KAPITEL 8 / *CHAPTER 8* [8]
DESIGN OF PROTECTED SERVER ROOMS BASED ON CISCO EQUIPMENT IN CLASS A OFFICE BUILDINGS

DOI: 10.30890/2709-2313.2024-32-00-023

Introduction

It is difficult to imagine a modern organization without a server IT system. Being a key link of the IT infrastructure, the server is an expensive and at the same time the most vulnerable part of the entire complex of computing and telecommunications equipment. It has always been the main target of virus attacks and attempts of unauthorized access to the system, so special attention should be paid to protecting the server room from these threats. At the same time, until recently, due attention was not paid to equally important causes of failures: unfavorable environmental conditions, for example, water leakage from the upper floor, as well as changes in the physical parameters of the equipment.

Most organizations using information systems locate them in premises often not intended for these purposes, which, of course, cannot but be reflected in the work of server equipment. The more functional and accurate the IT system, the more capricious and sensitive it becomes to the influence of negative external factors. This, first of all, refers to the servers that support the life of the entire network.

The most effective method of solving this problem is the use of an integrated approach to the creation of so-called protected server premises. Special equipment located in such rooms creates artificial conditions for the optimal operation of the equipment located in the server room, and also limits physical access to the room. But before making such a decision, the organization must "grow up", as it requires significant financial investments. Decisions about special equipment of a protected server room for the "heart of the IT system" are made by enterprises that have realized the need to optimize their information infrastructure, increase the efficiency, reliability and manageability of systems, as well as reduce the total cost of their ownership.

[8] ***Authors:*** *Antonenko Artem Vasylovych, Golubenko Oleksandr Ivanovych, Lashchevska Nataliia Oleksandrivna, Lemeshko Andriy Viktorovich, Balvak Andrii Anatolijovych, Mishkur Yurii Valentynovych, Solskyi Danyil Yaroslavovich, Ziniar Denys Arkadiiovych, Buriak Myroslav Serhiiovych, Prykhodko Andrii Pavlovich, Fedorenko Maksym Andrievich, Avramchuk Roman Serhiyovich*

8.1. Server room and organization requirements. Classification of date centers

Data centers (data centers) are divided into 4 categories - Tier 1, Tier 2, Tier 3 and Tier 4 (Tier 4 is the highest category). Compliance of one or another category indicates the level of reservation and infrastructure, physical security and reliability of both the infrastructure part and the structure as a whole. The official compliance of the category is confirmed by the Uptime Institute or TIA (Telecommunications Industry Association). There are four levels associated with different degrees of infrastructure readiness of data center equipment. Higher levels indicate not only higher readiness, but also cause increased construction costs. In all cases, higher-ranked levels include the requirements for lower-ranked levels. A data center may have different tier ratings for different parts of its infrastructure. For example, a data center may have a rating of Level 3 for electrical equipment, but Level 2 for mechanical equipment. However, the overall rating of this data center is the lowest in all parts of its infrastructure. Thus, if a data center has a level 4 for all parts of the infrastructure except electrical equipment, where the rating is 2, then the entire data center receives a rating of 2. The overall rating of the data center matches the rating of the weakest component. Attention should be paid to maintaining the functionality of mechanical and electrical systems at the correct level, as the load on the data center increases over time. A data center may drop from tier 3 or 4 to tier 1 or 2 as spare capacity is used to support new computing and telecommunications equipment. To be rated at any level, a data center must meet the requirements of the applicable data center standard. Although the concept of tiers is useful for establishing tiers within different data center systems, it is possible that circumstances may require some systems to have higher tiers than others. For example, a data center located in an area where local grid power is less reliable than the national average may be designed with a Level 3 electrical system, but the project's mechanical systems may only be Level 2. These mechanical systems can be provided with increased with the number of spare parts in order to ensure a low value of the MTTR (mean time to repair). It should also be noted that the human factor and operating techniques can also be very important. In this regard, the actual reliability of two level

3 data centers can be completely different. This section describes the four tiers of data center infrastructure as first defined by The Uptime Institute in their newsletter Industry Standard Tier Classifications Define Site Infrastructure Performance).

Tier 1: basic server. A tier 1 data center is a base tier server room without redundancy (redundancy). It has a single path for power distribution and cooling without redundant (redundant) components. Availability level 99.671%. At the first level, no more than 28.8 hours of idle time is assumed during the year. UPS and generators are single-module systems and have many single points of failure. Critically important loads may be subject to disconnection during preventive maintenance and preventive maintenance. A level 1 data center is prone to disruptions in the normal course of work from both planned and unplanned actions. It has power distribution and server room cooling systems, but may or may not have raised floors, a UPS, or a generator. If there are even UPS or generators, they are single-module systems and have many single points of failure. Every year, the infrastructure has to be completely shut down to perform preventive maintenance and preventive maintenance work. Urgent needs may require more frequent outages. Errors during operation or involuntary disconnection of the object's infrastructure components will interrupt the normal operation of the data center.

Tier 2: server with redundant components. A tier 2 data center has redundant (redundant) components, but only one path. It has a single path for power distribution and cooling, but has redundant (redundant) components on that distribution path. Assumes an annual downtime of 22 hours, which means 99.749% availability. Level 2 server equipment with redundant components is somewhat less prone to disruptions in the normal course of work from planned and unplanned actions than a basic data center. In this case, a false floor, UPS and generators are installed, but the project has an N+1 rating (Need plus One), which means a single-flow distribution path throughout the area. Maintenance and repair of the critical path of power supply and other elements of the object's infrastructure require stopping the data processing process.

