I. A. Mondikova, M. A. Vaichikauskas

CRYPTO SCHEMES BASED ON DIFFICULT DESCRETE LOGARITHM TASK

It is proposed algorithms and protocols, cracking of wich is required solving two hard computational tasks simultaneously: discrete logarithm task and factorization task. In compare of existing schemes, which could be cracked by solving one hard computational task, these schemes provide higher level of security, because of requirement of solving two hard computational tasks of different types simultaneously.

Cryptographic protocols, hard task, discrete logarithm task, hard computational (mathematichal) task, factorization task

УДК 681.5

Б. Я. Советов, В. В. Цехановский, В. Д. Чертовской, Р. А. Нечитайленко

Формирование математического описания многоуровневой адаптивной автоматизированной системы управления производством на стадии планирования

Рассмотрены требования к методам описания трехуровневых адаптивных автоматизированных систем управления производством (ААСУП). Проведен анализ локальных методов описания, предложены глобальные математические методы исследования ААСУП.

Адаптивное управление, анализ методов, выбор методов, формирование, глобальное описание, планирование, требования к методам

Адаптивные автоматизированные системы управления производством начали развиваться как новый класс систем на рубеже столетий [1]. Особый интерес к таким системам проявляется после перехода России к рыночным отношениям. Вместе с тем этот класс адаптивных систем является специфическим, и для его формального системного описания не подходят существующие теоретические методы ни автоматизированного, ни автоматического управления. Потребовалось сформировать новые методы на основе исследования известных методов. Такая процедура потребовала применения системного анализа к изучению адаптивных систем, включающего процедуры определения системной цели функционирования, структуры и ее функционального наполнения.

Первые две процедуры рассмотрены в публикации [2], продолжением которой является настоящая статья.

Постановка задачи. Провести системное функциональное наполнение трехуровневой структуры [2] адаптивной системы. Для этого необходимо сформулировать требования к математическому описанию, провести анализ известных методов и построить новый метод, пригодный для исследования адаптивных систем.

Решение задачи. Особенности воздействия среды и автоматизированного управления предъявили специфические и порой жесткие требования к методам математического описания процессов:

1. Достаточная адекватность описания процессов, происходящих в реальной системе.

2. Учет многоуровневого характера структуры систем с изменением масштабов описания по времени и координатам.

3. Системность и наглядность метода математического описания и простота алгоритма приложения.

4. Интеграция процессов функционирования и адаптации с элементами интеллекта.

5. Поддержание оптимальных режимов работы с помощью компьютерной техники.

6. Системное описание процессов оптимального планирования и управления с учетом линейных ограничений.

7. Однородность (однотипность) системного описания процессов оптимального планирования и управления.

8. Согласование (векторных) экономических интересов и координация темпов работы целенаправленных элементов, что позволяет увеличить эффективность работы системы управления.

9. Малое время расчетов и возможность работы в реальном масштабе времени.

10. Совместная оценка экономических свойств (через экономический интерес) и управленческих свойств.

11. Учет неопределенности в получении данных при идентификации управляющей части системы.

12. Учет значительной доли неформальных процедур. При формировании описания возникает много неоднозначностей, которые приходится исследовать дополнительно.

В формировании математического описания адаптивной системы можно выделить следующие этапы:

1. Описание отдельного элемента без учета специфики уровней структуры.

2. Описание отдельного элемента с учетом специфики уровней.

3. Описание взаимодействия элементов.

Два последних этапа составляют методы системного (глобального) описания процессов в системе. Здесь ограничимся первым этапом.

Необходимо, следовательно, определить системный метод совместного описания разнородных по сути и структуре процессов планирования и управления.

Такое описание может быть двух видов:

- названные процессы описываются одним *однородным* методом;
- процессы представлены разными согласованными методами (*системный* или *интегральный* метод).

Как показал анализ методов, в литературе фактически отсутствует однородный метод. В связи с этим анализ методов описания процессов планирования и управления проведем порознь для последующего формирования системного метода.

Одной из первых работ по описанию многоуровневых систем явилась публикация [3]. В ней рассматривались лишь двухуровневые системы, а предложенный теоретико-множественный метод не позволял получать конструктивные результаты.

Первоначально для описания пытались использовать частотные методы систем автоматического управления, однако описание ограничивалось либо двумя уровнями [4] без учета горизонтальных связей, либо одним элементом на нижнем уровне [5]. Требованиям относительной автономности процесса планирования и оптимизации процессов при этом не уделялось внимания.

