
    [q1,~] = qr(randn(n,n));
    [q2,~] = qr(randn(n,n));
    d = diag(10.^((0:n-1)·logcond/(n-1)));
    A = q1·d·q2;
```

где *logcond* — десятичный логарифм числа обусловленности, n — размерность матрицы.

Задается вектор неизвестных, и, умножая матрицу **A** на этот вектор, получаем вектор правых частей с известным решением.

При использовании указанного алгоритма в тестовых задачах для систем ОДУ точность задавали равной 12 верных значащих цифр, что достаточно для обеспечения заданной по умолчанию точности решения систем ОДУ 10^{-3}.

На первом этапе тестирования удостоверимся в корректности получаемых результатов для различных входных данных. Было сгенерировано 200 случайных матриц разных порядков (не выше 20) с числом обусловленности 10^{12}. Для всех этих матриц указанный алгоритм обеспечил верные результаты уже при двух итерациях уточнения.

На втором этапе исследовали зависимость числа итераций уточнения от размера матрицы. Зависимость оказалась достаточно слабой: для матриц до 616 × 616 требуется две итерации уточнения, от 616 × 616 до 1000 × 1000 требуется три итерации (параметры vpa установлены по умолчанию).

Также исследовали зависимость времени счета от размера матрицы. Результаты при использовании MZK и функции vpa приведены на рис. 1. Требуемая точность достигалась в обоих случаях.

Исследовали зависимость числа итераций уточнения от числа обусловленности $\mu(\mathbf{A})$ для матрицы 10 × 10 (табл. 2).

Отметим, что поскольку для $\mu(\mathbf{A}) > 8$ потребовались итерации уточнения, то для MATLAB с обычной точностью (без уточнений и без функции vpa) достижение требуемой точности оказывается невозможным, и при $n > 7$ гарантия точности решения отсутствует.

Таким образом, для гарантированно точного решения СЛАУ с приемлемыми затратами счета следует использовать алгоритм итерационного уточнения с вычислением правой части с повышенной разрядностью, что особенно актуально для задач высокой размерности с разреженными матрицами. Этот алгоритм реализован в пакете MZK в качестве основы для решения систем ОДУ с гарантированной точностью.

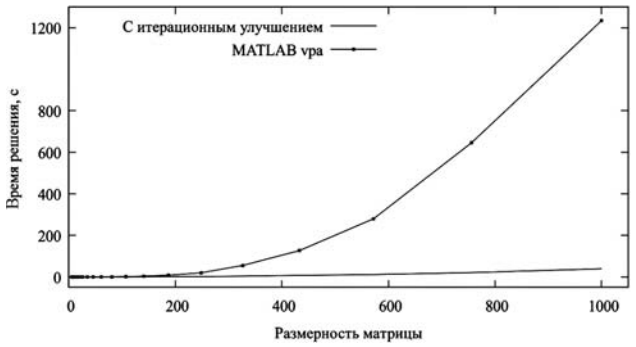

Рис. 1. Зависимость времени решения СЛАУ от размерности задачи

Таблица 2

Зависимость числа итераций уточнения *n* от μ(A)

μ(**A**)	8	9	10	11	12	13	14	15	16	17
n(μ)	0	1	1	2	2	2	3	5	6	> 7

Получение эталонного решения с помощью пакета MZK

При использовании пакета MZK единственным задаваемым параметром интегрирования является относительная точность, указывающая точность вычисления для каждой компоненты вектора решения на текущем шаге интегрирования с контролем точности.

Традиционно в математических пакетах при интегрировании задаются два параметра — относительная (*RelTol*) и абсолютная (*AbsTol*) погрешности. При этом значение *AbsTol* выбирается эмпирическим путем и, как правило, задается на несколько порядков меньше *RelTol*, например, в MATLAB по умолчанию рекомендованы $RelTol = 10^{-3}$, $AbsTol = 10^{-6}$. Из полученных решений (рис. 2—4) видно, что результат интегрирования методом ode15s в MATLAB, позиционируемым для решения жестких систем, оказывается достаточно чувствительным к выбору *AbsTol*.

С помощью пакета MZK траектория тестового контрольного решения была получена интегрированием ОДУ неявным методом Эйлера для double precision с последующим контрольным расчетом с повышенной точностью quadruple precision. Относительная точность задавалась равной $\varepsilon = 10^{-3}$ (аналог *RelTol*),

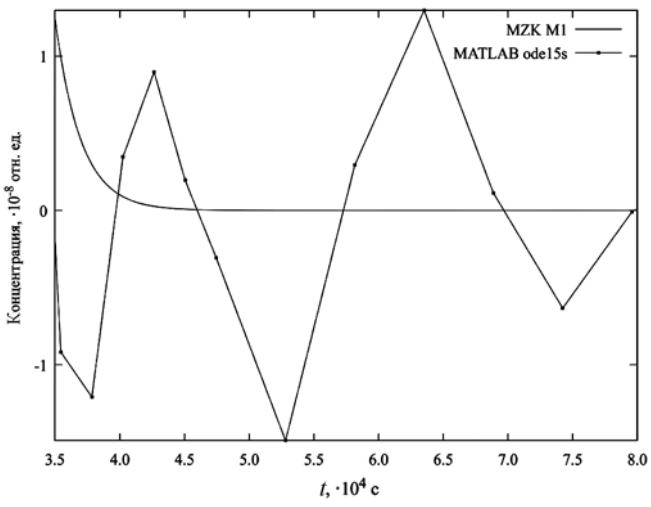

Рис. 2. Ложные колебания траектории решения в MATLAB методом ode15s для $RelTol = 10^{-3}$, $AbsTol = 10^{-6}$

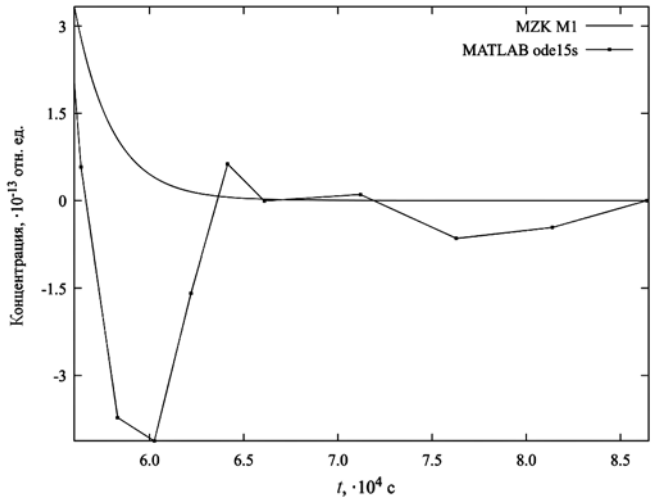

Рис. 3. Ложные колебания траектории решения в MATLAB методом ode15s для *RelTol* = 10^{-3}, *AbsTol* = 10^{-12}

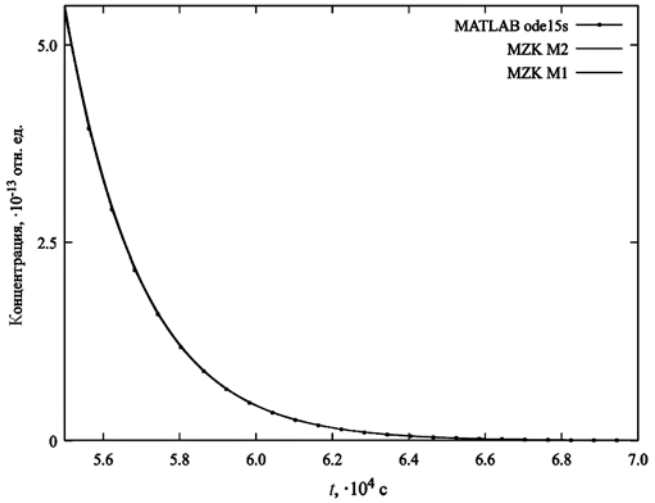

Рис. 4. Отсутствие ложных колебаний траектории решения в MATLAB методом ode15s для *RelTol* = 10^{-3}, *AbsTol* = 10^{-100}

что подразумевает получение как минимум двух достоверных десятичных знаков мантиссы в нормализованном представлении каждой компоненты вектора решения.

При возмущении элементов матрицы от 5 до 20 % интегрирование неявным методом Эйлера обеспечивает линейность возмущения, а также устойчивость решения с более заполненной матрицей. Контроль совпадения значений проводился для компонент вектора решения, не превышающих значений 10^{-25}.

Повышение порядка используемого метода обусловливает возрастание влияния погрешностей округления на конечный результат, что требует дополнительных исследований и анализа, выходящих за рамки статьи.

Следует отметить, что применение неявных методов высокого порядка точности позволяет при равной относительной точности достигать значительной экономии времени интегрирования за счет увеличения шага интегрирования. Так, метод второго порядка показал уменьшение времени интегрирования приблизительно в 3,5 раза по сравнению с методом первого порядка.

Получение решения с помощью MATLAB, анализ результатов

Для тестовой задачи с матрицей 1779 × 1779 и $\mu(A) \sim 10^{27}$ с помощью пакета MZK, в котором реализованы AL-устойчивые неявные методы M1, M2 и M4 [12], методом M1 (неявный метод Эйлера) получено точное решение для относительной точности $\varepsilon = 10^{-3}$. Точность решения была проверена с помощью вычислений в quadruple и double precision. В табл. 3 и 4 представлены значения отдельных компонент вектора численного решения ОДУ с матрицей 1779 × 1779, вычисленные с обычной и повышенной разрядностью.

Совпадающие в решениях значащие цифры (табл. 3) можно признать верными. Совпадающие во всех трех методах цифры (табл. 4) можно считать гарантированно верными (минимальное значение в последней колонке).

Таблица 3

Определение верных значащих цифр мантиссы нормализованных чисел результатов при вычислении с повышенной разрядностью ($\varepsilon = 10^{-3}$)

Компонента	Начальное значение, отн. ед.	Конечное значение, отн. ед.		Число верных значащих цифр
		Разрядность		
		Double (64 бит)	Quadruple (128 бит)	
56	0	$9{,}6208352 \cdot 10^{-12}$	$9{,}6208301 \cdot 10^{-12}$	6
82	8,5291	8,528585083555638	8,528585083556097	12
88	0	$4{,}28207 \cdot 10^{-15}$	$4{,}28210 \cdot 10^{-15}$	4
102	0,012503	0,012504453607224	0,012504453607233	12
306	0	$5{,}369878 \cdot 10^{-55}$	$5{,}370170 \cdot 10^{-55}$	2

Таблица 4

Определение верных значащих цифр при вычислении разными методами пакета MZK (quadruple precision)

Компонента	Метод			Число верных значащих цифр
	M1 $\varepsilon = 1\cdot10^{-3}$; $h_0 = 1\cdot10^{-12}$	M2 $\varepsilon = 1\cdot10^{-3}$; $h_0 = 1\cdot10^{-10}$	M2 $\varepsilon = 1\cdot10^{-5}$; $h_0 = 1\cdot10^{-10}$	M1 и M2 ($\varepsilon = 1\cdot10^{-3}$)/ M2 ($\varepsilon = 1\cdot10^{-3}$ и $\varepsilon = 1\cdot10^{-5}$)
56	$9{,}621150\cdot10^{-12}$	$9{,}621896\cdot10^{-12}$	$9{,}621895\cdot10^{-12}$	4/6
78	4,856970853893407	4,856970853765135	4,856970853765135	10/16
82	8,528585083553850	8,528585083548615	8,528585083548615	11/16
88	$4{,}280472\cdot10^{-15}$	$4{,}276675\cdot10^{-15}$	$4{,}276673\cdot10^{-15}$	2/6
100	3,148138326	3,148138314140	3,1481383141432	8/12
101	0,15507764376	0,155077643776481	0,155077643776483	9/14
102	$1{,}2504453606\cdot10^{-2}$	$1{,}250445360553e\cdot10^{-2}$	$1{,}250445360553\cdot10^{-2}$	10/16
306	$5{,}351\cdot10^{-55}$	$5{,}30947\cdot10^{-55}$	$5{,}30932\cdot10^{-55}$	2/4

Решение задачи размерности 2491 × 2491 методом переменного порядка точности ode15s в MATLAB приводит к ложным колебаниям вычисляемых значений для отдельных компонент вектора решений (см. рис. 2, 3). При существенном уменьшении значения *AbsTol,* например до 10^{-100}, наблюдается совпадение результатов в MATLAB и MZK (рис. 4).

Заключение и выводы

- Прецизионные методы решения задач нуклидной кинетики ориентированы на максимально полное использование современных библиотек ядерных данных и обеспечение устойчивых решений на разных временных сетках. Объективная сложность получения экспериментальных данных и аналитических решений для большей части нуклидов требует применения вычислительных методов с гарантированной точностью решения для всех элементов.
