DEVELOPMENT OF A PROJECT FOR ADVANCED TRAINING COURSES IN THE MS PROJECT PROGRAM

Fazylova L.S.
Karaganda Buketov University, Karaganda, Kazakhstan
E-mail: Leyla.fazylova@mail.ru

Methods of business process analysis, project management are currently the most important tools for improving business efficiency.

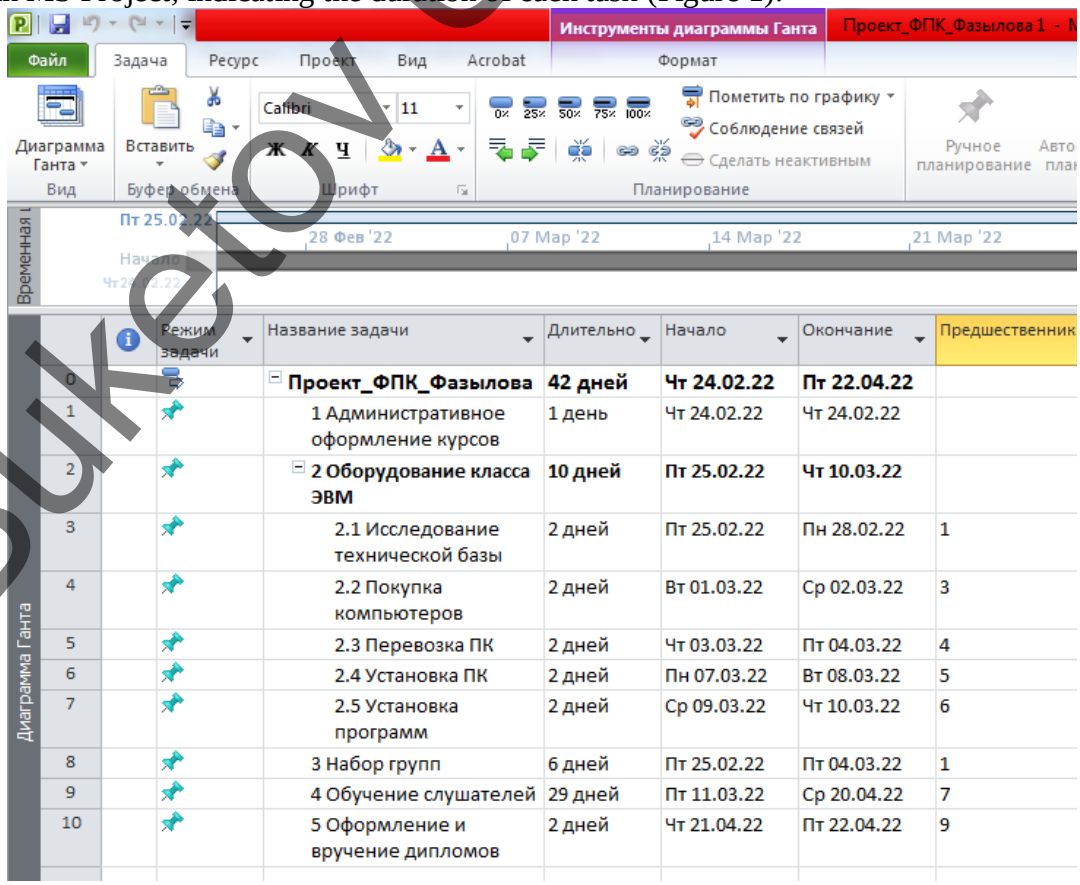
Optimization of project activities in an organization is possible through the introduction of project management systems, the use of modern tools, methods of planning and project control, the application of knowledge and world experience in project management.

Effective project management is the integration of software with management procedures and organizational structure. Currently, there are hundreds of different project management automation tools on the software market. Despite the functional differences of the programs, all of them allow you to build a network schedule, calculate the start and end dates of work, determine the critical path and cost of the project [1].

Project management in Microsoft Project is based on the basic principles of project planning and management, as well as on the skillful use of standard tools and tools of the program.

This paper discusses the creation of a project for advanced training courses for employees of an educational center. Emphasis is placed on the structural planning of the project, the assessment of the cost of the project, its resources and tasks.

