Introduction

The duty of the administrator of computer systems and networks is to ensure reliability of the company or institution that use informatics solutions. IT administrator's job should not be burdensome for other workers, particularly should not lead to interruptions in work related to the maintenance or servicing of entrusted equipment. Information systems administrator's job boils down to "putting out fires" in most cases, i.e. a rapid response to sudden problem hindering or preventing the work of the institution. Employees are joking in such situations that they finally have a chance to get to know the IT administrator - to the next failure. It should be emphasized that such situations are usually the result of unforeseen events. Sometimes such situations are results of erroneous opinions of institutions management concerning the responsibilities and time that must devoted to inspection and service by administrator. Thus IT administrators usually do not have enough time or motivation to work to prevent breakdowns. Moreover failures can be the result of negligence, what is the result of network administrator error resulting from ignored warning messages. If it comes to the necessity of "putting out fires", it is too late for prevention. Assuming that the failure carries no risk of data loss, and only the network traffic restrictions or disable less critical equipment, lack of prevention can go without consequences. In the case of damage of important devices or storage media, the situation becomes complicated for the management of the company and can, in extreme cases, lead to substantial perturbations in the execution of tasks of the company. In this case part of the blame falls on the IT administrator, who faces the problem of much greater importance than just for example a printer repair. The authors were forced to solve this kind of problem and also to develop and to implement preventive measures.

Available IT EQUIPMENT

Castle Hill in Kielce is a public institution consisting of the Centre for Civic and Patriotic Thoughts (OMPiO) and the Institute of Design (IDK). A computer network was organized in three subnets. The first is a network connected to the city of Kielce structural network through the Cisco router 867VAE-k9 functioning as a main gate, the second is a subnet for the administration of the institution and IDK connected through router TP-Link TL-WR940N functioning as a DHCP server for employee terminals. The third is a subnet separate of previous two, dedicated to the needs of OMPiO and connected via a TP-Link TL-WR740N. Multimedia museum exhibition composed of 8 multimedia projectors, a few web cams, several touch screens and a multimedia lighting system exposure operates as part of the OMPiO. Everything is controlled through a local network using a Dell server exposure. In addition, each of the projectors is assigned to a network media player. As part of the IDK there are two graphic workstations (Dell Precision T1700 and the Dell Precision R7610CTO), two network storage servers (Lenovo iOmega ix4-200d and the QNAP TS-420U), an auxiliary storage in the form of a USB drive (i-tec MySafe 2.5 "), a magnetic tape drive (Hewlett-Packard StorageWork DAT 160), four large universal access printers (Dell 2155cdn, Konica-Minolta C220, Canon iPF8300S) and several local network printers. All of this is monitored using a network server (Hewlett-Packard ProLiant DL120G6) and secured uninterruptible power supply (BlueWalker BlueW VI 3000RT and three APC Smart-UPS SC 1000). All of the hardware, with the exception of printers and two power supplies APC is mounted in a single rack cabinet 19 ".

---

1 Technical University of Kielce, Faculty of Management and Computer Modelling, Kielce, Poland, d.krzesimowski@tu.kielce.pl
2 Technical University of Kielce, Faculty of Mechatronics and Machine Engineering, Kielce, Poland, sciana@tu.kielce.pl
The genesis of failure and a temporary solution

At the beginning of December 2014 the equipment mentioned above was presented a bit differently, namely in the network functioned only one storage data node: iOmega, one uninterruptible power supply for monitoring server and there was no router TP-Link TL-940N. The simplified diagram of the computer network at the beginning of December 2014 is shown in Fig. 1. At that time, a decision was made to reorganise the network in terms of control of devices connected to the network wirelessly and increase readability of IP addressing for terminals. The decision was the result of start-up Italian Design School launched in October 2014 by IDK. Because of the large number of participants that connected their devices to the network, throughput dramatically decreased, especially on a link from the gate to the building of IDK. In addition, Cisco 867VAE-k9, which at that time worked as a DHCP server for all terminals, had not been configured to limit the data rate for a particular pool of IP addresses and MAC address filtering. School activities were associated with the generation of graphics file, which sizes significantly exceed of 100MB, transferred to and from iOmega network storage and external file servers. At the same time, most participants did not keep copies of these files on their devices, which was also the practice followed by all employees IDK as well as OMPiO and administrative staff. This meant that the data were stored in only one place, and movement from and to the nodes within the local network was like urban traffic jams during rush hours. The described data flow is presented in Fig. 2.