- При решении жестких систем ОДУ большой и сверхбольшой размерности следует учитывать влияние погрешностей округления на достоверность и точность получения конечного результата вычислений.
- Для гарантированно точного решения СЛАУ с приемлемыми затратами счета следует использовать алгоритм итерационного уточнения с вычислением правой части с повышенной разрядностью. Это особенно актуально для задач большой размерности с разреженными матрицами.
- Для получения гарантированно точного решения систем ОДУ в задачах нуклидной кинетики используется одностадийный неявный метод Эйлера с представленным алгоритмом решения СЛАУ, реализованным в пакете MZK с удвоенной и повышенной точностью вычислений. Полученное гарантированно точное решение следует использовать для настройки параметров неявных методов высокого порядка точности для решения систем ОДУ большой размерности.
- Пакет MZK, обеспечивающий достоверные решения с гарантированной точностью для всех вычисляемых нуклидов, может применяться для получения реперных значений в прецизионных расчетах задач нуклидной кинетики.

Список литературы

1. **Isotalo A. E., Aarnio P. A.** Comparison of depletion algorithms for large systems of nuclides // Ann. Nucl. Energy. 2011.Vol. 38. P. 261—268.
2. **Cetnar J.** General Solution of Bateman Equations for Nuclear Transmutations // Ann. Nucl. Energy. 2006. Vol. 33. P. 640—645.
3. **Митенкова Е. Ф., Новиков Н. В., Соловьева Е. В.** Библиотеки с расширенным представлением выхода продуктов деления в расчетах нуклидного состава топлива в быстром спектре // Атомная энергия. 2014. Т. 117, Вып. 6. С. 341—346.
4. **Mitenkova E. F., Novikov N. V.** Effect of fission yield libraries on the irradiated fuel composition in Monte Carlo depletion calculations // Proceedings of the 7-th Workshop Nuclear Measurements, Evaluations and Applications (NEMEA-7). 5—8 November 2013. Geel, Belgium, OECD 2014. P. 287—296.
5. **Bell M. J.** Origen: The ORNL Isotope Depletion and Generation Code. ORNL-4628. 1973.
6. **Митенкова Е. Ф., Соловьева Е. В.** Вычислительные ограничения программы ORIGEN2 в задачах нуклидной кинетики. М: ИБРАЭ РАН, 2019. 31 с.
7. **Yamamoto A., Tatsumi M., Sugimura N.** Numerical Solution of Stiff Burnup Equation with Short Half Lived Nuclides by the Krylov Subspace Method // J. Nucl. Sci. Technol. 2007. Vol. 44. P. 147—154.
8. **Pusa M., Leppänen J.** Computing the Matrix Exponential in Burnup Calculations // Nucl. Sci. Eng. 2010. Vol. 164. P. 140—150.
9. **Moler C., C. van Loan.** Nineteen Dubious Ways to Compute the Exponential of a Matrix, Twenty-Five Years Later // SIAM Rev. 2003.Vol. 45, N. 1. P. 3—49.

10. **Stankovskiy A., Van den Eynde, Advanced G.** Method for Calculations of Core Burn-Up, Activation of Structural Materials, and Spallation Products Accumulation in Accelerator-Driven Systems // Sci. Technol. Nucl. Install. Article. 2012. ID 545103. 12 p.

11. **Маничев В. Б., Жук Д. М.** Базовый набор тестовых задач для решателей систем ОДУ // Технологии инженерных и информационных систем. 2016. Т. 2, № 4. С. 70—84.

12. **Маничев В. Б., Митенкова Е. Ф., Жук Д. М., Кожевников Д. Ю., Соловьев А. В., Соловьева Е. В.** Использование AL-устойчивых методов решения систем ОДУ для задач изотопной кинетики реакторных систем // Информационные технологии. 2017. Т. 23, № 3. С. 177—183.

13. **Митенкова Е. Ф., Соловьева Е. В., Маничев В. Б., Фельдман Э. О.** Задачи изотопной кинетики на полном базисе выхода продуктов деления // Атомная Энергия. 2018. Т. 124, Вып. 1. С. 54—57.

14. **Shampine L. F., Reichelt M. W.** The MATLAB ODE Suite // SIAM Journal on Scientific Computing. 1997. Vol. 18. P. 1—22.

15. **MATLAB.** URL: https://ch.mathworks.com/help/matlab/index.html 01.09.2019).

16. **Higham N. J.** Accuracy and stability of numerical algorithms. SIAM: Society for Industrial and Applied Mathematics, 2nd ed., 2002. 680 p.

17. **Уоткинс Д.** Основы матричных вычислений. М.: Бином, 2006. 664 с.

18. **Manichev V., Zhuk D., Feldman E.** The basic set of test problems for ODE system solvers // ICMSC 2019. St. Petersburg, Russia. June 21—23 2019 (в печати).

V. B. Manichev[1], Associate Professor, e-mail: manichev@bmstu.ru, **E. F. Mitenkova**[2], Head Laboratory,
E. O. Feldman, Bachelor, **D. Ju. Kozhevnikov**[1], Lead Engineer,
E. V. Solovjeva[2], Researcher, e-mail: sol@ibrae.ac.ru,
[1] Bauman Moscow State Technical University, Moscow, 105005, Russian Federation,
[2] Nuclear Safety Institute of the Russian Academy of Sciences, Moscow, 115191, Russian Federation

Reliability and Calculation Accuracy of Nuclide Kinetics Problems

The current requirements in development of new generation reactors initiate the improvement of calculation base, including increasing the accuracy of solving nuclide kinetics problems. It is shown that when solving the stiff high dimensionality ODE systems the influence of rounding errors on the reliability and accuracy of final calculation results should be taken into account. For guaranteed accurate SLAE solution with reasonable calculation costs, an iterative refinement algorithm should be used with the calculation of the right-hand side with increased digit capacity. It's especial actual when using the most full nuclear data base because of objective complexity to obtain analytical solutions and experimental data for most nuclides of irradiated fuel. To obtain a solution with a guaranteed reliability and accuracy for all elements of high dimensionality ODE system, the MZK package implements the one-stage implicit Euler method with the described algorithm for solving LAE systems with double and increased computational accuracy. The results confirm the possibility to use the MZK package to obtain reference values in precision calculations of nuclide kinetics problems.

Keywords*: mathematical modelling, ordinary differential equation (ODE), linear algebraic equations (LAE), stiff systems, guaranteed accuracy, nuclide kinetics, rounding error*

DOI: 10.17587/it.26.231-238

References

1. **Isotalo A. E., Aarnio P. A.** Comparison of depletion algorithms for large systems of nuclides, *Ann. Nucl. Energy*, 2011, vol.38, pp. 261—268.

2. **Cetnar J.** General Solution of Bateman Equations for Nuclear Transmutations, *Ann. Nucl. Energy*, 2006, vol. 33, pp. 640—645.

3. **Mitenkova E. F., Novikov N. V., Solovjeva E. V.** Biblioteki s rasshirennym predstavleniem vyhoda produktov deleniya v raschetah nuklidnogo sostava topliva v bystrom spektre, *Atomnaya Energiya*, 2014, vol. 117, iss. 6, pp. 341—346.

4. **Mitenkova E. F., Novikov N. V.** Effect of fission yield libraries on the irradiated fuel composition in Monte Carlo depletion calculations, *Proceedings of the 7-th Workshop Nuclear Measurements, Evaluations and Applications (NEMEA-7)*, 5—8 November 2013, Geel, Belgium, OECD 2014, pp. 287—296.

5. **Bell M. J.** Origen: The ORNL Isotope Depletion and Generation Code, ORNL-4628, 1973.

6. **Mitenkova E. F., Solovjeva E. V.** Vychislitel'nye ogranicheniya programmy ORIGEN2 v zadachah nuklidnoj kinetiki, Moscow, Publishing house of IBRAE RAN, 2019, 31 p.

7. **Yamamoto A., Tatsumi M., Sugimura N.** Numerical Solution of Stiff Burnup Equation with Short Half Lived Nuclides by the Krylov Subspace Method, *J. Nucl. Sci. Technol.,* 2007, vol. 44, pp. 147—154.

8. **Pusa M., Leppänen J.** Computing the Matrix Exponential in Burnup Calculations, *Nucl. Sci. Eng.,* 2010, vol. 164, pp. 140—150.

9. **Moler C., C. van Loan.** Nineteen Dubious Ways to Compute the Exponential of a Matrix, Twenty-Five Years Later, *SIAM Rev.,* 2003, vol. 45, no. 1. pp. 3—49.

10. **Stankovskiy A., Van den Eynde, Advanced G.** Method for Calculations of Core Burn-Up, Activation of Structural Materials, and Spallation Products Accumulation in Accelerator-Driven Systems, *Sci. Technol. Nucl. Install. Article*, 2012, ID 545103, 12 p.

11. **Manichev V. B., Zhuk D. M.** Bazovyj nabor testovyh zadach dlya reshatelej sistem ODU, *Tekhnologii Inzhenernyh i Informacionnyh Sistem,* 2016, vol. 2, no. 4, pp. 70—84.

12. **Manichev V. B., Mitenkova E. F., Zhuk D. M., Kozhevnikov D. Yu., Solovjev A. V., Solovjeva E. V.** Ispol'zovanie AL-ustojchivyh metodov resheniya sistem ODU dlya zadach izotopnoj kinetiki reaktornyh sistem, *Informacionnye Tekhnologii*, 2017, vol. 23, no. 3, pp. 177—183.

13. **Mitenkova E. F., Solovjeva E. V., Manichev V. B., Fel'dman E. O.** Zadachi izotopnoj kinetiki na polnom bazise vyhoda produktov deleniya, *Atomnaya Energiya*, 2018, vol. 124, iss. 1, pp. 54—57.

14. **Shampine L. F., Reichelt M. W.** The MATLAB ODE Suite, *SIAM Journal on Scientific Computing*, 1997, vol. 18, pp. 1—22.

15. **MATLAB,** available at: https://ch.mathworks.com/help/matlab/index.html 01.11.2019.

16. **Higham Nicholas J.** Accuracy and stability of numerical algorithms, SIAM, 2002, 680 p.

17. **Uotkins D.** Osnovy matrichnyh vychislenij, Moscow, Binom, 2006, 664 p.

18. **Manichev V., Zhuk D., Feldman E.** The basic set of test problems for ODE system solvers, *ICMSC 2019.* St. Petersburg, Russia. June 21—23 2019 (in print).

УДК 004.83 + 005.8 DOI: 10.17587/it.26.239-251

А. И. Малахова, канд. техн. наук, доц., e-mail: aimalakhova@gmail.com,
Н. О. Никулина, канд. техн. наук, доц., e-mail: nikulinano@outlook.com,
Л. Р. Черняховская, д-р техн. наук, проф., e-mail: lrchern@yandex.ru,
Уфимский государственный авиационный технический университет, г. Уфа

Исследование содержания проблемы управления инновационными проектами в процессах стратегического планирования и развития производственно-экономических систем[1]

Успешное функционирование производственно-экономических систем возможно только в случае пристального внимания лиц, принимающих решения, к вопросам стратегического планирования как деятельности предприятия в целом, так и инновационных проектов различного вида, выполняемых в рамках производственно-экономических систем. Реализация инновационных проектов должна быть построена на принципах проектного менеджмента с привлечением методов и средств инженерии знаний для всесторонней оценки и анализа всей имеющейся информации о состоянии проекта на любом этапе жизненного цикла в целях принятия обоснованных решений в различных областях знаний. Эффективность управления инновационными проектами во многом определяется качеством принимаемых управленческих решений, которые осуществляются в условиях недостаточности данных и ресурсов, неопределенности последствий принимаемых решений, нестабильности внешних условий, недостаточно эффективного информационного взаимодействия управляющих проектом с той или иной стороны при наличии различных критериев выбора альтернатив. Уменьшение влияния вышеуказанных факторов неопределенности может быть достигнуто за счет использования формализованного подхода к управлению проектом на основе рекомендаций стандартов проектного менеджмента в совокупности с оказанием интеллектуальной поддержки принятия решений для участников проекта.

Ключевые слова: *управление инновационными проектами, производственно-экономическая система, проблемная ситуация, инженерия знаний, интеллектуальная поддержка принятия решений, интегрированная онтология, база знаний*

Введение

Понятие "инновации" подразумевает внедрение в производственный процесс достижений научно-технического прогресса, вовлечение научных коллективов и высококвалифицированных кадров в формирование высокотехнологичной продукции отечественных предприятий. При этом понятие "инновации" в литературе трактуется очень широко: от объекта — результата какой-либо уникальной творческой деятельности, до процесса, преобразующего идеи в реализуемый на рынке продукт. Так, в работе [1] приведены следующие виды инновационной деятельности: продуктовые, процессные, организационные, маркетинговые инновации. Различные виды инновационной деятельности могут быть сопоставлены с типами экономических объектов (предприятий, организаций), в которых они реализуются. Инновационная деятельность в разных странах регулируется в соответствии с национальным законодательством, кроме того, существует целый ряд международных неправительственных организаций, например, Организация экономического сотрудничества и развития, разрабатывающих методические рекомендации по внедрению инноваций.

