UDC 621.391
DOI: 10.15587/2312-8372.2017.118388

**Dorogyy Ya.**

# DEVELOPMENT OF A MODEL FOR OPTIMAL CONFIGURATION COMPONENTS SELECTION FOR ARCHITECTURE OF CRITICAL IT INFRASTRUCTURE AT ITS DESIGNING

*Запропонована модель, яка дозволяє приймати рішення стосовно оптимального вибору компонентів критичної IT-інфраструктури на стадії проектування. Модель дає інструментарій оцінювання варіантів реалізації архітектури на базі різних критеріїв, таких як вартість проектування варіанту архітектури, ефективність тощо. Застосовуючи певні налаштування запропонований інструментарій дозволяє вивчити каскадні ефекти взаємозалежності компонентів, провести оцінку на етапі проектування.*

**Ключові слова:** *критична IT-інфраструктура, Марківський процес прийняття рішень, модель вибору конфігурації.*

## 1. Introduction

To compete in the global market, enterprises increasingly interact with partners and customers outside their country of origin. The goal of the globalization of operations is reducing costs, gain labor and experience, and access to new markets.

As part of its global strategy and structure, many enterprises create subsidiaries in other countries. The enterprise must determine to what extent each branch is self-sufficient and independent of the headquarters when making decisions. Improvement of financial efficiency occurs with the active reaction of the branch to changes in the local market, and vice versa, in the case of following standardized global business processes such an improvement is unlikely [1]. At the same time, allowing the branch to make decisions without interference from the headquarters can create tension in the relationship, especially with respect to decisions related to the design and management of the IT infrastructure. Enterprises form their business strategy through their management mechanisms, and then coordinate their information resources to support the business strategy. Transition to a decentralized approach enables companies to use their IT resources to respond to conditions emerging in the local market, at the same time, there is a risk that IT investments may not coincide with the overall business strategy of the enterprise. Such shortcoming may increase the likelihood of spending financial resources, dissatisfaction with users, failures in security management, the creation of managers who do not want to invest in future IT initiatives and, finally, undermine the final financial result.

That is why, many enterprises have global-centralized decision-making processes for IT infrastructure, especially critical infrastructure enterprises. The main aim is reduce risks, optimize the allocation of resources, satisfy users, strengthen control and support the company's strategy [2].

The main argument in support of centralized design and management of IT infrastructure is the opportunity to participate in making IT solutions for influential and experienced professionals and managers. These specialists prefer IT projects on the basis of their relevance, and as a result, these projects receive adequate funding. In the case where the management body is decentralized, IT professionals can't understand the negative consequences of their ideal «local» solution for the entire company. The opposite argument – a centralized IT decision-making approach can limit the influence of local professionals and managers in decision-making, while they may have a better understanding of the problem itself and the relevant markets. IT professionals are at the epicenter of the problems caused by the conditions of the local market, may have better opportunities to determine the requirements for solutions and the priority of projects. Therefore, it is relevant to study the design and management of IT infrastructure.

## 2. The object of research and its technological audit

*The object of research is* a critical IT infrastructure. A critical IT infrastructure must:

– ensure the functioning of environmentally hazardous and socially significant production and technological processes, the violation of the regular mode of which can lead to an emergency situation of anthropogenic nature;

– perform the functions of an information system, the violation (stoppage) of which may lead to negative consequences in the political, economic, social, information, environmental and other fields;

– ensure the provision of a significant amount of information services, partial or complete suspension of

ISSN 2226-3780

which can lead to significant negative consequences for national security in many sectors.

The main problem in this industry is the complete absence of ready-made solutions, methodologies, tools that are suitable for modeling, designing and researching critical IT infrastructures.

## 3. The aim and objectives of research

*The aim of this work* is development of a model for choosing the optimal configuration of the components of the critical IT infrastructure at the design stage.

To achieve this aim, it is necessary to perform the following tasks:

1. To improve the existing mathematical apparatus of decision-making with the help of Markov decision-making processes for the study of critical IT infrastructures.

2. To investigate, using the built model, the choice of the data processing center (DPC) for the architecture of the critical IT infrastructure.

## 4. Research of existing solutions of the problem

Previous studies have identified five areas of IT design and management – strategic alignment, risk management, resource management, delivery of value and performance evaluation [3]. The work is devoted to the direction of strategic harmonization in the design of critical IT infrastructures and identifies the disadvantages and advantages of solutions related to centralized/decentralized design solutions for the architecture of the IT infrastructure. Strategic alignment requires managers to align the IT strategy with the overall business strategy as the main focus of their IT infrastructure. A decision support model is proposed to ensure the adoption of appropriate design decisions that coincide with the company's strategy in terms of centralization/decentralization, which includes knowledge of the future disadvantages/advantages of each design solution based on the proposed criteria when designing the IT infrastructure.

It is concluded in [4] that strategic coordination, depending on the context, can be decentralized, centralized or mixed. The study [5] interviewed 500 managers responsible for managing the IT infrastructure and conducting a further survey of 30 CIOs. As a result, it is determined that the strategic harmonization of IT solutions ensures revenue growth in the event of agreement with the business strategy of the enterprise, and otherwise may lead to counterproductive investments in the IT infrastructure.

The reconciliation of investments in the IT infrastructure, based on the needs of the business, affects the outcome of IT initiatives, such as the implementation of the ERP system. According to the arguments described above, some studies support centralization, and some studies support decentralization. For example, the study [6] shows that productivity is increasing, and losses are reduced when the enterprise uses central planning and control of the IT infrastructure. Another study [7] shows that the excellent CRM data processing characteristics and the localized nature of CRM efforts are better supported when using CRM technologies in close conjunction with a broader infrastructure and local management.

