В криптографии с открытым ключом эллиптические кривые являются основой ряда алгоритмов ECC – криптографии на эллиптических кривых. Ряд авторов для краткости называют ее просто эллиптической криптографией [3]. Интерес в криптографии к эллиптическим кривым обусловлен, с одной стороны, тем, что они являются богатым источником конечных абелевых групп, обладающих полезными структурными свойствами, с другой – тем, что на их основе обеспечиваются те же криптографические свойства, которыми обладают числовые или полиномиальные криптосистемы, но при существенно меньшем размере ключа.

Для решения задачи создания модели защиты автоматизированной системы от несанкционированного доступа предполагается построить математическую модель защиты автоматизированного рабочего места, которая будет включать в себя комплекс программ либо программную среду. Перед началом выполнения работы необходимо выделить существенные для построения модели параметры, а также определить их оптимальное количество.

После выполнения обозначенных выше пунктов предполагается исследовать область применимости построенной модели защиты, а также провести анализ работоспособности данной модели.

Библиографические ссылки

1. *Hashizume Naoki*, *Momose Fumiyuki*, *Chao Jinhui.* On Implementation of GHS Attack against Elliptic Curve Cryptosystems over Cubic Extension Fields of Odd Characteristics. – 2008.

2. *Brown Daniel R. L.* The Encrypted Elliptic Curve Hash. – 2008.

3. Элементарное введение в эллиптическую криптографию. Алгебраические и алгоритмические основы / А. А. Болотов [и др.]. – М. : КомКнига, 2006. – 328 с.

O. O. Karpova, Candidate for a Degree, Perm State Technical University
L. N. Krotov, Doctor of Physical and Mathematical Sciences, Professor, Perm State Technical University
E. L. Krotova, Candidate of Physical and Mathematical Sciences, Perm State Technical University
A. E. Osipovich, Student, Perm State Technical University

Approach to the Construction of Models of Protection of Automated Systems from Unauthorized Access

The main problem of constructing a model of protection of automated systems from unauthorized access are presented. A part of the job for software development required to reach one of the goals is formulated.

Key words: mathematical modeling, automatic control theory, information security.

УДК 65.011.46

M. Jurova, Cand. Sc., Brno University of Technology
E. Chytilova, PhD student, Brno University of Technology
T. Supina, PhD student, Brno University of Technology

THE DEVELOPMENT OF COMPETITIVENESS OF INDUSTRY ENTERPRISES IN CONDITIONS OF EUROPEAN UNION

The current status of industry in European Union and possibilities of its development are considered. The modern trends in optimization of planning and realization of manufacturing are described. In comparing with other countries of European Union we have still a lot of places for improvements, mostly in material and wage savings. The optimization of production tools is still not so popular to bring results in lower costs. Authors focused on modern trends, such as theory of constraint, optimized production technology, advanced planning and scheduling and other.

Key words: industry enterprises, European Union, competitiveness, theory of constraint (TOC), optimized production technology (OPT), just-in-sequence (JIS), single minute exchange of dies (SMED), advanced planning and scheduling (APS), Heuristic Factory Planning Algorithm (HFPA).

Industry is important sector of the national economy. Industry influences in important rate of development and positive routing in individual regions. Industrial production is that part of material transformation, which includes machine process of raw material extraction and obtained agricultural products, conveyances, electronic, pharmaceutical products, plastic and wooden products, etc. Scope of work for industry production isn't coincidence. The share on gross domestic product (hereinafter referred to as GDP) of country speak about significant of this topic.

For example, in Slovakia industrial production hold important place from the point of view inhabitant employment rate, in year 2009 worked in this economy branch 21,04 % working people, what present 497 833 people (in year 2008 it was 24,08 %). The research of ways optimization manufacturing is one of actual themes in current conditions of European business.

Получено 29.06.11

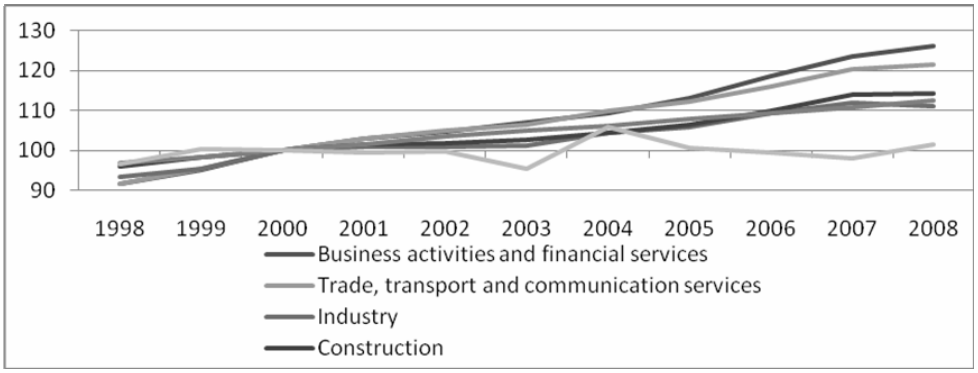

Fig. 1. Gross value added, EU-27
From: Europe in figures – Eurostat yearbook 2010 [1]