Fig. 1. Simplified diagram of the computer network at the beginning of December 2014.
Source: own work
The simplest solution, that increases the security of the network, was the purchase of another router and after the first edition of the course to create new, independent from the main gate, configurable corporate subnets. To that network has been connected to a router that controls a network of exposure, for all devices connected permanently to the local network, assigned fixed IP addresses, company devices uses DHCP, it was made available pool of IP addresses based on MAC. Devices do not registered as a company obtain the address of a separate DHCP pool, by binding prevented from connecting to the network via the previously set IP address that is not in the DHCP scope, this solution is presented in Fig. 3. In order to control the data rate was introduced in the network upload and download limits for each pool of IP addresses, giving the highest priority for wireless switches, server monitoring, printers and data nodes. Still, the data of all employees and members of the course were stored in a single node. Graph of data flow after rebuilding of the computer network in December 2014 is shown in Fig. 4.

---

**Fig. 2.** Graph of data flow at the beginning of December 2014.  
*Source: own work*

**Fig. 3.** Simplified diagram of the computer network at the end of December 2014, after changes in the IP addressing of terminals.  
*Source: own work*
The iOmega network drive was reorganized in RAID 5. A decision concerning such an organization of four drives 1 TB had to provide immunity to the failure of one disk and to provide users 3 TB of space for data. Furthermore, an important factor was an increased reading speed compared to the disc not held in such an array. The disadvantage of such a solution is a reduced writing speed due to the necessity of calculating checksums and reduction the access time to data in case of failure of one disk. In addition, the matrix reconstruction after replacing a damaged disk is an expensive operation in terms of computing. The risk of damage to another disk is increased in such situation, resulting in the loss of some data. The data storage node was not protected from lowering or power loss by uninterruptible power supply that is graphically explained in Fig. 5. This was the direct cause of physical damage of one drive just after the reorganisation of the network due to a power failure. It should be emphasized that this failure was not associated with work in the institution. Shortly after power was restored, iOmega driver started the procedure to recover the data on the basis of parity bits stored on three properly operating hard drives. In the meantime, there was another power outage, resulting in logical damage to another disk. After the power was restored the driver tried to recover the data, but in this case it was no longer possible.

![Graph of data flow at the end of December 2014, at the time of failure of the network storage node.](source: own work)

Castle Hill institution did not have the hardware or software that allows reading data from damaged disks and RAID reconstruction on independent drives. The data recovery was possible only in case of failure of a single disk, not being part of the structure of RAID. All hard drives of iOmega devices have undergone the procedure to recover data in an outside company, which significantly hindered the work in the institution, especially for IDK staff and training participants. Finally was recovered 95% of the data from the damaged RAID 5 matrix. Until the network drive was repaired, substitute action was taken in the form of access to the network resource with a size of 150 GB on Hewlett-Packard ProLiant control server, for the most important data: human resources and accounting.

Monitoring server is equipped with two data disks with a capacity of 250 GB each, arranged in RAID 1 and 60 GB disk for the operating system. Only administrative and financial staff can use this resource. At the same time, measures were taken to ensure the reliability of recording and storing data taking into account the need to use the emergency power supply and backup all the data on independent drives. Also it is taken into account the network traffic generated by different terminals and storage nodes, resulting from read and write the data, also associated with backup operations.
**Target solution**

The target solution includes the expansion of the network of high-performance graphics workstations (Dell Precision R7610CTO with two 600 GB SAS disks and one 250 GB SSD), an auxiliary graphics station (Dell Precision T1700 with two 1 TB drives), 16-port switch (Cisco SG100-16-EU), uninterruptible power supply (BlueWalker BlueW VI 3000RT), the server disks (QNAP TS-420U) with four disks with a capacity of 1 TB each. All of this was supplemented by an additional USB drive designed for emergency backup of HR and accounting data (i-tec MySafe 1 TB) and a magnetic drive (streamer, StorageWork Hewlett-Packard DAT 160) with a set of 7 160 GB DAT tapes. A distributed storage system, described above, has been operating since May 2015.