In works [8–11], the authors also point to the need to study the IT infrastructure in conjunction with the supporting systems. Designing of architecture in isolation from them can affect the optimality of the received IT infrastructure.

## 5. Research methods

**5.1. Description of the mathematical model for choosing the optimal configuration of the critical IT infrastructure components.** The proposed model has the following parameters:

$F$ – a finite set of branches of the enterprise ($F=\{1,..,f\}$);

$P$ – a finite set of IT platforms ($P=\{1,..,p\}$);

$T$ – a finite set of time samples ($T=\{1,..,t\}$);

$I$ – a finite set of design criteria;

$Z$ – set of categories of requests for architecture change ($Z=\{1,..,z\}$);

$f\in F$ – value of the index of the branch of the enterprise;

$p\in P$ – the value of the IT platform index;

$z\in Z$ – the value of the architecture change request index;

$i\in I$ – the value of the design criterion index;

$b_t\in I$ – the budget of the new project at the time $t$;

$c_{fp}$ – cost of designing/transitioning to a new platform $p$ for the branch $f$, taking into account all costs for software, hardware, integration and implementation;

$a_{fpz}$ – cost of request execution for architecture $z$ change to the platform $p$ for the branch $f$;

$b_{fpzi}$ – the winnings from the implementation of the request for changing the architecture $z$ to the platform $p$ for the branch $f$ by criterion $i$.

The state space of the model is described by the following variables:

$x_{zf}$ – the number of requests to change the architecture $z$ not yet completed for the branch $f$;

$cur_{fp}$ – current platform of the branch $f$;

$X$ – matrix of values $x_{zf}$;

$CUR$ – matrix of values $x_{zf}$;

$S$ – the state of the process ($S=[X,CUR,t]$).

Random variables used in the model:

$pr_{zft}$ – the number of requests to change the architecture $z$ for the branch $f$ at the time $t$;

$PR$ – the matrix of values $pr_{zft}$.

The solution space of the model is described by the following variables:

$y_{zft}$ – the number of requests to change the architecture $z$ for the branch $f$ at the time $t$;

$l_{fpt}$ – the flag of transition to the platform $p$ for the branch $p$ at the time $t$ that it is necessary to execute;

$Y$ – an array of variable solution spaces;

$\Re(S)$ – the set of possible solutions for the state $S$;

$C^i(Y)$ – the winning by the criterion $i$ that is connected with the decision $Y$;

$C(Y)$ – the winning by all criteria associated with the decision $Y$;

$RWD_n^i(S)$ – the maximum expected value of the win at the $n$-th stage in the state $S$ by criterion $i$;

$RWD(S)$ – the maximum expected value of the win at the $n$-th stage $S$ in the state by criterion $i$.

The model has a number of limitations. For a state $S=[X,CUR,t]$, the state space variables must satisfy the following constraints:

– budget limitation of the project:

$$\sum_f \sum_p c_{fp} l_{fpt} + \sum_z \sum_f a_{zpf} y_{zft} \le b_t; \quad (1)$$

– limitations of project scope:

$$y_{zft} \le x_{zf}; \quad (2)$$

– platform requirements:

$$\sum_p l_{fpt} = 1, \forall f, \quad (3)$$

$$y_{zft} \ge 0. \quad (4)$$

All solutions $Y$ satisfying the requirements (1)–(4), for the state $S$ form a set of possible solutions $\Re(S)$. The model is flexible. It is possible to add additional restrictions. For example, it is possible to take into account the implementation of design solutions that ensure the integrity of the system and its security.

Every possible decision is made to have a certain amount of directly expected costs and winnings. First, the expected winning $b_{fzi}$ by the criterion $i$ when executing the architecture change request $z$ for the branch $f$. The company also incurs the cost $a_{fz}$ of implementing the architecture change request $z$ for the branch $f$. Additional, there may also be costs $c_{fp}$ associated with branch $f$ migration to the platform $p$.

Taking into account the above, the winnings at the next design stage by the criterion associated with the decision $Y$ can be calculated by the formula:

$$C^i(Y) = \sum_z \sum_f \sum_i b_{zfi} y_{zft} - \sum_f \sum_p c_{fp} l_{fpt} - \sum_z \sum_f a_{fz} y_{fzt}. \quad (5)$$

The value $C^i(Y)$ can be either positive or negative. If

$$\sum_z \sum_f \sum_i b_{zfi} y_{zft} > \sum_f \sum_p c_{fp} l_{fpt} + \sum_z \sum_f a_{fz} y_{fzt},$$

then the winning associated with the selected design decisions, represented by the first term of the winning function at the next design stage, outweighs the costs that need to be done.

The uncertainty of the task lies in the frequency of change requests from each branch. In this paper, it is considered that the value $PR$ is statically independent. Let $S = [X]$, $[CUR]$ – the current state, $Y \in \Re(S)$ – the selected array of solutions, and $S' = [X']$, $[CUR']$ – the state after executing the shift request. Then the state value $S'$ changes according to (6)–(8):

$$x'_{zf} = x_{zf} - y_{zft} + pr_{zft}, \quad (6)$$

$$cur'_{fp} = l_{fpt}, \quad (7)$$

$$t' = t + 1. \quad (8)$$

The probability of transition from state $S$ to state $S'$ for a solution $Y$ is defined as (9):

$$P_{SS'(Y)} = \prod_{f \in F} \prod_{z \in Z} \wp \left\{ pr_{zft} \mid cur_{fp} = x'_{zf} - x_{zf} + y_{zft} \right\}. \quad (9)$$