В Российской Федерации сфера науки, технологии и инновации сегодня регламентиру-

[1] Работа выполнена при финансовой поддержке гранта Российского фонда фундаментальных исследований № 18-00-00345 (18-00-00238) "Методы и модели поддержки принятия решений при управлении инновационными проектами на основе инженерии знаний".

ется Федеральным законом № 127 "О науке и государственной научно-технической политике", принятым еще в 1996 г. Жизнь не стоит на месте, тем более в сфере высоких наукоемких технологий, меняется политическая и экономическая ситуация в стране и в мире, поэтому за истекшие более чем два десятка лет в этот закон были приняты более двадцати поправок, делались попытки принятия новых федеральных законов об инновационной деятельности. Вот только небольшая часть истории законотворческой деятельности в области регулирования сферы инноваций:

- проект Федерального закона "Об инновационной деятельности и о государственной инновационной политике" разработан в 1999 г. — отклонен Президентом РФ в 2000 г.;
- проект Федерального закона "Об инновационной деятельности в Российской Федерации" разработан в 2010 г., внесен на рассмотрение в Государственную Думу РФ 05.10.2010 г. — отклонен;
- проект Федерального закона "О государственной поддержке инновационной деятельности в Российской Федерации" разработан в 2011 г., внесен на рассмотрение в Государственную Думу РФ 22.11.2017 г. — отклонен;
- проект Федерального закона "О научной, научно-технической и инновационной деятельности в Российской Федерации" — разработан в марте 2018 г., пока не внесен на рассмотрение в Государственную Думу РФ [2].

На текущий момент Российская Федерация ставит перед собой цели долгосрочного развития, заключающиеся в обеспечении высокого уровня благосостояния населения и закреплении геополитической роли страны как одного из лидеров, определяющих мировую политическую повестку дня. Единственным возможным способом достижения этих целей является переход экономики на инновационную социально ориентированную модель развития [3].

Последовательная и устойчивая активизация инновационных процессов в производственно-экономических системах необходима для повышения конкурентоспособности предприятий, усиления конкурентной борьбы за высококвалифицированные кадры и для привлечения инвестиций, несущих в проекты новые знания и технологии.

В этих условиях государство целенаправленно принимает меры, способствующие развитию приоритетных направлений науки и техники. К таким направлениям относятся, в том числе, информационно-телекоммуникационные системы, энергоэффективность и энергосбережение, перспективные виды вооружения, военной и специальной техники [4]. Возникает необходимость опережающего развития специфичных научных исследований и разработок, включая экологически чистую энергетику, геномную медицину, новые технологии в сельском хозяйстве.

Согласно указанной Стратегии повышение инновационного потенциала страны играет одну из ключевых ролей для обеспечения безопасности государства и повышения его конкурентоспособности в мировом масштабе. При этом инновационное развитие по стране в целом и по отдельным регионам происходит неравномерно, что связано со специфическими особенностями регионов, в частности, со структурой промышленного производства, демографией, наличием наукоемких отраслей, уровнем социально-экономического развития и т.д.

1. Состояние инновационного развития Российской Федерации и Республики Башкортостан

Одной из причин, осложнивших реализацию инновационных проектов в стране, явился мировой экономический кризис 2008—2009 гг., который в целом замедлил развитие экономической системы страны, в том числе и его инновационной составляющей. Несмотря на все предпринимаемые усилия по результатам оценки совокупного уровня инновационной активности за 2016 г. Россия с 8,4 % занимает крайне слабую позицию среди других развитых стран — лидеров в данной сфере (например, Швейцария имеет совокупный показатель инновационной активности 75,3 %).

По данным Росстата за период с 2011 по 2018 г. показатели внутренних затрат на исследования и разработки в процентах от валового внутреннего продукта и совокупного уровня инновационной активности организаций промышленного производства остаются практически неизменными, а в некоторые периоды даже снижаются (рис. 1) [5].

По результатам отраслевого анализа динамики основных показателей инновационной деятельности можно сделать вывод, что наибольшей инновационной активностью обладают промышленные предприятия (9,2 %), в том числе предприятия энергетики (4,1 %) [6], причем чем больше масштаб самой организации, тем больше совокупный уровень ее инновационной активности.

Рис. 1. Целевые индикаторы реализации стратегии инновационного развития Российской Федерации

Результаты отраслевого анализа реализации инноваций в Республике Башкортостан (РБ) как по объемам финансирования проектов, так и по их совокупной численности подтверждают общую картину по стране — наибольшей инновационной активностью в регионе обладают промышленные предприятия (рис. 2). Наибольшее число инновационных проектов наблюдается в столице — г. Уфе, где сконцентрировано подавляющее большинство вузов и ведущих промышленных предприятий РБ.

На данный момент одной из главных проблем является низкий спрос российских производственных предприятий на инновации, часто руководство предприятий стремится закупить готовое оборудование или технологии (в том числе за рубежом), нежели вкладывать средства в развитие собственных разработок. Такой подход объясняется желанием получить быстрый возврат инвестиций за счет внедрения зарекомендовавших себя на рынке решений. Кроме того, процедуры закупки хорошо известны и не вызывают затруднений с точки зрения принятия решений, если финансовых и иных ресурсов достаточно для заключения договоров поставки. Внедрение же инноваций требует гораздо больших усилий и со стороны предприятия, и со стороны возможных инвесторов при высокой степени неопределенности при получении ожидаемого результата. Неопределенность касается не только качества и стоимости конечного инновационного продукта, но и сроков его получения. Поэтому ни частный, ни государственный сектор не проявляют достаточного интереса к внедрению инноваций. При этом для поддержки инновационной деятельности в свое время корректировались статьи Бюджетного и Налогового кодексов, благодаря чему было снижено бремя налоговой нагрузки на инновационные предприятия. Таким образом, к факторам, тормозящим развитие инноваций, можно отнести:

- нехватку собственных денежных средств компаний при высокой стоимости нововведений;
- сложность привлечения инвестиций;
- незнание методов инновационного проектирования;
- сложные схемы оценки перспектив внедрения инноваций;
- сложность определения экономического эффекта от использования интеллектуальной собственности.

Тем не менее, несмотря на все сложности инновационная деятельность открывает для предприятий путь к повышению конкурентоспособности, вопросы обретения которой для большинства производственных предприятий стоят сегодня как никогда остро. При этом основной целью иногда является не столько увеличение доли присутствия на рынке или повышение размера чистой прибыли, а элементарное сохранение рабочих мест и выживание в непростых условиях. Ни одно современное предприятие, вне зависимости от сферы деятельности и масштаба бизнеса, не может быть абсолютно уверенным в незыблемости своих позиций на рынке даже в ближайшей перспективе. Давно прошли те времена, когда организационные и производственные процессы выполнялись в неизменном виде годами, одни и те же сотрудники годами занимали свои рабочие места, а руководители разных рангов принимали решения, придерживаясь, казалось бы, раз и навсегда установленных правил, описанных в хорошо изученных инструкциях. Практически не

Рис. 2. Отраслевой анализ инновационной активности в РБ

менялось и внешнее окружение предприятия — одни и те же контрагенты с хорошо изученными потребностями, отработанные технологии взаимодействия с партнерами, неизменные вышестоящие управляющие структуры. В этих условиях можно было строить планы стратегического развития на 10...15 лет вперед.

Все изменилось после политического и экономического переустройства жизни российского общества, совпавшего с началом информационного века. Разрыв экономических и политических связей, ломка привычных схем взаимодействия, чехарда в законотворческой деятельности, падение курса национальной валюты сделали невозможным существование предприятий, не готовых быстро адаптироваться к изменениям. Положение усугубило введение международных санкций, ограничивающих сотрудничество с зарубежными предприятиями и использование "импортных" технологий и изделий. Горизонт стратегического планирования сильно приблизился и составлял не более 3...5 лет. К тому же не секрет, что смена владельцев бизнеса (особенно среднего и малого) в России в последние 20 лет — достаточно частое явление, что тоже не способствует активному ведению инновационной деятельности в рамках одного предприятия. Производственное предприятие для обеспечения своего устойчивого положения и дальнейшего перспективного развития должно трансформироваться в производственно-экономическую систему [7]. В этих условиях особо важное значение приобретает владение актуальной и достоверной информацией как о состоянии всех элементов производственно-экономической системы, так и о событиях, происходящих во внешней по отношению к ней среде и влияющих на достижение запланированных целей.

И здесь свою роль сыграло бурное развитие информационных и коммуникационных технологий, предоставивших дальновидным руководителям предприятий возможность использовать инструменты, позволяющие принимать обоснованные решения по управлению предприятием. К таким инструментам относятся и автоматизированные системы управления бизнес-процессами, и системы электронного документооборота, и корпоративные информационные системы. Но применение этих инструментов бессистемно при отсутствии продуманной стратегии развития предприятия не может дать серьезного экономического эффекта. В этих условиях применение инструментов управления производственно-экономической системой через реализацию инновационных проектов различной направленности может дать весьма ощутимые результаты.

2. Принципы и проблемы управления инновационными проектами в производственно-экономических системах

Инновационная активность производственно-экономической системы характеризует степень участия предприятия в осуществлении инновационной деятельности в целом или отдельных ее видов в течение определенного периода времени. На сегодняшний момент инновационная деятельность предприятий и организаций в основном осуществляется в рамках реализуемых ими проектов, поэтому к проводимым инновациям могут быть применены известные методы и подходы проектного менеджмента.

Управление проектами за долгие годы оформилось в отдельную масштабную дисциплину. Сегодня невозможно представить основную деятельность компаний без реализаций проектной, управленческую деятельность — без применения средств проектного управления. За все время развития проектного менеджмента прилагались объединенные усилия по составлению сводов знаний, которые содержали бы в себе рекомендации по управлению проектами на основе накопленного опыта специалистов в данной области. Две наиболее известные версии таких сводов были разработаны и опубликованы Институтом управления проектами (Project Management Institute, PMI: the PMBOK Guide, 2000) в Соединенных Штатах и Ассоциацией управления проектами (Association of Project Management, APM, 2000) в Великобритании. Использование PMBOK Guide (A Guide to the Project Management Body of Knowledge (PMBoK) — Свод знаний по управлению проектами) в Соединенных Штатах в качестве национального стандарта (ANSI, PMI 99-001-200) было одобрено Американским национальным институтом стандартизации (American National Standards Institute, ANSI) [8]. В России с учетом национальных особенностей ведения проектной деятельности осуществляется активная разработка собственных взаимосвязанных стандартов управления проектами на основе PMBoK [9].

Появление новых сфер деятельности, связанных с цифровыми технологиями, сетевой экономикой и другими современными методами организации бизнеса и производства, за-

ставляет по-новому взглянуть на классификацию проектов, предлагаемую в известных научно-методических источниках [10, 11], включив в нее класс инновационных проектов. В соответствии с Законом об инновационной деятельности РБ, "инновационный проект — комплекс направленных на достижение экономического эффекта мероприятий по осуществлению инноваций, в том числе по коммерциализации научных и (или) научно-технических результатов" [12]. Инновации могут затрагивать различные сферы деятельности, поэтому результаты инновационных проектов могут представлять ценность как для внешних потребителей (продукты и услуги), так и для внутренних подразделений предприятия (например, новые методы и технологии выполнения работ, новые организационные подходы к управлению предприятием и т.д.) (рис. 3).

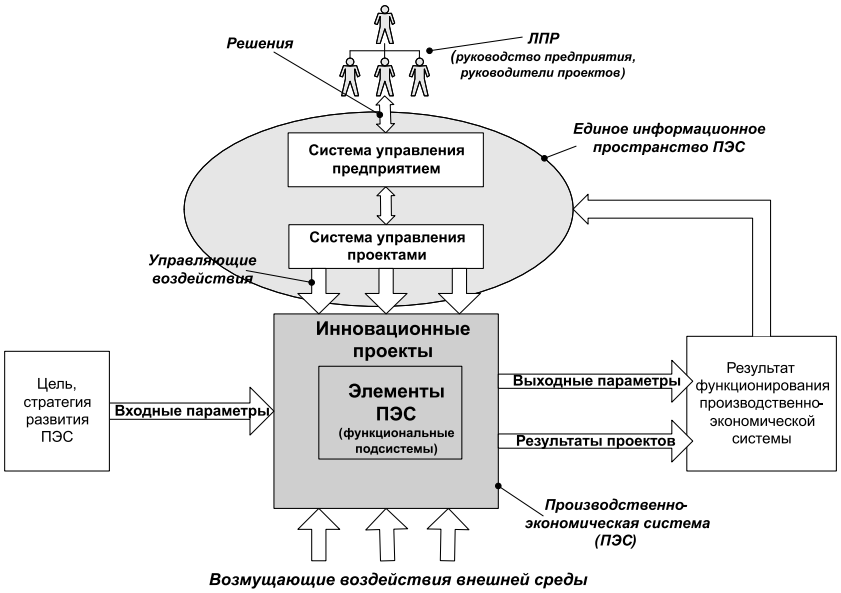

Рис. 3. Управление инновационным проектом в рамках производственно-экономической системы

Все составные части производственно-экономической системы должны функционировать в едином информационном пространстве, которое обеспечивают информационно-управляющие системы (такие как 1С: Управление производственным предприятием, 1С: ERP 2.0, SAP ERP и т.д.), предоставляющие лицам, принимающим решения (ЛПР), информацию о ходе производственно-хозяйственной деятельности.