Tier 3: with the possibility of parallel repairs. A Tier 3 server has multiple power and cooling paths, but only one path is active. Since the redundant components are not on the same distribution path, this system allows maintenance and repairs to be carried out in parallel with the operation of the data center. Unplanned outages are reduced to one event lasting 4 hours every 2.5 years, an average of 1.6 hours per year. Tier 3 shows an availability of 99.982%. The facility must be manned 24 hours a day. The capabilities of Level 3 allow you to carry out any planned activity of the object's infrastructure without any disruption to the normal operation of the technical equipment of the server room. Planned activities include preventive and programmatic maintenance, repair and replacement of components, installation or removal of components that affect performance, testing of components and systems, etc. On large facilities using water cooling, this means having two independent sets of pipes. Sufficient power and distribution capabilities must be available to simultaneously support the load on one path while performing repairs or testing on the other path. Unplanned actions, for example, errors during operation or involuntary failures of the infrastructure components of the object, will still cause an interruption of the normal operation of the data center. Level 3 facilities are often designed with the prospect of scaling resources to Level 4 when the business justifies the cost of the additional protection.

Tier 4: fault tolerance. A Tier 4 data center has multiple active paths for power and cooling distribution. Since in a level 4 data center at least two paths are normally active, the infrastructure provides an increased degree of fault tolerance. Refusals reduced to one 4-hour incident over a five-year period. Individual failures of equipment or communication channels are possible, but they do not affect the operation of computer equipment. Tier IV demonstrates 99.995% availability. Level 4 servers provide several ways to supply power to all types of computing and telecommunications equipment. Level 4 requires that all computer and telecommunications equipment have multiple power inputs. The equipment must be able to continue to function when one of these power inputs is disconnected. Equipment that does not have multiple built-in power inputs requires automatic switches (to switch to another electrical line) without interruption. Level 4 provides for the possibility and ability of the facility's infrastructure to allow any planned activity without disrupting the normal operation of the critical load. Fault-tolerant functionality also ensures the ability of the facility's infrastructure to withstand at least one worst-case failure (or event) without impacting the mission-critical load. This requires simultaneous activity of the distribution paths, usually in a "System + System" configuration. In terms of electrical equipment, this means having two separate UPS systems where each system has N+1 redundancy. Due to fire safety and electrical safety regulations, there will still be some downtime impact due to fire alarms going off or staff initiating the Emergency Power Off (EPO) process. Level 4 requires that all technical equipment in the server room have dual power supply, as specified in the Fault-Tolerant Power Compliance Specification of the Institute for Operational Problems.

A Level 4 facility infrastructure is most compatible with a high-availability IT concept that uses central processing unit (CPU) clustering, direct access storage devices (DASD), array of independent disk drives with redundancy (RAID), and redundant communications with in order to achieve reliability, availability and maintainability. In order to receive at least a "level 1" rating, the telecommunications infrastructure must meet a category recognized by the Uptime Institute or TIA (Telecommunications Industry Association).

A level 1 system must have one inspection hatch and an external cable channel. Access services will be located in one input room. The telecommunications infrastructure will be distributed from the input room to the main distribution area and to the horizontal distribution area throughout the data center through one cable channel. Although logical redundancy (duplication) may be built into the network topology, the level 1 system does not provide for any physical redundancy and any diversification, that is, the introduction of diversity (to increase the system's fault tolerance).

The following are some potential single points of failure of a level 1 system:

- disconnection of the provision of services, disconnection of the central office or disruption of the normal course of work along the length of the access route;

- failure of service provision equipment;

- router or switch failure, if they are not redundant (redundant);

- some critical event in the input room, main distribution area or observation deck may disrupt the normal operation of all telecommunication services for the data center;

- damage to the main line or horizontal cable distribution.

Tier 2 telecommunications infrastructure includes the requirements of Tier 1, as well as additional proprietary requirements. Critical telecommunications equipment, temporarily installed ISP equipment, routers and switches must have redundant components (power supplies). Data center trunk cables running from switches in horizontal distribution zones to trunk switches in the main distribution zone must have redundant fiber optic or copper pairs within a common star configuration. These redundant connections can be in the same or different shells. Logical configurations are possible, they can be in a ring or lattice topology superimposed on a star-type physical configuration. The purpose of level 2 equipment is to reduce the sensitivity (to single faults) of telecommunication services entering the building.

The Level 2 system has two inspection hatches and external cable ducts leading to the system. These two redundant outdoor cable channels will be located in the same input room. It is recommended to physically separate these cable ducts by spacing them at least 20 m apart along the entire length of the route from the reserved inspection hatches to the input room. It is also recommended that these external cable ducts enter the input room from opposite ends. It is not recommended that these redundant outdoor cable trunks enter the system in the same area as this will not provide the recommended distribution along the length of the route. For a system to receive a Level 2 rating (rating), all jumper cables and jumpers must be labeled on both ends of the cable with the name of the connection on both ends of the cable.

Below are some potential single points of failure of a layer 2 system:

- service equipment located in the input room, connected to the same electrical distribution system and supported by the same HVAC components or systems;

- redundant routed and central switched equipment, located in the main distribution area, connected to the same electrical distribution system and supported by the same HVAC components or systems;

- redundant distribution switched equipment located in the horizontal distribution zone, connected to the same electrical distribution system and supported by the same

HVAC components or systems;

- any critical event in the input room or main distribution area can disrupt the normal operation of all telecommunication services for the data center.

A Tier 3 telecommunications infrastructure must meet both Tier 1 and Tier 1 requirements, as well as their additional requirements. The data center must be served by at least two access providers. Services must be provided from at least two different central offices or local access providers. Cable channels from their central offices or local offices must be separated from each other at a distance of at least 29 m along the entire length of the channels, so that these channels can be considered laid on different routes (diversified).

