Assurance Quality and Efficiency in Corporate Information Systems

Ahmad AbdulQadir AlRababah
Faculty of Computing and Information Technology, King Abdulaziz University, Rabigh 21911, Kingdom of Saudi Arabia

Summary
The activity of any modern corporation is based on information technologies, where the main processed products are information. The analysis of corporate information systems is conducted from the point of view of ensuring their survivability. Therefore, one of the most important properties that CIS should possess is its survivability. CIS, which has the property of survivability, in the event of abnormal situations allows using the necessary elements to protect its functioning and ensure the stable operation of the corporation in additional to achieve the quality of their results and their ability to compete. The tasks of the survivability system for various provisions of the corporate information system are considered. The basic structure of the system for ensuring the survivability of the corporate information system is proposed. In this paper, we describe the main ways of giving information system survivability properties and provide a general description of the system designed for this.

Key words:
corporate information system, survivability system, corporation, survivability, survivability methods, survivability system structure, hardware, software, information support, information protection.

1. Introduction

One of the most effective forms of management in a market economy is the organizational form of the enterprise, such as a corporation, the target association of enterprises to improve the efficiency of their joint functioning. A special role among information technologies is played by the technology of organizational management. It is possible to define information technology as processing methods and organizational and managerial concepts of the formation and use of information, as well as the aggregate of all types of information technology; unity of procedures for collecting, storing, storing, processing and transmitting data using a certain set of technical means. Therefore, along with the concept of "corporation", such a notion as the "corporate information system" (CIS) has emerged and is widely used.

Strictly formulate the definition of CIS is rather difficult, since the very concept of "corporation" is too broad, so in the future we will mean that we are considering an information system that permeates all the components that determine the functioning of the corporation. In particular, the CIS includes a distributed corporate complex of technical means, corporate communication network, distributed corporate database, corporate subsystem of document circulation, corporate subsystem of decision support, etc. In other words, we define the CIS as an integrated system of methodical, software and hardware, information and organizational tools that support the life of the corporation.

In modern conditions, the life of a corporation is unthinkable without the use of CIS. The inefficient organization of the work of the CIS countries threatens significant losses for the corporation.

2. The survivability of CIS

In the classical definition, the survivability of a system is its ability to adapt to new, changed and, as a rule, unforeseen situations, to withstand adverse effects, while fulfilling its objective function at the expense of a corresponding change in the structure and behavior of the system [2]. Vitality can be considered as a property characterizing the ability of the system to function effectively when getting injuries (destruction) or restore this ability for a given time [4]. In other words, the technical, software, information, methodological, linguistic and organizational support of the CIS should contain such means that would allow to react in a certain way to the emergence of a situation leading to deterioration in the quality of functioning, and to ensure the continued operation of the CIS.

In view of the complexity of the task of ensuring survivability, its solution by one-off concrete measures is impossible. A continuous directed system of certain actions is needed that would be carried out throughout the life cycle of the CIS [5]. The complexity of giving KIS the vitality is explained in many ways by the complexity of the business processes taking place in the corporation and, as a consequence, by the complexity of modern information systems that are designed to automate these business processes.

In the simplest case, the concept of survivability is synonymous with fault tolerance, reliability and protection of hardware and software systems. However, the property of vitality fully manifests itself when the resources of these properties are exhausted. Thus, the concept of survivability includes the concepts of

Manuscript received April 5, 2019
Manuscript revised April 20, 2019

reliability, security and fault tolerance, but is not limited to these concepts.

Provision of vitality is also complicated because in today's conditions the modern system itself can generate new functions that were not laid in either the technical task or the design of the system, let alone the inadequate response to the occurrence of various unforeseen situations. This is due, for example, to factors such as:

- considerable dispersion of hardware;
- many distributed points of interaction with the user;
- extensive user interaction with the system;
- interaction with other automated systems;
- interaction with systems with decentralized management and administration,

In such conditions, the vitality of the CIS can be ensured only by special means, which are organically inscribed in the CIS itself.