В этом же пространстве находятся и системы управления проектами, представляющие собой либо обособленные системы (Primavera, Microsoft Project, Power Project и т.д.), так или иначе взаимодействующие с информационно-управляющими системами, либо интегрированные в систему управления предприятием в виде ее отдельного модуля.

Выполнение инновационных проектов немыслимо без привлечения высококвалифицированных, высокоинтеллектуальных участников, обладающих глубокими познаниями не только в предметной области, где выполняется проект, но и в области организационного, процессного и проектного управления [13, 14]. Это связано с тем, что инновационные проекты требуют к себе повышенного внимания со стороны руководства предприятия, поскольку они несут в себе бóльшие риски от невозврата инвестиций, нежели другие реализуемые проекты. Но даже наличие таких людей в команде проекта еще не гарантирует его успешного завершения.

Повышению эффективности управления инновационными проектами способствует изучение и применение на практике Свода знаний по управлению проектами [15], в котором определены различные аспекты управления проектами, в частности, разновидности жизненных циклов управления проектами и сопутствующие им процессы.

Авторы предлагают для каждой стадии жизненного цикла проекта определять перечень ЛПР для оказания адресной информационной поддержки в проблемных ситуациях. На ранних стадиях жизненного цикла, как правило, решения принимаются коллективно, что связано с широким кругом обсуждаемых вопросов, влияющих на судьбу проекта (рис. 4). На стадии исполнения планы воплощаются в результаты, за которые несут ответственность конкретные исполнители, принимающие решения согласно своей компетенции, навыкам и знаниям. Стадия завершения проекта предполагает, помимо административных процедур закрытия договоров и написания отчетов, обязательную фиксацию полученных знаний, что также делает необходимым взаимодействие ЛПР, а также привлечение инженеров знаний.

Чрезвычайно важную роль в управлении инновационным проектом играет предынвестиционная стадия жизненного цикла (рис. 5).

Анализ положения дел показал, что доля финансирования инновационных проектов предприятий государством либо из имеющих-

Рис. 4. Обобщенная модель управления инновационным проектом

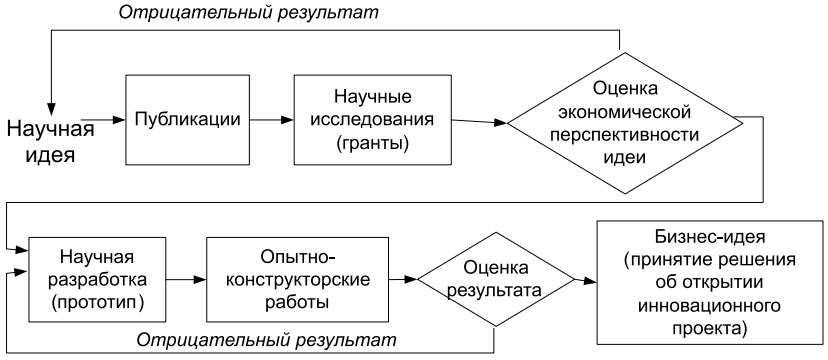

Рис. 5. Схема прединвестиционной стадии инновационного проекта

ся внешних источников остается крайне малой. В связи с этим предприятия при осуществлении инновационных проектов несут высокие риски невозврата именно собственных вложенных средств, что напрямую влияет на качество работы предприятия в целом. Отсюда следует, что особое внимание нужно уделять всестороннему анализу возможных проблем, с которыми могут столкнуться ЛПР при управлении инновационным проектом.

Как показывает практика, именно на этой стадии из-за недостатка сведений о различных аспектах реализации проекта в одной или нескольких областях знаний чаще всего и заканчивается его жизненный цикл.

3. Решение проблем управления инновационными проектами через организацию интеллектуальной поддержки принятия решений на основе инженерии знаний

Для повышения эффективности выполнения проектов разработаны и успешно применяются в различном сочетании множество решений — от основополагающих методов проектного менеджмента до методов математического моделирования и принятия решений.

Повсеместное признание, которое завоевывает управление проектами, является показателем того, что применение соответствующих знаний, процессов, навыков, инструментов и методов может иметь решающее значение для успеха проекта. Тем не менее хорошо извест-

на статистика выполнения проектов, которая в различных предметных областях имеет схожие результаты — около половины всех проектов заканчивается в срок, с заданным качеством и в рамках согласованного бюджета, у остальных проектов либо есть отдельные недостатки, либо они и вовсе не завершаются. По данным за 2018 г. согласно опросу более 4000 респондентов 69 % проектов достигли заявленных целей, 57 % проектов выполнены в рамках бюджета, 52 % проектов выполнены в срок, 52 % проектов столкнулись с "расползанием содержания", 15 % проектов провалились полностью [16, 17]. При этом 58 % организаций в полной мере осознают ценность проектного менеджмента, 93 % организаций используют стандартизированные практики в управлении проектами. Но, судя по результатам выполнения проектов, использования только лишь стандартов и методов проектного управления недостаточно для достижения поставленных целей. Таким образом, будущее за целым набором подходов — организации, использующие более одного формализованного подхода к управлению проектами и комбинирующие различные техники, показывают лучшие результаты.

Следовательно, нужно в первую очередь искать причинно-следственные связи, приводящие к неудачам проектов на различных стадиях их жизненного цикла, и устранять вероятные проблемы еще до их возникновения. Для решения этих задач как нельзя лучше подходят методы интеллектуального анализа данных и управления знаниями, позволяющие на основе прошлого опыта выполнения удачных и неудачных проектов прогнозировать и направлять ход реализации текущих проектов.

Инновации в отличие от многих других явлений и процессов сочетают в себе элементы многих систем, изучаемых в отдельности (технических, технологических, организационных, экономических, юридических, управления знаниями), и используют разные механизмы управления, свойственные для каждой из этих систем. Это делает чрезвычайно сложной задачу разработки системной модели инновационного проекта в формальной постановке, для которой возможно было бы применение точных методов поиска решений. Не секрет, что даже достаточное количество всех требуемых ресурсов не гарантирует достижения конечных целей проекта. Эффективное управление инновационным проектом возможно только при соблюдении следующих условий:

1) гибкая организационная структура, способствующая быстрому реагированию ЛПР на возникновение проблемных ситуаций как в проекте, так и во внешней среде;

2) полнота знаний о проекте;

3) высокая квалификация ЛПР.

В связи с динамично меняющимися условиями ведения бизнеса руководство предприятий все чаще задумывается о переходе от громоздкой неповоротливой иерархической модели управления к более гибким матричным или проектно-целевым. Такой переход обусловлен еще и тем, что конкурентное преимущество получают, как правило, компании, способные предоставить клиентам качественный товар или услугу в соответствии с их требованиями за более короткий срок. Удовлетворение потребностей клиентов приводит к необходимости иметь огромное число разнообразных сценариев исполнения производственных и организационных процессов, что свидетельствует о постепенном смещении акцентов с управления бизнес-процессами к управлению проектами. Поэтому компании, осуществляющие свою деятельность преимущественно через реализацию проектов различной природы, можно считать проектно-ориентированными. Эффективное управление проектно-ориентированной организацией возможно лишь в случае акцентированного внимания на вопросах стратегического планирования. Ускорение изменений в окружающей среде, появление новых запросов и изменение позиции потребителя, возрастание конкуренции, развитие современных технологий, а также ряд других причин привели к резкому возрастанию значения стратегического управления. Не только руководство компании, но и каждый сотрудник должен хорошо представлять себе цели своей деятельности, влияние успешного решения своих задач на достижение стратегических целей компании, а для этого каждому сотруднику в пределах его компетенции должна быть предоставлена полная и непротиворечивая информация о различных аспектах проекта, т.е. оказана информационная поддержка.

Организация информационной поддержки ЛПР должна быть основана на действующих документах, регулирующих и регламентирующих рассматриваемую деятельность. PMBoK предоставляет и содействует применению общего словаря терминов в профессии управления проектами для обсуждения, написания и употребления понятий управления проектами. Такой стандартный словарь является суще-

ственным элементом любой профессиональной дисциплины и может быть положен в основу онтологии управления инновационным проектом. Авторы предлагают при разработке системной модели инновационного проекта отталкиваться от хорошо известного стандарта, но рассматривать его с позиций того, как принимаемые разными участниками решения связаны с группами процессов и областями знаний — этими ключевыми понятиями PMBoK.

Область знаний трактуется как "выделенная область управления проектом, определяемая ее требованиями к знаниям и описываемая в терминах ее составных процессов, практик, входов, выходов, инструментов и методов" [8]. Процессы управления проектом представляют собой "систематическую последовательность операций, направленную на достижение конечного результата, когда один или несколько входов используются для последующих действий с целью получения одного или нескольких выходов". Руководитель проекта должен обладать определенным уровнем компетенций в каждой из областей знаний, который выражается во владении навыками и умениями применения соответствующих процессов управления, включенных в каждую область знаний. Все 49 процессов управления проектами поделены на 5 групп — процессы инициации, планирования, исполнения, мониторинга и контроля, завершения. Следует заметить, что процессы распределены по группам процессов и по областям знаний неравномерно [8, с. 25], поэтому предлагается три варианта пересечения областей знаний с некоторым набором процессов из групп процессов управления проектом (рис. 6).

Области знаний *1-й группы* охватывают полный набор процессов жизненного цикла проекта. Это такие области знаний, как управление заинтересованными сторонами и управление интеграцией, которая оказывает наибольшее влияние на слаженность работы команды над проектом, а также позволяет учитывать разнообразные аспекты внешнего воздействия на проект.

Области знаний *2-й группы* охватывают только процессы планирования, а также процессы мониторинга и контроля. Эти области знаний составляют хорошо известный "проектный треугольник" — управление расписанием, управление стоимостью и управление содержанием, баланс между сторонами которого означает высокую вероятность достижения конечной цели проекта в соответствии с заданными ограничениями продукта по срокам, цене и функционалу.

Области знаний *3-й группы* охватывают процессы, непосредственно связанные с ходом реализации проекта, когда стадия инициации пройдена, и есть команда, поставившая перед собой цель — выполнение проекта. Это процессы планирования, процессы выполнения, а также процессы мониторинга и контроля. Указанные группы процессов связаны с такими областями знаний, как управление качеством, управление коммуникациями, управление рисками, управление закупками и управление ресурсами. Знания, умения и навыки в этих областях необходимы для решения реальных задач, ежедневно возникающих в ходе выполнения проекта.

В соответствии с этим можно выделить правила принятия решений, предназначенные

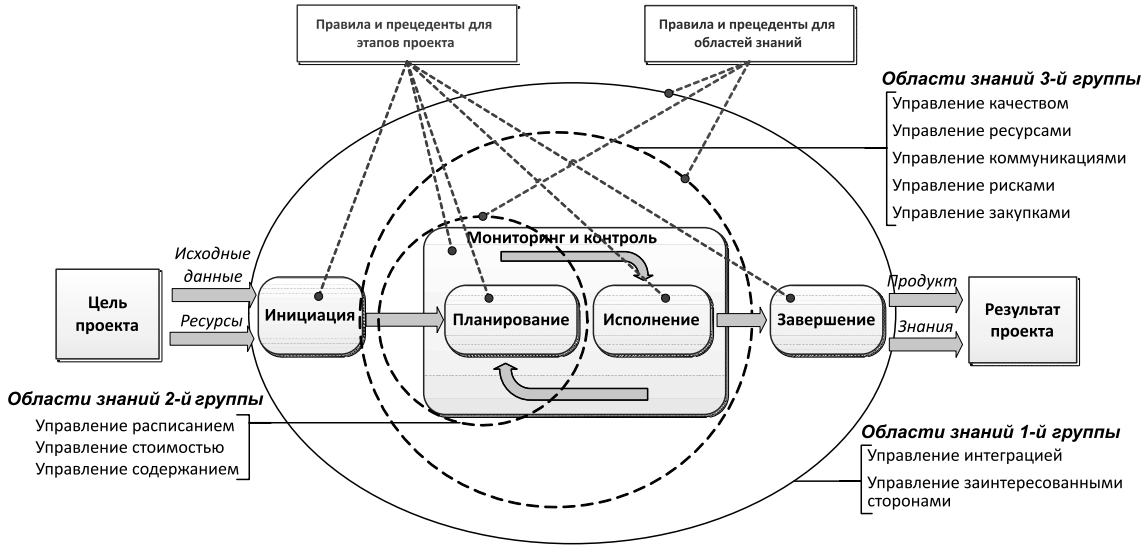

Рис. 6. Пересечение областей знаний и групп процессов проекта

для различных участников команды проекта (руководитель проекта, исполнитель, владелец ресурсов, заказчик, спонсор и т.д.) в различных ситуациях, связанных с различными областями знаний. При этом в проблемных ситуациях, требующих принятия решений, указанным лицам может потребоваться информационная поддержка, связанная с областями знаний при выполнении различных процессов управления проектом.