Materials and methods

1. Development of productivity rate in industry production

In one of tools for measure of amount use sources is productivity rate. Simplest formula for measure of productivity is in general given as quotient of outputs and inputs. It´s also possible to measure it as share falling for one employee, as well as on company level. In production companies we can see percentage expression of direct and indirect productivity rate where is amount of standard hours in local production department divided by amount of done hours direct and indirect employees. For comparing of development in productivity rate of industrial production, the productivity rate is expressing by receipts volume of own function and estate, which is made by one employee in industry per year.

2. Modern trends of increase of competitiveness

2.1. *The theory of constraint*

The theory of constraint (TOC) proposed by Dr. Goldratt emphasizes on the systematic management of project by discovering the uncertain factors hindering the project implementation, and suggests the global deployment of resources The concept of thinking globally and acting locally recommends the use of the global safety time and the reduction of the activity duration. However, a practical method to reduce the activity time and exert the management control remains nonexistent [7].

TOC uses the global safety time to schedule the project, and stresses that a system must have a constraint. Otherwise, its output would increase without the upper bound. Thus, TOC project management focuses on the constraint that blocks the achievement of goal of the project. Five steps used to apply the TOC skill to the project scheduling are given below:

1. Identify the project constraint.

2. Exploit the project constraint.

3. Subordinate everything else to the project constraint.

4. Elevate the project constraint, and

5. If, in the previous step, a new constraint has been uncovered, repeat the process. Do not let inertia become the project constraint [7].

2.2. *Optimized Production Technology* (OPT)

Production scheduling and inventory control system that (unlike manufacturing resource planning) recognizes bottlenecks (capacity constraints) and does not aim at full capacity utilization at all times. OPT's objective is to simultaneously raise throughput while reducing inventory and operating costs, and achieve a smooth, continuous flow of work in process [5].

2.3. *Just-in-sequence (JIS)*

Just in Sequence (JIS) is an inventory strategy that matches Just In Time and complete fit in sequence with variation of assembly line production. Components and parts arrive at a production line right in time as scheduled before they get assembled. Feedback from the manufacturing line is used to coordinate transportation to and from the process area. When implemented successfully, JIS improves a company's return on assets (ROA), without loss in flexibility, quality or overall efficiency. JIS is mainly implemented with automobile manufacturing [6].

Just in Sequence (JIS) is just one specialized strategy to achieve Just In Time (JIT). The process concept of JIT sees buffers at the production line as waste in capital bound. The aim is to eliminate buffers as much as possible at expense of stability when disturbances arise. Just In Sequence is one of the most extreme applications of the concept, where components arrive Just In Time and sequenced for consumption.[6]

2.4. *Single Minute Exchange of Die* (SMED).

Single-Minute Exchange of Die (SMED) is one of the many lean production methods for reducing waste in a manufacturing process. It provides a rapid and efficient way of converting a manufacturing process from running the current product to running the next product [4].

There are seven basic steps to reducing changeover using the SMED system:

1. OBSERVE the current methodology (A)

2. Separate the INTERNAL and EXTERNAL activities (B). Internal activities are those that can only be performed when the process is stopped, while External activities can be done while the last batch is being produced, or once the next batch has started. For example, go and get the required tools for the job BEFORE the machine stops.

3. Convert (where possible) Internal activities into External ones (C) (pre-heating of tools is a good example of this).

4. Streamline the remaining internal activities, by simplifying them (D). Focus on fixings – Shigeo Shingo

rightly observed that it's only the last turn of a bolt that tightens it – the rest is just movement.

5. Streamline the External activities, so that they are of a similar scale to the Internal ones (D).

6. Document the new procedure, and actions that are yet to be completed.

7. Do it all again: For each iteration of the above process, a 45 % improvement in set-up times should be expected, so it may take several iterations to cross the ten minute line [4].