Let us consider in more detail the critical places of the CIS, where the means of ensuring survivability should take effect at the right moment. From the structural point of view, the CIS consists of subsystems, each of which has the architectural structure of an independent system (Figure 1)

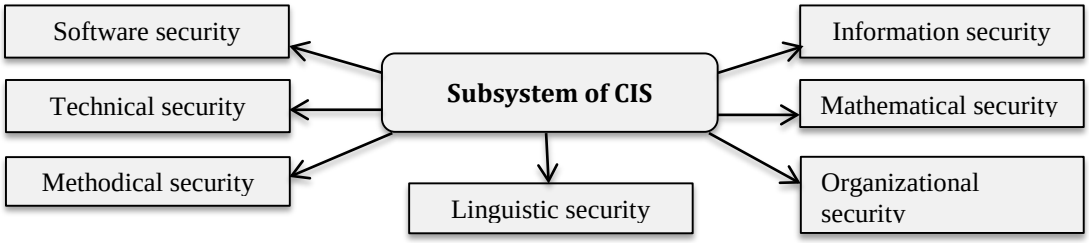

Fig. 1 Components of the CIS subsystem

The survivability of CIS should be differentiated for each subsystem and be provided at the level of each of its components. At the same time ensuring the sustainability at the level of each component of the subsystem should not be carried out autonomously, without taking into account the survivability mechanisms for the other components of the subsystem and for the CIS as a whole. The vitality of the CIS countries implies the existence of a functioning technological cycle shown in Fig. 2, special means of ensuring vitality for each components of the system.

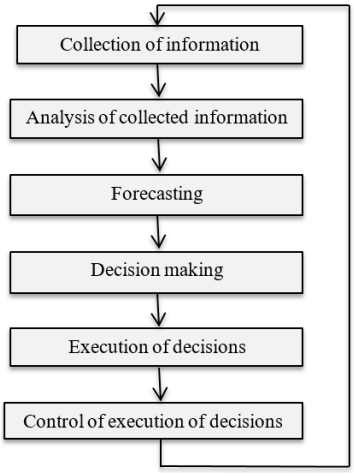

Fig. 2 Technological cycle of functioning means for ensuring the survivability of CIS

Let us consider in more detail the stages of this technological cycle: Collection of information. At this stage, information is collected in two types:

I. Information on the internal state of the CIS, such as congestion and disruptions hardware software, availability of free resources of communication networks, storage devices, integrity and consistency of information stored in databases, etc.;

II. Information on the external environment in which the CIS operates, on the impact of the external environment on the CIS and CIS on the external environment. There is information such as statistics of active connections to the system, information transferred from the external environment to the system, information originating from the system to the external domains.

All collected information is centrally formalized, classified and prepared for the next stage:

Analysis of collected information

The input for this stage is the information gathered at the first stage. The purpose of this stage is statistical and expert processing and analysis of input data to obtain an assessment of the current state of individual security, modules and subsystems of CIS, CIS and external environment according to some specialized criteria. In

addition, the deviations of the current state of the system from the project are estimated.

Forecasting

At this stage, the dynamics of changes in the state of collateral, software and hardware systems and subsystems of CIS, and also CIS countries as a whole is predicted. In addition, forecasts are generated for changing the state of the external environment and its interaction with the CIS. Forecasting is performed on the basis of assessments of the current states of the CIS and the external environment, as well as deviations of the CIS from the project state, which were obtained at the previous stage of the technological cycle.

Decision making

At this stage, decisions are made to counteract external and internal adverse impacts, both observed and forecasted at the third stage of the technological cycle. The prepared decisions can determine measures for reorganizing, reconfiguring and reconstructing the internal structure of the components of the system and the system as a whole, as well as measures to change the order and rules of interaction with the external environment, including obtaining and providing information. First of all, the system should be able to develop preventive solutions based on the data obtained at the forecasting stage. Such decisions would avoid the consequences of the majority of adverse effects on the system and ensure the regular conditions for its operation.