![Diagram](image)

**Fig. 5.** Power scheme of network nodes in December 2014. *Source: own work*

To increase the possibility of data recovery in case of failure within the computer network of Castle Hill, it was decided to reorganise the method of recording data to the iOmega network device. Currently four drives (one new) 1 TB each are organized in a RAID 0 + 1. This enables the employees use 2 TB of data. It is a matrix implemented as RAID 1, whose elements are RAID 0. So organized drives are characterized by the speed of RAID 0, which with data interleaved between the disks. The disadvantage is the increase in the cost of data storage in comparison with the previous solution (RAID 5). Another disadvantage is necessary to shut down the entire logical drive in case of failure of one of the physical disks. Considering the facilitation of recovery from a single physical disk, as compared to the recovery of data from the matrix, the best solution for four drives iOmega device would be to use a RAID 1 + 0. It is a matrix implemented as RAID 0, which elements are RAID 1. In the case of a single disk failure it is possible to recover lost data
without the need to mount his "partner" from the matrix. Unfortunately, the iOmega device driver does not provide the possibility of organizing drives in a RAID 1 + 0.

In the case of failure of one disk, IT administrator will replace it and start rebuilding the array. In the case of failure of two disks there is a possibility to recover the data using the resources of Castle Hill by launching two efficient drives in an external device having a free two SATA ports and an additional drive that can be a USB drive with an operating system. All employees and participants of design school use the iOmega network node to exchange data between terminals within the internal network.

Graphics workstation is available only to employees of the IDK as the main computing device and storage for graphic works. It has a 250 GB hard disk intended for an operating system and software, and two hard disks with the capacity of 600 GB each organized in the RAID 1 array. This type of disk organization is based on replication of the work of two or more physical disks. Established space has the size of smallest drive. Such a solution, despite of the ease in data recovery from damaged drives could not be used in the device iOmega, where capacity of resources available to users has a priority. The presence of these drives significantly reduces the device iOmega read and write operations, which aims to increase the processing speed and reliability of this node. Graphics software is installed on the graphic station, available to users through a remote terminal application. This allows to control both access to software and licensing decisions and future purchases, through monitoring the usage of the software that remains on the state in Castle Hill. In addition, end terminals of IDK employees are relieved, have are exempted their local storage resources, and organization of labour is improved through sharing of software between several people within a single license. It should be noted that at the same time only one user can use this kind of software. This approach works in Castle Hill through the efficient division of tasks between employees of IDK.

For the remaining employees in Castle Hill and for the participants as well as for employees of IDK, was launched a secondary graphic station. Two hard drives with a capacity of 1 TB each, organized in a RAID 1 array, are installed. On the secondary graphic station free software is installed, also for commercial applications, as well as temporary versions of the software that are tested by the employees of Castle Hill. It should be noted that this applies to any software reported to IT administrator. Central sharing and storing some data on server resources allows relieving the iOmega node and makes it easier to recover data in the event of failure of one of the nodes. It should be noted that has been retained access to the resource on the monitoring server for employees HR and accountant employees.

The server drives, with four drives of 1 TB each, works as a cumulative backup storage for all described four data storage nodes: monitoring server, iOmega, graphics server and the secondary graphics server. It is the most important and best-protected storage node in the whole Castle Hill institution. Simplified diagram of existing connections in the described computer network is shown in Fig. 6.

The main storage nodes are equipped with SATA hard drives with a capacity of 1 TB. iOmega node is equipped with three Seagate Barracuda LP and one Western Digital 10EZRX series Green. The second of mentioned discs is a superset, after a single failure of Seagate. In Castle Hill another one drive WD Green, treated as an emergency storage, is unused. The server QNAP is equipped with a four drives WD 10EFRX series Red. Seagate provide a transfer rate at 300 MB/s, sustained data rate of 95 MB/s, average latency 5.5 ms [1]. WD 10EZRX drive is faster, transfer rate is 750 MB/s and sustained data rate is 150 MB/s [2]. Exactly the same parameters are characterized by WD 10EFRX [3].
Fig. 6. Simplified diagram of the computer network in May 2015, after the extension of this network with new storage devices and workstations.