The data center should have two input rooms, preferably on opposite sides of the data center, but the physical distance between these two rooms should be at least 20m. It is not allowed for both rooms to enter access to equipment provided by the rovider, fire protection zones, switchboards and air conditioning systems. The equipment in each input room must be able to continue operating if the equipment in the other input room fails. The server must have duplicate trunk cable channels between the input rooms, the main distribution area and the horizontal distribution areas. Data center trunk cables running from switches in horizontal distribution zones to trunk switches in the main distribution zone must have redundant fiber optic or copper pairs within the overall star configuration. These redundant connections must be in cable sheaths laid along different routes.

A "hot" reserve must be provided for all critical telecommunications equipment, for central routers and switches. All cables, cross panels, and switch cords must be documented using spreadsheets, databases, or programs designed for organizational cable management. Documentation of the cabling system is a mandatory requirement for the data center to be granted the Tier 3 category.

Some of the potential single points of failure of a layer 3 system are listed below:

- any critical event in the main distribution zone can disrupt the normal course of work of all telecommunication services connected to the data center;

- any critical event in the horizontal distribution zone may disrupt the supply of all services to the zone it serves.

Level 4 telecommunications infrastructure must meet all of the above requirements, as well as its own additional requirements. The trunk cabling of the data center must be redundant. Cabling between two spaces must be laid along physically separated routes that coincide only within these two end spaces. Trunk wiring must be protected by laying in a cable conduit or by using cables with locked metal armour. Automatic redundancy should be provided for all critical telecommunications equipment, for equipment, for central routers and switches. Network connections should automatically switch to redundant equipment.

The data center should have a main distribution area and a secondary distribution area, preferably at opposite ends of the data center, but the physical distance between these two spaces should be at least 20m. Joint use of fire protection zones, switchboards and air conditioning systems by the main distribution zone and the secondary distribution zone is not allowed. A secondary distribution area is optional if the engine room is a single continuous space, in which case the introduction of a secondary distribution area is "likely to do little". Each of these zones (main distribution zone and secondary distribution zone) must have its own cable duct to each input room. A cable channel must also be provided between the main distribution zone and the secondary distribution zone. Redundant (redundant) distribution routers and switches must be distributed between the main and secondary distribution areas so that the data center networks can continue to operate if the main distribution area, or the secondary distribution area, or one of the input rooms completely fails.

Each of the horizontal distribution zones must be connected to both the main and secondary distribution zones. Critical systems should have horizontal cabling to two horizontal distribution zones. Duplicate horizontal wiring is optional even for Level 4 systems.

Below are some potential single points of failure of a layer 4 system:

- the main distribution zone (if there is no secondary distribution zone);

- in the horizontal distribution zone and horizontal cable distribution (if duplicate horizontal cable distribution is not installed).

For the design of a new data center, it is necessary to highlight four main criteria, namely:

- power source - electricity distribution, including UPS, standby diesel generator, power distribution unit (PDU) and intermediate distribution units;

- air conditioning and ventilation systems (HVAC) - they can include roof units and distributed units that provide localized air cooling. Air distribution under the floor can be an effective means of evenly distributing air over the entire floor. Additional cooling may be required between racks. The biggest challenge in today's data center is maintaining adequate cooling and ventilation given the intense heat transfer of today's server blades and hardware.

- fire protection systems – including a combination of the most likely fire detection and elimination systems, such as water systems, pre-action systems and dry systems (such as FM 200 and Inergen) for sensitive areas, such as information storage areas (hard drives area);

- security systems - physical access to the server room.

Depending on the strategy for acquiring a new data center (ie, build, buy, lease, or sublease), the level of improvements can vary from a full-on facility to minor modifications and improvements. Critical design considerations include the complete electrical equipment (power structure), including power distribution - ie the main distribution frame (MDF) and intermediate distribution system (IDF); UPS, diesel backup power systems and fire protection systems (ie water and dry systems); security monitoring systems; and mechanical systems (such as HVAK). A pre-action fire extinguishing system, i.e. a gas extinguishing system, is usually required by local fire codes. "Pre-action" means that the sprinkler pipes are charged with air, thereby detecting leaks or other malfunctions. When designing a data center, it is necessary to determine the optimal electrical and air cooling distribution system, based on rack density. The design of the space will focus on the support area, such as conference rooms and delivery rooms, as well as reception and production areas.

When designing a data center, excess capacity should be provided in basic infrastructure such as electrical and cable trenches, patch panels, conduits, and space for additional PDUs. In addition, a plan for the expansion of raised floors and support zones should be developed. But such an option gains the power of expansion if it is a rental property or other areas, such as storage, can be used to expand the space.

The location of the data center will have a significant impact on operational and economic efficiency. In many cases, location criteria will be limited by operational or technical requirements. For example, backup data centers that require synchronous replication will be limited to a radius of 50 to 80 kilometers from the primary data center. Global network costs may also limit the scope of site searches. However, many data centers may be located in remote locations. Thus, steps should be taken to optimize site selection. Critical factors include adequate and reliable capacity and communications infrastructure, favorable labor markets (ie, retention and attrition issues may require special attention), and lower cost real estate markets.

Many municipalities offer grants, tax breaks and other incentives to attract high-tech operations to their communities. IT management must also focus on operational issues such as proximity to support services and public safety services, as well as the level of security at the target location. The location of the data center will have a significant impact on security, operational efficiency and operating costs. Site criteria should include ensuring that there is sufficient distance to the workplace of employees, support workers and other components; sufficient area for parking, storage of water and fuel; space for access to the truck; and locations away from high-risk areas such as airport access corridors, floodplains, and areas prone to natural disasters such as earthquakes, tornadoes, or hurricanes. Avoid collisions near potentially hazardous areas such as cafeterias, machine shops, wet labs, or other areas where fires or mechanical vibrations may occur, all of which pose a risk to data center operations.