The model search functions are as follows:

$$RWD_1^i(S) = \max_{Y \in \Re(S)} C^i(Y), \quad (10)$$

$$RWD_n^i(S) = \max_{Y \in \Re(S)} \left\{ C^i(Y) + \sum_{S'} P_{SS'}(Y) RWD_{n-1}^i(S') \right\}, \; n > 1, \quad (11)$$

$$RWD(S) = \max_{Y \in \Re(S)} \sum_i \sum_j^n RWD_j^i(S). \quad (12)$$

**5.2. Description of the options for building platforms based on cloud IT infrastructures.** For cloud computing, it is necessary to manage applications, implement interaction with virtualization platforms and network infrastructure under a common scenario for the entire system. The system as a whole should support a large number of components and provide general management tools that can guarantee reliable, safe and high-quality provision of services to customers. The network, hardware and software infrastructure of the cloud system must meet the existing and new network standards:

– ISO/IEC 17789 (ITU-T Y.3502) – Information technology. Cloud computing. Reference architecture [12];
– NIST SP 500-291 – Standards of cloud computing [13];
– NIST SP 500-292 – Basic architecture of cloud computing [14];
– ISO/IEC Committee Draft 27017 – Fundamentals of information security management for cloud computing based on ISO/IEC 27002 [15];
– ISO/IEC Draft International Standard 27018 – Data protection framework for public cloud services [16];
– ISO/IEC Working Draft 27036-4 – Information security of relations with suppliers – Part 4: Guidelines for securing cloud services [17];
– ISO/IEC Draft International Standard 27040. Security of IEEE P2301 storage systems – Compatibility and Portability Profiles (CPIP) [18];
– IEEE P2302 – interaction of cloud systems (SIIF) [19];
– ANSI/TIA-942 [20], EN 50173-5 [21], ISO/IEC 24764 [22] – standards for the design of cloud data centers.

The National Institute of Standards and Technology (NIST) in [12] presented an overview of the reference cloud computing architecture that identifies key actors, their activities and functions in cloud computing (Fig. 1).

The main subjects of the reference architecture are:
– consumers – individuals, both physical and legal, who use the services of cloud providers;
– providers – individuals, both physical and legal, who are responsible for providing cloud computing;
– auditors – individuals or legal entities or organizations that perform independent evaluation of cloud computing;
– brokers – individuals, both physical and legal, that are the link between the provider and the consumer of cloud computing (options are possible without the involvement of the broker, that is, cloud services are delivered from the provider to the consumer directly);
– telecom operators – individuals, both physical and legal, or a company that has provided the services of connecting and delivering cloud services from the provider to the consumer.

ISSN 2226-3780

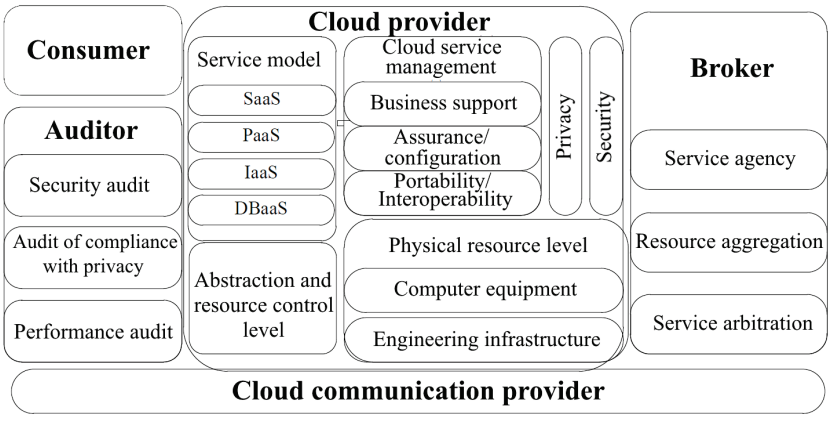


**Fig. 1.** The reference architecture of cloud computing of the USA National Institute of Standards and Technology

The main service models are:
– IaaS – infrastructure as a service.
– PaaS – platform as a service.
– SaaS – software as a service.

In addition to the main service models, there are such models:
– HaaS – hardware as a service.
– SecaaS – security as a service.
– BPaaS – business process as a service.
– DBaaS – database as a service.
– TaaS – trust as a service.
– SDPaaS – the cloud development environment as a service and others [23].

In addition, there are four main deployment models:
– Private.
– Community cloud.
– Public cloud.
– Hybrid cloud.

Based on the analysis of the standards discussed above, it is established that typical cloud architecture is client-server with support for virtualization technology built on the basis of a data processing center and has a hierarchical structure. Fig. 2 shows typical network architecture of the cloud system.

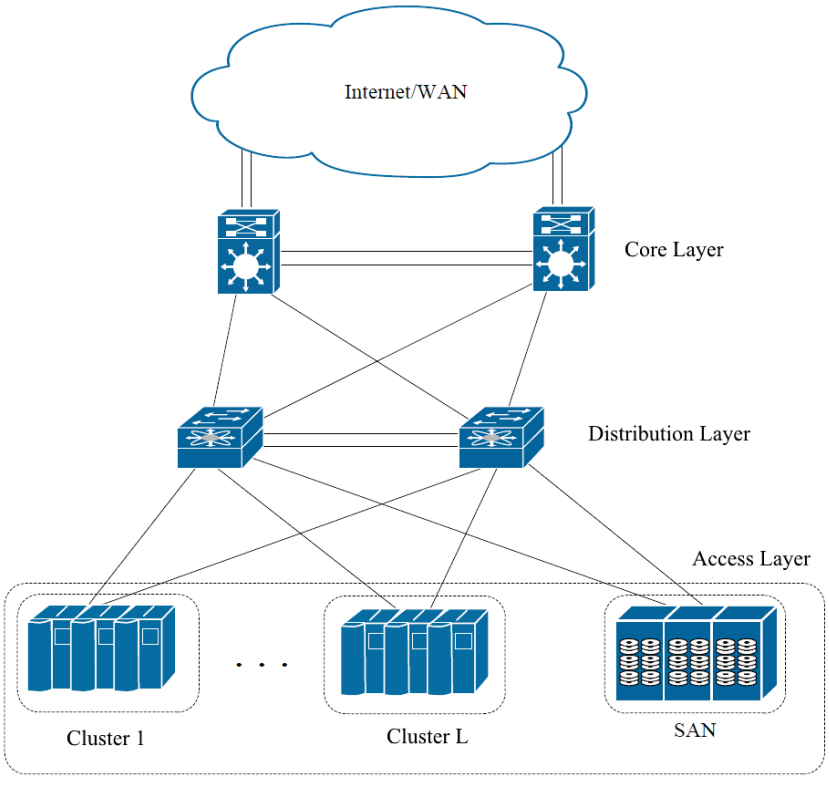


**Fig. 2.** Typical network architecture of cloud systems

The network structure consists of three main levels:

Core level. At this level, routers or switches of the third level of the OSI model are operating, which form the basis of the entire data center network with high-speed and ports (10/40/100 GbE) for routing flows between the WAN and the data center network.

– Aggregation/Distribution level. At this level also operate switches of the third level of the OSI model, the main purpose of which is to distribute the load between local data center networks.

– Access layer. At this level, there are endpoints (servers) and network equipment, connect the endpoints to the aggregation level. At the access level, there are clusters of data centers, consisting of a large number of physical servers and virtual machines running on each of them. At the same level, there is a shared storage area network (SAN). A group of interconnected storage components, computing and network resources that work together at the access level to provide access to services or applications to customers, is called a point of delivery or POD.

To date, there are two main topologies for connecting servers in clusters: Top of Rack (ToR) and End of Row (EoR) [24]. ToR topology involves placing a separate switch (or two for redundancy) on top of each server rack. The access level switches are connected to the top-level switches (aggregation level) by fiber-optic cables (Fig. 3).

The notation in Fig. 3: $m$ – the total number of servers in the cluster and k – the number of servers in each rack connected to the access layer switches by two patch cords to provide redundancy. Another topology (Fig. 4) involves the use of one (two for redundancy) switch at the end (EoR) or in the middle (MoR – Middle of Row) array of racks with servers [25].

In such design, the network load is completely consumed by the EoR switch.

From a network connectivity perspective, ToR and EoR/MoR architectures are opposite solutions. In the first case, the connectivity of the network is maximal. But it takes a lot of hardware and more ports on the aggregation level switch to which the access level switches are directly connected. In the second case, fewer ports are required on the aggregation level switch and lower costs for the access layer switch, but the connectivity of the network is minimal.

When choosing a topology, it is necessary to take into account the deployment overhead, the amount of equipment and other criteria. Therefore, the third option is the hybrid architecture of the access level network of the cluster of data processing centers between the topology of ToR and EoR. This option is formed on the basis of a combination of two concepts, including overhead and port savings. As a result, the option provides a minimum acceptable level of criticality of failures of access-level switches, while not reducing reliability in comparison with the topology of ToR. A model of such architecture is shown in Fig. 5.

Hybrid topology involves connecting several server racks to separate access level switches that can be located in the middle of the row.

Based on the presented cluster topologies, the architecture of the data processing center is formed. There are two main options for implementing a data processing center. The first version of the construction – the architecture of a data processing center with a single POD [26] is shown in Fig. 6.

The system is operable if it consists of a SAN storage network, at least one of the network routes to the access level clusters and at least one cluster with servers.

The second option is the network architecture of a virtual data center with several PODs. It is shown in Fig. 7.

Thus, taking into account the above, it is possible to distinguish the following types of platforms that will be used in this paper (Table 1).