A work plan was drawn up in advance. According to the plan, a structured list of tasks was compiled in MS Project, indicating the duration of each task (Figure 1).



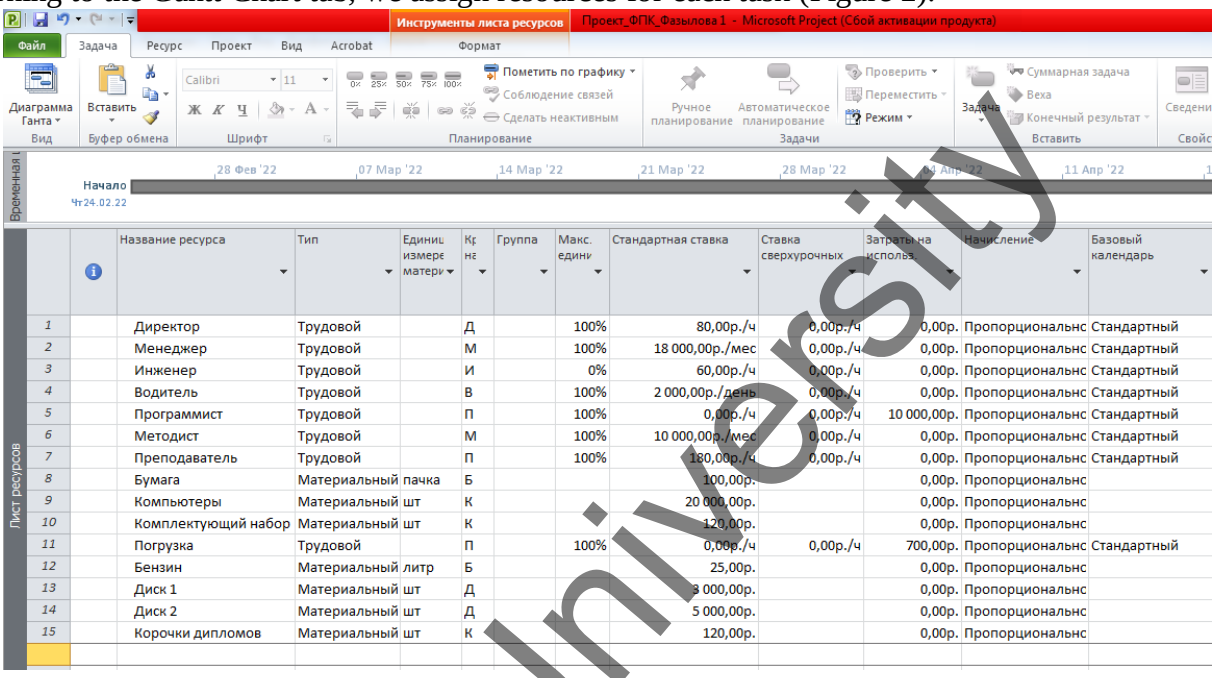
	Режим задачи	Название задачи	Длительность	Начало	Окончание	Предшественники
0		**Проект_ФПК_Фазылова**	**42 дней**	**Чт 24.02.22**	**Пт 22.04.22**	
1		1 Административное оформление курсов	1 день	Чт 24.02.22	Чт 24.02.22	
2		**2 Оборудование класса ЭВМ**	**10 дней**	**Пт 25.02.22**	**Чт 10.03.22**	
3		2.1 Исследование технической базы	2 дней	Пт 25.02.22	Пн 28.02.22	1
4		2.2 Покупка компьютеров	2 дней	Вт 01.03.22	Ср 02.03.22	3
5		2.3 Перевозка ПК	2 дней	Чт 03.03.22	Пт 04.03.22	4
6		2.4 Установка ПК	2 дней	Пн 07.03.22	Вт 08.03.22	5
7		2.5 Установка программ	2 дней	Ср 09.03.22	Чт 10.03.22	6
8		3 Набор групп	6 дней	Пт 25.02.22	Пт 04.03.22	1
9		4 Обучение слушателей	29 дней	Пт 11.03.22	Ср 20.04.22	7
10		5 Оформление и вручение дипломов	2 дней	Чт 21.04.22	Пт 22.04.22	9

Figure 1

The duration of each task is displayed on the Gantt chart.