It is necessary to choose a site that is far enough from neighboring structures to increase safety. Well removed from main thoroughfares or access streets is a better solution. If it is located in a multi-national building, the ends of the building must be occupied to minimize interference from neighboring tenants. It must be ensured that the site is properly serviced for all essential utilities, including electricity and water. The site plan must provide areas for development and expansion of the parking lot.

Finally, ensure that local codes, building ordinances, and zoning restrictions do not interfere with the intended operation of the data center, such as the operation of diesel generators.

The market always strives for classification and order - and office real estate is no exception. The modern scale of offices includes four classes - A, B, C and D. The last two according to the species scale are the "dying" class: tenants who care about the prestige of the company and the comfort of employees do not like them. But the differences between A and B Classes (taking into account the existence of their internal subgroups + and -) are not so obvious. Moreover, on online sites you can find the same business center, which in one case is indicated as A, and in another as B. Well, "trust, but verify", since the rental rate is directly related to building class.

A reliable assessment of the building requires 20 parameters. If we take into account all 20 parameters, then the condition for assigning the building to class A will be the presence of 16 of them, and to class B - 10. But for convenience, we will highlight and group the main ones:

- location;
- type of building, structural features (including parking), year of construction;
- life support systems;
- planning decisions and processing;
- BC infrastructure;
- security;
- building management.

Both A and B classes assume a favorable location: business districts, high traffic, proximity to transport interchanges and the subway, convenient entrances to the building. However, the "step accessibility" in BC is different: for employees, the difference of 5 and 20 minutes on foot from the subway to the place of work can be a fundamental point. Some owners of Class B buildings get out of the predicament by arranging for delivery by corporate shuttle buses. This is a good move. Among the significant differences, we include the image of the location: there should be no objects that can affect the image (landfills, industrial zones, prisons, etc.) in the vicinity of BCs of classes A and B. For class B, this condition is optional (not mandatory). Regarding the type of building, the differences here are more significant. Class A offices are located in new buildings originally designed as a business center, and class B offices are mainly located in reconstructed buildings or in business centers that have been in operation for more than 5-7 years. This is directly related to engineering and planning solutions, as well as architecture and design. For example, in Class A offices, insolation is better, as the glazing area is larger. A mandatory requirement is the availability of underground or covered parking. The parking ratio is not less than 1:100 m2. For B+ and B- buildings, this indicator is optional. Engineering systems of the building are the "invisible front" on which the comfort of employees directly depends. Class A provides for a central air conditioning system (not lower than two-pipe), uninterrupted power supply (or two independent power sources, at least 70 W per 1 m2), the presence of high-speed elevators with a waiting period of no more than 30 seconds, the establishment of at least two providers.

In modern buildings of Class A, the column pitch is quite wide: this helps to use the useful area as efficiently as possible. In order for the loss factor to be minimal, the building must meet the following parameters:

- have a pitch of columns of at least 8x8m;
- floor area from 1,000m2;
- stairs, elevators and bathrooms are located in the center of the floor;
- the layout of the offices is open.

Permissible values of loss factor for Class A offices are 12-18%, for Class B - no higher than 20%. Translated into financial language, this means that for every 100 square meters of your space, you need to pay for 112 or 120, respectively. The difference is quite obvious. In rooms of class B + and especially B-, office-corridor or mixed planning is often found. In class A premises - open. Preferences here depend only on the requirements of the tenant companies, but it is clear that the loss factor is higher in the first case.

The height of the ceilings should be at least 2.7 m. Here again the A class wins: it usually has this value close to 3 m, and for B class this parameter is optional. High-quality finishing includes suspended ceilings with rational lighting, plastic windows, linoleum or carpet on the floor, wallpaper for painting on the walls. For the convenience of tenants, a dining room or cafe, an ATM and payment terminals should be located in the building. Houses in the B class correspond to this. And the class provides more opportunities: the infrastructure here includes meeting rooms and a conference hall, and additional useful services are located on the first floor - shops, dry cleaners, bank branches, etc. Large shopping centers often have a fitness center in their composition.

A multi-level security system is an indispensable attribute of a prestigious BC. Class A buildings are equipped with automatic fire protection systems and video cameras. All premises, underground and surface parking lots are guarded, access control to the territory and premises is organized. Professional management means no headaches for tenants. Broken faucets, sockets, plumbing equipment - any of these malfunctions are solved promptly, without paralyzing the company's work. The same applies to cleaning and garbage removal. For example:

- in class A premises, the control system is centralized and automated. The management company must serve at least 25,000 m2 of space;

- in B + buildings, a third-party management company or its own operation service is involved;

- in B-buildings, maintenance is carried out by our own service or an outsourced company (at least 2 facilities, each of which has an area of 3,000 m2 or more).

Another important point should be noted. Buildings of classes A and B + must belong to one owner, and the pool of tenants must be balanced. Non-compliance with the "property" criterion is allowed for multifunctional complexes that include office and retail premises or apartments. For class B, this requirement is optional. Therefore, when choosing an office in such a business center, special attention should be paid to the absence of business competitors.

Taking into account the criteria given above, each of the classes A, B, C and D can be briefly characterized. Class A office buildings represent the newest and highest quality buildings on the market. As a rule, such buildings are presented with the best construction and have quality building infrastructure. Class A buildings are also well located, have good access and are professionally managed. As a result, they attract the highest tenants and also receive the highest rents. Class B is the next step down. Class B buildings tend to be a bit older but still have good quality and tenant management. Often, value-added investors target these buildings for investment, as well-located B-grade buildings can regain their A-grade glory with renovations such as improvements to facades and common areas. Class B buildings, as a rule, should not be functionally obsolete and should be in good maintenance. The lowest classification of office buildings and spaces is Class C. These are older buildings that are located in less desirable areas and often require major renovations. Architecturally, these buildings are the least desirable, and the building infrastructure and technology are outdated. As a result, Class C buildings have the lowest rental rates, have the longest leases, and are often targeted as redevelopment opportunities.