Execution of decisions

At this stage, special solutions for survivability are used to implement the solutions developed at the previous stage of the CIS technological cycle. The main requirements at this stage are the efficiency and reliability of the execution tools.

Control of execution of decisions

The final stage of the technological cycle of the functioning of the means of ensuring the survivability of the CIS is the control of the execution of decisions. At this stage, the quality of execution of decisions is analyzed and primary data on the reaction of the internal and external environment of the CIS to these decisions are collected. Based on these data, for several iterations of the technological cycle, adaptation of the CIS and its means of ensuring survivability to new operating conditions can be carried out.

The means of ensuring the vitality of the CIS should function continuously and continuously. This requirement is determined by a constant change in the conditions of operation of the CIS and occurrence of unforeseen influences both from outside and internal environment of the CIS.

To determine and systemize means of ensuring survivability, it is first of all necessary to consider the technological process, interaction with it (Figure 3). The term "external environment" includes:

- Global networks to which it is connected CIS, i.e. networks connected to the CIS by some communication channels, but not subject to the internal administrative policy of the CIS;
- Users of the system as external, interacting with the system through global networks, the entry points of which do not comply with the internal administrative policy of CIS, and internal, the entry points of which are part of the internal network of CIS and fully subject to its administrative policy;
- External automated systems (AS) with which the CIS is interacting, for example, information systems of partner corporations that have their own internal administrative policies that do not coincide with the CIS's administrative policy.

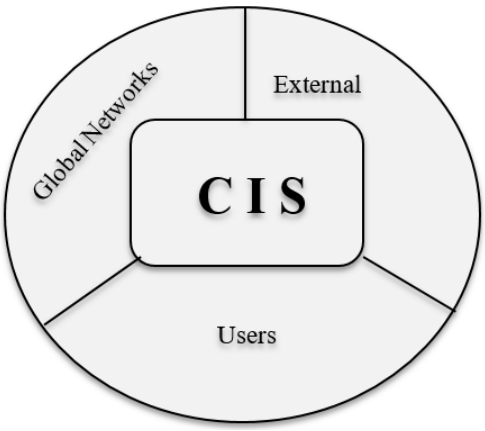

Fig. 3 External environment of functioning

CIS does not function autonomously; it is both a consumer and a provider of information in relation to the external environment. Thus, CIS can be represented as an information reservation with internal information flows, business rules, subject to a certain administrative policy. The external environment in which such an information reservation operates is not subject to its administrative policy and thus can develop negative or unforeseen impacts on CIS, and also negatively or unintentionally react to the impact of CIS on it. To ensure the vitality of the CIS, on the one hand, it is necessary to monitor and correct its interaction with the external environment (the reaction of the CIS to the external environment, the reaction of CIS to the consequences of its effects on the external environment). And, on the other hand, it is

necessary to monitor and correct the internal state of the CIS, related to the functioning of the hardware and software and the state of information support. To determine the ways of constructing a system for ensuring the survivability of CIS, let us first of all consider the standard technological process of the CIS functioning.

Simplified the technological process of the CIS functioning can be represented by the following scheme (Fig. 4):

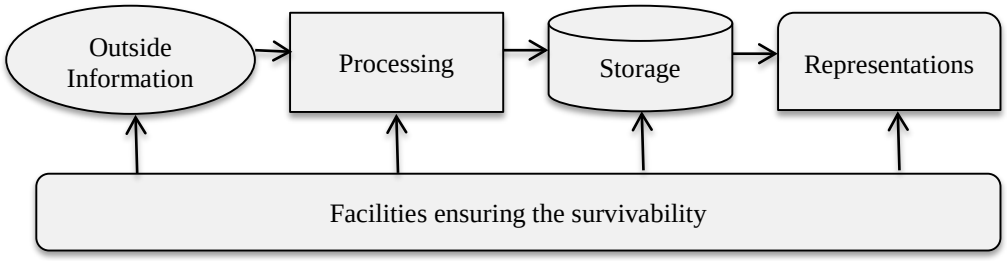

Fig. 4 the use of survivability in the technological process of functioning of CIS

This diagram shows the key objects to which survivability tools should be applied:

- Incoming information.
- Process of information processing.
- The process of storing information.
- Outgoing information.

