

Valeriia SOLODOVNYK<sup>1</sup>, Yuliia STEPANENKO<sup>2</sup>, Larysa MYRYTENKO<sup>3</sup>

Scientific supervisor: Andriy FESENKO<sup>4</sup>, Natalia LUKOVA-CHUIKO

DOI: <https://doi.org/10.53052/9788366249868.23>

## **BADANIE METOD I ŚRODKÓW OCHRONY CENTRALNYCH I ROZPROSZONE SYSTEMY INFORMACJI**

**Streszczenie:** Przeprowadzana jest analiza architektury scentralizowanych i rozproszonych systemów informatycznych. Rozważane są główne możliwości ich pojawienia się i ich uwarunkowania dla architektury danych. Rozważane są podejścia do ochrony przed podatnością systemu obu typów architektury i wyróżniane są najskuteczniejsze z nich.

**Słowa kluczowe:** rozproszone systemy informatyczne, centralizacja, serwer baz danych, telekomunikacja, użytkownik, administrator systemu, dostęp oparty na rolach, polityka, wymiana danych, aktualizacja, wsparcie techniczne.

## **RESEARCH OF METHODS AND MEANS OF PROTECTION OF CENTRALIZED AND DISTRIBUTED INFORMATION SYSTEMS**

**Summary:** The analysis of the architecture of centralized and distributed information systems is carried out. The main possibilities of their appearance and their conditions for data architecture are considered. Approaches for protection against vulnerability of the system of both types of architecture are considered and the most effective of them are singled out.

**Keywords:** distributed information systems, centralization, database server, telecommunication, user, system administrator, role based access, policy, data exchange, updating, technical support.

---

<sup>1</sup> Taras Shevchenko National University of Kyiv, Faculty of Informaiton Technology, Cyber Security and Information Protection: [valeriamin6@gmail.com](mailto:valeriamin6@gmail.com)

<sup>2</sup> Taras Shevchenko National University of Kyiv, Faculty of Informaiton Technology, Cyber Security and Information Protection: [juliasstepanenko2900@gmail.com](mailto:juliasstepanenko2900@gmail.com)

<sup>3</sup> Taras Shevchenko National University of Kyiv, Faculty of Informaiton Technology, Cyber Security and Information Protection: [myrutenko.lara@gmail.com](mailto:myrutenko.lara@gmail.com)

<sup>4</sup> Taras Shevchenko National University of Kyiv, Faculty of Informaiton Technology, Cyber Security and Information Protection: [aafesenko88@gmail.com](mailto:aafesenko88@gmail.com)

## 1. Formulation of the problem

The modern IT industry is characterized by a rapid growth in the number of information systems built using a variety of approaches and technologies. This trend is easily explained by the progressive development of computer structures and components of these systems. However, there are also problematic situations where government organizations, even with state-of-the-art equipment, can slow down this development. The main difference between distributed and centralized systems is, of course, the approach to their construction.

Figure 1 schematically shows the power of a distributed architecture.

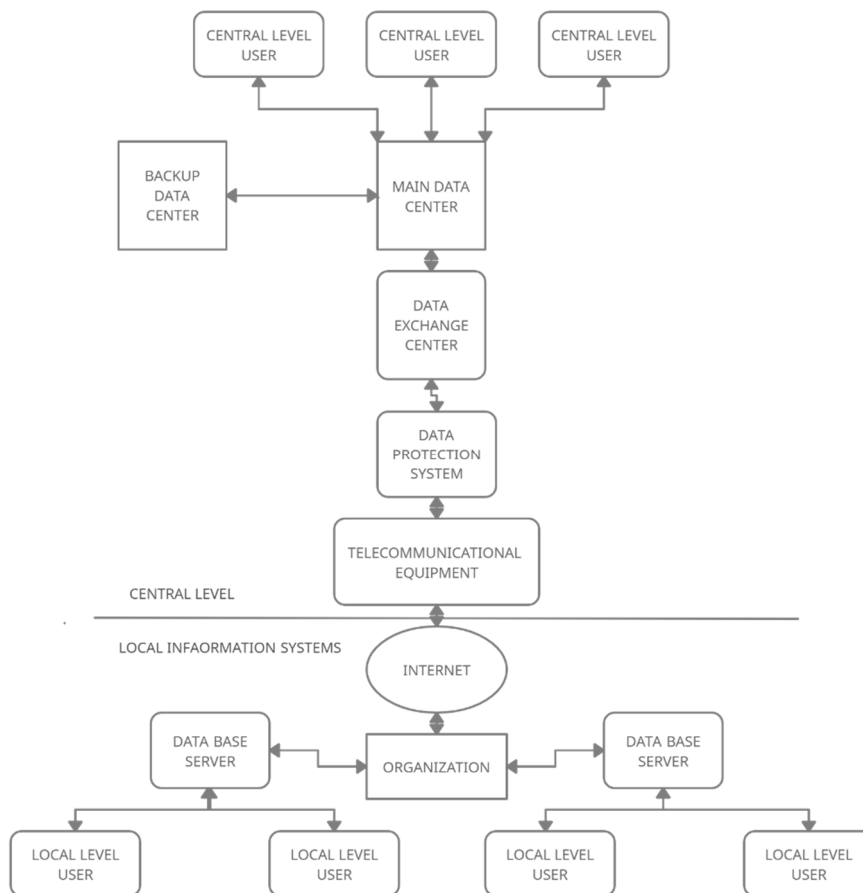


Figure 1. Distributed architecture scheme of information system

The main elements of the architecture shown in Figure 1 are:

- Main Data Processing Center - is responsible for storing and processing all data of the information system

- Backup Data Processing Center - responsible for fault tolerance
- Users - client software (software) in the technology of "thick client" (desktop).
- Database server, application server in the node - deals with storage, processing of all data in a particular node (local database in the node).

Required components of a distributed architecture system also include:

- Telecommunication network - provides connection and data exchange between different nodes. For example, the Internet or a corporate network.
- Information security system - is responsible for protecting each node of the system.
- Data exchange servers - are engaged in the implementation of data exchange between system nodes [1, 2].

The obvious advantages of this model are that it does not need to have permanent telecommunication equipment to communicate with the central level. We are able to transmit packets not only by telecommunication network, but also by external media. Also, the "thick client" interface is more ergonomic than the web-interface, especially during mass data entry operations through the user interface, although now this advantage is not significant.

Along with the positive characteristics of the use of distributed architecture are negative. The first disadvantage is that each node of the system has local databases, which complicates the exchange of information between them. However, the problem is not only in data exchange, but also in updating and technical support of operated systems. The presence of complex software elements such as database servers, applications, exchange and workstations does not facilitate the process of performing system tasks. It should be noted that for such an element as a database management system, which is one of the components of the system, there are options, both free and vendor, which in turn, if you choose the second option entails significant financial costs for implementation, support and service.

It is necessary to keep up with the constant updating of versions of all components, which compared to the centralized architecture is a significant item of financial and time costs. This is one of the most difficult tasks especially from the time of emergencies and depends little on data exchange algorithms. Another problem is that a distributed architecture has less flexibility and efficiency when creating new nodes in its architecture or moving them.

All these aspects affect the ability to ensure the required level of information security of the system, because at each node it all depends on the system administrator or manager, who may not have a sufficient level of responsibility for the rules of security systems. Problems also arise when there is a need to deploy a system point outside the physical boundaries of the organization. Also, maintaining the relevance of information circulated at the central level is a difficult conception for performers.

So at the moment we will highlight the following shortcomings of the architecture:

- There is a need for qualified system administrators in each node;
- Extremely high hardware costs and software licensing;
- Complex organizational chart of support and administration of each element of the system;

- Low or medium opportunities for quality information security.

Thus, speaking about the latest approaches to the development of information systems should address the issue of centralization of system architectures. Centralized information system architecture is a logical consequence of the development of telecommunications services, increasing their reliability and bandwidth, reducing the cost of data services, widespread penetration both in the geographical sense and among different segments of the population, business.

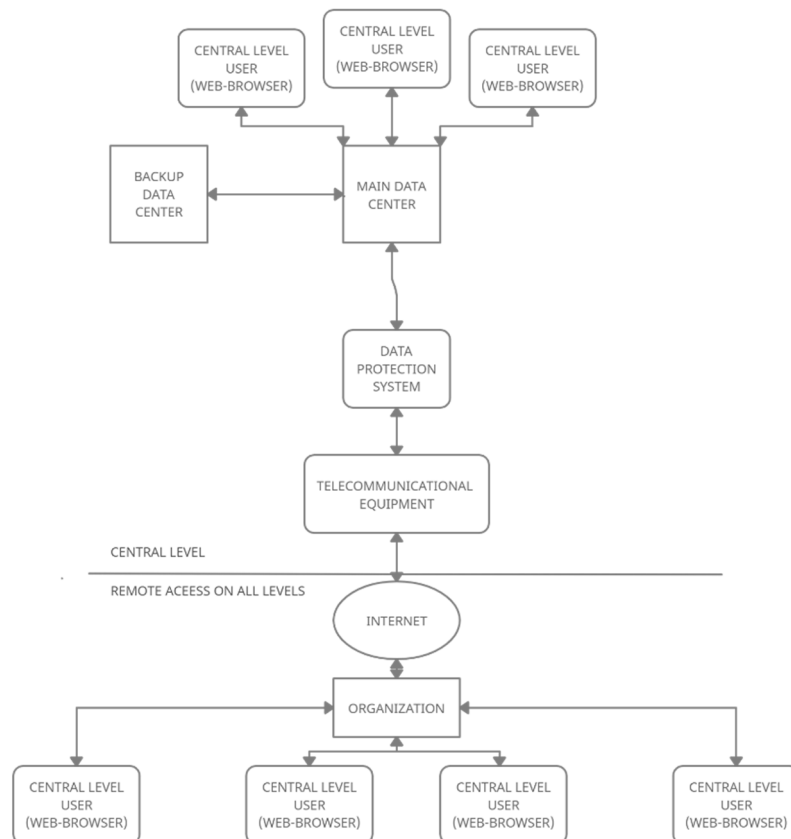


Figure 2. Centralized architecture scheme of information system

Figure two schematically shows the architecture of a centralized system. In this way we can see that this type of architecture consists of a powerful data center, the use of three-tier architecture and web-technologies.