The above is only a general guideline for the classification of buildings. There is no official standard for building classification. Homes should be considered in the context of their submarket; that is, a Class A building in one district may not be a Class A building in another. That is why we do not consider class D in more detail, since it does not make any sense. Taking into account all the recommendations, class A offices meet all the requirements of modern business. Class B + is somewhat inferior to them in terms of architectural and planning characteristics, parking lots, and infrastructure. Class B is a good and economical option, if the presentability and prestige of the business center is not a priority, and the tenant can put up with some inconveniences. Since we are planning to design a modern data center with the latest technologies, it was decided to build a data center on the basis of a class A office building.

8.2. Server room design

Organizing a server room is not a cheap process, so before you start designing, you need to decide why you need a server room. It is necessary to highlight the main goals, it depends on them what the server will be. In my opinion, there are three main goals for creating a server room:

- efficient placement of equipment in one place. As a result, in addition to convenience, we will also get an increase in productivity - there is no need to run from floor to floor in search of a specific server;

- protection of "strategic objects" from unauthorized access. Sometimes, a regular cleaning lady can cause damage due to carelessness while cleaning. And in general, it is better if the servers are less noticeable to ordinary users - therefore, if there is not one server, it is desirable to allocate a separate protected room for them;

- protect server equipment from power failures and adverse environmental conditions by maintaining constant climatic conditions inside the server room.

The server room is the "heart" of the functioning of any organization. The security and continuity of the server room affects the successful functioning of the entire office building. Therefore, the protection of this important room should be put on the first plan when organizing the server room. Moreover, this is a complex task, where it is necessary to limit access to the premises and protect the information stored on the hard drives of the server.

Access control systems allow you to limit access to the data center. In order to get into the server room, you need to show your ID (card or finger). Access rights can be assigned to each user, taking into account their area of responsibility and duties. The ACS functionality allows you to additionally implement the function of prohibiting repeated passage, access under duress, implementation of the logic of airlock cabins, forced blocking of all doors, multi-factor access.

There are three types of access control systems:

- based on autonomous biometric/contactless locks;
- based on access control terminals;
- based on access controllers.

When using the access control terminal (Fig. 10), the reading device and the control controller are in a single housing. Usually, you can also connect an additional reader to the terminal to implement two-way access points, a reed switch that monitors the state of the door, an exit button, and a siren. The terminal can be connected to a computer via RS232/485, Usb, Ethernet, Wi-Fi, GPRS interface. Such terminals are used to create one-way, two-way points of passage through doors, or to control turnstiles, gates, airlock cabins. The advantage of access control terminals is the possibility of equipping ACS elements directly at the passage point (all wires are mounted near the door). When creating network access control and control systems, only the communication line with the computer will be remote from the access point. But not always, in cases where there is no Ethernet network outlet near the door or a Wi-Fi network is not deployed at the enterprise.

When using access controllers, the reading device and the control controller are separate elements. Contactless card readers are connected to the controller via the Wiegand interface (up to 100 m), biometric readers - via the RS485 interface (up to 800 m). You can also connect a reed switch that monitors the state of the door, an exit button, a siren, security and fire sensors, and video surveillance cameras to the controller. The controller can be connected to a computer via RS232/485, Usb, Ethernet, Wi-Fi, GPRS interface. The advantage of using access controllers is the possibility of building highly secure access points when the controller and reader are separated and the controller is inside the room; construction of highly intelligent ACS with different operation logic, for example, prohibition of repeated passage, the second door will not open until the first door is closed, video recording of the passage event.

One controller can support up to four doors. When building an ACS with a large number of access points, the use of access controllers is the optimal solution. Access controllers allow you to create integrated security systems. For example, when the ACS is configured with video surveillance systems, security and fire alarms, building energy supply systems. Stand-alone biometric locks are used to create one-way access points based on a fingerprint or a contactless card, in the case of contactless locks, through a door. Access to the server room will be carried out using a fingerprint or a contactless card, the exit is free - by pressing the lock handle down. The advantage of this solution is the high integration of the solution and the absence of the need to lay power lines. An ID reader that closes the mechanism and power from finger batteries is arranged in one lock.

Autonomous biometric locks can be:

- mortise - when the lock is installed without binding to already existing mechanical locks, the element that closes the lock cuts into the door leaf;

- overhead - when the lock is installed without binding to already existing mechanical locks, the element that closes the lock is located on the inside of the lock;

- biometric door handles - the lock controls the tongue of an already existing mechanical lock.

Autonomous electronic locks can also save records of the passage, which can be downloaded to external media and viewed using special software. As a rule, electronic locks allow access to the premises around the clock, without the possibility of binding to temporary access zones. For our data processing center, a server room access system based on autonomous biometric locks was chosen. Namely, ZKTECO HL100 fingerprint biometric lock. The given lock has the following characteristics:

- autonomous lock by fingerprint, code, with the help of a mechanical key;
- number of fingerprint templates and passwords – 100;
- power supply: 4 AA batteries of 1.5V, which are designed for 2000 openings;
- zinc alloy body, steel executive mechanism;
- protection against hacking.