В рамках проведенных исследований были выделены основные проблемные ситуации, которые могут быть отнесены к приведенным областям знаний и характерны для этапов реализации проектов различного уровня и масштаба, выполняющихся в производственно-экономических системах (см. таблицу). Перечень областей знаний и основные процессы, относящиеся к ним (см. таблицу), соответствуют работе [8, с. 25].

Таблица 1

Типовые проблемные ситуации в областях знаний

Область знаний	Основные процессы	Типовые проблемные ситуации
Управление интеграцией проекта	1) разработка устава проекта; 2) разработка плана управления проектом; 3) руководство и управление работами проекта; 4) управление знаниями проекта; 5) мониторинг и контроль работ проекта; 6) интегрированный контроль изменений; 7) закрытие проекта или фазы	• Задержка разработки и согласования базовых проектных документов. •Заключение дополнительных соглашений. • Отсутствие информации о ходе проекта. • Низкая полнота предоставляемой информации.
Управление содержанием проекта	1) планирование управления содержанием; 2) сбор требований; 3) определение содержания; 4) создание иерархической структуры работ; 5) подтверждение и контроль содержания	• Изменение технологического (производственного) процесса. • Корректировка конструкторской, проектной, технической документации. • Несогласованность требований между заказчиком и исполнителем. • Нарушение принятой формализованной методологии проекта. • Разрастание масштаба проекта.
Управление закупками проекта	1) планирование управления закупками; 2) проведение закупок; 3) контроль закупок	• Задержка проведения конкурсных процедур. • Увеличение длительности проведения торгов. • Срыв сроков поставки. • Низкое качество поставляемой продукции.
Управление стоимостью проекта	1) планирование управления стоимостью; 2) оценка стоимости; 3) определение бюджета; 4) контроль стоимости	• Несоблюдение регламентированных сроков согласования платежей. • Несвоевременное поступление платежей или их отсутствие. • Превышение бюджета проекта.
Управление рисками проекта	1) планирование управления рисками; 2) идентификация рисков; 3) качественный анализ рисков; 4) количественный анализ рисков; 5) планирование реагирования на риски; 6) реагирование на риски; 7) мониторинг рисков	• Изменение нормативно-правовых актов. • Введение санкций. • Утечка кадров. • Отсутствие информации о ключевых аспектах реализации проекта. • Отсутствие аналогов продукта или технологий.
Управление расписанием проекта	1) планирование управления сроками; 2) определение операций; 3) определение последовательности операций; 4) оценка длительности операций; 5) разработка расписания; 6) контроль расписания	• Неопределенность сроков выполнения работ. • Перенос сроков в нарушение графика проекта. • Ограниченная пропускная способность технологического оборудования. • Увеличение срока прохождения государственной экспертизы. • Срыв сроков выполнения проектных работ. • Занятость членов проекта в других проектах и работах (конфликт ресурсов). • Неоптимальная загрузка ресурсов.
Управление качеством проекта	1) планирование управлением качеством; 2) обеспечение качества; 3) контроль качества	• Ненадлежащее качество изделия (брак). • Несоответствие изделия требованиям заказчика. • Несоответствие современным стандартам качества.

Окончание таблицы

Область знаний	Основные процессы	Типовые проблемные ситуации
Управление ресурсами проекта	1) планирование управления ресурсами; 2) оценка ресурсов; 3) приобретение ресурсов; 4) развитие команды; 5) управление командой; 6) контроль ресурсов	• Задержка поставки материалов, комплектующих и оборудования. • Нехватка ресурсов (в т. ч. трудовых). • Ремонт оборудования. • Отсутствие квалифицированных кадров. • Отсутствие мотивации. • Неопытность руководителя. • Исполнители не справляются с возложенным объемом работ. • Необходимость прохождения дополнительного обучения. • Отсутствие сертификатов. • Излишнее совмещение ролей в проекте.
Управление коммуникациями проекта	1) планирование управления коммуникациями; 2) управление коммуникациями; 3) мониторинг коммуникаций	• Отсутствие актуальности выполнения мероприятий. • Отсутствие единой базы для хранения информации по проекту. • Отсутствие утвержденных регламентов горизонтального и вертикального взаимодействия между участниками проекта.
Управление заинтересованными сторонами проекта	1) идентификация заинтересованных сторон; 2) планирование вовлечения заинтересованных сторон; 3) управление вовлечением заинтересованных сторон; 4) мониторинг вовлечения заинтересованных сторон	• Низкая вовлеченность высшего руководства со стороны заказчика. • Частые конфликты с заинтересованными сторонами. • Появление неучтенных ранее заинтересованных сторон, оказывающих существенное негативное влияние на проект. • Задержка согласования договора со стороны заказчика.

Интересно, что проблемные ситуации могут относиться как к процессному, так и к проектному управлению, которые не исключают, а взаимно дополняют и усиливают друг друга в случае выполнения инновационных проектов в производственно-экономической системе. Совместное использование разных типов управления предполагает "нацеленность действий на разные по своей природе объекты, например, на систему управления проектами для процессного подхода и на сами проекты для проектного" [18, с. 38]. При этом ЛПР, находящимися на разных уровнях организационной структуры управления производственно-экономической системы и исполняющими различные роли при управлении проектом, могут быть приняты различные решения при возникновении одной и той же проблемной ситуации. Следовательно, необходимо прогнозировать возможные негативные последствия принятых решений из-за неадекватной оценки проблемной ситуации, связанной с недостаточным опытом ЛПР или его некомпетентностью. Вопросы повторного использования знаний применительно к производственным сетям малых и средних предприятий рассматривались в работах [19—22], вопросы принятия решений при управлении взаимодействующими процессами в проектно-ориентированных организациях освещались в работах [23, 24]. В развитие этих подходов авторы предлагают классифицировать проблемные ситуации и принятые решения в соответствии с областями знаний и уровнем ЛПР в организационной структуре управления проектом.

В качестве эффективного инструмента для решения рассматриваемых задач предлагается разработка и применение методологии, представляющей собой комплекс моделей, методов и средств поддержки принятия решений на основе технологий инженерии знаний, обеспечивающих информационно-аналитическую поддержку управляющей системы на основе интегрированного описания ситуаций, требующих принятия решений, системного сочетания знаний и опыта экспертов, результатов математического и имитационного моделирования. Предлагаемая методология должна обеспечивать возможности уникального "наполнения" содержания моделей и методов в зависимости от специфики проекта, данных и знаний о составе этапов и стадий, перечня оцениваемых показателей и методик их оценки, позволяющей автоматизировать процесс подготовки решений, а также создавать алгоритмическое и программное обеспечение для процессов принятия управленческих решений, адаптируемое под конкретную отрасль и проект.

Для достижения поставленных целей в рамках разрабатываемой методологии предполагается создание интегрированной онтологии,

которая является центральным звеном базы знаний и включает в себя онтологию задач, моделей и методов поддержки принятия решений (ППР) и онтологию проектного менеджмента. По результатам процедур сбора, идентификации, переработки и анализа знания заносятся в интегрированную онтологию в виде правил ППР либо в виде прецедентов проблемных ситуаций. Правила выражают причинно-следственные отношения между событиями, являющимися причинами возникновения проблемных ситуаций в ходе реализации инновационного проекта, самими проблемными ситуациями и действиями, которые рекомендуется выполнить для их разрешения. Таким образом, правила служат связующим звеном между предметной областью реализации проекта и математическими методами поиска наилучших рациональных решений.

С учетом предложенного выше подхода к выделению проблемных ситуаций, возникающих в ходе выполнения инновационного проекта, становится возможным говорить о контекстно-ориентированных правилах и рекомендациях, учитывающих целый спектр характеристик проблемных ситуаций, например: кому из заинтересованных лиц проекта данная рекомендация предназначается, на каком этапе реализации проекта, в рамках какого процесса и к какой области знаний может быть отнесена. Работы по построению контекстно-ориентированных онтологий уже ведутся исследователями в других областях знаний [25—28]. Применительно к рассматриваемой задаче данный подход позволяет обеспечить необходимую полноту базы знаний, создаваемой для проектов различного уровня и масштаба, выполняющихся в производственно-экономических системах.

Заключение

Повышению эффективности управления инновационными проектами способствует оказание интеллектуальной и информационной поддержки принятия решений в проблемных ситуациях, возникающих в ходе реализации инновационных проектов. Использование интеллектуальной системы поддержки принятия решений (ИСППР) обычно не предполагает работу с ней в режиме реального времени в задачах, требующих быстрой реакции ЛПР на возникновение проблемных ситуаций. Тем не менее скорость принятия обоснованных, взвешенных решений играет далеко не последнюю роль в эффективном управлении проектом. Поэтому одной из задач при проектировании и реализации ИСППР является разработка удобного пользовательского интерфейса, требующего минимальных затрат времени на ввод информации о проблемной ситуации и оценку полученных результатов. В зависимости от модели представления знаний результаты работы ИСППР могут быть представлены как в виде набора прецедентов, максимально удовлетворяющих описанию текущей проблемной ситуации, так и в виде готового решения, выведенного на основании заложенных в базу знаний продукционных правил. Одним из способов, способствующих ускорению работы с системой, является классификация прецедентов проблемных ситуаций и, соответственно, решений, предпринимаемых для устранения их последствий. Классификация прецедентов проблемных ситуаций, встречающихся при управлении инновационным проектом, предлагается с позиций PMBoK, являющегося де-факто международным стандартом в области проектного менеджмента.

В целом предложенный подход к организации поддержки принятия решений ориентирован на применение в ходе управления инновационными проектами в процессах стратегического планирования и развития производственно-экономических систем.

В теоретическом аспекте предложенная методология интеллектуальной поддержки принятия решений обобщает и систематизирует накопленный опыт по управлению знаниями, математического и имитационного моделирования и формирует научный задел для дальнейшей разработки и комплексного использования технологий адаптивного управления и имитационного моделирования на базе современных информационных технологий применительно к решению поставленной задачи управления инновационными проектами в процессах стратегического планирования и развития производственно-экономических систем.

Список литературы

1. **Руководство** Осло: Рекомендации по сбору и анализу данных по инновациям / Совместная публикация ОЭСР и Евростата. М.: Государственное учреждение "Центр исследований и статистики науки" (ЦИСН), 2010. 107 с.

2. **Федеральный** закон от 23.08.1996 № 127-ФЗ "О науке и государственной научно-технической политике" (ред. от 23.05.2016). СПС Консультант Плюс. URL: https://минобрнауки.рф/документы/817/файл/8375/127-фз.pdf. (дата обращения: 07.07.2019).

3. **Стратегия** инновационного развития Российской Федерации на период до 2020 года (утверждена Распоряжением Правительства Российской Федерации от 8 декабря 2011 г. № 2227-р). СПС Консультант Плюс. URL: http://www.consultant.ru/document/cons_doc_LAW_123444/ (дата обращения: 15.07.2019).

4. **Указ** Президента РФ № 899 от 07.07.2011г. "Об утверждении приоритетных направлений развития науки, технологий и техники в Российской Федерации и перечня критических технологий Российской Федерации" (с изменениями на 16.12.2015). Электронный фонд правовой и нормативно-технической документации. URL: http://docs.cntd.ru/document/902287707 (дата обращения: 27.03.2019).

5. **Официальный** сайт Федеральной службы государственной статистики. URL: https://www.gks.ru/folder/14477 (дата обращения: 10.07.2019).

6. **Индикаторы** инновационной деятельности: 2018: статистический сборник / Н. В. Городникова, Л. М. Гохберг, К. А. Дитковский и др.. М.: НИУ ВШЭ, 2018. 344 с.

7. **Бечелова Т. Р.** Проблемы формирования производственно-экономических систем в региональной экономике // Современные проблемы науки и образования. 2012. № 2. URL: http://science-education.ru/ru/article/view?id=5826 (дата обращения: 11.07.2019).

8. **A Guide** to the Project Management Body of Knowledge (PMBoK Guide). Project Management Institute. 2017. Pensylvanya: Sixth Edition. PMI Publications, 2017.

9. **ГОСТ Р 58184—2018.** Система менеджмента проектной деятельности. Основные положения. М.: Стандартинформ, 2018.