2.5. *APS (Advanced Planning and Scheduling)*

APS takes into account constraints at enterprise level as well as at plant level. Materials and capacity issues are considered simultaneously, and manufacturing, distribution, and transportation issues are integrated. The APS planning engine is based on an optimization algorithm and a constraint-based planning algorithm. This enables companies to optimize plans according to financial and other strategic objectives of the enterprise and to create plans which satisfy multiple objective goals. Unlike traditional ERP systems, APS seeks to find feasible, near optimal plans while potential bottlenecks are considered explicitly. Many ERP and APS systems make it possible to include suppliers and customers in the planning procedure and thereby optimize a whole supply chain on a real-time basis. Unfortunately, no common (accepted) definition of APS systems exists, and several systems on the market do not fulfill the description above [2].

APS aim at automating and computerizing the planning processes by use of simulation and optimization. Still, the decision-making is done by planners with insight in the particular supply chain and know how on the system constraints but likewise important: a feeling for feasibility of created plans. Thus, APS aim to bridge the gap between the supply chain complexity and the day-to-day operative decisions. This requires, however, that planners are able to model and setup decision rules for the planning and optimization [2].

2.6. *Heuristic Factory Planning Algorithm- HFPA*

Planning work carried out gradually according to a predetermined order in accordance with the "preference", in which the algorithm immediately assigns the job to the machine, as work is available for planning. This means that when an individual works can be scheduled in the most appropriate moment, the single function (work) will be relocated at the end of the queue and wait for the next iteration. Given that the HFPA plan to work gradually without flinching, the work can be rescheduled in the event that a capacity has been allocated a machine. For this reason, grouping and sorting jobs can have a significant influence on the planning results [3].

To schedule the most business center for some time, the HFPA has used up most overloaded work, the so-called "bottleneck" work center, the planning of works. Therefore, HFPA has three-stage grading work center, sort of work and planning the work, with a total of five steps, one in each of the first two stages and three in the third [3].

These steps are listed below:

(P1) Sort work centers using the HFPA sorting mechanism.

(P2) Group and sort jobs using the HFPA grouping and sorting mechanism.

(P3) Scan the queue three times, each time scheduling some of the jobs using the bottleneck-oriented scheduling algorithm (BOSA).

(P3-1) Activate BOSA to schedule jobs one by one according to the sequence determined in (P2). If a job can be scheduled in its preferred interval without being preempted, schedule the job accordingly. Otherwise, put the job back into the queue.

(P3-2) After the regular scheduling, activate BOSA to schedule the jobs that were put back into the queue in (P3-1). If a job can be scheduled in its preferred interval with preemption, schedule the job accordingly. Otherwise, put the job back into the queue.

(P3-3) After the regular scheduling and the first rescheduling, activate BOSA to schedule jobs that were put back into the queue again in (P3-2). Advance and/or delay each job in order to find sufficient work center capacity for it [3].

Results and future work

On fig. 2 are shown variants of applying everyone from presented modern trends to several type of production.

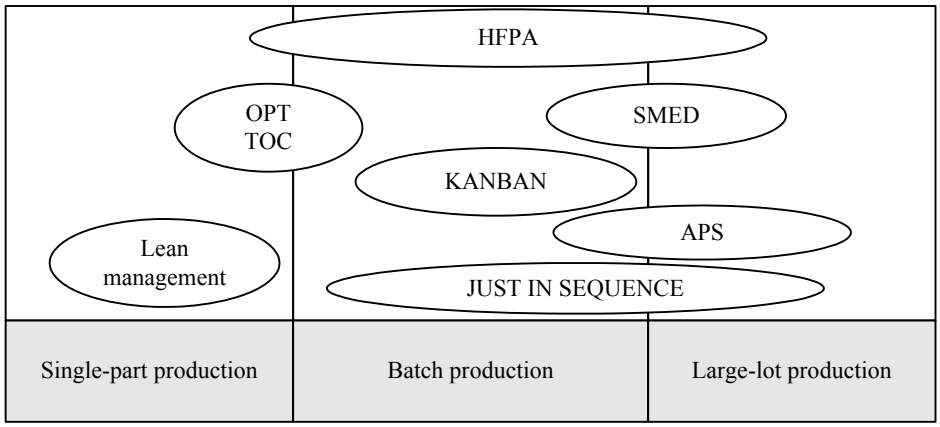

Fig. 2. Applying of modern trends in different types of production
Source: own research

HFPA is useful in the case single-part production, batch production and large-lot production. Lean management is useful for single-part production. SMED, APS, Just in sequence are useful for batch production and large-lot production. Kanban philosophy is useful in the case batch manufacturing. OPT, TOC are useful for single-part and batch manufacturing. In future authors will focus on research on limitations and conditions of every one of presented trends.