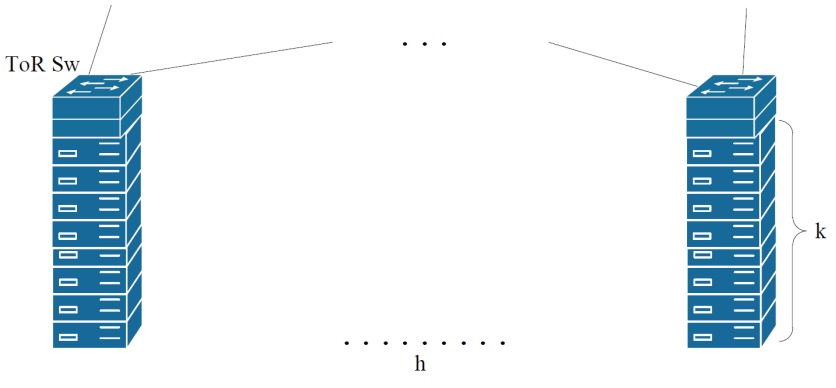


**Рис. 3.** ToR topology (Top of Rack)

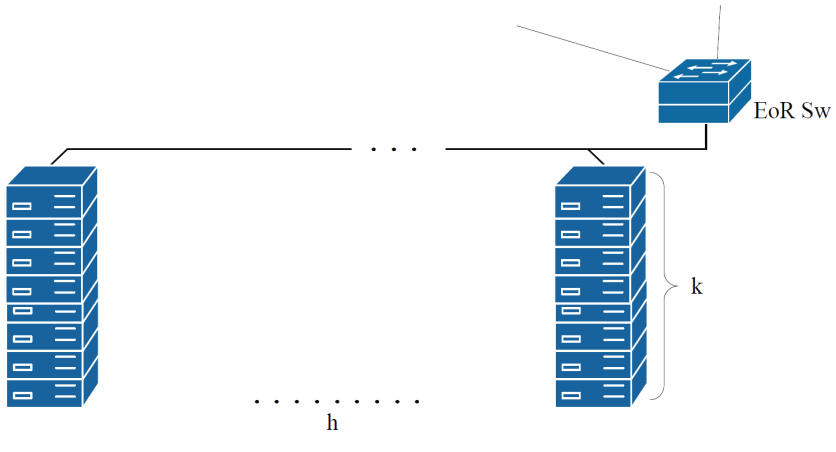


**Рис. 4.** EoR/MoR cluster topology (End of Row/Middle of Row)

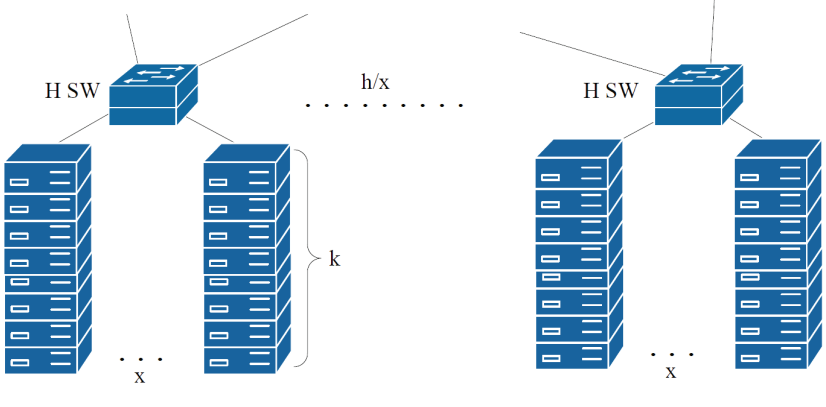


**Fig. 5.** Hybrid cluster topology

ISSN 2226-3780

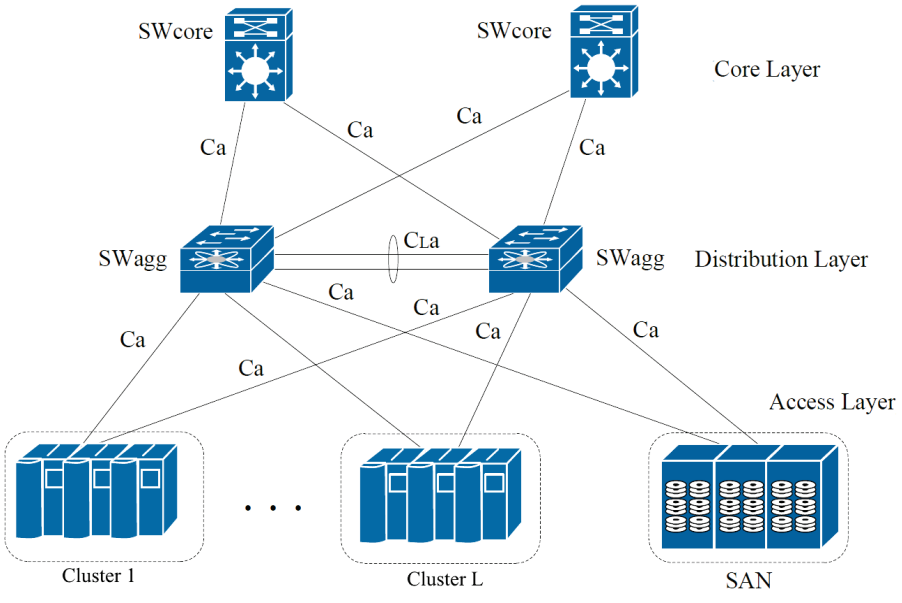


**Fig. 6.** The architecture of a data processing center (DPC) with a single point of delivery (POD)

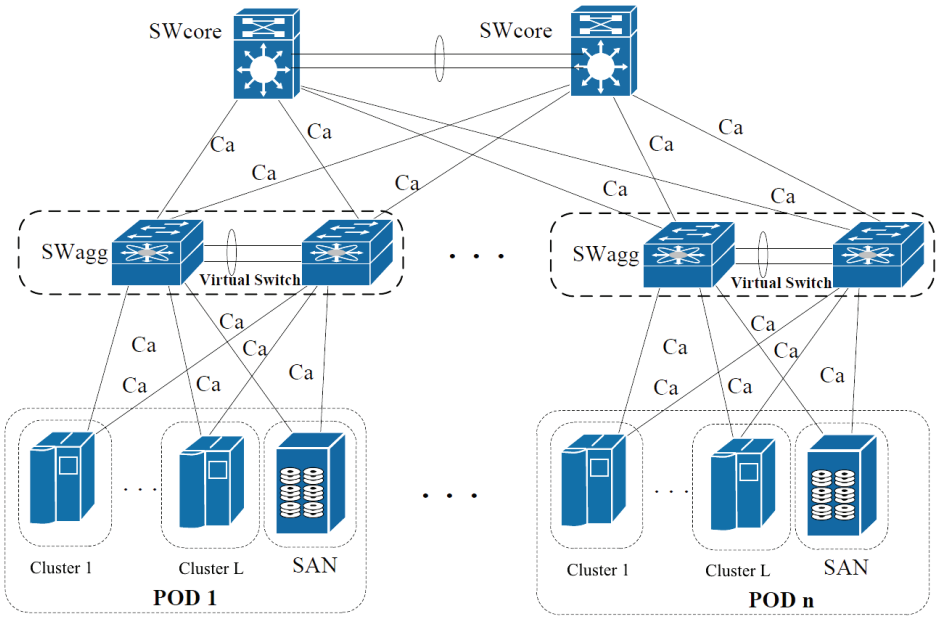


**Fig. 7.** The architecture of a data processing center (DPC) with multiple points of delivery (POD)

**Table 1**

Types of platforms

| Platform | Cluster type | DPC network Architecture | Centralization/ decentralization | Estimated cost, USD |
|---|---|---|---|---|
| 1 | ToR | 1 POD | C | 200000 |
| 2 | EoR/MoR | 1 POD | C | 300000 |
| 3 | Hybrid | 1 POD | C | 150000 |
| 4 | ToR | *n* POD | C | 600000 |
| 5 | EoR/MoR | *n* POD | C | 700000 |
| 6 | Hybrid | *n* POD | C | 550000 |
| 7 | ToR | *n* POD | DC | 900000 |
| 8 | EoR/MoR | *n* POD | DC | 1000000 |
| 9 | Hybrid | *n* POD | DC | 800000 |

The centralized solution provides that all the main components of the network are located at the headquarters of the enterprise (except for clusters). Decentralized solution – components are distributed between the headquarters and the branches of the enterprise.