One of the main tasks of project planning is to estimate as accurately as possible the timing and cost of the work required to achieve the project goal. After a list of project tasks is compiled, the duration of each of them is estimated and the resources necessary for their implementation are allocated.

To compile a list of resources, you need to go to the "Resource List" tab in MS Project. Returning to the Gantt Chart tab, we assign resources for each task (Figure 2).



	Название ресурса	Тип	Единиц измере матери	Кр на	Группа	Макс. едини	Стандартная ставка	Ставка сверхурочных	Затраты на использ	Начисление	Базовый календарь
1	Директор	Трудовой		Д		100%	80,00р./ч	0,00р./ч	0,00р.	Пропорциональнс	Стандартный
2	Менеджер	Трудовой		М		100%	18 000,00р./мес	0,00р./ч	0,00р.	Пропорциональнс	Стандартный
3	Инженер	Трудовой		И		0%	60,00р./ч	0,00р./ч	0,00р.	Пропорциональнс	Стандартный
4	Водитель	Трудовой		В		100%	2 000,00р./день	0,00р./ч	0,00р.	Пропорциональнс	Стандартный
5	Программист	Трудовой		П		100%	0,00р./ч	0,00р./ч	10 000,00р.	Пропорциональнс	Стандартный
6	Методист	Трудовой		М		100%	10 000,00р./мес	0,00р./ч	0,00р.	Пропорциональнс	Стандартный
7	Преподаватель	Трудовой		П		100%	180,00р./ч	0,00р./ч	0,00р.	Пропорциональнс	Стандартный
8	Бумага	Материальный	пачка	Б			100,00р.		0,00р.	Пропорциональнс	
9	Компьютеры	Материальный	шт	К			20 000,00р.		0,00р.	Пропорциональнс	
10	Комплектующий набор	Материальный	шт	К			120,00р.		0,00р.	Пропорциональнс	
11	Погрузка	Трудовой		П		100%	0,00р./ч	0,00р./ч	700,00р.	Пропорциональнс	Стандартный
12	Бензин	Материальный	литр	Б			25,00р.		0,00р.	Пропорциональнс	
13	Диск 1	Материальный	шт	Д			3 000,00р.		0,00р.	Пропорциональнс	
14	Диск 2	Материальный	шт	Д			5 000,00р.		0,00р.	Пропорциональнс	
15	Корочки дипломов	Материальный	шт	К			120,00р.		0,00р.	Пропорциональнс	

Figure 2

The Gantt chart shows all resource assignments.

Then the cost and terms of each task are specified. After adding these parameters, you can estimate the total cost and duration of the project. In the tab "Project Details" / "Statistics" we get information about the labor costs and the total cost of the project (Figure 3).