10. **Арчибальд Р. А.** Управление высокотехнологичными программами и проектами / Рассел Д. Арчибальд; Пер. с англ. Мамонтова Е. В.; Под ред. Баженова А. Д., Арефьева А. О. М.: Компания АйТи; ДМК Пресс, 2010. 464 с.

11. **Мазур И. И., Шапиро В. Д., Ольдерогге Н. Г., Полковников А. В.** Управление проектами: учеб. пособие. М.: Омега-Л, 2014. 959 с.

12. **Закон** Республики Башкортостан от 28 декабря 2006 года N 400-з "Об инновационной деятельности в Республике Башкортостан" (с изменениями на: 30.03.2015 г.). Электронный фонд правовой и нормативно-технической документации. URL: http://docs.cntd.ru/document/935106470 (дата обращения: 07.07.2019).

13. **Алетдинова А. А., Кравченко М. С., Королева Н. С.** Особенности инновационных проектов в сетевой экономике // Интернет-журнал "НАУКОВЕДЕНИЕ". 2016. Т. 8, № 5. URL: http://naukovedenie.ru/PDF/59EVN516.pdf (дата обращения: 20.07.2019).

14. **Никулина Н. О., Иванова И. Ф., Малахова А. И.** Применение интеллектуальных технологий в решении проблем инновационных проектов // Проблемы управления и моделирования в сложных системах: труды XXI Междунар. конф. (3—6 сентября 2019 г., Самара): в 2-х т. Самара: ООО "Офорт", 2019. Т. 2. С. 483—488.

15. **Павлов А. Н.** Эффективное управление проектами на основе стандарта PMI PMBoK 6th Edition. М.: Лаборатория знаний, 2019. 270 с.

16. **Pulse** of the Profession: Success in disruptive times. Expanding the value delivery landscape to address the high cost of low performance, February 2018. URL: https://www.pmi.org/learning/thought-leadership/pulse/pulse-of-the-profession-2018 (дата обращения: 17.07.2019).

17. **Никулина Н. О., Иванова И. Ф., Бармина О. В.** Проектный менеджмент в управлении бизнес-процессами. Уфа: РИК УГАТУ, 2017. 260 с.

18. **Новиков Д. А.** Методология управления. М.: Либроком, 2011. 128 с.

19. **Зандкуль К., Смирнов А. В.** Управление знаниями в производственных сетях: классификация и технологии для повторного использования знаний // Труды СПИИРАН. 2018. № 1 (56). С. 5—33.

20. **Sandkuhl K., Stirna J., Persson A., Wißotzki M.** Enterprise Modeling: Tackling Business Challenges with the 4EM Method. Springer, 2014. 309 p.

21. **Jakubowski J., Peterka J.** Design for Manufacturing in Virtual Environment using Knowledge Engineering // Management and Production Engineering Review. 2014. Vol. 5. N. 1. P. 3—10.

22. **Lillehagen F., Krogstie J.** Active Knowledge Modelling of Enterprises. Springer, 2009. 436 p.

23. **Черняховская Л. Р., Никулина Н. О., Ширяев О. В.** Интеллектуальное управление сложными деловыми процессами на основе онтологических баз знаний. Уфа: РИК УГАТУ, 2018. 186 с.

24. **Бармина О. В., Никулина Н. О.** Интеллектуальная система управления взаимодействием бизнес-процессов в проектно-ориентированных организациях // Онтология проектирования. 2017. Т. 7, № 1 (23). С. 48—65.

25. **Guizzardi G., Wagner G., Almeida J. P. A., Guizzardi R. S. S.** Towards Ontologica Foundations for Conceptual Modeling: The Unified Foundational Ontology (UFO) Story // Applied ontology. 2015. Vol. 10, N. 3—4. P. 259—271.

26. **Каныгин Г. В., Полтинникова М. С.** Контекстно-ориентированные онтологические методы в социологии // Труды СПИИРАН. 2016. № 48 (5). С. 107—124.

27. **Smirnov A., Sandkuhl K., Shilov N.** Multilevel Self-Organization and Context-Based Knowledge Fusion for Business Model Adaptability in Cyber-Physical Systems // IFAC Proceedings Volumes. 2013. Vol. 46, N. 9. P. 2045—2050.

28. **Blomqvist E., Hammar K., Presutti V.** Engineering Ontologies with Patterns: The eXtreme Design Methodology // Ontology Engineering with Ontology Design Patterns. IOS Press. 2016. Vol. 25. P. 23—50.

A. I. Malakhova, Assistant Professor, e-mail: aimalakhova@gmail.com,
N. O. Nikulina, Assistant Professor, e-mail: nikulinano@outlook.com,
L. R. Chernyakhovskaya, Professor, e-mail: lrchern@yandex.ru,
Ufa State Aviation Technical University, Ufa, 450077, Russian Federation

Studding the Problem of Innovative Projects Management in Strategic Planning and Progress Processes of Production and Economic Systems

Priority areas of science and technology progress should be supported by critical technologies, possessing a wide potential range of competitive innovative applications in different sectors of economy. In turn, development of the critical technologies can be carried out only within the innovative projects realization, since innovative projects specifically are carried out in close cooperation of science, economy and production. Successful functioning of production and economic systems is possible only in the case of decision-makers close attention to strategic planning issues of the whole enterprise activities, as well as to the innovative projects of various types carried out within the framework of production and economic systems. Innovative projects implementation should be based on the project management principles involving methods and means of knowledge engineering for a comprehensive assessment and analysis of all available information about the project state at any stage of the life cycle

in order to make reasonable decisions in various areas of knowledge. An innovative project managing effectiveness is largely determined by the quality of management decisions, which are made in conditions of insufficient data and resources, uncertainty in decisions consequences, instability of external conditions, lack of effective information interaction between project managers from one side or another within the presence of different criteria for choosing alternatives. Reducing the impact of mentioned uncertainties can be achieved by using a formalized approach to project management based on the project management standards recommendations in conjunction with the intellectual decision making support for project participants.

Keywords: *innovative projects management, production and economic system, knowledge engineering, intellectual decision making support, ontology, knowledge base*

DOI: 10.17587/it.26.239-251

References

1. **Oslo** Manual: Guidelines for Collecting and Interpreting Innovation Data, OECD/EQ, 2005, 107 p. (in Russian).

2. **Federal** law № 127-FL dated 23.08.1996 "On science and state scientific and technical policy" (ed. dated 23.05.2016), ATP Consultant Plus, available at: https://минобрнауки.рф/документы/817/ файл/8375/127-фз.pdf. (accessed 07.07.2019) (in Russian).

3. **Strategy** of Russian Federation innovative development for the period till 2020 (approved by the Russian Federation Government Order on December 8, 2011 № . 2227-r), ATP Consultant Plus, available at: http://www.consultant.ru/document/ cons_doc_LAW_123444/ (accessed 15.07.2019) (in Russian).

4. **The Presidential** Decree № 899 from 07.07.2011 "On approving the priority directions of science, technologies and technics development in Russian Federation and the list of critical technologies of Russian Federation" (as amended on 16.12.2015), Electronic Fund of legal and normative-technical documentation, available at: http://docs.cntd.ru /document/902287707. (accessed 27.03.2019) (in Russian).

5. **Official** web site of Federal state statistics service, available at: https://www.gks.ru/folder/14477 (accessed: 10.07.2019) (in Russian).

6. **Gorodnikova N., Gokhberg L., Ditkovskiy K.** et al. Indicators of Innovation in Russian Federation: 2018: Data book, Moscow, Publishing house of HSE, 2018, 369 p. (in Russian).

7. **Bechelova T. R.** Problems of production and economic systems formation in regional economy, *Sovremennye problemy nauki i obrazovanija,* 2012, no. 2, available at: http://science-education.ru/ru/article/view?id=5826. (accessed 11.07.2019) (in Russian).

8. **A Guide** to the Project Management Body of Knowledge (PMBoK Guide), Project Management Institute, Pensylvanya, Sixth Edition, PMI Publications, 2017.

9. **GOST** R 58184-2018, Moscow, Standartinform, 2018 (in Russian).

10. **Russell D. Archibald.** *Managing High-Technology Programs and Projects, 3rd Edition*. Wiley, 2003. 396 p.

11. **Mazur I. I., Shapiro V. D., Olderogge N. G., Polkovnikov A. V.** Project management: tutorial, Moscow, Omega-L, 2014, 959 p. (in Russian).

12. **The Law** of the Republic of Bashkortostan of December 28, 2006 № 400-z "On innovative activity in the Republic of Bashkortostan" (with changes on: 30.03.2015, Electronic Fund of legal and normative-technical documentation, available at: http://docs.cntd.ru/document/935106470. (accessed 07.07.2019) (in Russian).

13. **Aletdinova A. A., Kravchenko M. S., Koroleva N. S.** The innovative projects features in the network economy, *Internet-zhurnal "NAUKOVEDENIE" — Internet journal "SCIENCE"*, 2016, vol. 8, no. 5, available at: http://naukovedenie.ru/PDF/59EVN516.pdf. (accessed 20.07.2019) (in Russian).

14. **Nikulina N. O., Malakhova A. I., Ivanova I. F.** Application of intelligent technologies in solving the innovative projects problems, *Problemy upravlenija i modelirovanija v slozhnyh sistemah: trudy XXI Mezhdunar. konf.* [Proceedings of the XXI International Scientific Conference "Control and Modelling Problems in Complex Systems" (CMPCS-2019)], Samara, OOO "Ofort", 2019, vol. 2, pp. 483—488. (in Russian).

15. **Pavlov A. N.** Effective project management based on PMI PMBoK, Moscow, Laboratorija znanij, 2019, 270 p. (in Russian).

16. **Pulse** of the Profession: Success in disruptive times. Expanding the value delivery landscape to address the high cost of low performance, February 2018, available at: https://www.pmi.org/learning/thought-leadership/pulse/pulse-of-the-profession-2018. (accessed 17.07.2019).

17. **Nikulina N. O., Ivanova I. F., Barmina O. V.** Project management in business process management: textbook, Ufa, USATU RPC, 2017, 260 p. (In Russ).

18. **Novikov D. A.** Methodology of management, Moscow, Librokom, 2011, 128 p. (in Russian).

19. **Zandkul' K., Smirnov A. V.** Knowledge Management in production networks: classification and technology for knowledge reuse, *Trudy SPIIRAN — Proceedings of SPIIRAS*, 2008, no. 1(56), pp. 5—33 (in Russian).

20. **Sandkuhl K., Stirna J., Persson A., Wißotzki M.** Enterprise Modeling: Tackling Business Challenges with the 4EM Method, Springer, 2014, 309 p.

21. **Jakubowski J., Peterka J.** Design for Manufacturing in Virtual Environment using Knowledge Engineering, *Management and Production Engineering Review*, 2014, vol. 5, no. 1, pp. 3—10.

22. **Lillehagen F., Krogstie J.** Active Knowledge Modelling of Enterprises, Springer, 2009, 436 p.

23. **Chernyakhovskaya L. R., Nikulina N. O., Shirjaev O. V.** Intellectual management in complex business processes on the basis of ontological knowledge bases, Ufa, USATU RPC, 2018, 186 p. (in Russian).

24. **Barmina O. V., Nikulina N. O.** Intelligent system for interactive business processes management in project-oriented organizations, *Ontologija proektirovanija — Ontology of designing*, 2017, no. 7(1), pp. 48—65 (in Russian).

25. **Guizzardi G., Wagner G., Almeida J. P. A., Guizzardi R. S. S.** Towards Ontologica Foundations for Conceptual Modeling: The Unified Foundational Ontology (UFO) Story, *Applied Ontology*, 2015. vol. 10, no. 3—4, pp. 259—271.

26. **Kanygin G. V., Altinnikova M. S.** Context-oriented ontological methods in sociology, *Trudy SPIIRAN — Proceedings of SPIIRAS*, 2016, no. 48(5), pp. 107—124 (in Russian).

27. **Smirnov A., Sandkuhl K., Shilov N.** Multilevel Self-Organization and Context-Based Knowledge Fusion for Business Model Adaptability in Cyber-Physical Systems, *IFAC Proceedings Volumes*, 2013, vol. 46, no. 9, pp. 2045—2050.

28. **Blomqvist E., Hammar K., Presutti V.** Engineering Ontologies with Patterns: The eXtreme Design Methodology, *Ontology Engineering with Ontology Design Patterns,* IOS Press, 2016, vol. 25, pp. 23—50.