Actually, in the global competition, quick development of industry and technique is essential to research differences and conditions applying modern trends for industrial firms.

Authors plan primary research in Czech Republic about conditions and limitations of applying modern trends.

References

1. Europe in figures – Eurostat yearbook 2010. – URL: http://epp.eurostat.ec.europa.eu/cache/ITY_OFFPUB/CH_01_2010/EN/CH_01_2010-EN.PDF

2. *Hvolby H.-H.*, *Steger-Jensen K.* Technical and industrial issues of Advanced Planning and Scheduling (APS) systems // Computers in Industry. – 2010. – Vol. 61. – No. 9. – P. 810.

3. *Kung L.-C.*, *Chern C.-C.* Heuristic faktory planning algorithm for advanced planning and scheduling // Computers & Operations Research. – 2009. – No. 36. – P. 2513–2530.

4. *Shingo S.*, *Dillon A. P.* A Study of the Toyota Production System: From an Industrial Engineering Viewpoint (Produce What Is Needed, When It's Needed). – 1989.

5. *Verma R.* Management science, theory of constraints/optimized production technology and local optimization // Omega. – 1998. – Vol. 25, 2, doi: 10.1016/S0305-0483(96)00060-6.

6. *Wagner S. M.*, *Silveira-Camargos V.* Decision model for the application of just-in-sequence // Decision Sciences Institute Proceedings of the 40th annual conference. – New Orleans, USA, 2009.

7. *Wei C.-C.*, *Liu P.-H.*, *Tsai Y.-C.* Resource-constrained project management using enhanced theory of constraint // International Journal of Project Management. – 2002. – No. 20. – P. 561–567.

М. Юрова, CSc, Технологический университет г. Брно, Чехия
Е. Хитилова, аспирант, Технологический университет г. Брно, Чехия
Т. Шупина, аспирант, Технологический университет г. Брно, Чехия

Развитие конкурентоспособности промышленных предприятий в условиях Европейского Союза

Рассмотрено текущее состояние промышленности в странах Европейского Союза. Описаны современные тенденции в области оптимизации планирования и производства. В Чехии по сравнению со странами Европейского Союза имеется возможность модернизировать производство, главным образом, в области экономии материалов и заработной платы. В статье уделяется особое внимание современным тенденциям, таким как теория ограничений, оптимизация технологии, перспективное планирование и диспетчеризация и другие.

Ключевые слова: промышленное предприятие, Европейский Союз, конкурентоспособность, теория ограничений (TOC), оптимизированная технология производства (OPT), система «точно по графику» (JIS), система быстрой замены пресс-форм (SMED), перспективное планирование и диспетчеризация (APS), эвристический алгоритм планирования работы предприятия (HFPA).

УДК 004.04

Ю. Ф. Рубцов, кандидат технических наук, Пермский национальный исследовательский политехнический университет

ИССЛЕДОВАНИЕ ОБЩИХ ПОДХОДОВ К ОПТИМИЗАЦИИ МОДУЛЬНОЙ СТРУКТУРЫ ОБРАБОТКИ ИНФОРМАЦИИ В АВТОМАТИЗИРОВАННОЙ СИСТЕМЕ КОНТРОЛЯ И ИСПЫТАНИЙ

Показано, как на основе использования концепции виртуального измерительного канала достигается оптимизация системы коррелированных функций многих переменных. Решается задача оптимизации в рамках заданной архитектуры системы и выбранном техническом базисе.

Ключевые слова: критерий, оптимизация, погрешность, канал, функции, тракт, параметры.

Задача исследования любого конкретного варианта автоматизированной системы испытаний (АСИ) включает в себя составление математической модели как совокупности основных уравнений, связывающих свойства источников, параметры системы (q, $t_{го}$, $t_{ги}$, …) и критерий качества функционирования, исследование этих уравнений с целью оптимизации параметров рассматриваемой системы, определяющей принятый критерий [1].

Критерий оптимизации $\bar{\delta}^2_{изi}$ зависит от свойств источников сообщений (M_{p+1}, P_{oj}), параметров АСИ (q, $t_{го}$, $t_{ги}$, …). При этом часть переменных характеризует состояние входных сигналов (M_{p+1}) и воздейст-

Получено 15.08.11