Thus, the property of vitality is attached to a directed system of certain actions at all stages of its life cycle. At the stage of creating the CIS, special means for ensuring the life, organically integrated in the CIS. In the future, we will talk about them as a system for ensuring the survivability (SS) of CIS. The property of the CIS survivability is based on solving the problems of ensuring the survivability of each component of the CIS with the aim of achieving a stable technological process for the functioning of CIS countries as a whole. Below, we will consider the tasks that the system of ensuring the survivability of CIS should solve.

3. Tasks of the CIS system for ensuring the survivability

We define the concept of "ensuring" survivability, since in the literature there is mainly the notion of "increasing" vitality. The matter is that it is a question of a system of providing survivability within the CIS (actually a subsystem of CIS), created simultaneously with the CIS from the very beginning of its construction [5]. That is, everything that ensures the survival of the CIS is carried out within the framework of the survivability system. The term "increase" of survivability is rightfully used when the CIS is already created and functioning, i.e. already possesses a more or less developed property of vitality. In this case, additional methods and tools are used to increase the survivability of the CIS, not previously envisaged in the development of the survivability system, i.e. requiring changes in the provision of CIS subsystems or the technological cycle of the CIS operation. The development of survivability systems can also be interpreted as increasing the survivability of CIS.

We divide the tasks of the survivability system into two groups:

- Prevention of abnormal situations.
- Providing an exit from abnormal situations.

The first group includes the tasks of analysis and, if necessary, the correction of the functioning of the CIS for the purpose of ensuring its stable operation. The second group of tasks is to provide a way out of the contingency situation, if any, on the basis of reconfiguration, reconstruction, reorganization and adaptation methods.

In this part, the methods and tools for solving the problems of the first group will be examined in detail. A general approach to the solution of problems of the second group and an example of the solution of a typical particular problem of ensuring survivability in the destruction of communication channels are described in [3, 7]. Preventing the emergence of contingencies is solved as a two-pronged task in the creation of CIS: first, it is the availability of a modern quality management system for the quality of the products created and the receipt of an appropriate quality certificate for the developed CIS, and secondly, the development of special hardware and software coolants as subsystems CIS, allowing the administration of CIS to conduct prevention of abnormal situations.

The solution of the tasks of the first group is provided by the following functions of coolant:

A. Protection:

- Protection from negative influences of incoming information;
- Protection from unauthorized personnel;
- Protection against unauthorized environmental influences;
- Protection against faults and malfunctions of equipment;
- Protection from faults and software malfunctions;

B. Support of functioning:

- Support for processes of interaction with the external environment - Protection from unauthorized influences of maintenance personnel;
- Support for the accumulation of information - protection from malfunctions and hardware failures;
- Support of information processing;
- Support for storage technology;
- Support for internal information flows of CIS;

C. Correction of variances:

- Reorganization;
- Reconfiguration;
- Reconstruction
- Adaptation

Variance correction functions mainly serve to solve the tasks of the second group by normalizing the state of the system. Consider the tasks of coolant for the main types of CIS.

4. Tasks for ensuring the survivability of the technical maintenance of the CIS.

The technical support of the CIS includes:

- Storage devices.
- Hardware for information processing servers.
- Hardware of workstations of system users.
- Communication channels and equipment for information transfer.

The task of the coolant for technical maintenance is to prevent and prevent failures of its components and minimize the impact of possible failures on the functioning of the system. Coolant should provide constant monitoring of the state of all components of the technical support of the system, predict possible failures and apply measures in advance to overcome the current situation.