УДК 004.93'1 + 004.932 DOI: 10.17587/it.26.252-256

Г. К. Букалов, д-р техн. наук, проф., e-mail: gk.bukalov44@yandex.ru,
А. О. Бурыгин, аспирант, e-mail: g.t.m.p@yandex.ru,
И. Г. Панин, д-р техн. наук, проф., e-mail: igpanin@list.ru,
Костромской государственный университет

Применение методов построения сообществ для сегментации изображений текстильных строп

Рассматривается задача сегментации текстильной стропы графовыми методами обнаружений сообществ. Изображение проходит начальную сегментацию алгоритмом Meanshift, после чего идет построение взвешенного неориентированного графа (WRAG), вершины которого представляют регионы, полученные после начальной сегментации. Веса ребер вычисляются исходя из признаков цвета и текстуры региона изображения. Используется алгоритм FMCDRN для обнаружения сообществ на графе. Каждому сообществу соответствует маска реального объекта на изображении. Проведен вычислительный эксперимент, направленный на исследование эффективности предложенного метода.

Ключевые слова: *выделение сообществ на графах, сегметация изображения, Region Adjacency Graph, гистограмма ориентированных градиентов (HOG), критерий Ньюмена*

Введение

В работе рассматривается актуальная задача непрерывного тестирования текстильных строп. В соответствии с требованиями "Межотраслевых правил по охране труда при погрузочно-разгрузочных работах и размещении грузов" ПОТ РМ-007-98 с приложениями перед использованием грузоподъемных строп стропальщики или иные ответственные лица обязаны их тщательно осмотреть. При осмотре текстильных строп основное внимание должно быть обращено на состояние и целостность ленты (отсутствие разрывов, порезов, расслоения ленты, наличия поверхностных обрывов нитей ленты, повреждений, связанных с воздействием химических веществ, наличия прожженных отверстий). Ввиду ограниченной способности человека к обработке информации при большом объеме проверяемого материала число пропущенных дефектов резко возрастает. Для улучшения качества контроля строп и высвобождения человеческих ресурсов для более квалифицированного труда существует потребность в автоматизации процесса контроля.

Распознавание дефектов стропы по изображению принято делить на два процесса:

1. Сегментация изображения для выявления контура объекта распознавания через выявление масок объектов (данный этап можно пропустить, если входные данные нормализованы).

2. Нахождение и классификация дефектов в выбранной области изображения.

В данной статье рассматривается первая задача, а именно сегментация изображений, являющаяся фундаментальной проблемой в области компьютерного зрения, цель которой — разбиение изображения на уникальные и однородные области, которые соответствуют значимым частям изображения. Среди всего множества алгоритмов сегментации изображений был выбран графовый метод выявления регионов, который представляет компоненты изображения как математически обоснованные структуры, что упрощает задачу сегментации и делает вычисления более быстрыми и эффективными. Задача сегментации изображений на основе графов заключается в разбиении первоначального графа на несколько подграфов таким образом, чтобы каждый из них представлял значимый объект интереса, и дальнейшем создании масок по сообществам поверх оригинального изображения.

1. Описание процесса сегментации

Графовые сети могут упростить сегментацию и анализ изображений, но в первоначальном виде они теряют некоторую важную информацию, которая влияет на производительность сети и результативность сегментации, поэтому предлагается способ начальной сегментации изображения для построения графа областей смежности (далее Region Adjacency Graph — RAG) [1]. В этом случае начальные области считаются узлами графа, а если области являются смежными, то можно говорить о существовании ребра между ними. Далее ребра графа взвешиваются в соответствии со сход-

ством между значимыми визуальными признаками областей (текстурой и цветом). Алгоритм обнаружения сообществ применяется далее на графе смежности взвешенных областей (далее Weighted Region Adjacency Graph — WRAG) для разделения сети на набор сообществ. Эти сообщества используются для группировки похожих смежных областей на изображении. Все узлы, принадлежащие к одному сообществу, считаются принадлежащими к одной области и объединены в одну область на изображении. Процесс повторяется до тех пор, пока не появится разница между открытыми структурами сообщества двух последовательных итераций.

Таким образом, основной процесс сегментации изображения выполняется следующим образом:

1) моделируется изображение с WRAG, который использует преимущества топологических и визуальных свойств изображений (текстуры, цвета);

2) решаются задачи сегментации при использовании алгоритмов обнаружения сообществ;

3) итерационно решается проблема пересегментации/недосегментации.

Чтобы преодолеть возможные ограничения, предлагается структура с начальной сегментацией, исходное изображение делится на области, которые должны быть когерентными и сохраняют большую часть информации, необходимой для сегментации. Затем RAG используется для представления изображения, где каждая область представляет узел на графе. Если ребра находятся рядом, то они становятся ребрами между двумя регионами. Для взвешивания RAG используется комбинация текстурных и цветовых признаков для измерения сходства между узлами. Наконец, на основе эффективных алгоритмов обнаружения сообществ, которые обеспечивают наилучший баланс между вычислительными затратами и производительностью сегментации, извлекаются сообщества, представляющие регионы на изображении. Процесс повторяется итеративно до тех пор, пока не будет достигнута оптимальная сегментация.

Как уже отмечалось, целью начальной сегментации является разбиение изображения на однородные и как можно меньшие области. На этом этапе можно использовать несколько низкоуровневых методов сегментации, таких как Superpixels, Meanshift, Levelset и Watershed.

2. Определение метрик взвешенных узлов

На следующем шаге нужно определить метрики взвешенных узлов, их можно разбить на метрики сходства цвета и метрики структуры.

Метрика сходства цвета определяется исходя из цвета в сегментации и является важной и при этом простой составляющей. Каждый пиксель в цветном изображении представлен трехмерным вектором. Можно предположить, что значение интенсивности пикселей данной области распределено по нормальному закону. Поэтому распределение области R_i задается как

$$R_i N(\mu_i,\ var_i),$$

где μ_i — средний вектор интенсивности пикселей, вычисленный в трехмерном цветовом пространстве в областях R_i, а var_i обозначает дисперсию R_i.

Для измерения сходства между двумя распределениями выбираем среднее расстояние (Mean Distance, MD), поскольку оно, как правило, дает хорошее приближение с более низкой сложностью, которое и определяется следующим образом:

$$D_{MD}(R_i, R_j) = (\mu_i - \mu_j)^{\mathrm{T}}(\mu_i - \mu_j).$$

Для преобразования распределения расстояния цветовых параметров в метрику сходства используется ядро радиальной базисной функции:

$$c_{ij} = \exp\left(\frac{-D_{MD}(R_i, R_j)}{2\sigma^2}\right), \qquad (1)$$

где σ — параметр, определенный пользователем.

Выбор подходящего цветового пространства для сегментации цветного изображения является важным шагом для достижения лучшей производительности сегментации. В работе выбрано цветовое пространство LAB, которое больше всего соответствует зрительной системе человека и представляет собой трехосевое цветовое пространство с пространством L для обозначения светлости и пространствами A и B для обозначения красно-зеленого и желто-зеленого оттенков соответственно.

Использование только цветового признака в изображении не может обеспечить хороший результат сегментации, так как цветовой признак в некотором однородном объекте разложит закономерности изображения на различные сегменты, поэтому необходимо привлечь рассмотрение свойства текстур. Для этого в работе используется функция, называемая гистограммой ориентированных градиентов (Histogram of Oriented Gradients, HOG), хорошо известная в задачах обработки изображений и компьютерного зрения, которая применяется для обнаружения объектов на изображении. HOG вычисляет

число проявлений градиентной ориентации в локализованных частях изображения. Для построения гистограммы ориентированных градиентов необходимо выполнить следующие шаги:

- вычислить горизонтальный и вертикальный градиенты;
- разбить область изображения на небольшие ячейки размером $c \times c$ пикселей ($c = 8$). Для каждой ячейки вычисляется гистограмма направлений градиента. Гистограмма представляет собой вектор из 9 ячеек;
- использовать метод, называемый блочной нормализацией, чтобы сгруппировать отдельные ячейки в блоки и нормализовать их для обеспечения инвариантности к изменениям освещенности. Блок представлен ячейками 2×2 так, что каждый блок имеет размер $2c \times 2c$ пикселей (4 гистограммы);
- вычислить окончательный вектор признаков для всей области R_i, где гистограммы векторов градиентов блоков h_c сгруппированы в один вектор признаков HOG H_i:

$$H_i = [h_1, \ldots, h_c],$$

где h_c обозначает гистограмму векторов градиента блока, c — число блоков внутри области R_i. Чтобы вычислить сходство между двумя областями R_i и R_j, мы используем меру косинусного сходства, как определено формулой ниже:

$$t_{ij} = \cos(H_i, H_j) = \frac{H_i^{\mathrm{T}} H_j}{\|H_i\| \|H_j\|}, \qquad (2)$$

где оператор $\|\cdot\|$ обозначает L_2-норму, а H_i, H_j — соответственно HOG векторы регионов R_i и R_j.

Структурирование сложных сетей на сообщества — это процесс, который можно описать как объединение узлов в сообщества таким образом, что плотность ребер внутри сообществ выше, чем между самими сообществами. Наиболее используемый критерий для извлечения структуры сообщества в сетях введен Ньюменом [2] и определяет меру, названную модульностью:

$$Q = \sum (e_{ii} - a_i^2),$$

где e_{ii} обозначает долю ребер сети, которые входят в сообщество i, а a_i^2 — долю ребер, которые вставляются случайным образом. Значение модульности Q находится в диапазоне от 0 до 1. Высокое значение модульности означает сильную структуру сообщества сети.

Для обнаружения сообществ рассматривались следующие алгоритмы: FMCDRN [3], Infomap [4], FGMDO [5], Louvain [6].

3. Алгоритм определения оптимальных сообществ

Таким образом, для решения указанных задач предлагаемая структура должна использовать все присущие изображению свойства, а также эффективную оптимизацию по модульности/стабильности. Для этого необходимо выполнить следующие шаги:

1) начальная сегментация, при которой резко уменьшается число узлов в графе;

2) построение RAG с использованием пространственной априорной информации изображения. Пусть $G = (V, E)$ — неориентированный граф, где $v_i \in V$ — множество узлов, соответствующих областям изображения R_i, E — множество ребер, соединяющих пары соседних узлов. Другими словами, ребро рассматриваются между двумя узлами, если их соответствующие области являются смежными на изображении;

3) добавление весов (построение WRAG) при использовании сходства между областями, где цвет и текстура изображения сравниваются для двух соседних областей в RAG. Чтобы вычислить матрицу подобия W (для построения RAG), используются уравнения (1) и (2) для измерения подобия между каждыми двумя смежными областями, затем добавляются веса между ними. В данной работе сходство вычисляется с использованием комбинации LAB- и HOG-признаков, для чего используется гибридная модель, объединяющая оба этих признака. Выбирается текстура (HOG) и матрица подобия (взвешенная цветовая LAB-функция) следующим образом:

$$W = w_{ij} = a\sqrt{t_{ij} c_{ij}} + (1 - a) c_{ij}, (i, j) = 1, \ldots, n;$$

4) выявление сообществ в сети с использованием эффективных алгоритмов обнаружения сообществ [3—6], которые обеспечивают оптимальный баланс между вычислительными затратами и эффективностью сегментации.

4. Результаты исследования и оценка эффективности

Для исследования эффективности предложенной структуры сначала изучается влияние некоторых параметров, используемых при вычислении подобия между регионами. Проводятся первые эксперименты на 10 изображениях наборов данных с использованием нескольких значений параметра балансировки, чтобы найти подходящее значение, которое обеспечивает наилучшие результаты сегментации.

Затем выполняется сравнение между метриками изображения (цветом и текстурой), а имен-

но рассматривается производительность предлагаемого подхода в тех случаях, когда в процессе сегментации используются только текстура, только цвет или связка цвет—текстура.

Для оценки эффективности предлагаемой системы используется вероятностный индекс Рэнда (Probabilistic Rand Index или PRI) [7] и вариация информации (Variation of Information VOI), которые являются хорошо известными оценочными метриками для сегментации. PRI измеряет меру сходства между двумя кластерами данных (чем больше значение PRI, тем больше сходство между двумя сегментами изображения). Метрика VOI измеряет сумму информационного прироста и потери информации между двумя сегментами. Метрика VOI неотрицательна, чем она ниже, тем сходство больше:

$$VOI(C,\ C') = H(C) + H(C') - 2I(C,\ C'),$$

где $H(C)$ и $H(C')$ — энтропия сегментов C, C' соответственно, а $I(C,\ C')$ определяет меру общей информации между сегментами.

Также будем оценивать эффективность предлагаемого подхода с двух сторон: метриками точности (Precision) и полноты (Recall). Точность измеряет долю граничных пикселей, которые соответствуют своим истинным границам изображения:

$$Precision = \frac{|S_{test}| \cap |S_i|}{|S_{test}|},$$

где S_i — истинная сегментация по разметке; S_{test} — тестовая сегментация, а $|S|$ — число граничных пикселей в сегментации. Полнота показывает меру обнаруженных пикселей на границе сегментов, являющихся истинными:

$$Recall = \frac{|S_{test}| \cap |S_i|}{|S_i|}.$$

Тогда F-мера как гармоническое среднее полноты и точности определяется как (далее $\alpha = 0.5$):

$$F = \frac{Precision \cdot Recall}{(1-\alpha) \cdot Recall + \alpha \cdot Precision}.$$

Для выбора подходящей начальной сегментации, обеспечивающей наилучшие результаты сегментации, были проведены эксперименты с использованием двух алгоритмов начальной сегментации для поиска подходящего. Показано, что алгоритм Meanshift является более подходящим, чем алгоритм Superpixels для всех четырех метрик, а также более выгодным по времени работы.