## 6. Research results

Experimental studies are based on the problem of choosing the DPC architecture for a virtual critical IT infrastructure of an enterprise, consisting of a headquarters and two branches.

The following variants of possible solutions are used for the study (Table 2).

In fact, those who decide to choose the architecture for a critical IT infrastructure must decide whether to

design the entire IT infrastructure on a low-cost platform (Platform 3) or to find an option that will be more expensive but more reliable, efficient, and so on. Each solution must be evaluated in terms of future potential projects and changes in IT infrastructure, which these projects may require.

**Table 2**

Configuration options

| Configuration | Headquarters | Branch 1 | Branch 2 |
|---|---|---|---|
| 1 | Platform 1 | Platform 1 | Platform 1 |
| 2 | Platform 1 | Platform 1 | Platform 3 |
| 3 | Platform 1 | Platform 2 | Platform 3 |
| … | … | … | … |
| 84 | Platform 9 | Platform 9 | Platform 9 |

Table 3 shows the events that can cause the need for changes for the platforms.

Each type of event is further divided into several categories according to their size, the distribution of the shift request and the associated costs/winnings.

Table 4 shows the data structure used to study the proposed model.

This paper compares the aggregate winnings received from the recommendations, provides a model that considers the costs and benefits by criteria simultaneously.

For the simulation, the assumption is made that the actual number of architecture change requests for each branch for a certain period ($pr_{zft}$) corresponds to the Poisson distribution with the λ parameter. The value of λ ranges from 25 % to 200 % of the base value in 5 % increments (36 design points).

**Table 3**

Events that may cause the need for changes for platforms

| Event Type | Example | Winning | Costs |
|---|---|---|---|
| New application | Installing a new application through new business or IT needs | New financial benefits, provides a new application | Costs of deploying a new application in the IT infrastructure |
| Scaling | Increase in the number of transactions for increasing the number of users, etc. | Additional finance from new users | Costs for infrastructure scaling |
| Integration | Integration of new applications through changes in production processes, etc. | Additional financial revenues or savings from the use of improved manufacturing processes | Integration costs |
| Modification of the system | The need to combine different types of data, etc. | The benefits of using new approaches to decision-making | Costs for modifying components to support new types of data, etc. |
| Security | Special attention of hackers requires better firewalls, protection of server operating systems, etc. | Reducing the potential negative impact of attacks and data storage | Costs of activities aimed at improving safety |
| Criticality | The transition of the service to the rank of critical | Increased reliability, security, etc. | Costs for carrying out activities to transfer the service to the rank of critical |

**Table 4**

Data structure

| Headquarter/Branch 1/ranch *n* | | | | Platform 1 | | … | Platform 84 | |
|---|---|---|---|---|---|---|---|---|
| Category | Event | Event size | The expected frequency of an event, per month | Expected costs, k$ | Expected winning, k$ | … | Expected costs, k$ | Expected winning, k$ |
| 1 | New application | Insignificant | 20 | 10 | 15 | … | 12 | 13 |
| 2 | New application | Average | 5 | 20 | 30 | … | 22 | 44 |
| 3 | New application | Large | 1 | 50 | 70 | … | 55 | 80 |
| 4 | Scaling | Insignificant | 5 | 5 | 10 | … | 3 | 5 |
| 5 | Scaling | Average | 3 | 15 | 25 | … | 10 | 12 |
| 6 | Scaling | Large | 1 | 30 | 40 | … | 40 | 80 |
| 7 | Integration | Insignificant | 15 | 5 | 7 | … | 8 | 10 |
| 8 | Integration | Average | 8 | 10 | 12 | … | 15 | 30 |
| 9 | Integration | Large | 2 | 30 | 45 | … | 45 | 70 |
| 10 | Modification of the system | Insignificant | 20 | 5 | 6 | … | 3 | 5 |
| 11 | Modification of the system | Average | 10 | 10 | 17 | … | 12 | 18 |
| 12 | Modification of the system | Large | 1 | 25 | 55 | … | 30 | 44 |
| 13 | Security | Insignificant | 100 | 5 | 15 | … | 6 | 9 |
| 14 | Security | Average | 20 | 20 | 100 | … | 30 | 70 |
| 15 | Security | Large | 5 | 50 | 200 | … | 60 | 120 |
| 16 | Criticality | Insignificant | 5 | 5 | 40 | … | 2 | 5 |
| 17 | Criticality | Average | 2 | 10 | 70 | … | 12 | 60 |
| 18 | Criticality | Large | 1 | 100 | 800 | … | 120 | 700 |

ISSN 2226-3780

In the course of the research, the impact of changes in the distribution of requests for changing the architecture of subsidiaries on the choice of the platform is analyzed. The basic distribution of architecture change requests is set at 30 % for the headquarters, 35 % for branch 1 and 35 % for branch 2. To simplify the presentation of the results, modeling fixes the base level for headquarters at 30 % of requests, and for branches 1 and 2, this level varies from 0 % to 70 % in 5 % increments (14 simulation points). In total, such simulation scheme yields 504 simulation points. According to Table 4, the total number of architecture change requests for each branch is first determined, and then, the distribution of requests for architecture change by categories is determined, taking into account their relative occurrence frequency. Next, the corresponding costs and winnings for the branches are determined. Fig. 8 shows the recommendations (with 84 possible configurations given in Table 2) provided by the proposed model for various design simulation points.