To ensure the prediction of failures, it is necessary, first, to check the correct functioning of all components of the technical support, for example, to regularly check the surfaces of disks, memory elements of RAM, and so on. Secondly, almost all modern devices provide fairly complete information about their status, such as the temperature and speed of rotation of the discs, the temperature and clock speed of the processors, the speed of rotation of the cooling fans, etc. An analysis of the dynamics of the change of such information will allow identifying its possible deviations from the norm and taking corrective measures in advance.

In addition, all technical support has a certain resource, determined by the manufacturer. Coolant should monitor the remaining resource for all components of the technical support and promptly provide information on the need for replacement or recovery.

To minimize the negative impact of possible hardware failures, the coolant must ensure the system is always ready for possible reorganization, reconfiguration and reconstruction of the system. For example, if there is an increase in the probability of failure of some information storage device, its mirror copy should be made on another, possibly slower device or on the free parts of other devices. If the probability of failure of some information processing server is increased, the coolant should, as far as possible, maximize the unloading of this server due to unused reserve resources of the CIS, thereby preparing it for repair or replacement.

5. Tasks for ensuring the survivability of the CIS software include

- System software.
- Application software.
- Database management servers.
- Expert systems.
- Analytical information systems.
- Planning and control systems.

The task of software coolant is to control the correct operation of the software and minimize the damage to the system functioning caused by possible errors in the software modules. In this case, the tasks of the coolant can be divided into two subsets:

- Quality control of software (carried out at the stage of development and maintenance).
- Integrity control of program modules that are executed in the system.

The tasks of the first subset assume the existence of a system for evaluating the quality of software development. This process should include such activities as automated testing, verification, validation, joint scans. The software

developed and selected for the CIS creation must guarantee the reliability of the operation, the correct handling of erroneous situations, and provide means for monitoring its functioning.

The tasks of the second subset assume the availability of tools for monitoring the process of the functioning of the software and its adjustment. Coolant should ensure control of digital signatures and checksums of software modules installed on servers and workstations of CIS, the availability of only the software packages provided on the CIS servers, the correspondence of the set of operations executed by the program modules, the approved templates. In addition, the coolant must ensure the implementation of the software update policy that is part of the CIS.

If the software is found to be incorrectly functioning, or the composition of the software of a node, the SIC must isolate it by reconfiguring and reorganizing the system, and reconstructing the functions of this node at the expense of free resources of other nodes of the system, preparing it for software recovery and finding out the reasons for its integrity violation. In addition, the coolant should prepare other nodes containing similar software packages for possible isolation or updating if they encounter similar problems.

6. Tasks for ensuring the survivability of information support for CIS

Information support is information stored, processed and circulating in the CIS. All the information in the system can be divided into the so-called "useful" (knowledge received, processed and stored in the system) and "technological" (control information, internal routing tables, etc.).

The purpose of the information security software is to ensure the security of information stored and processed in the system and to ensure the security of the CIS and its external environment when working with this information. For information support, the tasks of the coolant are divided into three subsets:

1. Filter incoming information to filter out information that does not meet the requirements of the interface (this information is accumulated for further analysis).
2. Filtering outbound information by censoring to filter out information that is unfavorable to the outside world.
3. Providing security of the information stored and circulating in the system and restoring it in case of failures.

The tasks of the first subset assume the existence of a developed security perimeter that has both a centralized and a decentralized control that would be able to evaluate incoming information (service and "useful") and exclude information of unsafe content. Assessments of incoming information should be made on the basis of the internal administrative policy of the CIS, the signatures of malicious software, patterns of behavior of malicious software, etc.

Partially, the solution of the tasks of the second subset can be based on ensuring the security of confidential information, but such methods, firstly, will not cover the whole class of tasks, and secondly, they will require significant expenses and, thus, will be unacceptable. In this case, the choice of protection methods should be based on the fact that information unfavorable for the environment is not extracted by it purposefully, with the help of special means. An effective method in this case will be the creation of means for censoring information that falls into the external information environment. And the rules of censoring should be constantly supplemented on the basis of the reaction of the external environment to the information coming from the system.