IP video surveillance of the data processing center is designed for high-quality audio and video recording in the server room, control and monitoring using Ethernet and Internet, reliable storage and viewing of the video stream in real time. Information from IP cameras is transmitted to the video server (PC) using digital data transmission channels. IP video surveillance has higher intellectual capabilities compared to analog video surveillance. Modern IP cameras in automatic mode can make different decisions depending on the situation. Built-in video analytics capabilities may include appearance, virtual line, entry, exit, facial recognition, and more. The use of PoE technology (power supply of IP cameras through a standard twisted pair in the Ethernet network) in IP video surveillance of the data center does not require the laying of an electrical cable, which facilitates the process of installation or replacement and simplifies system maintenance.

The advantage of IP video surveillance in the data center:

- video recording in the format from M-JPEG to H.264 with an extension of up to 8 megapixels;
- remote access and multi-user mode;
- video analytics functions built into the IP camera;
- high reliability and safety;
- the ability to transmit a video stream using wireless data transmission technologies;

Functions of video analyst of IP cameras include:

- motion detector;
- recognition of persons;
- crossing the virtual line;
- entry/exit detection;
- detection of appearance/disappearance;
- polygonal privacy masks.

Our server room will be equipped with 10 Cisco 2916 cameras.

A mandatory condition for the organization of a server room is the presence of a false floor that can withstand the load of the installed equipment and the people working with it. The recommended distance between the floor and the false floor is 400 mm, while the distance between the false floor and the ceiling should be at least 2440 mm. The false floor used for server rooms is made of panels that are easily removed and create unobstructed access to the space under the floor. The panels of the false floor are made of a particularly strong material that is difficult to deal with in case of fire and are covered with a wear-resistant coating that has antistatic properties. To install heavy equipment, the construction of the raised floor includes additional elements - stringers, which can significantly increase the strength of the raised floor panels. The false floor, which is strengthened by stringers, can withstand:

- distributed load 4000kg/1m2;
- the maximum point load is 700 kg.

In the server room, a ramp with a slope of no more than 1:10 should be provided for the safe import and export of equipment, as well as the installation of ventilation grills and cable entries for telecommunication racks. A telecommunications or server cabinet is a prefabricated or welded structure and is used to house active and passive server and telecommunications equipment: servers, switches, optical or copper patch panels, hubs, uninterruptible power supplies, etc.

There are wall-mounted and floor-mounted server cabinets.

The height of the server cabinet is measured in units – U (1U = 44.45mm or 1.75 inches). Below are the main purposes of a telecommunications cabinet:

- compact placement of equipment;
- convenience in equipment maintenance;
- provision of conditions for normal operation of the equipment (temperature regime);
- protection against unauthorized access.

According to the design, two types of cabinets are distinguished:

- prefabricated - the advantage of such cabinets is the convenience of transportation to the place of installation and storage, but at the same time it takes time to assemble them;
- welded - their advantage is a rigid design, and therefore a large load capacity. However, transportation and installation of such a cabinet is very inconvenient due to its dimensions and mass.

The size type is characterized by the depth and width of the server cabinet (600x600 mm, 600x800 mm, 800x800 mm, 600x1000 mm) and is chosen taking into account the tasks and the type of equipment installed in the cabinet. Among the server cabinets installed on the floor, the most common is the telecommunications cabinet 42U with a depth of 800 mm. The height of 42U allows you to install a large amount of equipment, while providing good ventilation; the depth of 800 mm makes it possible to install the server in the 19-inch standard. If the depth of the server cabinet is 600 mm, the possibility of installing such equipment is almost 100% excluded, since manufacturers produce a very small number of 19-inch standard servers that can be installed in a 42U server cabinet, which has a depth of 600 mm. Wall-mounted 19-inch server cabinets have a depth of only 600 mm, therefore, it is quite difficult to choose a server for such a cabinet, as described above.

Server and telecommunications equipment will be housed in 19-inch Hyperline TTB closed cabinets:

- height: 42U;
- depth: 910 mm;
- installation method: floor;
- standard of the equipment to be placed: 19";
- front door: perforated steel door;
- design of the front door: perforation 75%, handle with a lock;
- rear door: perforated steel door;
- rear door construction: 75% perforation;
- permissible load: 800 kg;
- construction: prefabricated;
- material: cold-rolled steel.

The choice of such cabinets is associated with a higher degree of protection against physical effects on the equipment. The cabinets will need to be placed in the room in such a way that there is access to their front and back parts. Therefore, each row of server cabinets will be placed at a distance of 1 m, with alternating hot and cold corridors. Cabinets installed in one row will be connected to each other in a single structure with bolts from the sides of the frame. The organization of productive work of the server room is impossible without high-quality protection of the equipment against failures and voltage drops. Hard drives that have failed and the loss of valuable information that is difficult to restore and structure again are the result of savings on the necessary device or the incompleteness of organizational issues.

First of all, let's focus on the type of security guards that can be used to protect servers. It should be noted right away that uninterruptible power supplies such as Back-UPS (reserve architecture) cannot be used - their scope of application is limited to home PCs and workstations, and they are not suitable for such responsible equipment as servers, as they do not provide stabilization of the input voltage and show disappointing results of operation in electrical networks with low power quality. You can use linear-interactive sources equipped with an automatic voltage stabilizer as a power supply for server equipment. In addition to the fact that such devices do not depend on voltage surges and provide a high degree of protection for connected equipment, they also very economically consume the charge and resources of batteries, switching to autonomous power only when there is no power supply in the main network. The most favorable option for servers will be sources of uninterrupted On-line power supply (with double conversion of electricity), which are characterized by zero switching time to work from batteries and ensure truly uninterrupted functioning of the connected equipment. Such DCBs allow you to tightly adjust both the voltage and the frequency of the network and provide the best indicators of availability and performance. Such UPSs are recommended for powering loaded productive servers (file and application), as well as telecommunication systems, network and other equipment that requires increased power quality.