Source: own work

Also, average latency for both WD is 4.2 ms. The difference between the disks WD Red and WD Green is associated with resistance to vibration. Series Green is not protected in any way, so these discs require less power than disks of series Red. Seagate also does not have protection against vibration, but characterised by reduced energy consumption, hence the decision to cooperate both types of disk in one device iOmega. In turn, QNAP server is equipped with four WD drives series Red resistant to vibration, which increases the security of the stored data. This is important if one takes into account that this server is not permanently attached to the skeleton RACK cabinets.
The data flow within the network

Access to the network resources on each node and the maximum allowable bandwidth usage are dependent on the kind of a node: network devices, employees and participants of the courses. These groups are shown in the Table 1.

Table 1. Table of rating of network nodes.

<table>
<thead>
<tr>
<th>Number of IP addresses in the main IP pool</th>
<th>Group description</th>
<th>MIN download (kbps)</th>
<th>MAX download (kbps)</th>
<th>MIN upload (kbps)</th>
<th>MAX upload (kbps)</th>
</tr>
</thead>
<tbody>
<tr>
<td>50</td>
<td>network devices</td>
<td>47000</td>
<td>95000</td>
<td>47000</td>
<td>95000</td>
</tr>
<tr>
<td>100</td>
<td>company terminals connected without DHCP</td>
<td>15000</td>
<td>75000</td>
<td>15000</td>
<td>75000</td>
</tr>
<tr>
<td>18</td>
<td>company terminals connected with DHCP</td>
<td>15000</td>
<td>50000</td>
<td>15000</td>
<td>50000</td>
</tr>
<tr>
<td>77</td>
<td>DHCP pool for foreign terminals</td>
<td>10000</td>
<td>15000</td>
<td>6000</td>
<td>10000</td>
</tr>
<tr>
<td>9</td>
<td>DHCP pool for registered foreign terminals</td>
<td>12000</td>
<td>20000</td>
<td>8000</td>
<td>15000</td>
</tr>
</tbody>
</table>

Source: own work

Access to network resources has been developed as follows:
- HR-accountant section has access to the resources on the monitoring server and iOmega device;
- the remaining administrative staff has access only to the node iOmega;
- course participants can gain access to the node iOmega and the auxiliary graphic station;
- IDK workers gained access to resources of iOmega, graphic stations and an auxiliary graphic station.

It should be noted that none of the groups of employees do have access to the resources of the storage node. The objective is to improve the safety and flow control. An innovative template for copying data between personal workstations and the storage nodes for increase possible security of information was implemented. Innovation consists in the organisation of the data flow on the network in such way as to reduce the load on the network and not to cause overload. Furthermore, the safety of data in the event of failure of several devices and the flexibility to reorganize the network until the failure will be fixed must be ensured.

HR and accounting data from terminals of workers of this section are automatically and periodically copied to monitoring server. These data never get to nodes shared to any of the other user groups. Other undisclosed data by the workers' group can be manually stored on the iOmega resource. The results of the graphical workers of IDK sections are stored in graphic station node, occasionally in the iOmega node and auxiliary graphic station. The course participants write the results of their work primarily in the secondary graphic station and to a lesser extent in the iOmega device. All resources, except for personal terminals, are available from the monitoring server and are periodically tested for the presence of unwanted software. In addition, each of the servers and terminals has its own anti-virus and firewall system, which increases the level of protection of the internal network.
Periodically data from all public network nodes are automatically stored in the main storage node. In addition, HR and financial data are stored automatically on the USB external drive that is connected to a server QNAP, and periodically manually on magnetic tapes, along with other important data. Therefore, at any given time, there are at least two users’ copies of the data in the network nodes and four copies of the HR and financial data.

The number of copies of data may be greater due to their presence on local hard disks of terminals. It should be noted that because all these devices are in one RACK cabinet and are connected via a single switch (Cisco SG100-16-EU) network load during backup is almost no noticeable for the users of terminals connected to the network. Graph of data flow in currently existing computer network is shown in Fig. 7.

Fig. 7. Data flow graph in May 2015, after the rebuilding of the computer network.