The tasks of the third subset assume the structuring of all the information that is in the system, in terms of the requirements for its availability, as well as the links between the various blocks of information:

- It is necessary to allocate some set of the critical information which should be accessible in any situation. For the rest of the information it is necessary to set the maximum access time, which can depend on the current situation (regular, supernumerary, etc.). When information is lost, it is necessary to provide the possibility of partial (or complete) information recovery based on the remaining information. Minimize the "indirect" losses, i.e. the inability to use information related to the lost, because of the lack of self-sufficiency of the remaining information;
- The information stored in the CIS should be ranked according to the level of importance. To the storage and processing of the most important information, special requirements must be made. In addition, the information can be ranked by the maximum access time to it in different situations;
- The separation of data links will allow creating requirements for the storage of various blocks of information, preventing possible "indirect" information losses, developing a rational approach to redundancy when storing data in the CIS.

7. General structure of the system for ensuring the survivability of CIS

The achievement by the survivability system (SS) of its goal - the formation of the conditions for the operation of

the CIS for its main function, requires, first of all, the analysis and monitoring of the state of the CIS in real time. This is realized in two ways:

- Operative information acquisition and development of control actions in critical points, from the point of view of the possibility of occurrence of contingencies, points of the technological cycle of the CIS functioning.
- Regular, purposeful analysis, control and adjustment of the state of software and information support of CIS.

Online information is provided by the inclusion of special "resident" programs (filters) of coolant both in the operating system (OS) and in the software of the CIS subsystems. The inclusion of coolant filters in the OS is performed using the interfaces provided by the OS. Examples of such programs include file system filters, network filters, and interceptors of system calls.

The inclusion of "resident" coolant programs in the software and information support of the CIS subsystem is performed directly in the development of the CIS according to its technical design. As it was mentioned above, the coolant is a part of the CIS, developed simultaneously with the CIS, and the development of all types of CIS support should take into account the requirements of the technical design of the coolant.

Analysis, control and adjustment of the state of the CIS, from the point of view of a possible deviation from the regular mode of operation, are carried out by specialized program-methodical complexes (PMC) in the directions:

a) Packages of executable program modules;
b) Databases;
c) Software operation protocols;
d) Event logs of the OS;
e) Statistics of loading of communication channels;
f) Failure statistics of communication channels;
g) Statistics of the hardware load;
h) Statistics of hardware failures;
i) Input data;
j) Output data.

All tasks of coolant are conventionally divided into groups and build coolant in the form of interacting subsystems, each of which is designed to solve a specific group of problems. For example, it is advisable to put in a separate group the tasks of technical protection of information or the task of protecting against the emergence of contingencies that can lead to the distortion of information or software and thus indirectly or directly entail deterioration in the quality of the CIS. A clear division of coolant into subsystems by types of tasks will simplify the logic of both coolant and CIS, and thereby increase its reliability, reduce the complexity of development, the timing of creation and cost, and in the future will facilitate the maintenance of the CIS.

The solution of problems of providing a way out of contingencies is performed by specialized PMK, for example, as described in [7]. A general approach to the development of algorithms for this class of PMC is described in [3].

Functional coolant consists of two main blocks:

a) The core of the coolant, responsible for analyzing the information collected, forecasting, developing solutions and monitoring the implementation of decisions;
b) A block of "resident" modules integrated into the hardware and software of the CIS and responsible for collecting operational information and executing solutions developed by the coolant core. In Fig. 5 shows the interaction diagram of the coolant blocks.