One of the most important parameters when choosing a UPS for a server is the power rating. For modern server equipment, a power source of at least 1000 W will be required, and for integrated systems and cluster groups, a more powerful model - 4-5 kW will be required. In addition, all UPSs are characterized by such an indicator as autonomous operation time at full 100 percent load. Here it is already worth orienting yourself according to the situation, but the most favorable option is a source of uninterrupted power with the possibility of connecting external batteries, choosing the number and capacity of which you can achieve the required duration of the power mode from your own sources of electricity.

UPS for servers must be equipped with an interface for management and monitoring - it can be a USB or RS-232 connector for connecting to a PC and transmitting information about the battery status (charge amount, failure) and network parameters. This is also facilitated by special software, with the help of which the operation of the operating system is terminated and all data is saved in open programs and applications. Many models have an SNMP adapter for remote control and monitoring. With the help of this card, data is collected and stored about the parameters and state of the device, emergency and other critical situations in its operation. An additional plus will be the presence of a network Ethernet connector in the UPS, with the help of which you can organize the protection of the local information and computing network and the active equipment included in it (routers, switches, network adapters) from voltage surges.

Server UPS provide the possibility of installation in a telecommunications cabinet in a vertical position or in a 19-inch mounting rack using a set of guides (Rack version). When connecting several devices to this unit, it is necessary that it has the appropriate number of output power connectors. Advanced models are distinguished by the presence of a power distribution function, that is, individual control of output connectors, which is necessary for independent disconnection of individual load lines to increase the power supply backup time of the most critical equipment and applications. Also, the mentioned function allows you to perform a remote reboot of devices that have been suspended and to carry out their sequential inclusion.

In addition, server UPSs must support "hot" replacement of batteries, so as not to interrupt the supply of electricity, if necessary, remove the battery that has failed and install a new one. Many modern UPSs for the appropriate load, which certainly includes server equipment, are equipped with built-in speakers, which provide sound signals indicating the onset of an emergency situation (overload, lack of voltage in the power grid), and are also equipped with LCD displays. to display this or other critically important information. The Italian company "Riello" is the world leader in the production of UPS for server protection. One of the most popular products of this manufacturer are the devices of the "SDH" series - SDH 1000 and SDH 3000. These devices are built on the basis of digital sinusoidal technology and have high technical characteristics, as well as wide functionality in terms of interaction with connected equipment, collection, transmission and exchange of information, therefore they represent an ideal solution for uninterrupted power supply of critical and loaded server equipment and network systems that require the highest level of protection. In addition, these UPS are famous for the exceptional flexibility of the power supply system, the presence of automatic voltage regulation.

We will use the Riello SDH 3000 UPS to ensure uninterrupted operation of equipment in our data center. UPS with double conversion will provide the highest degree of protection against various failures in the electrical network, as IT systems are completely protected from the influence of the electrical network and are powered directly from the UPS. When using such a UPS, the equipment is protected from problems related to voltage drops, power outages, and other possible power grid failures. Characteristics:

- load power 2700W;
- input voltage: 140-300V;
- output voltage: 220/230/240V;
- power factor: 0.9;
- availability of battery: yes.

In the event of a power outage, our server room will be powered from a backup source - a 5 kW gasoline generator, which is automatically turned on when the mains voltage goes out. During the period of time required to start the generator, server equipment is supported by an uninterruptible power supply of the linear-interactive type connected after the generator. At the current stage of the development of information technologies, it is possible to cool the data center on one of three levels: the computer room, the row and the rack. Each of these approaches has its advantages and disadvantages. Historically the first and still one of the most popular approaches to cooling data centers is hall-level air conditioning. In this case, one or more large precision air conditioners are installed, which supply cooled air to the hall and remove heated air.

Streams of cooled air in this case can be supplied directly to the general space of the hall or distributed in cold corridors or directed to specific racks with the help of a false floor through perforated tiles. In the first case, the efficiency of the cooling system, as a rule, does not exceed 1-3 kW per rack. The use of a false floor increases this figure to 5 kW. To enhance the effect, special fans can be installed in individual racks that increase the air flow in a specific cabinet. The efficiency of such a system can reach 8 kW per rack, but its use is associated with a number of difficulties, in particular, increased local selection of cooled air in one point of the data center can lead to its deficiency in another area, as a result of which some racks may overheat. Moreover, in certain points of the false floor, due to turbulence, zones of negative pressure may even appear, which will lead to the suction of air from the room under the false floor. And if the speed of the air flow will be too high, for example, in the air conditioner itself, then the fans of the active equipment will simply not be able to suck it physically. With competent design, these problems can be circumvented, since often not all racks require the same cooling (for example, those cabinets where switching equipment is installed, in this case, require less cooling).

One of the disadvantages of hall-level cooling is that hot and cold airflows mix, reducing the overall efficiency of the cooling system. It should be noted that a significant part of the air coming out of the air conditioners bypasses the computer equipment and immediately returns to the cooling unit. As a result, it is not possible to use the entire capacity of the air conditioner. Note that the cooling capacity of such systems reaches 150 kW and above. To prevent the mixing of air flows, it is possible, with the help of special ducts, to organize the removal of hot air from the racks not just into the hot corridor, but immediately into the exhaust ventilation system of the building. At the same time, hood nozzles should be located above the hot corridor. This approach allows you to remove up to 10 kW of heat from each rack. For more efficient work, special doors are used, which are installed on the back wall of the cabinet. They isolate the heated air emission zone, which enters the exhaust ventilation system through a special hermetic air passage. As a rule, such doors have built-in fans that increase air flow, or even heat exchangers. In the case of using a scheme with such flow amplifiers, the efficiency of the cooling system can increase to 20 kW.