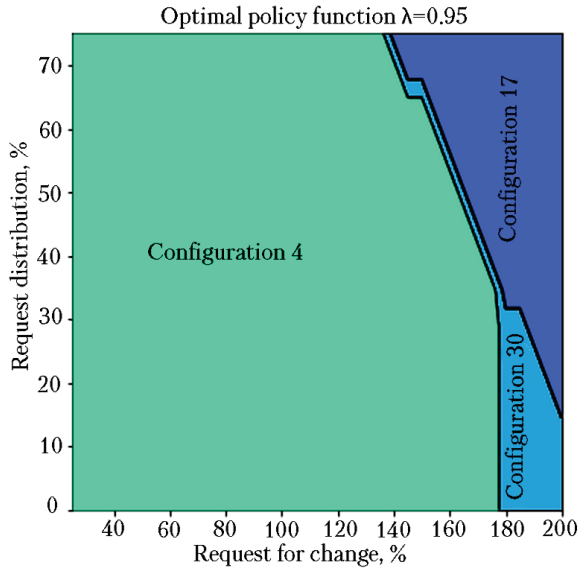


**Fig. 8.** Simulation results

As can be seen from Fig. 8, configuration 4 is optimal from the point of view of maximizing the aggregate winning.

## 7. SWOT analysis of research results

*Strengths.* When working with critical IT infrastructures, evaluating the choice of a particular implementation of architecture is one of the problems that all methods used for design face. The proposed model is both modular and scalable in the sense that it has sufficient flexibility in the selection and use of both simple and complex criteria for choosing architecture for a critical IT infrastructure. Modularity is achieved through the use of different configurations of elements, whereas scalability is presented in two forms:

– scalability in building a model (topology and functionality) of the critical IT infrastructure;

– scalability in terms of using different kinds of criteria necessary for comparing implementation options. From the point of view of modeling, the proposed approach allows creating models for evaluating implementation variants based on various criteria, it can be further used as input models for subsequent comparison using other criteria, which in turn makes it possible to find the optimal architecture of the critical IT infrastructure. Thus, the model allows to accumulate models of evaluation of implementation variants for reusable use.

The model is built on the use of the Markov decision-making process and provides all the necessary tools for building, planning, researching, managing, evaluating the architecture options for critical IT infrastructures.

*Weaknesses.* At this stage of model development, a single weakness is the lack of real work parameters for critical IT infrastructure components.

*Opportunities.* In the future, it is planned to use the proposed model to develop models for assessing the choice of components of all systems and critical IT infrastructure subsystems, with the ultimate goal of creating a library of models that will allow them to be selected and easily used for various studies. The proposed model and library of models will allow researchers to conduct a preliminary assessment of options for implementing the architecture of critical IT infrastructure for various criteria.

*Threats.* It is now difficult to predict the negative risks of the developed model. But it is possible to say for sure that no additional costs will be created by the developer of the critical IT infrastructure that will use the proposed model and the library of models developed in the future.

## 8. Conclusions

1. The existing mathematical apparatus of the Markov decision-making processes has been improved in order to study critical IT infrastructures. The usual Markov decision-making process is adapted to evaluate the choice of the optimal configuration of components of the critical IT infrastructure by various criteria.

2. The possibility of using the model is investigated. This model allows to evaluate the implementation options for various components and subsystems of the critical IT infrastructure. On a simple model for selecting the optimal data center architecture for a critical IT infrastructure, the operability of the proposed model is tested – a model is created in the MatLab package, its work is investigated.

As a result of modeling, among the 84 possible configurations of the data processing center, the best overall winning (configuration 4) is chosen.

### References

1. Ghemawat, P. Managing Differences: The Central Challenge of Global Strategy [Text] / P. Ghemawat // Harvard Business Review. – 2007. – Vol. 85, No. 3. – P. 58–68.
2. Simonsen, J. Involving Top Management in IT Projects [Text] / J. Simonsen // Communications of the ACM. – 2007. – Vol. 50, No. 8. – P. 52–58. doi:10.1145/1278201.127820
3. Wilkin, C. L. A Review of IT Governance: A Taxonomy to Information Accounting Information Systems [Text] / C. L. Wilkin, R. Chenhall // Journal of Information Systems. – 2010. – Vol. 24, No. 2. – P. 107–146. doi:10.2308/jis.2010.24.2.107
4. Grover, V. Fix IT-Business Relationships Through Better Decision Rights [Text] / V. Grove, R. M. Henry, J. B. Thatcher // Communications of the ACM. – 2007. – Vol. 50, No. 12. – P. 80–86. doi:10.1145/1323688.1323699
5. Shpilberg, D. Avoiding the Alignment Trp in Information Technology [Text] / D. Shpilberg, S. Berez, R. Puryear, S. Shah // MIT Sloan Management Review. – 2007. – Vol. 49, No. 1. – P. 51–58.