*Source: own work*
Additional security solutions

In order to prevent repetition of the situation from December 2014, same steps were taken to protect equipment against power failure. For these purposes, two uninterruptible cascade-connected power supplies were used. The main power supply is BlueWalker BlueW VI 3000RT, to which APC Smart-UPS SC 1000 is connected. BlueWalker power supply provides power protection for both graphics servers, monitoring server and for the Cisco switch. Additionally, it also provides over voltage protection for network used in the RACK cabinet. To the APC device storage devices are connected: iOmega and QNAP. In addition to the QNAP file server the secondary hard disk i-tec is connected. The decision of such list of connections between devices results from the fact that the highest priority was given to protecting data at the expense of failure of server operating systems. Operating systems can be reinstalling using optical discs without any problems. Software and data should be protected in the best possible way. It is possible to periodically save an important data on optical discs or magnetic tape drives, but it is not effective solution from the point of view of frequent updates of data and the need to archive media in physical locations. For this reason, streamer HP is used "on demand" and in case of necessary archiving of project documentation as well as HR and accounting. The total capacity of the magnetic tape 1120 GB is sufficient to hold the most important data for at least several years. HP streamer is connected periodically to a portable device with necessary drivers and operational system installed. The data on tapes are recorded by the network, directly from storage devices without necessity to make copies of the data on a device that supports streamer. Two additional APC Smart-UPS SC 1000 secure the two IDK graphic terminals with rendering software installed. Because most software of this type has been reinstalled on the graphics workstation, it is planned to protect the said power supply terminals HR and accounting terminals. This solution is presented in fig. 8.

Failure scenarios

Along with the reorganisation of the hardware of IT resources of Castle Hill the method of operation has been developed in the case of failure of individual network nodes. In the case of failure of the working terminals they will be replaced with new devices, network connections will be restored and, if necessary, data will be restored from a network location on local drives.

Procedures have been developed in the case of three different emergency situations for the network node iOmega. The first case involves physical or logical damage to one drive. This situation will not stop the operation of this device. Network and system administrator will notice a crash when viewing a log file of iOmega device. Resolving the emergency situation requires turn off the device, replacing a failed drive with a good one, being out of stock of the same capacity and switching on the machine. A damaged disk can be diagnosed at any terminal equipped with two free SATA ports. The second case involves physical or logical damage to two drives of the iOmega device. In this case, the device stops working, therefore failure is detected immediately. The administrator should turn the device off and find out which disks are damaged.
If two disks grouped in RAID 0 were damaged there is possibility to read the contents of the second group RAID 0, in which case there is no loss of data. So shaped disk group will be used to rebuild RAID 0 to RAID 0 + 1. The read data can be copied to the free resources to any terminal or to a portable drive. It is advisable to determine what kind of damage occurred. The physical failure eliminates disk from further work, while reformatting and re-inclusion in the matrix structure can repair logic failure. There is also a necessity to rebuild a matrix complementing irrevocably damaged disks.

If there is damage to one disk in the sections RAID 0, data recovery may be possible inside Castle Hill provided that the damage concerns disks containing various pieces of data (half RAID 0), thus matching each other. In such a situation, there is a theoretical possibility to match RAID 0 from healthy disks and
read data from them. On the other hand, if there is damage to the discs that cannot be paired, data recovery will not be possible using hardware and software in Castle Hill. Every user of iOmega should be informed about the breakdown, which aims to clarify the situation and abandonment of work on stored data, to appeal. If the removal of faults will require sending hard drives for recovering the data, users can be switched to form an ad-hoc emergency magazine (e.g. graphical auxiliary station) or to the main storage node. This is a possible thanks to keeping identical structure of the file and folder in comparison with the storage source, during backup operations.

Procedure in the case of damage to one of SAS drives in the graphic station includes disabling the drive and off grouping drives in a RAID array until replacement the hardware. In the graphic station to six hard drives can be installed simultaneously. Because in the configuration in Castle Hill one drive (250 GB SSD) is intended for the operating system and graphics software, it remains five disks for data. Installation of additional drives will increase data security and, with four drives, makes it possible to reorganisation of the matrix to the level of RAID 1 + 0, which would facilitate potential data recovery process. In the case of damage to the two currently installed disks it is possible to recover the data separately for each disk on any terminal with a free port SATA or SAS. It is worth emphasizing that damage of both SAS drives does not result in an interruption in work of the whole graphic station. Only damage to the operating system disk will trigger such a situation.

Damage to one of the two hard drives in the auxiliary graphic station also does not disable this network node. Damaged disc can be checked at any terminal and in case of logical damage repaired and re-incorporated into the structure of the auxiliary graphic station in a very short time. Damage to the two drives will interrupt the operation of this network node, while the data can be recovered within the possibilities existing in Castle Hill.