The main elements of centralized architecture are:

- Basic Data Processing Center - is responsible for storing and processing all information system data and interacting with remote users. Is a critical element.
- Data Backup Center is the same. as distributed architecture. it provides fault tolerance, backup data storage of the entire system at the central level.
- Users are a client interface that provides data visualization and user interaction with the system.

The necessary elements are also:

- Telecommunication system, but here it already provides connection to the system and data exchange between remote clients;
- Information protection system, which is a critical element in the architecture of the central level of the system [1].

To better understand the benefits of this common architecture, here is a list that most fully describes them:

- In the centralized architecture there is one database with which all system users interact.
- On the client side there is no complex software and hardware complex. Therefore, accordingly, there are no significant financial costs for their maintenance, because the only necessary system elements are the operating system and web-browser. The list of station administration works and the number of qualified system administrators has been reduced.
- The above-mentioned three-level architecture - "database server - application server - client", allows you to use modern database management systems, web-browser as a software execution environment. There is also a lack of direct access to the central database, which significantly reduces the risks of its unauthorized modification. It is much easier to create new system nodes and implement remote access from client workstations.
- Using a single set of software for all users regardless of level, we can talk about a single way to access the system, control the rights used by the user to access and, accordingly, reduced costs for software development for the system.
- Centralized architecture is characterized by a wide range of scalability during critical system load.
- It should also be noted greater manageability compared to a distributed system, because to provide reliable organizational procedures in one center is much easier than to perform the entire procedure at all system levels.

Thus, a centralized model can significantly simplify the organizational and technical components of the creation, implementation, operation of the system, as well as information security.

It should be noted that the presence of both distributed and centralized architecture, one of the most effective options for protecting information systems is the introduction of the staff of a computer security specialist or the creation of special services, both private and centralized, based on the situation. It will be able to acquaint employees and in particular specialists of the Department of Information Security with past violations and involve them in the introduction of effective data protection practices.

Employees should be taught the basic rules of secure data handling and online security, as most attackers actively use social engineering as a means to attack the system.

It follows from the above that the use of two-factor authentication should be a prerequisite for providing access to the user, whatever the type of architecture. At the same time, role-based access policies to certain parts of the systems can be effectively implemented.

For these types of architecture, you should pay attention to such technology as network microsegmentation with the help of vlan. It is about isolating resources from

the rest of the organization. This is a very effective tool for tracking actions in the system.

Another good practice may be to log the actions and then send them to the SIEM. This will help the administrator to see at what time, from what part of the system certain instructions or information were sent and how it affected the operation of the system [3, 4].

## 2. Conclusion

The analysis of key aspects of the functioning of distributed and centralized information systems. The peculiarities of the functioning of these systems, which arose in accordance with the progress in the field of technologies and models of their implementation in accordance with the needs of organizations, are considered.

Models of distributed and centralized information systems are reproduced for a better understanding of their main differences, which were described for each of the types of systems. The vectors of the most effective actions for maintaining the security of information systems and optimal use of human resources during their operation are identified. It is determined that the use of the above algorithms for embedding security solutions will have a positive impact on the security of the system structure and information circulating there by means of delimitation of access and configuration of security policies at all levels of the system.

## REFERENCES

1. Comparative characteristics of distributed and centralized architecture in the context of creating modern information systems. Access: [http://www.medirent.com.ua/press-center/publications/information\\_systems\\_construction.html](http://www.medirent.com.ua/press-center/publications/information_systems_construction.html).
2. Information protection strategies. Access: <https://buklib.net/books/28625/>
3. Segmentation strategies. Access: <https://docs.microsoft.com/ru-ru/azure/architecture/framework/security/design-segmentation>
4. How To Protect Your Business From A Data Breach: Seven Key Steps. Access: <https://www.forbes.com/sites/forbesfinancecouncil/2018/03/08/how-to-protect-your-business-from-a-data-breach-seven-key-steps/?sh=397caf5e6b68>
5. Top 15 ways to prevent data and security breaches. Access: <https://bigdata-madesimple.com/15-ways-to-prevent-data-security-breaches/>
6. TANENBAUM A.S., VAN STEEN M.: Distributed systems principles and paradigms 3rd ed., distributed-systems.net, 2017.
7. Major Centralized Systems are Hacked Multiple Times a Year. Access: <https://medium.com/@AxelUnlimited/major-centralized-systems-are-hacked-multiple-times-a-year-9c2ad612462b>