6. Neirotti, P. Assessing the strategic value of Information Technology: An analysis on the insurance sector [Text] / P. Neirotti, E. Paolucci // Information & Management. – 2007. – Vol. 44, No. 6. – P. 568–582. doi:10.1016/j.im.2007.05.005
7. Sen, A. IT Alignment Strategies for Customer Relationship Management [Text] / A. Sen, A. P. Sinha // Decision Support Systems. – 2011. – Vol. 51, No. 3. – P. 609–619. doi:10.1016/j.dss.2010.12.014
8. Casalicchio, E. Federated Agent-based Modeling and Simulation Approach to Study Interdependencies in IT Critical Infrastructures [Text] / E. Casalicchio, E. Galli, S. Tucci // Proceedings of the IEEE International Symposium on Distributed Simulation and Real-Time Applications (DS-RT'07). – Chania, Crete, Greek. – 2007. doi:10.1109/ds-rt.2007.11
9. Pederson, P. Critical Infrastructure Interdependency Modeling: A Survey of U.S. and International Research [Text]: Technical Report No. INL/EXT-06-11464 / P. Pederson, D. Dudenhoeffer, S. Hartley, M. Permann. – Idaho: Idaho National Laboratory, 2006. – 116 p. doi:10.2172/911792
10. Panzieri, S. An approach to model complex interdependent infrastructures [Text] / S. Panzieri, R. Setola, G. Ulivi // IFAC Proceedings Volumes. – 2005. – Vol. 38, No. 1. – P. 404–409. doi:10.3182/20050703-6-cz-1902.00068
11. Dorogyy, Y. Development of the approach for designing, modelling and research of critical IT infrastructure [Text] / Y. Dorogyy // Technology Audit and Production Reserves. – 2017. – Vol. 5, No. 2 (37). – P. 34–41. doi:10.15587/2312-8372.2017.112495
12. BS ISO/IEC 17789:2014. Information technology. Cloud computing. Reference architecture [Text]. – The British Standards Institution, 2014. doi:10.3403/30268907
13. NIST SP 500-291. NIST Cloud Computing Standards Roadmap [Text]. – National Institute of Standards and Technology, 2013. doi:10.6028/nist.sp.500-291r2
14. Marcus, B. Interfacing NIST IoT, Big Data, and Cloud Models [Electronic resource] / B. Marcus. – October 5, 2015. – Available at: \www/URL: https://bigdatawg.nist.gov/_uploadfiles/M0450_v1_3857254727.pdf
15. BS ISO/IEC 27017:2015. Information technology. Security techniques. Code of practice for information security controls based on ISO/IEC 27002 for cloud services [Text]. – The British Standards Institution, 2015. doi:10.3403/30259620
16. BS ISO/IEC 27018:2014. Information technology. Security techniques. Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors [Text]. – The British Standards Institution, 2014. doi:10.3403/30266768
17. BS ISO/IEC 27036-4:2016. Information technology. Security techniques. Information security for supplier relationships. Guidelines for security of cloud services [Text]. – The British Standards Institution, 2016. doi:10.3403/30275201
18. BS EN ISO/IEC 27040:2016. Information technology. Security techniques. Storage security [Text]. – The British Standards Institution, 2015. doi:10.3403/30249804
19. IEEE P 2302™/D 0.2. Draft Standard for Intercloud Interoperability and Federation (SIIF) [Electronic resource]. – The Institute of Electrical and Electronics Engineers, Inc., January 2012. – Available at: \www/URL: https://www.oasis-open.org/committees/download.php/46205/p2302-12-0002-00-DRFT-intercloud-p2302-draft-0-2.pdf
20. ANSI/TIA-942-2005. Telecommunications Infrastructure Standard for Data Centers [Text]. – Arlington: Electronic Components Industry Association (ECIA), 2005. – Available at: \www/URL: http://www.ieee802.org/3/hssg/public/nov06/diminico_01_1106.pdf
21. BS EN 50173-5:2007+A2:2012 Information technology. Generic cabling systems. Data centres [Text]. – The British Standards Institution, 2007. doi:10.3403/30141480
22. ISO/IEC 24764:2010. Information technology – Generic cabling systems for data centres [Electronic resource]. – International Organization for Standardization, 2010. – Available at: \www/URL: https://www.iso.org/standard/43520.html
23. Shelimanova, Zh. V. Taxonomic scheme of cloud computing [Text] / Zh. V. Shelimanova, O. V. Yanovska, A. A. Furmanov // Radioelektronni i kompiuterni systemy. – 2015. – Vol. 74, No. 4. – P. 51–55.
24. Data Center Networking – Connectivity and Topology Design Guide [Electronic resource]. – Available at: \www/URL: https://www.cdigroup.co.uk/wp-content/pdf-documents/data-centers/Enterasys-Data-Center-Design-Guide.pdf
25. SLA for App Service [Electronic resource] // Microsoft Azure. – July 2016. – Available at: \www/URL: https://azure.microsoft.com/en-us/support/legal/sla/app-service/v1_4/
26. Murray, P. Cloud Networking Architecture Description [Text] / P. Murray, B. Melander, V. Fusenig, M. Meulle, L. Vaquero // Scalable and Adaptable Internet Solutions. – 2011. – P. 14–69.


## РАЗРАБОТКА МОДЕЛИ ВЫБОРА ОПТИМАЛЬНОЙ КОНФИГУРАЦИИ КОМПОНЕНТОВ АРХИТЕКТУРЫ КРИТИЧЕСКОЙ ИТ-ИНФРАСТРУКТУРЫ ПРИ ЕЕ ПРОЕКТИРОВАНИИ

Предложена модель, которая позволяет принимать решения относительно оптимального выбора компонентов критической ИТ-инфраструктуры на стадии проектирования. Модель дает инструментарий оценки вариантов архитектуры на базе критериев, таких как стоимость проектирования варианта архитектуры, эффективность и тому подобное. Применяя определенные настройки, предложенный инструментарий позволяет изучить каскадные эффекты взаимозависимости компонентов, провести оценку на этапе проектирования.

**Ключевые слова:** критическая ИТ-инфраструктура, Марковский процесс принятия решений, модель выбора конфигурации.

***Dorogyy Yaroslaw,*** *PhD, Associate Professor, Department of Automation and Control in Technical Systems, National Technical University of Ukraine «Igor Sikorsky Kyiv Polytechnic Institute», Ukraine, e-mail: cisco.rna@gmail.com, ORCID: http://orcid.org/0000-0003-3848-9852*