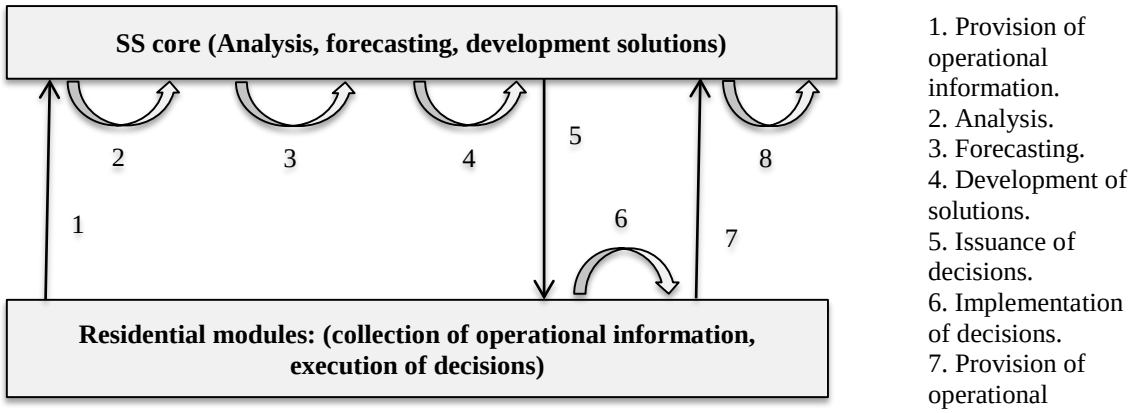

Fig. 5 Diagram of interaction of coolant blocks

The core of the coolant includes the following program-methodical complexes (PMC):

1) PMC interaction by the resident modules, designed to obtain the information they provide and transfer it to other PMC cores;
2) PMC analysis of the information received from the resident modules designed to assess the current state of the system and the impact on it of the developed solutions;
3) PMC forecasting the dynamics of the state of the system on the basis of statistics and analysis of the current state;
4) PMC development of solutions based on the forecasts;
5) PMC interaction with the administrator, providing the possibility of administrative management and configuration of the coolant as a whole; and uses specialized databases:

1. The database of statistics that is maintained and used by PMC analysis, forecasting and decision making;
2. The database of settings and rules, which is maintained by the PMC interaction with the administrator and is used to configure the PMCs that are part of the coolant core and the resident modules. In Fig. 6 is a block diagram of the coolant core.

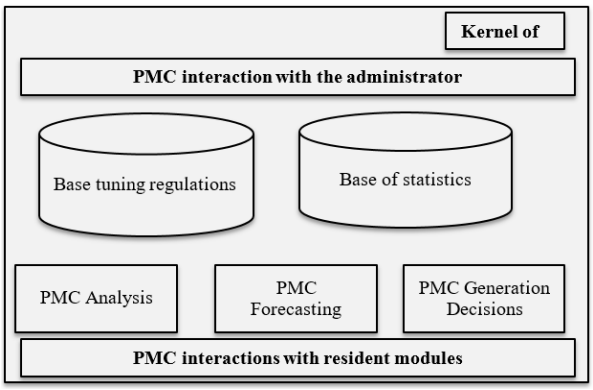

Fig. 6 Structural diagram of the coolant core

The module of the resident modules contains components integrated into the software and hardware systems of the CIS, providing:

- Interaction with the external environment;
- Data processing;
- Data storage;
- Transmission of information within the CIS.

One of the main tasks of coolant is to ensure the adaptation of CIS to operating conditions. Information basis of adaptation is the statistics of the frequency and execution time of program modules, access to databases, download of communication channels, hardware failures, etc. Accounting statistics allows you to reallocate the resources of the CIS, schedules for the implementation of programs for monitoring the state of the CIS, supplement the database of coolant management with new rules, etc.

8. Conclusion

At present, information technologies have reached a sufficient level for the development of CIS not to start from scratch. There are many professionally developed ready-made solutions that can be used to automate the business processes of the corporation. From this set, you can always choose the most suitable solution and adapt it for specific needs. This approach significantly reduces the cost of development and guarantees its successful and timely completion. There are many ready-made components, such as DBMS, OS, storage systems that can be used to build a new CIS.