Для выбора алгоритма детекции сообществ сравнивались алгоритмы FMCDRN, Infomap, FGMDO, Louvain. По всем параметрам наилучшую сегментацию изображения дает алгоритм FMCDRN.

При сравнении предложенного алгоритма с известными методами сегментации Modularity-based image segmentation, WiseCode [8], LC [9], EDISON [10] показано, что все метрики имеют лучшие показатели.

Заключение

В данной работе предложена структура системы сегментации изображений, которая учитывает преимущества присущих изображениям свойств и оптимизацию модульности/стабильности. При использовании как гистограммы ориентированных градиентов (HOG) текстурного признака, так и цветового признака матрица подобия строится адаптивно между различными областями путем оптимизации модульности/стабильности и объединения смежных областей изображений итеративно. Эксперименты показали, что предложенная структура системы дает наилучший качественный результат сегментации и обеспечивает лучшую производительность по сравнению со всеми современными методами с точки зрения PRI, VOI, точности и полноты. Поскольку общая структура основана на трех эффективных алгоритмах определения сообщества, она позволяет избежать проблемы наличия большого числа небольших областей в изображении и сохраняет информацию и закономерности в объекте, обеспечивает хорошую временную сложность и работает последовательно быстрее, чем современные алгоритмы.

Список литературы

1. **Wu Zhenyu, Richard Leahy.** An optimal graph theoretic approach to data clustering: Theory and its application to image segmentation // IEEE transactions on pattern analysis and machine intelligence. 1993. Vol. 15, N. 11. P. 1101—1113.

2. **Clauset A., Newman M. E., Moore C.** Finding community structure in very large networks // arXiv.org. 2004. Дата обновления: 30.08.2004. URL: https://arxiv.org/abs/cond-mat/0408187.

3. **Blondel V. D., Guillaume J. L., Lambiotte R., Lefebvre E.** Fast unfolding of communities in large networks // arXiv.org. 2008. Дата обновления: 25.07.2008. URL:https://arxiv.org/abs/0803.0476.

4. **Li Shijie, Dapeng Oliver Wu.** Modularity-based image segmentation // IEEE Transactions on Circuits and Systems for Video Technology. 2015. Vol. 25, N. 4. P. 570—581.

5. **Ronhovde P., Nussinov Z.** Local resolution-limit-free Potts model for com- munity detection // arXiv.org. 2008. Дата обновления: 15.04.2010. URL:https://arxiv.org/abs/0803.2548.

6. **Newman Mark E. J.** Fast algorithm for detecting community structure in networks // Physical review. 2004. Vol. E 69, N. 6.

7. **Unnikrishnan R., Pantofaru C., Hebert M.** Toward objective evaluation of image segmentation algorithms // Pattern Analysis and Machine Intelligence IEEE. 2007. Transactions on. P. 929—944.

8. **Rosvall M., Bergstrom C. T.** Maps of random walks on complex networks reveal community structure // Proceedings of the National Academy of Sciences. 2008. Vol. 105, N. 4. P. 1118—1123.

9. **Yang A., Wright Y., Sastry S.** Unsupervised segmentation of natural images via lossy data compression // Computer Vision and Image Understanding. 2008. P. 212—225.

10. **Christoudias C. M., Georgescu B., Meer P.** Synergism in low level vision // Pattern Recognition. Proceedings of 16th International Conference. IEEE. 2002. P. 150—155.

G. K. Bukalov, Professor, e-mail: gk.bukalov44@yandex.ru,
A. O. Burygin, PhD student, e-mail: g.t.m.p@yandex.ru, **I. G. Panin,** Professor, e-mail: igpanin@list.ru,
Kostroma State University, Kostroma, 156005, Russian Federation

Application of Community Building Methods for Segmentation of Textile Slings Images

There is problem of segmentation of textile slings by graph methods of community detection is considered. Image is initially segmented by the Meanshift algorithm, followed by the construction of a Weighted Region Adjacency Graph (WRAG), the vertices of which represent the regions obtained after the initial segmentation. The quality of the graph partitioning into subgraphs is determined by the Newman criterion. Edge weights are calculated based on the color and texture characteristics of the image region. Comparison of graph node weight metrics: color similarity metric defined by Mean Distance, texture property metric defined by Histogram of Oriented Gradients, and superposition of LAB and HOG image components. The FMCDRN algorithm is used to detect communities on the graph. Each community has a mask of the real object in the image. To determine the effectiveness of the proposed system, are use Probabilistic Rand Index (PRI), Variation of Information (VOI), and F-measure. Comparison of the effect of initial segmentation by Meanshift and Superpixel algorithms. Qualitative comparison of FMCDRN, Infomap, FGMDO, Louvain methods for highlighting communities on a graph. A computational experiment aimed at studying the effectiveness of the proposed method is carried out. Comparison of the proposed algorithm with modern image segmentation frameworks WiseCode, LC, EDISON.

Keywords: *community allocation on graphs, image segmentation, Region Adjacency Graph, histogram of oriented gradients (HOG), Newman criterion.*

DOI: 10.17587/it.26.252-256

Refences

1. **Wu Zhenyu, Richard Leahy.** An optimal graph theoretic approach to data clustering: Theory and its application to image segmentation, *IEEE transactions on pattern analysis and machine intelligence,* 1993, vol. 15, no. 11, pp. 1101—1113.

2. **Clauset A., Newman M. E., Moore C.** Finding community structure in very large networks, arXiv.org, 2004, available at: https://arxiv.org/abs/cond-mat/0408187.

3. **Blondel V. D., Guillaume J. L., Lambiotte R., Lefebvre E.** Fast unfolding of communities in large networks, arXiv.org, 2008, available at: https://arxiv.org/abs/0803.0476.

4. **Li Shijie, Dapeng Oliver Wu.** Modularity-based image segmentation, IEEE *Transactions on Circuits and Systems for Video Technology*, 2015, vol. 25, no. 4, pp. 570—581.

5. **Ronhovde P., Nussinov Z.** Local resolution-limit-free Potts model for com- munity detection, arXiv.org. 2008, available at: https://arxiv.org/abs/0803.2548.

6. **Newman Mark E. J.** Fast algorithm for detecting community structure in networks, *Physical Review*, 2004, vol. E 69, no. 6.

7. **Unnikrishnan R., Pantofaru C., Hebert M.** Toward objective evaluation of image segmentation algorithms, Pattern Analysis and Machine Intelligence IEEE, 2007, Transactions on, pp. 929—944.

8. **Rosvall M., Bergstrom C. T.** Maps of random walks on complex networks reveal community structure, *Proceedings of the National Academy of Sciences*, 2008, vol. 105, no. 4, pp. 1118—1123.

9. **Yang A., Wright Y., Sastry S.** Unsupervised segmentation of natural images via lossy data compression, *Computer Vision and Image Understanding*, 2008, pp. 212—225.

10. **Christoudias C. M., Georgescu B., Meer P.** Synergism in low level vision, in *Pattern Recognition*, 2002, *Proceedings. 16th International Conference on, IEEE*, 2002, pp. 150—155.

Адрес редакции:

107076, Москва, Стромынский пер., 4

Телефон редакции журнала **(499) 269-5510**
E-mail: it@novtex.ru

Технический редактор *Е. В. Конова*.
Корректор *Е. В. Комиссарова*.
Сдано в набор 10.02.2020. Подписано в печать 25.03.2020. Формат 60×88 1/8. Бумага офсетная.
Усл. печ. л. 8,86. Заказ IT420. Цена договорная.

Журнал зарегистрирован в Министерстве Российской Федерации по делам печати, телерадиовещания и средств массовых коммуникаций.
Свидетельство о регистрации ПИ № 77-15565 от 02 июня 2003 г.

Оригинал-макет ООО "Адвансед солюшнз". Отпечатано в ООО "Адвансед солюшнз".
119071, г. Москва, Ленинский пр-т, д. 19, стр. 1. Сайт: **www.aov.ru**

Рисунки к статье В. И. Васильева, А. М. Вульфина, М. Б. Гузаирова, В. М. Картака, Л. Р. Черняховской

«ОЦЕНКА РИСКОВ КИБЕРБЕЗОПАСНОСТИ АСУ ТП ПРОМЫШЛЕННЫХ ОБЪЕКТОВ НА ОСНОВЕ ВЛОЖЕННЫХ НЕЧЕТКИХ КОГНИТИВНЫХ КАРТ»

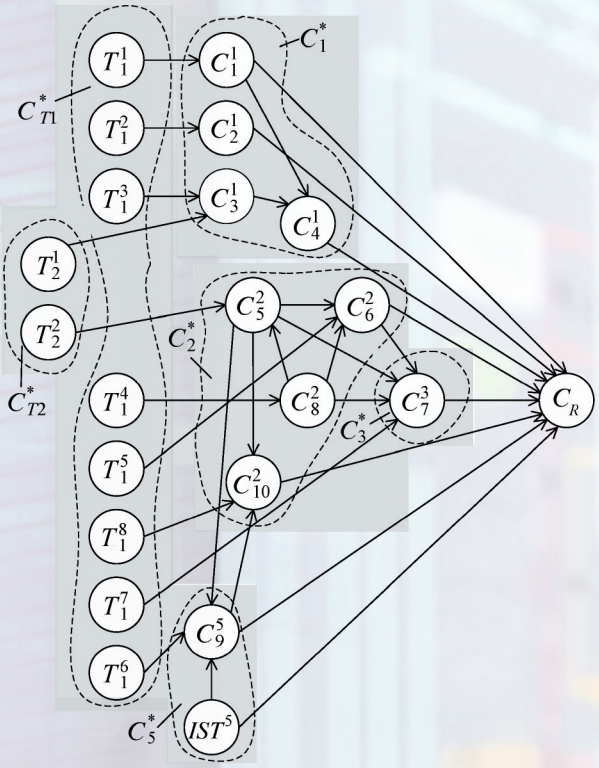

Рис. 4. Первый уровень декомпозиции НСКК для оценки рисков АИС

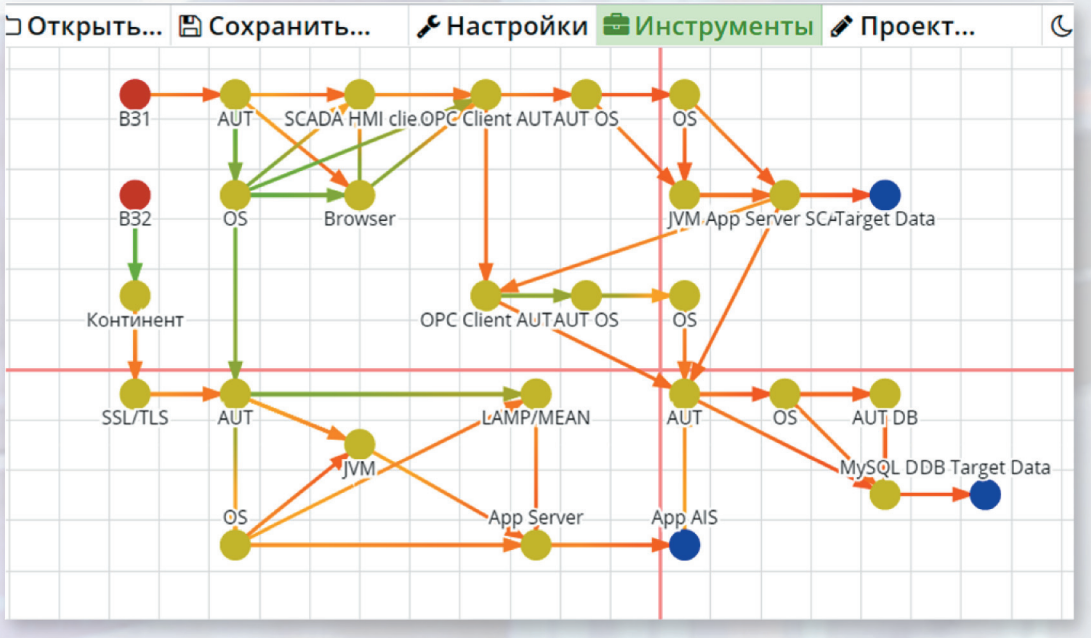

Рис. 6. НСКК для оценки рисков подсистемы сбора и хранения данных на станциях обслуживания (зона 1)

ISSN 1684-6400. Информационные технологии. 2020. Том 26. № 4. 193–256. Индекс: 72656 (Объединенный каталог «Пресса России»)