Другая группа работ [6]–[8] учитывала преимущественно динамику систем без учета требований оптимальности и процесса планирования. К тому же описание вертикального взаимодействия характеризовалось очень сложным алгоритмом со значительным привлечением неформальных процедур. Ввести интеллектуальность в такие математические модели весьма проблематично, а оценить экономические свойства и целенаправленность не представляется возможным.

К тому же работы [6], [8] имеют целью скорее исследование динамических свойств одноуровневой системы декомпозицией и переходом к двухуровневой структуре. Такие задачи являются согласованными по определению.

Применение таких методов, как оптимизация по силе, энергии, линейно-квадратичная оптимизация [9], сильно затруднено сложностью экономической интерпретации. Речь идет к тому же об описании отдельного структурного элемента, что затрудняет учет процедуры взаимодействия элементов.

Работа [10] посвящена процессу планирования в двух- и трехуровневых системах с так называемой веерной структурой, т. е. без учета горизонтальных связей.

Анализ известных методов показал, что сформулированным ранее требованиям не удовлетворяет ни один локальный метод. Следовательно, необходимо из локальных методов составить глобальные, предварительно более подробно ознакомившись с возможностями отдельных локальных методов.

Методы, пригодные для описания процессов планирования и управления, рассмотрим раздельно. В рамках данной статьи рассмотрим функцию планирования.

Планирование. Как упоминалось, в традиционных автоматизированных системах управления

производством решаются преимущественно задачи «прямого счета». При их использовании нельзя говорить даже о рациональном режиме работы системы, тем более – об оптимальном режиме.

В ERP-системах в дополнение к задачам «прямого счета» используются алгоритмы-ограничения.

Так, если a_{ij} – норма расхода материала на единицу продукции j, P_j – размер заказа клиента, b_i – наличное количество материала, то должно соблюдаться неравенство

$$\sum_{j=1}^{J} a_{ij} P_j \le b_j . \qquad (1)$$

Пусть t_{ij} – время изготовления детали j на оборудовании вида i; t_{kr} – время сборки изделия r на оборудовании вида k; P_j – план выпуска деталей (изделий); A_i – фонд времени работы оборудования.

Тогда при выпуске деталей (изделий) справедливо выражение

$$\sum_{j=1}^{J} t_{ij} P_j \le A_j . \qquad (2)$$

В то же время этот метод при последовательном рассмотрении выражений (1)–(2) имеет ограниченную сферу применения.

Итеративный характер расчета сильно затрудняет учет динамических изменений спроса и ресурсного обеспечения. Только ограничения на ресурсы не позволяют выявить лучшие режимы использования ресурсов даже при стабильном спросе.

Попытка описания многоуровневой схемы предпринималась в работе [7].

Пусть имеется модель, состоящая из K (k = 1, K) соединенных структурных элементов (подсистем). Ее частным случаем является модель с последовательным соединением подсистем. В этом случае возможно последовательное решение сначала для подсистемы 1, затем подсистемы 2 и т. д.

В более общем случае в силу однотипности структурных элементов можно математически описать лишь k-й элемент.

Тогда модель получает вид

$$\boldsymbol{y}_k = \boldsymbol{S}_k(\boldsymbol{M}_k, \boldsymbol{x}_k),$$

$$\boldsymbol{z}_k = \boldsymbol{T}_k(\boldsymbol{M}_k, \boldsymbol{x}_k),$$

где $\boldsymbol{x}_k$ – вектор входа структурного элемента; $\boldsymbol{y}_k$ – вектор выхода структурного элемента; $\boldsymbol{z}_k$ – вектор связей элементов; $\boldsymbol{T}_k$, $\boldsymbol{S}_k$ – векторные функции; $\boldsymbol{M}_k$ – вектор управления k-й подсистемы.

Могут существовать нелинейные ограничения, описываемые векторной функцией

$$\boldsymbol{h}_k (\boldsymbol{M}_k, \boldsymbol{x}_k, \boldsymbol{z}_k) \ge 0.$$

Взаимодействие структурных элементов определяется выражением

$$\boldsymbol{x}_k = \sum_{j=1}^{K} \mathbf{C}_{kj} \boldsymbol{z}_j ,$$

где $\boldsymbol{C}_{kj}$ – матрица соответствующего размера.