A data processing center is a specialized room where expensive large telecommunications and server equipment is located. The area of the server room is equipped with automatic gas fire extinguishing systems in accordance with established standards. Due to the fact that it is forbidden to use powder, water and other types of fire extinguishers in server rooms, special gases with unique properties that do not support combustion are used as fire extinguishing substances. The automatic gas fire extinguishing system for the server room ensures the preservation and operability of expensive server equipment. Fire localization using traditional methods in server rooms using water, fire extinguishers, and special powders is not the best solution.

The active substance in the form of powders or aerosols does not have the opportunity to penetrate directly to the flash point if it is in a hard-to-reach place, for example, inside a server cabinet. The powder settles on the outer surface, the fire continues to spread inside, while the command and control device received a signal that the fire extinguishing system has successfully worked.

Expensive server equipment becomes unusable when foam active components are used, causing huge damages that are equal to colossal losses due to fire. Automatic gas fire extinguishing systems are the most favorable when fighting fires that occur in server rooms. When designing and installing fire protection systems in server rooms, it is necessary to ensure that the following conditions are met:

- reliable back-up supply of electrical power to the fire protection system;
- equipment of a separate air duct, equipped with a valve for resetting the excess pressure of the supplied gas;
- unlocking the entrance door for the free exit of service personnel;
- reliable grounding of gas pipelines.

The device that manages and controls the fire extinguishing system and door opening is placed on the wall outside the protected server premises. Its work is carried out both in automatic and manual modes.

When plastic, cable braiding is smoldering or catching fire, there is no significant increase in temperature, smoke is the main signal that informs about fire danger. In server rooms, it is necessary to install smoke detectors, which are related to detectors for early detection of ignition sources. When several smoke detectors are triggered, the control device includes gas fire extinguishing for the server room.

In connection with the fact that stopping servers leads to economic losses, in specialized premises it is necessary to eliminate dangerous sources of fire without necessarily shutting down working equipment. Fire-extinguishing substances must have dielectric properties that allow them to be used when extinguishing server equipment under a voltage of up to one thousand watts.

Gas fire extinguishing for the server room must be designed for the fact that there are people in the room - service personnel, visitors. In this regard, automatic activation of the fire extinguishing system is unacceptable, in such a case, maintenance of server equipment must be carried out in manual mode. The automatic gas fire extinguishing system is used in server rooms that function without the participation of a person in the middle.

The automatic gas fire extinguishing system (Fig. 20) includes the following elements:

- pipelines supplying the active gaseous substance;
- control and management device;
- gas cylinders;
- fire detectors and alarms.

Highly sensitive sensors for early fire detection are the main components of the fire extinguishing system. In order to ensure quality control and quickly determine the source of smoke, active air sampling and analysis is carried out. Accelerated detection of fires also reduces operating costs. It is possible to eliminate the fire with the help of manual fire extinguishers. At the same time, we prevent the leakage of expensive fire extinguishing agent and prevent gas cylinders from being overcharged.

The latest automatic fire extinguishing systems use various gaseous fire-extinguishing substances:

- carbon dioxide - has an average efficiency, has an aggressive effect on equipment that protects against fire, is prone to losses, is harmful to people, the use of this component in installations with automated control is prohibited;
- inergen gas is a safe material for the human body, its efficiency is higher compared to carbon dioxide;
- refrigerators are presented in various modifications, which have a high degree of fire extinguishing efficiency.

Gas cooler 125 is rarely used in server rooms due to the fact that after its use, traces remain on the external surfaces of the equipment in the form of a white coating, which can later cause corrosion of metal objects.

The most favorable option is the gas refrigerator 127 - thanks to the ideal combination of factors such as quality, price, and efficiency. NOVEK 1230 (dry water) is a representative of a new generation of the most effective fire-extinguishing gaseous substances. It is characterized by a high rate of spread over the area of the room, the absence of negative effects on people and equipment, and it is safe for the ozone layer.

Conclusions

In this work, the main issues related to the construction of a server room were considered. Based on the requirements for the design of the server room, the optimal dimensions of the future server room were chosen, and the characteristics were chosen for the area from 14 m2 to 36 m2. The room will have the shape of a rectangle, close to a square. We also chose a room with a ceiling height of 2.8 m, based on the fact that a false floor will also be installed in the data center. Server and network equipment will be housed in 19-inch closed Hyperline TTB cabinets. The choice of such cabinets is associated with a higher degree of protection against physical effects on the equipment. The cabinets will need to be placed in the room in such a way that there is access to their front and back parts. Therefore, each row of racks will be placed at a distance of 1 m, with alternating hot and cold corridors. Cabinets installed in one row will be connected to each other in a single structure with bolts from the sides of the frame. Attention was also paid to both physical and fire protection of the server room. So, in terms of physical access, the server room will be protected by ZKTECO HL100 fingerprint biometric lock. The choice of such a lock is associated with ease of installation and reliable protection against unauthorized access. In addition to the biometric scanner, the server room will also be equipped with a video surveillance system. Sufficient attention was also paid to the fire safety system. So, to prevent damage to server equipment, a gas fire extinguishing system was chosen. This system is equipped with an interactive fire detection system, based on the analysis of the air carried out by the sensors of this system. Several Riello SDH 3000 uninterruptible power supplies were chosen for reliable and productive power supply of the server room. The uninterruptible power supplies will be able to keep the server room powered for 20 minutes, which is enough to start the gasoline generator. The cooling system of the server room was considered. There are a number of ways to cool a server room, including cooling with local air conditioners. But in our case, the cooling system of the entire server room was chosen, by alternating cold and hot corridors, as well as supplying cold air through the false floor.