Thus, all modern and professionally developed CIS have a similar structure, consist of similar components, have a similar technological cycle and perform similar functions. SS for such CISs will also have common features. This circumstance makes it possible to develop a template solution for SS, to describe its typical tasks, the structure, the construction method, and to determine the means that make up its composition.

However, each corporation is unique in its own way, possessing features specific only to it. This is the key to its competitiveness. Such uniqueness requires the creation of CIS for each corporation individually, which, in turn, requires an individual approach to the development of SS for each specific CIS. SS must be developed continuously and in parallel with the CIS and take full account of its specificity. Only under this condition it is possible to achieve the most effective functioning of the SS, the CIS and the corporation as a whole.

Acknowledgement

This work was funded by the Deanship of Scientific Research (DSR), King Abdulaziz University, Jeddah, under grant No. (D1439-190-830). The authors, therefore, acknowledge with thanks DSR technical and financial support.

References

[1] Caniëls, M.C. and R.J. Bakens, The effects of Project Management Information Systems on decision making in a multi project environment. International Journal of Project Management, 2012. 30(2): p. 162-175.
[2] Laudon, K.C. and J.P. Laudon, Management Information Systems: Managing the Digital Firm Plus MyMISLab with Pearson eText--Access Card Package. 2015: Prentice Hall Press.

[3] Levy, M. and P. Powell, Information systems strategy for small and medium sized enterprises: an organisational perspective. The Journal of Strategic Information Systems, 2000. 9(1): p. 63-84.
[4] Cassidy, A., A practical guide to information systems strategic planning. 2016: CRC press.
[5] Goodwin, P. and G. Wright, Decision Analysis for Management Judgment 5th ed. 2014: John Wiley and sons.
[6] Valacich, J. and C. Schneider, Information Systems Today: Managing in a Digital World Plus MyMISLab with Pearson eText--Access Card Package. 2015: Prentice Hall Press.
[7] AlRababah, A.A., A. AlShahrani, and B. Al-Kasasbeh, Efficiency Model of Information Systems as an Implementation of Key Performance Indicators. International Journal of Computer Science and Network Security (IJCSNS), 2016. 16(12): p. 139.
[8] Avison, D. and G. Fitzgerald, Information systems development: methodologies, techniques and tools. 2003: McGraw Hill.
[9] Bao, R., et al., Review of current methods, applications, and data management for the bioinformatics analysis of whole exome sequencing. Cancer informatics, 2014. 13(Suppl 2): p. 67.
[10] AlRABABAH, A.A., IMPLEMENTATION OF SOFTWARE SYSTEMS PACKAGES IN VISUAL INTERNAL STRUCTURES. Journal of Theoretical & Applied Information Technology, 2017. 95(19.(
[11] Revenaugh, D.L. and R. Papp, Information Systems Strategy & Implementation. AMCIS 2000 Proceedings, 2000: p. 254.
[12] Ziemba, E., I. Obłąk, and B.S. Informatyczna, Critical success factors for ERP systems implementation in public administration. Interdisciplinary Journal of Information, Knowledge, and Management, 2013. 8(1): p. 1-19.
[13] Chen, D.Q., et al., Information systems strategy: reconceptualization, measurement, and implications. MIS quarterly, 2010. 34(2): p. 233-259.
[14] Pearlson, K.E., C.S. Saunders, and D.F. Galletta, Managing and Using Information Systems, Binder Ready Version: A Strategic Approach. 2016 :John Wiley & Sons.
[15] Ein-Dor, P. and E. Segev, Organizational context and the success of management information systems. Management Science, 1978. 24(10): p. 1064-1077.

Ahmad AbdulQadir Al Rababah received Phd degree in 1998 in computer Engineering, now he is an associate professor at king Abdulaziz university(KSA), he has around 20 experience years of teaching and research in different fields of computing technology and engineering, his research interest areas are: information systems, software engineering, artificial intelligence and others.