Procedure in the case of failure monitoring server drives is the same as in the case of the graphic station. The difference lies in the reaction speed in such a situation. Because the monitoring server is used to coordinate the backup, any failures must be detected and eliminated as quickly as possible. Because there is the possibility to coordinate backup through software installed on the device iOmega, from the beginning of July 2015 this node will be the coordinator of backups. This solution increases data security through the fact that iOmega device is powered by a final stage of cascade of uninterruptible power supplies. In addition, iOmega device software is resistant to almost all currently known malicious software. [4]

There are procedures prepared against three emergencies within the server QNAP drives. The first case is a failure of one disk. The node will operate without interruption and information about the breakdown will appear in the server log. Data can be, if necessary, recovered, the hard drive must be replaced or repaired. In the case of failure of two hard drives with different sections RAID 0, if it is possibility to assemble them together, the node will continue to run. In the case of corruption of hard disks that cannot be combined in a pair, the node will be turned off. In this case, the data from each disk can be recovered individually on any terminal with a free SATA port.

In case of damage to the spare disk i-tec, like in the case of magnetic drive, will cause the necessity mount another drive of this type and will not affect the work in Castle Hill. In the event of several crashes at the same time, the action taken in accordance with the priorities are presented in Table 2.
Table 2. List of priorities for the purposes of emergency activities.

<table>
<thead>
<tr>
<th>Priority</th>
<th>Network node</th>
</tr>
</thead>
<tbody>
<tr>
<td>Low</td>
<td>Working terminals</td>
</tr>
<tr>
<td>Moderate</td>
<td>Auxiliary graphic workstation</td>
</tr>
<tr>
<td>High</td>
<td>Graphic workstation</td>
</tr>
<tr>
<td>High</td>
<td>Monitoring server</td>
</tr>
<tr>
<td>Very high</td>
<td>Storage node iOmega</td>
</tr>
<tr>
<td>Very high</td>
<td>Storage node QNAP</td>
</tr>
<tr>
<td>Moderate</td>
<td>Storage device HP StorageWorks</td>
</tr>
<tr>
<td>Moderate</td>
<td>Storage device i-tec</td>
</tr>
</tbody>
</table>

Source: own work

The first real test and conclusions

Administration of network and information systems involve a huge responsibility. This is particularly true in the case of the responsibilities for the protection of data, including personal data. Limiting activity to storage data on local terminals or single network node is often not sufficient to threats posed by reality. In this paper is described a case of a random event that caused the need to rebuild the network in the public institution of Castle Hill. Described failure was associated with loss of power source, which in turn was the cause of disk damage of the sole storage node. As a result of the failure, analysis were developed and a complex method of transferring data within a local network and secured individual storage nodes and workstations from power problems was implemented. In the event of a failure within the node the emergency procedures, the observance of which aims to restore the efficiency of the network and resources to the state before breakdown, were developed. At present the data in Castle Hill is stored in multiple copies on different network nodes and can be readily replicated to removable media at any time. All these solutions contribute to the effective increase of data security.

At the time of writing this paper, at the beginning of June 2015, in Castle Hill was a power failure, which was repaired after 27 hours. According to the assumptions after three hours, as a result of discharging of the battery of first stage power system, graphics workstations and monitoring server were turned off. The second stage worked without interruption for the next 24 hours providing power to the storage nodes. When the power returns, previously switched off servers have been automatically switched on. The power off of the network storage devices has not occurred. The log files that illustrate this situation are presented in fig. 9.

This event is a confirmation of the effectiveness of the solutions developed and implemented in the presented system even in situations of prolonged power failures that occur extremely rarely. The authors hope that the article will be inspired to take similar action in other companies or institutions before occurs to troublesome consequences of failure. The described solution can be developed through further cascading protection of important network nodes. The main limitation of this method is the maximum load current of existing power grid. For this reason, it is recommended to connect the power cascade to separate electrical circuits, but such issues often go beyond the responsibilities of the IT administrator.
Abstract

Protecting data stored in digital form is now one of the most important issues in enterprises and institutions. Currently complete data security is not guaranteed by the single network storage node. A distributed system, in which data is stored in multiple locations simultaneously, becomes a standard. It means duplication of information within a single storage node and within the nodes independently powered and managed. In the paper is presented the proposal of the functioning of medium-sized computer network with an innovative method of saving data.

Keywords: computer network, data flow, data storage, power failure, data loss

References