При последовательном соединении

$$\boldsymbol{x}_k = \boldsymbol{C}_{kk_1} \boldsymbol{z}_{k_1}.$$

Пусть целевая функция

$$F = \sum_{k=1}^{K} f_k (\boldsymbol{M}_k , \boldsymbol{x}_k) \to \max .$$

Цель: определить векторы $\boldsymbol{M} = \{\boldsymbol{M}_k\}$, $\boldsymbol{X} = \{\boldsymbol{x}_k\}$, k = 1, K, доставляющие максимум целевой функции.

Решение удобно выполнить, используя лагранжиан

$$L = \sum_{k=1}^{K} f_k (\mathbf{M}_k \mathbf{x}_k) + \sum_{k=1}^{K} \boldsymbol{\mu}_k^T (\mathbf{T}_k (\mathbf{M}_k \mathbf{x}_k) \mathbf{z}_k) +$$

$$+ \sum_{k=1}^{K} \mathbf{p}_k^T (\mathbf{x}_k \sum_{j=1}^{K} \mathbf{C}_{kj} \mathbf{z}_j) + \sum_{k=1}^{K} \gamma_k^T (\mathbf{h}_k (\mathbf{M}_k , \mathbf{x}_k , \mathbf{z}_k),$$

где $\boldsymbol{\mu}_k$, $\boldsymbol{p}_k$ – векторы множителей Лагранжа; γ_k – множители Куна–Таккера.

Пусть функции $\boldsymbol{T}_\text{k}$, $\boldsymbol{S}_k$, F непрерывны и имеют первые производные. Тогда максимум определяется с использованием лагранжианов.

Фактически процедуру решения одноуровневой задачи обращают в двухуровневую процедуру.

Нетрудно видеть, что методы связаны с частным случаем двухуровневых структур систем, при этом интервалы времени на разных уровнях одинаковы. Интегральное описание планирования и управления весьма затруднительно. Целевые функции уровней согласованы по самой постановке задачи, тогда как в адаптивной системе необходимо уметь согласовывать эти функции.

Более интересно применение статического линейного программирования (СЛП) при необходимости согласования целевых функций [10]. Общая постановка этой задачи имеет веерный вид. Имеется один элемент (Центр) на верхнем уровне

и K (k = 1, K) элементов (автономных производств, не имеющих горизонтальных связей) на нижнем уровне. Центр располагает ресурсом в количестве X_0, который необходимо распределить между производствами в количестве x_k в соответствии с их запросами s_k.

Элементы используют ресурсы с эффективностью $r_k f(x_k)$, где r_k – коэффициент эффективности; $f(x_k)$ – функция использования ресурсов.

Работа системы идет в условиях неопределенности. С одной стороны, Центр не знает точного значения r_k и судит о нем по диапазону изменения r_k и сообщениям s_k элементов. В общем случае может быть $r_k \neq s_k$.

С другой стороны, элементы не знают точного значения X_0 (дефицит или избыток).

Необходимо выработать закон взаимодействия Центра и элементов, чтобы соблюдалось условие $r_k = s_k$.

Центр руководствуется целевой функцией

$$\Phi = \sum_{k=1}^{K} f(\mathbf{x}_k) / s_k \rightarrow \min$$

при ограничении

$$\sum_{k=1}^{K} \mathbf{x}_k \leq X_0;$$

k-й элемент использует целевую функцию

$$\varphi_k = f(\mathbf{x}_k) / r_k \; \lambda \mathbf{x}_k \rightarrow \max,$$

где λ – цена единицы ресурса.

Возможны различные разновидности принципов работы системы, подробно описанные в [10].

В более поздних работах В. Н. Буркова рассматриваются специфические так называемые веерные трехуровневые структуры.

Заметим, что здесь речь идет о согласовании задач уровней, однако рассматриваются только вертикальные связи.

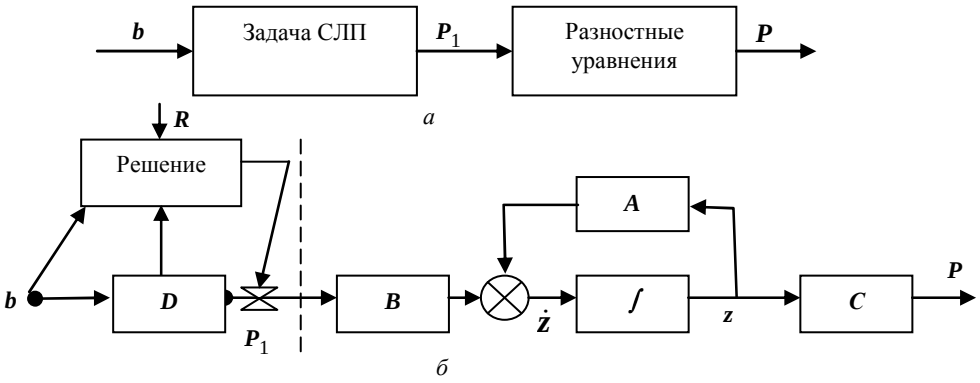
Более удобна другая форма задачи СЛП, решаемой при планировании производства:

$$\mathbf{DP}[\tau] \leq \mathbf{b}(\tau), \quad (3)$$

$$\mathbf{R}^{-}[\tau] \leq \mathbf{P}[\tau] \leq \mathbf{R}^{+}[\tau], \quad (4)$$

$$G(\mathbf{P}[\tau]) = \mathbf{FP}[\tau] \rightarrow \max, \quad (5)$$

где $\boldsymbol{D}$ – матрица норм расхода ресурсов; $\boldsymbol{P}$, $\boldsymbol{b}$, $\boldsymbol{R}$ – вектор-столбцы искомого плана, наличного количества ресурсов, спроса; $\boldsymbol{F}$ – вектор-строка прибыли за единицу готовой продукции; G – целевая функция; τ – интервал времени. Информационная схема задачи динамического линейного программирования представлена на рисунке: *а* – укрупненная, *б* – детальная).



Выражения (3)–(5) учитывает нелинейности и характерны для фиксированного интервала времени τ, но не охватывают возможную динамику процесса планирования.

Чтобы учесть динамику, необходимо к выражениям (3)–(5) добавить разностные уравнения перехода к последующим интервалам времени. При этом получается задача динамического линейного программирования (ДЛП).

Задача ДЛП тоже может быть представлена графически (рисунок, *а*). С учетом схемы динамической системы в пространстве состояний рисунок, *а* преобразуется в рисунок, *б*, на котором приняты следующие обозначения: $\boldsymbol{P}_1$ – вектор комплекта ресурсов; $\boldsymbol{z}$ и $\dot{\boldsymbol{z}}$ – вектор и его производная незавершенного производства; $\boldsymbol{A}$, $\boldsymbol{B}$, $\boldsymbol{C}$ – матрицы, характеризующие динамику процесса.

Штриховая черта на рисунке, *б* является границей между задачами, решаемыми аппаратом СЛП и ДЛП.

Таким образом, для формирования методов описания процесса планирования наиболее перспективны задачи СЛП и ДЛП.

СПИСОК ЛИТЕРАТУРЫ

1. Советов Б. Я., Цехановский В. В., Чертовской В. Д. Теория адаптивного автоматизированного управления. СПб.: Изд-во СПбГЭТУ «ЛЭТИ», 2009.

2. Советов Б. Я., Цехановский В. В., Чертовской В. Д. Проблемы адаптивного автоматизированного управления промышленным предприятием // Информационно-управляющие системы. 2009. № 6 (43). С. 18–24.

3. Месарович М., Мако Д., Такахара Я. Теория иерархических систем /Пер. с англ. М.: Мир, 1973.

4. Фаткин Ю. М. Оптимальное управление в иерархических структурах //ДАН АН СССР. 1972. Т. 202, № 1. С. 59–61.

5. Вавилов А. А., Чертовской В. Д. Система автоматического управления с самонастраивающимся по частотным характеристикам регулятором // Изв. АН СССР. Техн. кибернетика. 1968. № 6. С. 139–147.

6. Системы: декомпозиция, оптимизация и управление /Сост.: М. Сингх, А. Титли; Пер. с англ. М.: Машиностроение, 1986.

7. Цурков В. И. Динамические задачи большой размерности. М.: Наука, 1988.

8. Араки М., Икэда М., Иосикава Ц. Теория управления большими системами // J. Soc. Instrum. and Control Eng. 1983. № 10. С. 868–876.

9. Егоров А. И. Оптимальное управление линейными системами. Киев: Выща шк., 1988.

10. Бурков В. Н. Основы математической теории активных систем. М.: Наука, 1977.

B. Ya. Sovetov, V. V. Tsekhanovsky, V. D. Chertovsky, R. A. Nechitailenko

FORMING OF THE MATHEMATICAL DESCRIPTION OF MULTILEVEL ADAPTIVE AUTOMATED PRODUCTION CONTROL SYSTEM AT THE PLANNING STAGE

Requirements are considered methods of the description of three-level adaptive automated systems of management (AASM). Analysis of the local methods of description, proposed global mathematical methods of investigation of AASM.

Adaptive management, analysis methods, choice of methods, formation, global description, planning, requirements to methods