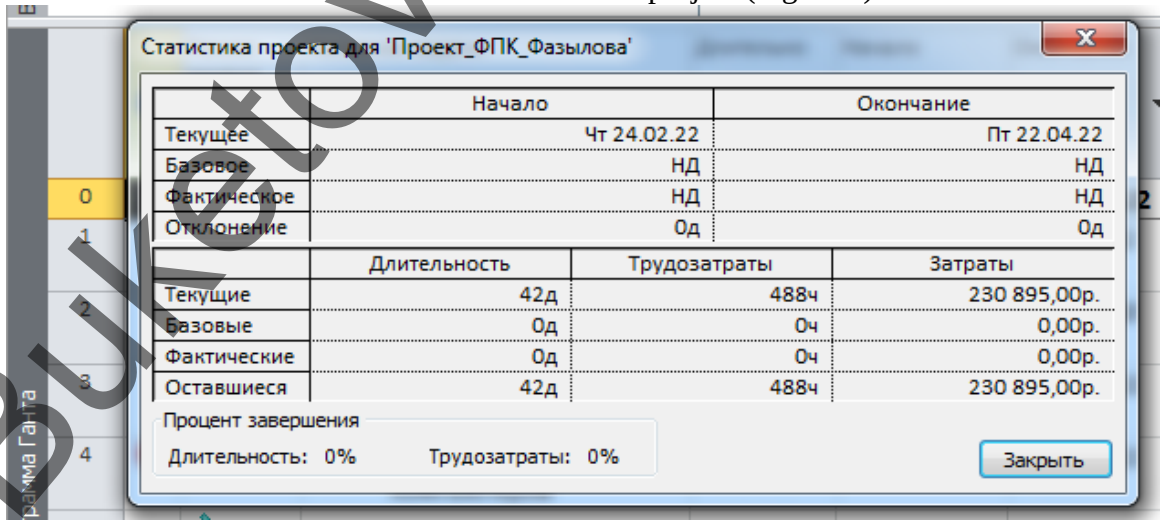


Figure 3

The practice of carrying out work on the description of business processes in various companies has shown that there is a great need to use a simple and inexpensive software product that is easy to learn and allows you to quickly and efficiently simulate various aspects of the business.

References

1. Shevtsova L.N. Project workshop: textbook / L.N. Shevtsova; Krasnoyarsk State Agrarian University. - Krasnoyarsk, 2016. - 107p.

THE AVALANCHE EFFECT OF A NOVEL STREAM CIPHER WITH A 3D SPONGE STRUCTURE

Ikramov A. [1,2], Juraev G. [2]

[1]*Institute of Mathematics of Academy of Sciences of Uzbekistan, Tashkent, Uzbekistan*

[2]*National University of Uzbekistan, Tashkent, Uzbekistan*

E-mail: a.ikramov@mathinst.uz

Abstract

We develop the special stream algorithm based on the SPONGE structure in order to obtain a secure and fast symmetric encryption algorithm. We research the avalanche effect to decide the number of rounds of the algorithm. The algorithm uses a secret key of 512 or 1024 bits and produces the key stream consisting of blocks of 2048 bits each.

Introduction

Both the Republic of Kazakhstan and the Republic of Uzbekistan does not have their own standardized stream cipher and relies on methods provided by manufacturers of hardware. Block symmetric encryption algorithms are not good with transmission of large data in real time. For example, streaming video or audio in encrypted mode is only possible with stream ciphers. Thus, the development of a new stream cipher is an actual problem for our countries.

The perfect stream cipher should act as random number generator. Pseudo-random number generators built with algorithms such as RC4 [2] are generally significantly faster than those based on block ciphers. The RC4 algorithm is widely used in various information security systems, in computer networks (for example, in the SSL protocol, for encrypting passwords, etc.). The development of a new approach to hash functions introduced with Keccak (or SHA-3) has led to an increasing interest in using SPONGE structures in other cryptographic applications [1]. The popular stream cipher RC4 was modified to use SPONGE structure and was called Spritz [2]. The resulting algorithm is more robust than the initial RC4. While non-linear operations in Keccak are simple, we focused on already established S-box used in AES.

The SPONGE structure itself represents a large array (usually 2-D or 3-D) that consumes data gradually and returns a small piece of stored information. The size of the array is designed to be so large that it is practically impossible to brute-force it. As the returning data is not enough to reconstruct the internal state the whole structure becomes practically irreversible for intruders. We continue our research of SPONGE structured stream cipher [4].

Design of a new stream cipher

We designed our stream cipher as a SPONGE structure with internal state's shape of $17 \times 16 \times 32$ bits. We address each bit within internal state using $S_{i,j,t}$, where $i \in \{0,1,2,\dots,16\}, j \in \{0,1,2,\dots,15\}, t \in \{0,1,2,\dots,31\}$. Another representation of the same internal state is $B_{i,j,p} \in \{0,1,2,\dots,255\}^{17\times16\times4}$ where each number is stored in exactly one byte.

Each round consists of the following operations in the given order:

1. Adding Input. We use XOR (exclusive OR) to add an array of the same size as the internal state:

$$S = S \oplus Input$$

2. Substitution. As was mentioned above, we selected AES substitution table as Sbox for our cipher. This is the only non-linear operation of the cipher. This substitution table provides security against linear and differential cryptanalysis [8]. We previously analyzed other substitution tables [9, 10, 11].

Each byte in the internal state is replaced with its corresponding substituted value:

$$B_{i,j,p} = Sbox(B_{i,j,p})$$